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 wichtigster IT-Systeme und Applikationen 146
10.4 Notbetrieb implementieren 146
10.5 Infrastruktur im Notbetrieb 147
10.6 Beweissicherung im Notbetrieb 149
10.7 Notbetrieb durchführen 149
10.8 Beispielhafter Ablauf 149

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

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

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

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

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

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

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

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

Teil III Ich will nicht, dass es passiert!

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

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

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

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

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

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

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

Teil IV Was wird uns die Zukunft bringen?

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

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

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 obfuskiert 73

Abb. 5.6 Excel 4.0 Makro obfuskiert 74
Abb. 5.7 Protected-View-Banner 74
Abb. 5.8 Minimaler VBA-Dropper, nicht obfuskiert 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, *TCP* Transmission Control Protocol, *DoH* DNS over HTTP/S, *LDAP* 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:

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

F. Oelmaier et al., *Krisenfall Ransomware*, Edition <kes>,
https://doi.org/10.1007/978-3-658-41614-0_1

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,
Prokurist, Leiter IT-Sicherheit & Computerkriminalität, IT-Krisenmanagement
Uwe Knebelsberger, 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 Herkunftsländer 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

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

F. Oelmaier et al., *Krisenfall Ransomware*, Edition <kes>,
https://doi.org/10.1007/978-3-658-41614-0_2

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 Angriffsdauer (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.