Ransomware und Cyber-Erpressung

Das Praxishandbuch für IT- und Systemverantwortliche

1 Auswirkungen

Ach, was ist schon eine kleine Erpressung unter Freunden?
– Bill Watterson

Lernziele

- Digitale Erpressung definieren und deren vier Arten (Enthüllung, Modifikation, Zugriffsverweigerung und Pseudo-Erpressung) erläutern
- Die Auswirkungen digitaler Erpressung auf moderne Organisationen verstehen
- Erkennen, dass Angreifer Technologiezulieferer nutzen können, um Opfer zu kompromittieren und digitale Erpressung im großen Stil durchzuführen

Unternehmen X war eine florierende Wirtschaftsprüfungsgesellschaft. Der Hauptsitz befand sich in einer großen amerikanischen Stadt. Jeden Tag übernahmen die Mitarbeiter die Buchhaltung, Finanzaufsicht, Steuervorbereitung und eine Vielzahl weiterer Aufgaben für hunderte von Kunden.

An einem Montagmorgen war plötzlich alles vorbei. Ein früh im Büro eingetroffener Mitarbeiter hörte furchterregenden Lärm. Jeder Computer schrie eine Nachricht: »Achtung! Was ist passiert? All Ihre Dateien, Dokumente, Fotos, Datenbanken und andere wichtige Daten wurden mit bewährten Algorithmen sicher verschlüsselt. Sie können im Moment nicht auf die Dateien zugreifen. Doch keine Sorge. Sie haben eine Chance!«

Überall im Büro lag Papier herum. Alle Drucker hatten die Lösegeldforderung ausgedruckt, bis die Papierschächte leer waren. Die von den Mitarbeitern zur Verarbeitung von Kreditkarten genutzten Kassensysteme hatten die Lösegeldforderung auf Quittungen ausgedruckt, bis die Tische überquollen.

Eine kühle Voicemail erwartete einen der Gesellschafter: »Hallo, Herr [ZENSIERT],« begann eine emotionslose männliche Stimme mit osteuropäischem Akzent, »ich möchte Sie darüber informieren, dass wir 500 Gigabyte Daten von Ihren Servern heruntergeladen haben. Falls Sie planen, Ihre Daten wiederherzustellen, ohne für die Entschlüsselung zu bezahlen, werden wir Ihre Unternehmensda-

ten im Darknet verkaufen. Wenn Sie uns nicht SOFORT kontaktieren, werden wir Ihre Kunden darüber informieren, dass wir im Besitz ihrer privaten Daten wie Sozialversicherungsnummern und Steuerformulare sind. Wir empfehlen Ihnen dringend, sich mit uns in Verbindung zu setzen. Eine E-Mail-Adresse haben wir in der Textdatei auf Ihrem Desktop hinterlassen.«

Nach einer kleinen Kunstpause fuhr die Stimme fort: »Wenn wir diese Daten veröffentlichen, ist Ihr Unternehmen so gut wie am Ende. Wir freuen uns auf Ihre Antwort per E-Mail.« Klick. Damit endete die Voicemail.

Die Kriminellen verlangten 1,2 Millionen US-Dollar für die Wiederherstellung des Zugriffs und dafür, die Kundendaten nicht zu veröffentlichen.

In der Zwischenzeit lag das Unternehmen brach. Datenbanken mit Kundendaten waren vollständig verschlüsselt und nicht nutzbar. Mitarbeiter hatten keinen Zugriff auf Netzwerkfreigaben, einschließlich der Kundendaten, Gehaltsabrechnungen, Personaldaten und vielem mehr. Alle Kunden, die auf die tägliche Buchhaltung oder auf zeitkritische Dienste angewiesen waren, waren aufgeschmissen.

Glücklicherweise funktionierte die cloudbasierte E-Mail des Unternehmens noch – und auch das nutzten die Kriminellen aus. »Guten Morgen«, schrieben sie in einer nachfolgenden E-Mail. »Ich denke, Sie verstehen immer noch nicht, in welcher Situation sich Ihr Unternehmen befindet. … Zunächst verkaufen wir die persönlichen Daten aller Mitarbeiter und Kunden auf dem Markt. … [Sie] werden sowohl von Ihren Mitarbeitern als auch von Ihren Kunden verklagt.« Die Kriminellen hängten die persönliche Steuererklärung des Mitgesellschafters an, um die Gefahr zu verdeutlichen.

Es war schnell klar, dass die Kriminellen auch die E-Mail-Accounts des Unternehmens geknackt hatten und die Antworten des Opfers überwachten. »Wir haben den Report Ihres [Antivirus-Anbieter] gesehen«, schrieben die Kriminellen. »Er enthält viele Fehler.«

Die Kriminellen folgten einem standardisierten Vorgehen. Tagein, tagaus nahmen sie das Internet nutzende Unternehmen in Geiselhaft. Zuerst verschafften sie sich Zugang zum Netzwerk der Opfer. Bei Unternehmen X trat der initiale Hack im Mai auf, als ein Mitarbeiter einen Anhang in einer Phishing-E-Mail öffnete. Der Computer des Mitarbeiters wurde mit Malware infiziert, genauer gesagt mit einem Trojaner für den Remote-Zugriff (bekannt als »RAT«), der den Kriminellen den entfernten Zugriff auf den Computer des Mitarbeiters ermöglichte. Die Antivirensoftware von Unternehmen X erkannte die Infektion nicht. Die Kriminellen lauschten etwa drei Monate lang. Gelegentlich loggten sie sich am Computer des Mitarbeiters ein. Wahrscheinlich wollten sie prüfen, ob der Zugang immer noch funktionierte, ansonsten taten sie aber nicht viel. Es ist möglich, dass die Kriminellen in dieser Zeit mit den Zugangsdaten für den gehackten Computer im Darknet hausieren gingen. Als »Initial Access Broker« bezeichnete Hacker sind darauf spezialisiert, sich Zugang zu Computern zu verschaffen. Sie verkaufen den Zugang an andere Kriminelle und schlagen so schnell Kapital aus

ihrem Verbrechen. Die Käufer – häufig organisierte kriminelle Gruppen – gehen dann den nächsten Schritt, spionieren das Netzwerk des Opfers aus und versuchen dann Lösegeld zu erpressen.

Im August loggten sich dann plötzlich Kriminelle, die später als die Ransomware-Gang »Twisted Spider«[1] identifiziert wurden, auf dem infizierten Computer des Mitarbeiters ein. Mittels gängiger Pentest-Tools stahlen sie die Passwörter des Computers, darunter auch den Benutzernamen und das Passwort des MSP (Managed Services Provider), der die Computer des Unternehmens per Fernwartung administrierte. Mit diesen Anmeldedaten konnten sie die vollständige Kontrolle über das Netzwerk von Unternehmen X übernehmen.

Die Twisted Spider Gang kam direkt zur Sache: Sie kopierten alle Dateien aus dem primären Datenrepository des Unternehmens und installierten dann eine schnelle und effektive Ransomware, die alle Server des Unternehmens verschlüsselte, inklusive der Datenbanken, Anwendungsserver, Domain Controller und mehr. Die Arbeitsplätze blieben außen vor. Um einzelne Accounts oder Computer kümmerte man sich gar nicht erst. Es war ein sauber ausgeführter Blitzeinbruch.

Die Kriminellen kannten die Achillesferse ihres Opfers. Sie wussten, dass schon die kurzfristige Unterbrechung des Geschäftsbetriebs wirkungsvoll war, doch viel verheerender waren die langfristigen Konsequenzen durch verärgerte Kunden, deren Daten gestohlen wurden. Die Twisted-Spider-Hacker demonstrierten, dass sie Zugang zu sensiblen, regulierten Daten wie Sozialversicherungsnummern und Steuerdaten hatten. Sie wiesen die leitenden Mitarbeiter des Opfers explizit darauf hin, dass sie von Angestellten und Kunden verklagt werden könnten. Sie machten klar, dass sie darauf vorbereitet waren, die Daten zu veröffentlichen und die Kunden direkt zu kontaktieren, um der Reputation des Unternehmens zu schaden. Das hätte wiederum zu Geschäftseinbußen und Gerichtsverfahren führen können. Für das Unternehmen ging es also ums nackte Überleben.

Unternehmen X, oder besser gesagt ihre Cyberversicherung, zahlte das Lösegeld, abzüglich einer Selbstbeteiligung von 25.000 US-Dollar. Die Autoren dieses Buches wurden mit den Verhandlungen betraut. Sie konnten einen hohen Preisnachlass aushandeln und den Fall für etwas weniger als 600.000 US-Dollar beilegen. Wie nicht anders zu erwarten gab Twisted Spider während der Verhandlungen Insiderinformationen preis: Unternehmen X hatte eine Versicherungspolice mit einer Ransomware-Grenze von 600.000 US-Dollar.

Sobald Twisted Spider den Zahlungseingang (in Form einer Kryptowährung) verifiziert hatte, lieferten die Kriminellen vorkonfigurierte Software zur Entschlüsselung der Dateien und »bestätigten« per Chat, dass sie die Daten gelöscht hätten. Sie lieferten per E-Mail sogar eine vollständige Liste aller angeblich ge-

1. Jon DiMaggio, Ransom Mafia: Analysis of the World's First Ransomware Cartel (Analyst1, 7. April 2021), *https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-Ransomware-CARTEL.pdf*.

löschten Dateien, wahrscheinlich um das Opfer mit einer Dokumentation zu versorgen, die die Kunden beschwichtigen bzw. die Notwendigkeit einer (Selbst-)Anzeige abwenden sollte. Allerdings erachteten die Cyberanwälte von Unternehmen X die Anzeige aus rechtlichen und ethischen Gründen für notwendig.

1.1 Eine Cyberepidemie

Unternehmen X war nicht das einzige, das unter einem solchen Angriff zu leiden hatte. Tausende (wenn nicht Millionen) von Organisationen wurden über das letzte Jahrzehnt mit digitaler Erpressung konfrontiert. Was als neuartiges Verbrechen begann, ist heute Alltag – mit hohen Kosten für die Gesellschaft.

Digitale Erpressung hat Krankenhäuser lahmgelegt, Schulschließungen erzwungen, die Nahrungsmittelversorgung unterbrochen und sogar zu massiver Treibstoffknappheit geführt. Heutzutage laufen über die technischen Lieferketten tausende Ransomware-Angriffe gleichzeitig ab.

Die durch Ransomware verursachten Kosten sollen 2021 20 Milliarden US-Dollar erreichen und laut des Forschungsunternehmens Cybersecurity Ventures[2] bis 2031 auf 265 Milliarden US-Dollar ansteigen. In einer globalen Umfrage gaben 37 % der Organisationen an, im Jahr 2020 von Ransomware-Angriffen betroffen gewesen zu sein[3], auch wenn sich das tatsächliche Ausmaß des Problems kaum abschätzen lässt, da viele Opfer die Verbrechen nicht melden.[4]

Durch ihren Erfolg beflügelt, haben Cyberkriminelle in immer ausgefeiltere Techniken und Geschäftsmodelle digitaler Erpressung investiert. Aus kleinen, einmaligen Angriffen ist ein florierendes kriminelles Geschäft mit Lizenznehmern, Tochterunternehmen, spezialisierter Software und benutzerfreundlichen Strategiebüchern (Playbooks) erwachsen.

Auch die Verteidiger müssen ihre Bemühungen erhöhen. Durch digitale Erpressung verursachte Schäden lassen sich deutlich reduzieren oder sogar verhindern, wenn bei Anzeichen für einen Angriff schnell und strategisch gehandelt wird. Da sich die Taktiken digitaler Erpressung schnell ändern, müssen sich auch die Taktiken der Verteidiger fortlaufend anpassen.

In diesem Kapitel schaffen wir die Grundlagen, indem wie die Auswirkungen digitaler Erpressung betrachten und verstehen, wie diese Art der Kriminalität entstanden ist. Wir diskutieren die Fortschritte der Schlüsseltechnologien, die die Verbreitung von Ransomware und anderen Formen digitaler Erpressung beson-

---

2. David Braue, »Global Ransomware Damage Costs Predicted to Exceed $265 Billion by 2031«, Cybercrime Magazine, 2. Juni 2022, *https://cybersecurityventures.com/global-Ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/*.
3. Sophos, The State of Ransomware 2021, 2021, *https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-Ransomware-2021-wp.pdf*.
4. Danny Palmer, »Ransomware Victims Aren't Reporting Attacks to Police. That's Causing a Big Problem«, ZDNet, 5. Oktober 2020, *www.zdnet.com/article/Ransomware-victims-arent-reporting-attacks-to-police-thats-causing-a-big-problem/*.

ders begünstigt haben. Moderne Cybererpresser-Gangs verwenden skalierbare Geschäftsmodelle, die häufig Partner und Spezialisten einbinden und die Veröffentlichung von Daten verstärkt als Druckmittel einsetzen. Wir schließen das Kapitel mit der Analyse des Geschäftsmodells digitaler Erpressung der nächsten Generation ab, was den Rahmen für die Reaktions- und Präventionstaktiken bildet, die wir in diesem Buch vorstellen.

1.2 Was ist Cybererpressung?

Definition: Cybererpressung

Cybererpressung ist ein Angriff, bei dem der Täter versucht, an etwas von Wert zu gelangen, indem er die Vertraulichkeit, Integrität und/oder Verfügbarkeit informationstechnischer Ressourcen bedroht.

Erpressung hat sich als Verbrechen allmählich gemeinsam mit der Menschheit entwickelt. Sie beschreibt den Akt, etwas von Wert »durch Gewalt, Einschüchterung oder unzulässige bzw. illegale Mittel«[5] zu erlangen. Während sich das Internet weiterentwickelte und Organisationen auf der ganzen Welt immer abhängiger von den Computerressourcen wurden, passten Cyberkriminelle alte Taktiken an diese neue digitale Welt an.

1.2.1 Die CIA-Triade

Um Druck zu erzeugen, greifen die Täter eines oder mehrere Sicherheitsziele für Informationen und Informationssysteme an, die durch den Federal Information Security Management Act (FISMA) von 2002 definiert wurden:

- Vertraulichkeit (Confidentiality)
- Integrität (Integrity)
- Verfügbarkeit (Availability)

Umgangssprachlich werden diese drei Ziele als »CIA-Triade« bezeichnet.[6] Die CIA-Triade wurde gezielt für den Einsatz bei Behörden, Lieferanten und Vertragsnehmern des Bundes entworfen, wurde aber von anderen Unternehmen und der Informationssicherheits-Community übernommen. Auch wenn digitale Erpressung jedes der drei CIA-Ziele verletzen kann, haben die heutigen Gegenspieler üblicherweise die Vertraulichkeit und Verfügbarkeit im Visier.

---

5. »Extortion«, Merriam-Webster, *www.merriam-webster.com/dictionary/extortion*.
6. »Standards for Security Categorization of Federal Information and Information Systems«, National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory, Februar 2004, *https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf*.

1.2.2 Arten digitaler Erpressung

Digitale Erpressungsversuche fallen in eine von vier Kategorien: Enthüllung, Modifikation, Zugriffsverweigerung und Faux:

- **Enthüllung** greift die Vertraulichkeit der Informationen an. Zum Beispiel kann ein Täter die Daten eines Opfers stehlen und damit drohen, diese zu veröffentlichen, wenn kein Lösegeld gezahlt wird.
- **Modifikation** greift die *Integrität* der Informationen an. Ein Täter könnte Schlüsselelemente der Daten einer Organisation verändern, etwa Patientendaten oder Banktransaktionen. Er könnte anschließend eine Zahlung dafür verlangen, die Daten wiederherzustellen oder die Änderungen zu dokumentieren.[7] Während diese Zeilen geschrieben werden, ist diese Art des Angriffs selten, doch die Angreifer könnten entscheiden, sie zukünftig verstärkt einzusetzen, wenn skalierbare Werkzeuge zur Modifikation verfügbar werden.
- **Zugriffsverweigerung** zielt auf die *Verfügbarkeit* der Informationen ab. Ransomware-Angriffe sind das gängigste Beispiel für einen solchen Angriff. In diesen Fällen verschlüsselt der Angreifer die Dateien des Opfers und verweigert die Freigabe des Entschlüsselungsschlüssels, bis ein Lösegeld gezahlt wird. Distributed-Denial-of-Service(DDoS)-Angriffe werden ebenfalls verwendet, um den Druck auf die Opfer zu erhöhen.[8,9]
- **Faux** ist ein Angriff, der eine digitale Erpressung zu sein scheint, tatsächlich aber keine ist. Beispielsweise hat sich die destruktive Malware »NotPetya« als Ransomware getarnt, war aber tatsächlich so entworfen, dass sie die Systeme der Opfer ohne Hoffnung auf Wiederherstellung zerstört hat. (Details zu den NotPetya-Angriffen finden Sie in Kapitel 7.)

7. »Enterprise Ransomware«, CyberCube, 2022, *https://insights.cybcube.com/enterprise-Ransomware-report*.
8. Lance Whitney, »How Ransomware Actors Are Adding DDoS Attacks to Their Arsenals«, TechRepublic, 2. Juni 2021, *www.techrepublic.com/article/how-Ransomware-actors-are-adding-ddos-attacks-to-their-arsenals/*.
9. Lawrence Abrams, »Ransomware Gangs Add DDoS Attacks to Their Extortion Arsenal«, Bleeping Computer, 1. Oktober 2020, *www.bleepingcomputer.com/news/security/Ransomware-gangs-add-ddos-attacks-to-their-extortion-arsenal/*.

Die »Täter«

- Wenn wir in diesem Buch von »Täter« sprechen, fassen wir alle Akteure zusammen, die an einem digitalen Erpressungsversuch beteiligt sind, nicht notwendigerweise einen einzelnen Akteur.
- Moderne digitale Erpressungsversuche verlangen häufig unterschiedliche Akteure. Zum Beispiel könnte ein »Initial Access Broker« den ersten Zugang zum Netzwerk des Opfers erlangen[10] und diesen dann an andere Täter verkaufen oder vermieten.
- Cybererpresser können Angestellte oder freie Mitarbeiter beschäftigen, die über spezielle Fähigkeiten verfügen und bei verschiedenen Stufen eines Angriffs zum Einsatz kommen. Der Einfachheit halber fassen wir all diese Akteure in diesem Buch als »Täter« zusammen.

1.2.3 Multikomponenten-Erpressung

Die Täter kombinieren vermehrt mehrere Formen der Erpressung, um ihre Gewinnchancen zu maximieren. Gegen Ende 2019 ebnete die Maze-Gruppe den Weg für den »Doppelerpressung«-Trend (engl. Double Extortion), bei dem Ransomware und die Enthüllung von Daten kombiniert wurden. Der Begriff »Doppelerpressung« beschreibt die Nutzung zweier unterschiedlicher Taktiken der digitalen Erpressung, etwa die Zugriffsverweigerung und die Enthüllung. Das erhöht den Druck durch den Täter und kann zu einer höheren Zahlung des Opfers führen.

Andere Gruppen wie RagnarLocker, Avaddon und SunCrypt haben DDoS-Taktiken mit traditioneller Ransomware oder Enthüllungsangriffen kombiniert.[11,12] So startete beispielsweise im Oktober 2020 die SunCrypt-Gang beim Angriff auf einen Hersteller von Haushaltsgeräten einen DDoS-Angriff gegen das Netzwerk des Opfers, nachdem die Ransomware-Verhandlungen ins Stocken gerieten. Laut eines durchgesickerten Transkripts schrieben die Kriminellen: »Wir befanden uns in Verhandlungen, und Sie haben nicht mehr reagiert, weshalb weitere Aktionen durchgeführt wurden.«[13]

Wir diskutieren die Ausweitung der Erpressungstaktiken ausführlich in Kapitel 2.

---

10. Victoria Kivilevich and Raveed Laeb, »The Secret Life of an Initial Access Broker«, KELA, 6. August 2020, *https://ke-la.com/the-secret-life-of-an-initial-access-broker/*.
11. Lawrence Abrams, »Another Ransomware Now Uses DDoS Attacks to Force Victims to Pay«, Bleeping Computer, 24. Januar 2021, *www.bleepingcomputer.com/news/security/another-Ransomware-now-uses-ddos-attacks-to-force-victims-to-pay/*.
12. Sean Newman, »How Ransomware Is Teaming up with DDoS«, Infosecurity Magazine, 18. Juni 2021, *www.infosecurity-magazine.com/opinions/Ransomware-teaming-ddos/*.
13. Newman, »How Ransomware Is Teaming up with DDoS«.

1.3 Auswirkungen moderner digitaler Erpressung

Cybererpressung kann Organisationen ernsthaften Schaden zufügen. Die Auswirkungen können Betriebsunterbrechungen, finanzielle Einbußen, Reputationsverlust und Gerichtsverfahren sein. Aber auch Dominoeffekte für Mitarbeiter, Kunden, Aktionäre und die größere Gemeinschaft sind möglich.

In diesem Abschnitt diskutieren wir die negativen Effekte digitaler Erpressung und schaffen die Grundlagen für Reaktion und Schadensminderung.

1.3.1 Betriebsunterbrechung

Zu den kurzfristigen Auswirkungen digitaler Erpressung zählen partielle oder vollständige Betriebsunterbrechungen. Das ist insbesondere dann der Fall, wenn die Täter Verweigerungstaktiken wie Ransomware oder DDoS-Angriffe nutzen.

So war beispielsweise das kalifornische Gesundheitssystem Scripps Health im April 2021 von einem Ransomware-Angriff betroffen, bei dem der Zugriff auf die elektronischen Gesundheitsdaten für fast vier Wochen unterbrochen war. Während dieser Zeit mussten viele Patienten in andere Einrichtungen verlegt und viele (nicht so dringende) Termine verschoben werden.[14] Später in diesem Sommer ließen mit der Ransomware-Gang REvil verbundene Hacker Ransomware bei 1.500 Organisationen auf der ganzen Welt platzen, die Schwachstellen in der beliebten Remote-Management-Software Kaseya ausnutzten.[15] Infolgedessen war die schwedische Lebensmittelkette Coop gezwungen, hunderte Filialen zu schließen. Die Lebensmittel verdarben und das Unternehmen hatte erhebliche Einnahmeverluste.[16]

In einer kürzlich durchgeführten Umfrage gab ein Viertel der Unternehmen an, dass sie den Betrieb aufgrund eines Ransomware-Angriffs zumindest teilweise einstellen mussten.[17] 29 % mussten nach Aussagen des Sicherheitsunternehmens Cybereason Personal entlassen.[18] Statistiken zu den Ausfallzeiten variieren stark, doch nach der Erfahrung der Autoren dauert die partielle Wiederherstellung üblicherweise zwischen zwei und fünf Tage. Die Wiederaufnahme des Normalbetriebs dauert zwei bis vier Wochen.

---

14. »147,000 Patients Affected by Scripps Health Ransomware Attack«, HIPAA Journal, 3. Juni 2021, *www.hipaajournal.com/147000-patients-affected-by-scripps-health-Ransomware-attack/*.
15. Liam Tung, »Kaseya Ransomware Attack: 1,500 Companies Affected, Company Confirms«, ZDNet, 6. Juli 2021, *www.zdnet.com/article/kaseya-Ransomware-attack-1500-companies-affected-company-confirms/*.
16. Lawrence Abrams, »Coop Supermarket Closes 500 Stores After Kaseya Ransomware Attack«, Bleeping Computer, 3. Juli 2021, *www.bleepingcomputer.com/news/security/coop-supermarket-closes-500-stores-after-kaseya-Ransomware-attack/*.
17. Ransomware: The True Cost to Business (Cybereason, 2021), S. 14, *www.cybereason.com/hubfs/dam/collateral/ebooks/Cybereason_Ransomware_Research_2021.pdf*.
18. Ransomware: The True Cost to Business, S. 12.

Die gute Nachricht (wenn man es so nennen will) ist, dass laut einer 2021 vom Sicherheitsunternehmen Sophos durchgeführten Umfrage 96 % der Ransomware-Opfer zumindest einen Teil ihrer Daten zurückerhalten haben, sei es durch Wiederherstellung aus Datensicherungen, durch von den Tätern bereitgestellte Dekryptoren oder auf andere Weise. Doch es gibt einen Haken: Die Opfer, die Lösegeld gezahlt hatten, konnten im Schnitt nur 65 % ihrer Daten wiederherstellen. Gerade mal 8 % der befragten Opfer konnten alle Daten wiederherstellen.[19] Permanenter Datenverlust kann zu Fehlern und zu vielen Jahren zusätzlicher Arbeit führen.

Definition: Dekryptor

Der Begriff »Dekryptor« beschreibt die Software, die die Daten entschlüsselt, die durch den Ransomware-Angriff verschlüsselt wurden. Zwar steht dieser Begriff (während diese Zeilen geschrieben werden) noch nicht im Wörterbuch, er ist aber bei Ransomware-Response-Profis üblich, weshalb wir ihn in diesem Buch verwenden. Ransomware-Dekryptoren können über verschiedene Quellen bezogen werden, z. B. als freie Dekryptoren von Sicherheitsanbietern, von Behörden oder Strafverfolgern entwickelte experimentelle Utilities oder als von den Tätern im Gegenzug für das Lösegeld erhaltene Software.

Durch Ransomware-Angriffe können Unternehmen sogar pleitegehen. 2019 musste der amerikanische Gesundheitsdienstleister Wood Ranch Medical seine Türen für immer schließen, nachdem ein Ransomware-Angriff alle Patientendaten verschlüsselt hatte. »Unglücklicherweise war der Schaden an unserem Computersystem so hoch, dass wir die dort gespeicherten Daten nicht wiederherstellen konnten. Da unser Backup-System ebenfalls verschlüsselt wurde, können wir unsere Krankenakten nicht wiederherstellen«, schrieb die Praxis in ihrer letzten Stellungnahme an die Patienten. »Wir werden unsere Praxis schließen und den Betrieb einstellen …«[20]

19. Sophos, The State of Ransomware 2021, S. 11.
20. Wood Ranch Medical, »Wood Ranch Medical Notifies Patients of Ransomware Attack«, 18. September 2019, *https://web.archive.org/web/20191229063121/https://www.woodranchmedical.com/*.

»Ransomware«

Ursprünglich bezeichnete der Begriff »Ransomware« eine Schadsoftware, die dem Opfer den Zugriff auf Ressourcen verwehrte, üblicherweise durch die Verschlüsselung von Dateien oder Geräten. Mit der Zeit hat sich der Begriff umgangssprachlich gewandelt und umfasst nun auch andere Arten digitaler Erpressung wie etwa die Enthüllung von Daten.

In diesem Buch verwenden wir den Begriff »Ransomware« gezielt für Schadsoftware, die den Zugriff auf Informationsressourcen verhindert. Im weiteren Sinne verwenden wir die Begriffe »digitale Erpressung/Cybererpressung«.

1.3.2 Finanzielle Einbußen

Digitale Erpressung kann sich katastrophal auf den Finanzstatus des Opfers auswirken. Verluste entstehen üblicherweise durch die kurzfristige Unterbrechung des Umsatzgenerierungsprozesses, Kosten durch Denial of Service, Wiederherstellungskosten und durch die Lösegeldzahlung selbst. So meldete die Reederei Maersk beispielsweise einen Gesamtverlust zwischen 250 und 300 Millionen US-Dollar, nachdem ihre IT-Infrastruktur 2017 durch die destruktive NotPetya-Ransomware, die die Festplatten infizierter Computer zerstört, ausgelöscht wurde. Zwar wurde eine Wiederherstellungsoption gegen Zahlung eines Lösegelds angeboten, doch tatsächlich ließen sich die Dateien nicht wiederherstellen.[21]

In diesem Abschnitt diskutieren wir drei gängige Ursachen finanzieller Einbußen durch digitale Erpressung: Umsatzverluste, Wiederherstellungskosten und Lösegeldzahlungen.

1.3.2.1 Umsatzverluste

Jede Betriebsunterbrechung führt offensichtlich zum Einbruch der Umsätze. Das gilt insbesondere für Unternehmen, die ihre Umsätze täglich generieren (im Gegensatz zu Non-Profit-Organisationen, Schulen und öffentlichen Einrichtungen, die auf Jahresbasis finanziert werden). Krankenhäuser, Einzelhändler, Dienstleister und Produktionsunternehmen sind von solchen Unterbrechungen besonders schwer betroffen. Zum Beispiel hatte Scripps Health nach einem Cyberangriff im Jahr 2021 Berichten zufolge Umsatzverluste in Höhe von 91,6 Millionen US-Dollar, im Wesentlichen durch »Volumenreduzierungen im Mai 2021 durch Verlegung von Notfällen und die Verschiebung von Operationen«.[22]

---

21. Mike McQuade, »The Untold Story of NotPetya, the Most Devastating Cyberattack in History«, Wired, 22. August 2018, *www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/*.
22. Robert King, »May Cyberattack Cost Scripps Nearly $113M in Lost Revenue, More Costs«, Fierce Healthcare, 11. August 2021, *www.fiercehealthcare.com/hospitals/may-cyber-attack-cost-scripps-nearly-113m-lost-revenue-more-costs*.

Betriebsunterbrechungsversicherungen können das Loch im Geldbeutel des Opfers stopfen. Üblicherweise greift diese Art Versicherung nach einer Sperrfrist (beispielsweise 24 Stunden), nach der der Versicherer die Einnahmeverluste bis zu einem festgelegten Betrag übernimmt.

1.3.2.2 Wiederherstellungskosten

Die Kosten für die Wiederherstellung nach einem Ransomware-Angriff können sich schnell aufsummieren. In Abhängigkeit von der Recovery-Strategie müssen neue Hardware (etwa neue Festplatten oder neue Arbeitsplatzrechner, um die infizierten Computer schnell zu ersetzen), Softwarelizenzen, externer IT-Support, Sicherheits- und Forensik-Dienstleistung und mehr eingekauft werden.

Die Stadt Baltimore hat Berichten zufolge 18 Millionen US-Dollar ausgegeben, um die Folgen eines Ransomware-Angriffs durch RobbinHood im Jahr 2019 zu beseitigen. Das hat zu erheblichen Kontroversen geführt, da das geforderte Lösegeld nur einen Bruchteil dieses Betrags ausmachte (etwa 76.000 US-Dollar in Bitcoin).[23] Ein Großteil des Betrags war ursprünglich für Parks und Freizeit eingeplant.[24] Auch Scripps Health hat angeblich 21,1 Millionen US-Dollar für Denial of Service und die Wiederherstellung nach dem Angriff im Jahr 2021 ausgegeben.[25]

Laut Sophos haben sich 2021 die Kosten für die Behebung eines Ransomware-Angriffs im Vergleich zum Vorjahr mehr als verdoppelt und lagen durchschnittlich bei 1,85 Millionen US-Dollar.[26] Laut IBMs *Cost of a Breach*-Report von 2021 lagen die Durchschnittskosten eines Ransomware-Angriffs bei 4,62 Millionen US-Dollar, wenn auch eine Datenschutzverletzung vorlag.

1.3.2.3 Lösegeldzahlungen

Natürlich kann sich auch die Lösegeldzahlung selbst dramatisch auf die Finanzen des Opfers auswirken. Das durchschnittliche Lösegeld hat sich in den letzten Jahren enorm erhöht. Viele Lösegeldzahlungen werden nie öffentlich, weshalb ein vollständiges Bild unmöglich ist, aber wir können Trends erkennen, die auf den Informationen von Unterhändlern, Versicherungen und Kryptowährungs-Forschungsunternehmen basieren. Das Incident-Response-Unternehmen Coveware meldete ein durchschnittliches Lösegeld von 136.576 US-Dollar für das zweite Quartal 2021, basierend auf einer Analyse der Fälle, bei denen es in den Zah-

23. Ian Duncan, »Baltimore Estimates Cost of Ransomware Attack at $18.2 Million as Government Begins to Restore Email Accounts«, The Baltimore Sun, 29. Mai 2019, *www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-Ransomware-email-20190529-story.html*.
24. Luke Broadwater, »Baltimore Transfers $6 Million to Pay for Ransomware Attack; City Considers Insurance Against Hacks«, The Baltimore Sun, 28. August 2019, *www.baltimoresun.com/politics/bs-md-ci-Ransomware-expenses-20190828-njgznd7dsfaxbbaglnvnbkgjhe-story.html*.
25. King, »May Cyberattack Cost Scripps Nearly $113M«.
26. Sophos, The State of Ransomware 2021, S. 12.

lungsprozess involviert war.[27] Auch wenn der Betrag unter der hohen Summe lag, die Coveware für 2020 angegeben hat, so ist das doch eine dramatische Steigerung im Vergleich zum durchschnittlichen Lösegeld von 36.295 US-Dollar im zweiten Quartal 2019 und nur 6.733 US-Dollar Ende 2018.[28]

Die Cyberversicherung Coalition meldete eine durchschnittliche Lösegeldforderung von 1.193.159 US-Dollar für das erste Halbjahr 2021 – eine Erhöhung um 170 % im Vergleich zum ersten Halbjahr 2020. (Beachten Sie, dass Lösegeld*forderung* und Lösegeld*zahlung* zwei verschiedene Dinge sind. Die Täter verhandeln und lassen sich auf Preisnachlässe von 50 % und mehr ein, insbesondere wenn es um höhere Beträge geht.) Coalition merkt an, dass »unsere Daten nur die Fälle berücksichtigen, in denen die Organisationen Ansprüche angemeldet haben und die Verluste über dem Selbstbehalt lagen«. Der durchschnittliche Verlust wird also noch höher liegen.[29]

Laut Chainalysis, einem Kryptowährungs-Forschungsunternehmen, sind die durchschnittlichen Lösegeldzahlungen deutlich gestiegen – von 12.000 US-Dollar im vierten Quartal 2019 auf 54.000 US-Dollar im ersten Quartal 2021.[30] Die Daten basieren auf Zahlungen an bekannte, Ransomware zugeordnete Wallet-Adressen.

Die Autoren dieses Buches können den Trend hin zu höheren Lösegeldforderungen bestätigen. Als wir 2016 mit der Bearbeitung digitaler Erpressungsversuche begannen, lagen die Lösegeldforderungen üblicherweise bei einigen tausend US-Dollar. Während die Täter ihre Fähigkeiten und die Reichweite ausbauten, explodierten auch die Lösegeldforderungen. Während wir diese Zeilen 2022 schreiben, haben wir es regelmäßig mit Lösegeldforderungen zwischen 750.000 und 5 Millionen US-Dollar zu tun. Offensichtlich hat sich die Landschaft verändert.

---

27. Coveware, »Q2 Ransom Payment Amounts Decline as Ransomware Becomes a National Security Priority«, 23. Juli 2021, *www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-Ransomware-becomes-a-national-security-priority.*
28. Coveware, »Ransomware Amounts Rise 3x in Q2 as Ryuk & Sodinokibi Spread«, 16. Juli 2019, *www.coveware.com/blog/2019/7/15/Ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread.*
29. Coalition, H1 2021: Cyber Insurance Claims Report, Juli 2021, S. 11–13, *https://info.coalitioninc.com/download-2021-h1-cyber-claims-report.html.*
30. Da die Chainalysis-Daten auf Zahlungen an mit Ransomware verknüpften Wallet-Adressen basierten, unterschätzten die frühen Reports die tatsächliche Höhe der Lösegeldzahlungen. Je mehr Adressen mit der Zeit bekannten Kriminellen zugeordnet werden konnten, desto höher wurden die Zahlungen. Die Analyse ist auch auf nachverfolgbare Kryptowährungen beschränkt (Chainalysis erfasst Bitcoin, Bitcoin Cash, Ethereum und Tether). Mehr und mehr Kriminelle wechseln aber zu Monero, weil man das wesentlich schwerer verfolgen kann.

Nützlich: Verzerrte Statistiken

Im Verlauf des Buches teilen wir mit digitaler Erpressung im Zusammenhang stehende Statistiken. Allerdings gibt es bei allen existierenden Studien zu Cybererpressung gravierende Einschränkungen. Insbesondere:

- **Untererfassung:** Es gibt keine allgemeine Meldepflicht für die Opfer digitaler Erpressung (und selbst wenn, würden es einige vorziehen, den Vorfall unter den Teppich zu kehren). In manchen Fällen macht der Täter eine digitale Erpressung ganz bewusst öffentlich. In anderen Fällen sind die Auswirkungen so groß, dass das Ereignis allgemein bekannt wird (etwa Ransomware-Angriffe auf Krankenhäuser). Allerdings werden viele digitale Erpressungen diskret behandelt, ohne sie bekannt zu machen. Diese Fälle werden von den veröffentlichten Statistiken einfach nicht berücksichtigt.
- **Statistische Verzerrung:** Viele Statistiken zur digitalen Erpressung stammen von Sicherheitsfirmen, Incident-Response-Unternehmen und Versicherungen. Entsprechend sind die verwendeten Daten häufig auf die eigenen Kunden oder die Kunden der Partner beschränkt und für ein breites Spektrum der Opfer digitaler Erpressung nicht repräsentativ. Veränderte Trends können durch Veränderungen des Geschäftsfelds der Autoren entstehen und müssen nicht das tatsächliche Bild digitaler Erpressung widerspiegeln. Irritierenderweise versuchen die Anbieter ihre Reports so zu verkaufen, als wären sie statistisch sauber erstellt worden, und Journalisten verkaufen diese Daten auch so.

Das hat zur Folge, dass Statistiken zur Cybererpressung stark variieren und ihre Genauigkeit sehr fraglich ist. Aufgeklärte Leser sollten alle Berichte und Studien zur digitalen Erpressung mit Vorsicht genießen.

In diesem Buch teilen wir Statistiken der etwas seriöseren Quellen und bemühen uns, offensichtliche Verzerrungen und Grenzen dieser Studien aufzuzeigen. Wir fordern die Leser auf, die Quelle jeder Statistik zur digitalen Erpressung sorgfältig zu prüfen. Die enthaltenen Informationen können nützlich sein, doch kein Bericht kann den aktuellen Stand digitaler Erpressung vollständig erfassen.

Glücklicherweise gibt es Anzeichen dafür, dass sich die Informationsqualität und Verfügbarkeit in Zukunft verbessern. In letzter Zeit fordern Gesetzgeber und Regierungsbehörden ein strengeres und besser standardisiertes Reporting für Fälle digitaler Erpressung oder allgemeiner Cybersicherheitsvorfälle. So legt zum Beispiel der amerikanische Cyber Incident Reporting for Critical Infrastructure Act von 2022 (CIRCIA) umfassende Anforderungen für die »abgedeckten Cybersicherheitsvorfälle« fest, die in »kritischer Infrastruktur« auftreten. Die US-Regierung beabsichtigt, diese Daten zu analysieren und regelmäßig Berichte und Statistiken zu veröffentlichen.[31,32]

31. Davis Wright Tremaine LLP, »The Cyber Incident Reporting for Critical Infrastructure Act of 2022: An Overview«, 20. Mai 2022, *www.jdsupra.com/legalnews/the-cyber-incident-reporting-for-6977192*.
32. Amendment to H.R. 2471, »An Act to Measure the Progress of Post-Disaster Recovery and Efforts to Address Corruption, Governance, Rule of Law, and Media Freedoms in Haiti«, 9. März 2020, S. 2464–2519, *www.congress.gov/117/bills/hr2471/BILLS-117hr2471eah.pdf*.

1.3.3 Reputationsverlust

Opfer digitaler Erpressung sehen sich dem Verlust von Vertrauen, öffentlichem Ansehen und der Reputation ausgesetzt, was zu größeren finanziellen Einbußen und rückläufigem Geschäftsvolumen führen kann. Laut Cybereason haben 53 % der Opfer einer Ransomware-Attacke einen Markenschaden erlitten.[33] Dieses Ergebnis wird umso wahrscheinlicher, wenn es bei der digitalen Erpressung zum Diebstahl sensibler Daten kam, was zum vollständigen Verlust der Privatsphäre der Betroffenen (Mitarbeiter, Kunden, Patienten) führen kann.

Die Kriminellen bauen auf die Angst vor Reputationsverlust. Ein Beispiel ist der von den Autoren behandelte Fall digitaler Erpressung im Jahr 2020, bei dem das Maze-Kartell der Unternehmensleitung folgende E-Mail geschickt hat:

> *Zuerst werden wir die persönlichen Daten Ihrer Mitarbeiter und Kunden auf dem Markt verkaufen, was uns bereits einen Gewinn einbringt. Dann informieren wir Ihre Kunden, dass ihre privaten Daten kompromittiert wurden. … Doch die größten Verluste werden Sie durch die Veröffentlichung der Daten erleiden, die wir von Ihren Servern heruntergeladen haben. Sie werden sowohl von Ihren Mitarbeitern als auch von Ihren Kunden verklagt werden. Nach der Veröffentlichung auf unserer Nachrichtenseite wird Ihr Unternehmen einen enormen Imageverlust erleiden. Ich denke, dass viele Ihrer aktuellen Kunden Ihre Dienste nicht mehr in Anspruch nehmen werden. Neue Kunden zu finden, wird in Zukunft problematisch sein, weil wohl niemand seine persönlichen Daten einem Unternehmen zur Verfügung stellen will, das sie nicht schützen kann.*[34]

Ransomware-Angriffe schaffen es nicht oft in die Schlagzeilen, insbesondere bei Branchen, in denen die Öffentlichkeit nicht direkt betroffen ist. Allerdings nehmen heutzutage die Täter die Dinge häufig selbst in die Hand und drohen, die Betroffenen zu informieren, auch wenn das Opfer selbst das nicht macht. So werden Scham und Angst vor Blamage genutzt, um den Druck zu erhöhen.

Moderne digitale Erpresser eröffnen routinemäßig Datenleck-Portale im Dark Web, auf denen gestohlene Daten veröffentlicht werden. Immer mehr digitale Erpressungen finden breite Beachtung durch die Medien, was zum Teil auch an der ausgefeilten Öffentlichkeitsarbeit der Täter liegt. Das Ergebnis ist ein potenziell höherer Reputationsverlust der Opfer, was die Täter stärkt.

1.3.4 Gerichtsverfahren

Gerichtsverfahren sind nach einer Cybererpressung mittlerweile üblich geworden. Dafür sind verschiedene Faktoren ausschlaggebend:

---

33. Ransomware: The True Cost to Business, S. 9.
34. E-Mail der Maze Ransomware-Gang, August 2020.

- *Der dramatische Anstieg veröffentlichter Daten* als Teil digitaler Erpressungen. Das erhöht die Publicity des Falls und kann, neben proaktiven Cybersicherheitsverordnungen, eine Anzeigepflicht für Datenschutzverstöße zur Folge haben.
- *Die steigende Zahl erfahrener Cyberrechtsanwälte und Regulierungsbehörden,* die die relevanten Gesetze/Vorschriften kennen und Erfahrung damit haben, auf Datenschutzverstöße, Betriebsausfälle und verwandte »Cyber«-Themen zu reagieren.
- *Eine Zunahme der Gesetze und Vorschriften, die ganz konkret auf Datenschutzverletzungen, digitale Erpressung und Cybersicherheit abzielen.* Beispiele sind die Europäische Datenschutz-Grundverordnung (General Data Protection Regulation, GDPR), die Datenschutzgesetze aller 50 amerikanischen Bundesstaaten und branchenspezifische Vorschriften wie der Health Insurance Portability and Accountability Act (HIPAA) und der Health Information Technology for Economic and Clinical Health (HITECH) Act. Hinzu kommen Vorgaben wie die vom amerikanischen Gesundheitsministerium (U.S. Department of Health and Human Services) veröffentlichte Ransomware-Anleitung, die festlegt, dass die Opfer davon ausgehen müssen, dass eine Verletzung stattgefunden hat, »bis die Organisation oder ein Geschäftspartner nachweisen kann, dass eine ›… geringe Wahrscheinlichkeit besteht, dass persönliche Gesundheitsdaten kompromittiert wurden‹«[35].

Gerichtsverfahren können von Kunden, Mitarbeitern, Herstellern, Anteilseignern und von jeder anderen Partei angestrengt werden, die durch die digitale Erpressung potenziell zu Schaden gekommen ist. So kam es beispielsweise bei Scripps Health im Jahr 2021 zu massiven Betriebsunterbrechungen durch einen Ransomware-Angriff, in dessen Verlauf man 147.000 Patienten darüber informierte, dass ihre persönlichen Daten möglicherweise gestohlen wurden.[36] Im Nachgang kam es zu mehreren Sammelklagen durch die Patienten, die dem Gesundheitsdienstleister Nachlässigkeit und falsches Risikomanagement vorwarfen.

Ein wachsender Trend der Kläger geht dahin, mögliche Schäden auch über Identitätsdiebstahl und Datenschutzververletzungen hinaus einzufordern. Nachdem Universal Health Service (UHS) im September 2021 von einem Ransomware-Angriff betroffen war, verklagte der Patient Stephen Motkowicz das Unternehmen, weil »der Datendiebstahl seine Operation verzögerte, wodurch die vom Arbeitgeber bereitgestellte Versicherung auslief und er eine andere Versicherung zu höheren Beiträgen abschließen musste«[37].

---

35. »Fact Sheet: Ransomware and HIPAA«, U.S. Department of Health and Human Services, Office for Civil Rights, 11. Juli 2016, *www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf*.
36. Heather Landi, »Before Attacking IT Systems, Hackers Stole Information from 147K Patients, Scripps Health Says«, Fierce Healthcare, 3. Juni 2021, *www.fiercehealthcare.com/tech/before-attacking-it-systems-hackers-stole-information-from-147-000-patients-scripps-health*.
37. Barry K. Graham et al. v. Universal Health Service, Inc., Case 2:20-cv-05375-GAM, 17. Mai 2021, *https://fingfx.thomsonreuters.com/gfx/legaldocs/bdwpkwqxqpm/HEALTH%20UHS%20DATA%20BREACH%20opinion.pdf*.

Gerichtsverfahren sind darüber hinaus teuer, zeitaufwendig und ziehen auch Jahre nach dem Angriff negatives Medieninteresse auf sich.

Fallstudie: Dominoeffekte

Die Auswirkungen (und möglichen Schäden) durch einen Cyberangriff können sehr weitreichend sein. So kam es zum Beispiel im Mai 2021 bei Colonial Pipeline zu einem vollständigen Ausfall der gesamten Infrastruktur, verursacht durch einen Ransomware-Angriff der Ransomware-Gruppe DarkSite[38]. Die Pipeline transportierte jeden Tag ca. 380 Millionen Liter Treibstoff entlang der Ostküste der USA. Eine Betriebsunterbrechung jeder Art hatte daher erhebliche Auswirkungen auf Endverbraucher und Unternehmen.

Colonial besaß Backups ihrer Systeme, doch die Wiederherstellung der Dienste war ein langwieriger Prozess. Das Unternehmen zahlte 75 Bitcoin (damals etwa 4,5 Millionen US-Dollar) für einen Dekryptor, doch dieser war so langsam, dass er letztlich nutzlos war. Der Betrieb konnte fünf Tage nach dem Angriff wieder aufgenommen werden, doch es dauerte wesentlich länger, bis man sich vollständig erholt hatte.

In der Zwischenzeit ging den von Colonial Pipeline abhängigen Tankstellen der Treibstoff aus und sie mussten schließen. EZ Mart, eine Tankstelle in North Carolina, war eine von ihnen. Laut dem Eigentümer von EZ Mart, Abeer Darwich, ging der Tankstelle der Treibstoff am 12. Mai aus. Er rief seinen Lieferanten Oliver's Oil an, der ihm mitteilte, dass er erst Treibstoff erhält, wenn die Pipeline wieder läuft. Die Tankstelle war zehn Tage lang nicht voll betriebsfähig, was zu Umsatzeinbußen und zu einem möglichen langfristigen Verlust von Kunden führte.

Nach dem Angriff reichte EZ Mart eine Klage ein, um Schadensersatz für die Betriebsunterbrechung zu fordern, die durch den vorgelagerten Anbieter verursacht worden war. Bemerkenswerterweise wurde die Klage dadurch bestärkt, dass die Kriminellen die Colonial Pipeline nicht direkt heruntergefahren hatten. Laut Gerichtsdokumenten haben die Pipeline-Betreiber vielmehr »entschieden, die Pipeline zum Teil oder ganz herunterzufahren, nicht weil die Angreifer die operativen Systeme erreicht hatten, sondern weil die Beklagten nicht sicher waren, ob sie das über die Pipeline bewegte Produkt würden korrekt abrechnen können«.[39]

Häufig haben betroffene Kunden oder Drittparteien außer einer Klage keine Regressansprüche oder Aussicht auf Schadenersatz. Im Fall von Colonial Pipeline hat der Betreiber Berichten zufolge »seine Verpflichtung gegenüber den Betroffenen eingestanden, aber bis heute weder Schadenersatz noch Mängelbeseitigung angeboten«.[40]

→

38. Joe Panettieri, »Colonial Pipeline Cyberattack: Timeline and Ransomware Attack Recovery Details«, MSSP Alert, 9. Mai 2022, *www.msspalert.com/cybersecurity-breaches-and-attacks/Ransomware/colonial-pipeline-Denial-of-Service/*.
39. *EZ Mart 1, LLC, on Behalf of Itself and All Others Similarly Situated, v. Colonial Pipeline Company, Case 1:21-cv- 02522-MHC*, 21. Juni 2021, S. 7, *https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/coloniallawsuit.pdf*.
40. EZ Mart 1, LLC, v. Colonial Pipeline Company, S. 7.

3 Anatomie eines Angriffs

Wenn du den Feind und dich selbst kennst, brauchst du den Ausgang hunderter Schlachten nicht zu fürchten.
– Sun Tzu

Lernziele

- identifizieren der Schlüsselaktivitäten während einer Cybererpressung
- gängige technische Methoden verstehen, die Cybererpresser nutzen, um sich Zugang zu den Netzwerken der Opfer zu verschaffen
- Tools und Taktiken verstehen, die die Täter nutzen, um sich Zugang zu verschaffen, den Zugriff auszuweiten, die Daten zu bewerten, den Angriff vorzubereiten und die Kontrolle zu übernehmen
- die Möglichkeiten der Entdeckung während jeder Phase erkennen

Eine digitale Erpressung ist niemals *nur* der Versuch einer Cybererpressung. Vom initialen Zugang des Täters eskalieren die Aktivitäten, breiten sich in der Umgebung aus und münden letztlich im Erpressungsversuch.

Zwar ist jeder Angriff anders, doch es gibt Aktivitäten der Täter, die den meisten, wenn nicht allen Fällen von Cybererpressung gemein sind. Diesen roten Faden zu verstehen, hilft Opfern dabei, auf Cybererpressungen zu reagieren, Schäden zu reduzieren und in manchen Fällen auch die Erpressung selbst zu verhindern.

In diesem Kapitel teilen wir einen Cybererpresser-Angriff in seine Schlüsselkomponenten auf und erläutern sie zusammen mit typischen Anzeichen für eine Kompromittierung und effektiven Response-Taktiken.

3.1 Übersicht

Cybererpresser-Angriffe beginnen und enden nicht mit dem Erpressungsversuch, auch wenn das der sichtbarste Teil ist. Die Autoren dieses Buches haben hunderte Fälle digitaler Erpressung (meist aus erster Hand) untersucht und gängige Taktiken identifiziert, die die Täter während dieser Angriffe verfolgen. Eine visuelle Darstellung des Vorgehens sehen Sie in Abbildung 3.1.

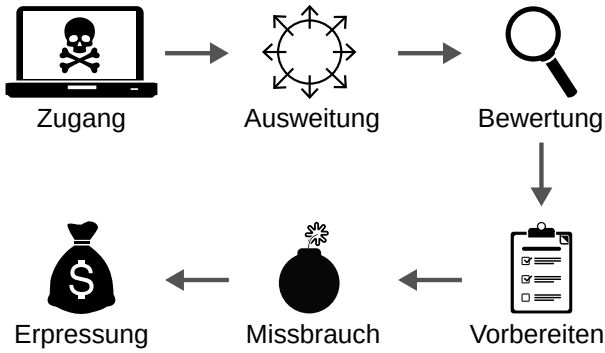

Abb. 3–1 *Anatomie eines Cybererpresser-Angriffs (Illustration mit freundlicher Genehmigung von LMG Security. Grafik: Computer, grmarc/Shutterstock; Totenkopf und Knochen, Sergey Sizkov/123RF; Kreis mit Pfeilen, bloomua/123RF; Lupe, olesya k/Shutterstock; Clipboard, HSDesain/Shutterstock; Bombe, AcaG/ Shutterstock; Geldsack, Pensiri Saekoung/123RF)*

Es ist wichtig anzumerken, dass Cybererpressung kein geradliniger Prozess ist. Die Täter können verschiedene Teile wiederholt durchlaufen oder den gesamten Prozess als Teil eines umfassenden Angriffs wiederholen.

Zu den gängigen Komponenten eines Cybererpresser-Angriffs gehören:

- **Zugang:** Der Täter verschafft sich nicht autorisierten Zugang zu den IT-Ressourcen des Opfers.
- **Ausweitung:** Der Täter versucht in einem sich wiederholenden Prozess den Zugang auszuweiten. Während dieser Phase sorgt der Täter üblicherweise für persistenten Zugriff, erkundet die Systeme, weitet seinen Zugriff aus und gibt den Zugang an andere Täter weiter.
- **Bewertung:** Der Täter schätzt die Stärken und Schwächen des Opfers ein, einschließlich der Datenrepositorys, der finanziellen Stellung, der betrieblichen Infrastruktur und so weiter. Diese Information wird genutzt, um die weitere Angriffsstrategie des Täters zu definieren und zu verfeinern.
- **Vorbereitung:** Der Täter passt die Umgebung an, um die Wirkung der nachfolgenden Phasen zu erhöhen. Das umfasst unter anderem die Zerstörung von Backups, die Demontage des Sicherheitssystems und die Überwachung von Systemen.

- **Missbrauch:** Der Täter greift aktiv die Vertraulichkeit, Integrität und Verfügbarkeit der IT-Ressourcen des Opfers an. Das wird üblicherweise durch die Ausführung einer Ransomware erreicht, durch das Ausschleusen von Daten auf Systeme, die unter der Kontrolle des Täters stehen, den Start eines Denial-of-Service-Angriffs u. Ä.
- **Erpressung:** Der Täter verlangt eine Zahlung oder Dienste, um die Verfügbarkeit, Integrität oder Vertraulichkeit der Daten oder technischer Ressourcen wiederherzustellen.

In den folgenden Abschnitten wollen wir jede dieser Komponenten im Detail diskutieren, Möglichkeiten der Früherkennung hervorheben und effektive Response-Strategien erläutern.

»Kill Chains« und »Angriffsframeworks«

Generell bricht eine »Kill Chain« detailliert alle Phasen und Strukturen eines Angriffs auf. Dieser ursprünglich militärische Begriff wurde 2011 als Konzept in einer Cybersicherheits-Response von Lockheed Martin[1] verwendet. Jeder Schritt der Kill Chain beschreibt eine bestimmte Aktivität oder ein bestimmtes Element eines Angriffs und wird zur Entwicklung von Defensivstrategien genutzt, die einen Angriff an diesem jeweiligen Punkt stoppen oder verhindern sollen.

Im Jahr 2013 hat MITRE das ATT&CK-Framework[2] entwickelt und das Modell der Kill Chain um detaillierte Taktiken und Prozeduren für jeden Teil eines Angriffs erweitert. Das MITRE-Framework ist ein ausgezeichnetes Modell, um die neuesten Taktiken der Täter zu analysieren und zu kommunizieren und um die unterschiedlichen Arten digitaler Erpressung zu verstehen.

Da sich die Angriffe von Cybererpressern ständig weiterentwickeln, haben die Autoren dieses Buches entschieden, eine allgemeine, abstrakte »Anatomie« der Angriffe von Cybererpressern zu verwenden. Diese Anatomie soll die Grundlage bilden, alle Arten digitaler Erpressung zu verstehen. Sie kann zusammen mit detaillierteren Kill-Chain-Modellen wie dem MITRE-ATT&CK-Framework bei der Analyse bestimmter Fälle oder Angriffstrends genutzt werden.

1. »The Cyber Kill Chain«, Lockheed Martin, *www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html*.
2. »ATT&CK«, Mitre, *https://attack.mitre.org/*.

3.2 Zugang

In der Zugangsphase versucht der Täter einen Fuß in die technische Umgebung des Opfers zu bekommen. Das kann der Zugriff auf einen Computer innerhalb des Netzwerks des Opfers sein, aber auch eine cloudbasierte Ressource wie z. B. eine virtuelle Maschine, eine gehostete Anwendung wie E-Mail oder ein entferntes System wie der Computer eines Mitarbeiters. An welchem Punkt der Täter auch immer eingedrungen ist, er wird diesen Erstzugang während der nächsten Phase (Ausweitung) nutzen, um sich in der Umgebung breitzumachen.

Typische Methoden für den Zugang sind:

- **Phishing:** Der Täter sendet eine E-Mail, einen Text oder eine andere Nachricht, die das Opfer dazu bringt, eine Aktion durchzuführen, die dem Täter Informationen und/oder Zugang zur Umgebung des Opfers verschafft.
- **Entfernter Login:** Der Täter kann sich über eine entfernte Login-Schnittstelle wie RDP (Remote Desktop Protocol) erfolgreich anmelden. Dazu nutzt er Zugangsdaten, die er erraten, gestohlen, gekauft oder auf anderen Wegen erhalten hat.
- **Softwareschwachstelle:** Eine Schwachstelle wird in den über das Internet zugänglichen Anwendungen, Servern oder Netzwerkgeräten gefunden.
- **Angriff auf Technologiezulieferer:** Der Täter hat (legitim oder durch Kompromittierung) Zugang zu den technischen Ressourcen eines Zulieferers (etwa einem Softwareanbieter oder Managed Service Provider [MSP]) und nutzt das aus, um sich Zugang zur Umgebung des Opfers zu verschaffen.

Schauen wir uns an, wie die Täter jede einzelne Methode anwenden und welche Möglichkeiten der Erkennung und effektiven Response sich uns bieten.

Definition: Indikatoren für Angriffe und Kompromittierung

Im gesamten Buch verwenden wir die Begriffe »Indicators of Attack« (Indikatoren für einen Angriff) und »Indicators of Compromise« (Indikatoren für eine Kompromittierung). Hier als Grundlage deren Definition:

- Indikatoren für einen Angriff (Indicators of Attack, IoA): Hinweise darauf, dass ein Täter versucht, sich unerlaubt Zugang zu Geräten oder Diensten zu verschaffen. Umfasst unter anderem die Erkennung wiederholt fehlgeschlagener Login- und Exploit-Versuche.
- Indikatoren für eine Kompromittierung (Indicators of Compromise, IoC): Hinweise auf einen erfolgreichen unerlaubten Zugriff, z. B. Logs erfolgreicher Authentifizierung, IDS/IPS-Warnungen oder anderes Systemverhalten, das auf verdächtige Aktivitäten hindeutet.

Quellen solcher Hinweise sind Log-Warnungen, forensische Artefakte und das Systemverhalten. Weitere Informationen zu solchen Hinweisquellen finden Sie in Kapitel 6.

3.2.1 Phishing

Eine Cybererpressung beginnt häufig mit einem Phishing-Angriff. Dabei sendet der Täter eine Nachricht, die das Opfer dazu bringen soll, eine bestimmte Aktion durchzuführen, etwa einen Link anzuklicken oder einen infizierten Anhang zu öffnen. Phishing-Kits, die diesen Angriff automatisieren, werden häufig für 5 bis 15 US-Dollar im Dark Web verkauft.

Phishing-Angriffe können über jede Form von Messaging durchgeführt werden, von E-Mail über SMS bis hin zu Social Media. (Wie wär's mit Brieftauben?[3]) Allerdings versuchen die Cybererpresser üblicherweise, einen Fuß in das Netzwerk der Organisation zu bekommen, und E-Mails sind in dieser Art von Umgebung die am weitesten verbreitete Methode der Kommunikation zwischen externen und internen Teilnehmern.

3.2.1.1 Remote-Access-Trojaner

Die Nutzdaten einer Phishing-Nachricht sind häufig sog. Remote-Access-Trojaner (RATs). Diese Software ermöglicht es dem Täter, aus der Ferne auf ein Computersystem zuzugreifen und es zu steuern.

Die Features der RATs variieren stark, erlauben dem Täter aber üblicherweise Folgendes:

- Aufbau eines Kommunikationskanals zwischen dem kompromittierten Endpunkt und dem steuernden Server
- Daten über den infizierten Computer abzurufen
- entfernte Kontrolle des infizierten Computers
- sich der Erkennung zu entziehen

Fortschrittliche RATs bieten zusätzliche Möglichkeiten, die dem Täter Folgendes erlauben:

- automatisches Stehlen sensibler Daten vom Computer des Opfers, unter anderem Debit-/Kreditkartennummern, gespeicherte Passwörter und Systeminformationen
- interaktives Einloggen per Virtual Network Computing (VNC) oder einem ähnlichen Programm
- Generierung von Reports über Nutzeraktivitäten, Kontostände, Webhistorie u. Ä.
- ausgefeilte Angriffe zur Rechteausweitung, um die Ausbreitung des Täters zu erleichtern
- Installation zusätzlicher Malware (auch Ransomware)

---

3. D. Waitzman, »A Standard for the Transmission of IP Datagrams on Avian Carrier«, 1. April 1990, *https://tools.ietf.org/html/rfc1149*.

- Nutzung der/des Computer(s) des Opfers für Angriffe auf andere Organisationen

Bösartige »Schweizer Taschenmesser« wie Emotet und Trickbot sind auf Phishing-Kampagnen angewiesen, um ihre Malware verbreiten zu können, die die Täter nutzen, um persistenten Zugang zu erlangen, Informationen zu stehlen und weitere Sicherheitsbedrohungen zu verteilen. Die Präsenz eines RATs ist häufig der Vorbote eines Cybererpresser-Angriffs.

Traditionell werden RATs über Social-Engineering-Attacken wie Phishing-Mails, bösartige Websites oder kompromittierte Anwendungen verteilt. Der einen RAT installierende Angreifer kann eine Cybererpressung durchführen oder den Zugriff an andere Kriminelle vermieten/verkaufen, die dann die Cybererpressung übernehmen.

Möglichkeiten der Entdeckung

Wenn eine Cybererpressung mit Phishing beginnt, ist üblicherweise das Gerät eines Nutzers der »Patient Null«, d.h. das erste System, in das der Täter eindringt. Dort sorgt der Täter für Persistenz, was üblicherweise irgendeine Form von Shell bedingt (weil die Firewall bei den meisten Geräten den eingehenden Internetzugriff verhindert). Der Täter nutzt dann gestohlene Zugangsdaten oder ungepatchte Schwachstellen, um seine Account-Rechte auszuweiten und sich in der Umgebung breitzumachen.

Konkrete Anzeichen sind:

- **Warn- und Alarmhinweise von E-Mail-Sicherheitssoftware:** In manchen Fällen wird die verdächtige E-Mail automatisch unter Quarantäne gestellt. In anderen Fällen wird die E-Mail zusammen mit einer Warnung an den Nutzer oder den E-Mail-Administrator (oder an beide) geschickt. Das E-Mail-System des Nutzers kann auch eine Warnung in die Betreff-Zeile oder in den Mailtext einfügen, wenn die E-Mail bestimmte Kriterien erfüllt, die für einen Phishing-Angriff charakteristisch sind.
- **Hinweis eines Nutzers:** Ein Nutzer könnte die Phishing-Mail an das Response Team melden. Ist das der Fall, sollte das IT-Team schnell nach anderen Nutzern suchen, die ähnliche E-Mails erhalten haben, und diese aus deren Posteingang entfernen. Hat ein Nutzer einen Link oder einen Anhang in der verdächtigen Mail angeklickt, sollte der Incident-Response-Prozess der Organisation angestoßen werden, um eine mögliche Infektion einzudämmen.
- **Malware-Analyse:** Durch die Analyse einer Malware können häufig bekannte Phishing-Kampagnen oder Hacker-Gruppen identifiziert und zusätzliche Indikatoren ermittelt werden, die bei der Suche in den betroffenen Umgebungen nützlich sind.

- **Logs der E-Mail-Anwendung:** Die Logdateien von Anwendungen können Warnungen zu verarbeiteten E-Mails enthalten oder einen Alarm bei blockierten Versuchen. Auf diese Weise können Nutzer mit einem hohen Risiko identifiziert werden, Perioden ungewöhnlicher Aktivität, Veränderungen in den Risikoprofilen der Nutzer und vieles mehr.
- **Antiviren-Logs:** Klickt ein Nutzer einen Link oder einen Anhang in einer Phishing-Mail an und lädt/startet eine Malware, kann die Antivirensoftware Alarm schlagen.
- **Event-Logs:** In gleicher Weise kann das Anklicken eines Links oder eines Anhangs, der zur Ausführung von Code führt, ungewöhnliche Aktivitäten in den Event-Logs festhalten, etwa die Ausführung privilegierter Befehle, die Einrichtung von Terminaufgaben oder den Start bzw. Stopp von Diensten.

3.2.2 Entfernter Login

Viele Cybererpresser-Angriffe können durchgeführt werden, weil es dem Täter gelingt, Zugang zu einem entfernten Login wie etwa der RDP-Plattform zu erlangen. Häufig kaufen Cybererpresser gestohlene Zugangsdaten im Dark Web von Initial-Access-Brokern, statt sie selbst zu stehlen oder zu erraten.[4] Die Erpresser nutzen diese Zugangsdaten dann, um sich ein Standbein in Netzwerk aufzubauen und den Angriff durchzuführen.

Es gibt gute Gründe, warum »offene« RDP-Dienste üblicherweise die Wurzel eines Großteils der Erpresserangriffe sind:

- Es sind keine speziellen Tools nötig, um sich entfernten Zugang zu verschaffen.
- RDP ist ein weit verbreitetes Protokoll, das häufig keinen Alarm auslöst. Das gilt insbesondere, wenn es von den Mitarbeitern oder einem IT-Administrator aktiv genutzt wird.
- Der Täter kann sich häufig über den kompromittierten Computer durch das Netzwerk hangeln, indem er per RDP auf andere Systeme zugreift.

Viele Organisationen verwenden RDP oder andere Tools für den Remote-Zugriff, damit sich die Mitarbeiter von zu Hause aus oder auf Reisen einloggen können oder damit IT-Administratoren bzw. -Hersteller jederzeit Zugriff auf das lokale Netzwerk haben. Das ist (leider) auch für die Täter praktisch, die Zugangsdaten häufig stehlen oder Passwortangriffe starten, um sich unerlaubten Zugang zu verschaffen.

Das riesige Angebot an gestohlenen Passwörtern, die über das Dark Web frei zugänglich sind oder verkauft werden, hat diese Angriffe noch weiter befeuert. Im Sommer 2020 haben Forscher mehr als 15 Milliarden gestohlene Benutzerna-

4. Victoria Kivilevich und Raveed Laeb, »The Secret Life of an Initial Access Broker«, KELA, 6. August 2020, *https://ke-la.com/the-secret-life-of-an-initial-access-broker/*.

men/Passwortkombinationen im Dark Web identifiziert.[5] Während diese Zeilen geschrieben werden, kosten RDP-Zugangsdaten zwischen 16 und 24 US-Dollar pro Zugang.[6]

Viele Leute nutzen das gleiche Passwort für mehrere Accounts.[7] Die Täter machen sich dies zunutze und fahren sog. »Credential Stuffing«-Angriffe, bei denen die gestohlenen Zugangsdaten bei vielen verschiedenen Login-Schnittstellen durchprobiert werden. Ist der Login bei einem anderen Account erfolgreich, können die Täter ihn entweder selbst nutzen oder verkaufen.

Im Jahr 2020 hat die Covid-19-Pandemie zu einem starken Anstieg der Telearbeit geführt. Als Reaktion darauf haben viele Organisationen schnell Remote-Zugänge geschaffen, ohne besonders auf die Sicherheit zu achten, und wurden daraufhin kompromittiert.

Möglichkeiten der Erkennung

Übliche Zeichen eines Angriffs oder der Kompromittierung eines Remote-Logins sind:

- **Fehlgeschlagene Login-Versuche:** Greift ein Täter über Passwort-Spraying oder Credential Stuffing an, gibt es häufig wiederholt fehlgeschlagene Login-Versuche (manchmal gefolgt von einem erfolgreichen Login). Das kann an den Systemgrenzen passieren, aber auch innerhalb des Netzwerks, wenn der Täter versucht, sich auszubreiten. Leider sind viele Umgebungen nicht so konfiguriert, dass fehlgeschlagene Login-Versuche auf Microsoft-Windows-Hosts innerhalb des eigenen Netzwerks festzuhalten werden. Die Täter können daher die Authentifizierungsversuche innerhalb des Netzwerks automatisieren, ohne entdeckt zu werden.
- **Ungewöhnliche erfolgreiche Login-Versuche:** Dazu zählen Logins zu ungewöhnlichen Zeiten oder von ungewöhnlichen Orten aus, unterschiedliche User-Agent-Strings und »unmögliches Beamen«, d.h. schnell aufeinanderfolgende Logins von unterschiedlichen geografischen Orten.
- **Anlegen neuer Accounts:** Solche Accounts können schnell für den Remote-Zugang genutzt werden.

---

5. Davey Winder, »New Dark Web Audit Reveals 15 Billion Stolen Logins from 100,000 Breaches«, Forbes, 8. Juli 2020, *www.forbes.com/sites/daveywinder/2020/07/08/new-dark-web-audit-reveals-15-billion-stolen-logins-from-100000-breaches-passwords-hackers-cybercrime/*.
6. »The Price of Stolen Remote Login Passwords Is Dropping. That's a Bad Sign«, Threats Hub (blog), 8. Juli 2022, *www.threatshub.org/blog/the-price-of-stolen-remote-login-passwords-is-dropping-thats-a-bad-sign/*.
7. »Online Security Survey: Google/Harris Poll«, Februar 2019, *https://services.google.com/fh/files/blogs/google_security_infographic.pdf*.

3.2.3 Softwareschwachstellen

Die Täter suchen routinemäßig nach Schwachstellen in weit verbreiteter Software und nutzen diese für ihre Angriffe. Das konnte man bei den Kaseya-Angriffen sehen, aber auch an den Reaktionen der Täter auf die ProxyShell- und Log4j-Schwachstellen (und viele andere). Im Fall von Accellion war die Cl0p-Gruppe in der Lage, eine kritische Lücke in den FTA-Geräten von Accellion auszunutzen und sensible Daten von mehr als 9 Millionen Einzelpersonen zu stehlen, was im Januar 2022 zu einer 8,1 Millionen US-Dollar schweren Sammelklage führte.[8]

Die Suchmaschine »Shodan.io« indexiert mit dem Internet verbundene Geräte und kann von Tätern und Verteidigern gleichermaßen genutzt werden, um potenziell gefährdete Geräte im Internet zu identifizieren.

Das zeitnahe Aufspielen von Patches kann das Risiko einer Kompromittierung eines Gerätes an den Systemgrenzen deutlich reduzieren. Allerdings ist den IT-Administratoren häufig nicht bewusst, dass ihre Firmware oder Software eine Sicherheitslücke enthält. Das gilt besonders für Organisationen mit beschränkten Ressourcen im IT-Management. Darüber hinaus gibt es Zero-Day-Lücken für die Perimeter-Geräte, die in High-End-Exploit-Kits eingebaut werden können, bevor der Hersteller Zeit hat, das Problem zu beheben.

Möglichkeiten der Erkennung

Übliche Zeichen für einen Angriff über eine Sicherheitslücke in einem Perimeter-System sind:

- Alarme zu Port- oder Schwachstellen-Scans bei Perimeter-Geräten. Das ist durchaus normal, weshalb es besonders wichtig ist, solche Alarme sorgfältig zu untersuchen. Widerstehen Sie der Versuchung, sich gemütlich zurückzulehnen.
- seltsame Fehlermeldungen, die mit dieser Anwendung oder diesem System in Zusammenhang stehen (den Prozessor oder den Speicher überlasten), oder der Absturz eines Systems/einer Anwendung
- unerwartete ausgehende Verbindungen von Servern oder Arbeitsplätzen
- ungewöhnliche oder unbekannte Prozesse oder Anwendungen, die auf den Perimeter-Systemen laufen

8. Sara Merken, »Accellion Reaches $8.1 Mln Settlement to Resolve Data Breach Litigation«, Reuters, 13. Januar 2022, *www.reuters.com/legal/litigation/accellion-reaches-81-mln-settlement-resolve-data-breach-litigation-2022-01-13/*.

Fallbeispiel: VPN-Schwachstelle

Wie konnten die Hacker einbrechen? Zwei Dinge waren schiefgelaufen. Erstens hatte die vom Schulbezirk genutzte FortiGate-VPN/Firewall-Software eine katastrophale Sicherheitslücke. Ein Patch war acht Monate vor dem Angriff veröffentlicht worden, doch der Schulbezirk hat ihn nie eingespielt. Zweitens hatten die lokalen Administrator-Accounts auf den Servern und Arbeitsplatzrechnern alle das gleiche Passwort. Sobald die Angreifer das System gehackt hatten, konnten sie sich mit normalen Tools für den Remote-Zugriff überall anmelden. RDP war für den lokalen Administrator verfügbar, was den Job der Täter noch leichter machte.

Einmal drin, waren die Täter sehr schnell mit der Verschlüsselung des Systems. Sie meldeten sich nur für jeweils ein paar Minuten an – gerade so lange, dass die Ransomware installiert werden konnte – und meldeten sich direkt wieder ab. Sobald das VPN kompromittiert war, dauerte es nur 15 bis 20 Minuten, bis die Täter die Ransomware auf die primären Server losließen. Die Arbeitsplätze haben sie gar nicht erst angefasst.

Glücklicherweise hatte der Schulbezirk Datensicherungen offline außerhalb des Netzwerks gespeichert, und diese waren nicht verschlüsselt. Dennoch dauerte es 10 Tage, bis alle Systeme wieder liefen. Unglücklicherweise enthielten die Server große Mengen an vertraulichen Informationen über die Schüler, darunter medizinische Daten, Daten zur psychischen Gesundheit und disziplinarrechtliche Daten. Der Schulbezirk musste einen Denial of Service starten, um das Risiko einer Datenschutzverletzung zu ermitteln.

Forensische Ermittler fanden heraus, dass der Angriff größtenteils automatisiert erfolgte. Die interaktiven Logins waren extrem kurz, also nicht lang genug, um Daten abgreifen oder auf sie zugreifen zu können. Das entsprach den meisten Dharma-Angriffen jener Zeit. Ein Team von auf Datenschutzverletzungen spezialisierten Anwälten kam zu dem Schluss, dass nur ein sehr geringes Risiko einer Datenschutzverletzung bestehe und dass der Vorfall die Definition einer Datenschutzverletzung nicht erfülle.

3.2.4 Angriffe auf Technologiezulieferer

Erschreckenderweise kann der Ausgangspunkt einer Cybererpressung ein Zulieferer sein, etwa ein IT-Anbieter, MSP, Gerätehersteller oder Cloud-Anbieter. Im Jahr 2019 wurden 22 Städte in Texas von einem Ransomware-Angriff der REvil-Gruppe getroffen, dessen Ursprung zum gemeinsamen MSP zurückverfolgt werden konnte.[9] Nach der Infiltrierung des MSP-Netzwerks nutzten die Täter das normale Werkzeug zur Remote-Administration (ConnectWise Control), um die Ransomware in die Netzwerke der Kunden einzuschleusen. Dank einer effektiven

9. »Texas Municipalities Hit by REvil/Sodinokibi Paid No Ransom, Over Half Resume Operations«, Trend Micro, 10. September 2019, *http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/texas-municipalities-hit-by-revil-sodinokibi-paid-no-ransom-over-half-resume-operations*.

Backup- und Wiederherstellungsstrategie und eines guten Response-Plans konnte der Betrieb in den Städten innerhalb einer Woche wieder aufgenommen werden.[10]

Auch Cloud-Anbieter leiden unter Ransomware-Angriffen, mit teils dramatischen Folgen für die Kunden. Im Mai 2020 wurde Blackbaud, ein führender Anbieter cloudbasierter Fundraising-Software, Opfer eines Ransomware-Angriffs. Die Kunden wurden im Juli darüber informiert, dass »die Cyberkriminellen einen Teil der Daten unserer selbst betriebenen Umgebung (private Cloud) erbeutet haben … Wir haben das von den Cyberkriminellen geforderte Lösegeld bezahlt und uns wurde zugesagt, dass die entwendeten Daten gelöscht wurden«.[11]

Blackbauds Lösegeldzahlung war nur ein kleiner Trost für die vielen Kunden, die sensible Daten in der Cloud gespeichert hatten. Viele von ihnen mussten eigene Denial of Services durchführen – häufig auf eigene Kosten. Ohne direkte Beweise war die Reaktionsmöglichkeit aber beschränkt. Innerhalb weniger Monate sah sich Blackbaud mit 23 Sammelklagen und etwa 160 Forderungen von Kunden und deren Anwälten konfrontiert. Außerdem gab es massenhaft Ermittlungen von Bundes- und Regulierungsbehörden.[12]

Möglichkeiten der Erkennung

Kunden haben üblicherweise nur wenig Einblick in die Betriebspraktiken und das Risikomanagement ihrer Zulieferer, auch wenn diese in großem Umfang auf sensible Daten und Netzwerkressourcen zugreifen können. Sie haben auch keine Möglichkeit, einen Einbruch in das Netzwerk des Zulieferers direkt zu erkennen, und müssen sich darauf verlassen, dass die Zulieferer effektive Möglichkeiten haben, die Verbreitung von Ransomware zu verhindern.

Sichtbare Zeichen für die Kompromittierung eines Zulieferers sind:

- ungewöhnliche Logins oder Aktivitäten von Zulieferer-Accounts
- von Zuliefereradressen ausgehende Spam-Mails
- ungewöhnlich langsame Dienste oder Totalausfälle
- Mitteilungen oder Medienberichte über einen Cybersicherheitsvorfall beim Zulieferer

10. O'Ryan Johnson, »MSP at Center of Texas Ransomware Hit: ›We Take Care of Our Customers‹«, Channel Program News, 17. September 2019, *www.crn.com/news/channel-programs/msp-at-center-of-texas-Ransomware-hit-we-take-care-of-our-customers-*.
11. »Security«, Blackbaud, *www.blackbaud.com/securityincident*.
12. Sergui Gatlan, »Blackbaud Sued in 23 Class Action Lawsuits After Ransomware Attack«, Bleeping Computer, 3. November 2020, *www.bleepingcomputer.com/news/security/blackbaud-sued-in-23-class-action-lawsuits-after-Ransomware-attack/*.