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.

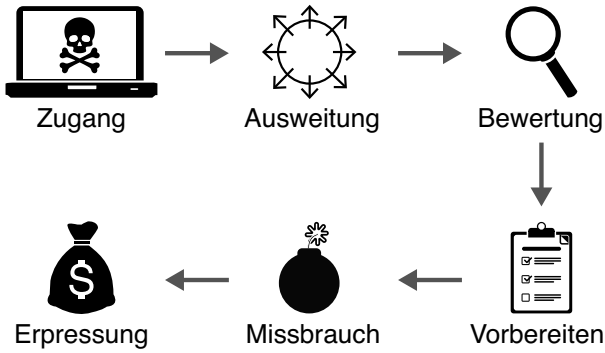

Abb. 3–1 *Anatomie eines Cybererpresser-Angriffs (Illustration mit freundlicher Genehmigung von LMG Security. Grafik: Computer, grmarc/Shutterstock; Totenkopf und Knochen, Sergey Sizkov/123RF; Kreis mit Pfeilen, bloomua/123RF; Lupe, olesya k/Shutterstock; Clipboard, HSDesain/Shutterstock; Bombe, AcaG/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