Sherri Davidoff · Matt Durrin · Karen E. Sprenger

Ransomware und Cyber-Erpressung

Das Praxishandbuch für
IT- und Systemverantwortliche

dpunkt.verlag

Inhalt

4 Die Krise beginnt!

5 Eindämmung

4 Die Krise beginnt!

Keine Panik, wenn es zur Krise kommt, sonst kannst du sie nicht genießen.

– Fiachra Murphy, 9 Jahre alt

Lernziele

- Cybererpressung als Krise verstehen
- Anzeichen eines Cybererpresser-Angriffs auch in den frühesten Phasen erkennen
- festlegen, wer bei einer Cybererpresser-Response beteiligt wird
- die Triage der Ereignisse verstehen, um Response-Bemühungen effektiv priorisieren zu können
- lernen, wie man eine effektive Response-Strategie entwickelt und wie man sie auf dem neuesten Stand hält

Bei einem Angriff durch Cybererpresser zählt jede Sekunde. Sie müssen sofort reagieren und eine Anfangsstrategie entwickeln.

Krisen verlaufen nie so, wie es die Verteidiger erwarten. Die Täter greifen die Opfer mit immer neuen und sich ändernden Taktiken an. Sie dürfen nicht erwarten, dass jemand ein Patentrezept aus dem Ärmel schüttelt, wenn Ihr Netzwerk unten ist und Cyberkriminelle um drei Uhr morgens damit drohen, Ihre Daten im Dark Web zu veröffentlichen.

Stellen Sie sich den Response-Prozess stattdessen wie die Muskeln in Ihrem Körper vor. Ihre Muskeln arbeiten aktiv zusammen, um ein breites Spektrum an Zielen zu erreichen, die Ihr Gehirn vorgibt. Auch Ihre Response-Prozesse sollten es erlauben, auf eine Vielzahl von Situationen zu reagieren. Die Taktiken der Täter ändern sich laufend, und das Umfeld jedes Opfers ist einzigartig. Daher sind Ransomware-Krisen nie gleich. Wenn man sich auf so eine Situation mit offenem Ausgang vorbereitet, ist es wichtig, die Response flexibel zu gestalten, damit Sie sich an die Situation anpassen können. In diesem Kapitel gehen wir die Aktivitäten durch, die notwendig werden, wenn ein Fall von Cybererpressung erkannt wird. Wir diskutieren Techniken, die Anzeichen eines Cybererpresser-Angriffs erkennen (idealerweise bevor sie zu einer echten Krise ausarten). Danach stellen wir ein Modell für die Triage vor, priorisieren die Response-

Bemühungen und entwickeln eine effektive Response-Strategie. Gleichzeitig zeigen wir auf, wie Sie während dieser kritischen Phase effektiv arbeiten können.

4.1 Digitale Erpressung ist eine Krise

Digitale Erpressung führt beim Opfer zu einer Krise – einem »labilen Zustand, der eine plötzliche oder signifikante Veränderung umfasst, die unmittelbare Aufmerksamkeit und Handeln verlangt, um Leben, Vermögen, Eigentum oder das Umfeld zu schützen«.[1] Der Krisenmanagement-Experte Steven Fink geht weiter und definiert eine Krise als eine Situation, die die folgenden Risiken birgt:[2]

- Zuspitzung der Situation
- genaue Untersuchung durch Medien oder Behörden
- Beeinträchtigung des normalen Geschäftsbetriebs
- Gefährdung des positiven öffentlichen Images der Organisation oder ihrer Verantwortlichen
- finanzieller Schaden der Organisation in irgendeiner Form

Natürlich bergen Krisen durch Cybererpressung Risiken in all diesen Kategorien und sollten als Teil des Krisenreaktionsprogramms der Organisation behandelt werden.

Häufig ist eine schnelle und kompetente Reaktion nötig, um eine Katastrophe abzuwenden oder Schäden zu minimieren. Einerseits können Cybererpressungskrisen leicht zu einer chaotischen Abwärtsspirale führen, wenn sie nicht sorgfältig überwacht werden. Andererseits kann eine effektive Response die Lösung erleichtern und ermöglicht es der Organisation, auf lange Sicht zu lernen und sich zu verbessern. Wie es der Merriam-Webster nennt, ist eine Krise ein »Wendepunkt zum Guten oder Schlechten«.[3]

Definition: Phasen einer Krise

Laut dem Experten Steven Fink verläuft jede Krise in vier Phasen:[4]

- prodromal: Die »Vorkrisen«-Phase mit Hinweisen und Vorboten eines Angriffs, die den Respondern die Möglichkeit bieten, die Auswirkungen der Krise zu minimieren, wenn man auf sie reagiert.

- akut: Laut Fink die »Zeit, in der das Chaos regiert«. Während dieser Phase wird die Krise von außen sichtbar, und die Verantwortlichen müssen handeln.
- chronisch: Während dieser Phase kommt es zu »Gerichtsverfahren, medialer Verbreitung, interne und durch Behörden veranlasste Untersuchungen beginnen …« Wie es der Name schon andeutet, kann die »chronische« Phase Jahre dauern.
- (Auf-)Lösung: Die Krise ist überwunden und die normalen Aktivitäten werden wieder aufgenommen.

Idealerweise erkennen die Verteidiger die Anzeichen eines bevorstehenden Ereignisses und überspringen die akute und chronischen Phase, um direkt zur Auflösung zu kommen. Zum Beispiel kann das IT-Personal Anzeichen für einen Remote-Access-Trojaner (RAT) im Netzwerk schnell erkennen und ihn unschädlich machen, bevor er das System infiltrieren, Daten stehlen und Ransomware installieren kann. Taucht eine Cybererpressung allerdings in den Schlagzeilen auf, haben Sie die akute Phase der Krise erreicht, und es gibt keinen Weg zurück.

4.2 Erkennung

Bevor ein Opfer auf einen Cybererpresser-Angriff reagieren kann, muss es erst bemerken, dass ein solcher Angriff stattfindet (Detection). Ein digitaler Erpressungsversuch kann entweder früh (in der Vorkrisen-Phase) oder spät (in der akuten Phase) erkannt werden. Sobald er sich zu einer akuten Krise ausgewachsen hat, sind die Risiken hoch. Idealerweise sollten Organisationen regelmäßig nach Bedrohungen suchen, um die prodromalen Zeichen eines digitalen Erpressungsversuchs zu erkennen, wenn sich der Angriff noch in der Anfangs- oder Ausbreitungsphase befindet. Weitere Informationen zur Suche nach Bedrohungen finden Sie in Abschnitt 5.8.

Wir wollen kurz die wesentlichen Anzeichen eines digitalen Erpressungsversuchs diskutieren, bevor wir uns der Triage und der Anfangsreaktion zuwenden.

Die meisten Cybererpresser-Angriffe werden in der akuten Phase entdeckt, wenn der Angriff bereits in vollem Gange ist. Allerdings ist es auch möglich (und gut), den Angriff in der (symptomatischen) Vorkrisen-Phase zu erkennen, wenn die einzelnen Teile schon vorhanden sind, der Angriff aber noch nicht gestartet wurde.

Wie Sie aus Kapitel 3 wissen, lauern die Täter Tage, Wochen oder sogar Monate in den Systemen, bevor sie die Cybererpressung starten. Frühe Anzeichen digitaler Erpressungsversuche erinnern daher an eine »normale« Kompromittierung und umfassen Folgendes:

- **Warnungen:** Überwachungssysteme wie Antivirus-, Anti-Malware- und Endpunkt-Monitoring können bestimmte Aktivitäten und Dateisignaturen von Erpresser-Malware erkennen und Alarm auslösen. Die Suche nach Bedrohungen oder die aktive Suche nach Malware kann außerdem ungewöhnliche oder verdächtige Dateien aufdecken. Weitere Informationen zur Suche nach Bedrohungen finden Sie in Kapitel 5.
- **Ungewöhnliche Authentifizierungsaktivität:** Achten Sie auf ungewöhnliche Authentifizierungsaktivitäten wie etwa eine erhöhte Anzahl fehlgeschlagener Authentifizierungsversuche, gesperrte Accounts oder Logins von ungewöhnlichen oder unerwarteten IP-Adressen.
- **Neue, nicht autorisierte Accounts:** Sobald sich die Täter Zugang verschafft haben, könnten sie versuchen, neue, privilegierte Accounts anzulegen. Untersuchen Sie Ihre Active-Directory- oder Authentifizierungsstruktur auf jüngst angelegte oder nicht legitime Administrator-Accounts für die Domain.
- **Ungewöhnliche Anwendungen:** Anwendungen wie Mimikatz und Cobalt Strike haben als Werkzeuge für das Pen-Testing ihre Daseinsberechtigung, werden von Tätern aber auch für Cyberangriffe genutzt. Führt die Organisation kein Pen-Testing durch, ist die Präsenz solcher Tools suspekt. Bei der Präsenz jeder Art von Malware sollten sofort die Alarmglocken läuten, insbesondere bei Anzeichen für RATs (siehe Kapitel 3).

Nach einem Angriff sind die Anzeichen eines digitalen Erpressungsversuchs üblicherweise offensichtlich und können Folgendes umfassen:

- **Lösegeldforderung:** Lösegeldforderungen finden sich an den unterschiedlichsten Orten, beispielsweise auf Desktops von Servern oder Arbeitsplätzen, in Verzeichnissen mit verschlüsselten Dateien, ausgedruckt im Drucker oder als E-Mail.
- **Direkte Kommunikation:** Haben die Täter Ihre Organisation studiert, könnten sie einzelne Personen direkt ansprechen (etwa durch einen Anruf) und so den Druck zur Zahlung des Lösegeldes erhöhen. Einige Erpresser nutzen auch die sozialen Medien, um die Organisation der Lächerlichkeit preiszugeben oder um den Druck zu erhöhen. Zum Beispiel könnten sie Twitter verwenden, um die Organisation direkt anzusprechen, oder etwas öffentlich posten und die Organisation »taggen«, um sie zur Zahlung zu bewegen.
- **Unzugängliche Ressourcen:** Viele Opfer erkennen einen Ransomware-Vorfall, wenn im Helpdesk Anrufe von Nutzern eingehen, die nicht mehr

auf ihre Dateien zugreifen können.

Sobald ein Angriff entdeckt wurde, wird es Zeit, zu handeln.

Tipp: Verstehen, was »normal« bedeutet

Eines der besten Werkzeuge im Arsenal des Verteidigers besteht darin, zu verstehen, was »normal« für seine Umgebung bedeutet. Wenn Sie Logs, Warnungen und die Muster des Datenverkehrs regelmäßig untersuchen, ist es sehr viel wahrscheinlicher, dass Sie ungewöhnlichen Datenverkehr oder auffälliges Verhalten wesentlich schneller erkennen.

4.3 Wer muss eingebunden werden?

Menschen sind das wichtigste Kapital während einer Krise durch eine Cybererpressung. Stellen Sie sicher, dass jedem Vorfall ein Incident Manager zugeordnet wird, der die Response, die Kommunikation und den Status überblickt. Der Incident Manager kann wiederum sicherstellen, dass weitere Leute ganz nach Bedarf eingebunden werden. Beachten Sie, dass der verantwortliche Incident Manager im Verlauf der Cybererpressung ausgetauscht werden kann (was auch oft der Fall ist), insbesondere wenn die Auswirkungen zunehmen.

Die Hauptakteure bei einer Cybererpressung sind üblicherweise:

- **IT:** Die Reaktion auf eine Cybererpressung verlangt viel Zeit und Energie von allen Mitgliedern des Incident-Response-Teams, insbesondere vom IT-Personal. Die Größe des IT-Personals wird sich üblicherweise daran orientieren, was für den Normalbetrieb erforderlich ist. Denken Sie über freie Mitarbeiter nach, die Sie beim Einrichten neuer Computer unterstützen, Dateien kopieren oder die Nutzer unterstützen, wenn die wiederhergestellten Systeme wieder online sind. Wenn Sie im Normalbetrieb bereits mit Managed-Service-Providern (MSPs) oder externen IT-Beratern arbeiten, müssen Sie diese in Ihre Response-Planung einbinden.
- **Leitung:** Ihr Führungsteam wird bei einer Cybererpresser-Krise schnelle und schwierige Entscheidungen treffen müssen. Daher ist es gut, wenn sie vorab über die wesentlichen Konzepte und Konflikte informiert sind. Darüber hinaus müssen sie in der Krise möglicherweise zusätzlich benötigtes Geld auftreiben, sich um die Medien kümmern und den Aufsichtsrat und die Aktionäre mit Updates und Erklärungen versorgen.

Das ist ein wahrer Drahtseilakt, und Sie tun gut daran, das im Vorfeld abzusprechen.

- **Finanzen:** Schlüsselakteure des Finanzteams können eingesetzt werden, um Geldmittel schnell zu bewegen, benötigte Mittel aufzutreiben, den Kapitalfluss zu untersuchen oder sich an anderen Aufgaben zu beteiligen, um die Organisation zu unterstützen.
- **Personalabteilung:** Eine Krise ist für alle Mitarbeiter verstörend, und Cybererpressung ist besonders beängstigend und unangenehm. In einigen Fällen werden sensible Mitarbeiterdaten veröffentlicht. Die Personalabteilung sollte darauf vorbereitet sein, Mitarbeiter einzustellen und (oft schwierige) Fragen zu beantworten.
- **Weitere interne Mitarbeiter:** Fälle von Cybererpressung können, je nach Größe und Struktur der Organisation, eine Vielzahl von Menschen einbinden. Dazu gehören Risikomanagement, Rechtsbeistand, Marketing, Kommunikation, Public Relations (PR), Sicherheitspersonal vor Ort und viele mehr.
- **Versicherung:** Wenn Ihre Organisation gegen Cybererpressung oder ähnliche Dinge wie Unterstützung bei der Response auf Einbrüche oder Betriebsunterbrechungen versichert ist, könnten Sie den Versicherer einschalten. Achten Sie darauf, den Versicherer im festgelegten Zeitfenster zu benachrichtigen. Das erhöht die Wahrscheinlichkeit, dass die Response-Aktivitäten übernommen werden. In vielen Fällen muss der Versicherer der Response-Strategie zustimmen, bevor sie durchgeführt wird. Sobald Sie Ansprüche geltend machen, wird der Versicherer möglicherweise Kontakte zu Personen oder Organisationen herstellen, die darauf spezialisiert sind, Unternehmen bei Cybererpressungen zu unterstützen. Das können Rechtsberater, Lösegeld-Unterhändler, Zahlungsvermittler und sogar auf Call-Center und Nachrichten spezialisierte Unternehmen sein.

Tipp: Cyberversicherung und Wahl des Anbieters

Um Kosten und Verluste geltend machen zu können, müssen Sie möglicherweise vom Versicherer vorgegebene Anbieter auswählen, etwa externe Rechtsberater oder Incident-Response-Unternehmen. Zusätzlich könnten Sie die Zustimmung des Versicherers einholen müssen, bevor Sie Schlüsselentscheidungen treffen, z.B. ob Sie das Lösegeld zahlen.

Es ist klug, sich vorab für einen Anbieter zu entscheiden und vom Versicherer eine Zusage für den bevorzugten Anbieter einzuholen. Je nach Versicherer ist das mit einem einfachen

Fragebogen und einer Vorabgenehmigung per E-Mail erledigt oder es muss ein komplexer, tiefergehender Prüfungs-/Genehmigungsprozess durchlaufen werden.

Unabhängig von Ihrer Situation werden Sie den von Ihnen gewählten Anbieter vorab kennenlernen und idealerweise in Übungen und Trainings einbinden wollen. Das sorgt bei Krisen für eine reibungslose Response, reduziert Verzögerungen und verbessert somit den Ausgang.

- **Externe Rechtsberater:** Auch wenn Sie bereits über einen internen Rechtsberater oder externen Anwalt verfügen, sollten Sie über einen auf Cybererpressung spezialisierten Anwalt nachdenken, der sich mit Gesetzen und Bestimmungen bei Lösegeldzahlungen und Datenlecks auskennt. In manchen Fällen wird die Cyberversicherung auf einem externen Rechtsbeistand bestehen, um die Ansprüche zu übernehmen.
- **Incident-Response-/Forensik-Unternehmen:** Ein erfahrenes Incident-Response-Unternehmen kann Sie durch brenzlige Situationen bei einer digitalen Erpressung hindurchlotsen, für eine schnelle Wiederherstellung sorgen, das Risiko einer Neuinfektion reduzieren und sicherstellen, dass der Vorfall endgültig abgeschlossen wird. Das gilt insbesondere, wenn das von Ihnen engagierte Team Erfahrung mit Cybererpressung hat. Gibt es ein mögliches Datenleck, kann das Unternehmen schnell für Sicherheit sorgen und einen forensischen Denial of Service durchführen.
- **Lösegeld-Unterhändler:** Ein erfahrener Lösegeld-Unterhändler hilft dabei, eine Beziehung zum Täter aufzubauen, falls eine Interaktion nötig sein sollte. Diese Verhandlungen können heikel sein, und ein falscher Schritt kann nachhaltige Konsequenzen haben.
- **Public Relations:** Steuern Sie von Beginn an den Nachrichtenaustausch zu einem Vorfall. Neben öffentlichen Meldungen kann ein gutes PR-Team Texte für Helpdesk-Mitarbeiter vorbereiten, die Anrufe von der Belegschaft erhalten. Sie können zur Öffentlichkeit sprechen, Führungskräfte schulen und Anrufe der Medien abfangen.
- **Zulieferer von Schlüsseltechnologien:** Binden Sie Schlüsselzulieferer wie MSPs, Softwareanbieter, Cloud-Anbieter und andere in Ihre Response-Planung mit ein. Die Täter nutzen vermehrt die Zulieferer, um sich in Opferorganisationen einzuschleusen. Sie müssen sich mit den Zulieferern abstimmen, um Beweise sichern zu können oder um von deren Umgebung ausgehende Gefahren abzuwehren.
- **Strafverfolger und/oder Regulierer:** Ihre Beziehungen zu den Strafverfolgern können bei einer Cybererpressung wertvoll sein. In manchen Fällen haben die Ermittler Zugang zu speziellen Dekryptoren, die öffentlich nicht verfügbar sind. Eine Meldung an die Strafverfolger

kann sich im Nachgang auch positiv für Sie auswirken. Das amerikanische Finanzministerium hat beispielsweise gesagt, dass das Office of Foreign Assets Control (OFAC) »die vollständige und zeitnahe Kooperation eines Unternehmens mit den Strafverfolgungsbehörden, sowohl während als auch nach einem Ransomware-Angriff« in Ihrem Sinne positiv berücksichtigt, wenn es um mögliche Strafverfolgung geht.[5]

Fallstudie: FBI-Dekryptor

Ein Finanzdienstleister aus Nordkalifornien wurde Opfer der Ransomware BitPaymer. Die Autoren wurden mit der Response beauftragt. Das war der zweite Angriff auf diese Organisation innerhalb eines Monats. Während des ersten Angriffs (bevor die Autoren einbezogen wurden) verfügte die Organisation glücklicherweise über Backups, die von den Tätern nicht verschlüsselt wurden, sodass die Daten wiederhergestellt werden konnten.

Leider hat die Organisation den Betrieb wieder aufgenommen, ohne einen vollständigen Denial of Service zu simulieren. Von der Organisation unbemerkt wurde bei der Wiederherstellung der Daten aus den Backups auch der Dridex-RAT wieder eingespielt. Das war für die Täter die ursprüngliche Hintertür in das Netzwerk.

Ein paar Tage nachdem der Betrieb wieder aufgenommen worden war, erhielt das Opfer einen Anruf vom FBI. Der Agent übermittelte eine unheilvolle Warnung: Die Täter saßen immer noch im Netzwerk und kommunizierten aktiv mit einem Server, der vom FBI überwacht wurde. In Anbetracht dieser bösartigen Aktivitäten stand ein weiterer Ransomware-Angriff kurz bevor.

Der CIO machte Feierabend und wollte der Sache am nächsten Morgen nachgehen. Doch es war zu spät. Als die Mitarbeiter am nächsten Tag zur Arbeit kamen, waren alle Arbeitsplätze und Dateien gesperrt. Die Ransomware war über Nacht ausgeführt worden. Arbeitsplätze, Server, Datenbanken und mehr waren verschlüsselt. Diesmal waren auch die Backups verschlüsselt. Die Täter waren verärgert, weil sie die ganze Arbeit wiederholen mussten, und verdoppelten ihre Lösegeldforderung. Die Organisation hatte keine Möglichkeit, die Daten wiederherzustellen, zumindest dachten das die Verantwortlichen.

Glücklicherweise arbeitete das FBI an einem experimentellen Dekryptor, der speziell zur Entschlüsselung von Dateien gedacht war, die durch den BitPaymer-Stamm verschlüsselt worden waren. Da die Opfer keine wirkliche Alternative hatten, besorgten die Autoren eine Kopie des FBI-Dekryptors und wandten ihn auf die verschlüsselten Dateien an.

Zum Glück war die Entschlüsselung (größtenteils) erfolgreich. Letztlich konnten etwa 80% der Daten des Opfers wiederhergestellt werden, und die restlichen Daten bestanden aus Kundendaten, die auf Papier archiviert worden waren. Dank des experimentellen Dekryptors des FBI musste das Opfer kein Lösegeld zahlen.

4.4 Triage

Stellen Sie sich einen Auffahrunfall auf der Autobahn vor, in den 32 Autos verwickelt sind. Menschen sind verletzt und manche in ihren Autos gefangen. Andere konnten sich befreien, stehen nun aber inmitten der Wrackteile herum und laufen Gefahr, von nachfolgenden Autos angefahren zu werden. Ersthelfer

erscheinen auf der Bildfläche, können aber nicht überall sein. Was also tun sie angesichts dieses Durcheinanders? Sie führen Triage durch. Sie priorisieren und koordinieren ihre Rettungsbemühungen entsprechend des Verletzungsgrades und des unmittelbaren Risikos.

Während einer Cybererpressung muss ein ähnlicher Prozess ablaufen. Es gibt viel zu viel zu tun, um alles auf einmal erledigen zu können. Die Erst-Responder müssen das Risiko abwägen und einen Plan entwickeln. In diesem Abschnitt wollen wir diesen »Triage«-Prozess diskutieren.

Definition: Triage

Historisch gesehen wurde der Begriff Triage in der Medizin genutzt, um zu beschreiben, wie Menschen priorisiert werden, die Erste Hilfe benötigten. Der Merriam-Webster definiert Triage[6] wie folgt:

1. a: Sortieren und Zuteilen von Behandlungsmöglichkeiten für Patienten, insbesondere Kriegs- und Katastrophenopfer, nach einem Priorisierungssystem, das die Anzahl der Überlebenden maximiert

   b: Sortierung von Patienten (etwa in der Notaufnahme) entsprechend der Dringlichkeit einer Behandlung

2. Zuweisung einer Prioritätenreihenfolge für Projekte basierend auf der optimalen Nutzung von Mitteln und anderen Ressourcen, wo sie am dringendsten benötigt werden oder wo der größte Erfolg zu erzielen ist

Bei einer digitalen Erpressung muss die Triage erfolgen, sobald das Opfer den Angriff erkannt hat. Das Response Team muss die Auswirkungen des Angriffs schnellstmöglich bewerten und gemeinsam einen Plan entwickeln. Die während der Triage-Phase getroffenen Entscheidungen haben weitreichende Folgen für den Ausgang. Die Ergebnisse beeinflussen die nachfolgende Response-Strategie und das letztendliche Ergebnis.

4.4.1 Warum ist Triage wichtig?

Genau wie die Ersthelfer bei einem großen Verkehrsunfall kann das Incident-Response-Team nicht auf jeden Ausfall, jede Auswirkung und jedes Risiko reagieren. Daher muss das Team zusammenarbeiten, um den aktuellen Status des Angriffs zu bewerten und um zu bestimmen, welche Aktivitäten die größte unmittelbare Linderung versprechen. Hat eine Organisation im Vorfeld eines realen Angriffs keinen Incident-Response-Plan entwickelt (und eingeübt), wird sie die Triage wohl überspringen. Ihre Reaktion wird chaotische Züge annehmen,

bei der sich die Verteidiger gegenseitig im Weg stehen, Arbeiten doppelt erledigen, Änderungen überschreiben und wertvolle Beweise verlieren. Noch schlimmer ist, dass der verursachte Schaden unnötig wächst, weil der Angriff nicht schnell genug gestoppt und der Täter nicht aus dem Netzwerk ausgesperrt werden kann.

Ein effektiver Triage-Prozess stellt sicher, dass das Response Team die Arbeiten richtig priorisiert und den Wert der zur Verfügung stehenden Ressourcen maximiert.

4.4.2 Beispielhaftes Triage-System

Auch wenn die Triage ein wichtiger Schritt ist, müssen Sie daran denken, dass sie schnell eingesetzt wird, häufig während die ersten Schritte der Response unternommen werden. Denken Sie an die Notaufnahme eines Krankenhauses, wenn die Opfer des Auffahrunfalls eingeliefert werden. Die Helfer brauchen einfache, klare Richtlinien für die Priorisierung und die Maßnahmen. Ein *Triage-System* ist die Referenztabelle, die den Helfern einfach zu verstehende diagnostische Richtlinien und die nächsten Schritte liefert.

Ihr Triage-System sollte geradlinig und einfach sein, damit die Ersthelfer Entscheidungen schnell und sicher treffen können. Tabelle 4.1 zeigt ein Beispiel für ein einfaches Cybersicherheit-Triage-System:

Triage-Skala	Reaktionszeit	Beschreibung	Indikatoren
sofort	ASAP (<1 Stunde)	Betriebsausfall, glaubwürdiger Erpressungsversuch, Datenleck, aktueller nicht autorisierter Zugriff	Ausfälle, Erpressung, Veröffentlichung von Daten im Internet/Dark Web, Anzeichen für nicht autorisierten Zugriff, kompromittierte E-Mail-Accounts, Warnungen von Strafverfolgern
Dringend	< 4 Stunden	Angriff verlangt zeitnahe Reaktion, um Ausfall und/oder Datenleck zu vermeiden	Anzeichen einer Malware-Infektion, fehlgeschlagene Command-and-Control-Kommunikation, branchenweite Warnungen, potenziell kompromittierter Account
Standard	1–2 Arbeitstage	potenziell bedrohlich, situative Dringlichkeit	Phishing-E-Mails, sporadische Warnungen über bösartige Software, Verstöße gegen die Personalrichtlinien
Geplant	2 Wochen+	weniger dringend oder administrative Aspekte/Richtlinien	Kleinere technische Pannen der Sicherheitssoftware, Probleme mit der Logging-Konfiguration, Forensik für künftige Gerichtsverfahren, Aktualisierung der Richtlinien, Überprüfung von Prozessen etc.

Tab. 4–1 *Ein einfaches Cybersicherheit-Triage-System*

4.4.3 Den aktuellen Status einschätzen

Die Ersten, die Anzeichen einer Cybererpressung erkennen, müssen den aktuellen Status schnell bewerten und die Auswirkungen sowie Risiken einschätzen, um die richtigen nächsten Schritte einzuleiten. Allerdings sind diese Leute nicht unbedingt Experten auf diesem Gebiet. Je nach Organisationsform, Personalbestand, Uhrzeit und anderen Faktoren sind nur IT-Mitarbeiter, Manager und PR-Angestellte mit wenig Erfahrung vor Ort. Stellen Sie im Vorfeld die Definition einiger einfacher Fragen sicher, die die Ersthelfer nutzen können, um die Situation zu beurteilen. Hier einige Beispiele:

4.4.3.1 Betriebliche Auswirkungen

- Welche Prozesse sind betroffen und wie wichtig sind sie für die Organisation? Sehr wahrscheinlich sind bestimmte Systeme für das Funktionieren der Organisation unabdingbar, während andere einen längeren Ausfall verkraften können.

- Ist die Organisation bis zu einem gewissen Grad betriebsbereit? Falls nicht, gibt es schnelle Behelfslösungen, mit denen die Organisation zügig ein Mindestmaß an Betriebsbereitschaft wiederlangen kann?
- Welche finanziellen Auswirkungen hat der Ausfall über die Zeit?
- Hat die Organisation eine Versicherung gegen Betriebsausfall oder andere Ansprüche, die den Verlust durch die Ausfälle abfangen?
- Stehen Drittparteien unter Druck? Ist die Organisation Teil einer Lieferkette, kann sich der Ausfall einiger Systeme oder Daten auf Parteien außerhalb der Organisation auswirken.
- Für welche Systeme bestehen zusätzliche Risiken? Wird nicht sofort etwas unternommen, ist es sehr wahrscheinlich, dass einige Systeme weiter geschädigt werden oder Daten verloren gehen.

4.4.3.2 Datensensibilität

- Welche Arten sensibler Daten besitzt die Organisation?
- Wie hoch ist das Risiko, dass diese sensiblen Informationen nicht autorisierten Parteien zugänglich waren oder in deren Besitz gelangt sind?
- Welchen rechtlichen, regulatorischen oder vertraglichen Pflichten ergeben sich? Fällt die Organisation beispielsweise unter die HIPAA-Regeln? Welche gesetzlichen Meldepflichten für Datenschutzverletzungen gelten?

Beachten Sie, dass die gesetzlichen Meldepflichten häufig auf dem aktuellen Wohnsitz des Betroffenen basieren, dessen Daten gestohlen oder verloren wurden, und nicht auf dem geografischen Standort der Organisation. Operiert Ihre Organisation zum Beispiel von New Jersey aus und gingen Daten von Betroffenen in New York verloren, müssen Sie bei diesen Betroffenen sehr wahrscheinlich den behördlichen Meldepflichten von New York nachkommen. Konsultieren Sie für die Details einen qualifizierten Anwalt.

4.4.4 Wiederherstellungsziele berücksichtigen

Während des Triage-Prozesses sollten Responder zwei sehr wichtige Metriken berücksichtigen, die operative Wiederherstellungsbemühungen begleiten und den Erfolg der Response messen. Wie in NIST 800-34, »Contingency Planning Guide for Federal Information Systems« definiert, ist:[7]

- **Recovery Point Objective (RPO)** »der Zeitpunkt, zu dem Daten nach einem Ausfall wiederhergestellt sein müssen«.
- **Recovery Time Objective (RTO)** »die Gesamtzeit, für die sich die Komponenten eines Informationssystems in der Wiederherstellungsphase befinden können, bevor sie sich negativ auf die Ziele des Unternehmens oder Einsatz-/Geschäftsziele auswirken«.

Idealerweise sollten diese Ziele vor einem Cyberangriff definiert werden. Bei einem Fall von Cybererpressung – insbesondere bei Ransomware oder einem ähnlich zerstörerischen Angriff – ist für Responder und Leitung ein klares Verständnis der RPOs und RTOs des Opfers von besonderer Bedeutung.

Wiederherstellung braucht immer Zeit, und es gibt viele Entscheidungspunkte, an denen sich Responder für längerfristige Ziele entscheiden (etwa forensische Beweissicherung) statt für die kurzfristigen Wiederherstellungsbemühungen. Sorgen Sie dafür, dass jeder die RPOs und RTOs des Opfers kennt, bevor Sie eine Grundlage für die Ausrichtung während des Wiederherstellungsprozesses schaffen.

4.4.5 Die nächsten Schritte bestimmen

Die Ersthelfer müssen eine erste Einschätzung vornehmen und sich dabei am Cybersicherheit-Triage-System der Organisation orientieren. Die gewonnenen Informationen nutzen sie dann, um einen Triage-Status und die nächsten Schritte festzulegen. Das geschieht meist informell, doch die Ergebnisse sind wesentlich besser, wenn die Helfer klare Richtlinien, Training und Support haben.

Es ist unabdingbar, dass die Ersthelfer ausreichend geschult sind, um zu verstehen, wie man den richtigen Triage-Status ermittelt. Ein scheinbar kleiner Vorfall, z.B. die Verschlüsselung eines einzelnen Rechners, kann die Spitze eines Eisbergs sein, die eine schwerwiegende Datenschutzverletzung ankündigt. Stellen Sie sicher, dass die Ersthelfer die Möglichkeit haben, zu verstehen, welche Systeme sensible Daten enthalten oder für den Betrieb unabdingbar sind, und dass sie wissen, wie man die richtige Triage-Kategorie korrekt ermittelt.

Ebenso wichtig sind die nächsten Schritte: Wen kontaktiert der Ersthelfer mit welcher Dringlichkeit? Ein um sechs Uhr morgens erkannter Ransomware-Angriff kann sich über die gesamte Organisation ausbreiten, aber nur einen kleinen Teil des Netzwerks betreffen, wenn der Ersthelfer sofort handelt. Es ist besonders wichtig, dass die Ersthelfer bei Bedarf agieren können und über klare Eskalationsverfahren und Kontaktlisten verfügen, die alle Uhrzeiten abdecken.

Planspiele (Tabletop-Übungen) sind extrem nützliche Werkzeuge. Sie stellen sicher, dass der Responder geschult ist und die benötigten Ressourcen besitzt. Zwar kann nicht jedes mögliche Szenario mit Tabletop-Übungen durchgespielt werden, doch die Teilnehmer müssen die Logistik einer Krise durchdenken, die Kommunikationsprozeduren ausbauen und ihre Rolle verstehen.

Nach Abschluss der Triage-Phase übergibt der Ersthelfer die Verantwortung an jemanden, der den Vorfall längerfristig bearbeitet. Er sollte dann in einem der Triage-Kategorie angemessenen Zeitraum Bericht erstatten.

4.5 Ihre Ressourcen bewerten

Ressourcen umfassen Geld, Menschen und andere Werkzeuge, die für die Response benötigt werden. Bevor es zu einer Krise kommt, müssen Sie sicherstellen, dass Sie ein gutes Verständnis für die verfügbaren Ressourcen haben und wissen, wie man sie anzapft. Auf diese Weise können Sie sicherstellen, dass Ihre Response-Pläne realistisch sind und dass Sie die Ressourcen auch nutzen können, wenn sie benötigt werden. Zum Beispiel könnte nicht ausreichend IT-Personal verfügbar sein, um die notwendigen Arbeiten zu erledigen, doch während der Planungsphase können Sie zusätzlichen Personalbedarf identifizieren und Vereinbarungen treffen, um den Bedarf schnell zu decken.

Tritt eine Krise ein, sollten Sie Ihre Einschätzung der Ressourcen überprüfen und sich ein genaues und aktuelles Bild machen. In diesem Abschnitt gehen wir die wesentlichen Ressourcen durch, die für die Response auf eine Cybererpressung benötigt werden.

4.5.1 Finanzen

Viele Responder glauben, dass das Budget für die Response auf Cybererpressung unbeschränkt ist. Die Wahrheit sieht ganz anders aus. Die Opfer sind während einer Krise finanziell besonders gefährdet, und der Cashflow muss während der Response aufmerksam beobachtet werden. Finanzpersonal und/oder leitende Mitarbeiter müssen möglicherweise Notkredite aufnehmen, auf Geldmittel für den Katastrophenfall zurückgreifen oder andere Möglichkeiten finden, einen vollständigen Betriebsstillstand zu verhindern. Zusätzlich könnte das Opfer Gläubiger, Kreditgeber oder andere wichtige Interessenvertreter informieren müssen und über den Finanzstatus der Organisation auf dem Laufenden halten.

4.5.2 Versicherung

Cyberversicherungen haben bei Ransomware- und Cybererpresser-Angriffen eine wichtige Rolle eingenommen. Die Versicherer haben ein starkes Interesse daran, effektive Response-Praktiken zu unterstützen und Schäden zu minimieren, da sie im Falle eines Anspruchs einen Teil der Rechnung bezahlen müssen. Im Gegensatz zu Verkehrsunfällen kann der Versicherer den Ausgang des Falles beeinflussen, indem er während des Response-Prozesses unterstützt und berät.

Ein Großteil der Opfer verfügt nicht über die Ressourcen, eigene geschulte und erfahrene Response-Mitarbeiter zu beschäftigen (das gilt insbesondere für kleinere und mittelgroße Unternehmen, Non-Profit-Organisationen und öffentliche Einrichtungen). Um diese Lücke zu schließen, haben Versicherer Incident-Response-Teams zusammengestellt, die während des Response-Prozesses wertvolle Dienste leisten.

Zu den von den Cyberversicherern angebotenen Response-Services gehören (unter anderem):

- Hotline zur Meldung von Cyberangriffen
- eine Reihe von (meist geprüften) Dienstleistern für:
    - Incident-Response-Services
    - Lösegeldverhandlungen
    - Rechtsberatung (besonders wichtig, um Denial-of-Service-Untersuchungen zu vermeiden)
    - Public Relations
    - Unterstützung beim Krisenmanagement
- Mittel für Response-/Wiederherstellungsdienste und Lösegeldzahlungen
- Absicherung bei Betriebsunterbrechungen
- Absicherung bei Betriebsunterbrechungen anhängiger Unternehmen

Natürlich unterscheiden sich die Cyberversicherer voneinander, und einige bieten mehr Dienste an als andere. Stellen Sie sicher, dass Ihre Responder mit den Diensten Ihres Versicherers vertraut sind und dessen Anforderungen kennen, wenn Sie sich auf einen Fall von Cybererpressung vorbereiten.

4.5.3 Beweissicherung

Wenn digitale Erpresser zugeschlagen haben, muss Ihr Response-Team (unter anderem) verstehen, wie die Täter in das System gelangt sind, welche Daten sie

abgreifen konnten und ob sie sich immer noch im System befinden. Die Antworten auf diese Fragen ermöglichen es dem Recovery-Team, den Schaden einzudämmen, die Hacker auszusperren, das Risiko zu minimieren und gesetzliche oder regulatorische Denial of Services zu unterstützen.

Leider sind in vielen Fällen die Anhaltspunkte schlicht nicht verfügbar (oder nur schwer zu beschaffen), die man benötigt, um sich ein genaues Bild des Vorfalls machen zu können. Mit jeder verstrichenen Minute erhöht sich das Schadensrisiko.

Bevor es zur Krise kommt, sollten Sie klären, welche Anhaltspunkte Sie in Ihrer Umgebung finden, die im Falle einer Cybererpressung nützlich sein könnten. (Eine detaillierte Liste mit Beweisquellen finden Sie in Kapitel 5.) Stellen Sie dann sicher, dass die Anhaltspunkte verfügbar sind, wenn Sie sie benötigen.

4.5.4 Personal

Bei einer Cybererpressung fällt viel zusätzliche Arbeit an – wenn auch nur für bestimmte Mitarbeiter. Einerseits wird Ihr IT-Personal wahrscheinlich überlastet sein, andererseits werden viele andere Mitarbeiter Däumchen drehen, während sie darauf warten, dass das Netzwerk wieder online geht.

Wägen Sie die zusätzliche Arbeitslast während einer Krise sorgfältig ab und planen Sie unterbeschäftigte Mitarbeiter für andere Arbeiten ein (wenn möglich). Kaufen Sie zusätzliche Support-Mitarbeiter sowie Dienstleister nach Bedarf ein. Es ist sinnvoll, die entsprechenden Kontakte im Vorfeld einer Krise aufzubauen und zu wissen, wen Sie im Notfall anrufen können.

4.5.5 Technische Ressourcen

Die Wiederherstellung des Normalbetriebs verlangt Zugriff auf Hardware, Software, Backups und andere technische Ressourcen. Zum Beispiel müssen die Responder nach einem Ransomware-Angriff üblicherweise eine mehrere Segmente umfassende Netzwerkumgebung aufbauen, Daten von Backups wiederherstellen und die »gesäuberten« Systeme sorgfältig überwachen, damit die Bedrohung wirklich beseitigt wird. Wenn Sie während dieser Arbeiten Beweise sichern, benötigen Sie zusätzlichen Speicher für die Daten sowie Arbeitsplätze oder forensische Ausrüstung, um die Beweise sichern zu können. Überprüfen Sie, ob Ihre Backups brauchbar und für die Wiederherstellung verfügbar sind, wenn Sie sie brauchen. Weitere Details finden Sie in den Kapiteln 6 und 9.

4.5.6 Dokumentation

Bei digitalen Krisen werden die Responder oft schnell ausgebremst, weil ihnen kritische Informationen fehlen, etwa ein Netzwerkdiagramm der vollständigen Umgebung, eine Dokumentation der Anwendungsabhängigkeiten, Details zur Domain-Konfiguration, zu Datenbeständen und vielem mehr. Je mehr Zeit die Responder damit verplempern, die benötigten Daten zu suchen, desto weniger Zeit bleibt ihnen, die Gefahr einzudämmen und die Umgebung wiederherzustellen. Während dieser Zeit kann der Täter aktiv Daten von einem Server ausschleusen oder wichtige Datenrepositorys verschlüsseln.

Steht die vollständige Dokumentation zur Verfügung, sparen Sie Zeit und Geld, und das ist der Schlüssel zu einer effektiven Response auf eine Cybererpressung. Idealerweise sollten Kopien der Dokumentation offline oder in gedruckter Form verfügbar sein. Dann ist sie auch verfügbar, wenn die Umgebung durch Ransomware verschlüsselt wurde oder aus anderen Gründen nicht zugänglich ist. In den Checklisten am Ende dieses Buches finden Sie eine Liste der Dokumentation, die bei digitalen Krisen nützlich ist.

4.6 Eine Strategie für die initiale Reaktion entwickeln

Jede Krise ist einzigartig. Basierend auf den Ergebnissen der Ersteinschätzung und Triage müssen Responder zügig eine Response-Strategie entwickeln. Die Response-Strategie ist ein lebendiges Dokument, das den sich entwickelnden Response-Prozess begleitet, einschließlich der Beweissicherung, Eindämmung, Denial of Service, Wiederherstellung und anderen Aktivitäten. Während der Response muss die Strategie immer wieder neu bewertet und aktualisiert werden.

In diesem Abschnitt diskutieren wir die wesentlichen Schritte bei der Entwicklung und Pflege einer erfolgreichen Response-Strategie.

4.6.1 Ziele festlegen

Stellen Sie sicher, dass die Ziele Ihrer Response-Bemühungen klar definiert und kommuniziert sind. Ihre Ziele sollten realistisch sein und sich an den Prioritäten Ihrer Organisation orientieren. Nehmen wir zum Beispiel ein Krankenhaus, das Opfer eines Ransomware-Angriffs wurde und dessen Patientendaten verschlüsselt wurden. Hier einige mögliche Ziele:

- während der Betriebsunterbrechung die Krisenmanagement-Pläne aktivieren, die festlegen, dass das Krankenhaus einen bestimmten Teil der Patienten mittels Backup-Prozeduren behandeln kann, während

andere Gruppen von Patienten in andere lokale Krankenhäuser verlegt werden

- Wiederherstellung des normalen Zugriffs auf die elektronischen Patientenakten innerhalb von 10 Werktagen
- letztlich die Wiederherstellung aller Patientendaten ohne dauerhafte Zerstörung
- Minimierung des Risikos der Enthüllung von Patientendaten
- Erfüllung aller relevanten Meldepflichten bei Sicherheits- und Datenschutzverletzungen

Häufig sind die Responder gezwungen, sich zwischen konkurrierenden Prioritäten zu entscheiden. Zum Beispiel könnte ein Breach Coach das Response-Team anweisen, Beweise auf einem Schlüsselserver zu sichern, während der CIO das gleiche Team anweisen könnte, den Server sofort wiederherzustellen. Es ist wichtig, einen klaren Prozess der Entscheidungsfindung zu etablieren und sicherzustellen, dass die Entscheidungsträger alle wichtigen Akteure anhören, um die Response-Aktivitäten sinnvoll priorisieren zu können.

4.6.2 Einen Aktionsplan entwickeln

Der Leiter des Response-Teams sollte wichtige Meilensteine und Arbeiten benennen, die zum Erreichen der Ziele notwendig sind, wobei er die Teammitglieder mit einbeziehen sollte. Diese Aufgabenliste sollte dann an einem Ort zu finden sein, wo die Teammitglieder sie sehen können. Die Mitarbeiter sollten dazu ermuntert werden, die Liste während der Response zu aktualisieren (oder den Teamleiter mit Updates versorgen). Die Liste sollte als lebendes Dokument betrachtet werden, da sich Aufgaben und Prioritäten ändern können, wenn das ganze Ausmaß des Cybererpresser-Angriffs deutlich wird.

4.6.3 Verantwortlichkeiten zuweisen

Der nächste Schritt besteht darin, die Aufgaben an die entsprechenden Mitarbeiter oder Drittparteien zu verteilen – einschließlich IT, Rechtsabteilung, Versicherer, Incident Responder, PR und andere. Weiterhin muss die Führungsmannschaft die notwendigen Investitionen verstehen und aktiv bei Schlüsselentscheidungen eingebunden werden, die sich auf das Budget und den Zeitrahmen der Response auswirken.

Es ist wichtig, bei der Zuweisung von Verantwortlichkeiten realistisch zu bleiben. Sie können nicht erwarten, dass einzelne Responder rund um die Uhr arbeiten. Die Response auf eine digitale Erpressung ist ein Marathon, kein Sprint. Stellen Sie einen Personalwechsel sicher und sorgen Sie für zusätzliche Unterstützung durch externe Mitarbeiter oder Dienstleister, um Aufgaben erledigen zu können, die das hausinterne Team realistisch nicht bewältigen kann. Außerdem sollten Sie Ihre Responder auffordern, sich zu melden, wenn sie überlastet sind. Andernfalls werden die Teammitglieder langsam den Anschluss verlieren, und wichtige Arbeiten verschieben sich oder werden gar nicht abgeschlossen.

Tipp: Kümmern Sie sich um Ihre Responder

Im Chaos der Krise arbeiten Responder viele Stunden mit nur wenigen Pausen. Definieren Sie klare Arbeitsperioden für Ihr Personal, einschließlich der Pausen, und holen Sie sich bei Bedarf externe Unterstützung. Sorgen Sie für Essen und organisieren Sie frühzeitig gestaffelte Arbeitsschichten.

Die Response auf eine Krise ist auch ohne Unterbrechungen stressig genug. Benennen Sie einen einzelnen Kontaktpunkt für Anfragen und Updates und stellen Sie sicher, dass der Responder arbeiten kann, ohne ständig gefragt zu werden, ob er schon fertig ist. Das bringt Ruhe in den Response-Prozess und führt zu einer schnelleren Wiederherstellung.

4.6.4 Zeit- und Arbeitsaufwand sowie die Kosten schätzen

Während die Response-Strategie entwickelt wird, ist es besonders wichtig, dass das Response-Team klar die Optionen und Kostenschätzungen an das Führungsteam kommuniziert. Damit kann das Führungsteam fundierte Entscheidungen treffen und frühzeitig die Finanzierung sichern, die die Opferorganisation durch die Krise führt.

Tipp: Dokumentieren Sie fortlaufend

Als Teil der Response-Strategie sollten Sie Raum für die Dokumentation lassen und jedes Mitglied des Incident-Response-Teams auffordern, sich bei jedem Schritt Notizen zu machen. In der Hitze des Gefechts erfolgen Änderungen schnell, Schritte werden isoliert vorgenommen und Systeme können umkonfiguriert werden. Werden solche Dinge nicht dokumentiert, gehen sie verloren oder werden vergessen, was sich auf die Wiederherstellung auswirkt. Verlassen Sie sich nicht darauf, dass die Teammitglieder sich

»erinnern« oder »später« dokumentieren – das Team läuft auf reinem Adrenalin (und Pizza). Ist alles gesagt und getan, macht sich Erschöpfung breit, und die Aktivitäten während der Response verblassen. Dokumentieren Sie fortlaufend.

Fügen Sie an den Anfang der Response-Strategie einen Abschnitt ein, in dem Status-Updates und Änderungen dokumentiert werden. Machen Sie es den Teammitgliedern leichter, ihren Fortschritt festzuhalten.

Die Dokumentation sollte Datumsangaben und Zeitstempel enthalten sowie die Initialen oder den Namen des Responders. Akzeptable Formate der Dokumentation sollten vereinbart werden, bevor es zu einem Vorfall kommt. Sollen Notizen in Word oder in Textdateien verfasst werden? Können Sie handgeschrieben sein? Sollen Fotos gemacht werden, wenn sie hilfreich sind?

4.7 Kommunizieren Sie

Während des gesamten Response-Prozesses ist eine effektive Kommunikation besonders wichtig. Finanzielle und betriebliche Auswirkungen müssen den betroffenen Parteien erklärt werden. Wichtige Interessenvertreter benötigen Informationen, um vernünftige Entscheidungen treffen zu können. Entscheidungen müssen denen klar kommuniziert werden, die sie implementieren. Aufsichtsbehörden könnten Updates benötigen. Die Medien könnten anklopfen. Gerüchte könnten die Runde machen.

Eine effektive Kommunikation ist für die Koordinierung des Response-Teams wichtig und sorgt für Entscheidungen, die mit den verfügbaren Ressourcen und der Risikobereitschaft der Organisation übereinstimmen. Darüber hinaus ist eine gute Kommunikation wichtig, um das Vertrauen der wichtigsten Interessenvertreter, Kunden, Regulierungsbehörden und sogar der Öffentlichkeit zu gewinnen.

Hier eine kurze Liste der Leute, die Sie in Ihre Kommunikationspläne mit einbeziehen sollten:

- das Response-Team
- betroffene Parteien
- die Öffentlichkeit

Wir wollen uns das in den nächsten Abschnitten etwas genauer anschauen.

Tipp: Hören Sie zu!

Kommunikation ist keine Einbahnstraße. So wichtig es ist, Updates und Informationen zu teilen, so wichtig ist es auch, dem Response-Team die Möglichkeit zu geben, Informationen und Feedback zu geben. Das gilt auch für diejenigen, die von der Cybererpressung betroffen sind. Nehmen Sie sich die Zeit zuzuhören. Kann sich die Organisation kein Call-Center leisten, können Versicherer oder Breach Coaches Drittparteien empfehlen, die diese Aufgabe übernehmen.

4.7.1 Response-Team

Naturgemäß müssen Sie innerhalb des Response-Teams (das üblicherweise aus IT, Juristen, Versicherern, Führungskräften und anderen besteht) effektiv kommunizieren. Während einer hektischen und stressigen Krise entstehen leicht Fehler. Das gilt insbesondere für die abteilungsübergreifende Koordination, da die Teammitglieder nicht laufend miteinander arbeiten. Achten Sie auf eine umfassende Kommunikation und geben Sie dem Team regelmäßig die Möglichkeit, Informationen zum Fortschritt, zu Schwachstellen und Plänen zu teilen. Regelmäßige Kontakte reduzieren auch den Stress, da sie Struktur und Routine im Response-Prozess bieten.

Am Anfang einer digitalen Krise sollte das gesamte Response-Team Folgendes wissen:

- Wer hat die Leitung?
- Wo findet man die aktuelle dokumentierte Response-Strategie?
- Wo werden die Arbeit und die Erkenntnisse dokumentiert?
- Welche Formen der Kommunikation sind erlaubt?
- Wie oft sind Updates zu liefern?
- Terminierung und Format regelmäßiger Meetings
- weitere Schlüssel-Metadaten

Die Mitglieder des Response-Teams sollten dazu ermuntert werden, Informationen intern mit dem Team zu teilen und offen zu kommunizieren. Gleichzeitig sollte die Kommunikation außerhalb des Response-Teams auf bestimmte, klar definierte Sprecher beschränkt werden.

Tipp: Puls-Check!

Mitten in der Krise passiert es leicht, dass man von schnell aufeinanderfolgenden Ereignissen überrollt wird und vergisst, Luft zu holen. Während der Planung der Response

sollten Sie daher routinemäßig die Zeit und ein Verfahren für einen »Puls-Check« einplanen, bei dem Sie:

- **den Status überdenken:** Fassen Sie Updates der Responder zusammen, gehen Sie das Feedback durch, beobachten Sie die aktuellen operativen Fähigkeiten der Organisation, bewerten Sie die aktuellen Risiken und bestimmen Sie die aktuellen Ressourcen.
- **die Dokumentation aktualisieren:** Sorgen Sie dafür, dass Response-Aktivitäten und Schlüsselinformationen fortlaufend in einem zentralen Repository (z.B. einem Ticketing-System) dokumentiert werden.
- **die Response-Strategie überprüfen:** Überprüfen Sie Ihre Response-Strategie, inklusive der Ziele, Aufgaben, Verantwortlichkeiten, veranschlagten Fristen, Arbeitsaufwand, Kosten etc. Passen Sie die laufenden Response-Prozesse dem Bedarf an.
- **kommunizieren:** Sorgen Sie dafür, dass Schlüsselinformationen an Responder, Interessengruppen und Drittparteien weitergegeben werden. Dazu gehören aktualisierte Response-Pläne, Ergebnisse von Denial-of-Service-Untersuchungen u. Ä. Informieren Sie je nach Bedarf das Response-Team. Achten Sie auf öffentliche Nachrichten. Holen Sie Feedback ein.

Im Wesentlichen ist der Puls-Check eine schnelle, routinemäßige Prüfung, mit der Sie Ihr Response-Team informieren. Regelmäßige »Puls-Checks« stellen sicher, dass

- sich Response-Aktivitäten an den aktuellen Bedürfnissen und Risiken orientieren,
- die Dokumentation genau, vollständig und aktuell ist,
- die Beziehungen bestmöglich gepflegt werden.

Ihr Team synthetisiert Informationen und nutzt sie, um intelligente und fundierte Entscheidungen zu treffen. Diese Aktivität zieht sich vom Anfang bis zum Ende des gesamten Response-Prozesses durch.

4.7.2 Betroffene Parteien

Ist der Geschäftsbetrieb eines Opfers beeinträchtigt oder sind sensible Daten in Gefahr, wirken sich die Effekte schnell auf Drittparteien aus. Je nach Opfer gehören dazu Kunden, Patienten, Schüler/Studierende, Gemeindemitglieder, Partner und andere. Das gilt insbesondere in den Fällen, in denen die Täter direkt an die Kunden oder andere betroffene Parteien herantreten.

Eine Cybererpressung hat für die Opfer häufig einen Vertrauensverlust bei den betroffenen Parteien und Communities zur Folge. Dieses Vertrauen wieder aufzubauen kostet Zeit und Mühe. Wann immer möglich sollte man mit den wichtigen Interessenvertretern proaktiv kommunizieren, um Vertrauen aufzubauen und zu erhalten. Sie sollten dabei zeitnah, zuverlässig, ehrlich und transparent informieren.

Hier einige Tipps, wie man betroffene Parteien auf dem neuesten Stand hält:

- **Bauen Sie eine effektive Kommunikationsmethode auf.** Wählen Sie eine Kommunikationsmethode, die einfach gepflegt werden kann und leicht zugänglich ist. Regelmäßige Veröffentlichungen oder eine häufig aktualisierte Webseite versorgen ein breites Publikum mit Updates. Prüfen Sie Ihre Kommunikationsoptionen, wenn die technische Infrastruktur des Opfers beeinträchtigt oder offline ist.
- **Wählen Sie einen Sprecher.** Stellen Sie eindeutig klar, wer während der Cybererpressung der primäre öffentliche Sprecher ist. Häufig ist es sinnvoll, diese Rolle einer einzelnen Person zuzuordnen, um einen gleichbleibenden Ton und Inhalt zu wahren. Mehrere Sprecher können durch Unterschiede in der Nachrichtenübermittlung für Verwirrung sorgen. Wählen Sie einen Manager oder PR-Mitarbeiter und bleiben Sie dabei.
- **Entwickeln Sie Muster im Voraus.** Wann immer möglich sollten Sie Kommunikationsmuster schon im Vorfeld entwickeln, damit leitende Mitarbeiter, PR- und Rechtsabteilung die Gelegenheit haben, sie in Ruhe zu überprüfen und zu genehmigen und nicht erst mitten im Chaos eines Notfalls.
- **Nutzen Sie eine formale PR-Strategie.** Entscheiden Sie vorab, wer Inhalte für unterschiedliche Kommunikationsarten entwickelt und genehmigt. Zum Beispiel könnten Sie ein externes PR-Team für die öffentliche Kommunikation einbinden wollen – oder sogar für die Kommunikation mit Regulierungsbehörden und andere Drittparteien.
- **Achten Sie auf Zeit und Zielgruppe.** Ein schnelles Update für die Öffentlichkeit muss für die breite Masse aufbereitet werden, während sich ein Update für leitende Mitarbeiter schwerpunktmäßig eher mit dem Betrieb und mit realistischen Zeitplänen für die Wiederherstellung beschäftigen wird.
- **Bleiben Sie konstant.** Achten Sie auf einen konstanten Informationsfluss, selbst wenn das Update lautet, dass es kein Update gibt. Formulieren Sie klare Erwartungen (»Unser nächstes Update kommt am …«). Lange Zeiten des Schweigens führen unweigerlich zu Spekulationen und Angst – zwei der schlimmsten Reaktionen bei einem Ransomware-Angriff.
- **Vermeiden Sie Funkstille.** Tauchen Sie nicht unter. Das Ausbleiben einer zeitnahen Kommunikation kann als Zeichen schlechter Nachrichten gedeutet werden und zu unnötigen Untersuchungen oder Spekulationen zum aktuellen Stand oder zur Schwere eines Vorfalls führen.

Fallstudie: Abwesenheitsnotiz

Eine kleine Anwaltskanzlei wurde Opfer eines Ransomware-Angriffs. Während an einer Lösung gearbeitet wurde, erhielten die Mitarbeiter plötzlich besorgte Anrufe und Nachrichten von Mandanten. Schnell kam auch eine Anfrage der Medien, obwohl das Unternehmen Ransomware nicht als Grund für den Ausfall genannt hatte.

Es stellte sich heraus, dass ein übermotivierter Anwalt der Kanzlei nach dem Ransomware-Angriff eine Abwesenheitsnotiz für seine E-Mails eingerichtet hatte. Die E-Mail lautete:

> *Unsere Computer wurden gestern von einem Ransomware-Virus befallen. Wir tun alles in unserer Macht Stehende, um das Problem zu beheben und unsere Systeme wiederherzustellen. In der Zwischenzeit bitten wir die Unannehmlichkeiten zu entschuldigen. Im Notfall erreichen Sie uns telefonisch unter [zensiert].*

Diese Nachricht ging an jeden einzelnen seiner E-Mail-Kontakte, auch an externe Dritte.

Während Manager und Incident Responder davon ausgehen können, dass Informationen zu digitaler Erpressung vertraulich zu behandeln sind, ist das für Laien nicht immer offensichtlich. Kommunizieren Sie im Vorfeld klar Ihre Erwartungen bezüglich der Vertraulichkeit und untermauern Sie diese Erwartungen noch einmal, wenn es tatsächlich zu einer Cybererpressung kommt.

4.7.3 Die Öffentlichkeit

Sie können nicht erwarten, dass Informationen zu einer digitalen Erpressung vertraulich bleiben. Die Täter können sich jederzeit dafür entscheiden, gewonnene Daten zu veröffentlichen, einschließlich der Details zu den Verhandlungen, der internen Kommunikation, gestohlene Daten und anderes Material. Nichts ist tabu. Häufig informieren Cybererpresser Journalisten, die Betroffenen oder die Öffentlichkeit. Das Opfer hat auf den Zeitpunkt kaum Einfluss.

Das PR-Team des Opfers sollte so früh wie möglich eingebunden werden. Dazu gehören sowohl interne als auch externe PR-Mitarbeiter. Idealerweise sollte das PR-Team über vorbereitete Stellungnahmen bei Anfragen verfügen sowie über Pressemitteilungen, deren Nutzung im Vorfeld genehmigt wurde.

Schafft es ein Vorfall bis in die Nachrichten, sollte man ein erfahrenes PR-Team engagieren, bevorzugt eines, das Erfahrung damit hat, das Image einer Organisation nach einer Cybererpressung wieder aufzupolieren.

4.8 Fazit

Krisen durch Cybererpressung sind nicht vorhersehbar und potenziell katastrophal. Eine effektive Response kann die Auswirkungen drastisch reduzieren und eine schnelle Wiederherstellung fördern.

In diesem Kapitel haben wir diskutiert, wie man digitale Erpressung erkennt, haben ein System für die Triage vorgestellt und Ratschläge für die Entwicklung einer Response-Strategie gegeben. Der Anfang der Response auf eine Cybererpressung ist eine kritische Phase, bei der die Responder die Lage schnell einschätzen und Aktivitäten priorisieren müssen. Das Ergebnis der Triage-Phase bildet die Grundlage für den Rest des Response-Prozesses.

Im nächsten Kapitel stellen wir effektive Techniken vor, um den Schaden einzudämmen, d.h. die Verschlüsselung durch Ransomware aufzuhalten, das Ausschleusen von Daten zu unterbinden, die Täter auszusperren sowie nach weiteren Bedrohungen zu suchen.

4.9 Sie sind dran!

Jede Cybererpressung ist einzigartig. Die Optionen und Prioritäten des Response-Teams hängen von der Branche, Größe und dem Standort des Opfers ab sowie von den Details des jeweiligen Angriffs.

Basierend auf dem, was Sie in diesem Kapitel gelernt haben, wollen wir die Schlüsselelemente des Triage-Prozesses und der Response-Strategie durchgehen.

Schritt 1: Wählen Sie Ihr Opfer

Wählen Sie eine Charakteristik in jeder Spalte aus, um die Organisation Ihres Opfers zu beschreiben:

Branche	**Größe**	**Standort**
Krankenhaus	groß	weltweit
Finanzinstitut	mittel	USA
Hersteller	klein	Europäische Union
Anwaltskanzlei		Australien
Universität		Indien
Cloud-Anbieter		Land/Standort Ihrer Wahl
Organisation Ihrer Wahl		

Schritt 2: Wählen Sie Ihr Angriffsszenario

Wählen Sie aus einem der folgenden Angriffsszenarien:

A	Ransomware schlägt zu! Alle Dateien des Opfers wurden gesperrt, einschließlich der zentralen Datenrepositorys, Server und Arbeitsplätze.
B	Eine bekannte Bande digitaler Erpresser behauptet, alle sensiblen Daten des Opfers gestohlen zu haben, und droht mit deren Veröffentlichung, wenn das Opfer eine sehr hohe Lösegeldforderung nicht erfüllt. Die Gang veröffentlicht den Namen des Opfers auf ihrer Website im Darknet, zusammen mit einer Auswahl der vermeintlich gestohlenen Daten.
C	Doppelerpressung! A und B treten gleichzeitig ein.
D	Das Opfer wird von einem Denial-of-Service-Angriff seiner Internetinfrastruktur getroffen, die seinen Zugriff und die Dienste einfriert. Der Täter droht mit der Fortführung oder sogar Erweiterung des Angriffs, wenn kein Lösegeld bezahlt wird.

Schritt 3: Diskussion

Ihr Opfer ist mit einer Cybererpressung konfrontiert. Mit dem Wissen um das Opfer und das Szenario im Hintergrund beantworten Sie die folgenden Fragen:

1. Wie könnte sich der Vorfall auf den Normalbetrieb des Opfers auswirken? Welche Prozesse haben für die Wiederherstellung wahrscheinlich die oberste Priorität?
2. Warum ist es für das Team wichtig, während des Vorfalls auf die Dokumentation zugreifen zu können? Nennen Sie zwei Arten von Dokumenten, die die Responder bei einem Vorfall benötigen könnten.
3. Auf wen könnten sich die Effekte des Vorfalls auswirken? Berücksichtigen Sie nicht nur die Mitarbeiter der Organisation, sondern auch möglicherweise betroffene Dritte.
4. Welchen Druck können Drittparteien erzeugen, der Ihre Response beeinflusst? Berücksichtigen Sie jede Drittpartei, die von der Organisation des Opfers abhängig ist, das rechtliche Umfeld, ob die Organisation einer Regulierung unterliegt etc.
5. Stolperstein: Ein Angestellter postet in den sozialen Medien öffentlich etwas über den Vorfall. Wie gehen Sie damit um?

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

Z