edv-buchversand.de

Ransomware und Cyber-Erpressung

Das Praxishandbuch für IT- und Systemverantwortliche

» Hier geht's direkt zum Buch

DAS VORWORT

Dieses Vorwort wird Ihnen von www.edv-buchversand.de zur Verfügung gestellt.

Vorwort

Als der Hip-Hop-Song »Virus« im Jahr 2000 veröffentlicht wurde, ahnte niemand, dass er prophetisch war. Im Liedtext beschreibt der Protagonist (Deltron Zero), der »einen Supervirus entwickeln will«, seine Pläne zur Infizierung und Zerstörung aller Computer auf dieser Welt: »Vernichte deine Umgebung mit einer sanften Berührung/Schrotte dein ganzes Computersystem und werfe dich auf Papyrus zurück«[1].

Mehr als zwei Jahrzehnte später hat Ransomware epidemische Ausmaße angenommen und legt Krankenhäuser, Schulen, Anwaltskanzleien, Kommunen, Unternehmen und Organisationen aller Art lahm. Opfer rund um die Welt werden regelmäßig infiziert und zurück zu Papier und Bleistift gezwungen (wenn sie das Glück haben, noch Büromaterial vorzuhalten).[2,3] Noch schlimmer ist aber, dass die Angreifer die mögliche Veröffentlichung der Informationen als erhebliches Druckmittel erkannt haben, das zu riesigen – und schwerwiegenden – Datenlecks führen kann.

Heutzutage betrachtet man Daten als Waffe. Indem sie die Vertraulichkeit, Integrität und Verfügbarkeit von Daten gefährden, schöpfen Kriminelle Profite ab und zwingen den Opfern ihren Willen auf. Nach Jahren eskalierender Ransomware-Angriffe, dreister Veröffentlichung von Daten und einer Flut von neuen Opfern in den Schlagzeilen haben die Täter ihre Strategien verfeinert und ein flexibles, erfolgreiches Geschäftsmodell aufgebaut.

Die Auswirkungen digitaler Erpressung sind weitreichend. Der Geschäftsbetrieb wurde eingestellt, manchmal temporär, in manchen Fällen aber auch für immer. Patientendaten wurden vernichtet und die Leben dieser Patienten gefährdet. Wichtiges geistiges Eigentum wurde an Mitbewerber verkauft. Private E-Mails und persönliche Daten werden regelmäßig der Öffentlichkeit zugänglich gemacht.

---

1. Deltron 3030, »Virus«. Deltron 3030, 23. Mai 2000, *https://genius.com/Deltron-3030-virus-lyrics*.
2. *www.beckershospitalreview.com/cybersecurity/georgia-health-system-reverts-to-paper-records-after-Ransomware-attack-5-details.html*.
3. *www.forbes.com/sites/tommybeer/2020/09/28/report-big-us-hospital-system-struck-by-cyberattack-forcing-staff-to-resort-to-paper-and-pen/*.

Gerichtsverfahren, die sich mit Ransomware und Datenlecks beschäftigen, nehmen deutlich zu, obwohl Opfer und Versicherer Finanzmittel für Entschädigungen und Schadensbegrenzung zurücklegen. Strafverfolgungsbehörden auf der ganzen Welt versuchen jeden Tag, cyberkriminelle Gruppen zu zerschlagen, auch wenn die Kriminellen über die Medien verlautbaren lassen, davor keine Angst zu haben.

Das Problem ist so allgegenwärtig, dass sich die Leute die volle Tragweite und die Auswirkungen oft gar nicht vorstellen können. Gleichzeitig wird Cybererpressung kaum bekannt. Schließlich melden sich die Opfer nicht gerne bei den Medien, wenn sie gehackt wurden. Die Fälle werden üblicherweise heimlich, still und leise abgewickelt. Folglich ist das wahre Ausmaß digitaler Erpressung unbekannt, aber zweifellos weit größer, als es die Statistiken andeuten.

Die Reaktion (Response) auf einen Angriff ist von wesentlicher Bedeutung. Die in den Stunden, Tagen und Monaten nach einem Ransomware-Angriff vom Opfer unternommenen Schritte können dessen Ausgang wesentlich beeinflussen.

Dieses Buch ist ein praktischer Leitfaden für die Reaktion auf digitale Erpressungsversuche wie Ransomware, Enthüllung von Daten, Denial of Service und viele mehr. Während des gesamten Buches beziehen wir uns auf bekannte Fallbeispiele, aber auch auf eine große Menge unveröffentlichter Fälle, die von den Autoren während ihrer Arbeit als Response-Experten bearbeitet wurden. Die Leser werden auf digitale Erpressungsversuche besser reagieren, den Schaden minimieren und die Wiederherstellung beschleunigen können.

Wie im Buch immer wieder hervorgehoben wird, ist die Cybererpressung üblicherweise die letzte und sichtbarste Phase eines Einbruchs. Häufig haben Cyberkriminelle über einen längeren Zeitraum Zugriff auf die Umgebung oder auf Daten des Opfers, greifen Schlüsselinformationen ab, spionieren ihre Opfer aus und installieren Malware und andere Tools, um ihre Position zu verbessern.

Durch die Nutzung effektiver Präventionsmaßnahmen innerhalb der Gesellschaft können wir das Risiko digitaler Erpressung und Cyberkriminalität im Allgemeinen verringern. Im letzten Kapitel dieses Buches tauchen wir in die der Cybererpressung zugrunde liegenden Ursachen ein und geben Empfehlungen, um dieses Risiko zu reduzieren.

Da sich die Akteure, Tools und Taktiken digitaler Erpressung ständig wandeln, konzentrieren wir uns im gesamten Buch auf bewährte Response- und Präventionstechniken, die Ihnen auch langfristig von Nutzen sein werden.

Wer sollte dieses Buch lesen?

Dieses Buch ist als wertvolle Quelle für all jene gedacht, die an der Prävention, Response, Planung und Entwicklung von Strategien im Bereich digitale Erpressung tätig sind. Dazu gehören:

- Chief Information Officer (CIO) und Chief Information Security Officer (CISO), die für die Planung der Response auf digitale Erpressung und für die Entwicklung von Präventionsstrategien verantwortlich sind
- Experten für Cybersicherheit, Incident Responder, Forensiker, Unterhändler, Krypto-Zahlungsdienstleister und alle anderen, die bei der Response auf Ransomware und Cybererpressung mitarbeiten
- technische Mitarbeiter wie Systemadministratoren, Netzwerktechniker, Helpdesk-Mitarbeiter, Sicherheitsteams und andere Personen, die für die Response auf Cyberangriffe und den Schutz der Umgebung verantwortlich sind
- leitende Angestellte, die die Gefahren digitaler Erpressung und die effektive Response sowie die Präventionsstrategien besser verstehen wollen
- Gesetzgeber, Regulierer, Strafverfolger und jeder, der sich mit den rechtlichen Grundlagen digitaler Erpressung befasst
- jeder, der mehr über Ransomware und Cybererpressung lernen will

Wie dieses Buch aufgebaut ist

Dieses Buch wurde als praktischer Leitfaden für die Response und Prävention von Ransomware und Cybererpressung entworfen. Hier eine Zusammenfassung des Weges, den wir in diesem Buch gehen:

- **Kapitel 1, Auswirkungen:** Cybererpressungen gefährden die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, um gegenüber dem Opfer Druck ausüben zu können. Die vier Arten digitaler Erpressung sind Zugriffsverweigerung, Modifikation, Enthüllung und Pseudo-Erpressung (Faux Extortion). Die Auswirkungen digitaler Erpressung reichen von der Betriebsunterbrechung bis zu finanziellen Einbußen, Reputationsverlust, Gerichtsverfahren und mehr. Neben direkten Angriffen auf die Opfer kompromittieren die Täter technische Zulieferer wie Managed Services Provider (MSPs), Cloud-Anbieter und Softwarehersteller.
- **Kapitel 2, Evolution:** Ransomware und digitale Erpressung gibt es schon länger, als den meisten Menschen bewusst ist, und tritt in unterschiedlichsten Formen auf. In diesem Kapitel betrachten wir die Geschichte der Ransomware und die Auswirkungen auf die betroffenen Organisationen. Danach verfolgen wir ihre Evolution hin zu der florierenden kriminellen Wirtschaft, die sie heute antreibt.
- **Kapitel 3, Anatomie eines Angriffs:** Die eigentliche Erpressung ist die letzte Phase eines digitalen Erpressungsversuchs. Die Angreifer verschaffen sich zuerst Zugang zur technischen Umgebung des Opfers und unternehmen dann Schritte, um den Zugang auszuweiten, das Opfer zu analysieren und sich auf die Erpressung vorzubereiten. In diesem Kapitel gehen wir die Phasen eines digitalen Erpressungsversuchs durch. Dabei identifizieren wir Anzeichen einer

Kompromittierung und geben Tipps zur Reaktion, die einen laufenden Angriff abschwächen oder sogar beenden können.

- **Kapitel 4, Die Krise beginnt:** Die frühen Phasen der Response auf eine digitale Erpressung bestimmen ganz wesentlich, wie schnell sich eine Organisation erholt und den normalen Betrieb wieder aufnehmen kann. In diesem Kapitel zeigen wir, wie man die üblichen frühen Anzeichen für eine Cybererpressung erkennt. Wir behandeln auch das Konzept der Triage und erläutern, warum die Entwicklung einer klaren und effektiven Response-Strategie in der frühen Phase besonders wichtig ist.
- **Kapitel 5, Eindämmung:** Schlägt ein Cybererpresser zu, kann schnelles Handeln die Schäden reduzieren und die Wiederherstellung beschleunigen. In diesem Kapitel diskutieren wir Techniken, die das Ausschleusen von Daten verhindern, die Verschlüsselung/Löschung von Dateien unterbinden und den Angreifer aus der Umgebung des Opfers aussperren. Am Ende des Kapitels sprechen wir über Methoden, Beweise, Werkzeuge, Techniken, Personal und die Ergebnisse bei der Suche nach Bedrohungen.
- **Kapitel 6, Untersuchung:** Sich Zeit für eine Untersuchung zu nehmen, ist für die kurz- und langfristige Lösung von Cybererpressungen besonders wichtig. In diesem Kapitel erklären wir, wann eine Untersuchung beginnt, wie wir das Ausmaß eines Angriffs eingrenzen, wie wir »Patient Null« finden und wie wir Täter identifizieren. Wir diskutieren zudem die Beweissicherung, die die langfristigen Schäden von Cybererpresser-Angriffen reduzieren kann.
- **Kapitel 7, Verhandlung:** Wie kann man mit Kriminellen verhandeln? Dieses Kapitel ist ein praktischer Leitfaden für den Beginn, die Durchführung und den Abschluss der Verhandlungen während einer Erpressung. Sie lernen etwas über das Feilschen, über Lebenszeichen und den Abschluss des Deals. Wir diskutieren auch gängige Fehler während der Verhandlungen und wie man sie vermeidet.
- **Kapitel 8, Zahlung:** Auch wenn die Zahlung eines Lösegelds für einige nicht wünschenswert oder sogar undenkbar ist, wählen viele Opfer diesen Weg. In diesem Kapitel diskutieren wir die Vor- und Nachteile der Zahlung eines Lösegelds und die Einzelheiten des Zahlungsprozesses wie Zahlungsarten, Vermittler, Termine und was nach der Zahlung zu tun ist. Wir diskutieren auch durch Sanktionen verbotene Zahlungen und die notwendige Sorgfalt, die die Opfer walten lassen müssen, bevor sie eine Zahlung vornehmen.
- **Kapitel 9, Wiederherstellung:** Das Ziel jeder Störung besteht darin, den normalen Betrieb wieder aufzunehmen. In diesem Kapitel behandeln wir den Prozess der Wiederherstellung sowie Strategien, die das Risiko des Datenverlustes und der Neuinfektion reduzieren, damit das Opfer den Betrieb vertrauensvoll wieder aufnehmen kann. Hierbei beschreiben wir auch wesentliche Verbesserungen für Ihre Umgebung, die zukünftige Risiken minimieren und Ihre Defensivkraft stärken.

- **Kapitel 10, Prävention:** Digitale Erpressung ist üblicherweise die letzte Phase eines Cyberangriffs. Prävention erreichen Sie grundsätzlich am besten durch ein starkes, ganzheitliches Cybersicherheitsprogramm. In diesem Kapitel behandeln wir die wesentlichen Punkte für den Aufbau eines solchen Cybersicherheitsprogramms. Wir sprechen auch konkrete defensive Schritte an, die das Risiko eines digitalen Erpressungsversuchs reduzieren oder dessen Auswirkungen abschwächen. Wir schließen das Kapitel mit den umfassenden Veränderungen ab, die notwendig sind, um die Epidemie digitaler Erpressungen zu bekämpfen.

Weitere Elemente

In jedem Kapitel sind weitere Elemente enthalten, die wichtige Informationen, Konzepte oder Beispiele hervorheben. Einige Elemente nutzen Icons, um sie einfach erkennen zu können:

- **Lernziele:** eine Aufzählung der im jeweiligen Kapitel behandelten Themen
- **Fallbeispiele:** reale Fälle digitaler Erpressung, die die diskutierten Konzepte demonstrieren
- **Definition:** Erklärung der für Cybererpressung oder Cybersicherheit spezifischen Begriffe

- **Tipp:** praktische Tipps für den Leser

- **Nützlich:** für den Leser nützliche Hintergrundinformation

- Diskussion eines Schlüsselbegriffs und seiner Verwendung in diesem Buch.

Fragen

Am Ende jedes Kapitels gibt es den Abschnitt »Sie sind dran!«, in dem wir Ihnen die Möglichkeit bieten, ein eigenes Szenario aufzubauen. Wir stellen Fragen, über die Sie nachdenken und mit anderen diskutieren können. Wir hoffen, dass dieser Abschnitt Ihnen Möglichkeiten liefert, digitale Erpressungsversuche aus allen Blickwinkeln zu betrachten und zu verstehen, dass es nicht die eine richtige Reaktion auf solche Angriffe gibt.

Checklisten

Am Ende des Buches finden Sie eine Reihe von Checklisten, die Sie immer wieder heranziehen können, um Cybererpressung zu verhindern oder, falls nötig, darauf zu reagieren. Sie fassen die Informationen dieses Buches auf hohem Niveau in einem einfachen Referenzformat zusammen.

Bleiben Sie auf dem neuesten Stand

Regelmäßige Updates und Kommentare zu den neuesten Entwicklungen im Bereich digitale Erpressung und Ransomware finden Sie auf der Webseite der Autoren: *ransombook.com*.

Angriffstaktiken entwickeln sich stetig weiter und mit ihnen auch die Best Practices für Response und Prävention. In diesem Buch stellen wir die Grundlagen für die Response auf digitale Erpressungsversuche vor und wie man diese verheerenden Angriffe verhindert.

Auf der Website der Autoren finden Sie die neuesten Nachrichten, Tipps zur Response, Diskussionsthemen und mehr. Neben dem Teilen von Informationen und Erfahrungen hoffen wir, dass unsere globale Community zusammenarbeiten kann, um etwas Licht ins Dunkel digitaler Erpressung zu bringen und das Risiko zu reduzieren.

Danksagungen

Es braucht ein ganzes Dorf, um ein Buch zu produzieren, und dieses ist keine Ausnahme. Wir möchten den vielen Menschen danken, die dazu beigetragen haben: vom Konzept bis zur Produktion und allem dazwischen.

Zuallererst danken wir unseren Lektoren Haze Humbert und James Manly, deren langjährige Verlagserfahrung und professionelle Einblicke unbezahlbar waren. Wir wissen besonders zu schätzen, wie sie die Herde zusammengehalten und den Prozess geduldig vorwärtsgetrieben haben, während sie uns gleichzeitig Zeit ließen, uns durch die unbekannten Gefilde der Zusammenarbeit während der Pandemie zu navigieren.

Wir danken auch unseren Kollegen Michael Ford und Ben Mayo, die sich die Zeit genommen haben, das Buch in den frühen Phasen Korrektur zu lesen, um sicherzustellen, dass wir die Bedürfnisse unserer Leser umfassend abdecken. Michael hat auch ausführliches und wichtiges Feedback zum gesamten Buch gegeben, für das wir ihm nicht genug danken können. Wir möchten auch Pearsons exzellentem Redaktions- und Produktionsteam danken, einschließlich Julie Nahil, Menka Mehta, Aswini Kumar und Jill Hobbs.

Man *kann* ein Buch nach dem Umschlag beurteilen, und wir schätzen uns glücklich, dass der Künstler Jonah Elgart sein unglaubliches Können für diese Arbeit zur Verfügung gestellt hat. Er hat die Konstruktion echter Piratenschiffe recherchiert, Bilder und Ideen geteilt und sogar einige »Easter Eggs« in der Zeichnung versteckt. Danke, Jonah, dass du unsere geschriebenen Worte mit einem so schönen Kunstwerk schmückst.

Marc Grens, Experte für Kryptowährungszahlungen und Mitgründer von DigitalMint, hat sich freundlicherweise die Zeit für ein ausführliches Interview genommen und viele Fragen zur Entwicklung von Due Diligence und Zahlungsprozessen bei Kryptowährungen umfassend beantwortet. Seine Expertise in diesem Bereich war unbezahlbar, und wir sind sehr dankbar für die Möglichkeit, diese Informationen an unsere Leser weitergeben zu können.

Die Cyberversicherungs-Veteranen Bob Wice und Frank Quinn nahmen sich die Zeit für ein ausführliches Interview, sodass wir einen Blick hinter die Kulissen der Cyberversicherung und des Risikomanagements werfen konnten. Danke für

euer Vertrauen und die Möglichkeit, dieses Wissen mit den Lesern dieses Buches zu teilen.

Ransomware und digitale Erpressung sind ein komplexes und sich schnell weiterentwickelndes Thema. Wir haben durch Erfahrung gelernt, indem wir – mit der Unterstützung unseres unglaublichen Teams – eine Vielzahl von Fällen bei LMG Security bearbeiteten. Vielen Dank an unsere Kollegen bei LMG, insbesondere Derek Rowe, Madison Iler und Dan Featherman. Dank auch an unseren langjährigen Anwalt (jetzt Richter) Shane Vannatta, der uns durch die frühen Tage von Ransomware und Cybererpressung führte.

Wir danken auch unseren vielen Kollegen, die uns über die Jahre hinweghalfen, ein Verständnis für Ransomware und Cybererpressung zu entwickeln: Scott Koller, Ryan Alter, Randy Gainer, David Sande, Marc Kronenberg, Bill Siegel, David Sherman, Katherine Keefe, Brett Anderson, Luke Green, Sue Yi, Mike Wright, Jody Westby, Sean Tassi, Peter Enko, Dave Chatfield, Mark Greisinger, Vinny Sakore, Andrew Lipton, Michael Phillips, Marc Schein und Michael Kleinman.

Jeder von uns möchte auch noch ein paar persönliche Dankesworte aussprechen.

Von Sherri: Vielen Dank an meine Kleinen, Violet und Thunder, deren Liebe und Enthusiasmus mir jeden Tag Auftrieb gaben. Mein Mann Tom Pohl und meine großartigen Freunde Annabelle Winne und Jeff Wilson waren immer für mich da: Sie spornten mich an, hörten zu und gaben kluge Ratschläge. Ohne euch wäre das nicht möglich gewesen. Ich bin auch meinen Freunden und meiner Familie dankbar, insbesondere meinem Vater E. Martin Davidoff, meiner Mutter Sheila Davidoff, meiner Schwester Laura Davidoff Taylor sowie Jessie Clark, Shannon O'Brien, Kaloni Taylor, Steve McArthur, Kevin Head, Samantha Boucher, Deviant Ollam, Kelley Sinclair und so vielen anderen. Eure stete Unterstützung hat mir mal wieder durch den langen Weg des Schreibens eines Buches geholfen. Mehr als alles andere bin ich glücklich, mit Karen Sprenger und Matt Durrin arbeiten zu können, meinen unglaublichen Mitautoren! Ich habe so viel von euch gelernt, sowohl an vorderster Front bei der Response auf Erpressungsfälle als auch beim Schreiben dieses Buches. Ein besseres Team kann man sich nicht wünschen.

Von Matt: Ich möchte besonders meiner Frau Karah Durrin und meiner Tochter Lauren Durrin danken. Sie waren während des Schreibens meine stille Inspiration, und es wäre ohne ihre großartige und unermüdliche Unterstützung nicht möglich gewesen. Ich möchte auch allen Freunden und Verwandten danken, die mir geholfen haben, diesen Weg zu gehen. Neben den Menschen in meinem persönlichen Leben geht ein dickes Dankeschön an das Team von LMG Security, das mir die Möglichkeit bot, Cybersicherheit zu meinem Beruf zu machen. Es war ein wilder Ritt, doch ich bin froh, von einer so wunderbaren und talentierten Gruppe von Menschen umgeben zu sein. Schließlich möchte ich noch meinen Partnern Sherri Davidoff und Karen Sprenger danken. Ohne diese beiden großar-

tigen Frauen hätte ich meine Leidenschaft für Cybersicherheit wohl nie entdeckt. Sherri glaubte an mich und gab mir die Möglichkeit, in das Geschäft einzutauchen. Karen ist nicht nur eine fantastische Sicherheitsexpertin, sondern sie lehrte mich auch, wie man ein sauberes forensisches Festplatten-Image erzeugt. Ich bin sehr dankbar, euch beide als Freunde und Mentoren zu haben. Danke euch beiden, ich freue mich auf unsere nächsten gemeinsamen Abenteuer!

Von Karen: Neben den Obengenannten möchte ich meiner Mutter Genie Thorberg danken, meiner größten Heldin und die Person, die mir gezeigt hat, wie man einen Computer nutzt. Mein Vater Bob Sprenger gab mir zu gleichen Teilen Liebe und Lebensweisheiten. Meine Schwester Rhonda Johnson war die erste und beste von vielen starken Frauen, die mir den Weg wiesen. Meinen Partnern bei diesem Abenteuer, Sherri Davidoff und Matt Durrin, danke ich für Liebe, Lacher und ihr Engagement während dieses Projekts. Zwar bin ich noch nicht zur Nachteule geworden, doch ihr habt eine einschüchternde Aufgabe möglich und, kaum zu glauben, unterhaltsam gemacht. Ich freue mich darauf, in den vielen noch kommenden Jahren viele Cybercrime-News-Links auszutauschen. Ich hatte das große Glück, an den Schlüsselstellen meiner Karriere für von Frauen geführte Unternehmen arbeiten zu können. Dank an Linda Wright und Desiree Caskey, die mir vor vielen Jahren den Einstieg ermöglichten – bevor ich erkannte, dass es nur wenige Frauen in technischen Berufen gibt. Und an Sherri ein besonderes Dankeschön, dass sie das Risiko eingegangen ist und mir den Freiraum gegeben hat, um mit Cybersicherheit und Akquisition auf eigenen Beinen stehen zu können. Durch die Arbeit mit dir habe ich viel gelernt und bin gewachsen. Schließlich möchte ich meinen beiden Pudeln Jasper und Gracie danken, die während der ganzen Zeit viele Stunden zu meinen Füßen lagen und mir Gesellschaft leisteten, sowie Sadie, die gegen Ende dazugestoßen ist. Ohne die drei wäre das alles nicht möglich gewesen.