Alexander Dörsam

Den Tätern auf der Spur

Spannende Fälle aus IT-Sicherheit und IT-Forensik

Springer

Den Tätern auf der Spur

Alexander Dörsam

Den Tätern auf der Spur

Spannende Fälle aus IT-Sicherheit und IT-Forensik

Springer

Alexander Dörsam
Antago GmbH
Heppenheim, Deutschland

ISBN 978-3-658-16465-2 ISBN 978-3-658-16466-9 (eBook)
https://doi.org/10.1007/978-3-658-16466-9

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer

Einbandabbildung: designed by deblik, Berlin © sitcokedoi / AdobeStock

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer ist Teil von Springer Nature
Die eingetragene Gesellschaft ist Springer Fachmedien Wiesbaden GmbH
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Danksagung

Dieses Buch entstand in einer Hochzeit digitaler Angriffe und gibt Erfahrungen wieder, die nur dank höchstem Vertrauen meiner Weggefährten gesammelt werden konnten. Dafür und für das ständige Konfrontieren mit neuen Herausforderungen bei gleichzeitiger Unterstützung gilt mein Dank.

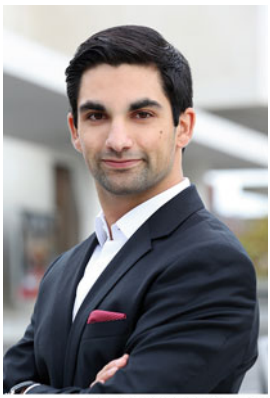
Des Weiteren danke ich meinem Team, auf welches ich mich immer verlassen kann. Ohne den Rückhalt, den Einsatz und die tatkräftige Unterstützung, angefangen von trivialen bis hin zu hoch technischen Angelegenheiten, wäre es sicher nicht möglich gewesen, gemeinsam so erfolgreich digitale Angriffe zu analysieren und darauf zu reagieren.

Mein größter Dank gilt jedoch meiner Familie und meiner Lebensgefährtin. Ohne die moralische und auch tatkräftige Unterstützung wären die Belastungen und Herausforderungen der letzten Jahre nicht zu meistern gewesen.

Somit schreibe zwar ich dieses Buch, aber dennoch handelt es sich um eine außerordentliche Teamleistung, dass ich über die folgenden Sicherheitsvorfälle berichten kann.

Inhaltsverzeichnis

Über den Autor



Fotografin: Sandra Hauer

Alexander Dörsam Jahrgang 1987, ist gefragter Referent und Live-Hacker und gibt sein Know-how über IT-Sicherheit in Fachartikeln, Rundfunk und Fernsehen weiter. Als Leiter der Information Security und Gesellschafter der Antago GmbH beschäftigt er sich täglich mit Sicherheitsvorfällen – z. B. bei Banken, Pharmaunternehmen und Energiekonzernen. Darüber hinaus betreibt er Forschung, unter anderem im Bereich der Sicherheit von Gebäudeleitsystemen, der Anti-Forensik und der Evidence Injection.

Dörsam begann schon im Alter von 12 Jahren mit seinem ersten, damals modernen Intel-Pentium-2-Computer mit der Administration von Netzen und Maschinen. Als Teenager sammelte er Erfahrungen in der Beratung von kleinen Unternehmen und fing an, Webserver und Webseiten aufzusetzen. Vor allem die Belastbarkeit von Netzen und die Themen IT-Sicherheit und Hacking interessierten ihn. Mystische Geschichten von Kevin Mitnick und Filme wie „Hackers" taten ihr Übriges – aus dem Interesse wurde eine Leidenschaft.

So stellte er im heimischen Jugendzimmer ein eigenes kleines Labor zusammen, in dem er von SPS-Steuerungen bis hin zu Computer-Clustern unterschiedlichste Strukturen aufbaute und analysierte. Eine Vielzahl vernetzter Computer sowie durch ihn in Betrieb genommene Klöckner Möller easy, Siemens Simatic S5 und S7 bildeten den Kern der Testumgebung.

Früh war ihm klar, dass sein berufliches Ziel im Bereich der IT-Sicherheit liegen würde. Über Praktika im Bereich der Elektronik bis hin zur Fachhochschulreife verfolgte er den kürzesten Weg ins Studium der Informatik. 2008 konnte er die erste Etappe mit dem Bachelor of Science erfolgreich abschließen. In seiner Abschlussarbeit entwickelte er einen Weg, das bis dato als sicher geltende ITAN-Verfahren des Onlinebankings auszutricksen und Überweisungen automatisiert umzuleiten. Seine Arbeit mit dem Titel „Security flaw of ITAN based online banking" war gleichzeitig auch seine erste Publikation.

Neben dem Studium arbeitete Dörsam parallel als Sicherheitsberater für Webapplikationen und unterstützte Kunden bei der Absicherung gegen professionelle Angriffe. Darüber

hinaus war er Teil des Netzwerkteams des Fraunhofer Instituts für Graphische Datenverarbeitung, wo er unter anderem Controller-basierte WLAN-Netze plante und ausrollte. Seine Praxisphase verbrachte er bei der Deutschen Bank in Eschborn, für die er Sicherheitskonzepte entwickelte.

Mit seiner Abschlussarbeit „Android devices as an attacking tool" für den Master of Science in Informatik widmete er sich 2010 der Idee, komplexe Angriffe auf Infrastrukturen mit sehr einfacher und mobiler Hardware zu realisieren. Dörsam entwickelte eine Software für ein Google-G1-Telefon, mit welchem er unter anderem in der Lage war, komplexe Netzwerkstrukturen anzugreifen und beispielsweise automatisiert Voice-over-IP-Telefonate abzuhören.

Mit diesem umfangreichen Wissen gelang ihm 2010 der Einstieg in die auf IT-Sicherheit spezialisierte Antago GmbH. Dort zeichnete er für Security-Projekte in mittelständischen Unternehmen bis hin zu DAX-30-Konzernen verantwortlich. 2013 übernahm er die Leitung des gesamten technischen IT-Security-Teams und damit die Verantwortung für die Durchführung aller Projekte sowie die Weiterentwicklung des Unternehmens in technischen Sicherheitsbelangen. Gleichzeitig übernahm er Gesellschaftsanteile der Antago GmbH und richtete die Gesellschaft noch stärker auf hoch technische Analysen und die Behandlung von Sicherheitsvorfällen aus.

1

Einleitung

„Den Tätern auf der Spur“ basiert auf echten IT-Sicherheitsvorfällen und führt Sie durch eine Welt von Erpressung, Spionage und digitalem Vandalismus. Sie werden erfahren, wie Angreifer in Strukturen eindringen, welche Methoden dafür eingesetzt werden und welche Folgen daraus resultieren. In diesem Buch werden unterschiedlichste Fälle aus Sicht der IT-Forensik und des Krisenmanagements beschrieben. Eine noch direktere Berichterstattung als die folgende ist kaum möglich. Alle Fälle werden nach Rücksprache und mit Freigabe der betroffenen Unternehmen vorgestellt. Jeder einzelne Fall steht repräsentativ für eine bestimmte Art von Vorfällen und ereignete sich innerhalb der letzten zwei bis drei Jahre. Bei den vorgestellten Fällen handelt es sich nicht um exotische Einzelerscheinungen, obwohl auch diese rasant zunehmen, sondern

A. Dörsam, *Den Tätern auf der Spur*,
https://doi.org/10.1007/978-3-658-16466-9_1

um gängige Praxis und damit auch um die für Sie wahrscheinlichsten Szenarien.

Um möglichst nicht selbst Opfer von Angriffen zu werden oder sich – falls erforderlich – selbst helfen zu können, werden Ihnen abschließend Grundlagen der IT-Sicherheit vermittelt.

Dieses Buches richtet sich an Personen mit einem rudimentären IT-Hintergrundwissen, die sich für IT und IT-Forensik interessieren.

Die Ausrichtung des Buches auf digitale Einbrüche ist darin begründet, dass dieses Thema so stark wie noch nie im Fokus liegt. Kaum eine Woche vergeht ohne Meldungen von Datenverlusten oder digitalen Erpressungen. Selbst Versicherungen haben diesen Trend erkannt und bieten neben klassischen Absicherungen gegen Diebstahl, Einbruch oder Erpressung nunmehr auch die Möglichkeit an, digitale Einbrüche im weitesten Sinne abzusichern. Dies wirft die Frage auf, woher dieser augenscheinliche Anstieg von IT-Sicherheitsvorfällen gekommen ist. Sicherlich ist das Phänomen „Hacking“ durch mehrere Anreize getrieben. Denn es war noch nie so einfach, in digitale Systeme einzubrechen, wie heute.

Dies hat mehrere Gründe:

Auf der einen Seite hat das ursprüngliche Hacker-Ethos „Wissen ist für alle da“ sich bis heute durchgesetzt. Eine Vielzahl von Angriffswerkzeugen ist frei im Internet zugänglich. Neben den eigentlichen Programmen erhält der an (Un-)Sicherheit interessierte Nutzer obendrein häufig eine Benutzeranleitung auf Video, meist sogar in HD.

Die Schwierigkeit, an geeignete Werkzeuge für das Attackieren digitaler Systeme zu kommen, reduziert sich zun-

ächst auf die Fähigkeit, danach zu „googeln“. Mit dem Veröffentlichen solcher Werkzeuge und der damit einhergehenden Inflation von notwendigem Spezialwissen auf Seiten der Angreifer steigt entsprechend auch die Wahrscheinlichkeit eines Angriffes. Je einfacher etwas wird, desto wahrscheinlicher ist auch dessen Umsetzung. Dies ist auch der Grund dafür, dass im Folgenden keine Exoten vorgestellt werden, sondern die am häufigsten aufgetretenen Fälle.

Auf der anderen Seite sieht die Lage so aus, dass zwar die Möglichkeit eines Angriffes immer verbreiteter wird, im Gegenzug das Schutzniveau in IT-Infrastrukturen aber nach meiner eigenen Erfahrung nicht ähnlich stark anwächst. So basieren Angriffe wie „CEO Fraud“ oder „Fake President“ beispielsweise auf technischen Hintergründen, die bereits seit vielen Jahren bekannt sind. Dennoch können solch „alte“ Methoden heute noch erfolgreich gegen Unternehmen, Behörden und Einzelpersonen eingesetzt werden [1].

1.1 Der CEO-Fraud

„CEO Fraud“ ins Deutsche übersetzt bedeutet „Geschäftsführer-Betrug“. Bei diesem Betrug handelt es sich um ein ähnliches Vorgehen wie bei dem bekannten „Enkeltrick“. Eine fremde Person gibt sich als eine vertrauenswürdige, bekannte Person aus. Glaubt dies der Angegriffene, wird der Angreifer versuchen, durch das gewonnene Vertrauen beispielsweise an das Geld des Opfers zu kommen [2].

Der Enkeltrick greift auf sehr einfache Werkzeuge zurück, die sich in einen psychologischen und einen technischen Teil differenzieren lassen.

Technisch sind dazu lediglich ein Telefon und ein Telefonbuch notwendig. Psychologisch wird der Angreifer auf Basis der Beziehungsstellung des Enkels das Opfer um Hilfe bitten und es damit in die „Helfer-Rolle" versetzen. Diese „Helfer-Rolle" wird bei vielen Betrugsarten verwendet, da sie aus verschiedenen Gründen von Menschen eingenommen wird (vgl. [3]).

Alternativ zur Helfer-Rolle wird das Opfer unter Druck gesetzt und versucht, es so zum „unvernünftigen" Handeln zu drängen. Mit diesem technisch sehr einfachen Vorgehen werden bis heute noch immer eine Vielzahl an Senioren um ihr Geld gebracht. Einzig eine erwähnenswerte Form der Professionalisierung hat hier eingesetzt, denn „moderne" Täter fälschen ihre Telefonnummern. Manche bauen ihre Masche darauf auf, dass beispielsweise von der Telefonnummer „110" angerufen wird. Hierzu bedarf es allerdings weiterer technischer Hilfsmittel und einer noch stärkeren kriminellen Energie. Im Ergebnis werden die Senioren nicht von einer beliebigen, ggf. nicht vertrauenswürdigen Telefonnummer angerufen, sondern von der äußerst vertrauenswürdig erscheinenden „110". Ein Ansatz könnte hier sein, dass der „Enkel" behauptet, er bräuchte das Geld als Kaution bei der Polizei.

Nahezu identisch zum Enkeltrick wird bei dem angesprochenen „CEO Fraud" vorgegangen. Die Unterschiede liegen allerdings darin, dass statt des Telefons meist, aber nicht ausschließlich, eine E-Mail verwendet wird. Statt des

„Enkels“ ist dann der Geschäftsführer in der Leitung und fordert beispielsweise eine Überweisung oder die Weitergabe von Informationen. Dieser Umstand zeigt auf, dass in hoch technologisierten Zeiten wie den unseren immer noch mit einfachen Mitteln ein Betrug durchgeführt werden kann.

Das wirft die Frage auf, wie stark die Schere zwischen den Fähigkeiten der Angreifer und den Fähigkeiten der Verteidigung gegen solche Angriffe auseinandergeht und warum das so ist. Denn professionelle digitale Einbrecher verfügen über weitaus mehr Werkzeuge als jene, welche für den digitalen „Enkeltrick“ notwendig sind.

Unabhängig von diesem speziellen Szenario beobachte ich neben dem tatsächlichen Anstieg von Sicherheitsvorfällen auch eine gesteigerte Wahrnehmung der Fälle.

Behauptet ein Unternehmen beispielsweise, dass noch nie etwas passiert sei, ist die eigentliche Frage, ob das Unternehmen überhaupt hätte erkennen können, dass etwas passiert ist. Die aktuelle, subjektive Wahrnehmung der Vielzahl von Angriffen basiert demnach eventuell auch darauf, dass wir mehr Vorfälle erkennen können als in den vergangenen Jahren. Diese verbesserte Wahrnehmung liegt primär daran, dass die Entwicklungen im Bereich „Erkennung“ sehr stark vorangeschritten sind. Speziell hat sich der Zweig Security Information and Event Management (SIEM) weiterentwickelt. SIEM-Konzepte haben zum Ziel, Informationen und Protokolle innerhalb einer Infrastruktur zu korrelieren und mögliche Unregelmäßigkeiten zu melden.

Allerdings nehmen wir auch deshalb ein Mehr an Sicherheitsvorfällen wahr, weil sich die Art der Vorfälle geändert hat und diese öfter in der Presse publiziert werden.

Stellen wir uns vor, ein professioneller Angreifer hat Daten entwendet. Sie gehen am Montagmorgen zur Arbeit und bemerken nichts Ungewöhnliches, alles ist genauso wie am Freitag zuvor. Die Daten sind trotz des Diebstahls ja immer noch bei Ihnen vorhanden, der Angreifer hat lediglich die Informationen kopiert. An einem regulären „Montagmorgen" zu erkennen, dass am Wochenende alle Dateien kopiert wurden, wäre hier die Aufgabe. Diese Form von Angriff wird mit einer hohen Wahrscheinlichkeit lange Zeit unerkannt bleiben, da kein offensichtlicher Schaden eingetreten ist. Nach einem Bericht der Firma FireEye liegt die Reaktionszeit bei Sicherheitsvorfällen in Europa und dem Nahen Osten bei ca. 469 Tagen. So lange bleiben erfolgreiche Hackerangriffe im Schnitt unbemerkt [4].

Der Trend geht jedoch immer mehr in Richtung der professionellen Erpressung der Opfer digitaler Einbrüche. Angreifer stellen explizite Forderungen und drohen mit entsprechenden Maßnahmen, sollten diese nicht erfüllt werden. Ein solcher Angriff wird, im Gegensatz zu einem reinen Datendiebstahl, nicht unbemerkt an Ihnen vorübergehen. Das bedeutet subjektiv betrachtet, ein unentdeckter Datenabfluss über Jahre fühlt sich „besser" an, da der Schaden nicht wahrgenommen wird, als eine akute Erpressung durch einen Angreifer. Denn bei der Erpressung werden Sie direkt mit dem Schaden konfrontiert.

Die Entwicklung dieses Trends, weg vom „stillen" Datendiebstahl hin zur offensiven Erpressung, ist mehr als spannend. Denn warum kommt es erst jetzt vermehrt zu diesen digitalen Erpressungen?