KEVIN D. MITNICK
MIT ROBERT VAMOSI

DIE KUNST DER ANONYMITÄT IM INTERNET

SO SCHÜTZEN SIE IHRE IDENTITÄT UND IHRE DATEN

mitp

Dank

Dieses Buch ist meiner liebevollen Mutter Shelly Jaffe gewidmet und meiner Großmutter Reba Vartanian, die beide während meines gesamten Lebens eine Menge für mich geopfert haben. Ganz egal, in welche Lage ich mich selbst gebracht habe, meine Mutter und meine Oma waren immer für mich da, vor allem dann, wenn ich sie gebraucht habe. Dieses Buch wäre niemals möglich gewesen ohne meine wundervolle Familie, die mir in meinem Leben so viel bedingungslose Liebe und Unterstützung zuteilwerden ließ.

Am 15. April 2013 verstarb meine Mutter nach einem langen Kampf gegen den Lungenkrebs. Das Ende kam nach leidvollen Jahren, die vom Ringen mit den Nebenwirkungen der Chemotherapie geprägt waren. Es gab nur wenige gute Tage nach den schrecklichen Behandlungen, mit denen die moderne Medizin diese Krebsarten bekämpft. Normalerweise bleibt den Patienten nur eine kurze Zeit – meist nur ein paar Monate –, bis sie dieser Krankheit erliegen. Ich empfinde die Zeit, die ich mit meiner Mutter verbringen durfte, während sie diesen schrecklichen Kampf gegen den Krebs führte, als ein großes Glück. Ich bin so dankbar dafür, von solch einer liebevollen und fürsorglichen Mutter großgezogen worden zu sein, und sie war zugleich auch meine beste Freundin. Meine Mutter war ein so unglaublich wunderbarer Mensch und sie fehlt mir sehr.

Am 7. März 2012 starb meine Großmutter überraschend während einer Behandlung im Sunrise Hospital in Las Vegas. Unsere Familie hatte erwartet, dass sie wieder nach Hause zurückkehrt, doch so kam es nicht. Die letzten Jahre des Lebens meiner Großmutter waren durch den Kampf meiner Mutter gegen den Krebs sehr belastet gewesen. Wir vermissen meine Großmutter sehr und ich wünschte, sie wäre hier, um diesen Erfolg mit mir zu genießen.

Ich hoffe, dieses Buch erfüllt die Herzen meiner Mutter und meiner Großmutter mit Freude und dass es sie stolz macht, dass ich Menschen helfe, ihr Recht auf Privatsphäre zu schützen.

Ich wünschte, mein Vater, Alan Mitnick, und mein Bruder, Adam Mitnick, wären hier, um die Veröffentlichung dieses wichtigen Buches zu feiern, das erklärt, wie man in Zeiten, in denen Spionage und Überwachung die Norm sind, anonym sein kann.

Ich hatte das Glück, beim Schreiben dieses Buches mit dem Sicherheits- und Datenschutzexperten Robert Vamosi zusammenarbeiten zu können. Robs bemerkenswerte Sicherheitskenntnisse und seine Talente als Autor umfassen auch seine Fähigkeiten, spannende Geschichten zu finden, Themen zu recherchieren und die Informationen, die ich ihm gebe, in einem Stil und auf eine Art zu Papier zu bringen, dass auch Leser, die keine Technik-Profis sind, sie verstehen können. Ich ziehe meinen Hut vor Rob, der eine enorme Menge harter Arbeit in dieses Projekt investiert hat. Um ehrlich zu sein, ohne ihn hätte ich das nicht geschafft.

Ich möchte unbedingt auch den Menschen danken, die meine berufliche Karriere begleitet und sich auf außergewöhnliche Art eingebracht haben. Mein Literaturagent David Fugate von LaunchBooks handelte den Vertrag aus und vermittelte zwischen dem Verlag Little, Brown. Das Konzept zu *Die Kunst der Anonymität im Internet* wurde von John Rafuse von 121 Minds entwickelt, der mein Agent für Vorträge und andere Engagements ist, und er kümmert sich auch um die strategische Geschäftsentwicklung in meinem Unternehmen. Ganz auf eigene Initiative kam John mit einer faszinierenden Buchidee auf mich zu und brachte auch gleich einen Cover-Entwurf mit. Er ermutigte mich sehr, dieses Buch zu schreiben, um die Menschen auf der Welt zu lehren, wie sie ihr Recht auf Privatsphäre vor Übergriffen durch Big Brother und Big Data schützen können. John ist klasse.

Ich bin dankbar dafür, dass ich mit Little, Brown an der Entwicklung dieses aufregenden Projekts arbeiten konnte. Mein Dank gilt meinem Lektor, John Parsley, für all seine harte Arbeit und seine großartigen Ratschläge bei diesem Projekt. Danke, John.

Ich möchte meinem Freund Mikko Hypponen, Chief Research Officer bei F-Secure, dafür danken, dass er seine wertvolle Zeit dem Schreiben eines Vorworts für dieses Buch gewidmet hat. Mikko ist ein sehr renommierter Sicherheits- und Datenschutzexperte, dessen Schwerpunkt seit über 25 Jahren die Malware-Forschung ist.

Ich möchte auch Tomi Tuominen von F-Secure danken, dass er sich zwischen seinen beruflichen Terminen Zeit genommen hat, das Manuskript unter technischen Gesichtspunkten durchzusehen und mir zu helfen, Fehler zu entdecken und alles, was zuvor übersehen wurde.

1

Ihr Passwort kann geknackt werden!

Jennifer Lawrence konnte das lange Wochenende am Labor Day wohl nicht genießen. Die Oscarpreisträgerin war eine von mehreren Prominenten, die eines Morgens im September 2014 feststellen mussten, dass ihre intimsten Fotos – darunter zahlreiche Nacktaufnahmen – überall im Internet kursierten.

Halten Sie einfach mal einen Moment lang inne und lassen Sie all die Fotos vor Ihrem geistigen Auge vorüberziehen, die momentan auf Ihrem Computer, Ihrem Smartphone oder bei Ihrem E-Mail-Provider gespeichert sind. Sicher, viele davon sind völlig harmlos. Es würde Ihnen überhaupt nichts ausmachen, wenn die ganze Welt die Sonnenuntergänge, die niedlichen Schnappschüsse von Ihrer Familie oder sogar das witzige Selfie mit Ihren verstrubbelten Haaren zu sehen bekäme. Aber wären Sie wirklich damit einverstanden, jedes einzelne Foto mit der Öffentlichkeit zu teilen? Wie würden Sie sich fühlen, wenn plötzlich all diese Bilder online auftauchten? Auch wenn sie nicht alle im engeren Sinne anzüglich sind, so sind private Fotos doch Aufnahmen intimer Momente. Wir sollten selbst entscheiden können, ob, wann und auf welche Art wir solche Bilder mit anderen teilen, doch wenn wir Cloud-Dienste nutzen, haben wir diese Wahl oft nicht.

Was Jennifer Lawrence passiert war, beherrschte während des langen Labor-Day-Wochenendes die Nachrichten. Es war Teil eines Vorfalls, der als »The Fappening« bekannt wurde: ein großer Leak[1], bei dem Nackt- und Beinahe-Nacktfotos von Rihanna, Kate Upton, Kaley Cuoco, Adrianne Curry und fast 300 weiteren Stars – hauptsächlich Frauen – öffentlich wurden, weil man es irgendwie geschafft hatte, auf deren Handyfotos zuzugreifen und diese zu verbreiten. Wie nicht anders zu erwarten, waren einige Leute

durchaus interessiert daran, sich diese Fotos anzusehen. Doch vielen Menschen rief dieses Ereignis auch auf beunruhigende Art in Erinnerung, dass ihnen das Gleiche hätte passieren können.

Wie konnte es also dazu kommen, dass jemand auf die privaten Fotos von Jennifer Lawrence und den anderen zugreifen konnte?

Da all diese Stars ein iPhone hatten, konzentrierten sich die Spekulationen zunächst auf eine schwere Datenpanne bei Apples iCloud, einem Cloud-Speicher-Dienst für iPhone-Nutzer. Dabei werden Fotos, neue Dateien, Musik und Spiele, sobald auf dem physischen Gerät kein Platz mehr ist, stattdessen auf einem Server von Apple gespeichert, normalerweise für eine geringfügige monatliche Gebühr. Google bietet einen ähnlichen Service für Android-Handys an.

Apple, ein Unternehmen, das sich sonst so gut wie nie zu Datenschutzfragen in den Medien äußert, stritt jeden Fehler auf seiner Seite ab und bezeichnete den Vorfall als »gezielten Angriff auf Benutzernamen, Passwörter und Sicherheitsfragen«. Weiter heißt es in der Erklärung, dass in keinem der von Apple untersuchten Fälle irgendwelche Pannen in Apple-Systemen, einschließlich der iCloud oder der App »Mein iPhone suchen«, Ursache des Problems waren.[2]

Die Fotos waren als Erstes in einem Hacker-Forum aufgetaucht, das dafür bekannt war, dass dort kompromittierende Bilder gepostet wurden.[3] Innerhalb dieses Forums finden angeregte Diskussionen über die digitalen forensischen Werkzeuge statt, die genutzt werden, um sich solche Fotos heimlich zu beschaffen. Wissenschaftler, Ermittler und Strafverfolgungsbehörden nutzen eben diese Tools, um auf Daten auf elektronischen Geräten oder in der Cloud zuzugreifen, in der Regel zur Aufklärung einer Straftat. Und natürlich dienen diese Tools auch noch anderen Zwecken.

Eines der Tools, das in diesem Forum offen besprochen wurde, war der Elcomsoft Phone Password Breaker, kurz EPPB, der Strafverfolgungs- und Regierungsbehörden Zugang zur iCloud ermöglichen soll. Er ist frei verkäuflich, und er ist nur eines von vielen derartigen Werkzeugen, wenn auch offenbar das beliebteste in diesem Internetforum. Wer den EPPB einsetzen möchte, braucht den iCloud-Benutzernamen der Zielperson sowie Informationen zu ihrem Passwort. Doch für die Leute, die in diesem Forum unterwegs sind, ist die Beschaffung von iCloud-Benutzernamen und Passwörtern kein Problem. Und so kam es, dass jemand an einem Feiertagswochenende im Jahr 2014 auf einer beliebten Onlineplattform für Softwareentwickler (GitHub) ein Tool namens iBrute bereitstellte, ein Mechanismus zum Kna-

cken von Passwörtern, der speziell dazu entwickelt worden war, an die iCloud-Zugangsdaten von praktisch jedem zu gelangen.

Nutzt man iBrute und EPPB zusammen, kann man sich als eine andere Person ausgeben, um sich dann eine vollständige Kopie der in der Cloud gespeicherten iPhone-Daten dieses Opfers auf ein anderes Gerät herunterzuladen. Dass dies grundsätzlich möglich ist, kommt Ihnen zugute, wenn Sie beispielsweise Ihr Telefon gegen ein neueres Modell austauschen. Doch ein Angreifer kann diese Funktion ausnutzen und so alles sehen, was Sie jemals mit Ihrem mobilen Gerät gemacht haben. Er kommt dadurch an weit mehr Informationen, als wenn er sich lediglich in den iCloud-Account seines Opfers einloggen würde.

Der Forensiker und Sicherheitsexperte Jonathan Zdziarski erklärte dem Magazin *Wired*, dass seine Untersuchungen, beispielsweise der unbefugt veröffentlichten Fotos von Kate Upton, auf den Gebrauch von iBrute und EPPB hindeuteten. Durch den Zugriff auf ein wiederhergestelltes iPhone-Back-up erlangt ein Angreifer jede Menge persönlicher Informationen, mit denen er das Opfer später erpressen kann.[4]

Im Oktober 2016 wurde der 36-jährige Ryan Collins aus Lancaster, Pennsylvania, im Zusammenhang mit diesem Hackerangriff zu einer 18-monatigen Gefängnisstrafe verurteilt, und zwar wegen des »unbefugten Zugriffs auf geschützte Computer, um an Informationen zu gelangen«. Konkret wurde er des illegalen Zugriffs auf über 100 Apple- und Google-E-Mail-Konten beschuldigt.[5]

Um Ihren iCloud- oder einen anderen Online-Account zu schützen, brauchen Sie ein gutes Passwort. Das versteht sich eigentlich von selbst. Und doch weiß ich aus meiner Erfahrung als Penetrationstester (Pen-Tester) – also als jemand, der dafür bezahlt wird, Computernetzwerke zu hacken, um deren Schwachstellen zu finden –, dass viele Leute, sogar Führungskräfte großer Unternehmen, ziemlich faul sind, wenn es um Passwörter geht. Kaum zu glauben, doch Michael Lynton, CEO von Sony Entertainment, nutzte »sonyml3« als Passwort für sein Domain-Benutzerkonto. Da ist es nun wahrlich nicht überraschend, dass seine E-Mails gehackt und im Netz verbreitet wurden, zumal die Angreifer den administrativen Zugriff auf fast alles innerhalb des Unternehmens hatten.

Neben den Passwörtern im beruflichen Kontext gibt es auch noch die, die Ihre ganz privaten Konten schützen. Ein Passwort, das schwer zu erraten ist, bietet zwar auch keinen echten Schutz vor Hacking-Tools wie oclHashcat