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

(ein Passwort-Cracker, der Grafikprozessoren – sogenannte GPUs – zum ultraschnellen Knacken von Passwörtern einsetzt), doch immerhin würde es den Prozess so sehr verlangsamen, dass sich der Hacker möglicherweise ein leichteres Ziel sucht.

Im Juli 2015 wurde das Seitensprungportal Ashley Madison Ziel eines Hackerangriffs. Man kann davon ausgehen, dass viele der Passwörter, die dabei öffentlich wurden, auch an anderer Stelle genutzt werden, zum Beispiel fürs Onlinebanking oder für Arbeitsrechner. Am häufigsten tauchten unter den 11 Millionen online geposteten Ashley-Madison-Passwörtern folgende Kombinationen auf: »123456«, »12345«, »password«, »DEFAULT«, »123456789«, »qwerty«[6], »12345678«, »abc123« und »1234567«. Haben Sie eines Ihrer eigenen Passwörter wiedererkannt? Dann sind Ihre Daten alles andere als sicher, da diese gängigen Passwörter in fast alle Tools zum Knacken von Passwörtern integriert sind, die im Netz kursieren. In jedem Fall ist es sinnvoll, ab und zu auf der Seite *www.haveibeenpwned.com* zu überprüfen, ob der eigene Account bereits gehackt wurde.

Im 21. Jahrhundert können wir bessere Passwörter finden – wesentlich bessere, mit längeren und viel komplizierteren Kombinationen aus Buchstaben und Ziffern. Das klingt zunächst schwierig, aber ich zeige Ihnen sowohl eine maschinelle als auch eine händische Methode, um das zu bewerkstelligen.

Am einfachsten ist es, sich die Passwörter nicht mehr selbst auszudenken, sondern den gesamten Prozess zu automatisieren. Dazu gibt es verschiedene digitale Passwort-Manager. Diese speichern nicht nur die Passwörter an einem gesicherten Ort ab, an dem sie bei Bedarf mit nur einem Klick zugänglich sind, sondern sie generieren auch ein neues, wirklich starkes, einzigartiges Passwort für jede Seite, für die man eines braucht.

Man sollte sich aber darüber im Klaren sein, dass diese Lösung zwei Nachteile hat. Der erste ist, dass es ein Master-Passwort gibt, das Zugang zum Passwort-Manager gewährt. Wenn nun jemand Ihren Computer mit einem Schadprogramm infiziert, das durch Keylogging, also das Überwachen sämtlicher Tastatureingaben, Ihr Master-Passwort und Ihren Passwort-Speicher stiehlt, dann heißt es: Game over. Diese Person kennt dann alle Ihre Passwörter. Bei meinen Jobs als Pen-Tester habe ich manchmal den Passwort-Manager durch eine modifizierte Version ersetzt (das funktioniert nur bei quelloffenen Passwort-Managern), die uns das Master-Passwort übermittelte. Vorher hatten wir uns bereits den Admin-Zugang zum Netzwerk unseres Auftraggebers verschafft. Nun hatten wir es auf all die vertrau-

lichen Passwörter abgesehen. Mit anderen Worten: Wir nutzten den Passwort-Manager als Hintertür, um an die Schlüssel zum Königreich zu gelangen.

Der andere Nachteil liegt auf der Hand: Wenn Sie das Master-Passwort verlieren, dann verlieren Sie alle Ihre Passwörter. Im Grunde ist das nicht so schlimm, schließlich können Sie ja auf jeder einzelnen Website Ihr Passwort zurücksetzen lassen, aber wenn Sie viele Accounts haben, ist das ein Riesenaufwand.

Ungeachtet dessen sollten die folgenden Tipps mehr als ausreichend sein, um einen hohen Passwortschutz sicherzustellen:

Zunächst einmal sollten Sie keine Passwörter, sondern sogenannte »Passphrasen« verwenden. Gute Passphrasen sind lang: mindestens 20 bis 25 Zeichen. Zufällige Zeichenfolgen wie *ek5iogh#skf@skd* eignen sich am besten. Leider können sich Menschen solche Zufallsfolgen nur schwer merken. Aus diesem Grund sollten Sie einen Passwort-Manager nutzen. Damit fahren Sie wesentlich besser, als wenn Sie sich Ihre Passwörter selbst ausdenken. Ich bevorzuge Open-Source-Passwort-Manager wie Password Safe und KeePass, die Daten nur lokal auf dem Rechner abspeichern.

Eine weitere wichtige Regel für mehr Passwort-Sicherheit lautet: Nutzen Sie niemals dasselbe Passwort für zwei oder mehr Accounts. Ich weiß, das ist hart, denn heutzutage braucht man für nahezu alles ein Passwort. Das spricht also wieder für den Einsatz eines Passwort-Managers, der beliebig viele gute, einzigartige Passwörter generiert und auch speichert.

Doch selbst wenn Sie ein starkes Passwort haben, kann man Sie mit der richtigen Technologie überlisten. Es gibt Programme, die Passwörter erraten, wie John the Ripper, ein kostenloses Open-Source-Programm, das sich jeder herunterladen kann.[7] Es arbeitet nach den vom Benutzer eingestellten Konfigurationsparametern, das heißt, dass man beispielsweise angeben kann, wie viele Zeichen beim Raten genutzt werden sollen, ob auch Sonderzeichen oder Zeichensätze aus anderen Sprachen berücksichtigt werden sollen usw. John the Ripper und die anderen Passwort-Cracker vertauschen dann immer wieder die Zeichen anhand bestimmter Regeln, die sich als extrem effektiv zum Knacken von Passwörtern erwiesen haben. Letztlich läuft es darauf hinaus, dass sie so lange jede mögliche Kombination aus Ziffern, Buchstaben und Symbolen innerhalb der vorgegebenen Parameter ausprobieren, bis sie Erfolg haben. Doch zum Glück legen sich die meisten von uns nicht gleich mit ganzen Staaten an, denen unbegrenzt Zeit und Ressourcen zur Verfügung stehen. Wesentlich wahrscheinlicher ist es, dass wir

es mit unserem Partner oder einem Familienmitglied zu tun haben oder mit jemandem, dem wir auf den Schlips getreten sind. Diese Leute haben weder die Zeit noch die Ressourcen, um ein 25-stelliges Passwort zu knacken.

Nehmen wir nun mal an, dass Sie sich entschieden haben, Ihre Passwörter auf die altmodische Art zu generieren, und dass Sie sich wirklich sichere Passwörter ausgedacht haben. Es mag Sie überraschen, aber es ist tatsächlich völlig okay, sie aufzuschreiben. Nur sollten Sie nicht schreiben: »Postbank: 4the1sttimein4ever*.« Das wäre zu offensichtlich. Stattdessen sollte man den Namen, also im Beispiel den der Bank, durch etwas Kryptisches ersetzen, etwa »Keksdose« (weil manche Leute früher ihr Geld in Keksdosen versteckt haben) und sich dazu dann nur »4the1st.« notieren. Der vollständige Satz ist gar nicht nötig, denn der Rest fällt einem dann von selbst ein. Aber jemand anderem vielleicht nicht.

Jeder, der eine ausgedruckte Liste mit solchen unvollständigen Passwörtern findet, sollte einigermaßen verwirrt sein – zumindest am Anfang. Dazu eine kleine Geschichte: Ich war bei einem Freund, einem sehr bekannten Microsoft-Mitarbeiter, zu Besuch. Während des Abendessens sprachen wir mit seiner Frau und seinem Kind über die Sicherheit von Passwörtern. Plötzlich stand die Frau meines Freundes auf und ging zum Kühlschrank. Sie hatte all ihre Passwörter auf einen einzigen Zettel geschrieben und diesen mit einem Magneten an die Kühlschranktür gepinnt. Mein Freund schüttelte nur den Kopf, und ich konnte mir ein Grinsen nicht verkneifen. Passwörter aufzuschreiben ist sicherlich keine optimale Lösung, selten genutzte starke Passwörter zu vergessen allerdings ebenfalls nicht.

Einige Websites, zum Beispiel die von Banken, sperren den Zugang nach mehreren falschen Passworteingaben, in der Regel drei. Es gibt aber auch noch immer viele Websites, die das nicht tun. Und selbst wenn eine Seite jemanden nach drei Fehlversuchen aussperrt, ist das kein wirklicher Schutz, denn die Bösewichte nutzen John the Ripper oder oclHashcat sowieso auf eine andere Art. (oclHashcat ist übrigens viel wirkungsvoller als John the Ripper, weil es den Hacking-Prozess auf mehrere GPUs verteilt.) Hacker probieren in der Regel nicht alle möglichen Passwörter live auf der Seite aus.

Angenommen, es gab eine Datenpanne und im Datenschutt, der dabei zutage tritt, befinden sich auch Nutzernamen und Passwörter. Doch diese Passwörter sind zunächst einmal ein ziemliches Durcheinander. Wie kann das also jemanden dabei helfen, in Ihren Account einzubrechen?

Dazu müssen Sie Folgendes wissen: Immer dann, wenn Sie ein Passwort eingeben, sei es nun, um Ihren Laptop freizuschalten oder um einen Online-Dienst zu nutzen, durchläuft das Passwort den Algorithmus einer Einwegfunktion, bekannt als Hashfunktion bzw. Streuwertfunktion. Das ist nicht das Gleiche wie Verschlüsselung. Eine Verschlüsselung geht in beide Richtungen, das heißt, man kann sowohl ver- als auch entschlüsseln, wenn man den Schlüssel hat. Ein Hash dagegen ist wie ein Fingerabdruck, der eine bestimmte Zeichenfolge repräsentiert. Eine solche Einwegfunktion lässt sich nicht umkehren, zumindest nicht leicht.

In der Passwort-Datenbank Ihres herkömmlichen PCs, Ihres mobilen Endgeräts oder Ihres Accounts in der Cloud ist nicht »AlleMeineEntchen12345&« gespeichert, sondern dessen Hashwert. Diese Folge aus Zahlen und Buchstaben ist ein sogenanntes Token, das für das entsprechende Passwort steht.[8]

Im geschützten Speicherbereich Ihres Computers befinden sich also nicht die Passwörter selbst, sondern die Passwort-Hashwerte, und diese sind es auch, die bei einem gezielten Angriff oder einer Datenpanne in falsche Hände geraten können. Sobald ein Hacker diese Passwort-Hashwerte hat, stehen ihm verschiedene öffentlich zugängliche Tools wie John the Ripper oder oclHashcat zur Verfügung, um den Hash zu knacken und an das eigentliche Passwort zu gelangen, sei es auf die brachiale Art, das heißt mit der sogenannten Brute-Force-Methode (jede mögliche alphanumerische Kombination ausprobieren), oder indem er eine Liste von Wörtern, beispielsweise ein Wörterbuch, nutzt. John the Ripper und oclHashcat erlauben es, die Wörter, die man ausprobiert, nach bestimmten Regel zu modifizieren. Dazu stehen zahlreiche Algorithmen zur Wahl, zum Beispiel »Leetspeak«, ein System, bei dem Buchstaben durch Ziffern ersetzt werden, zum Beispiel »k3v1n m17n1ck«. Dieser Algorithmus würde also alle Passwörter in verschiedene Leetspeak-Varianten umwandeln. Solche Methoden zum Knacken von Passwörtern sind natürlich wesentlich effektiver als »Brute Force«. Die einfachsten und verbreitetsten Passwörter werden als Erstes geknackt, bei den komplexeren dauert es etwas länger. Wie lange genau, hängt von verschiedenen Faktoren ab.

Wenn Hacker nun also einen Passwort-Cracker zusammen mit einem geklauten Benutzernamen und einem Passwort-Hash einsetzen, können sie sich Zugang zu einem oder mehreren Ihrer Accounts verschaffen. Dazu pro-

bieren sie das Passwort auf weiteren Websites aus, die mit Ihrer E-Mail-Adresse oder anderen Erkennungszeichen in Verbindung stehen.

Im Allgemeinen gilt: Je mehr Zeichen Ihr Passwort hat, desto länger brauchen Programme wie John the Ripper, um alle erdenklichen Varianten auszuprobieren. Doch da die Prozessoren der Computer immer schneller werden, hat sich auch die Zeit, die nötig ist, um beispielsweise alle möglichen sechs- oder sogar achtstelligen Passwörter zu berechnen, deutlich verkürzt. Aus diesem Grund empfehle ich Ihnen, Passwörter mit 25 oder mehr Zeichen zu verwenden.

Nachdem Sie nun sichere Passwörter generiert haben – und zwar viele davon –, lautet die Regel: Verraten Sie sie niemandem. Eine Selbstverständlichkeit, sollte man meinen. Untersuchungen in London und anderen Großstädten haben jedoch gezeigt, dass Leute bereit sind, im Austausch gegen banale Dinge wie einen Stift oder ein Stück Schokolade ihr Passwort preiszugeben.[9]

Ein Freund von mir gab einmal seiner Freundin sein Netflix-Passwort. Es war einfach praktisch zu diesem Zeitpunkt, er fand es schön, dass sie nun den Film aussuchen konnte, den sie dann beide zusammen anschauten. Doch bei den Filmempfehlungen von Netflix stehen unweigerlich auch die »Weil Sie … gesehen haben«-Filme, darunter auch solche, die er mit seinen Exfreundinnen gesehen hatte. Die Abenteuerkomödie *Eine für 4* war zum Beispiel ein Film, den er sich alleine niemals angesehen hätte – und seine Freundin wusste das.

Natürlich hat jeder eine Vergangenheit, und man fände es wahrscheinlich sogar merkwürdig, sich mit jemandem zu treffen, der vorher in keiner Beziehung war. Aber welche Freundin möchte schon plötzlich ganz unmittelbar mit dem Beweis für die Existenz dieser Vorgängerinnen konfrontiert werden?

Genauso wie man Online-Dienste durch Passwörter schützt, sollte man auch den Zugang zu seinen verschiedenen Geräten mit Passwörtern sichern. Die meisten von uns habe heute einen Laptop, viele auch noch einen Desktop-PC. Vielleicht sind Sie gerade allein zu Hause, aber was ist mit den Gästen, die später zum Abendessen vorbeischauen? Wollen Sie es wirklich darauf ankommen lassen, dass einer von ihnen Ihre Dokumente, Fotos und Spiele sieht, einfach indem er an Ihrem Schreibtisch sitzt und die Maus bewegt? Dazu gleich noch ein abschreckendes Beispiel in Zusammenhang mit Netflix, das sich zu der Zeit ereignete, als Netflix noch vor allem

DVDs per Post verschickte. Damals spielte jemand einem Paar, das ich kenne, einen fiesen Streich. Während einer Party bei sich zu Hause ließen die beiden den Browser und ihren Netflix-Account offen. Einige Zeit später entdeckten sie dann jede Menge anzüglicher B- und C-Movies auf ihrer Warteliste – allerdings erst, nachdem bereits einige dieser Filme in ihrem Briefkasten gelandet waren.

Noch wichtiger ist der Passwortschutz im Büro. Überlegen Sie mal, wie oft es vorkommt, dass Sie plötzlich den Schreibtisch verlassen müssen, weil Sie jemand zu einer spontanen Besprechung ruft. Jeder, der an Ihrem Schreibtisch vorbeikommt, könnte dann das Kalkulationsblatt für das Budget des nächsten Quartals sehen oder all die E-Mails in Ihrem Posteingang. Und wenn Sie Ihren Schreibtisch für längere Zeit verlassen, etwa in der Mittagspause oder für ein längeres Meeting, kann es sogar noch schlimmer kommen: Jemand könnte von Ihrem Schreibtisch aus in Ihrem Namen eine E-Mail schreiben oder die Zuteilung des Budgets fürs nächste Quartal verändern – es sei denn, Sie haben einen passwortgeschützten Bildschirmschoner, der nach ein paar Sekunden Inaktivität von allein startet.

Um sich zu schützen, gibt es zudem sehr kreative Methoden, etwa eine Software zum Sperren des Bildschirms, die Bluetooth nutzt, um zu prüfen, ob Sie sich in der Nähe Ihres Computers befinden. Sobald Ihr Handy nicht mehr in Bluetooth-Reichweite ist, weil Sie beispielsweise mal kurz zur Toilette gehen, wird der Bildschirm sofort gesperrt. Es gibt auch Varianten dieser Software, die ein anderes Bluetooth-Gerät, zum Beispiel ein Armband oder eine Smartwatch, verwenden und dasselbe leisten.

Online-Accounts und -Dienste mit Passwörtern zu schützen ist zwar sinnvoll, hilft aber auch nichts, sobald jemand das physische Gerät in seinen Besitz bringt, vor allem dann nicht, wenn diese Online-Accounts auch noch offen sind. Wenn es also eine Gruppe von Geräten gibt, die auf jeden Fall passwortgeschützt sein sollte, dann sind es die mobilen. Bei ihnen ist das Risiko, dass sie gestohlen werden, am größten. Dennoch fand die Verbraucherorganisation Consumer Reports heraus, dass 34 Prozent der US-Amerikaner ihr Mobilgerät überhaupt nicht schützen, nicht einmal mit einer einfachen vierstelligen PIN zum Entsperren des Bildschirms.[10]

Im Jahr 2014 gab ein Polizist in der Stadt Martinez in Kalifornien zu, Nacktfotos vom Handy einer Frau gestohlen zu haben, die wegen des Verdachts auf Alkohol am Steuer mit der Polizei zu tun hatte. Die Tat des Polizisten ist eindeutig ein Verstoß gegen den 4. Zusatzartikel zur Verfassung

der Vereinigten Staaten, der amerikanische Bürger vor staatlichen Übergriffen schützen soll.[11] Insbesondere verbietet dieser Artikel unangemessene Durchsuchungen und Beschlagnahmungen, die ohne richterlichen Beschluss und ohne hinreichenden Verdacht durchgeführt werden. Konkret bedeutet das, dass amerikanische Polizisten beispielsweise begründen müssen, warum sie Zugang zu einem Mobiltelefon haben wollen.

Es gibt also mehr Situationen, in denen ein Mobiltelefon in falsche Hände geraten kann, als man vielleicht zunächst denkt. Wenn Ihr Handy bisher noch nicht passwortgeschützt ist, nehmen Sie sich doch einfach jetzt einen Moment Zeit und kümmern Sie sich darum.

Üblicherweise lässt sich ein Smartphone auf drei verschiedene Arten sperren, egal, ob man Android, iOS oder ein anderes Betriebssystem nutzt. Am bekanntesten ist die PIN, ein Code aus Ziffern, die in der richtigen Reihenfolge eingegeben werden müssen, um das Gerät zu entsperren. Sie müssen sich dabei nicht auf die Anzahl an Stellen beschränken, die Ihr Telefon vorschlägt, sondern können in den Einstellungen manuell einen sichereren Code festlegen, beispielsweise einen siebenstelligen (so lang waren auch die Telefonnummern, die Sie sich in Ihrer Kindheit noch selbst merken mussten). Auf jeden Fall sollten es mehr als vier Stellen sein.

Bei einigen Mobilgeräten ist es auch möglich, einen textbasierten Code einzustellen, der wie das auf Seite 21 beschriebene Beispiel aussieht. Auch hier gilt wieder, dass Sie mindestens sieben Zeichen verwenden sollten. Moderne Geräte zeigen auf der Bildschirmtastatur sowohl Ziffern- als auch Buchstaben gleichzeitig an, was es leichter macht, zwischen diesen Zeichengruppen zu wechseln.

Eine andere Sperrmethode arbeitet visuell: Seit 2008 sind Android-Handys mit einer sogenannten Mustersperre ausgestattet. Dabei erscheinen neun Punkte auf dem Bildschirm, die man in beliebiger Reihenfolge miteinander verbinden kann. Diese Reihenfolge bildet dann den Code zum Entsperren des Geräts. Eine geniale Methode, könnte man meinen, schließlich ist die Sequenz aufgrund der schieren Menge an möglichen Kombinationen nahezu nicht zu knacken. Doch Menschen sind nun einmal bis zu einem gewissen Grad berechenbar: Auf der PasswordsCon 2015 berichteten Forscher, dass die Teilnehmer einer Studie nur von wenigen der 140.704 Möglichkeiten, die Punkte zu verbinden, tatsächlich Gebrauch machten.[12] Um welche Muster es sich dabei handelte? Oft war es einfach der erste Buchstabe des Namens der Person. Außerdem fand man heraus, dass Menschen ten-

denziell öfter die Punkte in der Mitte und weniger die in den vier Ecken nutzen. Diese Erkenntnisse sollten Sie im Hinterkopf behalten, wenn Sie das nächste Mal ein solches Muster einstellen.

Schließlich gibt es noch eine dritte Methode: die biometrische Erkennung. Apple, Samsung und die anderen bekannten Hersteller bieten den Nutzern derzeit die Option an, zum Entsperren des Smartphones ihren Fingerabdruck scannen zu lassen. Man sollte sich jedoch darüber im Klaren sein, dass selbst diese Methode nicht völlig sicher ist. Nach der Veröffentlichung von Touch ID waren Experten überrascht. Vielleicht hatten sie erwartet, dass Apple seine Geräte angesichts der neuen Fingerabdruckscanner, die aktuell auf dem Markt sind, entsprechend aufrüstet. Sie stellen jedoch fest, dass viele der alten Methoden, mit denen sich die Scanner austricksen lassen, noch immer beim iPhone funktionierten. So kann man beispielsweise mit Babypuder und transparentem Klebeband den Fingerabdruck von einer glatten Oberfläche abnehmen und damit das Gerät entsperren.

Andere Telefone nutzen die eingebaute Kamera, um das Gesicht des Besitzers zu identifizieren, aber auch die Gesichtserkennung lässt sich austricksen, indem man ein hochauflösendes Foto der Person vor die Kamera hält.

Für sich genommen sind biometrische Methoden also keineswegs sicher. Im Idealfall stellen sie daher nur eine von mehreren Maßnahmen zur Authentifizierung dar. Scannen Sie also Ihre Fingerkuppe oder schauen Sie in die Kamera und geben Sie anschließend Ihre PIN oder Ihren Sperrcode ein. Auf diese Weise ist Ihr Mobilgerät wirklich gut geschützt.

Was passiert nun, wenn Sie sich ein sicheres Passwort ausgedacht, es aber nicht aufgeschrieben haben? Gerade wenn Sie einen Account nur selten nutzen, ist das Passwort schnell vergessen. Kein Wunder also, dass uns die Möglichkeit, ein Passwort zurücksetzen zu lassen, oft wie ein Geschenk des Himmels erscheint. Allerdings haben auch Möchtegern-Hacker durch die Reset-Funktion ein leichtes Spiel. Denn mithilfe der Hinweise, die wir in den sozialen Medien preisgeben, können sie sich Zugang zu unseren E-Mails und anderen Diensten verschaffen, indem sie einfach das Passwort zurücksetzen.

In der Presse wurde beispielsweise über einen Fall berichtet, in dem Betrüger herausfanden, wie die letzten vier Stellen der Kreditkartennummer ihres Opfers lauteten. Diese nutzten sie dann bei einem Anruf beim Provider des Opfers als Identitätsnachweis, um die autorisierte E-Mail-

Adresse ändern zu lassen. Dadurch konnten sie das Passwort zurücksetzen, ohne dass der rechtmäßige Besitzer des Accounts davon wusste.

Im Jahr 2008 wiederum wollte ein Student der University of Tennessee namens David Kernell ausprobieren, ob er es schaffen würde, sich Zugang zum persönlichen Yahoo-E-Mail-Konto der damaligen Vizepräsidentschaftskandidatin Sarah Palin zu verschaffen.[13] Er hätte versuchen können, das Passwort zu erraten, aber wahrscheinlich wäre der Account nach drei Fehlversuchen gesperrt worden. Daher nutzte er stattdessen die Passwort-Reset-Funktion, ein Vorgehen, das er später als »einfach« beschreiben sollte.[14]

Sicher haben Sie auch schon mal sonderbare E-Mails von Freunden oder Kollegen bekommen, in denen dann Links zu Pornoseiten im Ausland waren, und später erfahren, dass das E-Mail-Konto dieser Person gehackt wurde. Zu solchen feindlichen Übernahmen von E-Mail-Konten kommt es oft, weil deren Passwortschutz zu schwach ist. Entweder jemand kam durch ein Datenleck an das Passwort oder der Eindringling nutzte die Passwort-Reset-Funktion.

Beim Anlegen eines E-Mail- oder sogar Onlinebanking-Accounts werden Ihnen häufig sogenannte Sicherheitsfragen gestellt, in der Regel sind es drei. Oft gibt es auch ein Drop-down-Menü, sodass man aus verschiedenen Fragen die auswählen kann, die man beantworten möchte. Die meisten dieser Fragen sind naheliegend.

Wo wurden Sie geboren? Wo gingen Sie zur Schule? Wo haben Sie studiert? Ein Klassiker ist auch die Frage nach dem Mädchennamen der Mutter – offenbar wird dieser schon mindestens seit 1882 als Sicherheitsfrage genutzt.[15] Weiter unten werde ich ausführlicher darauf eingehen, dass Unternehmen das Internet nach persönlichen Informationen durchsuchen und diese sammeln. Die Antworten auf die üblichen Sicherheitsfragen zu finden, ist daher kinderleicht. Schon nach ein paar Minuten Internetrecherche zu einer bestimmten Person ist man wahrscheinlich in der Lage, deren Sicherheitsfragen zu beantworten.

Erst in der letzten Zeit wurden die Sicherheitsfragen ein wenig verbessert. In den USA könnte eine Frage dann zum Beispiel lauten: »In welchem Bundesstaat wurde Ihr Schwager geboren?« Das ist schon ziemlich speziell, wobei man bedenken sollte, dass das korrekte Beantworten solcher »guten« Fragen wiederum eigene Risiken birgt, auf die ich gleich noch eingehen werde. Aber viele der vermeintlichen Sicherheitsfragen sind nach wie vor zu einfach, etwa: »Was ist der Heimatort Ihres Vaters?«