Avira Passwort-Sicherheitsreport

Räumen Sie Ihr digitales Leben auf

avira.com

Mai 2019

Einleitung

Technologie ist zum Hauptthema des 21. Jahrhunderts geworden: Sie ist eng mit der Wirtschaft, Politik und Wissenschaft verknüpft – und einfach überall in unserem Leben. Wenn eine neue Technologie erscheint, ist es normal, dass immer mehr Menschen davon angezogen werden und daher mittlerweile einen Großteil ihrer Zeit digital vernetzt sind. Doch mit jeder Minute, die sie im Cyberspace verbringen, werden riesige **Datenmengen** generiert.

Einfach gar keine digitalen Spuren zu hinterlassen, ist nicht möglich. „Allein im Jahr 2019 zu leben reicht schon aus, um Daten zu generieren – ob absichtlich oder ungewollt. Diese Daten werden durch Data-Mining, Raffination und Produktisierung monetarisiert", erklärt das Future Today Institute.

„*Obwohl die Anzahl an Daten-Leaks in den letzten Monaten wesentlich gestiegen ist, neigen die Menschen dazu, erst Sicherheitsmaßnahmen zu ergreifen, wenn ihre privaten Daten massiv gefährdet sind*", sagt **Matthias Ollig, CTO bei Avira**. „*Wir wissen, dass die Hauptursache dafür Bequemlichkeit ist – daher glauben wir fest daran, dass gut funktionierende und einfach zu nutzende Lösungen, die das digitale Erlebnis erheblich verbessern und Spaß machen, die Menschen in der vernetzten Welt schützen können.*"

Einem Bericht zufolge sind von den **7,7 Milliarden** Menschen auf der Welt schätzungsweise **4,4 Milliarden aktive Internet-Nutzer** und **3,5 Milliarden** in irgendeiner Form Nutzer von **sozialen Medien**. Das ist nicht nur eine große Zahl vernetzter Menschen – die Anzahl vernetzter Konten und privater Daten, die über diese Personen gesammelt werden, ist noch größer.

Was hält private Informationen davon ab, unkontrolliert im Cyberspace umherzuschwirren? Sehr, sehr wenig. Eine wachsende Anzahl an Rechtsvorschriften wie die DSGVO und HIPPA regeln, wie Unternehmen mit persönlichen Daten umgehen und diese schützen sollen. Doch ein Blick auf die größten Leaks der Jahre 2018 und 2019 zeigt, dass Cyber-Kriminelle einfach Daten aus anderen legalen und illegalen Quellen sammeln und zusammenführen. Und davon gibt es viele.

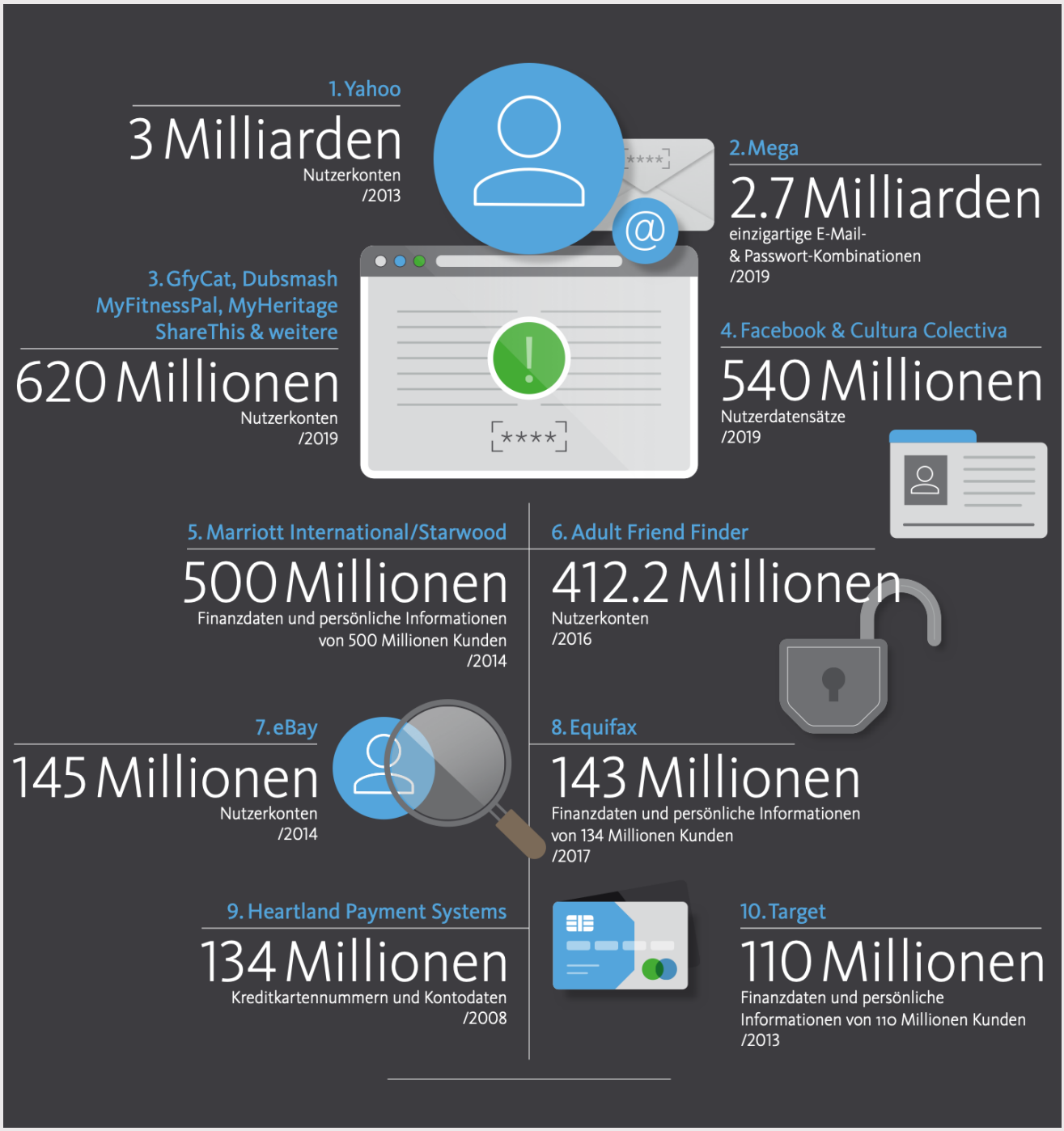
Auf persönlicher Ebene kann viel getan werden, um Nutzerkonten sicherer zu machen. Auf technischer Ebene bedeutet dies, Zwei-Faktor-Authentifizierungen und Passwort-Manager zu nutzen und nicht dieselben Passwörter und Nutzernamen für mehrere Konten zu verwenden. Das Problem besteht darin, dass diese Möglichkeiten bekannt sind, jedoch ignoriert werden.

Aufräumen macht Spaß

Um Passwort- und Kontosicherheit stärker ins Bewusstsein der Nutzer zu rücken, ist Angstmacherei keine Lösung. Obwohl Forschungsergebnisse immer wieder zeigen, dass die Verbraucher oft miserable Sicherheitsgewohnheiten haben (wiederverwendete, kurze Passwörter) und das Interesse an Passwort-Managern nach einem großen Datendiebstahl steigt, ist der Effekt nur von kurzer Dauer.

Spaß scheint ein größerer Motivator zu sein als Angst. „*Unsere Forschungsergebnisse zeigen, dass von den vier Hauptgründen für die Nutzung eines Passwort-Managers drei mit Bequemlichkeit und Zeitersparnis zu tun haben, nicht mit Sicherheit. Es ist paradox: Einen Passwort-Manager zu nutzen, bedeutet in erster Linie mehr Spaß zu haben und nur ganz nebenbei das Online-Leben viel, viel sicherer zu machen*“, sagt **Tim Gaiser, Leiter der Identity Protection Unit.**

Hall of Fame:
Die größten Daten-Leaks (1)



Hall of Fame:
Die größten Daten-Leaks (2)

Datenschutzverletzungen werden immer umfangreicher und geschehen immer häufiger. Bisher gab es **2019** schon mindestens vier große Daten-Leaks, bei denen jeweils mehr als **200 Millionen Datensätze kompromittiert** wurden. Das Schlimmste daran ist, dass es sich dabei um Ansammlungen von Daten handelt, die aus unterschiedlichen Quellen stammen – quasi eine Art digitales Potpourri. Die Daten wurden also bereits gestohlen – und erst im Nachhinein veröffentlicht. Es ist nicht einmal klar, woher diese privaten Daten eigentlich stammen.

Aus einer nicht-technischen Perspektive betrachtet gibt es drei Hauptformen von Daten-Leaks: Hacking, Scraping und Dropping.

Hacking – In diesem Fall entstehen die Listen dadurch, dass Kriminelle die Datenbanken von Unternehmen hacken und exfiltrieren – aus unterschiedlichen Gründen und mit unterschiedlichen Zielen. Wenn Nationalstaaten die Akteure sind, geht es meist um Informationen; wenn kriminelle Hacker am Werk sind, haben Sie es auf das Geld abgesehen, das sie durch den Verkauf der Listen erhalten.

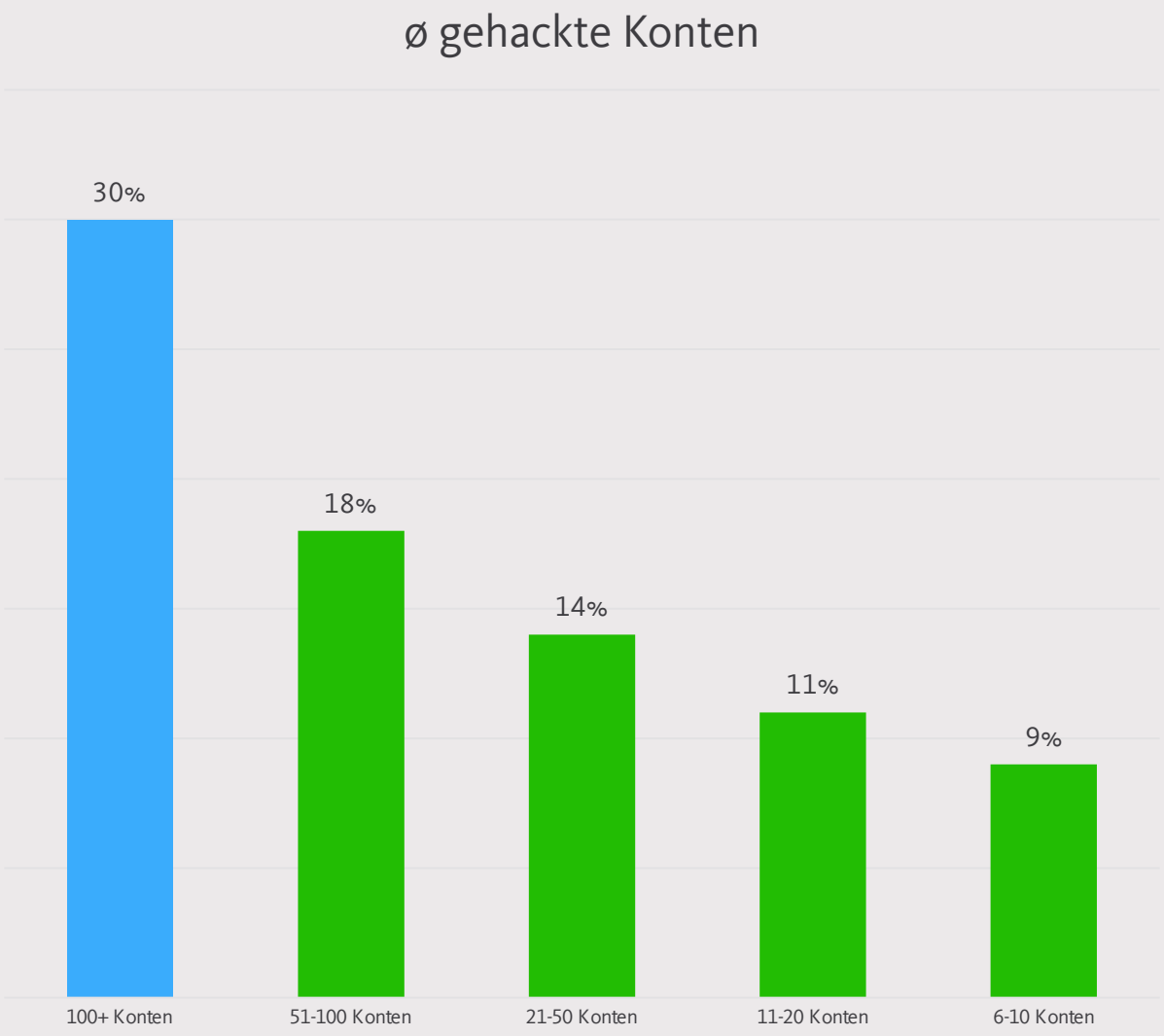
Scraping – Mithilfe einer Vielzahl von Tools werden die Daten von verschiedenen Webseiten extrahiert und zusammentragen. Meist ist nicht klar, woher die Daten stammen und ob sie der Datenschutzgrundverordnung unterliegen. Trotz dieser Ungewissheit können sich auf den Listen viele persönliche Daten befinden.

Dropping – Hierbei geht es um ungeschützte Datenbanken, die einfach über das Internet zugänglich sind. Da Unternehmen, soziale Netzwerke und Daten-Broker immer mehr Informationen über Online-Aktivitäten sammeln und diese in Cloud-Speichern ablegen, wird diese Art von Daten-Leaks immer häufiger.

Meist treten diese drei Formen nicht unabhängig voneinander auf. Wenn ein krimineller Hacker die Daten eines Unternehmens stiehlt, sie mit den Informationen eines Daten-Scrapers kombiniert und sie dann ungesichert auf einem Online-Server speichert, wo andere unautorisierte Hacker sie sehen können, dann haben wir einen Fall wie den der riesigen Collection #1. Man nimmt an, dass es sich dabei um ein Konglomerat aus verschiedenen gestohlenen Datenbanken handelt, das verkauft und von einem Hacker-Forum für diverse kriminelle Zwecke genutzt wurde. Collection #1 wurde nur entdeckt, weil die Hacker ihre Listen ungesichert auf einem Cloud-Server gespeichert hatten.

Mehr Konten – mehr Leaks (1)

Je mehr Nutzerkonten eine Person besitzt, desto größer ist die Wahrscheinlichkeit, dass diese gehackt werden. Studien haben gezeigt, dass die Wahrscheinlichkeit eines Datendiebstahls für Personen mit 6 bis 10 Konten bei 9 % liegt – und dass diese auf bis zu 30 % steigt, wenn jemand über 100 Konten besitzt. Der Hauptgrund für diesen Anstieg liegt in der Wiederverwendung von Nutzernamen und Passwörtern für mehrere Konten. Hacker haben leichtes Spiel, wenn der Nutzername von John Doe „JnDough“ lautet – ob nun für sein E-Mail- oder Bankkonto – und das Passwort „JnB2Gud“ ist.



Die Daten wurden von Avira zwischen dem 1. Januar und 25. März 2019 erhoben.

Mehr Konten – mehr Leaks (2)

Wir beobachten zwei bedenkliche Trends: Zum einen gibt es viele wertvolle Daten, die über Sie erhoben und gesammelt werden. Jedes Mal, wenn Sie online irgendetwas tun – ob Sie nun einfach surfen oder etwas in einem sozialen Netzwerk posten –, wird dies dem Datenberg hinzugefügt. Dabei geht es nicht nur darum, was Sie direkt tun, sondern auch darum, was die unzähligen Daten-Tracker und Webseiten über Sie aufzeichnen.

Zum anderen gibt es viele schlechte Angewohnheiten im Umgang mit privaten Daten – auf individueller wie auf organisatorischer Ebene. An oberster Stelle dieser Liste stehen schwache Passwörter, für mehrere Konten verwendete Passwörter, wiederverwendete Nutzernamen und nur dürftig gesicherte Datenbanken.

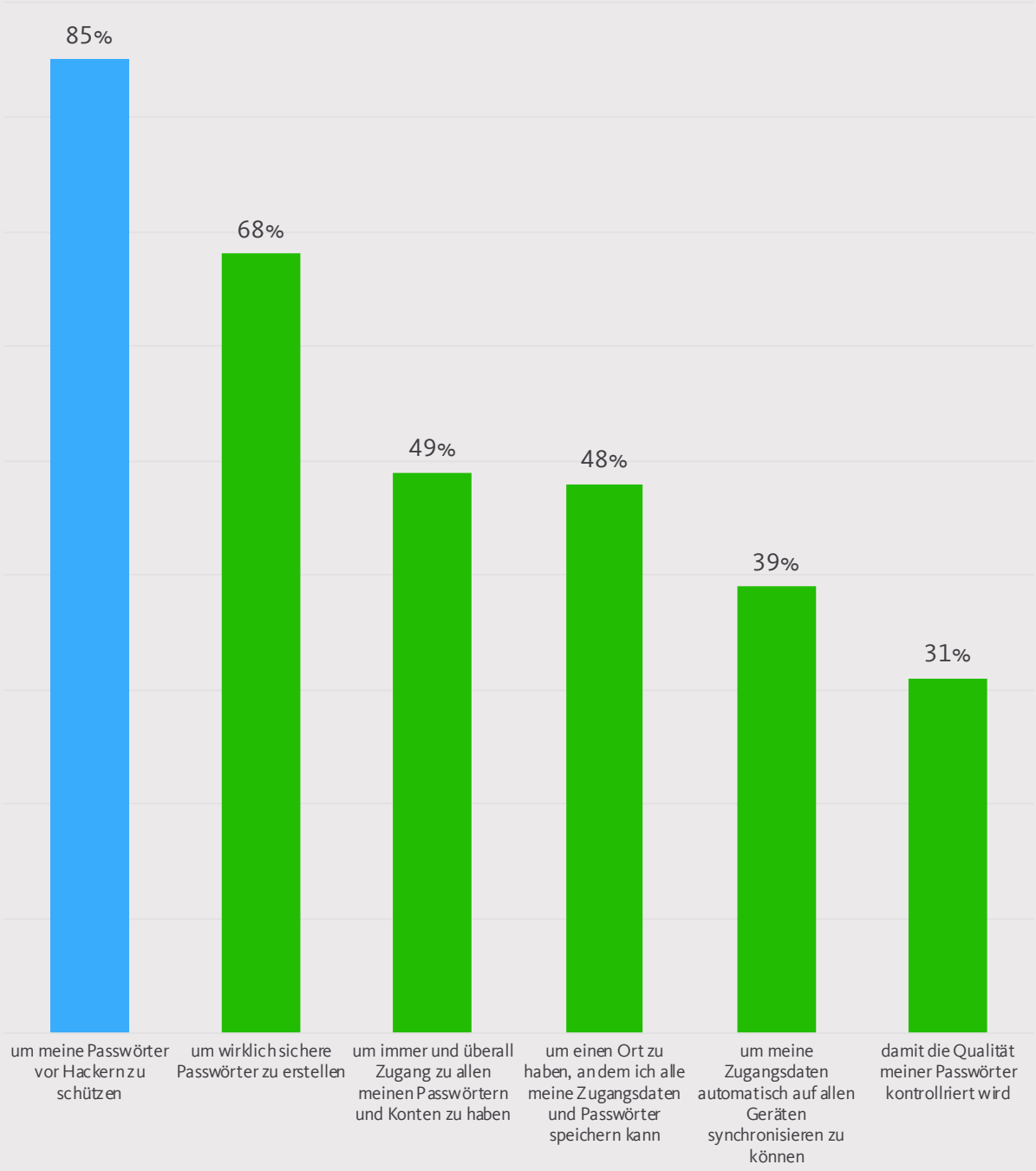
Zusammengenommen ergibt das eine Fülle an Informationen, die nur darauf wartet, abgeschöpft zu werden. Es ist, als ob Sie Ihre Brieftasche bei heruntergelassener Scheibe auf dem Vordersitz Ihres Autos liegenlassen. Angesichts dieser Beute in Reichweite bedienen sich ganze Hacker-Armeen – unabhängige und vom Staat unterstützte –, die sozusagen einfach nur durchs Fenster greifen müssen.

Wird über diese Datendiebstähle berichtet, steigt das Interesse an Passwort-Managern. Wie Google Trends zeigt, schnellen nach einer entsprechenden Berichterstattung die Suchanfragen für Passwort-Manager in die Höhe. Diese Nachrichten bewirken auch ein gesteigertes Interesse an unserer Lösung. „*Nachrichten über Leaks führen zu bis zu 60 % mehr Installationen und bis zu 20 % mehr Registrierungen im Vergleich zu einem normalen Tag*“, berichtet **Tim Gaiser, Leiter der Identity Protection Unit.**

„Passwort-Management funktioniert oft nach dem Schmerzvermeidungsprinzip: Die Leute wählen so kurze und einfache Passwörter wie möglich – und nutzen diese dann so oder in variierter Form für viele verschiedene Seiten. Diese Strategie reduziert allerdings auch den Aufwand für Hacker und fordert sie sozusagen heraus, schon bekannte Passwörter bei allen vorhandenen Konten eines anvisierten Nutzers auszuprobieren .“

Tim Gaiser, Leiter der Identity Protection Unit

Gründe für die Nutzung eines Passwort-Managers



Quelle: Avira Online-Befragung (Multiple-Choice-Fragen) mit 718 Teilnehmern im Alter von 20 – 65 Jahren (Deutschland, 2018)

Von Gleichgültigkeit zu Wertschätzung

Um zu erfahren, wie sich die Bewertung eines Passwort-Managers über einen Zeitraum von vier Wochen hinweg entwickelt, begleiteten wir Tim, einen **neuen Nutzer** des Avira Password Manager. Als waschechter 23-jähriger Millenial startete er mit viel digitalem Ballast – 30 verschiedenen Nutzerkonten mit drei Basis-Passwörtern, die er, wenn erforderlich, mit zusätzlichen Buchstaben oder Zahlen leicht abänderte.

Wie viele andere auch glaubte Tim, dass die Verwendung desselben oder eines ähnlichen Passworts für alle seine Online-Konten ausreicht, um seine Daten zu schützen. Tim nutzte drei ähnliche Passwörter für 30 Nutzerkonten und fügte nur eine Zahl oder einen Großbuchstaben hinzu, wenn es erforderlich war. Er dachte, dass seine Passwörter schwer zu hacken seien. „Ich bin mir ziemlich sicher, dass keiner meine Nutzerkonten hacken kann, da ich sie mit gesundem Menschenverstand erstelle."

Sein ursprüngliches Ziel war bescheiden: Zeit beim Einloggen zu sparen und sich das Leben durch weniger Passwort-Resets, die er bisher regelmäßig vornehmen musste, leichter zu machen.

Zu Beginn brauchte er eine Stunde, um seine Zugangsdaten für alle Konten einzugeben, da er einige Nutzernamen und die genauen Passwörter vergessen hatte. Als er dann alle seine Konten und Passwörter an einer Stelle zusammengefasst sah, war er geschockt und wunderte sich, dass er noch nicht gehackt worden war. „Es wäre so einfach für jemanden gewesen, alle meine Daten in die Finger zu bekommen", meint er.

Nach vier Wochen war er ein überzeugter Kunde, der den Password Manager auf allen seinen Geräten nutzte, vom Computer bis hin zum Smartphone.

„Ich hatte mein Aha-Erlebnis, als ich die Auto-Fill-Funktion der Browser-Erweiterung entdeckt habe... Alle Daten sind im Handumdrehen verfügbar – ich gehe auf eine Webseite, klicke auf das Login- bzw. Registrierungsfeld und der Password Manager speichert entweder meine Daten auf dem Dashboard oder meldet mich direkt auf der Seite an.
Ich kann Avira Password Manager definitiv jedem empfehlen, der seine Online-Konten besser schützen möchte. Ich hätte ihn viel früher nutzen sollen. Es war wirklich ein Schlag ins Gesicht, festzustellen, wie riskant meine bisherige Vorgehensweise war."

Quelle: Qualitative Langzeitstudie (ein Monat) von Avira

Räumen Sie jetzt auf!

Es wird Zeit, Passwort-Management als Vergnügen zu betrachten – nicht als Sicherheitsmaßnahme.

Hier sind **fünf Vorschläge**, wie Sie mit einem Passwort-Manager mehr Freude in Ihr Online-Leben bringen und es aufräumen können:

- **Schätzen Sie Ihre Passwörter** – Passwörter werden komplett unterschätzt, obwohl sie Ihnen starken Schutz bieten. Wir brauchen sie – und wir brauchen sichere. Ein Passwort-Manager hilft Ihnen dabei, starke Passwörter zu erstellen und macht Sie darauf aufmerksam, wenn Sie – möglicherweise unbeabsichtigt – dasselbe Passwort wiederholt verwenden.

- **Verwahren Sie Ihre Passwörter sicher** – Viele Leute bewahren Ihre Passwörter nicht sicher auf – auf dem Schreibtisch oder an der Pinnwand und über diverse Geräte hinweg verteilt. Oder sie versuchen, sich alle Passwörter zu merken. Mit einem Passwort-Manager können Sie Ihre Passwörter und Notizen fein säuberlich aufbewahren und verwalten.

- **Haben Sie stets alles in Reichweite** – Ein guter Passwort-Manager ist immer an Ihrer Seite – und synchronisiert die Passwörter auf allen Ihren Geräten. So müssen Sie sie nicht überall erneut eingeben.

- **Räumen Sie anderen (schnell) hinterher** – Falls jemand anderes Ihre Daten durch einen Leak oder Hackerangriff verliert, warnt Avira Password Manager Pro Sie per EMail. Er hilft Ihnen sogar dabei, die betroffenen Passwörter schnell zu ändern und so das Risiko einer Veröffentlichung Ihrer Daten zu reduzieren.

- **Bleiben Sie sicher** – Natürlich sollte ein Passwort-Manager die Passwörter auf Ihren Geräten und in der Cloud mit einer Verschlüsselung auf militärischem Niveau schützen. Und nur Sie sollten Ihr Master-Passwort kennen. Wahre Passwortsicherheit sollte bei Ihnen anfangen und aufhören.

Über Avira

Avira schützt Menschen in der vernetzten Welt – und gibt allen die Möglichkeit, ihr digitales Leben zu verwalten, zu schützen und zu optimieren.

Aviras Angebot erstreckt sich auf ein Portfolio aus Sicherheits- und Leistungsanwendungen für Windows, Android, Mac und iOS. Unsere Schutztechnologien ergänzen wir außerdem durch OEM-Partnerschaften. Immer wieder stehen unsere Sicherheitslösungen an der Spitze von unabhängigen Tests zur Erkennung, Leistung und Benutzerfreundlichkeit.

Avira ist ein Unternehmen in Familienbesitz mit 500 Mitarbeitern. Hauptsitz ist Tettnang am Bodensee mit weiteren Niederlassungen in Rumänien, Indien, Singapur, China, Japan und den USA. Ein Teil der Einnahmen von Avira kommt der Auerbach Stiftung zugute, die Bildungsinitiativen sowie Kinder und Familien in Not unterstützt.

Weitere Informationen zu Avira finden Sie unter www.avira.com.

avira.com