Tod dem Passwort – Es lebe das Passwort

Adrian Bachmann

Das Passwort lebt immer noch

Schon bereits vor einigen Jahren kündigten die Medien (siehe z.B. [1]) aber auch Fachkreise den Tod von Passwörtern an. Biometrie in allen Facetten (z.B. Fingerabdruck, Iris, Handvenen, Herzrate, Stimme) ist nur ein Beispiel, welches den nahen Tod herbeiführen sollte. Jahre später hantieren wir auch in Zeiten von Blockchain und Kryptowährungen nach wie vor täglich mit Passwörtern. An der Situation hat sich dabei wenig geändert: Jeder Nutzer verfügt über unzählige Accounts und es werden immer mehr. Ein jeder dieser Accounts möchte dabei mit einem Passwort abgesichert werden. Mal mindestens 8 Zeichen, mal maximal 8, mal mindestens mit einer Ziffer und einem Sonderzeichen, mal garantiert ohne Sonderzeichen und manchmal auch ohne jegliche Vorgaben. Dabei den Überblick nicht zu verlieren, ist nahezu unmöglich. Und so kommt es wie es kommen muss: Nutzer verwenden wo immer möglich das gleiche Passwort oder variieren dieses nur geringfügig. Für böse Buben ein gefundenes Fressen. Da hilft es auch wenig, dass Umfragen zufolge 98% der Hacker keine Skimaske vor dem Computer tragen [2]. Nur was kann der einzelne Nutzer tun, wenn die gefühlten 200 benutzen Accounts nach wie vor nach einem Passwort lechzen? Um es vorweg zu nehmen: Lösungen zur Entmachtung des Passworts sind in Sicht, dürften aber noch etwas Zeit beanspruchen. Es gilt daher praktikable Lösungen für das momentane Passwortchaos zu finden.

Das Account 1x1 für Nutzer

Mit den nachfolgenden zwei Grundregeln lässt sich das Risiko eines Account-Missbrauchs massgeblich senken und den Komfort für den Nutzer sogar erhöhen.

1. Nutze pro Dienst ein eigenes, sicheres Passwort. Kein Passwort Recycling! Nein, wirklich nicht! Die Nutzung eines sicheren Passwortsafes (z.B. Keepass [3] oder lastpass [4]) ist hierfür ab einer bestimmten Anzahl Accounts zwingend empfohlen. So dürfte es auch kein Problem sein, jeweils automatisch generierte, starke Passwörter zu verwenden, da man sich diese aller Voraussicht nach nicht mehr merken kann und jeweils aus dem Safe holen muss. Eine Mehrfachverwendung des gleichen Passworts, vielfach in Kombination mit der eigenen E-Mail-Adresse als Benutzername, eröffnet Kriminellen Tür und Tor, um nach einem erfolgreichen Angriff auf einen Dienst weitere Dienste eines Nutzers zu missbrauchen. Im 2017 wurden über 90'000 Accounts und deren Passwörter von Schweizer Internetdiensten entwendet [5, 6]. Ob Du selber davon betroffen bist, kann über eine Online-Abfrage bei der Melde- und Analysestelle des Bundes (MELANI) festgestellt werden [7]. Ohne Passwort Recycling kann man solchen Account-Diebstählen deutlich entspannter entgegenblicken, da dann nur der jeweilig spezifische Account betroffen ist, nicht noch mutmasslich viele weitere persönliche Accounts plötzlich auch gefährdet sind und sich somit ein abenderfüllendes Passwortwechseln aufdrängt.
2. Nutze wo immer möglich eine starke bzw. 2-Faktor Authentisierung (z.B. SMS/mTAN, OTP-App, FIDO-Device wie YubiKey) zur weiteren Absicherung Deines Accounts. Damit lässt sich der Schutz massgeblich erhöhen. Trotz Absicherung mit einem weiteren Faktor wäre es aber ein Irrtum anzunehmen, dass Regel Nr. 1 damit seine Bedeutung verliert.

Immer öfter bieten Internetdienste inzwischen auch die Nutzung eines vertrauenswürdigen und sicheren Identity Providers (IdP) wie Google, Microsoft oder Facebook anstelle eines lokalen Accounts an. Dies ist eine komfortable Möglichkeit, die Anzahl Accounts zu reduzieren, wobei der verwendete IdP-Account dabei zwingend über eine starke Authentisierung abgesichert sein sollte. Es ist damit zu rechnen, dass die Bedeutung von Identity Provider künftig stark zunehmen wird, was auch aktuelle, nationale Initiativen im Umfeld von eID, SwissID, SwissPass, etc. zeigen.

Dr. Adrian Bachmann studierte Wirtschaftsinformatik an der Universität Zürich und verfasste dort auch seine Dissertation zum Thema Datenqualität im Software Engineering Prozess. Nach einigen Jahren im IT Projekt- und Risikomanagement bei einer grösseren Schweizer Bank berät er seit 2011 seine Kunden in Themen der Informationssicherheit und leitet entsprechende Projekte.

Kontaktadresse:
Dr. Adrian Bachmann
Partner, IT Security Consultant
TEMET AG
Basteiplatz 5
CH-8001 Zürich
Tel: +41 79 464 01 46
E-Mail: adrian.bachmann@temet.ch
http://www.temet.ch

Passwort ja – aber sicher!

Offensichtlich werden wir noch einige Zeit mit Passwörtern umgehen müssen. Dabei stellen nebst recycelten insbesondere schwache Passwörter ein grosses Sicherheitsproblem dar. Betrachten wir die 20 am häufigsten verwendeten Passwörter in der Schweiz, so ergibt sich eine Liste des Schreckens (Stand 02.03.2018) [8]:

1. 123456
2. 123456789
3. 12345678
4. 1234
5. 12345
6. 111111
7. 1234567
8. hallo
9. abc123
10. password
11. qwertz
12. passwort
13. 1234567890
14. 666666
15. soleil
16. sommer
17. 123123
18. daniel
19. blabla
20. andrea

Darüber hinaus sind in der Schweiz offenbar besonders Jahrgänge und Postleitzahlen in Passwörtern beliebt. Insbesondere die Zahlen 12, 01, 11, 14, 13, 10, 99, 77, 69 und 22 scheinen es den Schweizer Nutzern angetan zu haben.

Sichere Passwörter sollten nicht nur mindestens 8 Zeichen, sondern auch eine gewisse Komplexität aufweisen. Wörter, Namen oder Tastaturmuster sind dabei möglichst zu vermeiden. Mit der Nutzung eines Passwortsafes lassen sich für jeden genutzten Dienst rasch und unkompliziert sichere Passwörter erzeugen, verwalten und bei Bedarf abrufen inkl. automatischem Abfüllen in die Login-Maske der Internetdienste. Es besteht also keine Notwendigkeit, sich unzählige, aus einem Buchstaben-, Zahlen-, und Sonderzeichensalat zusammengesetzte, sicherere Passwörter merken zu müssen.

Der Mensch als Schwachstelle

Es ist offenkundig, dass nicht (nur) Passwörter ein Problem darstellen, sondern vor allem die Komponente Mensch. Unser Umgang mit Passwörtern stellt Sicherheitsspezialisten seit Jahren vor Herausforderungen und motiviert dazu, alternative Verfahren und Lösungen zu suchen. Das regelmässige Ändern oder Minimalvorgaben bezüglich Komplexität sind nur zwei Beispiele, die dazu führen sollen, dass Passwörter (vermeidlich) sicherer werden sollen. In der Praxis zeigt sich dafür, dass z.B. Post-it Zettelchen dem Nutzer als Gedankenstütze dienen und somit solche Passwort-Regeln das Risiko eines erfolgreichen Account-Missbrauchs gar noch erhöhen.

Lasst Euch von diesem Artikel inspirieren und ändert Euer Passwort-Verhalten noch heute. Die Einrichtung eines Passwortsafes dauert nur wenige Minuten, erspart das unzählige Anklicken von «Passwort vergessen»-Links und dient der massgeblichen Verbesserung der Account-Sicherheit.

Tot dem universal, überall verwendeten, schwachen Passwort – es lebe das sichere, spezifische Passwort und dieses wo immer möglich in Kombination mit einer starken Authentisierung.

PS: Kurz vor dem GzD dieser readme Ausgabe wurde im c't 07/18 das Leitthema «Vergessen Sie Passwörter!» behandelt. Dabei werden weitere Punkte im sicheren Umgang mit Passwörtern diskutiert und unter anderem auch 15 Passwortmanager einem Test unterzogen. Lektüre uneingeschränkt empfohlen! [9]

Referenzen

[1] https://www.tagesanzeiger.ch/digital/internet/Tod-dem-Passwort-/story/26979882
[2] http://www.der-postillon.com/2012/01/umfrage-98-prozent-aller-hacker-tragen.html
[3] https://keepass.info
[4] http://www.lastpass.com
[5] https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/passwoerter-von-21000-e-mail-konten-im-umlauf.html
[6] https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/passwoerter-von-70000-e-mail-konten-im-umlauf.html
[7] https://www.checktool.ch
[8] http://www.swissleak.ch
[9] c't magazin für computer technik, Ausgabe 07/18 vom 17.03.2018, Heise Zeitschriften Verlag, https://goo.gl/rSS9Eg