GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Passwörter zu 773 Mio. E-Mail-Adressen im Internet – FAQ

Nachdem Anfang Januar der Hacker-Angriff auf Politiker und andere Prominente die Schlagzeilen bestimmt hat, berichten nun die Medien über eine riesige Passwort-Sammlung für ca. 773 Millionen Online-Konten, die im Netz verfügbar ist. Wir versuchen nachstehend, die wichtigsten mit diesem Datenleck verbundenen Fragen zu beantworten. Wir haben das als FAQ gestaltet, die bei Bedarf aktualisiert werden soll.

Was sind das für Daten zu den 773 Mio. E-Mail-Adressen?

Im Internet kursieren immer wieder Listen mit E-Mail-Adressen und Daten, die diesen zugeordnet werden. Diese Daten können Passwörter (oder etwas, das aussieht, als ob es Passwörter sein könnten) oder auch Telefonnummern, Kreditkarten-Daten oder vieles anderes sein. Die neue, sehr umfangreiche Liste scheint eine Zusammenfassung solcher kleineren Datensätze zu sein.

Die Qualität dieser Daten ist unklar. Es ist durchaus möglich, dass diese Daten sehr alt sind. Die GWDG hat in der Vergangenheit immer wieder kleinere Datensätze mit im Internet kursierenden Daten zu Konten, die zu Systemen der GWDG passten, erhalten. In solchen Fällen gab es meist die Hälfte der Konten schon gar nicht mehr. In Fällen, in denen Informationen zum Passwort vorlagen, hatten angesprochene Kontoinhaber fast immer mitgeteilt, dass sie ein solches Passwort für das GWDG-Konto nicht verwendet hätten. In einer einstelligen Zahl von Fällen war in den Datenlecks tatsächlich ein Passwort aufgetaucht, das (auch) für das GWDG-Konto verwendet wurde.

Sind auch Konten der GWDG, Max-Planck-Gesellschaft oder Universität Göttingen betroffen?

Definitiv ja. Stichproben haben das bestätigt.

Kann ich feststellen, ob ich selbst betroffen bin?

Ja, der australische Sicherheitsforscher Troy Hunt sammelt Informationen aus Datenlecks und stellt diese auf seiner Webseite „Have I Been Pwned" (https://haveibeenpwned.com) zur Verfügung. Dort kann in einem Webformular die eigene E-Mail-Adresse eingegeben werden, um die Sammlung zu durchsuchen. Die Webseite informiert dann, ob die E-Mail-Adresse gefunden wurde, und gibt zusätzlich Informationen, in welchen Datenquellen diese enthalten war.

Wenn ich betroffen bin, kann ich dann feststellen, welches Passwort von mir betroffen ist?

Nein (außer man verschafft sich Zugang zu den Rohdaten des Datenlecks). „Have I Been Pwned" liefert nicht zurück, welche Passwörter (oder sonstigen Informationen) zu welchem Konto in den Listen auftauchen. Das ist auch gut so, denn sonst könnte dieser Dienst böswillig missbraucht werden.

Ist es sicher, in „Have I Been Pwned" nach meiner E-Mail-Adresse zu suchen?

Ihre E-Mail-Adresse auf einer unbekannten Webseite anzugeben, kann prinzipiell Risiken beinhalten. Vielleicht wird die Adresse dort gespeichert und in der Folge an Spam-Versender verkauft, die Sie später mit unerwünschten E-Mails überhäufen.

Troy Hunt ist allerdings ein Sicherheitsforscher mit einer guten Reputation, sodass hier nicht angenommen werden muss, dass „Have I Been Pwned" missbräuchlich genutzt wird.

Ob man den Dienst nutzen will, mag dann auch noch davon abhängen, ob man seine E-Mail-Adresse eher als eine weitverbreitete oder als eine geheime Information betrachtet.

Meine E-Mail-Adresse taucht in der Datensammlung auf. Was mache ich nun?

Das lässt sich leider nicht einfach beantworten, weil eben unklar ist, welche Informationen in der Datensammlung zu ihrer E-Mail-Adresse stehen. Sicher ist nur, dass die E-Mail-Adresse in der Liste auftaucht. Alles andere kann falsch, harmlos, veraltet oder leider auch sensibel sein.

Wir versuchen, mit den nächsten Fragen und Antworten ein paar Hilfestellungen zu geben.

Wie gefährdet bin ich, wenn eine meiner E-Mail-Adressen in der Datensammlung gefunden wird?

Das lässt sich leider nicht einfach beantworten, da ein Treffer auf die Anfrage nach der E-Mail-Adresse zunächst nur sagt, dass die E-Mail-Adresse in der Datensammlung auftaucht.

In der weiteren Erläuterung steht dann noch, in welchen Quellen die E-Mail-Adresse auftaucht. Die Erläuterungen zu den Quellen am Ende der Antwort können hilfreich für die Einschätzung sein. Bei einigen der Quellen waren gar keine Passwort-Informationen enthalten, sondern z. B. nur Namen, Telefonnummern und Anschriften. Auch solche Informationen können sensibel sein (vielleicht sind es aber auch nur Informationen, die sowieso öffentlich sind).

Zu anderen Quellen wird angegeben, dass in den Datensätzen Passwörter enthalten wären. Da aber nicht klar ist, welche Passwörter das jeweils sind, kann nicht festgestellt werden, ob das Passwort, das im Datenleck auftaucht, überhaupt ein wirklich irgendwann verwendetes Passwort ist oder ob das Passwort vielleicht vor Jahren ersetzt wurde.

Welches Konto ist gefährdet, wenn eine meiner E-Mail-Adressen in der Datensammlung auftaucht?

Wenn eine Ihrer E-Mail-Adressen in der Datensammlung auftaucht und in der Erläuterung steht, das in dem Datenleck auch Passwörter enthalten waren, dann muss das Passwort nicht zu dem Konto gehören, dass mit der E-Mail-Adresse direkt verbunden ist (z. B. zu ihrem GWDG-Konto).

Häufig werden bei irgendwelchen Dienstleistern im Internet lokale Konten angelegt, bei denen E-Mail-Adressen des Kunden als Kontoname verwendet werden. Die meisten Internet-Nutzer dürften mehrere solche Konten haben. Es könnte also sein, dass die Information über Sie nicht aus einem Datenleck des E-Mail-Providers stammt, sondern von einem Dienstleister, bei dem Sie ihre E-Mail-Adresse als Kontoname „wiederverwenden". Wenn Sie sich dann an die Sicherheitsempfehlung gehalten haben, für jeden Dienst ein anderes Passwort zu verwenden, wäre nur dieser eine Dienst betroffen und nicht Ihr E-Mail-Konto.

Vielleicht ist also nur ein Konto betroffen, das Sie bei irgendeinem Dienst bekommen, der völlig belanglos ist. Etwas, was man letztlich ignorieren kann.

Kann ich den Status meiner Passwörter prüfen?

Im Prinzip ja. „Have I Been Pwned" bietet auch die Möglichkeit an, nach einem beliebigen Passwort in der Datensammlung zu suchen. Man bekommt dann als Antwort, ob dieses Passwort irgendwo in der Datensammlung auftaucht. Das muss nicht heißen, dass es in Verbindung mit der eigenen E-Mail-Adresse auftaucht. Auch hier gilt wieder: Nur wenn etwas gar nicht gefunden wird, kann man beruhigt sein. Wenn das Passwort gefunden wird, könnte es auch zu einer ganz anderen E-Mail-Adresse in der Datenbank enthalten sein. Bei einem guten Passwort wäre das aber unwahrscheinlich. Man sollte daher davon ausgehen, dass man dann betroffen ist (zum weiteren Vorgehen s. u.)

Ist es nicht riskant, auf einer fremden Webseite wie „Have I Been Pwned" ein Geheimnis wie ein Passwort einzugehen?

Ja. Eigentlich gilt die Sicherheitsempfehlung: Geben Sie Ihr Passwort nie auf einer fremden Webseite ein (oder auf fremden Rechnern oder in anderen unsicheren Situationen).

Anderseits ist Troy Hunt – wie schon gesagt – ein bekannter Sicherheitsforscher mit einer guten Reputation. Hier sind Risiken und Nutzen abzuwägen: Dieser Seite trauen oder im Unklaren bleiben?

Bei der Entscheidung über die Nutzung von „Have I Been Pwned" kann man die Möglichkeit der Nutzung von Alternativen (s. u.) und die Sensibilität des zu prüfenden Passworts berücksichtigen. Alternativen zu nutzen, wäre vorzuziehen.

Eine Möglichkeit zur Risikoreduktion wäre noch, die Abfrage nach E-Mail-Adresse und Passwort nicht unmittelbar hintereinander und nicht vom selben Gerät abzuschicken. Das erschwert zumindest die Zuordnung des eingegebenen Passworts zur E-Mail-Adresse.

Kann man sein Passwort prüfen lassen, ohne es auf der Webseite „Have I Been Pwned" einzugeben?

Ja, für technik-affine gibt es eine Alternative. Troy Hunt bietet einen Zugriff über eine API (Applicaton Programing Interface) an. Man kann die API nutzen, um nach einem Passwort zu suchen, ohne das Passwort selbst zu übermitteln. Dazu muss man den SHA-1-Hash des Passworts berechnen, die ersten fünf (von 40) Zeichen des Hashes über die API eingeben. Als Antwort erhält man alle Hashes, die mit den fünf Zeichen beginnen und kann in diesen dann lokal suchen, ob der vollständige Hash (oder genauer die Zeichen 6-40 des Hashes) in der Antwortliste auftaucht.

Ein Beispiel, wie man das nutzen kann, steht weiter unten (gegen Ende der FAQ).

Man hat auf dem Weg also das Passwort selbst keiner externen Stelle mitgeteilt, sondern nur einen Hash und von dem auch nur ein Achtel. Die Restrisiken, die mit dem Vorgehen verbunden sind, scheinen vertretbar.

Die GWDG bereitet z. Z. einen Dienst vor, der die Funktionalität von „Have I Been Pwned" mittels einer Kopie des Datenbestands der Password-Hashes anbietet. Wir informieren Sie, sobald dieser bereitsteht. Für GWDG-Nutzer würde damit der Vorbehalt bzgl. der Eingabe von Passwörtern auf fremden Webseiten entfallen. Der Dienst kann dann für alle GWDG-Nutzer empfohlen werden.

Was sollte ich tun, wenn ich betroffen bin?

Wenn Anfragen nach der E-Mail-Adresse und nach einem zugehörigen Passwort einen Treffer ergeben haben, sollte man das betreffende Passwort sofort ändern.

Sie sollten auch überlegen, welche Konsequenzen der Vorfall gehabt haben könnte. Auch wenn die Antworten von „Have I Been Pwned" noch nicht definitiv aussagen, dass die Kombination E-Mail-Adresse/Passwort zusammen in einem Datenleck aufgetaucht ist, muss angenommen werden, dass dies der Fall ist und ein Angreifer Zugriff auf alle Daten gehabt haben könnte, die über diese Kombination gesichert waren.

Bei Beurteilung der Konsequenzen muss berücksichtigt werden, auf welche Daten ein Angreifer Zugriff gehabt haben könnte und wie sensibel diese sind oder waren. Im Falle von personenbezogenen Daten kann es sich um einen meldepflichtigen Datenschutzvorfall handeln. Forschungsdaten können ebenfalls Vertraulichkeits- oder Geheimhaltungsanforderungen unterliegen. Informieren Sie ggf. die Datenschutz- und IT- bzw. Informationssicherheits-Verantwortlichen Ihrer Einrichtung!

Was kann ich tun, um den Schaden von Passwort-Leaks zu minimieren?

Für den Umgang mit Passwörtern gilt die Empfehlung, für jeden Dienst ein eigenes Passwort zu verwenden. Ein Datenleck bei einem Dienstleister gefährdet dann nicht auch noch Daten bei anderen Dienstleistern. Die IT-Sicherheitsrichtlinien von GWDG, MPG und Universität fordern auch explizit, dass die dienstlichen Passwörter nicht auch noch an anderer Stelle verwendet werden.

Was kann ich tun, wenn ich mir nicht alle Passwörter merken kann, wenn ich für jeden Dienstleister ein anderes Passwort verwenden soll?

Das eine dienstliche Passwort, welches man täglich mehrmals benötigt, wird man sich wahrscheinlich merken können. Für Passwörter bei Dienstleistern, die man selten nutzt, ist Passwort-Merken sicherlich illusorisch. Solche Passwörter muss man irgendwo notieren. Die beste Lösung dafür sind Passwort-Manager. Das sind Programme, die in einer verschlüsselten Datei Passwörter sicher aufbewahren. Die Verschlüsselung der Datei wird dabei mit einem Master-Passwort geschützt. Man muss sich dann nur noch das Master-Passwort merken. Das Master-Passwort sollte dann natürlich auch ein starkes Passwort sein (länger als einfache Passwörter, komplex und nicht von fremden Personen zu erraten).

Passwort-Manager können auch starke Passwörter erzeugen. Die kann man sich dann sicherlich nicht merken. Aber da der Passwort-Manager sowieso dazu dient, bei Bedarf ein Passwort aus der verschlüsselten Datei herauszukopieren, um sich damit bei einem bestimmten Dienst anzumelden, kann man auf diese Weise ohne großen Aufwand starke Passwörter nutzen.

Wie kann man die API-Methode nutzen?

Diese Methode lässt sich z. B. mit Bordmitteln von Betriebssystemen wie Linux, FreeBSD oder macOS nutzen. Das nachstehende Shell-Skript implementiert eine Abfrage eines Passworts, die Berechnung des SHA-1-Hashes, die API-Abfrage und die Auswertung der Antwort:

```
if [ "$1" = "-v" ]
then
        silent=""
elif [ "$1" = "" ]
then
        silent="-s"
else
        echo
        echo Usage:
        echo "      $0 [-v]"
        echo
        echo Check Password in https://haveibeenpwned.com/Passwords
        echo
        echo "  -v: visible password during input, instead asking twice for
password"
        echo
        exit
fi
read $silent -p "Enter Password:" password
if [ "$silent" = "-s" ]
then
        echo ""
        read -s -p "re-enter Password:" second
        echo ""
        if [ "$password" != "$second" ]
        then
                echo "Passwords don't match!"
                exit
        fi
fi

sha1=`echo -n $password | openssl sha1 | cut -c 10-49 | tr 'a-z' 'A-Z'`
first5=`echo $sha1 | cut -c 1-5`
match=`echo $sha1 | cut -c 6-40`

result=`wget -q -O - https://api.pwnedpasswords.com/range/$first5 | grep
$match`
if [ "$result" = "" ]
then
        echo "No match found"
else
        echo "No of Matches : " `echo $result | sed -e "s/.*://" `
fi
password=""
second=""
```

Die wichtigsten Empfehlungen auf einen Blick

- Falls Sie Ihr Passwort oder Ihre Passwörter unter https://haveibeenpwned.com/Passwords geprüft haben und eines Ihrer Passwörter dort gefunden wurde, ändern Sie es bitte unverzüglich.
- Falls Ihre E-Mail-Adresse auf https://haveibeenpwned.com gefunden wird und Sie auf eine Prüfung des Passworts verzichten, empfehlen wir sicherheitshalber, Ihr entsprechendes Passwort zu ändern.
- Das Passwort sollte neu sein, also nicht schon einmal in dienstlichen oder privaten Kontexten verwendet worden sein.
- Passwort-Manager wie KeePass (https://keepass.info) bieten die Möglichkeit, sichere und individuelle Passwörter für beliebige IT-Dienste und Webseiten zu generieren und zu verwalten.

Stand: 23.01.2019