Test: Sind Ihre Passwörter sicher?

Vor einiger Zeit haben wir ihnen eine Seite vorgestellt, mit der man prüfen kann, ob die eigene E-Mail-Adresse gehackt wurde. Sollte das der Fall sein, so ist es eine der wichtigsten Aufgaben, das Passwort sofort zu ändern. Heute möchten wir Ihnen eine andere, ähnliche Seite vorstellen, mit der man die eigenen Passwörter überprüfen kann. Dabei wird geschaut, ob das eingegebene Passwort schon einmal in einer Liste von veröffentlichten (geleakten) Passwörtern aufgetaucht ist. Wenn das der Fall ist, so bedeutet es, dass Ihr Passwort den Internetkriminellen bekannt ist.

Die Seite, um die es heute geht und die einen Test der Passwörter durchführt ist englischsprachig, aber leicht zu bedienen. Die Seite heißt:
Has your password leaked?

Trägt man ein Passwort auf dieser Seite ein, so wird es mit über 988 Millionen Passwörtern abgeglichen, die zum Beispiel durch Datenlecks bekannt wurden und daraufhin im Internet veröffentlicht wurden. Diese Listen sind auch den Internetkriminellen bekannt und sie versuchen, Zugangsdaten für verschiedene Internetdienste zu erlangen. Sobald ein Passwort auf einer dieser Listen auftaucht, gilt es absolut unsicher.

Wie kann man die Seite benutzen?

Zunächst einmal können Sie mit dieser Seite Ihre bestehenden Passwörter überprüfen. Dabei brauchen Sie sich keine Sorgen zu machen, denn die Seite speichert keine Passwörter und die Seite weiß auch nicht, *wofür* Sie dieses Passwort verwenden. Es spielt also keine Rolle, ob es sich dabei beispielsweise um ein E-Mail-Passwort, ein Amazon-Passwort oder ein Passwort für die Online-Apotheke handelt. Es wird bei der Überprüfung lediglich abgeglichen, ob das angegebene Passwort schon einmal irgendwann im Internet öffentlich aufgetaucht ist, völlig unabhängig davon, wofür das Passwort verwendet wurde.

Auf der Seite wird an der Stelle “Your Password” ein Klick ausgeführt, man gibt das zu testende Passwort ein und geht auf die Schaltfläche “Check now”. Danach wird ein kurzes Ergebnis angezeigt. Eine grüne Schrift bedeutet, dass das Passwort weiterhin als sicher gilt, eine rote Schrift bedeutet, dass das Passwort umgehend geändert werden sollte.

Sollte ein Treffer erfolgen, also die rote Schrift “**Oh no! Your password has been leaked”**, so ist dringend davon abzuraten, dieses Passwort weiterhin zu verwenden. Hierbei muss man allerdings klarstellen: Ein Treffer bedeutet nicht zwangsläufig, dass **Ihre persönlichen** Zugangsdaten gehackt

wurden. Es gibt hier keinen Rückschluss auf Ihre Person oder Ihre persönlichen Passwörter. Es bedeutet nur, dass das Passwort, das Sie verwenden, schon einmal veröffentlicht wurde. Es könnte sein, dass Sie Ihr Passwort auf einer anderen Internetseite in der Vergangenheit schon einmal genutzt haben. Es kann sich dabei aber auch um das Passwort einer anderen Person gehandelt haben. Denn es ist ja durchaus denkbar, dass irgendwo auf der Welt eine andere Person schon einmal das gleiche Passwort verwendet hat wie Sie. Ein Treffer bedeutet nun, dass dieses Passwort den Kriminellen als Passwort bekannt ist und nicht mehr genutzt werden darf.

Hintergründe

Wenn Kriminelle versuchen, einen Zugang zu hacken, dann arbeiten Sie mit Programmen, die das Passwort knacken. Diese Programme arbeiten in Sekundenschnelle und versuchen, das korrekte Passwort herauszufinden. Dabei werden Listen von beliebten Passwörtern und solchen Passwörtern verwendet, die bei anderen Internetseiten durch Datenlecks bekannt wurden. Wenn ein Passwort auf einer dieser Listen steht, ist es in Sekundenschnelle gefunden und der Zugang wurde geknackt. Wenn das Passwort nicht auf der Liste steht, muss das Hackerprogramm sehr sehr viel länger daran arbeiten, den Zugang zu knacken – sofern es überhaupt gelingt. Daher sollte man tunlichst vermeiden, dass das eigene Passwort auf einer dieser Listen steht. Und das ist der Grund, warum diese Prüfung so viel Sinn macht. Bei jedem neuen Passwort, das Sie sich neu ausgedacht haben und das Sie in Zukunft verwenden möchten, geben Sie das Passwort vor der Benutzung als Test auf der Seite ein. Sollte hier ein Treffer angezeigt werden, so denken Sie sich bitte ein anderes Passwort aus.

Ein Beispiel zum besseren Verständnis:

Ich melde mich 2016 auf einer Internetseite an und denke mir für die Anmeldung das Passwort “kf5at94h” aus. Die besagte Internetseite hat keinen guten Schutz und wird 2020 gehackt. Ich verwende die besagte Internetseite seit 2020 aber gar nicht mehr, habe fast vergessen, dass ich dort angemeldet bin bzw. war. Die Anmeldedaten der betroffenen Internetseite werden von den Kriminellen ausgelesen und im Internet veröffentlicht. Jeder Hacker nutzt fortan diese Passwortliste, auf der auch mein Passwort “kf5at94h” aus 2016 steht. Wenn ich nun das gleiche Passwort in 2023 immer noch für andere Aktivitäten verwende, zum Beispiel bei meiner E-Mail-Adresse, und es als Test auf der Seite eingebe, so erhalte ich einen Treffer, dass mein Passwort veröffentlicht wurde. Meine E-Mail-Adresse wurde zwar nicht gehackt (**noch nicht**), aber das Passwort, das ich verwende, ist den Internetkriminellen bekannt. Zur Sicherheit ändere ich also sofort das Passwort meiner E-Mail-Adresse. Dabei beachte ich, dass das E-Mail-Passwort auf der Internetseite meines Anbieters geändert und danach in meinem E-Mail-Programm (auf PC und Smartphone) gespeichert werden muss.

Fazit

Mit Hilfe dieser Seite ist es besonders leicht, herauszufinden, ob das eigene Passwort noch als “sicher” gilt oder ob es bereits in einem Datenleck vorkam. Doch auch dann, wenn man ein neues Passwort nutzen will, ist es sinnvoll, dieses erst einmal auf die beschriebene Weise zu kontrollieren, ob es nicht vielleicht in einem der Datenlecks enthalten ist. Wenn jemand bei der Erstellung des Passworts ordentlich und korrekt vorgeht, ein Passwort mit 12 Zeichen generiert und dabei Ziffern, große Buchstaben, kleine Buchstaben und Sonderzeichen nutzt, dann ist das Passwort mit extrem hoher Wahrscheinlichkeit als sicher einzustufen und wird in keiner der Datenleck-Listen vorkommen.

Und sollte eines Ihrer Passwörter einen Treffer auslösen und Sie wollen es ändern, dann müssen Sie sich an die Internetseite/Firma wenden, bei der das jeweilige Passwort zur Zeit genutzt wird. Dort muss das Passwort geändert werden. Der Vorgang zum Ändern des Passworts funktioniert immer recht einfach, aber bei jeder Internetseite/Firma ein klein wenig anders. Nehmen Sie sich Zeit, diese Aufgabe kann niemand für Sie erledigen und es ist oft nicht nach 5min getan. Man muss sich die Zeit nehmen, die Passwörter zu erneuern und die passenden Schritte durchführen.