26.04.2024

# Passkeys: Online mehr Sicherheit ohne Passwort

Drei Fragen zum Welt-Passwort-Tag an Ayten Öksüz, Datenschutzexpertin der Verbraucherzentrale NRW

**In Online-Shops, sozialen Netzwerken, beim E-Mail-Postfach – Passwörter sind meist die einzige Zugangssicherung zu Online-Accounts. Dabei gibt es mittlerweile ein Verfahren, das dem Passwort überlegen ist, und zwar bei Komfort und Sicherheit: Es heißt Passkeys, was übersetzt „Hauptschlüssel“ bedeutet. Statt mit einem Passwort loggt man sich per Fingerabdruck, Gesichtsscan oder mit einer PIN ein. Im Hintergrund verifiziert ein sogenannter Authenticator die Anmeldung. Zentraler Bestandteil hierbei sind Passkeys, zufällig generierte lange Zeichenketten. Aktuell rüsten immer mehr Online-Dienste wie Amazon, Ebay und PayPal nach und bieten Verbraucher:innen die Möglichkeit, sich mit einem Passkey anzumelden. „Passkeys können mehr Sicherheit bei Online-Accounts bieten, insbesondere, weil viele Menschen noch immer schwache Passwörter nutzen“, sagt Ayten Öksüz, Datenschutzexpertin der Verbraucherzentrale NRW. „Vor allem sind sie ein guter Schutz vor Phishing.“**

## Was sind Passkeys?

Das bisher verbreitete Verfahren zur Authentifizierung bei Webdiensten ist die Kombination aus Benutzername und Passwort. Kriminelle, die das Passwort erfahren, können damit in den jeweiligen Online-Account einbrechen. Mit Passkeys ist das anders. Statt mit einem Passwort loggt man sich per Fingerabdruck, Gesichtsscan oder mit einer PIN ein – wenn der gewünschte Online-Dienst das anbietet. Nötig dafür ist ein Gerät oder ein Programm, das die persönlichen Passkeys speichert. Dieses wird Authenticator genannt und kann ein spezieller Hardware-Stick sein (FIDO2), ein Programm auf dem Computer oder eine App auf dem Smartphone. Der Authenticator erstellt bei der Registrierung des Online-Accounts einen privaten Schlüssel, der beim Authenticator verbleibt, und einen öffentlichen, der an die Server des Online-Dienstes geschickt wird. Bei der nächsten Anmeldung wird dann durch das Zusammenspiel mehrerer Komponenten die eigene Identität bestätigt, ohne dass der private Schlüssel dem Online-Dienst gegenüber preisgeben wird.

drei fragen an ... drei fragen an ... drei fragen an ...

**Pressestelle**

*Verbraucherzentrale*
*Nordrhein-Westfalen e.V.*

*Mintropstraße 27*
*40215 Düsseldorf*

*Tel. (0211) 91380-1101*

*presse@verbraucherzentrale.nrw*
*www.verbraucherzentrale.nrw*

**Welche Vor- und Nachteile haben Passkeys gegenüber Passwörtern?**

Studien zeigen, dass noch immer zu viele Menschen in Deutschland zu schwache Passwörter oder ein und das selbe Passwort für ihre Online-Accounts verwenden. Gleichzeitig gelingt es Kriminellen immer wieder, über Phishing-Angriffe an Zugangsdaten von Internetnutzer:innen zu gelangen. Beides führt zu einer stetig wachsenden Zahl an erfolgreichen Hacker-Angriffen auf Online-Accounts. Passkeys setzen genau hier an, denn ein Passwort wird dabei nicht mehr benötigt. Und anders als Passwörter sind Passkeys auch wirklich geheim, denn sie werden nicht an die jeweiligen Online-Anbieter herausgegeben. Und die öffentlichen Schlüssel auf den Servern der Online-Dienste sind alleine wertlos. Damit sinkt das Risiko für Angriffe auf Server von Online-Diensten, bei denen Kriminelle in der Vergangenheit schon milliardenfach Login-Daten gestohlen haben. Auch kann das Abgreifen von Zugangsdaten über Phishing-Angriffe deutlich eingedämmt werden, da Passkey-Nutzer:innen keine Passwörter weitergeben können und gefälschte Webseiten, auf denen die Zugangsdaten angegeben werden sollen, vom System direkt erkannt und verweigert werden. Allerdings sind Passkeys grundsätzlich an ein konkretes Gerät gebunden. Mit Passwörtern kann man sich zur Not auch mal am Computer von Freunden einloggen. Mit Passkeys hingegen geht das in der Regel nur, wenn man das Gerät, auf denen die Schlüssel gespeichert sind (z.B. das Smartphone), dabei hat. Auch können Probleme bei einem Verlust des Gerätes auftreten: Ist das Gerät mit den Passkeys weg und gibt es kein Backup oder ähnliches, muss der Zugang zu jedem einzelnen Online-Dienst neu hergestellt werden. Im schlimmsten Fall könnte man den Zugriff auf seine Accounts ganz verlieren.

**Worauf sollte man bei der Nutzung von Passkeys achten?**

Wer Passkeys nutzen will, muss sich für einen Authenticator entscheiden, der die privaten Schlüssel (Passkeys) verwalten soll. Es gibt drei Varianten: Den FIDO2-Sicherheitsschlüssel (FIDO2-Stick genannt) von verschiedenen Herstellern, dann die Betriebssysteme von Apple (iCloud-Schlüsselbund), Google (Google Passwortmanager) oder Microsoft (Windows Hello) und schließlich Passwortmanager (diverse Anbieter). Der FIDO2-Stick gilt als besonders sicher, da die Passkeys lokal auf dem Stick gespeichert werden. Cloud-Lösungen bieten mehr Flexibilität bei der Nutzung von Passkeys über mehrere Geräte hinweg, speichern die privaten Schlüssel aber eben nicht lokal, sondern auf den Servern der Anbieter. Wichtig: Bei einem Wechsel des eigenen Smartphones sollte man daran denken, die Passkeys auf das neue Gerät zu übertragen (sofern nicht in einer Cloud gespeichert). Wechselt mit dem Gerät auch das Betriebssystem, z.B. von Android auf iOS, könnte das Übertragen umständlich bis unmöglich werden. Zudem ist die Nutzung von Passkeys von der Betriebssystem- und Browserversion abhängig. Für ein optimales Funktionieren und aus Sicherheitsaspekten müssen Betriebssystem und Browser stets auf dem neusten Stand gehalten werden.

## Weiterführende Infos und Links:

- Mehr zu Passkeys unter: www.verbraucherzentrale.nrw/node/94842



## Für weitere Informationen

*Pressestelle Verbraucherzentrale NRW*
*Tel. (0211) 91380-1101*
*presse@verbraucherzentrale.nrw*