Cybersicherheitsagentur Baden-Württemberg
(CSBW)

Barrierefreie Version
CSBW-Factsheet: Cybersecurity-Wissen kompakt

Zum Thema: Passkeys: Sicher anmelden ohne Passwort

Ein nicht vorhandenes Passwort, kann nicht erraten oder geleakt werden.

Passwörter sind der Schlüssel zur digitalen Identität. Benutzerkonten, in denen sensible Informationen hinterlegt sind, werden bisher bestenfalls mit komplexen Passwörtern geschützt. Der Einsatz von Passkeys ist ein neues Authentisierungsverfahren, mit dem die Notwendigkeit, das Merken und die Verwaltung von Passwörtern obsolet werden.[1]

Was sind Passkeys?

Passkeys sind Schlüssel für passwortlose Authentifizierungsverfahren, um sich in Onlinediensten oder Konten anzumelden. Die Verifikation erfolgt über einen lokalen Schlüssel, der auf den Endgeräten hinterlegt ist. Einige Dienste bieten neben der lokalen Autorisierung geräteübergreifende Passkeys in Form von Softwaremodulen an.

Ergänzt wird dieses Verfahren um eine Zwei-Faktor-Authentifizierung. Hierdurch wird sichergestellt, dass der Verlust von Endgeräten nicht einem Verlust von Zugangsdaten gleichkommt.

Wie funktionieren Passkeys?[2]

Über die Sicherheitseinstellungen einer Website oder App lassen sich bei bestimmten Diensten Passkeys zur Benutzerverifikation aktivieren. Dabei wird auf dem Gerät lokal ein geheimer Schlüssel hinterlegt. Ein dazu passender öffentlicher Schlüssel liegt bei dem Onlinedienst. Wird als Authentifizierungsverfahren Passkey ausgewählt, vergleicht der Onlinedienst den eigenen Schlüssel mit dem Geheimschlüssel auf dem Gerät. Hierbei sendet der Onlinedienst Daten in Form einer Aufgabe (die sogenannte Challenge) an das Gerät, die nur mit dem privaten Schlüssel auf dem Endgerät lösbar ist. Der Schlüssel wird dabei nicht herausgegeben. Der Onlinedienst erkennt anhand der Signatur, dass der Account auch zum Endgerät gehört.

Ist damit Dritten ein Zugriff möglich, wenn sie das Endgerät haben?

Damit Unbefugte nicht automatisch Zugang zu Accounts haben, wenn sie beispielsweise ein Endgerät ausleihen oder stehlen, werden Passkeys mit einer Zwei-Faktor-Authentifizierung versehen. Zusätzlich zu einem Passkey müssen

Nutzende biometrische Daten, wie einen Fingerabdruck, eine Gesichtserkennung oder wahlweise auch eine PIN hinterlegen. Erst wenn beim Anmeldeverfahren Passkey und die biometrischen Daten bzw. die PIN übereinstimmen, erfolgt der Login.

Wie kompliziert ist die Anwendung von Passkeys?

Nutzende erleben das komplex wirkende Anmeldeverfahren als höchst komfortabel. Sie öffnen lediglich die Seite und greifen über den hinterlegten Fingerabdruck oder mittels einer PIN auf den Account zu.

Was sind Vorteile von Passkeys?[1]

1. Passkeys erreichen grundsätzlich die erforderliche Komplexität: Sie bestehen aus zufällig und automatisch generierten, langen Zeichenketten. Diese sind sehr schwer zu erraten.
2. Passkeys können nicht vergessen werden.
3. Es gibt für jeden Account nur einen Passkey. Damit können selbst bei erfolgreichem Diebstahl nicht gleichzeitig mehrere Accounts geknackt werden.
4. Passwörter werden bei Onlinediensten gespeichert, der geheime Passkey nicht. Letzterer liegt ausschließlich auf dem Endgerät.

Geräteübergreifende Nutzung von Passkeys

Passkeys lassen sich in der Regel auf mehreren Geräten nutzen und über die Cloud synchronisieren. Ist der geheime Schlüssel nur auf dem Smartphone hinterlegt, kann dieser auch für die Anmeldung am PC genutzt werden. Dazu ist es erforderlich, einen QR-Code vom PC-Bildschirm zu scannen. Außerdem müssen die beiden Geräte über eine aktivierte Bluetooth-Verbindung miteinander kommunizieren. Diese dient durch die Herstellung einer lokalen Verbindung der zusätzlichen Sicherheit. Nach Bestätigung der biometrischen Daten auf dem Smartphone, kann auf einen Onlinedienst via PC zugegriffen werden.

Folgen bei Verlust von Endgeräten

Passkeys können entweder über lokale Backups wiederhergestellt oder mit einem Clouddienst synchronisiert werden. Stehen beide Möglichkeiten nicht zur Verfügung, bieten diverse Dienste an, die eigene Identität anderweitig zu verifizieren und einen neuen Passkey zu erhalten. Lokale Passkeys sind meist an das jeweilige Betriebssystem gebunden. Daher kann bei einem Gerätewechsel eine Übertragung der Passkeys bei unterschiedlichen Betriebssystemen kompliziert oder gar unmöglich werden.

Welche Geräte unterstützen Passkeys?[3]

Passkeys sind bei einigen Diensten bereits in die Betriebssysteme und Browser integriert. Das Passkey-Verfahren wird mit den folgenden Betriebssystemen bzw. Browsern unterstützt:

1. Windows: ab Version 10
2. macOs: ab Ventura
3. iOS: ab Version 16
4. Android: ab Version 9
5. Browser: Aktuelle Versionen von Edge,
6. Chrome, Safari (Firefox voraussichtlich ab Version 120; Ende November 2024)

Quellen:

[1] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Passkeys/passkeys-anmelden-ohne-passwort_node.html

[2] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Passkeys/Kryptografie-hinter-Passkey/kryptografie-hinter-passkey_node.html

[3] https://www.heise.de/hintergrund/Bestandsaufnahme-Passwort-Nachfolger-Passkeys-9048722.html

Für weitere CSBW-Factsheets QR-Code scannen:

www.cybersicherheit-bw.de

CSBW – Abteilung 1: Prävention – Stand 11.2024
Kontakt: schulungen@cybersicherheit.bwl.de