2048: 30 JAHRE DSGVO

Ein kritischer Rückblick auf die europäische Digitalisierung

DIE SCHLEICHENDE EVOLUTION

Auf dem sicheren Weg in eine passwortlose Zukunft

DAS ELEKTRONISCHE ICH

Ein Plädoyer für gut gemachte digitale Identitäten

Handelsblatt Journal

Eine Sonderveröffentlichung von Euroforum Deutschland

NOVEMBER 2023 | WWW.HANDELSBLATT-JOURNAL.DE

CYBERSECURITY & DATENSCHUTZ

SECURING THE DIGITAL AGE

euroforum

Medienpartner

Handelsblatt

Substanz entscheidet.

Advertorial

Vom Passwort zum Passkey

Die schleichende Passwort(r)evolution in eine passwortlose Zukunft

> 92 % der IT-Verantwortlichen sehen Passkeys als wichtigen Meilenstein, das Risiko von Cyberangriffen zu reduzieren.

Peter van Zeist,
Principal Solutions Consultant, LastPass

von Peter van Zeist

Das Interesse an passwortloser und Passkey Authentifizierung ist groß. 79 % aller Datenverstöße sind auf kompromittierte Anmeldeinformationen zurückzuführen.[1] Es ist also keine Überraschung, dass Passwörter nicht mehr zeitgemäß sind.

Passwörter für Cloud-Apps, die nicht ausreichend von herkömmlichen Identitätstools wie SSO, MFA und PAM geschützt werden, sind ein beliebter Eintrittspunkt für Cyberbedrohungen. Solche Bedrohungen können nur abgewendet werden, wenn es gelingt, sich von Passwörtern loszusagen und sicherere Authentifizierungsmethoden einzuführen. 92 % der IT-Verantwortlichen sehen Passkeys als wichtigen Meilenstein, das Risiko von Cyberangriffen zu reduzieren.[2]

Passkeys kommen, Passwörter bleiben

Die passwortlose Realität wird jedoch kein klarer Schnitt sein. Die komplette Umstellung auf passwortlose Zugänge nach dem FIDO2 Standard zu allen Webseiten, Geräten und Diensten wird, dem Lindy Effekt folgend, Jahre, wenn nicht sogar Jahrzehnte dauern. Es handelt sich um einen komplexen Change Management Prozess, der neben der Unterstützung und Entwicklungsanstrengungen von Millionen Technologieanbietern auch die Beteiligung der Benutzer:innen erfordert.

Da immer mehr Webseiten Passkeys einführen und Endbenutzer:innen ihre Passwörter durch diese ersetzen, besteht das Risiko einer „Schatten-IT“ in privat verwalteten Authentifikationssystemen wie Browsern oder Betriebssystemen; jedoch mit Passkeys statt wie bisher mit Passwörtern. Das sind die Folgen, wenn Unternehmen keine unternehmensweite Passkey-Lösung anbieten.

Passwortmanager als ideale Lösung

Endbenutzer:nnen benötigen einen sicheren und einfachen Speicherort für ihre Passkeys sowie ihre Passwörter, die sie noch nicht umgestellt haben. Passwortmanager sind die einzige Lösung, die gleichzeitig eine Speicherung für Passwörter, Passkeys und sensible Informationen bietet und einen Abruf dieser über alle Geräte, Browser und Betriebssysteme hinweg ermöglicht.

Als Branchenführer im Bereich der Passwortverwaltung und der passwortlosen Authentifizierung wird LastPass letztlich das Master-Passwort vollständig entfernen. Das sorgt für maximale Usability und Benutzerakzeptanz und somit für erhöhte Sicherheit. Schon heute bieten wir die Möglichkeit eines passwortlosen Logins in den Tresor über den LastPass-Authentifikator sowie über FIDO2-kompatible Authentifikatoren. Die Erstellung, Speicherung und Verwaltung von Passkeys wird ebenfalls in naher Zukunft unterstützt.

lastpass.com

1 Verizon DBIR, 2023

2 Workforce Authentication Report 2023, FIDO Alliance und LastPass

Illustration: Getty