LastPass

Werken zonder wachtwoorden: veilig en eenvoudig

Wachtwoorden veroorzaken veel problemen.

IT-beheerders melden dat gebruikers **gemiddeld 63 wachtwoorden** nodig hebben voor de toepassingen die ze in hun dagelijks werk gebruiken.[1]

Bijna driekwart (73%) van de IT-beheerders geeft aan dat hun organisatie minstens iedere drie maanden een wachtwoord moet herstellen en **bij 92% is dit iedere zes maanden het geval.**

Door de enorme hoeveelheid wisselende aanmeldingsgegevens is bijna **een derde (31%) van de helpdesk-tickets gerelateerd aan wachtwoorden.**

De vraag is niet meer of ook uw bedrijf hiermee te maken krijgt, maar wanneer.

35% Iets meer dan een derde (35%) van de IT-beheerders heeft in de afgelopen 2 jaar een zakelijk gegevenslek ervaren.

Probeer niet langer om een evenwicht te vinden tussen gebruiksgemak en beveiliging: kies voor allebei. **Laat medewerkers zich zonder wachtwoord aanmelden bij hun digitale kluis.**

Uw bedrijf voldoet al aan de voorwaarden.

U maakt al gebruik van de benodigde technologie. Wachtwoordbeheerders en meervoudige verificatie zijn de basis voor een toekomst zonder wachtwoorden.

64% van de IT-beheerders zegt dat hun bedrijf een wachtwoordbeheerder heeft. Hetzelfde percentage gebruikt single sign-on. **MFA is zelfs nog gebruikelijker, met 67%.**

De juiste strategie. IT-beheerders zijn early adopters met een toekomstgerichte blik.

57% Voor meer dan de helft van de IT-beheerders (57%) staat wachtwoordloze technologie in de planning voor hun organisatie.

WAAROM ZOU U KIEZEN OM ZONDER WACHTWOORDEN TE GAAN WERKEN?

Als u de drempels rondom wachtwoorden wegneemt voor uw medewerkers, krijgen ze sneller toegang tot de toepassingen en gegevens die ze het meeste nodig hebben.

Met eenvoudige toegang moedigt u de aanname door gebruikers aan, zodat uw algehele wachtwoordbeveiliging uiteindelijk een stuk sterker wordt.

U kunt zelfs strengere vereisten afdwingen voor het hoofdwachtwoord, omdat gebruikers dit niet meer hoeven in te voeren voor toegang tot hun kluis.

Hoe werkt wachtwoordloze technologie?

Gebruikers krijgen zonder wachtwoord toegang tot hun LastPass-kluis op hun bureaublad met behulp van één van drie veilige mechanismen om hun identiteit te verifiëren: met de LastPass Authenticator, of met hardwaresleutels of biometrische technologie die compatibel zijn met FIDO2.

Bij wachtwoordloze aanmeldingen zijn indirect toch nog wachtwoorden betrokken – in ieder geval voorlopig. Hoofdwachtwoorden zijn nodig om een LastPass-account te registreren en om beveiligingsgerelateerde wijzigingen in het account door te voeren.

Het is tijd om na te denken over een wereld zonder wachtwoorden

Over het algemeen zeggen IT-beheerders meer ontspannen en veiliger te kunnen werken als ze wachtwoordloze technologie zouden kunnen inzetten.

44% meer ontspannen

33% veiliger

32% minder gestrest

Offer geen veiligheid op voor gebruiksgemak, als u allebei kunt krijgen.

Uw bedrijf is beter beveiligd tegen cyberrisico's als medewerkers veilige verificatiemethoden gebruiken voor toegang tot hun kluis, in plaats van zwakke of hergebruikte wachtwoorden.

Werk zonder wachtwoorden met LastPass

Bronnen:
1. Het onderzoek is uitgevoerd door Lab42, met respondenten uit de Verenigde Staten, Australië, Canada, Frankrijk, Duitsland en het Verenigd Koninkrijk.

07.17.2023/PDF/LP2023