LastPass

Autenticazione senza password: una realtà semplice e sicura per la tua azienda

Le password sono una fonte di problemi concreta.

Secondo gli amministratori informatici, gli utenti **usano in media 63 password** per svolgere le proprie mansioni quotidiane.[1]

Il 73% degli amministratori IT (quasi 3/4) riferisce che la propria organizzazione deve essere sottoposta a un ripristino delle password almeno ogni 3 mesi, **un tasso che sale al 92% se l'intervallo di riferimento si estende a 6 mesi.**

Una delle conseguenze di questa enorme mole di password modificate è che **quasi 1/3 (il 31%) delle richieste di assistenza ricevute dal supporto tecnico è legato alle password.**

Non bisogna più chiedersi, dunque, se sia possibile che la propria azienda venga violata, ma quando.

35% Poco più di 1/3 degli amministratori informatici (il 35%) ha subito una violazione informatica negli ultimi 2 anni.

Perché continuare a perdere tempo cercando di fare l'equilibrista tra la sicurezza e la praticità, quando puoi avere entrambe semplicemente consentendo ai dipendenti di **accedere alla propria cassaforte digitale senza alcuna password?**

La tua azienda può già contare su:

Tutti i componenti essenziali – le applicazioni per gestire le credenziali, insieme all'MFA, sono il fondamento di un futuro senza password.

64% Tasso di amministratori IT presso aziende che usano un gestore di password, una percentuale che corrisponde a quelle in cui è in uso l'SSO. **Il tasso di utilizzo dell'MFA è ancora più alto, pari al 67%.**

Una strategia idonea – gli amministratori informatici sono utenti precoci e lungimiranti.

57% Oltre metà degli amministratori IT (il 57%) riferisce che le tecnologie di autenticazione senza password sono già state inserite nella tabella di marcia aziendale.

PERCHÉ DOVRESTI LIBERARTI DALLE PASSWORD?

Eliminare i problemi legati alle password consente ai dipendenti di accedere rapidamente alle applicazioni e alle credenziali di cui hanno più bisogno.

Un'autenticazione più semplice ne favorisce l'utilizzo e una maggiore adozione da parte del personale, migliorandone di riflesso l'approccio alle password.

Imposta requisiti di sicurezza ancora più severi per la password principale, dal momento che gli utenti non dovranno digitarla per accedere alla cassaforte.

Come funziona l'autenticazione senza password?

Gli utenti ottengono l'accesso senza password alla cassaforte LastPass sul computer utilizzando uno dei tre meccanismi di autenticazione sicura: LastPass Authenticator, l'autenticazione biometrica basata su FIDO2 o le chiavi hardware conformi a FIDO2.

L'autenticazione senza password non elimina le password, almeno per ora! La password principale continuerà a essere necessaria per creare un account LastPass e per applicarvi modifiche che hanno effetti sulla sicurezza.

Finalmente è arrivato il momento di liberarsi dalle password.

In generale, gli amministratori informatici si sentirebbero più tranquilli e protetti se potessero adottare un sistema per l'autenticazione senza password.

44% **più tranquilli**

33% **più protetti**

32% **meno stressati**

Non devi accontentarti di scegliere tra sicurezza e semplicità se puoi averle entrambe

Quando i dipendenti possono contare su metodi di autenticazione sicuri per accedere alla cassaforte, invece delle solite password vulnerabili o riutilizzate, garantiscono alla tua azienda maggiore protezione dalle minacce informatiche.

Liberati dalle password con LastPass

Fonti:
1. Ricerca condotta da Lab42 su un campione di professionisti operanti nei seguenti Paesi: Stati Uniti, Australia, Canada, Francia, Germania e Regno Unito.

07.17.2023/PDF/LP2023