Whitepaper | Autenticazione passwordless

Autenticazione passwordless

La fine delle password sembra davvero più vicina

Index

Introduzione

I costi associati all'utilizzo delle password e i rischi di sicurezza che ne conseguono hanno ormai superato i benefici, spingendo il mondo della sicurezza informatica ad intraprendere da un paio d'anni la strada verso l'autenticazione senza password (password-less).

L'utilizzo di tecnologie come la biometria, la crittografia asimmetrica e standard aperti come FIDO (Fast IDentity Online) mirano alla sostituzione delle password grazie all'utilizzo di dispositivi largamente diffusi come smartphone, sensori di impronte digitali e fotocamere con riconoscimento facciale.

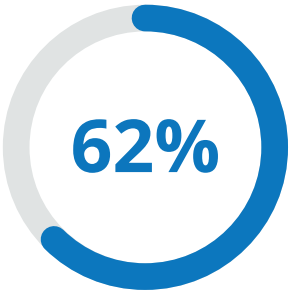
L'adozione di metodologie di autenticazione alternative alle password consente e consentirà a sempre più organizzazioni di offrire agli utenti convenienza e facilità d'uso ed allo stesso tempo di abbattere notevolmente le minacce e i costi elevati ai quali oggi queste sono continuamente esposte.

I problemi delle password in numeri

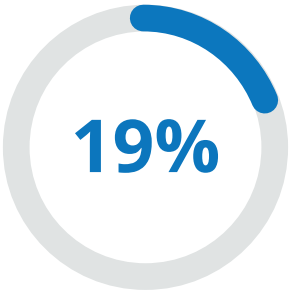
L'autenticazione basata sull'utilizzo di password è intrinsecamente vulnerabile agli attacchi che prendono di mira l'anello più debole della catena di sicurezza: l'utente. È inevitabile infatti che gli utenti commettano errori quando si parla delle proprie password.

Utilizza password contenti nomi o date di nascita

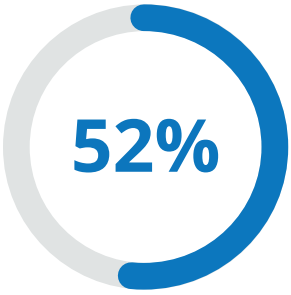
Riutilizza la stessa password per più account



Riutilizza la stessa password sia in ambito personale che lavorativo



Sceglie password più complesse in ambito aziendale



Ha condiviso password con altre persone

La percentuale di data breach legati ad applicazioni web che coinvolgono compromissione di credenziali.

Da quanto emerge da un sondaggio condotto da Google in collaborazione con Harris Poll[1] il 24% degli americani utilizza password banali (Password, abc123 ...) o variazioni di queste, mentre il 59% degli intervistati ha ammesso di aver utilizzato il proprio nome, quello di una persona cara o del proprio animale domestico o una data di nascita come parte di una password utilizzata per accedere ad un account in loro possesso.

Nonostante il 91% dei partecipanti ad un sondaggio di LastPass[2] abbia affermato di essere consapevole del rischio associato all'utilizzo della stessa password per più account, il 59% degli intervistati ha dichiarato di avere comunque questa abitudine. Nel 61% dei casi la paura di dimenticarsi la password è stata la motivazione che ha portato al riutilizzo della credenziale. Ciò non si limita solo alla sfera personale ma anche all'ambito lavorativo: i risultati di un altro sondaggio di LogMeIn[3] dimostrano che il 62% della popolazione intervistata riutilizza la stessa password sia per account personali che aziendali (e solamente il 19% sceglie password più complesse in ambito lavorativo).

E ancora: secondo Transmit Security[4] il 52% degli utenti presi in esame afferma di aver condiviso la password di un proprio account ad un'altra persona.

Considerate le cattive abitudini in materia di password e il gran numero di modalità con cui queste vengono prese di mira dagli attaccanti (*credential stuffing, dictionary attack, bruteforce attack, MITM, keylogging, traffic interception, phishing e altre forme di social engineering*) non sorprende che dal *Verizon Data Breach Investigations Report*[5] del 2021 emerga che ci siano episodi di compromissione di password alla base dell'89% dei casi di *data breach*[6].

[1] https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/PasswordCheckup-HarrisPoll-InfographicFINAL.pdf

I tentativi di arginare la piaga dei furti di password incoraggiando la scelta di password complesse e richiedendo cambi password frequenti si scontrano poi con la resistenza degli utenti di fronte alla scomodità comportata dai requisiti delle password che gli vengono imposti e con la difficoltà di ricordarle.

Il tutto risulta così controproducenti sotto diversi aspetti:

- **Tempo**: i dipendenti impiegano in media 24 ore all'anno per effettuare login alle postazioni di lavoro, reti e sistemi. La prospettiva peggiora se si prende in considerazione i reset password, causa di significativi ritardi per i dipendenti e di occupazione delle risorse dell'*Help Desk*. IBM[7] stima che gli amministratori spendano 27 ore all'anno per risolvere problemi di accesso ogni 100 utenti.
- **Costi**: Secondo Yubico[8] le imprese devono sostenere in media costi legati ai reset password per 5,2 milioni di dollari l'anno. Il costo medio di un reset password stimato da Forrester[9] si attesta infatti attorno ai 70$ per singolo reset.
- **Abbandono da parte dell'utente**: secondo Mastercard[10] nel 33% dei casi gli utenti non completano un acquisto online per via della password dimenticata.
- **Frustrazione dei dipendenti**: da uno studio di 1Password[11] emerge come il 44% dei dipendenti percepisca il login come un'attività frustrante che intacca il loro umore e la loro produttività, mentre il 25% ammette di non aver completato task a seguito di problemi di autenticazione.
- **Sicurezza**: la frustrazione nei confronti dell'autenticazione porta gli utenti ad adottare comportamenti rischiosi che compromettono la sicurezza (password scritte su fogliettini adesivi attaccati al monitor, password salvate all'interno di file non sicuri, password condivise etc.).

[2] https://www.darkreading.com/vulnerabilities-threats/password-reuse-abounds-new-survey-shows

[3] https://www.darkreading.com/vulnerabilities-threats/password-reuse-abounds-new-survey-shows

[4] https://www.transmitsecurity.com/blog/why-password-sharing-kills-your-bottom-line

[5] https://www.verizon.com/business/resources/reports/dbir/

[6] Un incident, ovvero un evento di sicurezza che compromette integrità, confidenzialità o disponibilità di un'informazione, che ha avuto come risultato certo, non potenziale, l'avvenuta esposizione dei dati a soggetti non autorizzati.

La MultiFactor Authentication (MFA) classica non basta

Una delle strategie più efficaci per il contrasto agli attacchi che prendono di mira le credenziali degli utenti è l'abilitazione della *MultiFactor Authenthication* (MFA), ovvero una modalità di autenticazione che richiede a un utente di fornire almeno due fattori[12] di verifica per poter completare l'accesso.

Una delle strategie più efficaci per il contrasto agli attacchi che prendono di mira le credenziali degli utenti è l'abilitazione della MultiFactor Authenthication (MFA), ovvero una modalità di autenticazione che richiede a un utente di fornire almeno due fattori di verifica per poter completare l'accesso.

L'applicazione di un ulteriore fattore oltre al nome utente e alla password garantisce un livello di sicurezza più elevato, richiedendo informazioni aggiuntive semplici da fornire per gli utenti autentici, complesse da avere a disposizione per i criminali informatici: venire a conoscenza della password non è più sufficiente per ottenere l'accesso.

La scelta dell'MFA non risulta però essere priva di difetti: gli *account takeover*[13] sono ancora possibili per via delle sofisticate tecniche utilizzate dagli attaccanti per bypassare l'MFA (SIM swapping, smishing etc.), al punto tale che durante la RSA Conference del 2022 la FIDO Alliance ha predetto che gli attacchi volti a bypassare l'MFA diventeranno la tendenza nel 2023[14].

Inoltre, se da un lato più numerosi sono i fattori richiesti più il livello di sicurezza aumenta, dall'altro più è elevato il numero di fattori peggiore è l'esperienza per gli utenti, alimentando così frustrazione e avversione da parte di questi ultimi.

L'unica soluzione che consente di azzerare le possibilità di account takeover e allo stesso tempo garantire agli utenti un'esperienza di login fluida e senza frizioni è l'autenticazione passwordless, ovvero un processo di autenticazione in cui l'utilizzo di password non è previsto.

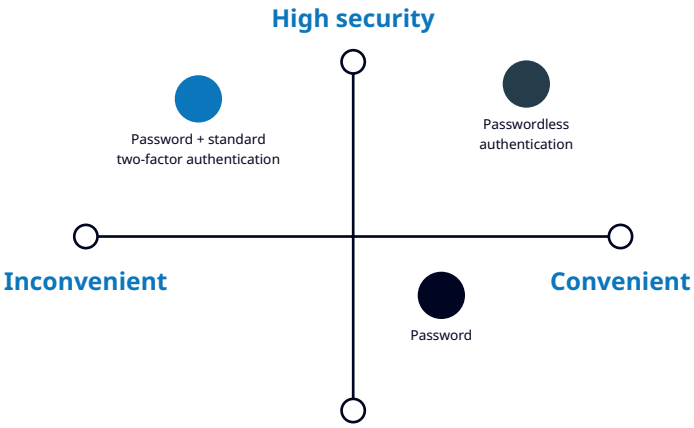


Grafico Microsoft, metodologie di autenticazione a confronto - https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2KEup

[7] https://blog.hypr.com/tips-for-low-friction-authentication

[8] https://www.yubico.com/press-releases/yubicos-2019-state-of-password-and-authentication-security-behaviors-report/

[9] https://www.forrester.com/report/best-practices-selecting-deploying-and-managing-enterprise-password-managers/RES139333

[10] https://www.transmitsecurity.com/blog/5-reasons-ciam-is-a-boon-for-business

[11] https://www.cpomagazine.com/cyber-security/43-of-employees-engage-in-risky-online-behavior-to-circumvent-complex-authentication-requirements/

[12] Le tipologie di fattori che possono essere forniti per verificare un utente tipicamente appartengono a 3 categorie: un elemento che l'utente conosce (es: domande di sicurezza), un elemento che l'utente possiede (es: OTP, cellulare), un elemento intrinseco all'utente (es: fattori biometrici come volto o impronte digitali).

[13] Presa di possesso di un account da parte di un attaccante utilizzando credenziali rubate.

[14] https://www.slideshare.net/LoriGlavin2/welcome-and-fido-updatepptx

Come funziona l’autenticazione passwordless

Con il termine autenticazione passwordless si intende una forma di MFA in cui la password è sostituita da un’alternativa sicura.

Basata su tecnologie quali la biometria (qualcosa che l’utente è), PIN (qualcosa che l’utente sa), dispositivi mobile/token hardware (qualcosa che l’utente ha) congiuntamente all’utilizzo della crittografia a chiave pubblica[15], l’autenticazione *passwordless* non prevede che venga condivisa alcuna informazione segreta tra l’utente e il sistema presso cui si autentica. Grazie a una coppia di chiavi crittografiche che sta alla base dell’autenticazione *passwordless* tutto ciò che riguarda l’identità dell’utente rimane privato: nessun *secret* condiviso tra client e server significa nessuna possibilità per i malintenzionati di portare a termine attacchi tipicamente mirati alle password quali brute *forcing*[16] e *phishing*[17].

[15] La crittografia a chiave pubblica (o asimmetrica), è un tipo di crittografia che prevede l’utilizzo di una coppia di chiavi composta dalla chiave pubblica, che deve essere distribuita, e dalla chiave privata, appunto segreta. Il meccanismo si basa sul fatto che, se con una delle due chiavi si cifra un messaggio, quest’ultimo sarà decifrabile solo con l’altra.

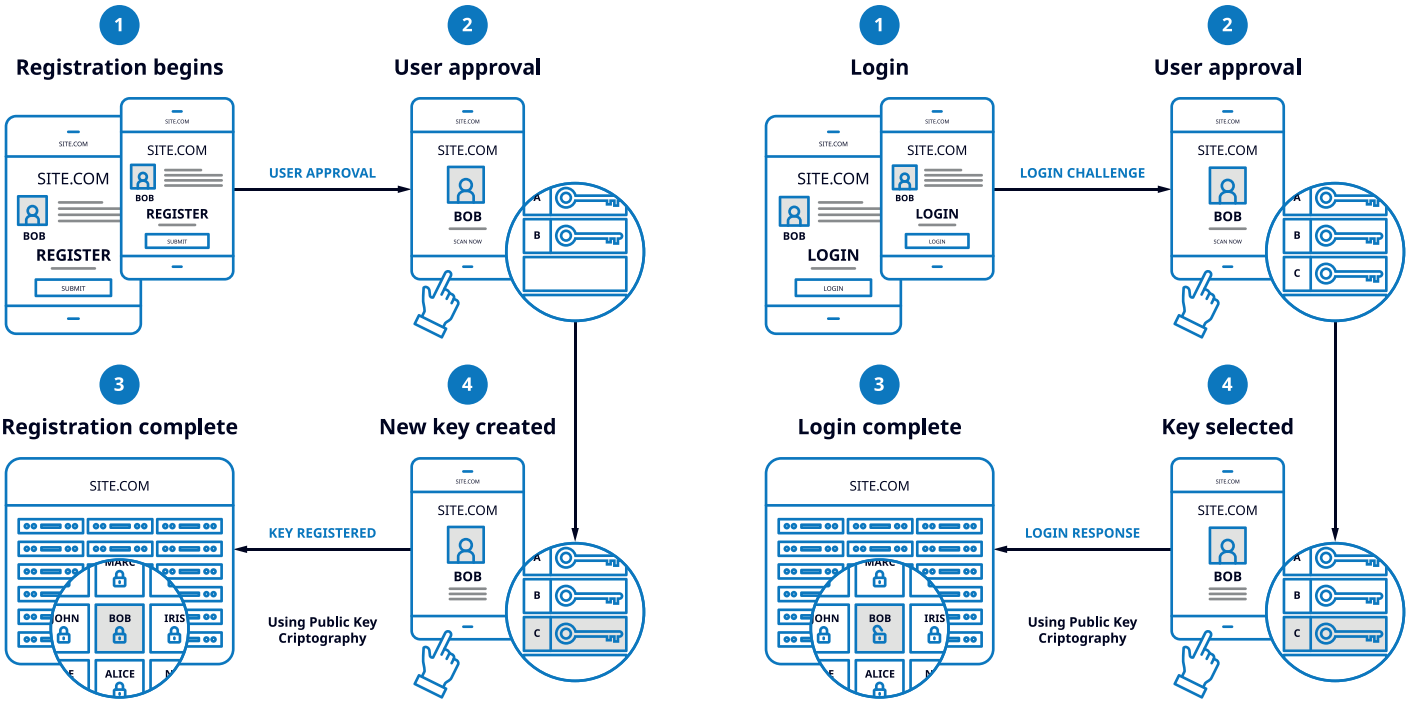
[16] Con attacco brute force si intende una modalità utilizzata dagli attaccanti per ottenere in maniera fraudolenta l’accesso ad un account. Tale modalità prevede il tentativo di tutte le possibili combinazioni di caratteri che possono costituire la password finché quest’ultima non viene individuata.

[17] Il phishing è un metodo ingannevole che spinge gli utenti a rivelare password, otp etc. utilizzato da criminali che si spacciano, tipicamente via mail, per un’istituzione legittima.

Una nuova coppia di chiavi viene generata sul *device* dell'utente al momento della registrazione presso un servizio a seguito dell'utilizzo di uno dei fattori elencati in precedenza. La chiave privata rimane in possesso dell'utente e non lascia mai il dispositivo. La corrispondente chiave pubblica viene invece condivisa con il sistema presso cui l'utente si deve autenticare.

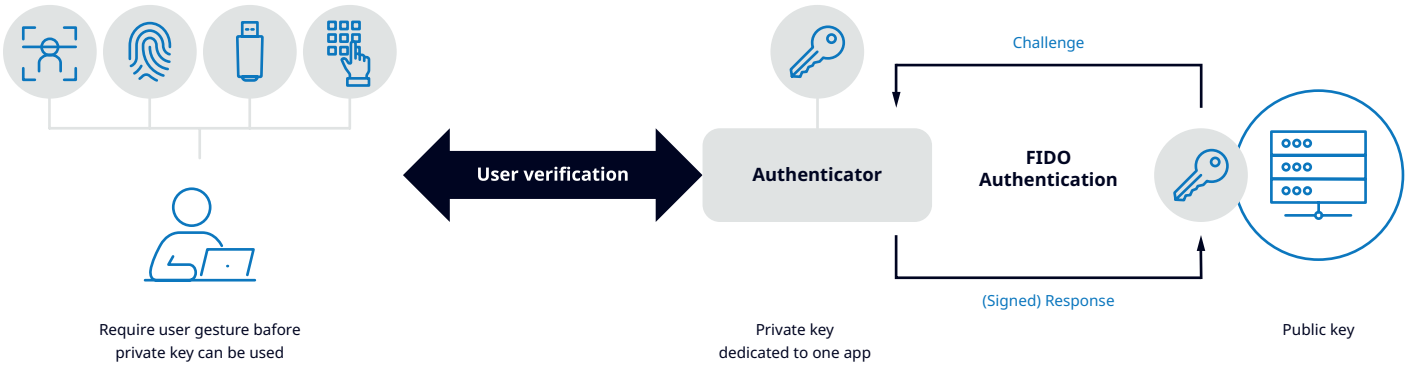
L'utente in fase di login attiva la propria chiave privata autenticandosi presso il proprio dispositivo per mezzo di pin, fattori biometrici come scansione del volto o dell'impronta digitale, dispositivi mobile o chiavette di sicurezza. Una volta attivata la chiave privata, questa viene utilizzata per firmare la *challenge* (tipicamente una stringa casuale di bit) inviata al dispositivo dal sistema a cui si vuole accedere. La *challenge* firmata verrà rimandata a quest'ultimo che la decifrerà e la confronterà con quella inviata al *device* dell'utente all'inizio del processo di login, consentendo, in caso di corrispondenza, l'accesso al sistema.

L'autenticazione è pertanto data dalla prova di possesso da parte del *device* dell'utente della chiave privata, utilizzabile solamente a seguito di un'azione sicura e *user-friendly* sul proprio dispositivo come la pressione di un dito o l'inserimento di un pin.



FIDO - Fase di registrazione - https://fidoalliance.org/how-fido-works/

FIDO - Fase di accesso - https://fidoalliance.org/how-fido-works/



Fido Alliance - Fido Authentication - https://fidoalliance.org/fido-masterclass/

La FIDO Alliance e lo Standard FIDO2

Alla base dei processi di registrazione e login in modalità passwordless vi è lo standard FIDO2, il più recente fra gli *open standard* pubblicati dalla Fido Alliance.

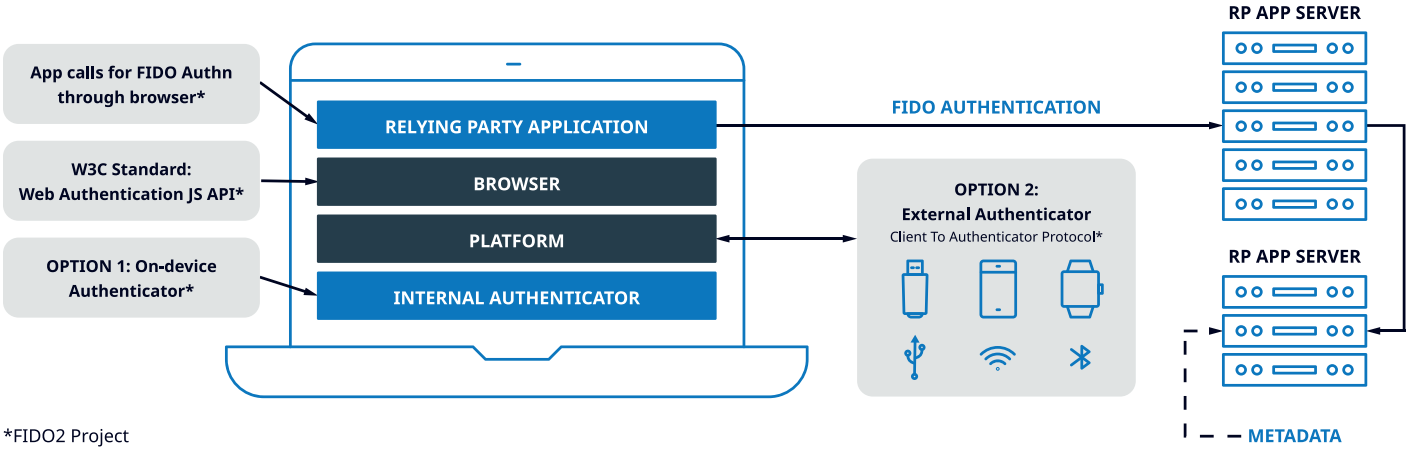
Quest'ultima consiste in un'associazione di settore aperta con una missione mirata: produrre standard di autenticazione per contribuire a ridurre l'eccessiva dipendenza dalle password promuovendo lo sviluppo, l'uso e la conformità agli standard per autenticazioni più semplici e sicure.

Alcuni dei più grandi nomi della tecnologia tra cui Apple, Meta, Amazon, Microsoft, Google e molti altri sono membri dell'*Alliance*. Ad essi si aggiungono enti normativi come il National Institute for Standards and Technology (NIST[18]), aziende di cybersecurity come Okta e Yubico e società finanziarie come PayPal, Visa, Mastercard e Bank of America.

La FIDO Alliance ha attualmente pubblicato tre serie di specifiche: *FIDO Universal Second Factor* (FIDO U2F), *FIDO Universal Authentication Framework* (FIDO UAF) e il già citato FIDO2, che include la specifica *Web Authentication* (WebAuthn) del W3C[19] e *FIDO Client to Authenticator Protocol* (CTAP).

In particolare, WebAuthn definisce una Web API[20] standard che viene implementata dai browser per consentire alle applicazioni web di sfruttare l'autenticazione FIDO. Utilizzando WebAuthn, i browser web possono invocare l'interfaccia CTAP per interagire con gli autenticatori integrati o collegati all'host tramite USB, Bluetooth (BLE) o NFC al fine di permettere all'utente di portare a termine autenticazioni *passwordless* presso applicazioni web e sistemi operativi che supportano lo standard FIDO2.

Tra gli autenticatori integrati (noti anche come "*platform authenticators*") vi sono PIN, sensori di impronte digitali e fotocamere per il riconoscimento facciale incorporate nei PC. Tra gli autenticatori esterni ("*cross-platform*" o "*roaming authenticators*") rientrano invece le FIDO Security Key e i dispositivi mobile o indossabili (smartwatch etc.).



*FIDO2 Project

FIDO Alliance - FIDO2 specifications - https://fidoalliance.org/specifications/

Ma come viene implementato lo standard dai dispositivi aventi a bordo autenticatori integrati e dai device FIDO2?

Nel primo caso un modulo hardware o software noto com TPM (*Trusted Platform Module*) memorizza in maniera protetta le chiavi private, consentendone l'utilizzo solo a seguito di autenticazioni basate su PIN o biometria.

In maniera simile, anche i device FIDO2 come le chiavette di sicurezza mostrate nella figura a lato mantengono al sicuro al proprio interno le chiavi private, richiedendo la verifica di un PIN o di tratti biometrici quali impronte digitali per potervi accedere.

Per portare ad esempio a termine un'autenticazione per mezzo di una chiavetta di sicurezza (registrata) è quindi necessario inserirla nella porta USB (o avvicinarla al lettore NFC[21]) del proprio pc, dopodiché autenticarsi localmente[22] nei confronti della chiavetta inserendo il PIN memorizzato all'interno della stessa oppure scansionando l'impronta digitale attraverso un apposito lettore presente sulla chiavetta[23].

Solo a quel punto sarà possibile avere accesso alla chiave privata, corrispettiva della chiave pubblica che viene mantenuta presso il servizio nei confronti del quale si intende autenticarsi.

Si noti che l'utilizzo di una coppia di chiavi crittografiche differente per ogni servizio mette gli utenti al riparo dai tentativi di *phishing*: l'utente otterrà infatti esito negativo qualora tenti inavvertitamente di autenticarsi ad un sito rispetto al quale non ha precedentemente registrato la chiavetta di sicurezza.

Yubico - YubiKey Bio, chiavetta di sicurezza FIDO dotata di lettore per impronte digitali (delimitato dall'anello argentato).

[18] Agenzia del governo degli Stati Uniti d'America parte del Department of Commerce (Ministero del Commercio) con il compito di sviluppare standard tecnologici.

[19] Il World Wide Web Consortium, anche conosciuto come W3C, è un'organizzazione non governativa internazionale che ha come scopo quello di favorire lo sviluppo delle potenzialità del World Wide Web stabilendo standard tecnici inerenti sia i linguaggi di markup che i protocolli di comunicazione.

[20] Costrutti di codice presenti nei browser, utilizzabili dagli sviluppatori per interagire con i componenti del browser o altri software/hardware presenti sul pc dell'utente implementando funzionalità complesse in modo semplice.

[21] Interfacce e fattore di autenticazione richiesto dalla chiavetta per verificare l'identità di un utente variano a seconda del produttore e del modello di FIDO Security Key.

[22] PIN e tratti biometrici non lasciano mai il dispositivo.

[23] Interfacce e fattore di autenticazione richiesto dalla chiavetta per verificare l'identità di un utente variano a seconda del produttore e del modello di FIDO Security Key.

Il settore workforce, terreno fertile per l'autenticazione passwordless

Mosse dalla volontà di mettersi al riparo dai *data breaches* adottando soluzioni di autenticazione *phishing-resistant* e dalla volontà di abbattere frustrazione e costi (economici e in termini di tempo) legati ai continui problemi di accesso dovuti alle password, le organizzazioni e i loro dipendenti hanno costituito storicamente l'ambito di applicazione perfetto nel quale l'autenticazione *passwordless* ha potuto cominciare a prendere piede.

Il settore della *workforce* si caratterizza infatti per l'elevato numero di applicazioni con i quali i dipendenti hanno a che fare quotidianamente per portare a termine i propri *task*, per la centralità dello scenario di accesso alla postazione di lavoro aziendale e per il prestarsi bene all'utilizzo di dispositivi di sicurezza fisici, i cui costi gravano sulle aziende che ne stabiliscono l'adozione e non sui propri dipendenti che ne diventano poi utilizzatori.

Costi di adozione che al primo impatto potrebbero intimorire le organizzazioni e dissuaderle dall'abbracciare la filosofia *passwordless*. Tali investimenti iniziali e una strada non priva di ostacoli nel raggiungere l'obbiettivo non devono tuttavia frenare le aziende dall'intraprendere questo percorso: da un'indagine condotta da Forrester[24] su mandato di Yubico per valutare l'impatto economico comportato dall'introduzione delle proprie chiavette FIDO nel contesto di cinque aziende nord-americane, emerge infatti come l'investimento iniziale sia stato ampiamente giustificato da un *Return of Investement* (ROI[25]) particolarmente elevato (203%) e da un payback *period*[26] decisamente ridotto (11 mesi).

In particolare, la percentuale rappresentativa del ROI è motivata da benefici considerevoli in termini di risparmio dato da: la riduzione dei costi dell'*Help Desk*, l'innalzamento della sicurezza che consente di eliminare i costi legati ai data *breaches* e infine la dismissione della precedente modalità di autenticazione ormai sostituita da quella *passwordless*. Questi fattori superano di gran lunga i costi legati alle chiavette FIDO dovuti all'acquisto e alla distribuzione delle stesse, al deployment e alla manutenzione della soluzione e al *training* degli utenti utilizzatori, accertando di fatto la bontà di un investimento nell'ottica *passwordless*.

Per quanto riguarda invece la difficoltà nel raggiungimento dell'obbiettivo *passwordless*, dovuta principalmente al gran numero di applicazioni in ambito *workforce* e alla presenza di applicazioni *legacy*[27], adottare un modello di *rollout* progressivo della soluzione *passwordless* su base applicazione[28] o fare affidamento su soluzioni che consentano di effettuare l'accesso alla postazione di lavoro in modalità *passwordless* e allo stesso tempo di implementare *Single-Sign-On* (SSO[29]) per gli applicativi acceduti a seguito del logon al pc, possono costituire due validi approcci per affrontare in maniera strutturata ed adeguata un cambiamento di una simile rilevanza e complessità.

[24] https://www.yubico.com/blog/as-told-by-adopters-yubikeys-roi/

[25] Il ROI, traducibile con "Ritorno sull'investimento", indica il profitto di un investimento derivante dal capitale investito. Viene calcolato pertanto dividendo l'utile netto ottenuto per il capitale investito, dove per utile netto si intende il guadagno totale al netto di tutti i costi.

[26] Il periodo di pareggio (payback period), detto anche periodo di recupero, è il tempo necessario che occorre attendere affinché le entrate comportate dall'investimento compensino le uscite sostenute.

[27] Vecchie applicazioni sviluppate sulla base di tecnologie obsolete che continuano ad essere utilizzate perché l'organizzazione non intende o non può rimpiazzarle.

[28] Approccio che prevede di prendere in esame ed intervenire su un applicativo dopo l'altro andando così ad espandere progressivamente il perimetro di applicazioni che fanno uso di metodologie di autenticazione passwordless.

[29] Proprietà di un sistema di controllo d'accesso che consente ad un utente di effettuare un'unica autenticazione valida per più sistemi software o risorse informatiche alle quali è abilitato.

Le passkeys: l'applicazione più recente dello standard FIDO2

La scomodità percepita delle chiavi di sicurezza fisiche (acquisto, registrazione, trasporto e smarrimento le principali) e le difficoltà che i consumatori devono affrontare con i *platform authenticators* (ad esempio la necessità di registrare nuovamente ogni nuovo dispositivo) hanno comportato tuttavia un'adozione limitata delle modalità di autenticazione *passwordless*, rimaste circoscritte prevalentemente ai dipendenti interni delle aziende e non alla clientela finale.

Per questo motivo la FIDO Alliance ha recentemente proposto dei cambiamenti allo standard WebAuthn al fine di ridurre ulteriormente l'utilizzo delle password anche in ambito *consumer*.

I cambiamenti proposti allo standard sono mirati a facilitare l'implementazione degli autenticatori (specialmente i *platform authenticators*) in una maniera tale da consentire la sincronizzazione delle credenziali FIDO, ovvero le chiavi private, tra i diversi dispositivi dell'utente.

Così facendo, l'utente in possesso sul proprio cellulare di una serie di credenziali FIDO utilizzate per autenticarsi presso diversi servizi, si troverà a disposizione tutte le chiavi private anche su un nuovo dispositivo, eliminando l'esigenza di registrare quest'ultimo presso tutte le applicazioni alle quale era solito autenticarsi in modalità *passwordless* con il vecchio *device*.

All'utente che vuole accedere tramite un nuovo dispositivo basterà pertanto autenticarsi tramite biometria[30] o PIN sul nuovo *device* e sfruttare la chiave privata che era stata generata sul vecchio.

Tale implementazione del protocollo FIDO si contrappone dunque all'interpretazione più classica attuata ad esempio dalle chiavette di sicurezza FIDO, le cui chiavi private mantenute all'interno vengono ora definite dalla FIDO Alliance come "*Hardware-bound FIDO Credentials*" o "*Single Device FIDO Credentials*", perché appunto legate e limitate al device sul quale sono state generate in fase di registrazione.

Al contrario, nei casi di un'implementazione del protocollo da parte degli autenticatori tale da consentire la sincronizzazione delle credenziali FIDO, la terminologia utilizzata dalla FIDO Alliance è quella di "*Multi Device FIDO Credentials*", espressione rispetto alla quale Google, Apple e Microsoft preferiscono il più commerciabile "*Passkeys*".

La FIDO Alliance è chiara nel sottolineare che è responsabilità delle diverse piattaforme OS far sì che le credenziali vengano sincronizzate da un *device* all'altro: questo comporta che la sicurezza delle credenziali sincronizzate, tipicamente tramite servizi cloud come *iCloud KeyChain* di Apple, dipendano dal meccanismo di autenticazione utilizzato per accedere a questi servizi cloud e alla procedura di recupero delle credenziali FIDO nel momento in cui tutti i vecchi dispositivi non sono più a disposizione dell'utente.

Un livello di sicurezza dunque inferiore rispetto a quello garantito dalle chiavette di sicurezza FIDO2, dove l'unico modo per avere accesso è essere in possesso del *device* che è stato registrato, ma in ogni caso decisamente più elevato rispetto all'utilizzo delle password.

Si può quindi immaginare l'utilizzo delle *passkeys* per l'accesso a servizi non critici (notizia del luglio 2023 l'ingresso di TikTok[31] nella Fido Alliance e l'adozione da parte del social delle *passkeys*), mentre destinare l'utilizzo di *hardware-bound FIDO credentials* come quelle mantenute all'interno delle chiavette di sicurezza in ambito aziendale, per utenti ad alto rischio (come gli amministratori di sistema) o per garantire l'accesso ad informazioni particolarmente sensibili.

[30] I cambiamenti proposti allo standard non prevedono modifiche alle modalità con le quali si fa uso della biometria: non cambia infatti il principio per cui il template biometrico non lascia mai il dispositivo.

[31] https://newsroom.tiktok.com/en-us/passkeys-fido-alliance

Conclusioni

In futuro raramente ci si troverà a che fare con le password nel quotidiano, sia nell'ambito lavorativo che personale. Per i dipartimenti di sicurezza e IT delle aziende, l'implementazione di esperienze di accesso intuitive ridurrà sia i costi operativi sia la frustrazione dei dipendenti dovuta alle difficoltà di ricordarsi tutte le password e alla conseguente necessità di richiederne spesso la reimpostazione.

Il tutto innalzando notevolmente il livello di sicurezza, sia che si adottino soluzioni *hardware-bound* quali le chiavette di sicurezza FIDO, sia che ci si affidi alle più fruibili *passkeys* sincronizzate tra tutti i propri dispositivi.

Con sempre più organizzazioni che entrano a far parte della FIDO Alliance e sempre più aziende che scelgono soluzioni *passwordless* FIDO la strada è tracciata: la fine delle password sembra davvero più vicina.

Key Takeaways

1. Fare affidamento sulle password non è più sostenibile, né per le aziende alle prese con costi e rischi di sicurezza elevati, né per gli utenti, alle prese con sempre più credenziali da ricordare e *user experience* frustranti.

2. La FIDO Alliance e lo standard FIDO2 prevedono l'utilizzo della crittografia a chiave pubblica e di tecnologie largamente diffuse come biometria e smartphone per raggiungere l'obbiettivo di abbattere la dipendenza dalle password.

3. Nessuna condivisione di *secret* (password) tra client e server e credenziali crittografiche univoche per ogni applicazione consentono di eliminare i rischi di *phishing* e di tutte le altre forme di attacco mirate alle password.

4. Grazie alle *passkeys* gli utenti possono accedere alle applicazioni da qualunque dispositivo in loro possesso semplicemente inserendo il PIN del *device* o tramite scansione del volto o dell'impronta, la stessa azione che compiono più volte al giorno per sbloccare il proprio dispositivo.governments, tech providers, and industry players.

Autori

Matteo Ferrario

Advanced Cybersecurity System Engineer

at NTT DATA

Santo Amendola

Senior Director

at NTT DATA

NTTDATA

NTT DATA Italia è parte della multinazionale giapponese NTT DATA, uno dei principali player a livello mondiale nell'ambito della Consulenza e dei Servizi IT. Digitale, Consulenza, Cyber Security e System Integration sono solo alcune delle principali linee di business. La nostra missione è creare valore per i nostri clienti attraverso l'innovazione. NTT DATA conta su una presenza globale in oltre 50 Paesi, più di 190.000 professionisti e una rete internazionale di centri di ricerca e sviluppo. NTT DATA è presente in Italia con oltre 6.000 dipendenti e in 11 città: Milano, Roma, Torino, Treviso, Genova, Bologna, Pisa, Napoli, Salerno, Bari e Cosenza.


NTT DATA