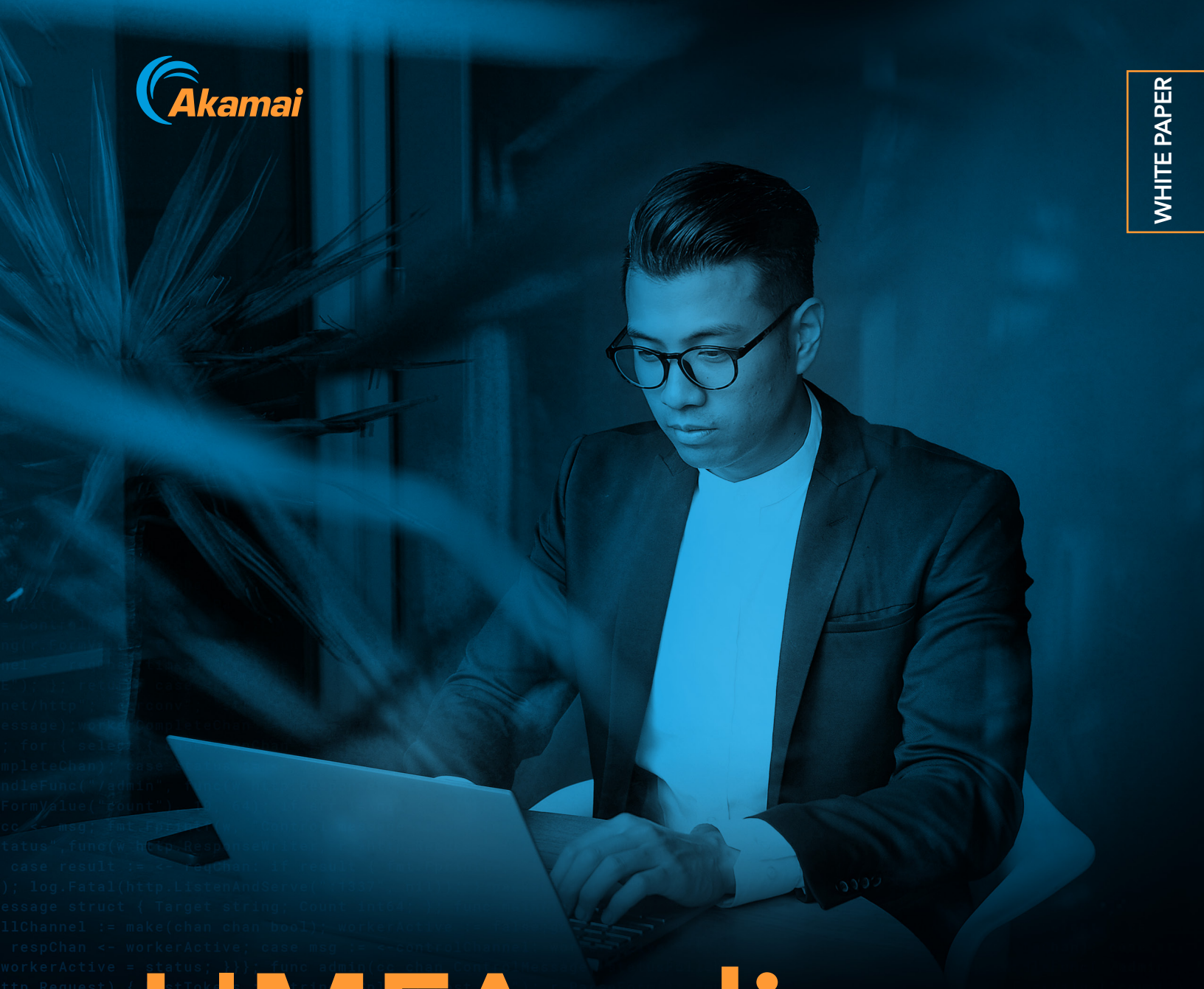
Akamai

WHITE PAPER



L'MFA odierno: una sicurezza illusoria?

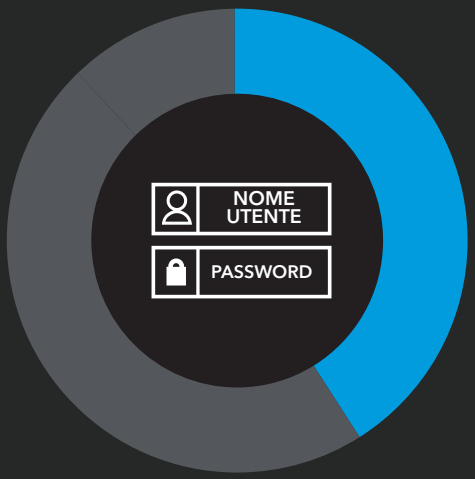
I nomi utente e le password non sono sufficienti

L'ottanta percento delle violazioni della sicurezza riguarda la compromissione di credenziali.[1] E, benché ciò sia parzialmente dovuto a una gestione fallace delle password, anche le password complesse e indecifrabili sviluppate da algoritmi possono essere problematiche.[2] Un recente controllo del dark web ha rivelato 15 miliardi di accessi rubati da 100.000 violazioni.[3]

L'imperativo della connettività digitale, la dipendenza dai servizi cloud e la realtà degli ambienti ibridi, insieme all'utilizzo delle password, rendono gli utenti vulnerabili a una miriade di vettori di attacco di autenticazione:

- **Credential stuffing**
- **Password spray e altri meccanismi di forza bruta**
- **Rilevamento locale e attività interne**
- **Phishing e social engineering**
- **Registrazione della pressione dei tasti**
- **Proxy dannosi e campagne di risposta**

Inoltre, la pandemia globale ha esacerbato questo status quo, dimostrando la necessità di un accesso sicuro indipendente dal dispositivo e dalla posizione. Se si considera che il 100% delle violazioni relative alle credenziali si verifica dopo che un utente è stato autenticato, dovrebbe essere evidente che le password non sono in grado di garantire un'autenticazione accurata.



Nonostante le vulnerabilità note, il 41% delle organizzazioni considera ancora i nomi utente e le password uno degli strumenti di gestione degli accessi più efficaci.[4]

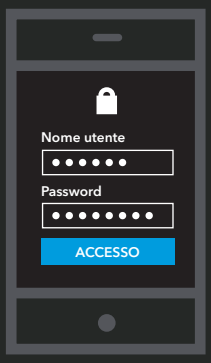
500%

Akamai ha riscontrato un aumento degli attacchi di phishing, social engineering, credential stuffing e di forza bruta. Tra marzo e maggio 2020, abbiamo assistito a un aumento di malware di quasi il 500%.

Vantaggi dell'MFA (Multi-Factor Authentication)

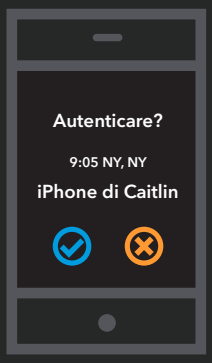
Non sorprende, quindi, che la popolarità della tecnologia MFA (Multi-Factor Authentication) sia cresciuta costantemente. In parole semplici, la tecnologia MFA protegge la vostra azienda utilizzando più di un'origine di convalida per verificare l'identità prima di concedere l'accesso.

L'MFA richiede una combinazione corretta di almeno due delle tre credenziali di autenticazione seguenti:



Un identificativo noto

Si tratta di un'autenticazione basata sulle conoscenze. Potrebbe assumere la forma di una password, un PIN, una risposta a una domanda di sicurezza o un pittogramma.



Un elemento che l'utente possiede

Si tratta di un'autenticazione basata su token, hard o soft. Potrebbe trattarsi di una smart card, un token o di una password monouso, una notifica push o di un codice SMS inviato a un dispositivo mobile.

Qualcosa che rappresenta l'utente

Si tratta di un'autenticazione contestuale o basata su biometria. Potrebbe trattarsi di un comportamento, segnali di posizione o un orario, un'impronta digitale, il riconoscimento facciale, uno schema vocale o parlato o una firma.

L'implementazione di una soluzione MFA riduce in modo significativo il rischio di accessi non autorizzati e violazioni del sistema. In effetti, le organizzazioni che utilizzano la tecnologia MFA hanno il 99,9% di probabilità in meno di subire violazioni rispetto a quelle che non la usano.[5] La tecnologia MFA consente e semplifica l'accesso sicuro a tutti gli ambienti: applicazioni cloud, on-premise, basate sul web, SaaS e IaaS. Una soluzione MFA è anche un componente fondamentale nella migrazione del sistema di sicurezza aziendale a framework come Zero Trust e SASE.

Avvalendosi della richiesta di più dati rispetto ai semplici nomi utente e password e unendo l'experience di accesso e l'integrazione con altri strumenti di sicurezza basati sul cloud, le tecnologie MFA possono anche contribuire ad aumentare l'usabilità e la produttività degli utenti. Inoltre, l'autenticazione gestita a livello centralizzato fa fronte a molti problemi e requisiti di conformità.

Ma l'MFA tradizionale non è sicura come pensate

Un servizio MFA basato su notifiche push standard può essere facilmente manipolato da un hacker per ottenere il controllo dell'account. Le odierne tecnologie MFA vi mettono a rischio, a meno che non vengano integrate con funzioni di sicurezza aggiuntive.

L'MFA è una forma di sicurezza perimetrale, ma il cloud e lo stile di lavoro odierno non hanno perimetro. L'MFA non è progettata per bloccare gli attacchi non correlati agli accessi. Protegge solo l'accesso al perimetro, quando l'utente cerca di ottenere l'accesso al sistema. I cybercriminali hanno sviluppato meccanismi di phishing e social engineering relativamente semplicistici ma altamente efficaci per aggirare questa realtà.

Considerate questo scenario:

1. **In conseguenza a una qualche forma a social engineering, un dipendente inserisce un nome utente e una password reali in un sito falso (di phishing) gestito da un autore di attacchi.**
2. **Una volta ottenute queste credenziali, l'autore di attacchi le inserisce nel vero portale di accesso.**
3. **Ciò causa l'invio di una notifica push al telefono del dipendente.**
4. **Il dipendente accetta la notifica push come normale procedura di accesso.**
5. **L'autore di attacchi ha quindi completato due forme di verifica e gli viene concesso l'accesso.**

Questa è una vulnerabilità critica della sicurezza delle notifiche push standard: qualsiasi autore di attacchi con una serie di credenziali rubate può causare l'invio di notifiche push al telefono di un dipendente. L'unico ostacolo tra una violazione della sicurezza e il normale svolgimento dell'attività è la capacità del dipendente di distinguere una notifica push legittima da uno scam. Per ottenere l'accesso, all'autore degli attacchi basta aver successo con un unico dipendente su migliaia.

MFA anti-phishing

Una soluzione MFA veramente sicura utilizza gli standard FIDO2. Al livello più basilare, ciò significa che la sicurezza viene fornita dalla tecnologia anziché dipendere dalle decisioni degli utenti.

Come funziona? Gli standard FIDO2 utilizzano una coppia di tecniche che impediscono il phishing.

Innanzitutto, la richiesta di autenticazione (la verifica MFA) viene sempre inviata alla workstation da cui ha avuto origine la richiesta di accesso. Il browser su tale workstation indirizzerà la richiesta di autenticazione a una chiave di sicurezza collegata localmente. Applicato allo scenario precedente: invece dell'invio della notifica push dal servizio MFA al telefono del dipendente generato dall'autore di attacchi, la verifica MFA torna indietro alla workstation dell'autore di attacchi. Poiché l'autore di attacchi non dispone della chiave di sicurezza del dipendente, non sarà possibile fornire alcuna risposta. Viene così evitato il controllo di un account.

Definizione: standard e specifiche di autenticazione

Fast IDentity Online (FIDO) Alliance

L'ente responsabile dello sviluppo, dell'utilizzo e della conformità agli standard per l'autenticazione.

FIDO2

Il termine generale che indica la più recente serie di specifiche di autenticazione di FIDO Alliance; gli standard inclusi nella raccolta sono CTAP1, CTAP2 e WebAuthn. FIDO2 consente agli utenti di sfruttare i dispositivi comuni per autenticarsi facilmente ai servizi online sia in ambienti mobili che desktop

WebAuthn

Uno standard web pubblicato dal World Wide Web Consortium (W3C) che è un componente fondamentale di FIDO2. L'obiettivo del progetto è standardizzare un'interfaccia per l'autenticazione degli utenti in applicazioni e servizi basati sul web utilizzando la crittografia a chiave pubblica.

Client to Authenticator Protocol (CTAP)

Una specifica sviluppata da FIDO Alliance che consente una comunicazione sicura tra un autenticatore di roaming (come uno smartphone) e un autenticatore interno: il client o la piattaforma.

In secondo luogo, il browser invia alla chiave di sicurezza i dati, oltre alla richiesta di autenticazione. Questi dati includono il nome del dominio di origine che ha inviato la richiesta di autenticazione, come visualizzato dal browser. Se l'autore dell'attacco inoltrasse semplicemente la richiesta di autenticazione ricevuta alla workstation del dipendente, questi dati conterrebbero il nome di dominio del sito di phishing. La chiave di sicurezza riconoscerebbe la mancata corrispondenza tra il nome di dominio del sito in cui è stata effettuata originariamente la registrazione e il nome di dominio che richiede l'autenticazione e si rifiuterebbe di rispondere. Di nuovo, l'attacco sarebbe contrastato.

Se una soluzione MFA più sicura e anti-phishing rappresenta una possibilità, perché non viene più ampiamente utilizzata? Perché sono necessarie chiavi di sicurezza fisiche, costose e ingombranti. O lo erano, fino ad ora.

MFA di prossima generazione sull'edge

Durante la valutazione e l'implementazione delle tecnologie MFA, i reparti IT hanno dovuto affrontare un compromesso. Per ottenere la massima sicurezza, devono spendere di più per implementare l'hardware, acquistare chiavi di sicurezza fisiche per ogni dipendente e gestire la distribuzione e l'utilizzo di tutte le chiavi. Il reparto IT deve anche convincere ogni utente ad adottare l'experience tutt'altro che ideale offerta dalle chiavi, un altro componente hardware da utilizzare e monitorare.

L'alternativa è una minore sicurezza sotto forma di comode notifiche push agli smartphone dei dipendenti che non aggiungono costi. La facilità di quest'ultimo metodo, rappresenta il motivo per il quale l'MFA con notifiche push sia oggi così ampiamente utilizzato. Ed è anche il motivo per cui così tante aziende rischiano di essere violate.

Ma non è più necessario barattare la sicurezza con i costi e la facilità di adozione.

Akamai MFA introduce un nuovo fattore di autenticazione. Digitalizza la sicurezza di FIDO2 con uno smartphone e un browser web e la combina con l'experience familiare e di facile utilizzo di una notifica push, che può essere utilizzata su qualsiasi piattaforma come autenticatore di roaming. Non sono richieste chiavi di sicurezza fisiche. La soluzione offre le funzionalità più sicure degli standard FIDO2 a basso costo, con facilità di installazione e utilizzo, nonché interoperabilità con provider di identità comuni.

Proteggete la vostra organizzazione contro gli attacchi di phishing, credential stuffing e il controllo degli account con Akamai MFA. Scoprite di più sull'esclusiva tecnologia MFA di Akamai e preparatevi per un futuro sicuro, effettivamente senza password.

Maggiori informazioni alla pagina akamai.com/mfa.

Fonti:

1. https://enterprise.verizon.com/resources/reports/dbir/
2. https://www.infosecurity-magazine.com/opinions/problem-password-everything-1/
3. https://www.forbes.com/sites/daveywinder/2020/07/08/new-dark-web-audit-reveals-15-billion-stolen-logins-from-100000-breaches-passwords-hackers-cybercrime/?sh=27fa6368180f
4. https://www.businesswire.com/news/home/20200616005047/en/Weakest-Link-Prevails-Overreliance-Passwords-Continues-Compromise
5. https://www.hipaajournal.com/multi-factor-authentication-blocks-99-9-of-automated-cyberattacks/