VALUTAZIONE

Valutazione del rischio: la sicurezza MFA (Multi-Factor Authentication)

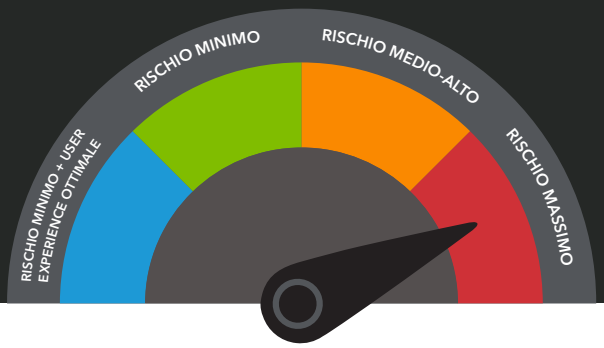
Comprendere la scala di rischio delle soluzioni di autenticazione odierne

L'80% di tutte le violazioni collegate ad attacchi informatici riguarda il furto delle credenziali utente o una scarsa gestione delle password[1] e più di 613 milioni di password sono state esposte durante violazioni di dati.[2] L'aggiunta dell'MFA (Multi-Factor Authentication) come ulteriore livello di sicurezza degli accessi riduce significativamente i rischi, tuttavia molte delle soluzioni MFA tradizionali possono comunque essere compromesse con relativa facilità.

Quanto è matura la sicurezza dell'autenticazione della vostra organizzazione? Comprendere i rischi dei modelli di autenticazione odierni:

Rischio massimo

Autenticazione tramite nome utente e password



Le organizzazioni che si affidano esclusivamente alla complessità delle credenziali per la sicurezza dell'autenticazione sono decisamente vulnerabili agli attacchi. I nomi utente e le password sono meno sicuri che mai. I dettagli di accesso vengono rubati, violati e raccolti da criminali fortemente motivati, che li usano o vendono nel dark web guadagnandoci rapidamente.

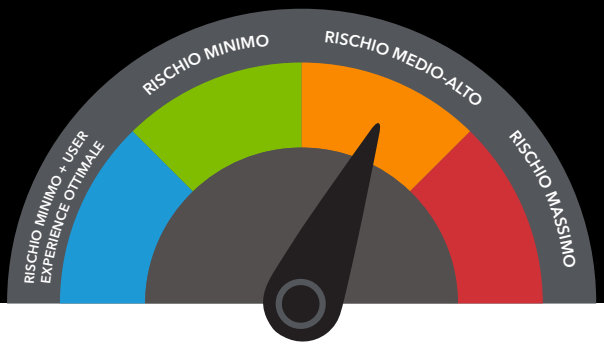
In che modo i criminali bypassano nomi utente e password:

- **Credential stuffing**
- **Phishing**
- **Password spray**
- **Forza bruta**
- **Violazione dei dati precedente/password riutilizzate**
- **Reimpostazione di password**
- **Registrazione della pressione dei tasti**
- **Rilevamento locale**

Inoltre, il fatto che gli utenti tendono a usare le stesse password su più siti mette ulteriormente a rischio la sicurezza aziendale; la vostra sicurezza dipende dalla sicurezza dell'account personale meno sicuro dei vostri utenti. Le vulnerabilità intrinseche perfino delle password più complesse e generate da algoritmo dimostrano la necessità dell'autenticazione MFA. Infine, è fortemente sconsigliato fare affidamento su un unico livello di sicurezza, in questo caso su un'autenticazione a fattore unico. La sicurezza migliore include sempre più livelli di difesa.

Rischio medio-alto

MFA (Multi-Factor Authentication) standard



L'aggiunta della funzionalità MFA al vostro stack di sicurezza dell'autenticazione migliora immediatamente la sicurezza aziendale. La funzionalità MFA, inclusa l'autenticazione a due fattori (2FA), si basa su almeno due fattori di autenticazione separati per verificare un utente. Il primo fattore è, in genere, una password. Il secondo (e possibilmente terzo) fattore può essere qualcosa che conoscete, come un PIN o una domanda di sicurezza; qualcosa che avete, come un dispositivo, un codice/password a un solo uso o un token hardware/software; oppure qualcosa che siete, inclusi i dati biometrici, come le impronte digitali e il riconoscimento facciale o segnali contestuali come la posizione.

Sebbene la funzionalità MFA tradizionale riduca enormemente il rischio rispetto all'autenticazione a fattore unico tramite nome utente/password, è comunque vulnerabile a diversi metodi per bypassare la sicurezza dell'autenticazione:

- **Phishing**
- **Uso di proxy trasparenti (attacchi MITM, Man-In-The-Middle)**
- **Intercettazione del codice di autenticazione tramite e-mail o SMS**
- **Credential stuffing**
- **Attacchi replay**
- **Scambio di SIM**
- **Social engineering**
- **Vulnerabilità nelle pagine online che gestiscono operazioni MFA**

Esistono molti esempi ben documentati di criminali che hanno bypassato l'autenticazione multifattore. Una violazione di dati di alto profilo nel 2020 è stata portata a termine usando una combinazione di social engineering e phishing per bypassare una soluzione MFA, e avrebbe potuto essere evitata con l'uso di chiavi di sicurezza fisiche.

Rischio minimo

MFA FIDO2 tramite chiave di sicurezza fisica

FIDO2 è il più robusto metodo di autenticazione basato su standard disponibile e risolve le vulnerabilità di sicurezza delle MFA tradizionali, eliminando i rischi di phishing, MITM e attacchi di replay. Lo standard FIDO2 rispetta le specifiche di autenticazione Web del World Wide Web Consortium e il corrispondente protocollo Client to Authenticator di FIDO Alliance. Questo modello di autenticazione guarda al futuro delle MFA: autenticazione tramite credenziali di accesso crittografate che non escono mai dal dispositivo dell'utente e non vengono memorizzate su un server. FIDO2 supporta anche l'eventuale evoluzione verso un'autenticazione completamente senza password.

Lo svantaggio è che l'unico modo per abilitare l'autenticazione MFA FIDO2 è quello di acquistare chiavi di sicurezza fisiche che ogni utente userà come fattore di autenticazione.

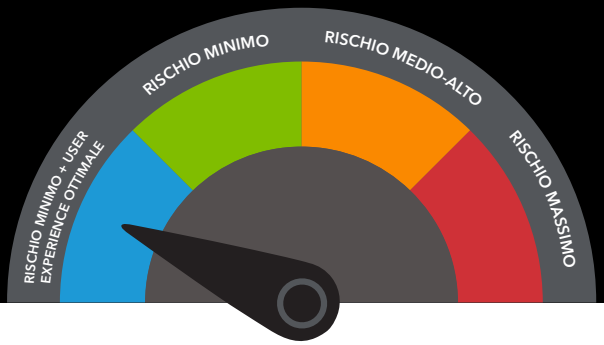
Sebbene lo standard FIDO2 sia il più sicuro in assoluto, l'implementazione tramite chiavi di sicurezza fisiche può presentare molte sfide:

- **Costo dell'acquisto e della gestione delle chiavi per ciascun utente**
- **Complessità della distribuzione e gestione delle chiavi**
- **Sostituzione delle chiavi fisiche smarrite**
- **Impossibilità di aggiornare o applicare patch alle chiavi fisiche**
- **Distribuzione non omogenea: solo alcuni dipendenti ottengono le chiavi**

L'acquisto, la configurazione, l'emissione e la gestione delle chiavi di sicurezza fisiche per tutti i dipendenti sono dispendiosi in termini di costi e tempo. Inoltre, l'obbligo per gli utenti di inserire una chiave fisica nel loro dispositivo ad ogni accesso riduce la produttività e crea un'esperienza utente laboriosa.

Rischio minimo + User experience ottimale

MFA di prossima generazione sull'edge



Akamai MFA è una soluzione FIDO2 innovativa dotata di un fattore di autenticazione a prova di phishing e protetto da crittografia. Il servizio sfrutta un'applicazione per smartphone al posto di una chiave di sicurezza fisica, risolvendo le sfide che spesso impediscono alle imprese di implementare l'autenticazione MFA FIDO2. Può essere implementato rapidamente e facilmente usando uno smartphone esistente, garantendo il più alto livello di sicurezza dell'autenticazione con una user experience ottimale. Akamai MFA elimina il rischio di phishing e supporta l'eventuale evoluzione futura di un'autenticazione senza password.

Per maggiori informazioni su Akamai MFA e per accedere a una prova gratuita di 60 giorni, visitate il sito: **akamai.com/mfa**.

Fonti:

1. https://www.infosecurity-magazine.com/blogs/pwned-passwords-business-risk/
2. https://haveibeenpwned.com/Passwords

Akamai garantisce experience digitali sicure per le più grandi aziende a livello mondiale. L'Akamai Intelligent Edge Platform permea ogni ambito, dalle aziende al cloud, permettendovi di lavorare con rapidità, efficacia e sicurezza. I migliori brand a livello globale si affidano ad Akamai per ottenere un vantaggio competitivo grazie a soluzioni agili in grado di estendere la potenza delle loro architetture multicloud. Più di ogni altra azienda, Akamai avvicina agli utenti app, experience e processi decisionali, tenendo lontani attacchi e minacce. Il portfolio Akamai di soluzioni per l'edge security, le web e mobile performance, l'accesso aziendale e la delivery di contenuti video è affiancato da un servizio clienti di assoluta qualità e da un monitoraggio 24 ore su 24, 7 giorni su 7, 365 giorni all'anno. Per scoprire perché i principali brand mondiali si affidano ad Akamai, visitate il sito www.akamai.com o blogs.akamai.com e seguite @Akamai su Twitter. Le informazioni di contatto internazionali sono disponibili all'indirizzo www.akamai.com/locations. Data di pubblicazione: 03/21.