News

Cybersecurity III – L'importanza del secondo fattore di autenticazione

La **compromissione delle password** è una minaccia significativa alla sicurezza informatica. Una password compromessa può infatti significare una possibile **violazione di dati**, un **accesso non autorizzato** ad account e informazioni sensibili, per arrivare fino al **furto di identità**. Spesso si sente parlare del furto di un account Netflix o Instagram; spesso questi non hanno particolari conseguenze ma altre volte non è così.

Rizzoli EDUCATION

News

COS'È LA PASSWORD

Possiamo dire che password è una **parola d'ordine** che in combinazione con lo username garantisce l'**autenticazione dell'utente**, ovvero il riconoscimento da parte di un sistema informatico che l'utente sia chi dice di essere. Lo username è pubblico e permette al sistema informatico di identificare l'utente; mentre la **password**, a cui lo **username** è associato univocamente, è un segreto noto solo all'utente. Costituisce quindi quello che si dice un **fattore di autenticazione di conoscenza** (knowledge), perché sfrutta qualcosa che l'utente sa per confermare la sua identità.

PERCHÉ LA PASSWORD NON È PIÙ SUFFICIENTE

Probabilmente la password è il fattore di autenticazione più vecchio tra quelli a nostra disposizione oggi e, forse anche per questo, ha molti limiti. Esistono diverse tecniche per cercare di appropriarsi di una password:

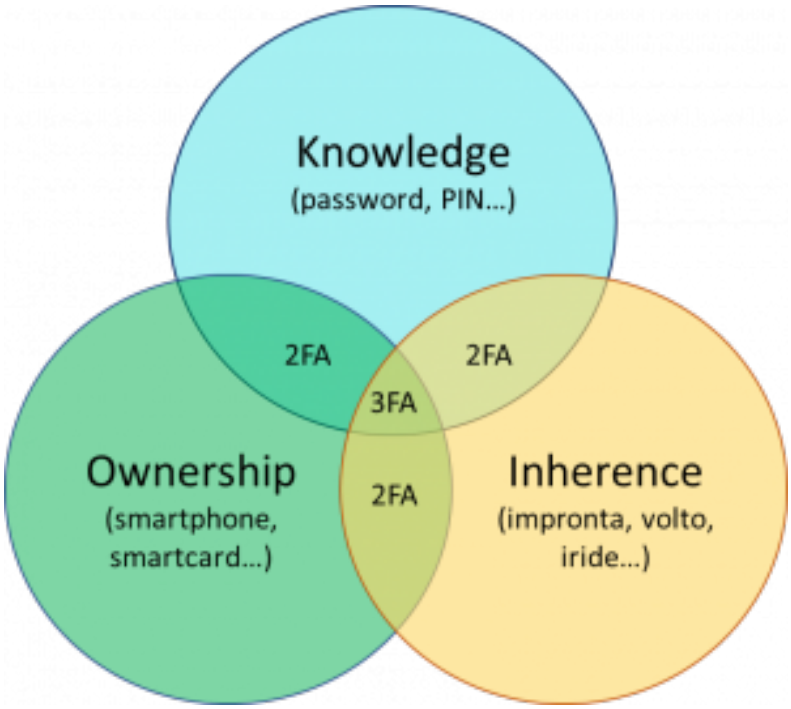
- Attacco **Brute Force**, in cui l'attaccante tenta tutte le possibili combinazioni
- Attacco a **Dizionario**, in cui l'attaccante usa liste di password comuni e combinazioni con più probabilità di essere utilizzate
- Attacco **Keylogging**, consiste nella registrazione di tutti i tasti digitati sulla tastiera

Oltre alle diverse possibilità di attacco, la più grande debolezza della password è il fattore umano: inventarsi e ricordare password complesse è un compito fastidioso, cambiarle spesso come richiedono alcuni servizi lo rende ancora più gravoso. Per queste ragioni l'utente tende ad adottare comportamenti "a rischio", come il riutilizzo della stessa password su diversi servizi (password reuse) o l'uso di informazioni legate a sé come la data di nascita o il nome.

ALTRI FATTORI DI AUTENTICAZIONE

Per difendersi e adottare un approccio più sicuro non è più sufficiente quindi irrobustire la propria password (per esempio incrementando lunghezza e complessità per rendere difficoltosi gli attacchi Brute Force e a Dizionario) ma occorre munirsi di un **secondo fattore di autenticazione**. Per ottenere quella che si definisce l'autenticazione forte (Strong Authentication) bisognerebbe adottare un secondo fattore appartenente ad una categoria diversa. Oltre ai **fattori di conoscenza** (come password, pin, o segno di sblocco nel caso degli smartphone) esistono infatti anche **fattori di proprietà** (ownership), per esempio una chiavetta di autenticazione, uno smartphone o una smartcard, e **fattori biometrici (inherence)**, come l'impronta, il volto o l'iride.

News



LE APP AUTHENTICATOR

Un modo comodo e veloce per avere un secondo fattore di autenticazione sempre a portata di mano sono le **applicazioni authenticator**, come per esempio Google Authenticator o Microsoft Authenticator. Queste applicazioni permettono di registrare i propri account, per esempio quello di gmail, Facebook o Tiktok, generalmente scansionando un QR code. Dopo aver impostato il servizio per richiedere un secondo fattore, ad ogni accesso oltre all'inserimento della password verrà richiesto un TOTP, ovvero un **codice numerico univoco** che viene rigenerato ogni 30 o 60 secondi dall'applicazione. Questo metodo è sicuro perché quando si registra il servizio tramite QR code, l'applicazione e il server che eroga il servizio si mettono d'accordo su un algoritmo di generazione in modo tale che i codici generati dall'app all'apparenza casuali vengano riconosciuti come autentici.

In certi casi queste app supportano anche l'autenticazione biometrica, e allora quando l'utente cercherà di accedere ad un servizio, riceverà anche una notifica dall'app authenticator che chiederà di sbloccare lo smartphone con l'impronta o con il volto.

APPROFONDIMENTI

L'utilizzo di più di un fattore di autenticazione rende molto più difficile agli attaccanti compromettere l'account di un utente. Se cercate informazioni sulle password compromesse o volete verificare se i vostri dati siano stati compromessi durante un data breach, un attacco informatico che ha portato alla perdita di dati, un sito molto interessante da visitare è Have I Been Pwned; qui potrete scaricare i database delle password coinvolte in attacchi informatici, potrete verificare se la vostra email o il vostro numero di telefono compaiono nei dati compromessi durante degli attacchi passati o verificare se una password fa parte delle password compromesse: provate per esempio a cercare la password "pippo", scoprirete che è comparsa oltre 44 mila volte nei data breach censiti sul sito.

News