Autenticazione

1. Introduzione
2. A un fattore - SFA
3. A più fattori - MFA
4. Cause
5. Tipologie di MFA
6. Conseguenze

1. Introduzione

- **Cos’è l’autenticazione?**

Processo di verifica dell’identità di un utente o sistema.

- **Differenza tra autenticazione e autorizzazione**

L’autenticazione conferma "chi sei", l’autorizzazione definisce "cosa puoi fare".

- **Perché è importante proteggere gli accessi?**

Per prevenire accessi non autorizzati e proteggere dati sensibili.

2. Autenticazione a un solo fattore (SFA)

- **Esempi: password, PIN**

Metodi comuni ma vulnerabili perché basati su informazioni memorizzabili.

- **Vulnerabilità delle sole password**

Facili da rubare, spesso deboli o riutilizzate.

- **Tecniche di attacco: phishing, brute-force, credential stuffing**

Modi in cui gli hacker rubano credenziali.

3. Autenticazione a più fattori (MFA)

- **Definizione e funzionamento**

Uso di più elementi per verificare l'identità dell'utente.

- **I tre principali fattori di autenticazione:**
  - **Qualcosa che sai** → Password o PIN.
  - **Qualcosa che hai** → Smartphone, token fisico o smart card.
  - **Qualcosa che sei** → Impronta digitale, volto, retina.
- **Differenza tra MFA e 2FA**

MFA usa almeno due fattori distinti, mentre 2FA ne usa esattamente due.

4. Cause dell'adozione della MFA

- **Aumento degli attacchi informatici**

Crescita del cybercrime rende MFA necessario.

- **Vulnerabilità delle credenziali statiche**

Le password da sole non bastano più.

- **Necessità di protezione per dati sensibili e accessi critici**

MFA riduce il rischio di furti di dati.

- **Normative di sicurezza (es. GDPR, PSD2 per i pagamenti online)**

Obbligo legale di adottare misure di protezione.

5. Conseguenze dell'MFA

Vantaggi:

- **Maggiore sicurezza degli account**

Riduce il rischio di accessi non autorizzati.

- **Riduzione del rischio di attacchi**

Protezione da phishing e furto di credenziali.

- **Conformità alle normative**

Aziende e governi lo richiedono sempre più spesso.

Svantaggi:

- **Maggiore complessità per gli utenti**

Richiede un passaggio aggiuntivo per accedere.

- **Possibile indisponibilità del secondo fattore**

Problemi se si perde il telefono o il token.

- **Rischio di attacchi sofisticati come SIM swap**

Hacker possono prendere il controllo del secondo fattore.