VERIFICA DELL'IDENTITÀ
PER ACCESSI PIÙ SICURI

MULTIFACTOR AUTHENTICATION

Datasheet

Le aziende del Gruppo MEET IT

Via di Corticella, 89/2
40128 Bologna BO

+39 05 14070383
www.3cime.com | info@3cime.com

Viale Alcide De Gasperi, 37
33100 Udine UD

+39 0432 524001
info@ntonline.it | www.ntonline.it

PROTEGGI. IDENTIFICA. ACCEDI.

Password forti e conservate al sicuro non sono più sufficienti. Per proteggere i tuoi accessi, utilizza l'Autenticazione Multifattoriale, in modo da essere protetto anche in caso di un furto di password.

Secondo il *"Point of Entry: Why Hackers Target Stolen Credentials, BleepingComputer" del 6 agosto 2024*:
"Il furto di credenziali è una preoccupazione crescente, con gli attaccanti che utilizzano sempre più metodi come phishing e attacchi di forza bruta per acquisire le credenziali. Nel 2023, è stato il metodo più comune per ottenere accesso iniziale negli attacchi, superando persino i ransomware."

L'autenticazione multifattoriale (*Multi-Factor Authentication - MFA*) è un **metodo di verifica digitale dell'identità dell'utente che utilizza almeno due fattori di riconoscimento** per garantire l'accesso esclusivamente alle persone autorizzate. Questa tecnologia **protegge risorse** come servizi, infrastrutture ICT, spazi online e reti, **riducendo significativamente il rischio di attacchi esterni, violazioni della sicurezza interna e problemi di conformità**.

Il servizio utilizza un **messaggio push, un QR code, una password monouso (OTP) o un token** come fattori per il riconoscimento dell'identità, da inserire a seguito delle proprie credenziali di accesso. L'app informa l'utente di ogni tentativo di accesso, chiedendo se si desidera accettarlo o bloccarlo dal dispositivo prescelto per l'autenticazione.

Il metodo multifattoriale è ideale per proteggere l'accesso a **reti, VPN, servizi web, sistemi operativi, infrastrutture virtuali, applicazioni e cloud**, in modo da ridurre la probabilità di interruzioni della rete e le violazioni dei dati.

COME VIENE VERIFICATA L'IDENTITÀ?

Qualcosa che sai (password)

Qualcosa che hai (token su smartphone o token hardware programmabile)

Qualcosa che hai (DNA smartphone) per impedire l'utilizzo ai dispositivi clonati

Oppure, qualcosa che sei (impronte digitali)

VISITA IL SITO *MEETIT.CLOUD*

SOLUZIONI AVANZATE

L'autenticazione multifattoriale (MFA) rappresenta il metodo più efficace per proteggere gli accessi aziendali. Eppure la sicurezza non si ferma più alle sole password: è necessario adottare soluzioni avanzate che garantiscano protezione anche in caso di credenziali compromesse.

Requisito: integrazione con **Active Directory in ambiente Microsoft Windows**

MFA On-Premise per Active Directory

Abilitare l'autenticazione personalizzata a più fattori con **applicazioni di autenticazione** o **token hardware programmabili** per l'accesso a Windows, Desktop remoto, IIS, VPN e applicazioni cloud.

Iscrizione singola

Consentire l'accesso sicuro e senza attriti a Microsoft 365 e altre applicazioni cloud leader, da qualsiasi luogo utilizzando le **credenziali Active Directory esistenti.**

Restrizioni di accesso contestuali

Impostare **restrizioni di accesso personalizzate** per utente, gruppo o unità organizzativa, utilizzando le informazioni contestuali relative all'accesso di un utente, per verificare l'identità dichiarata da tutti gli utenti e autorizzare, negare o limitare l'accesso alla rete.

Tutti i tentativi di accesso che non soddisfano queste condizioni vengono **bloccati**.

Gestione delle sessioni e auditing dettagliato

Strumenti di **monitoraggio real time** e di rilevamento dei rischi che segnalano immediatamente le attività di accesso sospette. Un audit centralizzato fornisce rapporti dettagliati per supportare le indagini forensi e dimostrare la conformità alle normative.

VISITA IL SITO *MEETIT.CLOUD*

FOCUS ON

Password rubate nel DarkWeb

Il DarkWeb è una raccolta di siti web anonimi e pubblicamente disponibili che nascondono gli indirizzi IP in modo che gli utenti non possano identificarne l'host.

In questo contesto accade che **informazioni sensibili e password siano pubblicate illecitamente**, rese disponibili e vendute, a seguito di violazioni andate a buon fine.

L'Autenticazione Multifattoriale per i login evita che le password rubate siano utilizzabili dai non addetti ai lavori.

VANTAGGI

- Massimi livelli di **sicurezza informatica** enterprise
- **Protezione degli accessi** di tutti gli utenti aziendali
- **Conformità a GDPR** e policy interne
- Ottima **user experience**
- **Semplicità**
- **Scalabilità**
- **Flessibilità**
- **Gestione centralizzata**
- **Integrabilità** con altri servizi
- **Supporto** dedicato
- **Costi molto contenuti**
- **Affidabilità**
- **Mobilità**
- Disponibile **Online/Offline**
- **Non richiede hardware** aggiuntivo
- **Tecnologia non distruttiva**
- **Implementazione rapida**

VISITA IL SITO *MEETIT.CLOUD*