CONFINDUSTRIA
VENETO EST
Area Metropolitana
Venezia Padova Rovigo Treviso

Appuntamenti con l'InnovAzione 2025

Protezione e gestione delle identità privilegiate

Igor Lazzarin - Henko

29 Settembre 2025

La chiave universale

Le utente privilegiate sono come il passpartout, chi ce l'ha può accedere ovunque e fare qualsiasi cosa, spesso potendo anche cancellare le tracce dell'operato.

Fortunatamente c'è una sola chiave e viene affidata solo a personale di fiducia, competente, formato, e che non sbaglia mai… o no?

I problemi delle chiavi universali

Nel mondo reale queste chiavi:

- Non esistono quasi mai in unica copia
- Possono essere facilmente condivise
- Possono essere rubate o copiate
- L’operato di chi le usa è difficilmente tracciabile
- Sono spesso troppo potenti rispetto all’attività da svolgere

Identità privilegiate

In ambito IT gli utenti con privilegi amministrativi sono i possessori dei passpartout e ne hanno assoluto bisogno per:

- Svolgere attività di manutenzione, supporto e modifica delle configurazioni
- Accedere i dati (es. backup) senza restrizioni
- Gestire la sicurezza del sistema

Violazioni di sicurezza

- 81% delle violazioni utilizza password rubate o troppo deboli
- 54% delle aziende memorizza le password amministrative in Excel o Word
- 59% degli account amministrativi sono assegnati a terze parti esterne alle aziende
- Il 52% delle aziende non sa a chi siano gli effettivi utilizzatori delle credenziali amministrative

Sicurezza delle identità privilegiate

I sistemi di protezione delle identità privilegiate e delle loro credenziali sono molteplici, la loro efficacia non sempre certa.

- Procedure e formazione
- Limitazione degli account amministrativi
- Complessità credenziali
- MFA
- Utilizzo password manager
- Rotazione periodica delle password
- Controllo del riutilizzo
- Auditing dei gruppi di sicurezza
- AV / EDR
- Monitoring Dark web
- Jump box
- Airgapping
- Firewall
- ….

PAM

Il Privileged Access Management è un sistema che permette di:

- Concedere accesso just-in-time alle risorse critiche
- Minimizzare i diritti amministrativi degli utenti
- Monitorare le sessioni con privilegi per supportare gli audit
- Analizzare le attività eseguite con privilegi inusuali
- Creare report sull'accesso e le attività degli utenti con privilegi

L’amministrazione Just in Time

L’arma sicuramente più efficace nel controllo delle identità privilegiate è il Just in time, ovvero la creazione di una identità temporanea all’inizio di una azione amministrativa e la sua automatica disabilitazione ed eliminazione al suo completamento.

Questo permette di limitare l’esposizione al minimo:

- Vengono assegnati i diritti minimi per l’operazione
- L’utente amministratore viene elevato solo a richiesta
- Non rimangono credenziali attive non controllate
- Eventuali leak non impattano sulla sicurezza dell’azienda
- Cache locali non permettono di elevare l’accesso in seguito

Governance e Conformità

La direttiva NIS2 nella sezione per l'igiene informatica impone:

- Gestione degli account amministrativi
- Autenticazione continua
- Controllo degli accessi dei fornitori
- Minimizzazione accessi

Cosa possono fare le aziende?

Gli imprenditori cosa possono fare? Insieme ai fornitori che li seguono possono:

a. Identificare gli asset e il loro ruolo nella rete
b. Stilare una lista degli amministratori interni ed esterni identificandone i ruoli e i permessi per asset, e mantenerla aggiornata
c. Passare l'autenticazione amministrativa da condivisa a personale
d. Attivare l'autenticazione MFA sui sistemi critici
e. Attivare il Just in Time per tutti gli amministratori con profili minimizzati di accesso
f. Attivare la registrazione delle sessioni amministrative
g. Eliminare gli account amministratori locali
h. Attivare un sistema di auto elevazione per gli utenti finali
i. Eseguire audit delle anomalie

Per informazioni:
ricercainnovazione@confindustriavenest.it

Grazie per l’attenzione.