CONFINDUSTRIA
VENETO EST
Area Metropolitana
Venezia Padova Rovigo Treviso

Appuntamenti con l'InnovAzione 2025

Identità sotto attacco: come proteggerle con l'ITDR e un SOC sempre vigile

Paolo Bain - Henko

14 luglio 2025

Entrare nelle aziende cambiando identità

Se ho una banca molto sicura, e se un ladro si traveste da direttore, con i suoi vestiti, con il suoi lineamenti e con i suoi documenti.

Tutto perfettamente uguale all'originale.

Riuscirà ad entrare?

Cos'è l'identità digitale e perché è il "nuovo perimetro"

Le aziende si dotano di sistemi per evitare che possano essere effettuati attacchi alle reti e ai sistemi.

Ma alcuni utenti aziendali hanno la possibilità di accedere. Usando vpn, desktop remoti, o semplicemente la loro email.

L’identità digitale quindi è rappresentata da credenziali e sistemi di accesso che permettono di identificare gli utenti che possono accedere ai sistemi e quelli che invece non possono.

Introduzione a ITDR – Identity Threat Detection and Response

Se c’è un furto di identità digitale come posso difendermi?

Posso dotarmi di strumenti che rilevino comportamenti non consueti dell’utente e che possano:

- Riconoscere comportamenti anomali legati alle identità (es. login in orari strani o da Paesi inusuali).
- Bloccare attività sospette in tempo reale.
- Reagire subito a escalation di privilegi non giustificati.

Microsoft Office 365 come scelta primaria per il furto di identità digitale

E’ uno strumento diffusissimo.

Contiene dati e comunicazioni importanti per aziende

Permette nativamente il collegamento da remoto

Gli utenti possono avere accessi in AD, Sharepoint, Crm, e altri prodotti Microsoft o altri sistemi compatibili

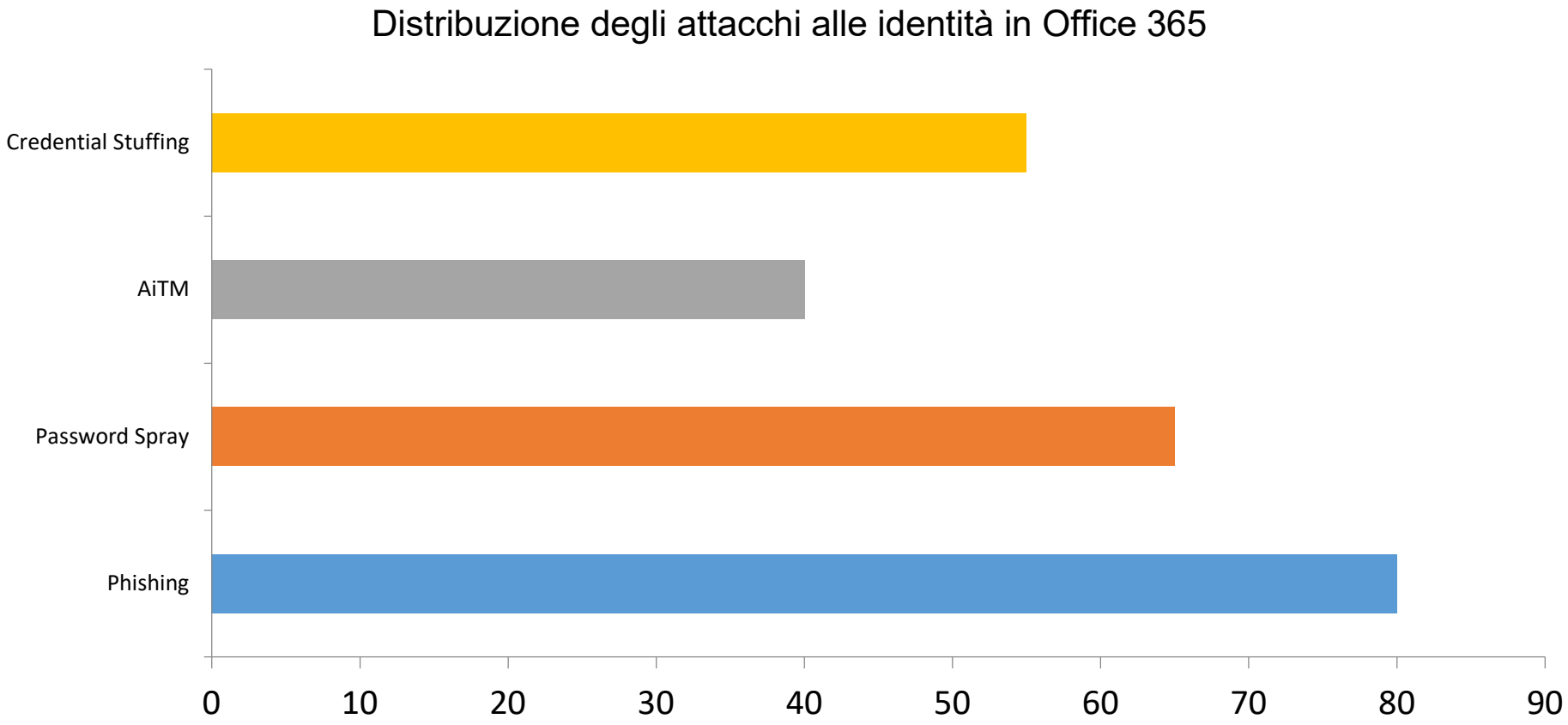
Spesso è configurato con livelli di sicurezza «migliorabili»

I Dati di Microsoft sugli attacchi su 365

- 600 milioni di attacchi alle identità al giorno rilevati da Microsoft.
- Oltre il 99% degli attacchi basati su password: brute-force, spray, phishing.
- 7.000 attacchi alle password al secondo bloccati da Microsoft Entra.
- Solo il 41% delle aziende usa MFA.
- Crescita degli attacchi AiTM che bypassano la MFA

Tipi di attacco

- Phishing mirato: email che imitano notifiche di login.
- Password spray: uso di password comuni su molti account.
- Credential stuffing: uso di credenziali rubate da altri servizi.
- Adversary-in-the-Middle (AiTM): intercettazione delle sessioni di autenticazione.


Distribuzione degli attacchi alle identità in Office 365
Credential Stuffing
AiTM
Password Spray
Phishing
0
10
20
30
40
50
60
70
80
90

La minaccia dell'IA nel phishing

L'accesso da parte di algoritmi che utilizzano l'intelligenza artificiale a email, contatti, discussioni permette di creare email praticamente perfette indirizzate alle persone giuste in azienda e assolutamente credibili, aumentando a dismisura la possibilità che gli utenti vengano ingannati.

Gli attaccanti non dormono mai

Molto spesso gli attacchi hacker vengono svolti nei momenti di minor sorveglianza dei sistemi, durante i weekend e di notte.

Per questo motivo spesso gli ITDR sono spesso accompagnati da un servizio SOC (Security Operation Center) che monitora costantemente i report che arrivano dal sistema ITDR e in caso di necessità può intervenire.

Cosa possono fare le aziende?

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

1) Mappare dove sono i dati e quali utenti possono accederci
2) Stilare una lista degli utenti e di cosa possono fare diminuendo al minimo i permessi.
3) Attivare MFA su Office 365 e su qualsiasi sistema di collegamento remoto
4) Controllare la lista degli utenti rimuovendo quelli vecchi e non utilizzati.
5) Fare formazione ai propri dipendenti sull'utilizzo corretto e sicuro degli strumenti aziendali come le email.
6) Chiedere di inserire un ITDR e/o servizi SOC nella propria infrastruttura.

Cosa possono fare le aziende?

Formazione interna per tutti i dipendenti:

- Sul corretto utilizzo delle password (che devono essere complesse e avere la scadenza)
- Sui ruoli corretti degli utenti (evitando gli amministratori)
- Fare formazione ai propri dipendenti sull'utilizzo corretto e sicuro degli strumenti aziendali come le email e altri strumenti.

Grazie per l’attenzione !

Paolo Bain
Henko srl
www.henko.it