Microsoft mette al bando le password “deboli”

Apr 03, 2019 Marco Schiaffino Gestione dati, In evidenza, News, RSS, Scenario, Tecnologia 0

Con Azure AD Password Protection gli amministratori possono impedire agli utenti di impostare le password di uso comune. L’elenco è aggiornato automaticamente.

La mossa decisiva per contrastare l’uso di password comuni e facilmente individuabili? Questa volta potrebbe averla azzeccata **Microsoft**.

L’azienda di **Satya Nadella** ha infatti annunciato la disponibilità di **Azure AD Password Protection**, un sistema che permette agli amministratori di rete di limitare la scelta delle password.

L’idea è quella di arginare il fenomeno del **password spraying**, cioè la tecnica che i pirati usano per eseguire attacchi di brute forcing contro gli account aziendali utilizzando database con le password più comuni.

Il password spraying funziona come un brute forcing al contrario: al posto di provare tutte le possibili password su un singolo account, i cyber-criminali tentano l’accesso con la stessa password su tutti gli account che individuano.

Questa modalità di attacco (ne abbiamo parlato in questo articolo) “distribuisce” i tentativi di accesso ed è molto difficile da individuare rispetto a un attacco portato con le modalità classiche. **Gli accessi falliti, infatti, non hanno una frequenza tale da allertare i sistemi di controllo**.

I pirati, di solito, per portare questi attacchi usano i database disponibili sul Web che contengono gli elenchi di password sottratte ai servizi online, come il mastodontico **Collection#1**, individuato lo scorso gennaio su Internet.

Azure AD Password Protection utilizza in pratica la stessa fonte per creare una black list di password che gli utenti non possono utilizzare all'interno della rete. Quando un utente prova a impostare una password considerata debole, viene visualizzato un messaggio che gli chiede di utilizzarne un'altra.

Come viene spiegato nella documentazione relativa (purtroppo il sito traduce automaticamente i contenuti con risultati drammatici, consigliamo la versione in inglese) la black list viene generata partendo dalle 500 password di uso più comune e le possibili varianti. **Nel complesso, si arriva a un milione di password "bandite" dai sistemi**.

Il database, poi, viene aggiornato automaticamente da Microsoft attraverso le risorse reperite attraverso i sistemi di intelligence che eseguono un costante monitoraggio delle password rubate in circolazione.

Rispetto alle solite policy, che controllano solo lunghezza della password e presenza di maiuscole/minuscole, caratteri speciali e numeri, con Azure AD Password Protection si passa certamente a un altro livello. Quanto sarà efficace, però, lo scopriremo solo nel prossimo futuro.

Please follow and like us:

Il backup si sposta verso il cloud

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/04/03/microsoft-mette-al-bando-le-password-deboli/