SCRIPT #05 · MICROSOFT 365

Accessi da paesi non abituali

Analizza i log di accesso ed evidenzia connessioni da paesi non presenti in una whitelist definita.

AUTORE	COPYRIGHT	PREREQUISITI
Francesco Larossa	© 2026 SysAdmin Italia	Modulo Microsoft.Graph, permessi AuditLog.Read.All

Cosa fa questo script

Lo script recupera i log di accesso delle ultime N ore da Microsoft Graph e li confronta con un elenco di paesi attesi (dove l'azienda opera normalmente), segnalando ogni accesso riuscito proveniente da un paese non incluso in quella lista.

Come si usa

Definisci l'elenco dei paesi attesi (codici ISO a due lettere) e il numero di ore da analizzare.

```
.\Report-AccessiPaesiInsoliti.ps1 -PaesiAttesi @("IT","DE","FR") -OreIndietro 24
```

In quale contesto usarlo

Un accesso riuscito da un paese mai visto prima, specialmente se distante geograficamente da un accesso recente dello stesso utente, e uno dei segnali piu affidabili di un account compromesso, ed e tra i controlli che l'accesso condizionato di Entra ID puo automatizzare, ma che vale la pena verificare anche manualmente in ambienti senza licenze Entra ID P1/P2.

Codice completo

Il codice è lo stesso del file Report-AccessiPaesiInsoliti.ps1: per usarlo scarica il file dalla pagina invece di copiarlo da questo PDF.

```
<#
.SYNOPSIS
    Analizza i log di accesso ed evidenzia connessioni da paesi non abituali.
#>
param(
    [string[]]$PaesiAttesi = @("IT"),
    [int]$OreIndietro = 24,
    [string]$PercorsoCSV = "C:\Report\AccessiInsoliti.csv"
)

Import-Module Microsoft.Graph.Reports
Connect-MgGraph -Scopes "AuditLog.Read.All" -NoWelcome

$dataLimite = (Get-Date).AddHours(-$OreIndietro).ToString("yyyy-MM-ddTHH:mm:ssZ")

$accessi = Get-MgAuditLogSignIn -Filter "createdDateTime ge $dataLimite and status/errorCode eq 0" -All

$risultati = $accessi | Where-Object { $_.Location.CountryOrRegion -notin $PaesiAttesi } |
```

```
    Select-Object @{N="Utente";E={$_.UserPrincipalName}},
    @{N="Paese";E={$_.Location.CountryOrRegion}},
    @{N="Citta";E={$_.Location.City}},
    @{N="IP";E={$_.IPAddress}},
    @{N="Orario";E={$_.CreatedDateTime}}

$risultati | Export-Csv -Path $PercorsoCSV -NoTypeInformation -Encoding UTF8 -Delimiter ";"
Write-Host "Trovati $($risultati.Count) accessi da paesi non attesi nelle ultime $OreIndietro ore." `
    -ForegroundColor $(if($risultati.Count -gt 0){"Red"}else{"Green"})
```