SCRIPT #04 · MICROSOFT 365

Regole di inoltro email sospette

Individua regole di inoltro automatico verso indirizzi esterni al dominio aziendale.

AUTORE	COPYRIGHT	PREREQUISITI
Francesco Larossa	© 2026 SysAdmin Italia	Modulo ExchangeOnlineManagement

Cosa fa questo script

Lo script controlla ogni mailbox alla ricerca di regole di inoltro (sia a livello di mailbox che di singola regola cliente) che puntano verso un indirizzo email esterno al dominio aziendale, un pattern tipico dopo la compromissione di un account.

Come si usa

Esegui lo script indicando il tuo dominio principale, cosi da distinguere gli inoltri interni (normali) da quelli esterni (sospetti).

```
.\Report-RegoleInoltroSospette.ps1 -DominioAziendale "azienda.it"
```

In quale contesto usarlo

L'inoltro silenzioso della posta verso un indirizzo esterno e una delle tecniche piu usate dagli attaccanti dopo aver compromesso un account, per continuare a leggere email sensibili (fatture, comunicazioni finanziarie) anche dopo che la vittima ha cambiato la password. Un controllo periodico su questo fronte e essenziale.

Codice completo

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

```
<#
.SYNOPSIS
    Individua regole di inoltro automatico verso indirizzi esterni al dominio aziendale.
#>
param(
    [Parameter(Mandatory=$true)]
    [string]$DominioAziendale,
    [string]$PercorsoCSV = "C:\Report\InoltriSospetti.csv"
)

Import-Module ExchangeOnlineManagement
Connect-ExchangeOnline -ShowBanner:$false

$mailbox = Get-Mailbox -ResultSize Unlimited

$risultati = @()

foreach ($mb in $mailbox) {
```

```
    if ($mb.ForwardingSmtpAddress -and $mb.ForwardingSmtpAddress -notlike "*@$DominioAziendale*") {
        $risultati += [PSCustomObject]@{
            Utente = $mb.UserPrincipalName
            Tipo   = "Inoltro mailbox"
            Destinazione = $mb.ForwardingSmtpAddress
        }
    }

    $regole = Get-InboxRule -Mailbox $mb.UserPrincipalName -ErrorAction SilentlyContinue |
        Where-Object { $_.ForwardTo -or $_.RedirectTo }

    foreach ($r in $regole) {
        $destinazioni = @($r.ForwardTo) + @($r.RedirectTo) | Where-Object { $_ -and $_ -notlike "*$DominioAziendale*" }
        foreach ($d in $destinazioni) {
            $risultati += [PSCustomObject]@{
                Utente = $mb.UserPrincipalName
                Tipo   = "Regola: $($r.Name)"
                Destinazione = $d
            }
        }
    }
}

$risultati | Export-Csv -Path $PercorsoCSV -NoTypeInformation -Encoding UTF8 -Delimiter ";"
Write-Host "Trovate $($risultati.Count) regole di inoltro verso l'esterno." -ForegroundColor $(if($risultati.Count `
    -gt 0){"Red"}else{"Green"})
Disconnect-ExchangeOnline -Confirm:$false
```