Change MFA Phone via Graph API

This automation sets the primary mobile number as MFA method according to a UPN. This can be used, for example, if from an internal store or user interface (e.g. ServiceNow) the users should automatically set the MFA method a first time. For example, this code can be placed in an Azure Runbook or Azure Function and executed via a trigger.

Requirements

To execute this code you need to create an App Registration and add the Permissions "UserAuthenticationMethod.ReadWrite.All". How you can create an App Registration and how you get the variables "TenantId", "ClientId" and "ClientSecret" with the according values, you can view this manual: Get app details and gr... | LNC DOCS (lucanoahcaprez.ch)

PowerShell Code

This code must be filled with the correct variables for everything to work. On the one hand it needs the standard variables for the Graph Authentication: "$TenantID", "$ClientID", "$Clientsecret". And on the other hand the variables "$Email" and "$PhoneNumber" are used to locate the user to whom the mobile number should be set as MFA method.

```
$Email = "<youremail>"
$PhoneNumber = "<yourphonenumber>"

# Filter empty spaces
if($PhoneNumber.contains(" ")){
$PhoneNumber = $PhoneNumber.replace(" ","")
}

$TenantId = "<yourtenantid>"
$ClientId = "<yourappregistrationid>"
$ClientSecret = "<yourclientsecret>"

$Body = @{
```

```
"tenant" = $TenantId
"client_id" = $ClientId
"scope" = "https://graph.microsoft.com/.default"
"client_secret" = $ClientSecret
"grant_type" = "client_credentials"
}

$Params = @{
"Uri" = "https://login.microsoftonline.com/$TenantId/oauth2/v2.0/token"
"Method" = "Post"
"Body" = $Body
"ContentType" = "application/x-www-form-urlencoded"
}

$AuthResponse = Invoke-RestMethod @Params

$Headers = @{
   "Authorization" = "Bearer $($AuthResponse.access_token)"
}



# Get User ID By UPN
$UsersResponse = Invoke-RestMethod -Method GET -Uri "https://graph.microsoft.com/v1.0/users/$email" -
ContentType "Application/Json" -Headers $Headers
$UserId = $UsersResponse.id

# Change Phone Number for MFA

$PhoneMethod = @"
{
   "phoneNumber":"$PhoneNumber",
   "phoneType":"mobile"
}
"@
$MFAResponse = Invoke-RestMethod -Method PUT -Uri
"https://graph.microsoft.com/beta/users/$UserId/authentication/phoneMethods/3179e48a-750b-4051-897c-
87b9720928f7" -ContentType "Application/Json" -Body $PhoneMethod -Headers $Headers

Start-Sleep 30
```

```
# Compare Phone Numbers

$MFAMethod = Invoke-RestMethod -Method GET -Uri
"https://graph.microsoft.com/beta/users/$UserId/authentication/phoneMethods" -ContentType "Application/Json"
-Headers $Headers

$AzurePhoneNumber = $MFAMethod.value.phoneNumber.Replace(" ","")

if($AzurePhoneNumber -eq $PhoneNumber){
   Write-Output "success"
}else{
   Write-Output "Failed to compare Azure Phone Number to Input from SNOW."
}
```

Revision #2
Created 24 May 2023 08:08:12
Updated 21 July 2024 15:11:16