Securing Active Directory: Who can add computers to the domain? Only the domain admin?

https://sid-500.com/2017/09/09/securing-active-directory-who-can-add-computers-to-the-domain-only-the-domain-admin-are-you-sure/

“Only Domain administrators can add computers to the domain.” I can’t count how often I have heared these words. But when installing a new domain, a counter is configured and this counter allows each domain user to add up to 10 computers to the domain. This is the default setting. The setting can be changed and must be considered in the IT security concept.

The ms-DS-MachineAccountQuota

The setting can be found in dsa.msc (enable advanced features!) Open dsa.msc (Active Directory Users and Computers). If not already enabled, enable Advanced Features. Next open the properties of your domain (right click), click on Attribute editor and navigate to the Attribut ms-DS-MachineAccountQuota. Are you surprised? Every user (Domain User) can add up to 10 Computers.

Unbenannt.PNG
Image not found or type unknown

1.PNG
Image not found or type unknown

Or run a simple One-Liner in PowerShell. Don’t care about the domain name. We call it from Get-ADDomain.

```
Get-ADObject ((Get-ADDomain).distinguishedname) -Properties ms-DS-MachineAccountQuota
```

Unbenannt.PNG
Image not found or type unknown

Who added client01 to the domain?

Who has added client01 to the domain? Petra is a domain user and added client01 to the domain. We can see it by running a simple one-liner. Ok, I have to admit it’s a three liner. We examine the ms-DS-CreatorSID attribute of the computer account.

```
Get-ADComputer client01 -Properties mS-DS-CreatorSID | Select-Object -Expandpropert
y mS-DS-CreatorSID | Select-Object -ExpandProperty Value | Foreach-Object {Get-ADUser -Filt
er {SID -eq $_}}
```

Unbenannt.PNG
Image not found or type unknown

Changing the default value

A value of 0 means that domain users are are not allowed to add computer accounts.

Open the properties of the domain and double click ms-DS-MachineAccountQuota. Modify the value. The number represents the number of computers that you want users to be able to add to the domain. I recommend changing it to 0.

Unbenannt.PNG
Image not found or type unknown

Or use PowerShell. Again: Don’t worry about the domain name. It will be filled in automatically.

```
Set-ADDomain (Get-ADDomain).distinguishedname -Replace @{"ms-ds-MachineAccountQuota"="0"}
```

Unbenannt.PNG
Image not found or type unknown

The impact

The user is informed that the maximum number has been reached. The following error occured attempting to join the computer to the domain:

Unbenannt.JPG
Image not found or type unknown

Revision #1
Created 5 January 2024 05:02:59 by ColtM
Updated 7 August 2024 23:24:39 by ColtM