Let’s split it, baby!

“Gott-Modus” abschaffen, Sicherheit erhöhen?

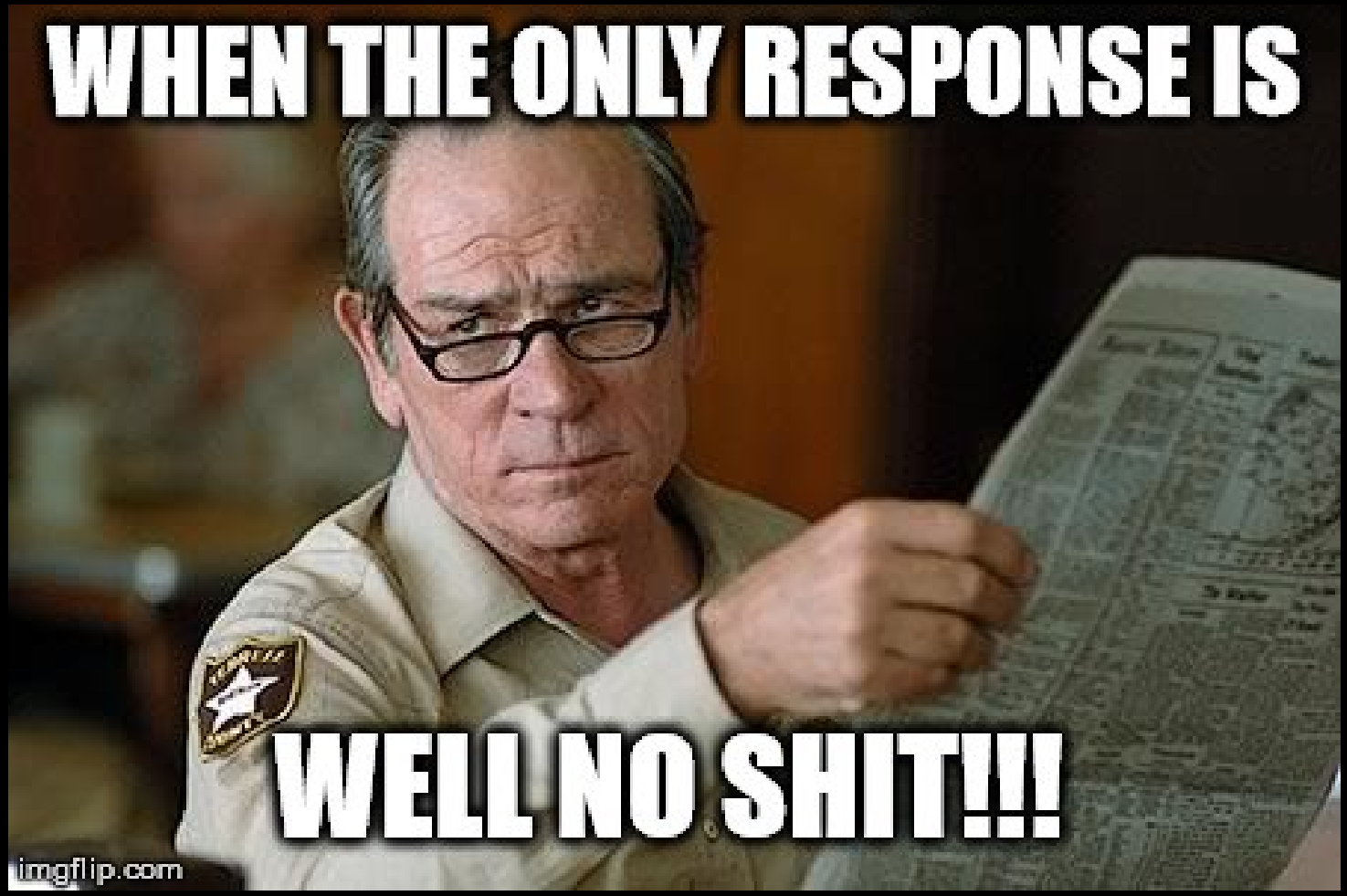
Das Problem…

…oder: Die Geister, die ich rief ;-)

- **CVE-2019-0724:**
  In Microsoft Exchange Server besteht eine Sicherheitsanfälligkeit bezüglich Rechteerweiterungen. Ein Angreifer, der diese Sicherheitsanfälligkeit erfolgreich ausnutzt, kann die gleichen Rechte wie ein Domänenadministrator erlangen.

Das Problem...

...oder: Die Geister, die ich rief ;-)



Die Ursache…

…oder zumindest eine von vielen ;-)

- Im Gegensatz zu vielen anderen Server-Applikationen verwendet Exchange keine Service-Accounts…
- …sondern agiert mit der Identität der Exchange Server.
- Für eine Web-Applikation macht das vieles einfacher ☺

- Es ist klar, dass die Maschinen dafür ein paar Rechte kriegen mussten…
- …ob alle davon wirklich benötigt wurden, wurde allerdings nicht ernsthaft hinterfragt.
- **Bis Januar 2019.**

Die Antwort…

…ist wie immer „it depends“

- **Split Permissions** → Der Gruppe „Exchange Windows Permissions“ werden Rechte entzogen.
  Achtung! NICHT „Exchange Trusted Subsystem“!
- Das Default-Modell: **Shared Permissions**

- Nicht zu verwechseln:
  - **Split Permissions** → Exchange-Server haben weniger Rechte im AD
  - **RBAC Split Permissions** → Exchange Server haben die gleichen Rechte

Split Permissions implementieren…

…ist ganz einfach!

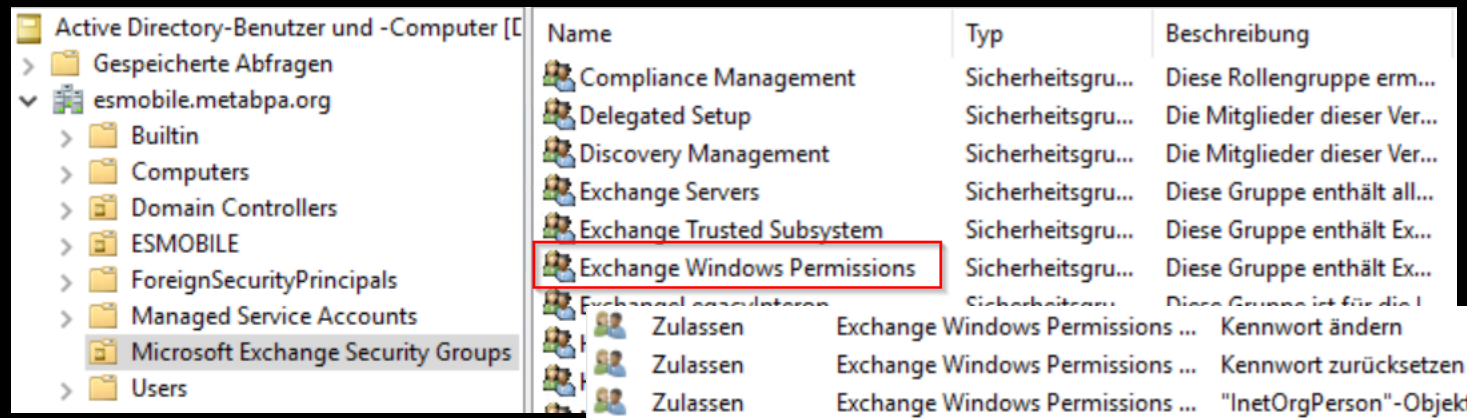
```
Setup /p /ActiveDirectorySplitPermissions:true
```

und zurück:

```
Setup /p /ActiveDirectorySplitPermissions:false
```

Auf einen Blick

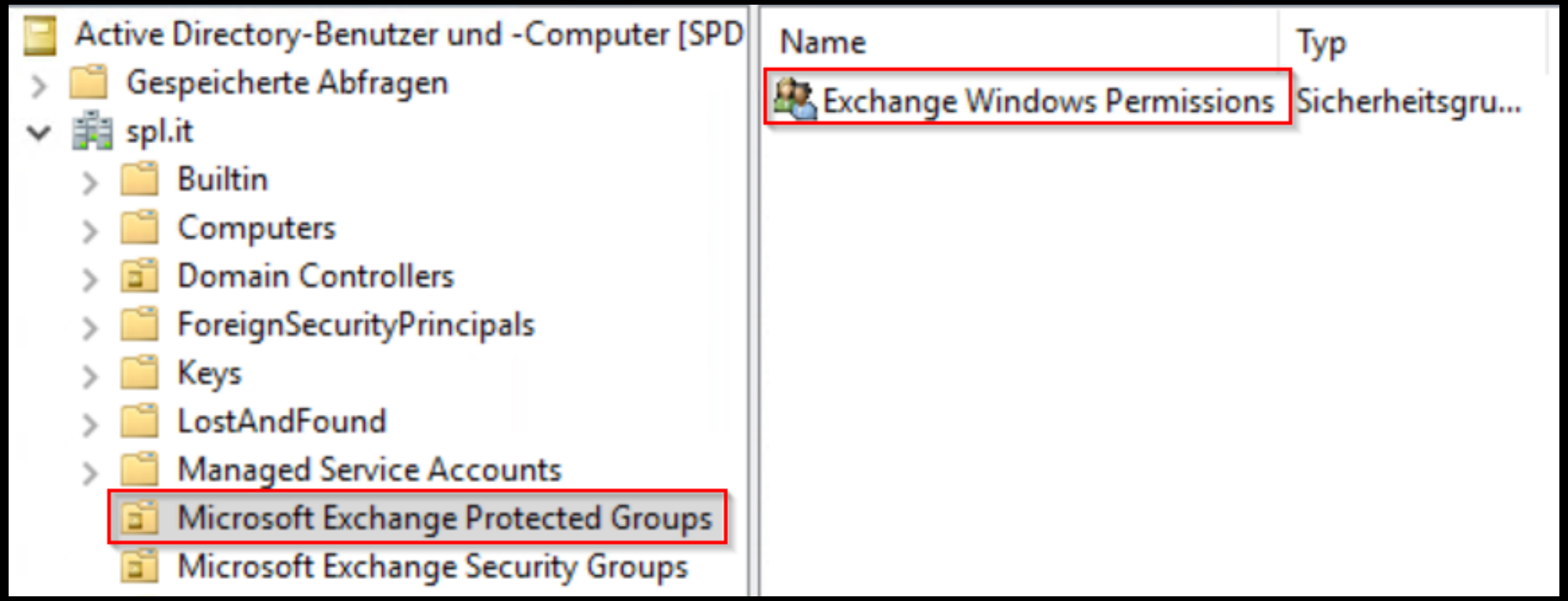
In welchem Permissions-Modell ist mein AD-Forest?



Zulassen	Exchange Windows Permissions ...	Kennwort ändern	Keine	Speziell
Zulassen	Exchange Windows Permissions ...	Kennwort zurücksetzen	Keine	Speziell
Zulassen	Exchange Windows Permissions ...	"InetOrgPerson"-Objekte erstellen	Keine	Dieses und alle untergeordneten Objekte
Zulassen	Exchange Windows Permissions ...	"Computer"-Objekte erstellen	Keine	Dieses und alle untergeordneten Objekte
Zulassen	Exchange Windows Permissions ...	"Gruppe"-Objekte erstellen	Keine	Dieses und alle untergeordneten Objekte
Zulassen	Exchange Windows Permissions ...	"Organisationseinheit"-Objekte erstellen	Keine	Dieses und alle untergeordneten Objekte
Zulassen	Exchange Windows Permissions ...	"Benutzer"-Objekte erstellen	Keine	Dieses und alle untergeordneten Objekte
Zulassen	Exchange Windows Permissions ...	"Kontakt"-Objekte erstellen	Keine	Dieses und alle untergeordneten Objekte
Zulassen	Exchange Windows Permissions ...		Keine	Dieses und alle untergeordneten Objekte
Zulassen	Exchange Windows Permissions ...		Keine	Dieses und alle untergeordneten Objekte
Zulassen	Exchange Windows Permissions ...		Keine	Dieses und alle untergeordneten Objekte
Zulassen	Exchange Windows Permissions ...		Keine	Dieses und alle untergeordneten Objekte
Zulassen	Exchange Windows Permissions ...		Keine	Dieses und alle untergeordneten Objekte
Zulassen	Exchange Windows Permissions ...		Keine	Dieses und alle untergeordneten Objekte
Zulassen	Exchange Windows Permissions ...		Keine	Dieses und alle untergeordneten Objekte
Zulassen	Exchange Windows Permissions ...	Unterstruktur löschen	Keine	Speziell
Zulassen	Exchange Windows Permissions ...	Unterstruktur löschen	Keine	Speziell
Zulassen	Exchange Windows Permissions ...	Löschen	Keine	Untergeordnete "Computer"-Objekte
Zulassen	Exchange Windows Permissions ...	Löschen	Keine	Untergeordnete "Gruppe"-Objekte

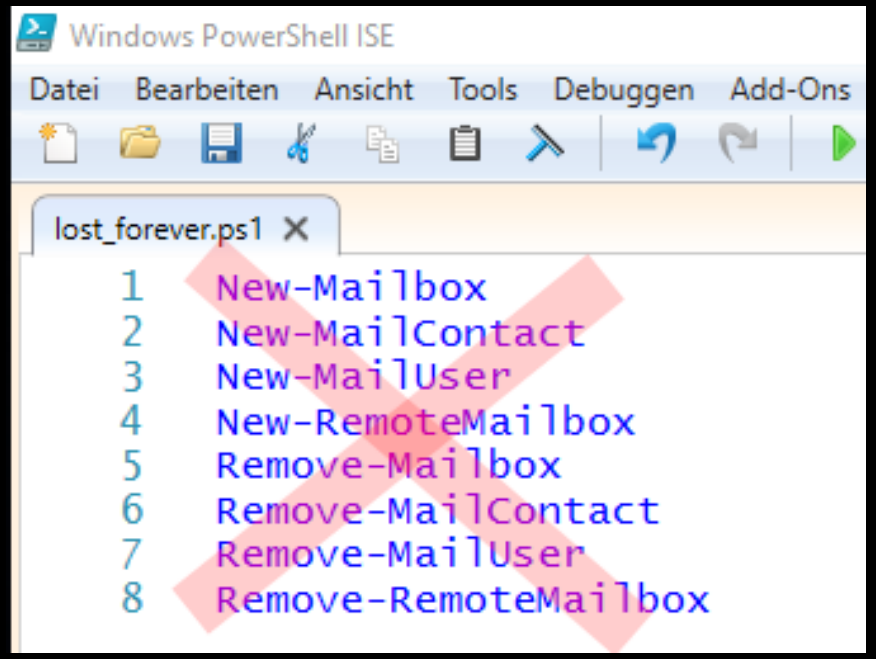
Auf einen Blick

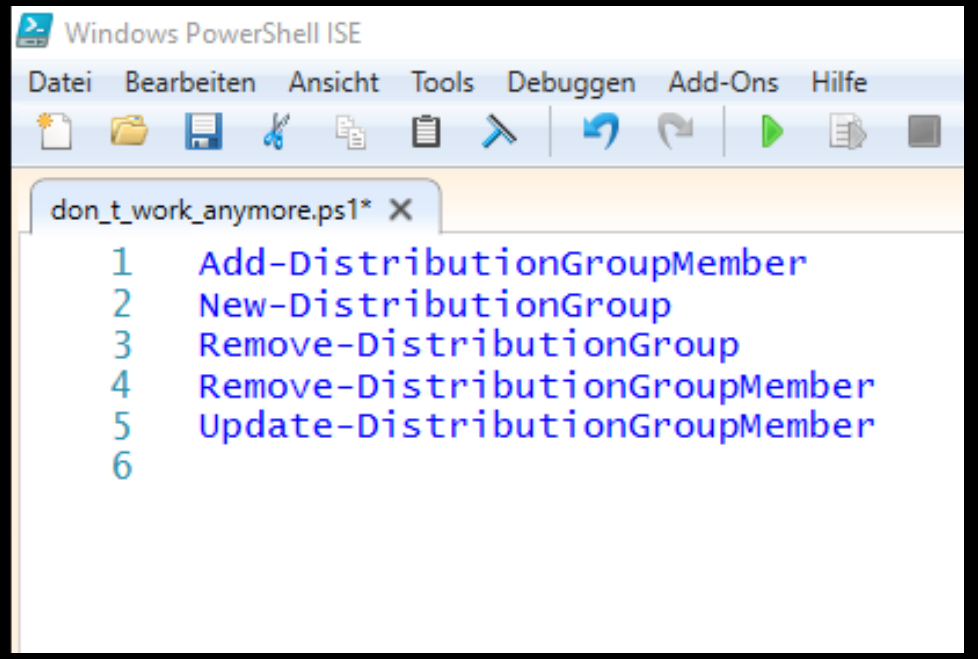
In welchem Permissions-Modell ist mein AD-Forest?



Split Permissions for President?

- Dokumentation: https://docs.microsoft.com/de-de/exchange/understanding-split-permissions-exchange-2013-help





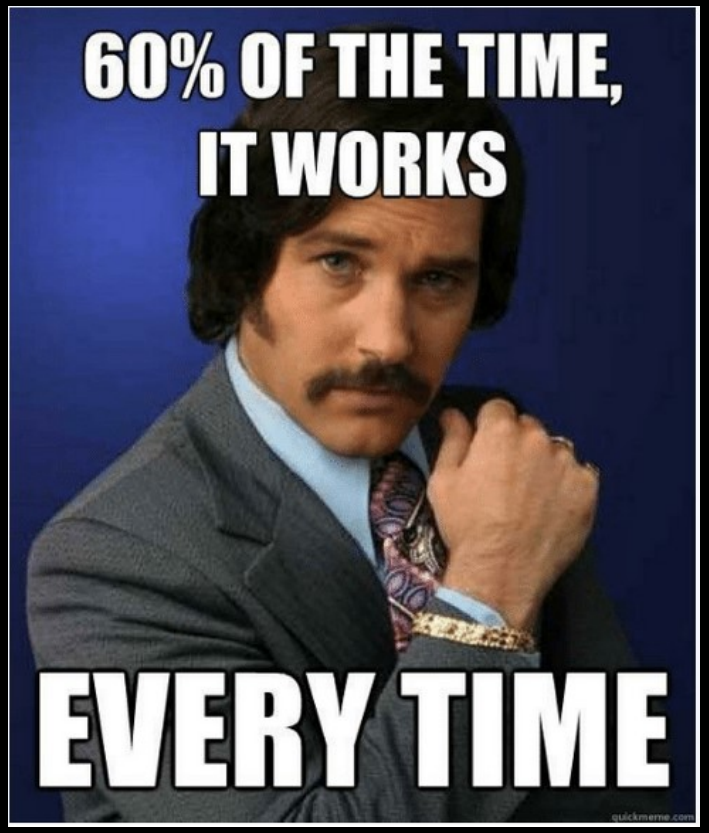
Noch einmal zum Verständnis…

- Wann und warum funktioniert

  `Add-ADPermission`

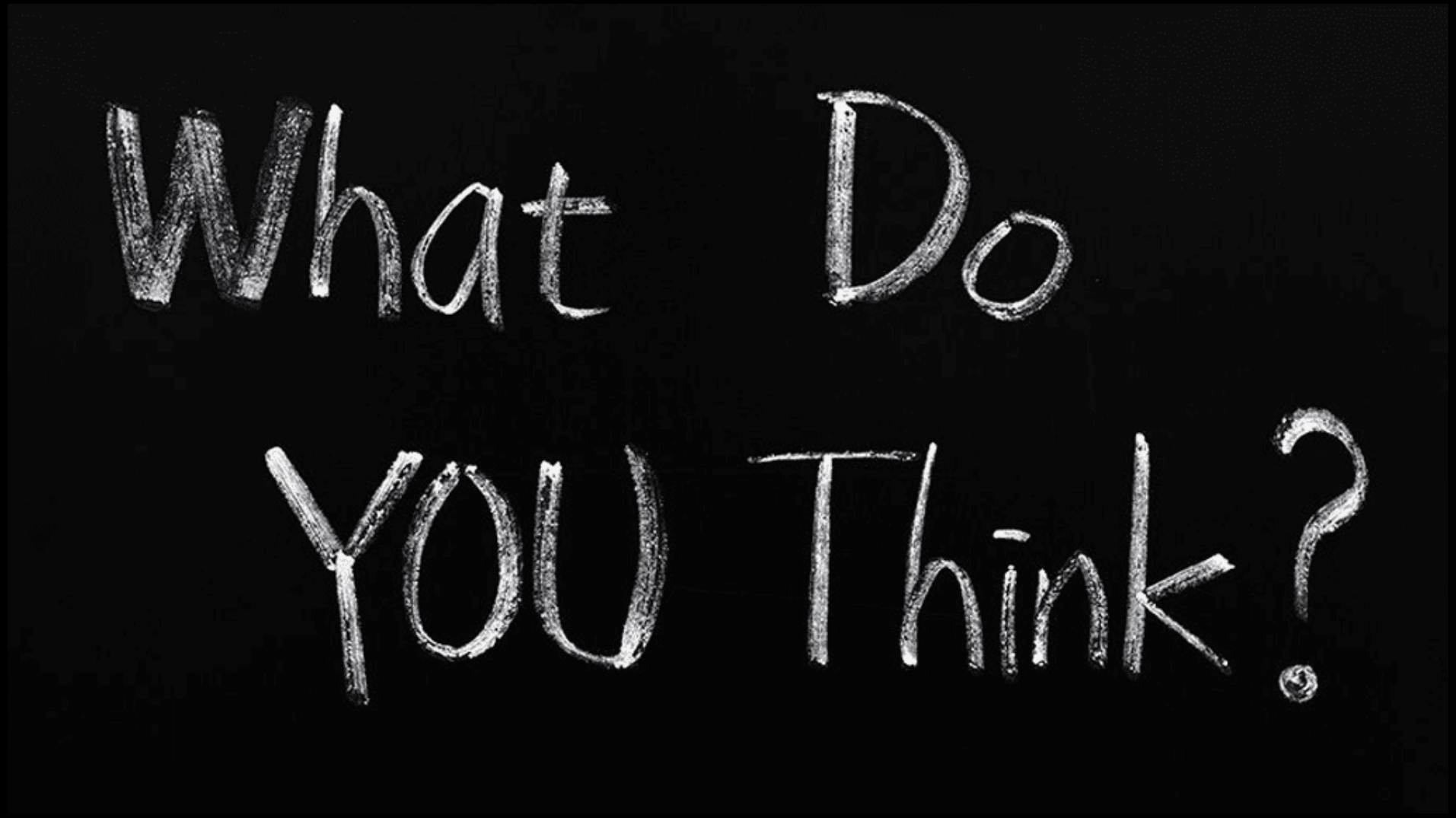
  ?

- *Hint: Es gibt icht nur User- und Gruppenobjekte*



Was geht kaputt?

- IDM-Systeme, die `New-Mailbox` zur User-Generierung verwenden…
- …oder für die Mitgliedschaften in Verteilergruppen Exchange-Cmdlets nehmen.
- Auch die Gruppenpflege durch die User ist betroffen.


What Do
YOU Think?