



## Exchange - Outlook Sicherheitsproblem Forwarding

Wie finden wir auf einem Exchange Server heraus, wer sich E-Mails ganz plump nach Hause schickt.

Mit diesem Powershell Befehl erstellen wir einen Bericht, aus dem hervorgeht, welcher E-Mail Benutzer sich über einen Outlook Client eine Regel erstellt hat, mit dem Ziel eingehende E-Mails weiterzuleiten. Egal ob intern oder extern.

```
Get-Mailbox -ResultSize unlimited | Get-InboxRule -ErrorAction SilentlyContinue | Where-Object {($_.redirectto -ne $null) -or ($_.forwardto -ne $null)} | Format-List MailboxOwnerID,name,from,redirectto,ForwardTo | Out-File C:\Temp\OutlookForwarding.txt
```

### Ergebnis der Überprüfung:

Ein Benutzer leitet sich E-Mails, die an ihm persönlich „An“ adressiert sind oder er in Copy „Cc“ steht, weiter.

```
MailboxOwnerId : ndsedv.de/KONFIGURATION/SITES/Essen/User/NDS GmbH/IT - Main Operations/Hartleiner, Andreas
Name           : die meinen Namen im Feld "An" oder "Cc" enthält
From           :
RedirectTo     : {"hartleiner_a@hotmail.com" [SMTP:hartleiner_a@hotmail.com]}
ForwardTo      :
```

### Ausgeführte Aktionen:

Auf dem Exchange Server habe ich mir die, seitens des Benutzers eingerichteten Outlook-Regeln, ausgeben lassen. Mithilfe der „RuleIdentity“ werde ich die Regel löschen.

```
Get-InboxRule -Mailbox Andreas.Hartleiner@ndsedv.com
```

```
Welcome to the Exchange Management Shell!
Full list of cmdlets: Get-Command
Only Exchange cmdlets: Get-ExCommand
Cmdlets that match a specific string: Help *<string>*
Get general help: Help
Get help for a cmdlet: Help <cmdlet name> or <cmdlet name> -?
Exchange team blog: Get-ExBlog
Show full output for a command: <command> | Format-List

Show quick reference guide: QuickRef
VERBOSE: Connecting to a-...de.
VERBOSE: Connected to a-...de.
[PS] C:\Windows\system32>Get-InboxRule -Mailbox Andreas.Hart... com

Name                                     Enabled Priority RuleIdentity
-----
die meinen Namen im Feld "Cc" enthält    True     1         16461504361504178178
die meinen Namen im Feld "An" oder "Cc" enthält True     2         16533561955542106114
Kategorien der E-Mails löschen (empfohlen) True     3         16605619549580034050
LZnet (... )                            True     4         16677677143617961986
C:\Windows\system32>
```



## Exchange - Outlook Sicherheitsproblem Forwarding

Detaillierte Ansicht der Ausgabe:

Get-InboxRule -Mailbox Andreas.Hartleiner@ndsedv.com | Select Name, Description | fl

```
Machine: a-ssb-...
[PS] C:\Windows\system32>Get-InboxRule -Mailbox Andreas.Hartleiner@ndsedv.com | Select Name, Description | fl
Name      : die meinen Namen im Feld "Cc" enthält
Description : If the message:
             the message was received from '...' Marc'
             and my name is in the Cc box
             and the message includes specific words in the subject 'T... progress'
Take the following actions:
             forward the message to '... Siegfried' and ... trow, ...

Name      : die meinen Namen im Feld "An" oder "Cc" enthält
Description : If the message:
             my name is in the To or Cc box
Take the following actions:
             redirect the message to 'hart...@hotmail.com'

Name      : Kategorien der E-Mails löschen (empfohlen)
Description :

Name      : LZnet ...
Description : If the message:
             the message includes specific words in the subject or body 'lebensmit...'
Take the following actions:
             move the message to folder 'LZ ...'

Name      : ...
Description : If the message:
             the message was received from '...'
Take the following actions:
             move the message to folder '...'

[PS] C:\Windows\system32>
```



## Exchange - Outlook Sicherheitsproblem Forwarding

Die vom Benutzer erstellte(n) Regel(n) wurden gelöscht:

Remove-Inboxrule -Mailbox [Andreas.Hartleiner@ndsedv.com](mailto:Andreas.Hartleiner@ndsedv.com) -Identity "16461504361504178178"

Remove-Inboxrule -Mailbox [Andreas.Hartleiner@ndsedv.com](mailto:Andreas.Hartleiner@ndsedv.com) -Identity "16533561955542106114"

```
Machine: a-ssb-...
[PS] C:\Windows\system32>Remove-Inboxrule -Mailbox Andreas.Hart...@ndsedv.com -Identity "16461504361504178178"
Confirm
Are you sure you want to perform this action?
Removing inbox rule ".../#KONFIGURATION/SITES/... GmbH/IT - Main Operations/Hart...,
Andreas\16461504361504178178" from mailbox ".../#KONFIGURATION/SITES/... GmbH/IT - Main
Operations/Hart... Andreas".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (default is "Y"): Y

Confirm
Using Outlook Web App or Windows PowerShell to modify your rules will delete any rules that were previously turned off
using Outlook. If you want to preserve the rules you turned off using Outlook, click Cancel and use Outlook to edit
your rules. If you want to proceed, click OK.
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (default is "Y"): Y
[PS] C:\Windows\system32>Remove-Inboxrule -Mailbox Andreas.Hart...@ndsedv.com -Identity "16533561955542106114"

Confirm
Are you sure you want to perform this action?
Removing inbox rule "...de/#KONFIGURATION/SITES/... GmbH/IT - Main Operations/Hart...,
Andreas\16533561955542106114" from mailbox "...de/#KONFIGURATION/SITES/.../User/... GmbH/IT - Main
Operations/Har... Andreas".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (default is "Y"): ^Y
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (default is "Y"): y
[PS] C:\Windows\system32>
```

Ergebnis:

Get-InboxRule -Mailbox [Andreas.Hartleiner@ndsedv.com](mailto:Andreas.Hartleiner@ndsedv.com)

Aus den 5 Regeln wurden 3.

```
Machine: a-ss...de
[PS] C:\Windows\system32>Get-InboxRule -Mailbox Andreas.Hart...@ndsedv.com

Name                                     Enabled Priority RuleIdentity
----
Kategorien der E-Mails löschen (empfohlen) True     1       16605619549580034050
LZn                                     True     2       16677677143617961986
...                                     True     3       16749734737655889922

[PS] C:\Windows\system32>
```