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:

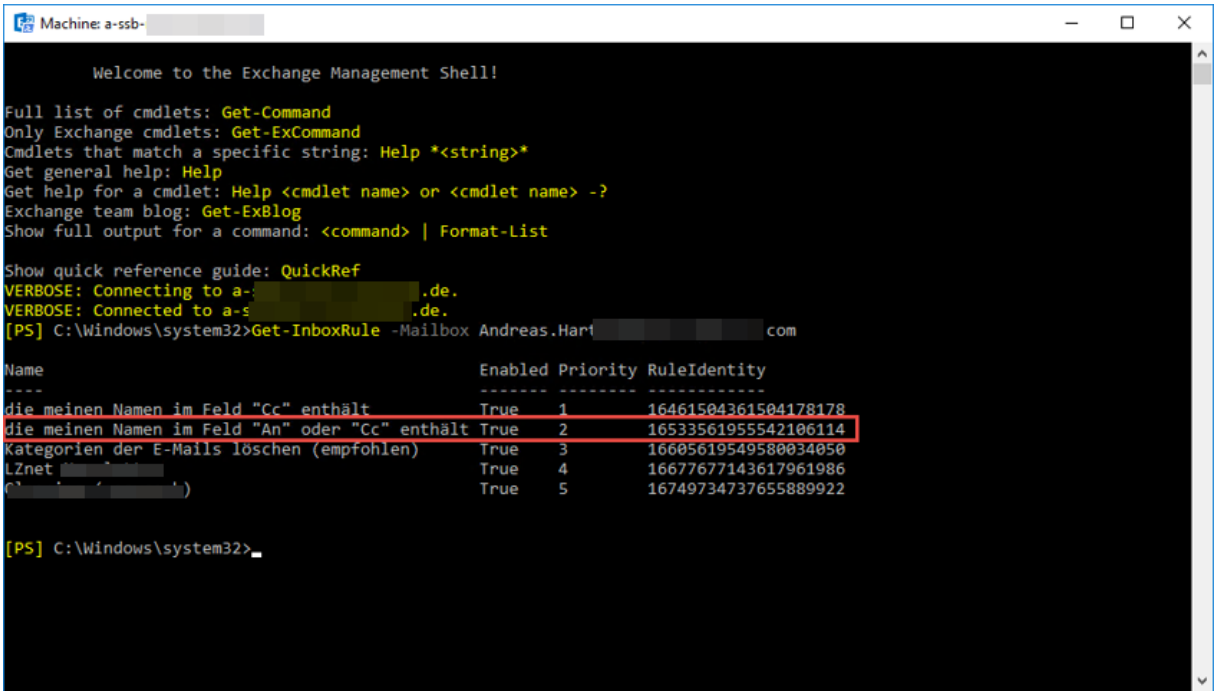
Ein Benutzer leitet sich E-Mails, die an ihm persönlich „An" adressiert sind oder er in Copy „Cc" steht, weiter.

```
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.

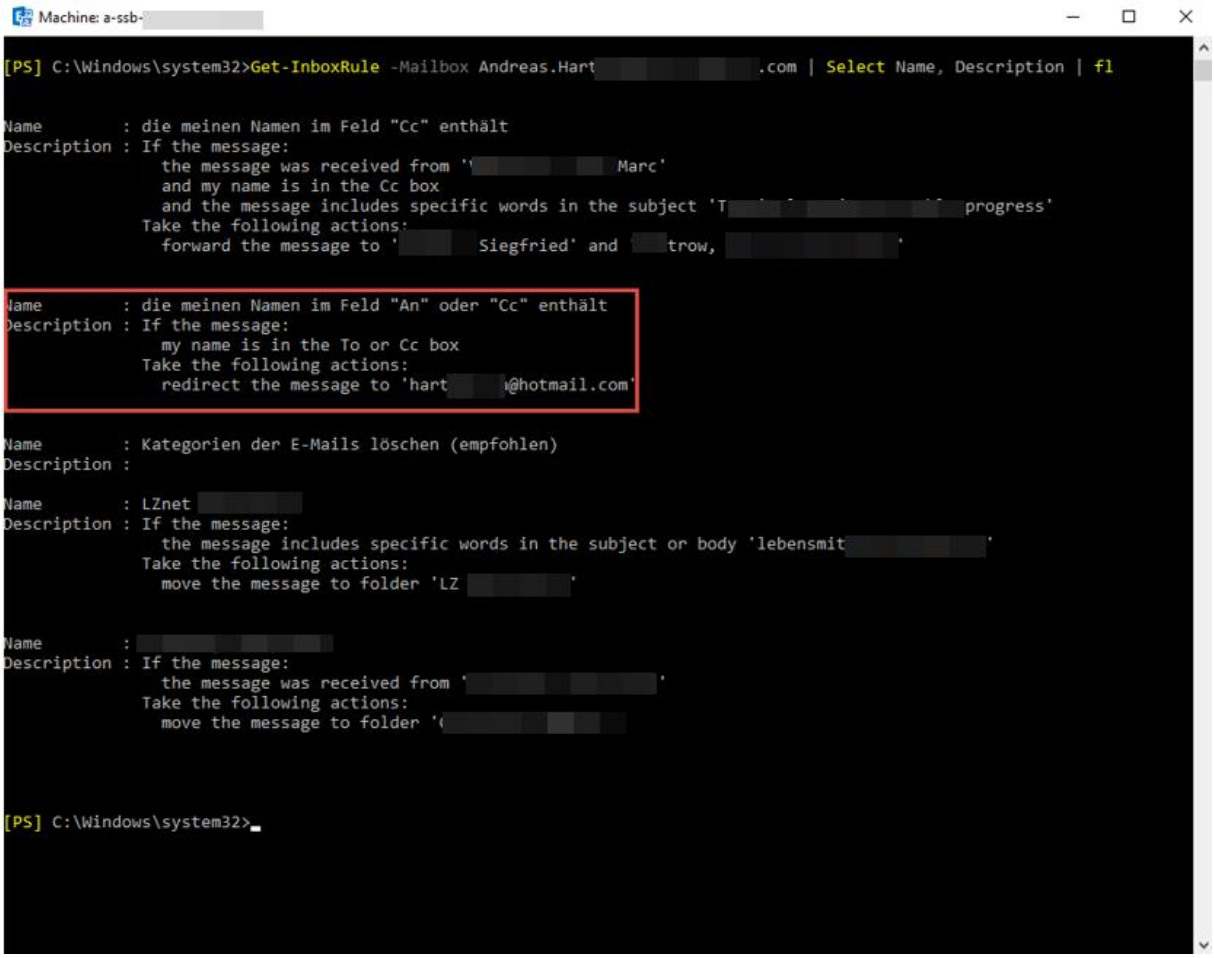
```
Get-InboxRule –Mailbox Andreas.Hartleiner@ndsedv.com
```



Exchange - Outlook Sicherheitsproblem Forwarding

Detaillierte Ansicht der Ausgabe:

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

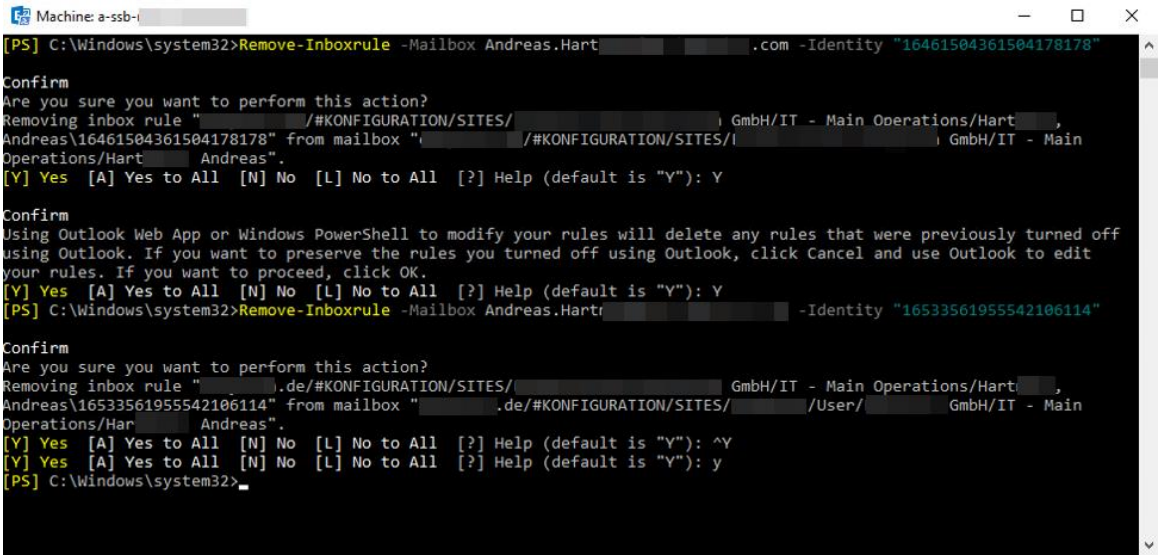


Exchange - Outlook Sicherheitsproblem Forwarding

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

Remove-Inboxrule –Mailbox Andreas.Hartleiner@ndsedv.com -Identity "16461504361504178178"

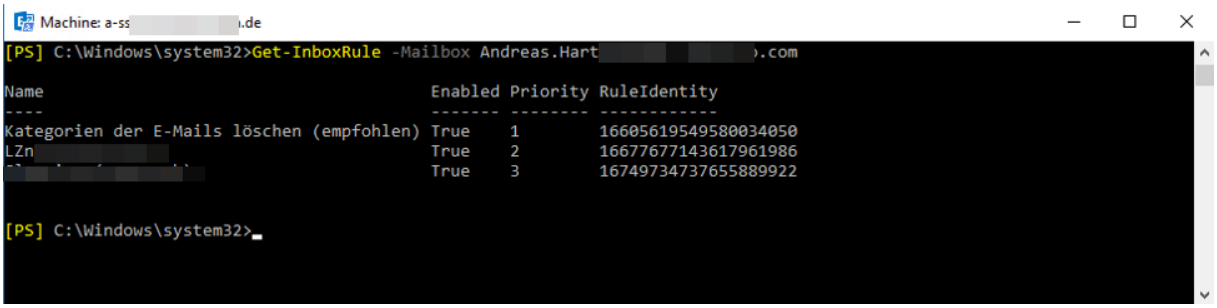
Remove-Inboxrule –Mailbox Andreas.Hartleiner@ndsedv.com -Identity "16533561955542106114"



Ergebnis:

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

Aus den 5 Regeln wurden 3.



Erstellt von Jörn Walter **25.04.2019**