File Server auf Ransomware-Dateien prüfen

Zum Schutz unserer Daten können wir mittels des Ressourcen-Managers für Dateiserver, eine Dateiprüfung so konfigurieren, dass diese uns alarmiert sobald Ransomware eine blockierte Dateiendung erstellt.

Zur Vorbereitung installieren wir den Ressourcen-Manager für Dateiserver mittels Power Shell Skript, gerne auch über die GUI:

```
If (-not(Get-WindowsFeature FS-Resource-Manager | Where-Object {$_.Installed -match “True”}))
{Install-WindowsFeature –Name FS-Resource-Manager –IncludeManagementTools}
Else
{Write-host "FSRM is already installed" -ForegroundColor Green}
```

Die E-Mail Benachrichtigungseinstellungen setzen wir mit diesem Befehl.

```
Set-FsrmSetting -SmtpServer "SMTP.ndsedv.de" `
-AdminEmailAddress "administrator@ndsedv.de" `
-FromEmailAddress " fsrm@ndsedv.de " `
-ReportLocationScheduled "$Scheduledpath" `
-ReportLocationIncident "$Incidentspath" `
-ReportLocationOnDemand "$Interactivepath"
```

Mit diesem Befehl konfigurieren wir das LOG den Speicherort und die Quota, in unserem Fall aber nicht notwendig:

```
$hostname=gc env:computername
$Incidentspath="\\SERVER\quota$\$hostname\Reports\Incidents"
$Scheduledpath="\\SERVER\quota$\$hostname\Reports\Scheduled"
$Interactivepath="\\SERVER\quota$\$hostname\Reports\Interactive"
New-Item -Itemtype Directory -path "C:\LOGS\FSRM\Templates", "C:\LOGS\FSRM\Logs", `
"\\SERVER\quota$\$hostname", "$Incidentspath", "$Scheduledpath", "$Interactivepath"
```

Mit diesem Befehl konfigurieren wir die Berichtsorte, in unserem Fall aber nicht notwendig:

```
$logfile = "C:\LOGS\FSRM\FSRM_Deploy_$(get-date -format `"yyyyMMdd_hhmmsstt`").log"
Start-Transcript -path $logfile
```

Anlegen einer neuen Dateigruppe mit allen bekannten Dateiendungen z.B.:

```
New-FsrmFileGroup -Name "Ransomware" –IncludePattern @
("*.locky","*.key","RECOVERY_FILE*.txt", "restorefiles.txt", "recoverfile*.txt")
```

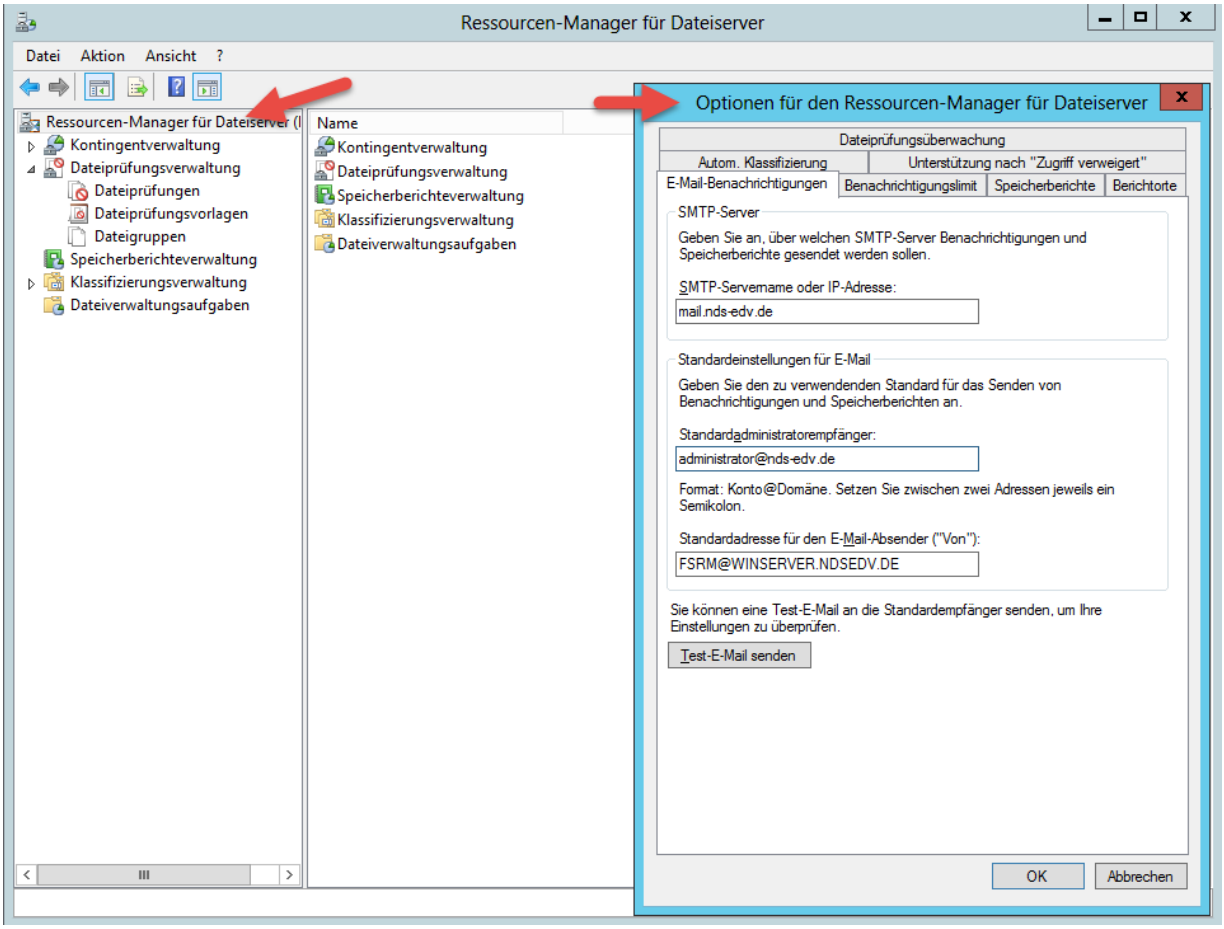
Einrichten einer E-Mail-Benachrichtigung; Aktion:

```
FscreenNotification = New-FsrmAction -Type Email `
-MailTo "[Source Io Owner Email]" `
-Subject "Unauthorized file from the [Violated File Group] file group detected" `
-Body "User [Source Io Owner] attempted to save [Source File Path] to [File Screen Path] on the
[Server] server.
This file is in the [Violated File Group] file group."
```

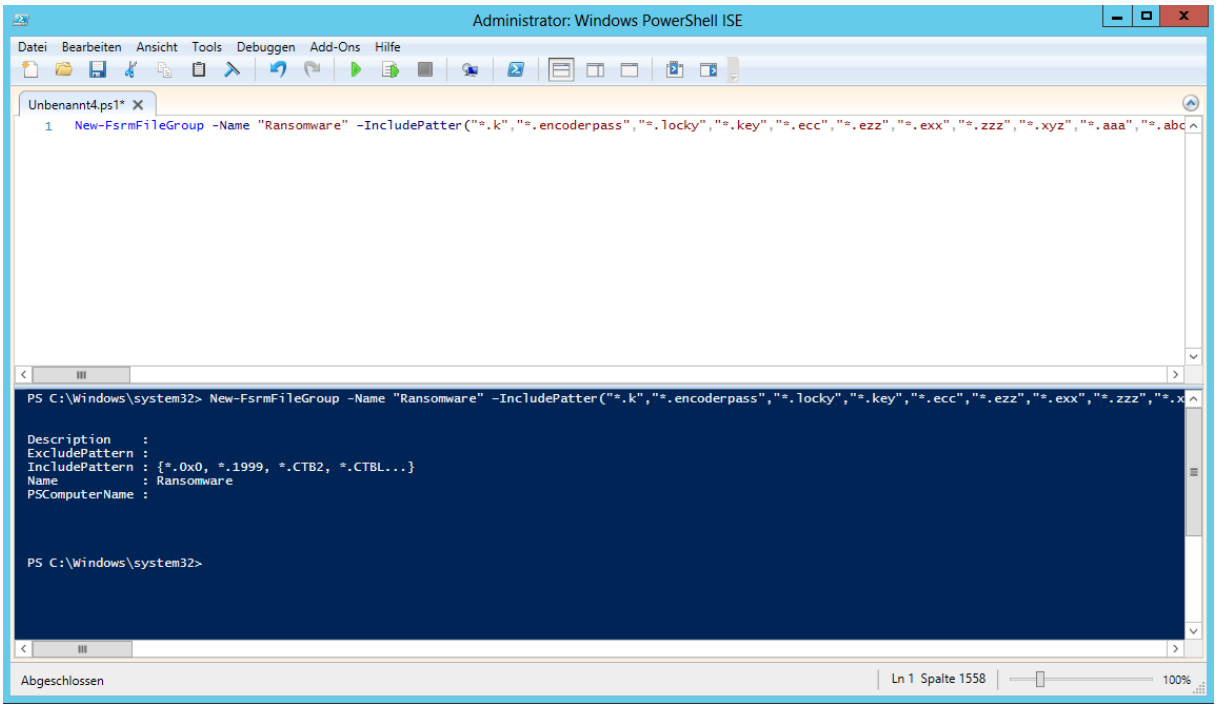
Erstellt von Jörn Walter www.der-windows-papst.de – 01.02.2016

File Server auf Ransomware-Dateien prüfen

Als erstes konfigurieren wir die E-Mail-Benachrichtigung, damit im Falle einer Aktion nicht nur ein Eintrag in der Ereignisanzeige erstellt, sondern auch direkt eine E-Mail versendet wird.



Da es sich um eine Vielzahl von Dateiendungen handelt, kann diese **Dateigruppe** mittels Powershell-Skript erstellt werden.

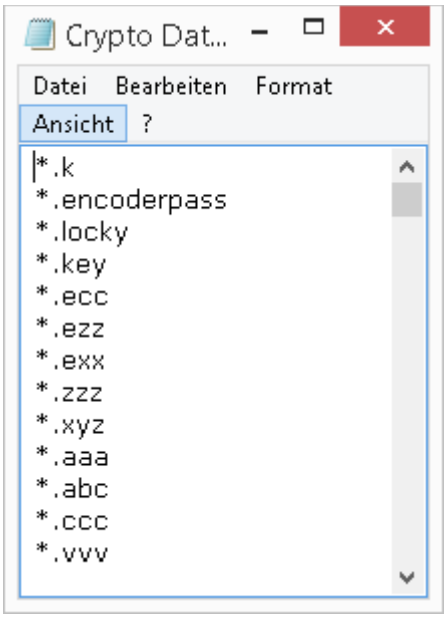


Erstellt von Jörn Walter www.der-windows-papst.de – 01.02.2016

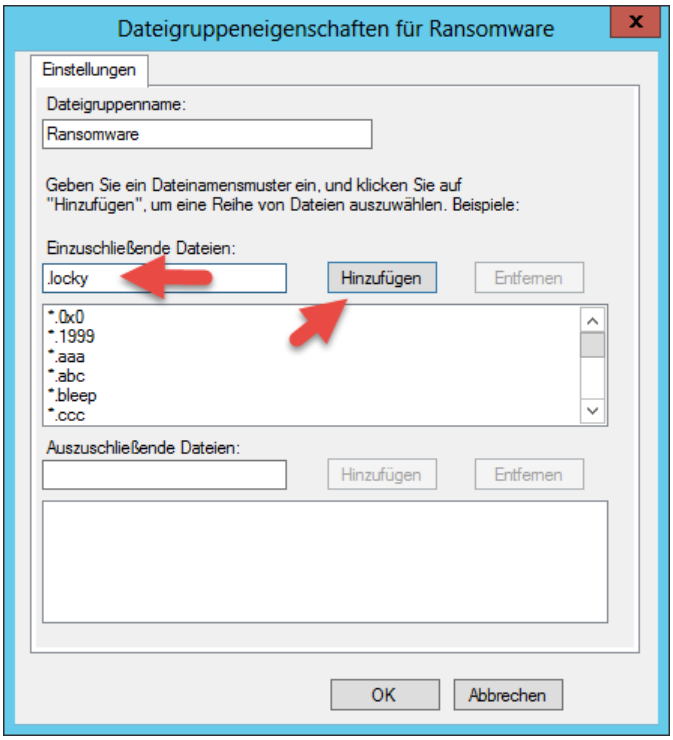
File Server auf Ransomware-Dateien prüfen

Wenn man später die Dateigruppe Ransomware aktualisieren möchte, dann mit diesem Befehl:

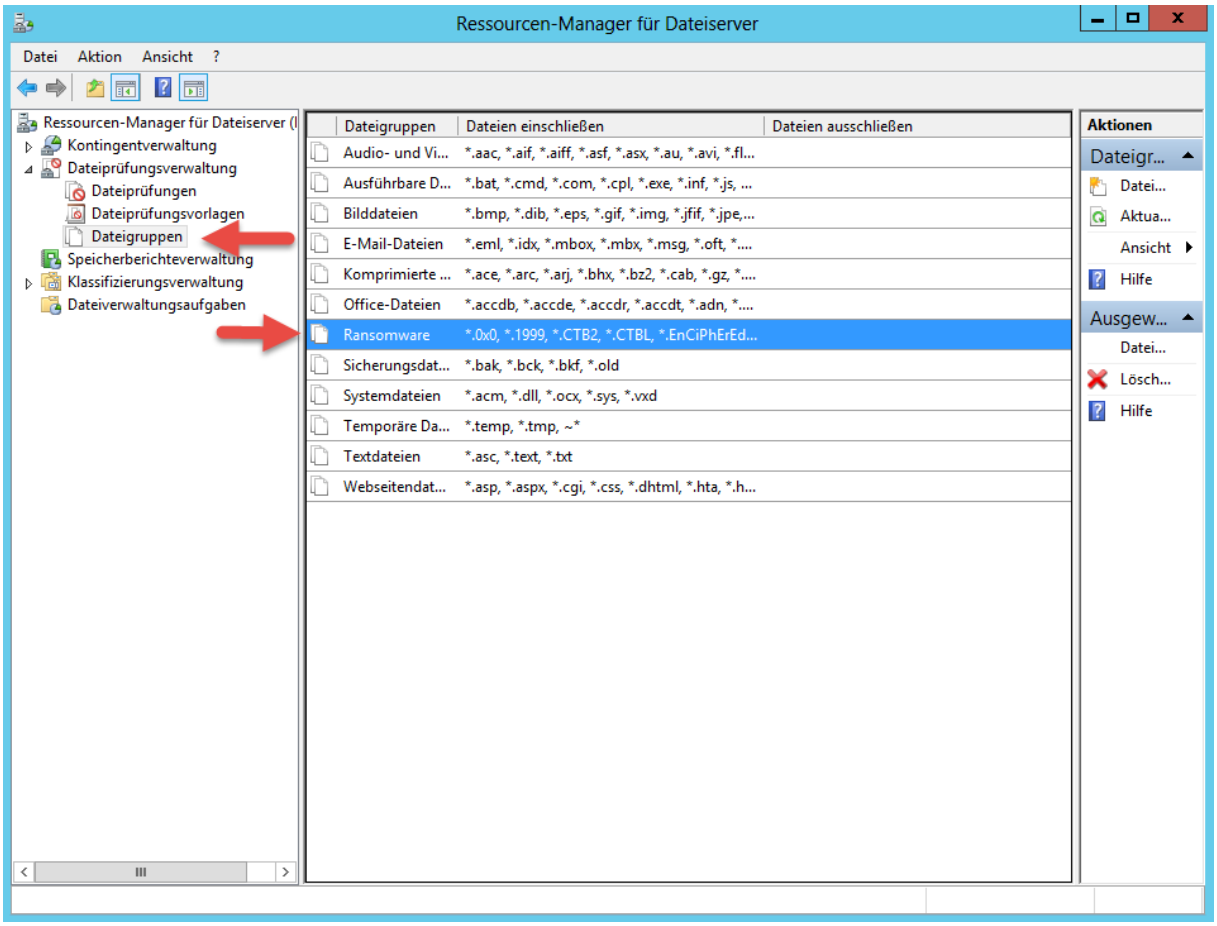
```
$extension = Get-Content .\ransomendungen.txt

Set-FsrmFileGroup -Name "Ransomware" -IncludePattern ($extension)
```



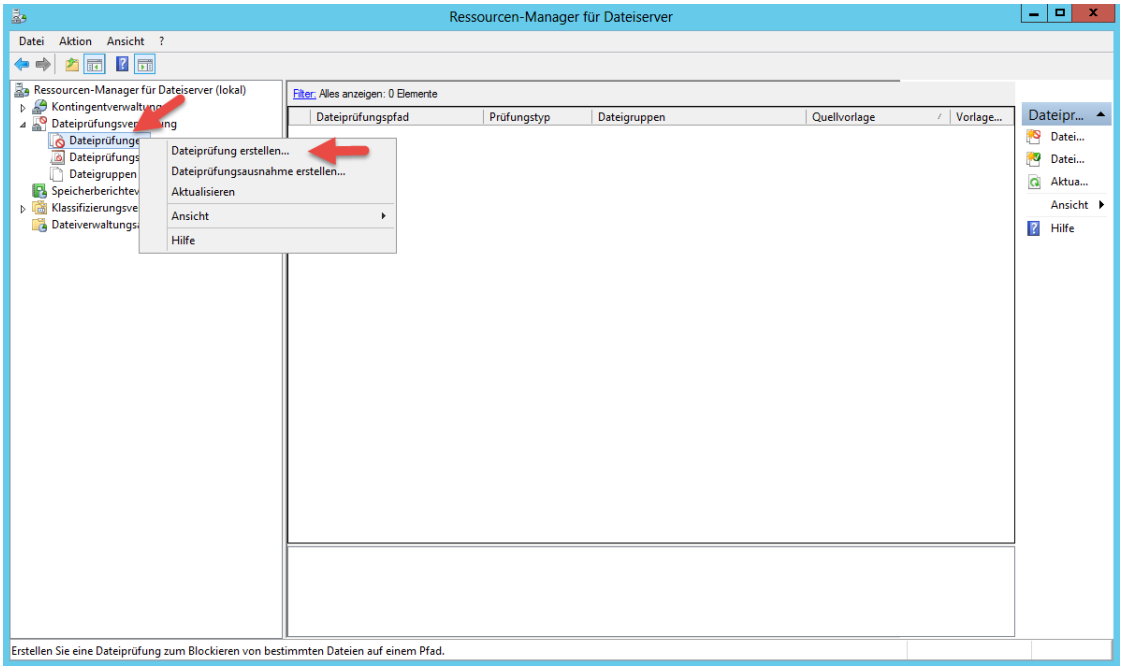
Manuell würde wir die einzelnen Dateiendungen über > **Einzuschließende Dateien > Hinzufügen**.



Die Dateigruppe ist nun erstellt.

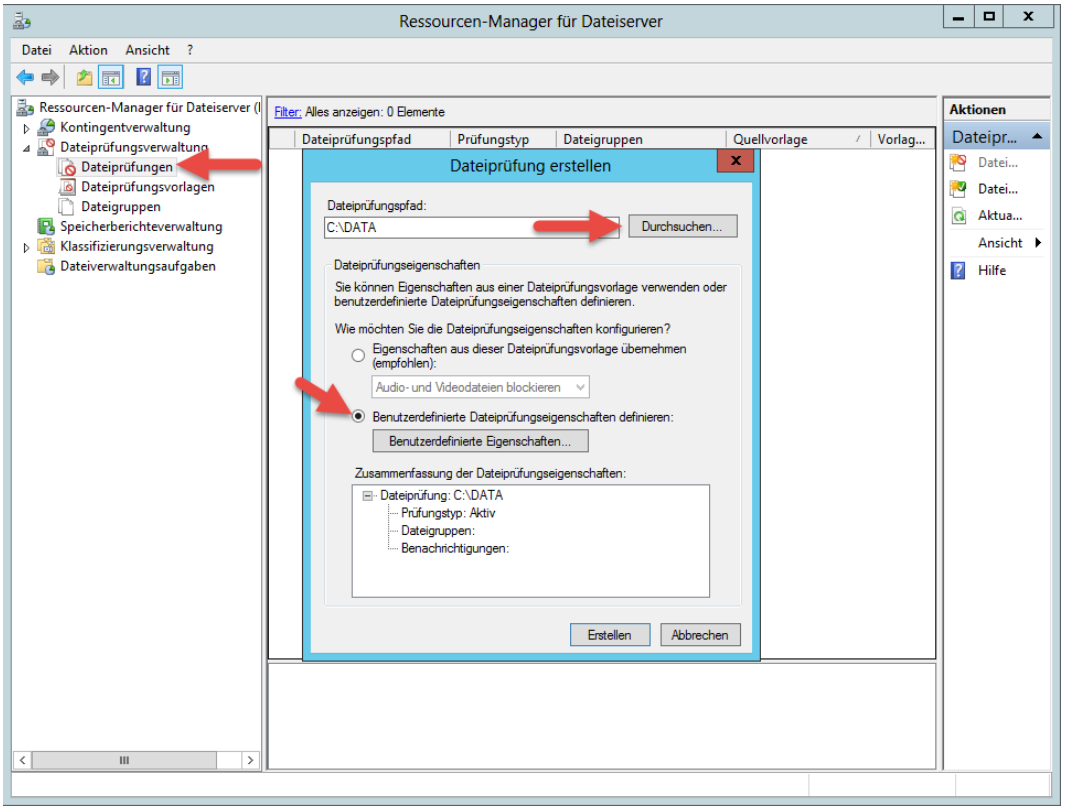


Als nächstes erstellen wir einen neuen Auftrag > **Dateiprüfung erstellen** auf Vorlage von Audio- und Videodateien blockieren.

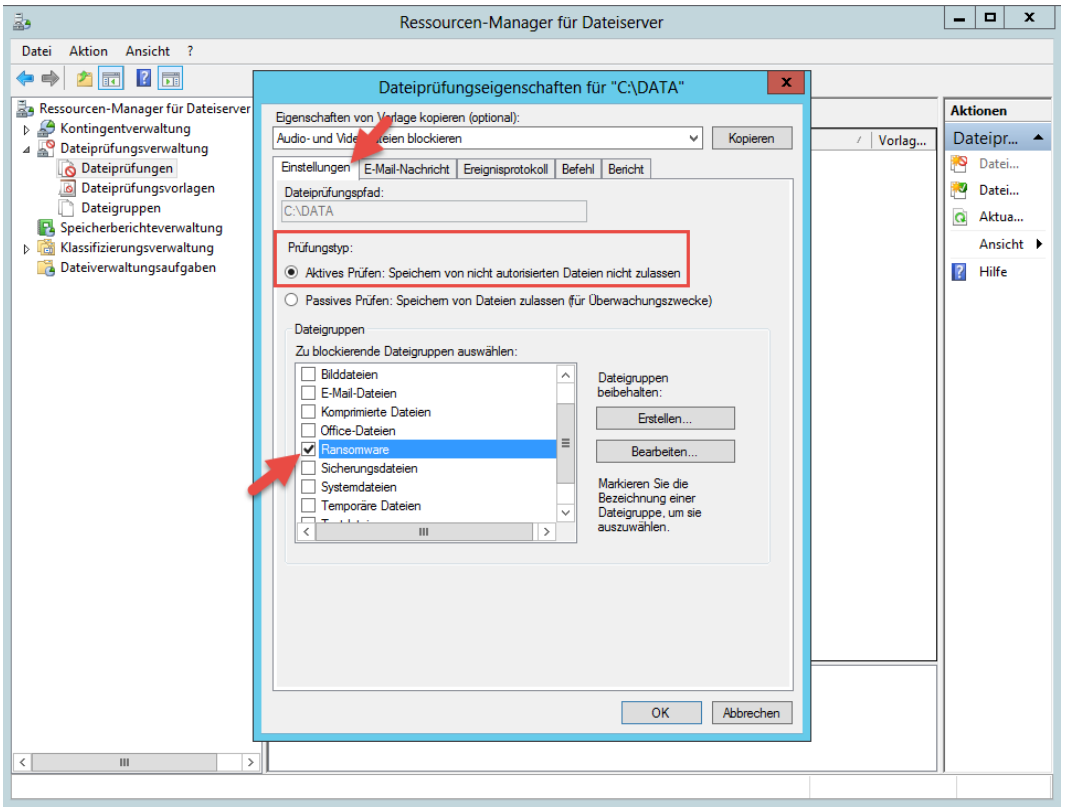


File Server auf Ransomware-Dateien prüfen

Über > **Benutzerdefinierte Eigenschaften...** konfigurieren wir den Prüfungstyp und die eben erstellte Dateigruppe kommt zum Einsatz.

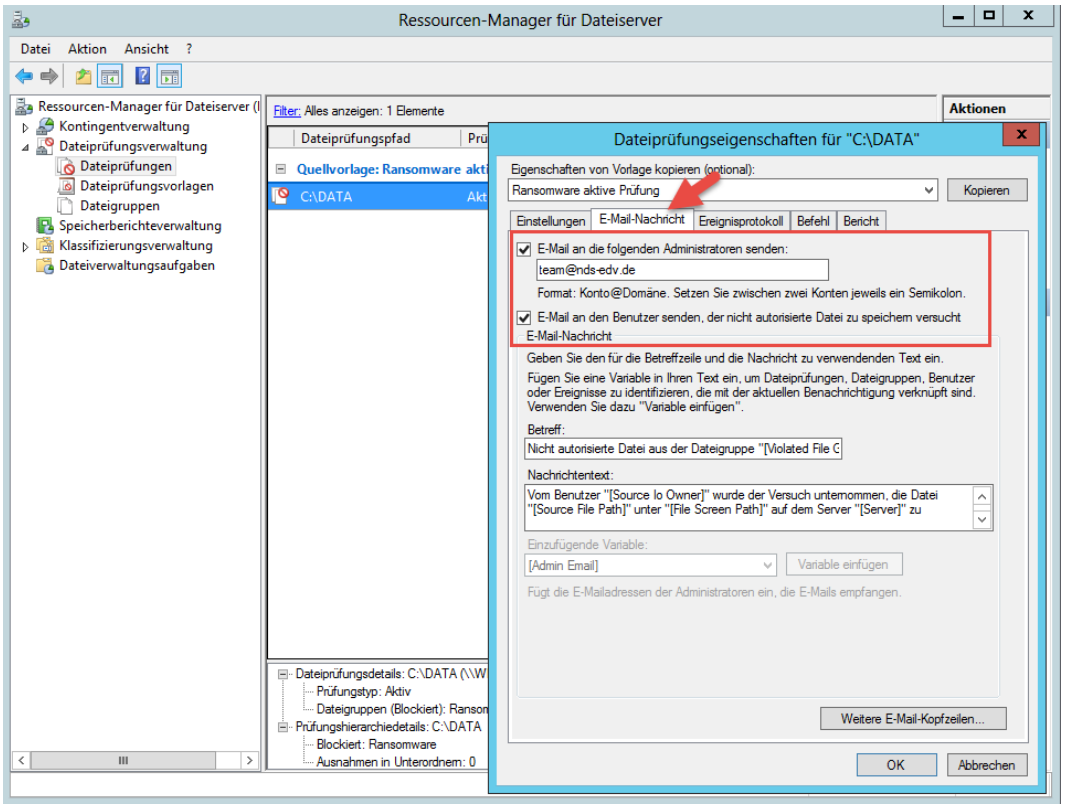


Über Einstellungen definieren wir den Prüfungstyp und die Dateigruppe in der die zu überwachenden Dateiendungen enthalten sind.

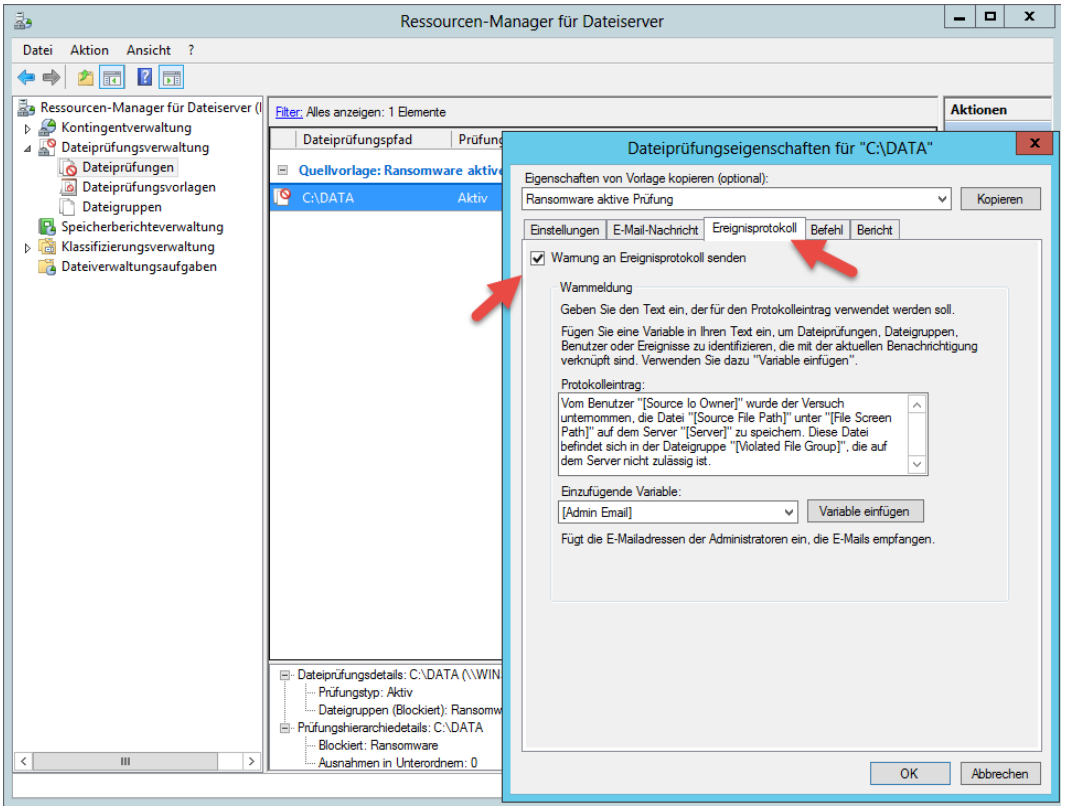


File Server auf Ransomware-Dateien prüfen

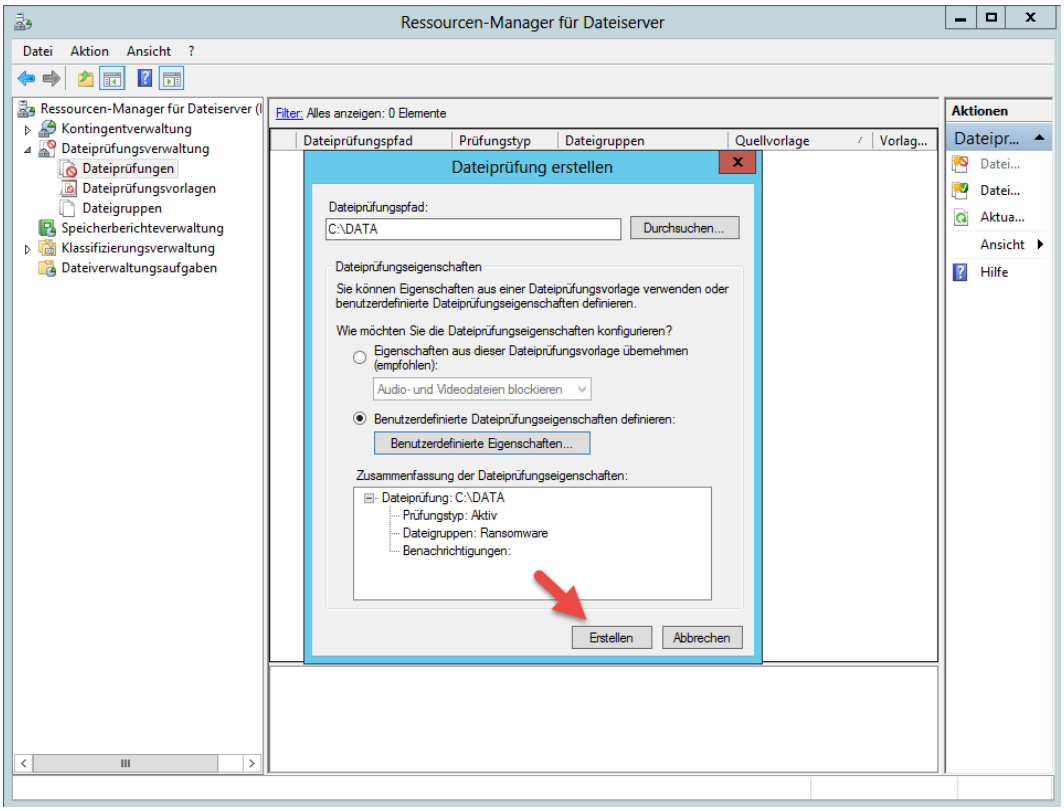
Über den Reiter **E-Mail Nachricht** stellen wir den Empfänger der Warnmeldung ein.



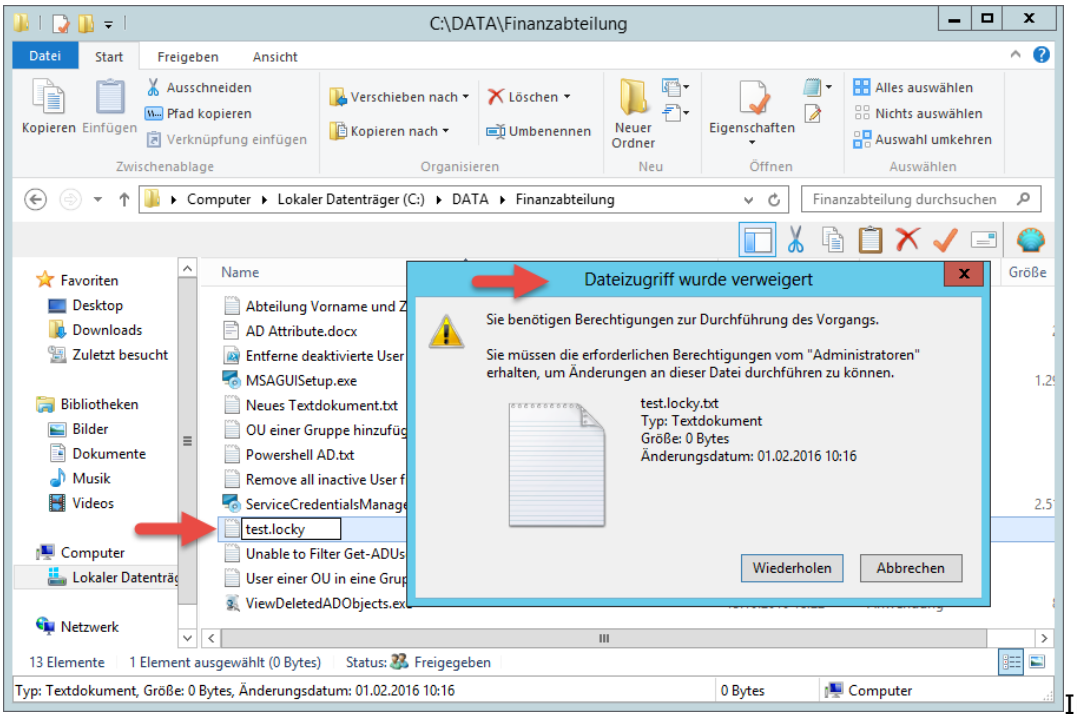
Aktivieren das Schreiben in das Ereignisprotokoll. E können auch noch weitere Variablen in das Event-Log eingefügt werden.



Mit klicken auf > **Erstellen** ist der Dateiprüfung konfiguriert und aktiv.



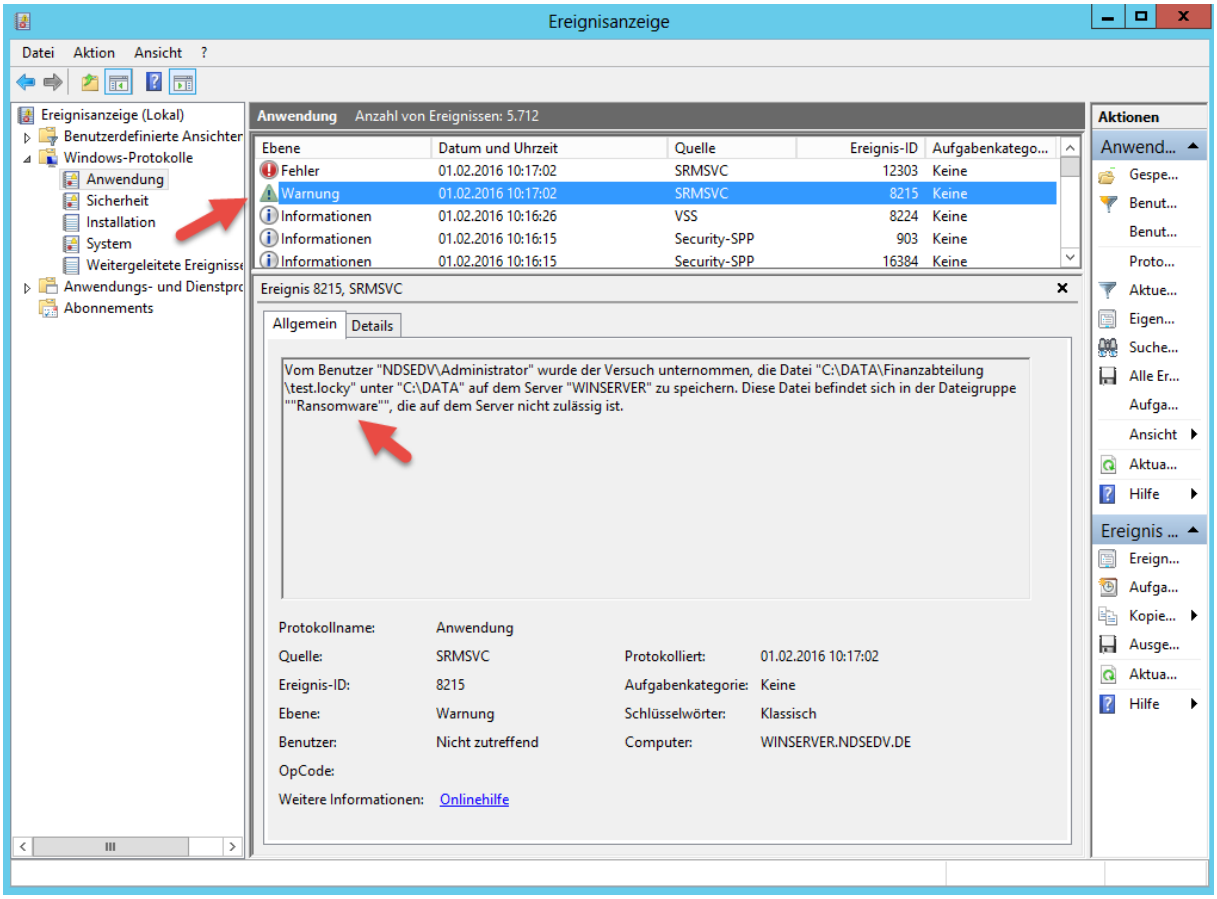
Jetzt versuche ich eine Datei mit der Endung .locky zu erstellen. Es erscheint sofort die Meldung das der **Dateizugriff verweigert** wurde.



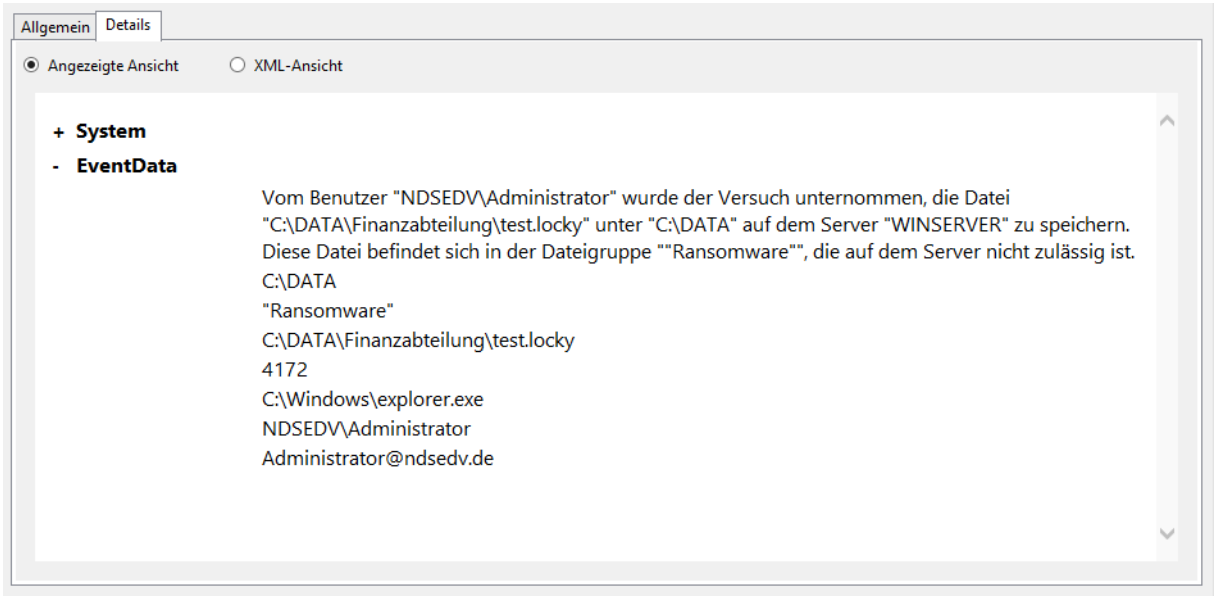
In der

File Server auf Ransomware-Dateien prüfen

Ereignisanzeige unter > Anwendung erscheint sofort der Warnhinweis mit der **Ereignis-ID 8215**



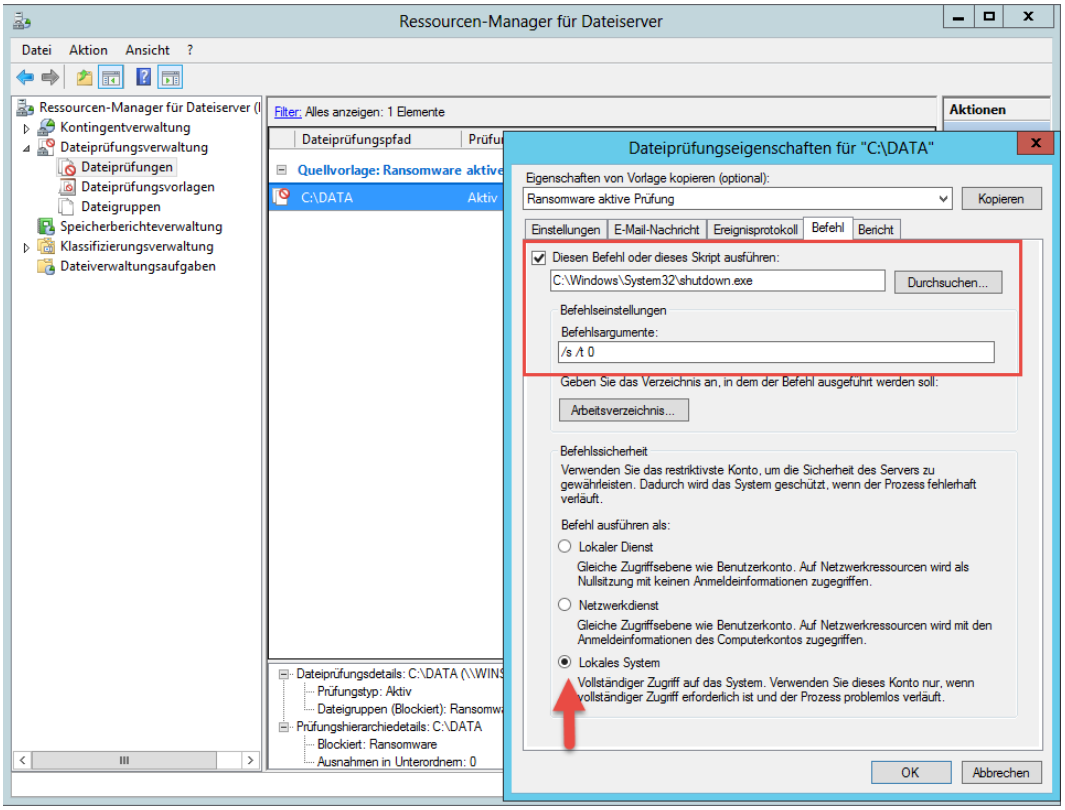
In der Detailansicht etwas deutlicher zu erkennen. Durch wen, in welchen Pfad und Server sowie ausgelöst durch welche Dateigruppe.



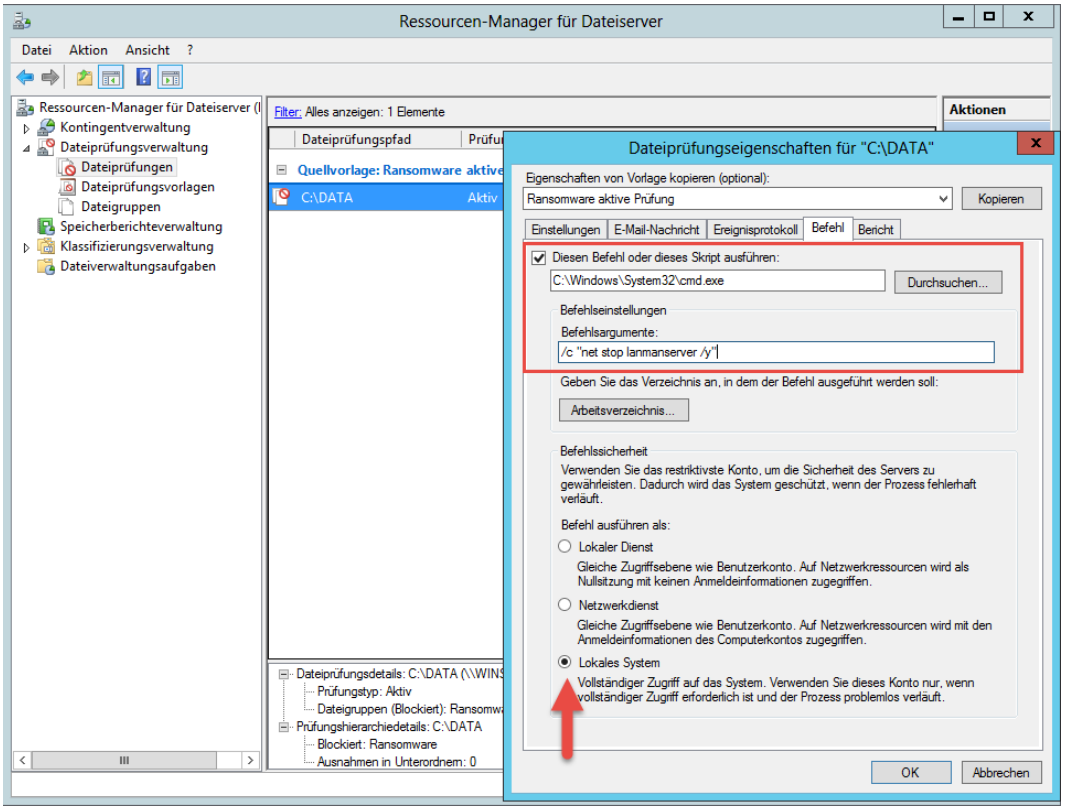
Wenn mit einem Monitoring-Tool wie z.B. Nagios gearbeitet wird, kann die Ereignis ID 8215 überwacht werden.

File Server auf Ransomware-Dateien prüfen

Als weitere Schutzmaßnahme kann man den Server auch direkt herunterfahren lassen, bevor schlimmeres passiert,



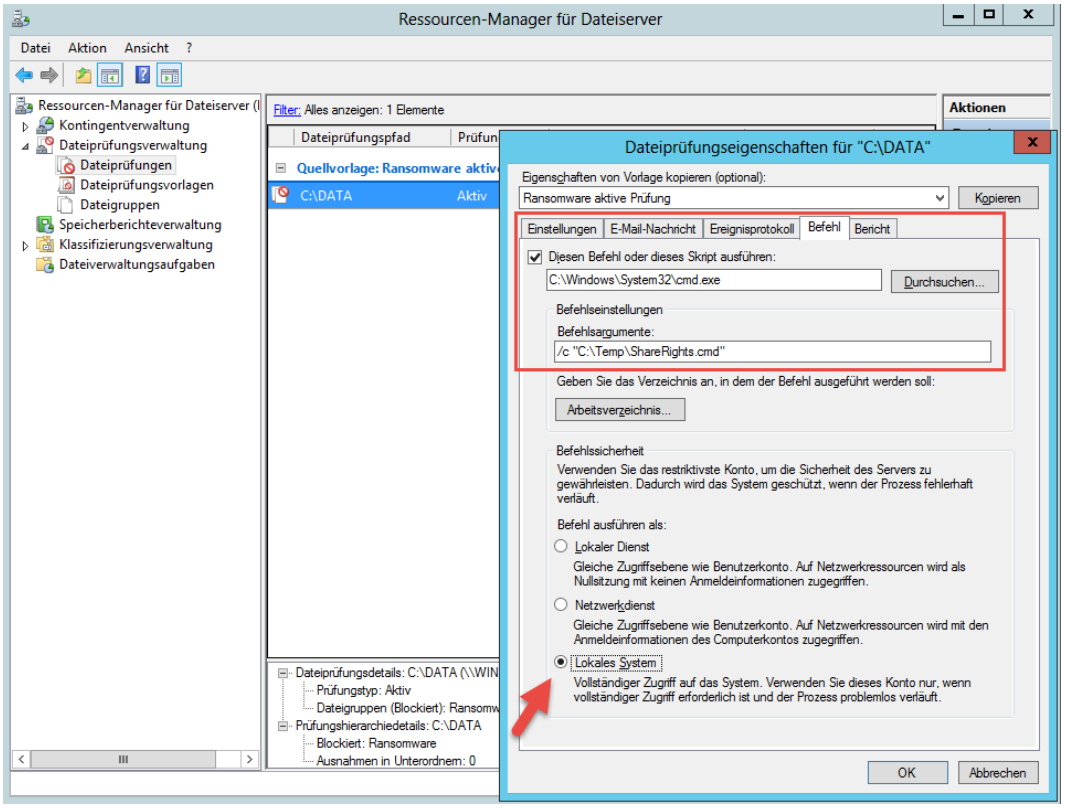
…oder man stoppt die Bereitstellung der Shares.



File Server auf Ransomware-Dateien prüfen

Update: 08.05.2016

Eine weitere Alternative ist der Entzug der Berechtigung auf eine Freigabe mittels Skript. Diese Idee kommt von http://www.netwrix.com/



Crypto Dateiendungen.txt

Powershell.txt