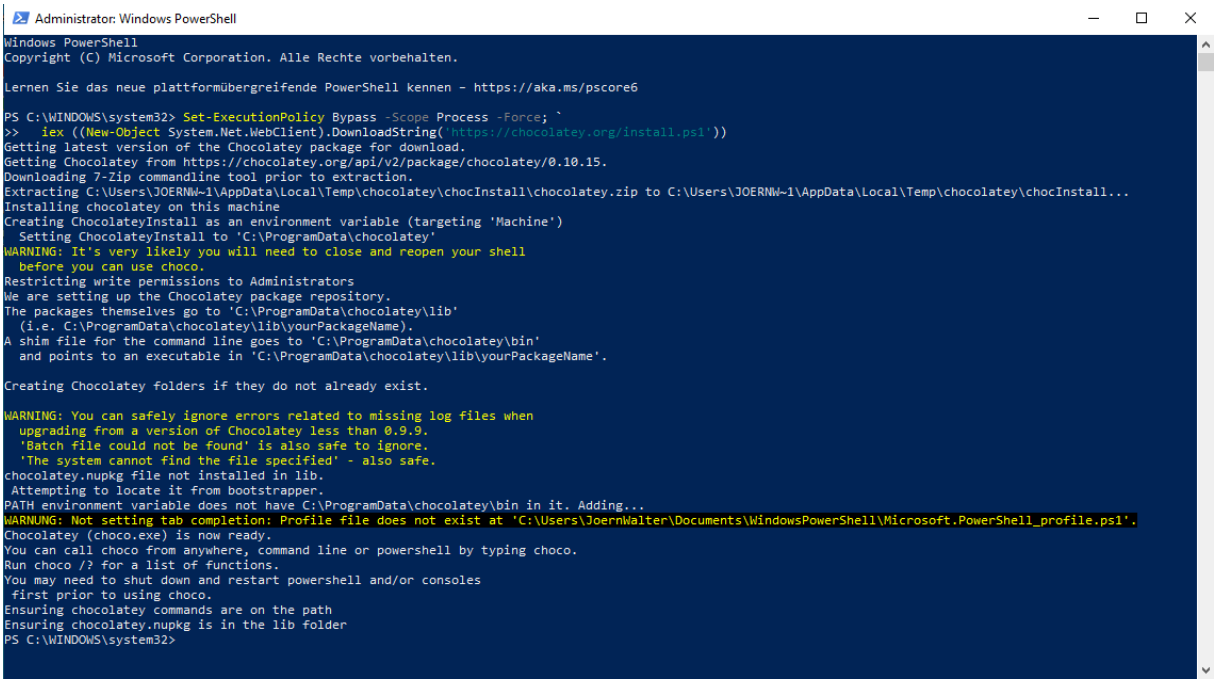
DNS-Abfragen protokollieren

Sysmon (System Monitor) ist ein zeitgleich ein Systemdienst und Treiber, der nach der Installation immer aktiv bleibt. Sysmon überwacht alle Systemaktivitäten und schreibt diese ins Windows Ereignisprotokoll.

Neuinstallation von Sysmon

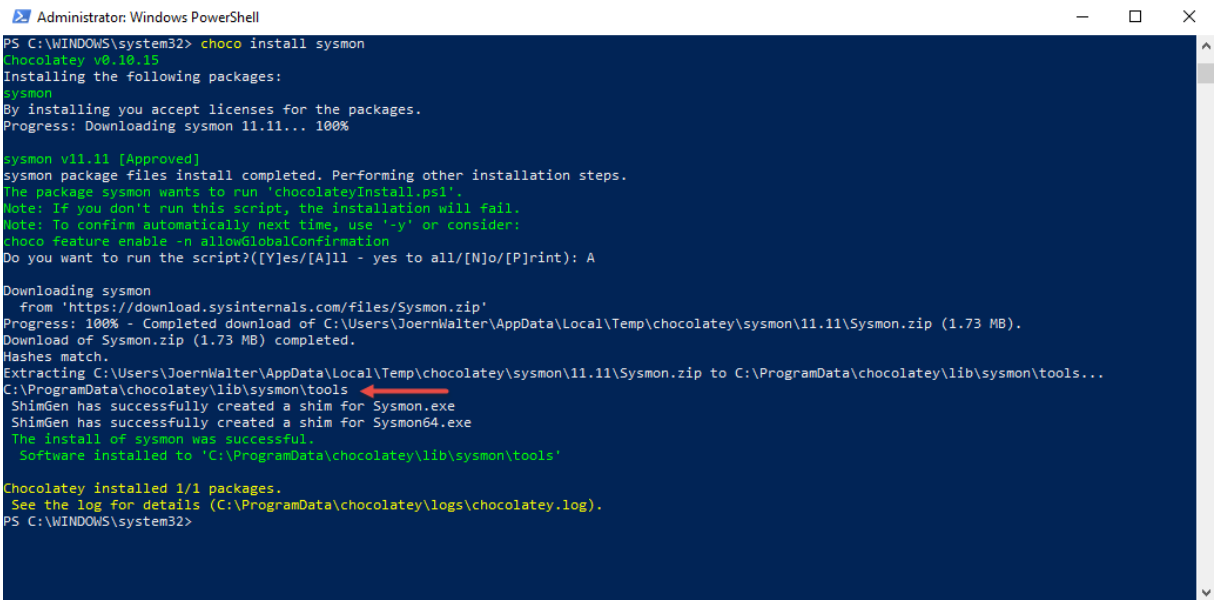
Set-ExecutionPolicy Bypass -Scope Process -Force; `

Invoke-Expression ((New-Object System.Net.WebClient).DownloadString('https://chocolatey.org/install.ps1'))



choco search sysmon
choco install sysmon

Sysmon wurde heruntergeladen und ist bereit zur Nutzung.

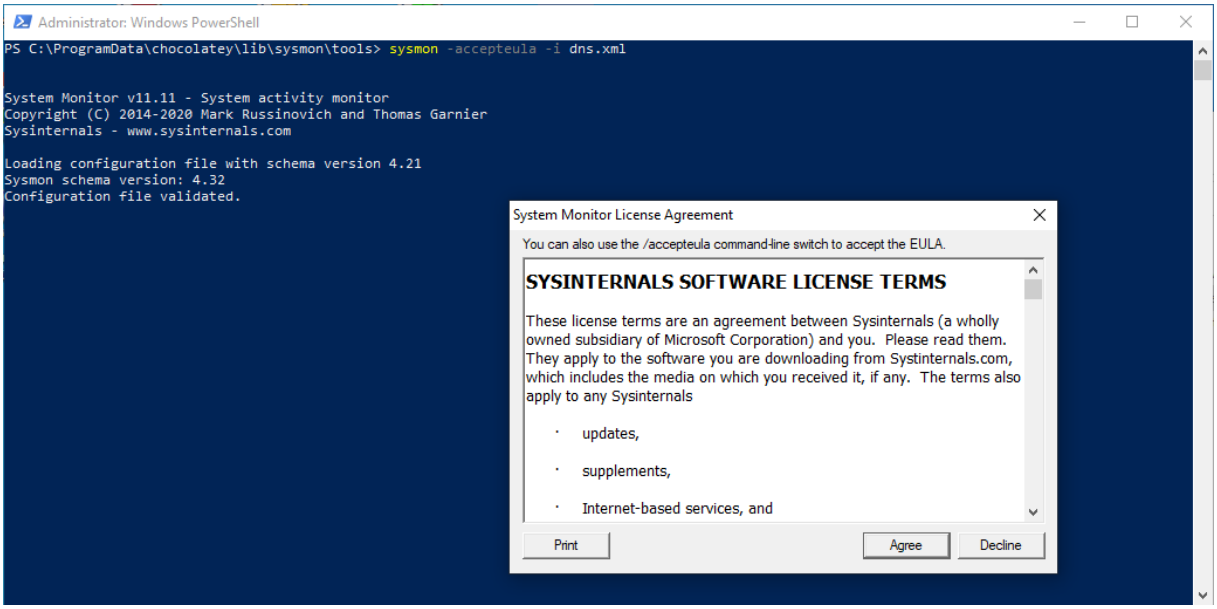


Alternativ kann man Sysmon auch von Microsoft direkt herunterladen.

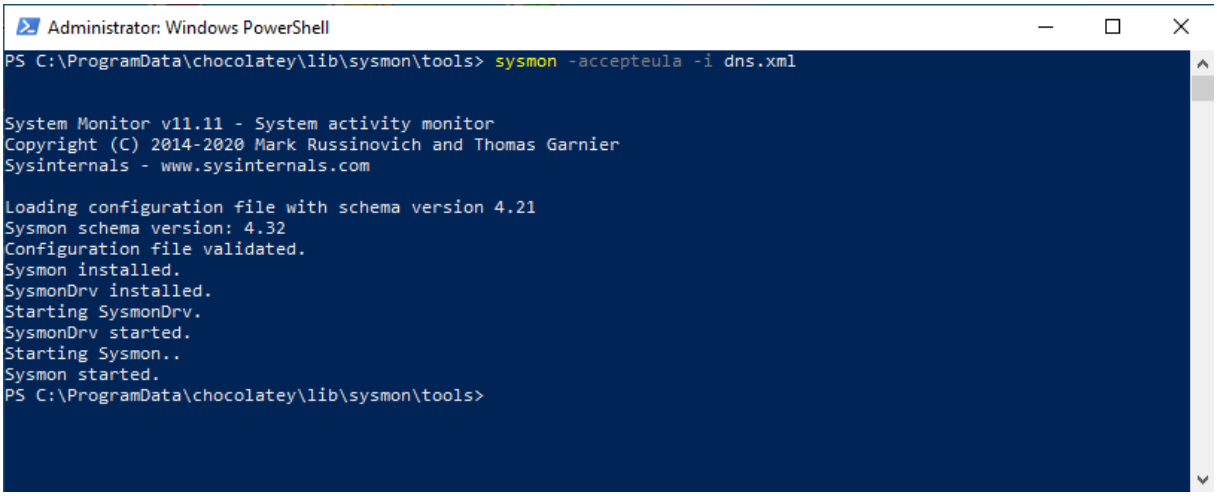
DNS-Abfragen protokollieren

https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Wechseln in den Installationspfad „**C:\ProgramData\chocolatey\lib\sysmon\tools**“ und installieren SYSMON nun mit einer voreingestellten Konfigurationsdatei, die nur DNS-Abfragen ins Protokoll schreibt.

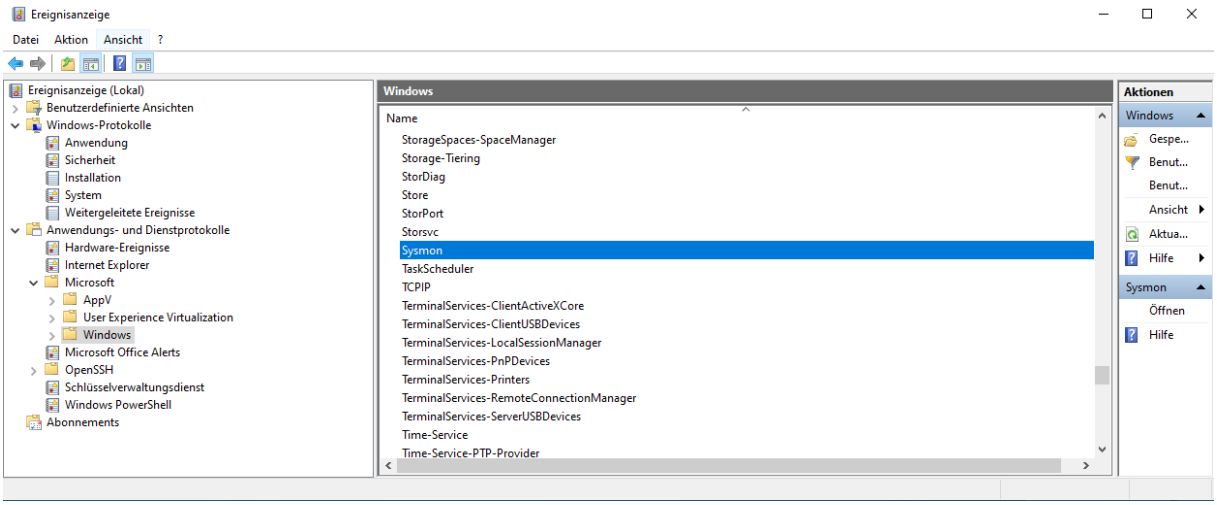


sysmon –accepteula –i dns.xml



DNS-Abfragen protokollieren

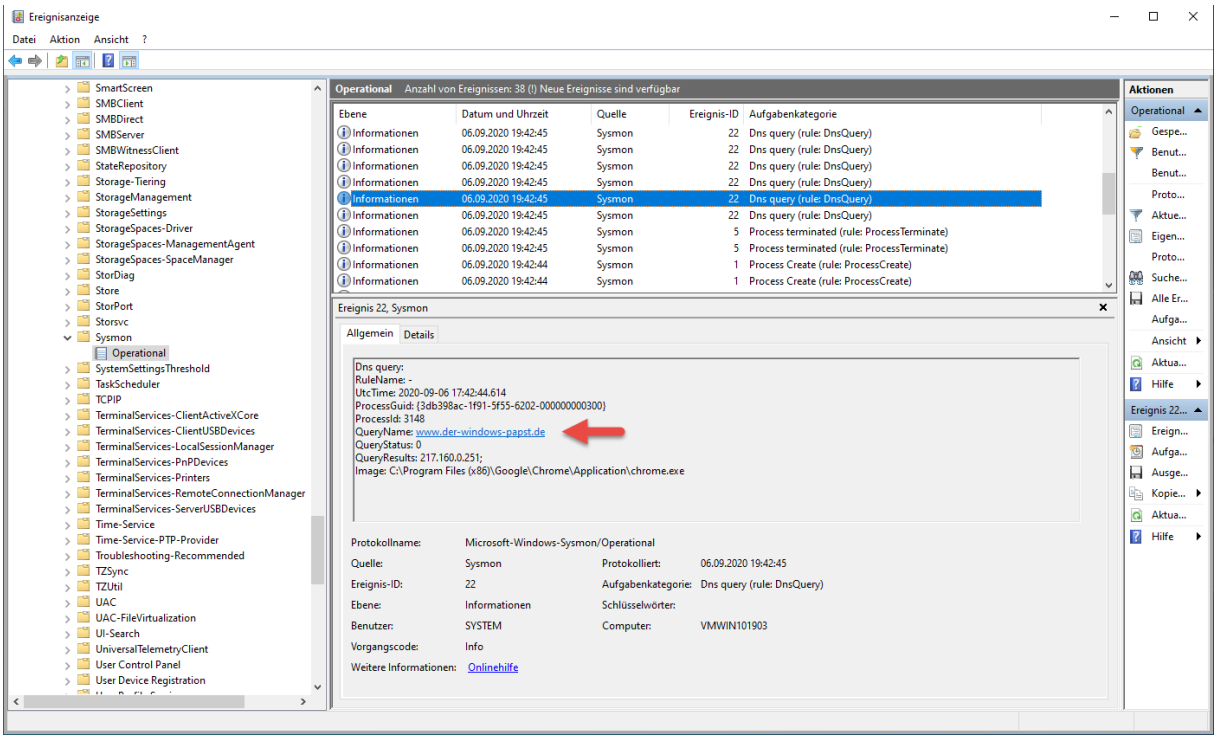
Nach der erfolgreichen Installation finden wir in der Ereignisanzeige nun den neuen Order Sysmon. Sysmon protokolliert ab sofort jede DNS-Abfrage.



Die Ereigniseinträge finden wir unter:

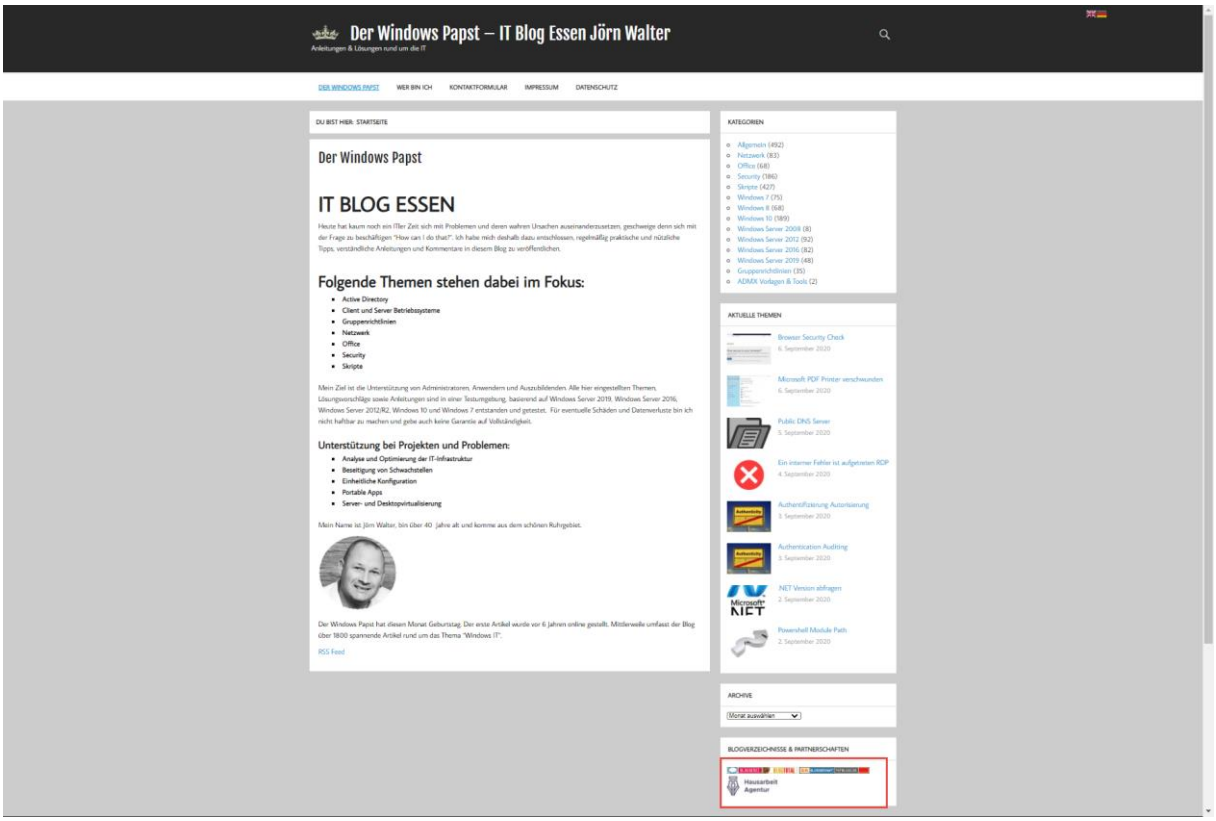
Anwendungen und Dienste / Microsoft / Windows / Sysmon / Operational

Öffne ich nun z.B. den Google Chrome und die Webseite „Der Windows Papst" finden wir nun z.B. alle DNS-Abfragen rund um die Webseite https://www.der-windows-papst.de.

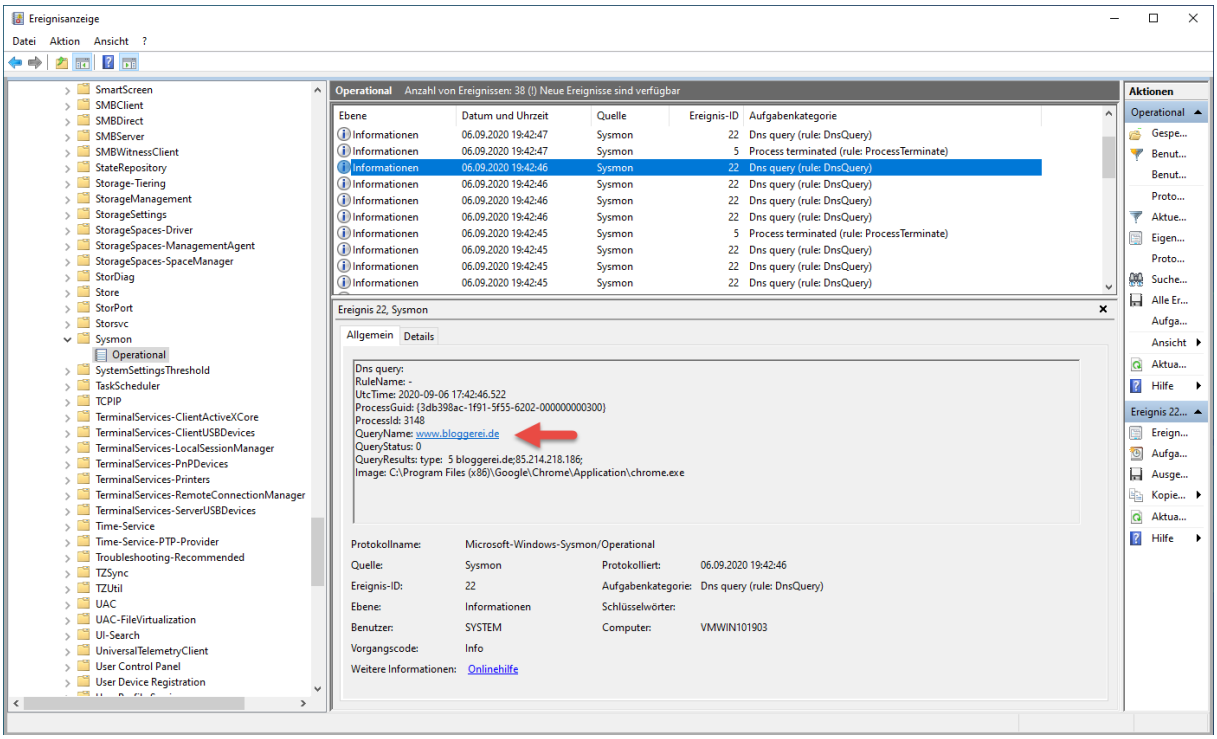


DNS-Abfragen protokollieren

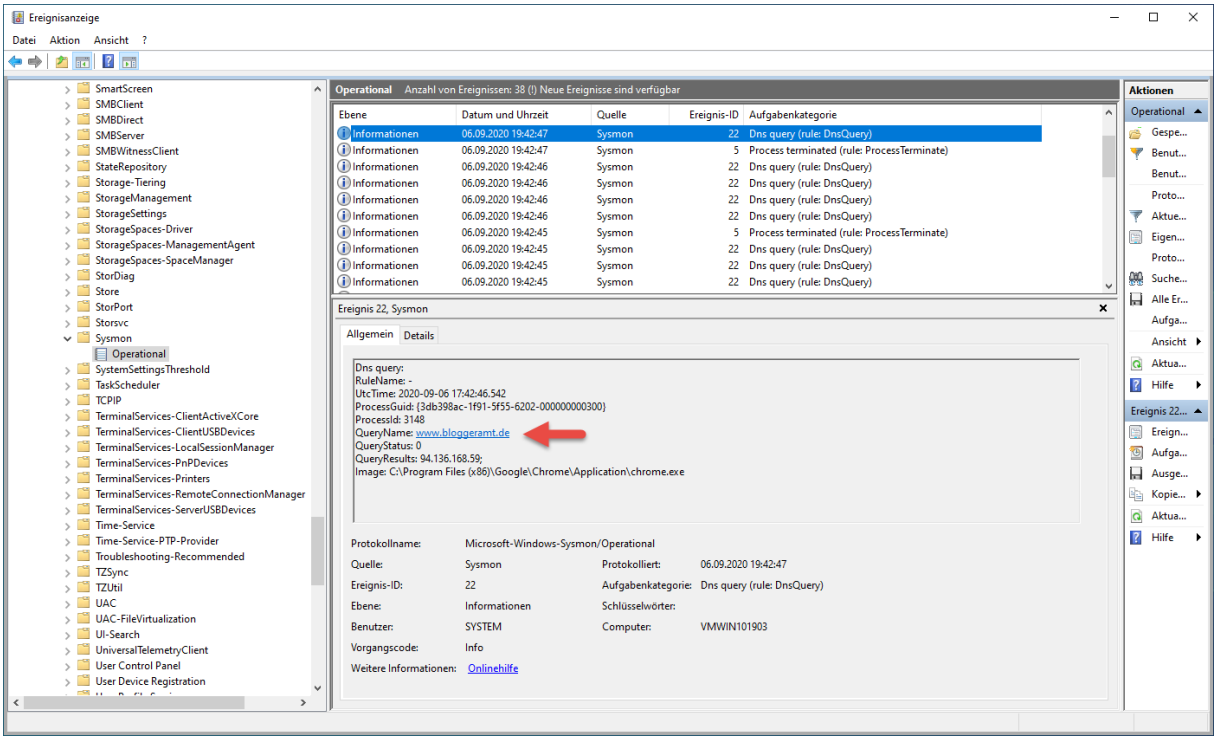
Da ich auf meiner Hauptseite ein paar Verlinkungen habe (unten links), werden diese durch den Browser angefragt und aufgelöst.

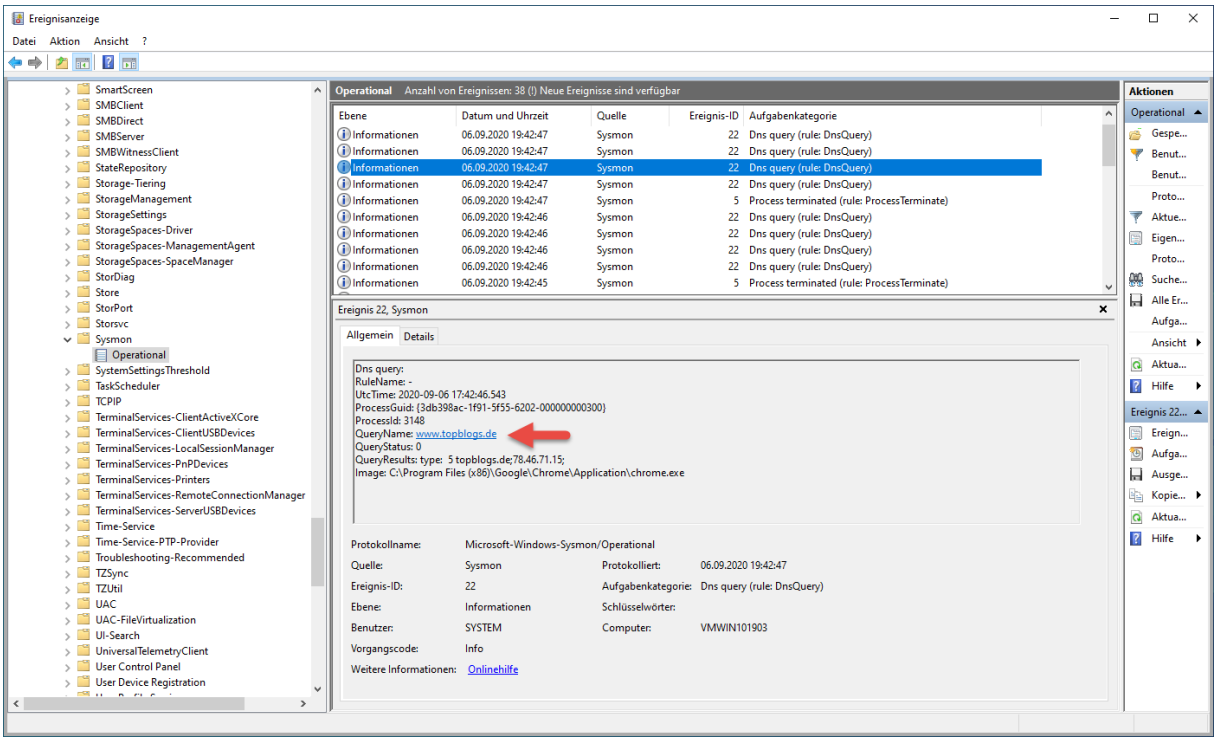


4 Beispiele infolge…



DNS-Abfragen protokollieren

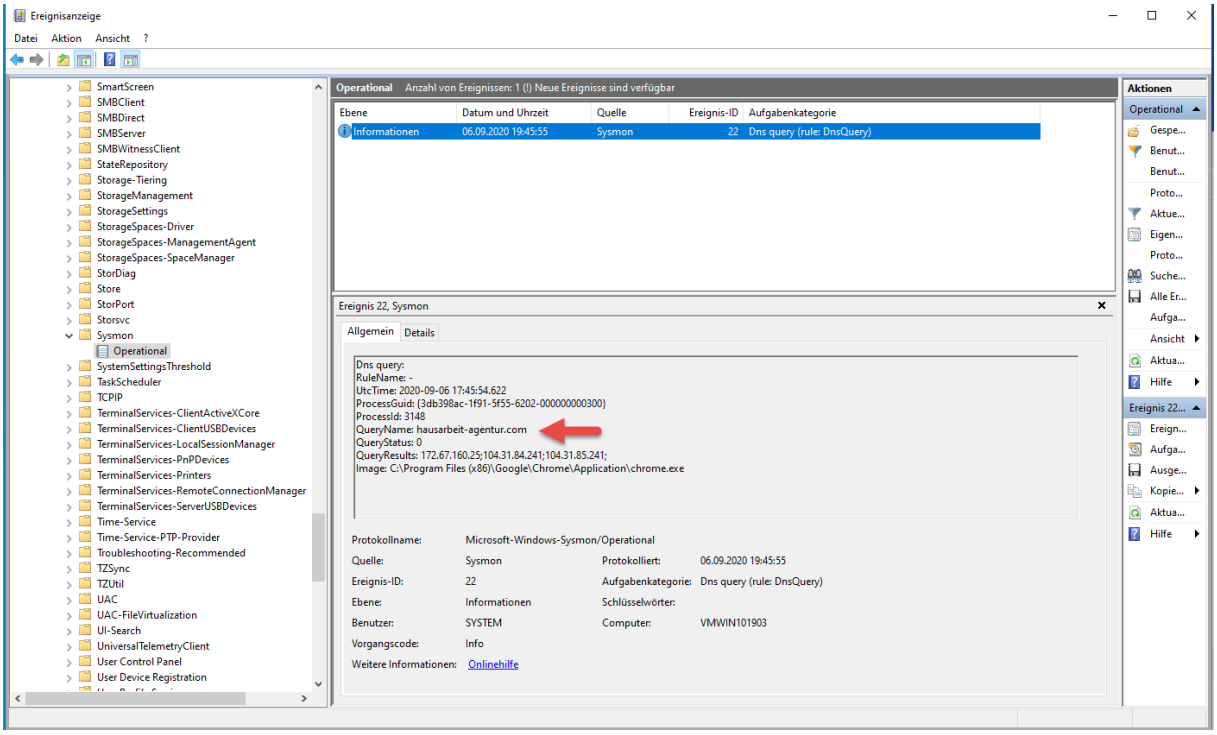




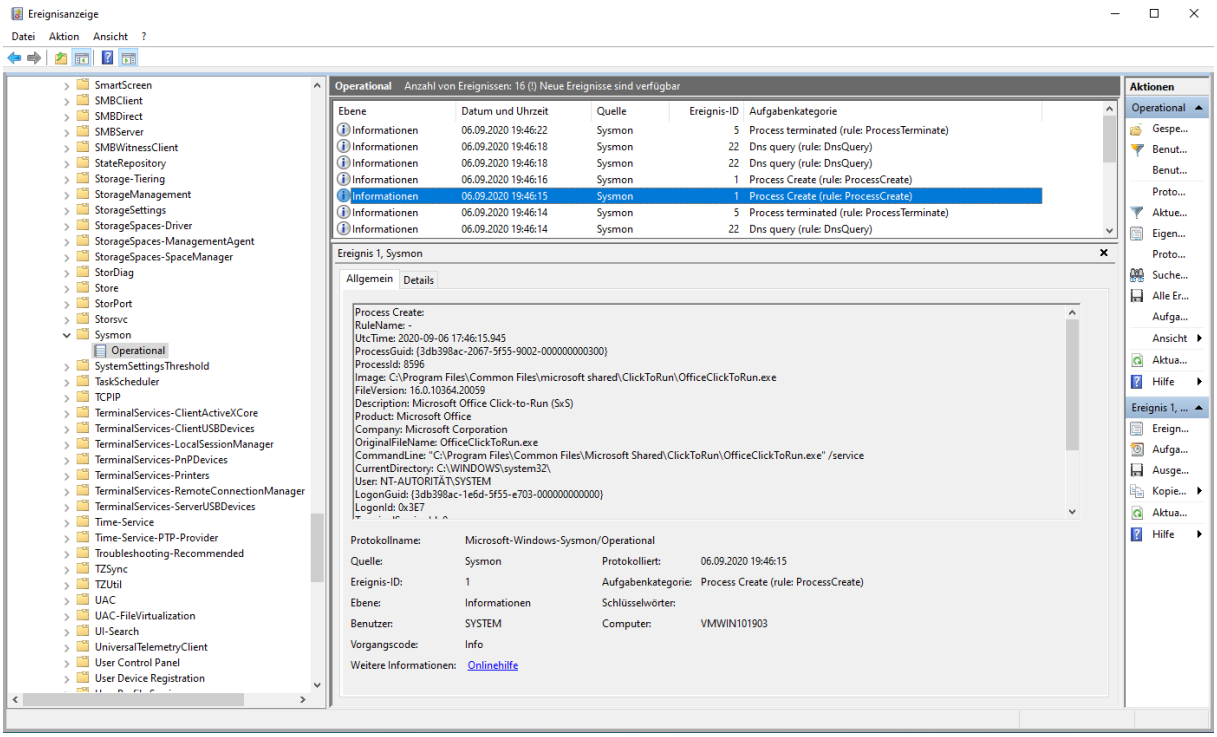
Erstellt von Jörn Walter **06.09.2020**

DNS-Abfragen protokollieren

Klicke ich z.B. auf den Link von Hausarbeit, wird auch dieser versucht aufzulösen.



Auch die auf dem System laufenden Anwendungen und Aufgaben werden entsprechend ins Protokoll geschrieben.



Wenn Sysmon bereits installiert ist, dann laden wir nur noch die DNS-Konfiguration.

sysmon.exe -c dns.xml