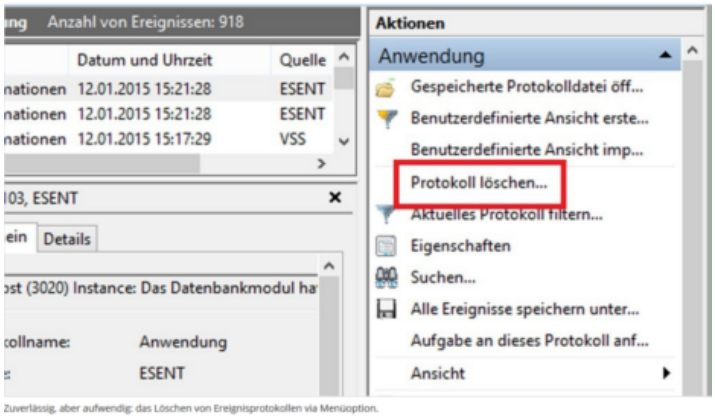
Windows 7/8/10: Ereignisanzeige manuell oder automatisch löschen

Was haben Sie gestern am Rechner gemacht? Ein Werkzeug des Betriebssystems erteilt Ihnen – aber auch Schnüfflern – entsprechend Auskunft. Wer bestimmte Protokolle regelmäßig löscht, ist davor geschützt.

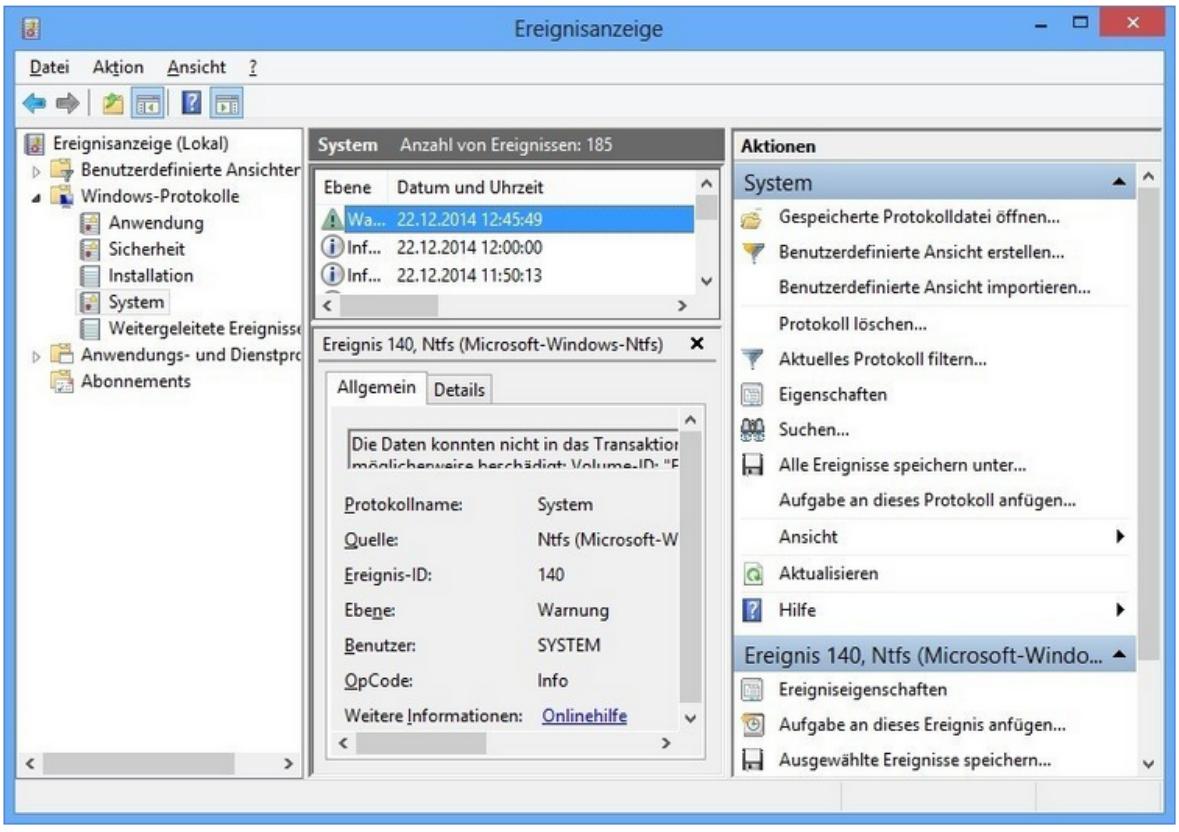
Die Ereignisanzeige von Windows existierte schon zu XP-Zeiten, sie steckt außerdem in Windows 7, 8(.1) und 10 – und ist trotzdem weitgehend ungenutzt. Der Grund hierfür ist, dass Microsoft das System-Bordmittel nicht einfach zugänglich gemacht hat. Obwohl kaum bekannt, hat es die Ereignisanzeige in sich: Darin protokolliert Windows vieles, was Sie am PC machen. Wann etwa das Hochfahren erfolgte, ist im Tool aufgeführt. Auch aufgetretene Software-Fehler sind darin zu finden. Wer vor Spionage sicher sein will, löscht etwaige verräterische Datensätze. Wahlweise geschieht das manuell oder via exklusivem Spezial-Programm.

Ereignisanzeige: Protokolle löschen

Zuverlässig, aber aufwendig: das Löschen von Ereignisprotokollen via Menüoption.

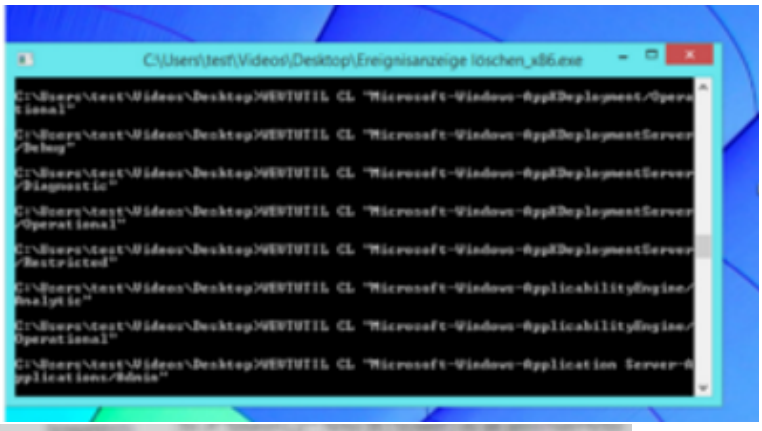


Egal, auf welche Weise eine andere Person auf Ihren PC zugreift: Wer die nötigen Kenntnisse hat, öffnet die Ereignisanzeige, schaut sich deren Inhalte an und spioniert Sie so aus. Um verräterische Protokolle händisch zu beseitigen, starten Sie zunächst die Ereignisanzeige: Hierzu die **Windows-Taste und R** drücken, **eventvwr** eintippen und auf OK klicken. Eine eventuelle Warnmeldung der Benutzerkonten-Steuerung ist mit Ja zu bestätigen. Zum Aufruf der Ereignisanzeige tippen Sie alternativ **eventvwr.msc** ein. Beide Kommandos akzeptiert übrigens auch die Startmenü-Suche. Über die Kategorien im linken Fensterbereich navigieren Sie zu den verschiedenen Datensätzen. Wer rechts auf Protokoll löschen klickt und dann Leeren wählt, beseitigt die eingeblendeten Spuren.

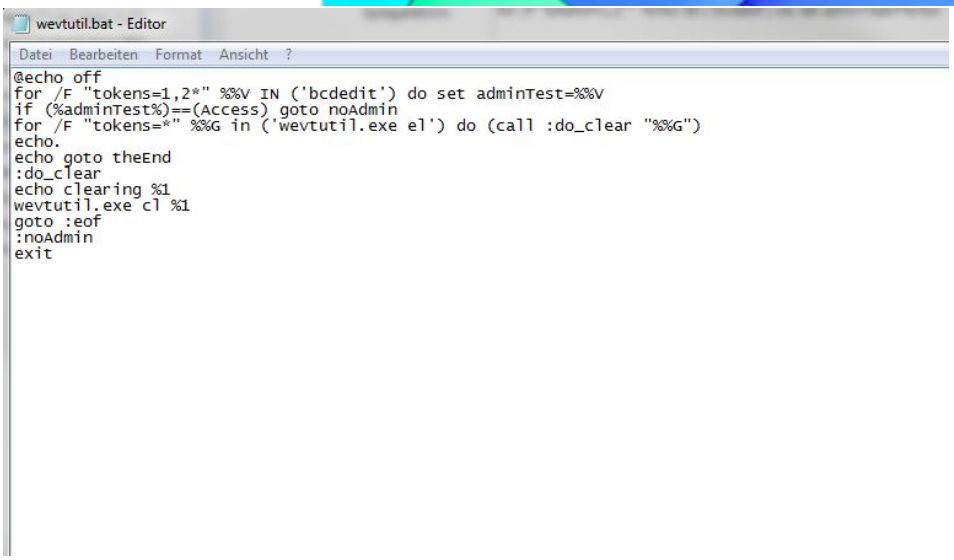


Nachteil der beschriebenen Methode: Um sämtliche Protokolle zu löschen, ist es nötig, die Schritte für jede einzelne Kategorie der Ereignisanzeige zu wiederholen. Das nervt – insbesondere, wenn Sie etwa eine wöchentliche Bereinigung wünschen.

Alternativ: Alle Ereignisprotokolle unter Windows löschen



So klappt das Aufräumen deutlich schneller. Ein exklusives Tool fegt verräterischen Ballast blitzschnell weg. Möchten Sie die Ereignisprotokolle nicht einzeln entfernen, können Sie sie mit einer Batch-Datei automatisch leeren. Erstellen Sie dazu ein Textdokument mit dem folgenden Inhalt (siehe Bild) und benennen Sie Datei in "Ereignisanzeige.bat" um.



Hier in Textform (mit Ergänzungen, die freundlicherweise von Günter Immisch bereitgestellt wurden):

```
@echo off
COLOR 1E
for /F "tokens=1,2*" %%V IN ('bcdedit') do set adminTest=%%V
if (%adminTest%)==(Access) goto noAdmin
for /F "tokens=*" %%G in ('wevtutil.exe el') do (call :do_clear "%%G")
echo.
echo goto theEnd
:do_clear
echo clearing %1
wevtutil.exe cl %1
goto :eof
:noAdmin
echo.
echo.
echo Alle Ereignisse der Ereignisanzeige wurden gelöscht.
echo.
echo.
pause
```

Kopieren Sie den blau markierten Text in die Zwischenablage und fügen ihn anschließend im Windows-Editor ein. Speichern Sie als Ereignisanzeige.bat.
Klicken Sie anschließend mit der rechten Maustaste auf die Batch-Datei und wählen Sie den Eintrag "Als Administrator ausführen". Dann öffnet sich ein Konsolen-Fenster, über das automatisch alle Daten gelöscht werden. Das geöffnete Programmfenster schließt sich am Ende wieder.