Die Windows-Ereignisanzeige

2015 V 2

Kennen Sie das…

Ihr PC

- startet sehr langsam
- braucht eine längere Zeit beim Herunterfahren
- hängt sich oft aus
- Programme starten nicht richtig

Dann sollten Sie Ihren PC mit der Ereignisanzeige überprüfen!

Was ist die Ereignisanzeige?

Die Ereignisanzeige ist das Sammelbecken aller PC-Aktivitäten und ist ab Windows NT als wichtiges Diagnosetool auf Ihrem PC.

Vom Hochfahren bis zum Herunterfahren des PCs protokolliert Windows **alle** Ereignisse.

- Beispiele:
  - Wann wurde der PC zuletzt benutzt?
  - Programmfehler
  - Treiberfehler

Mit Hilfe der Ereignisanzeige können Fehler im Betriebssystem oder Anwendungen lokalisiert werden

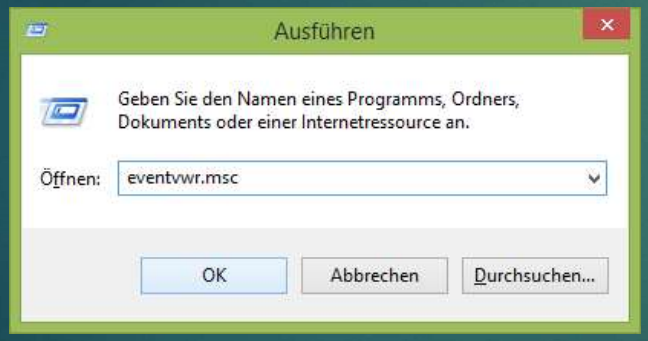
Die Darstellung der Ereignisanzeige hat sich zu Windows XP in Windows Vista, Windows 7 bzw. Windows 8.1 geändert.

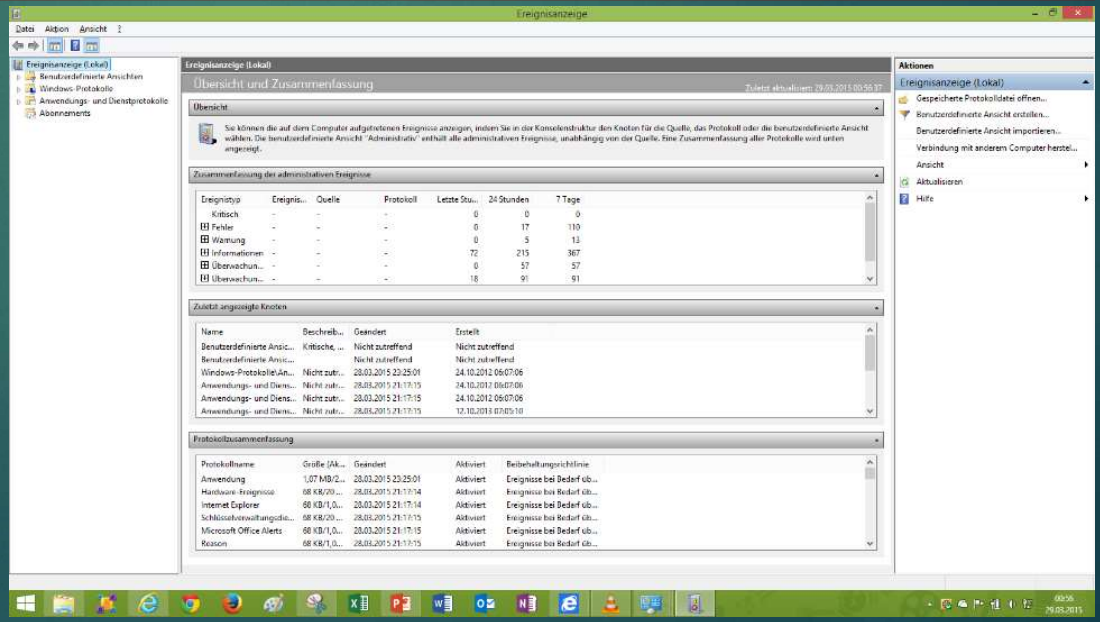
Wie wird die Ereignisanzeige gestartet?

Es geht auch mit der Tastenkombination:

Windows-Taste + [R]

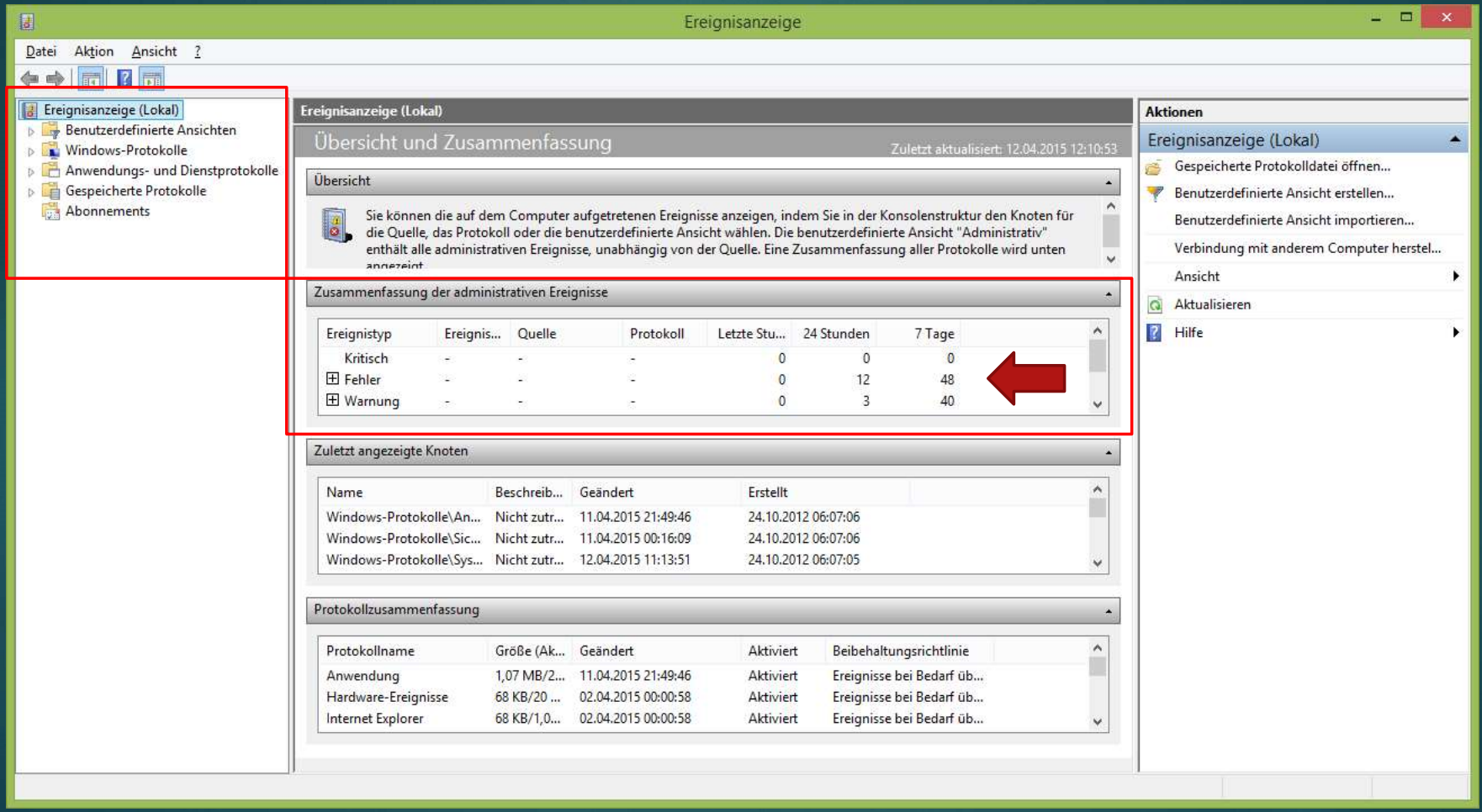
Tippen Sie dann ein: **eventvwr.msc**





Windows XP bis Windows 8.1

Ereignisanzeige



Öffnen Sie die Windows-Protokolle

Klicken Sie auf den kleinen Pfeil vor Windows-Protokolle

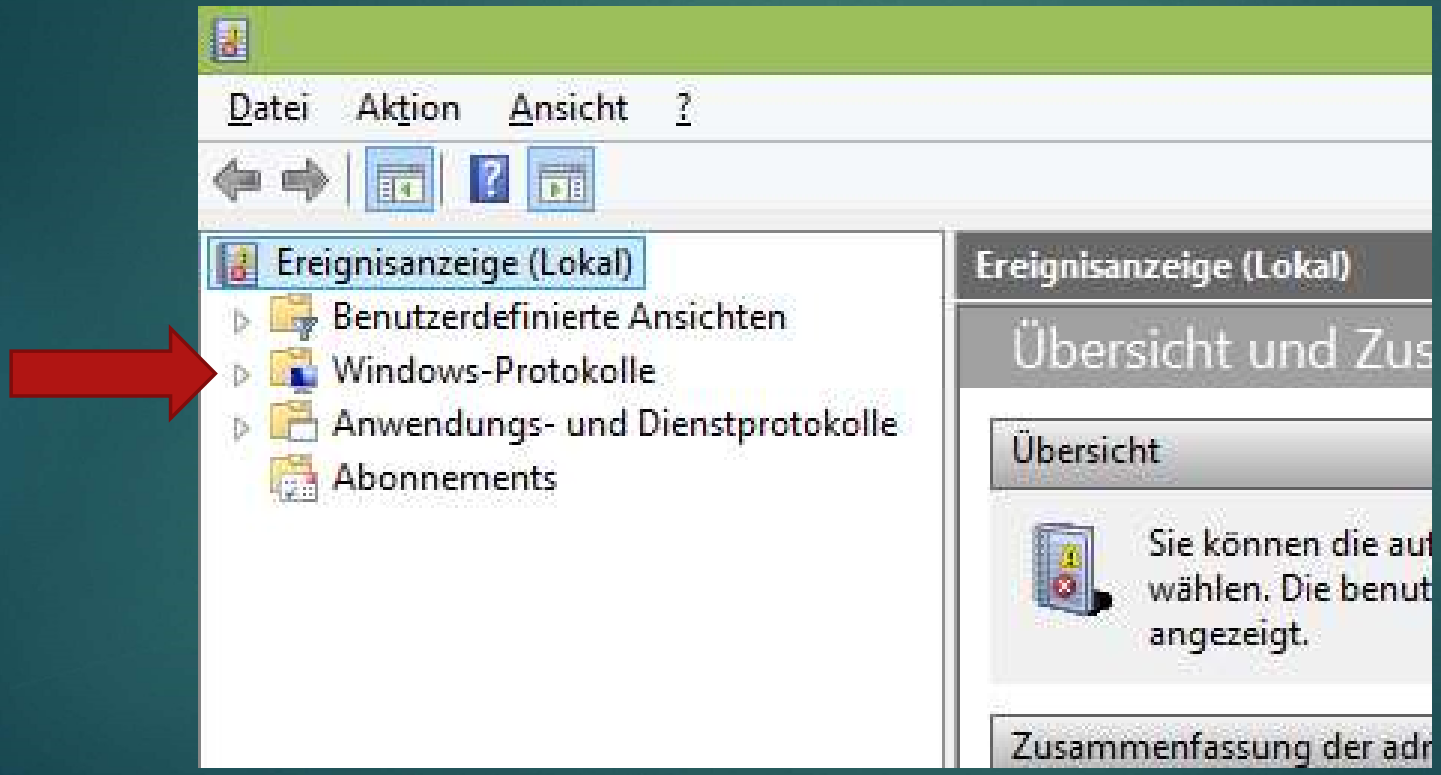
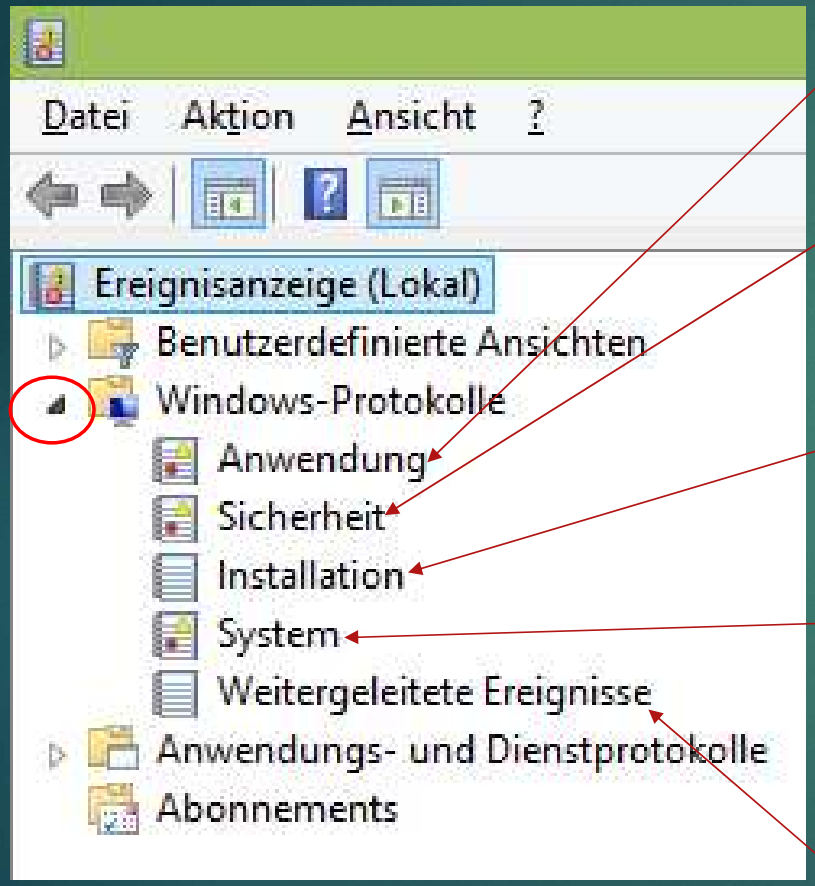


Abbildung: Windows Vista, Windows 7, Windows 8.1

Windows-Protokolle



Anwendung
Alle Ereignisse, die von Programmen und Tools ausgelöst werden

Sicherheit
Alle sicherheitsrelevante Ereignisse werden gespeichert. Auch erfolgreiche oder fehlgeschlagene Anmeldungen.

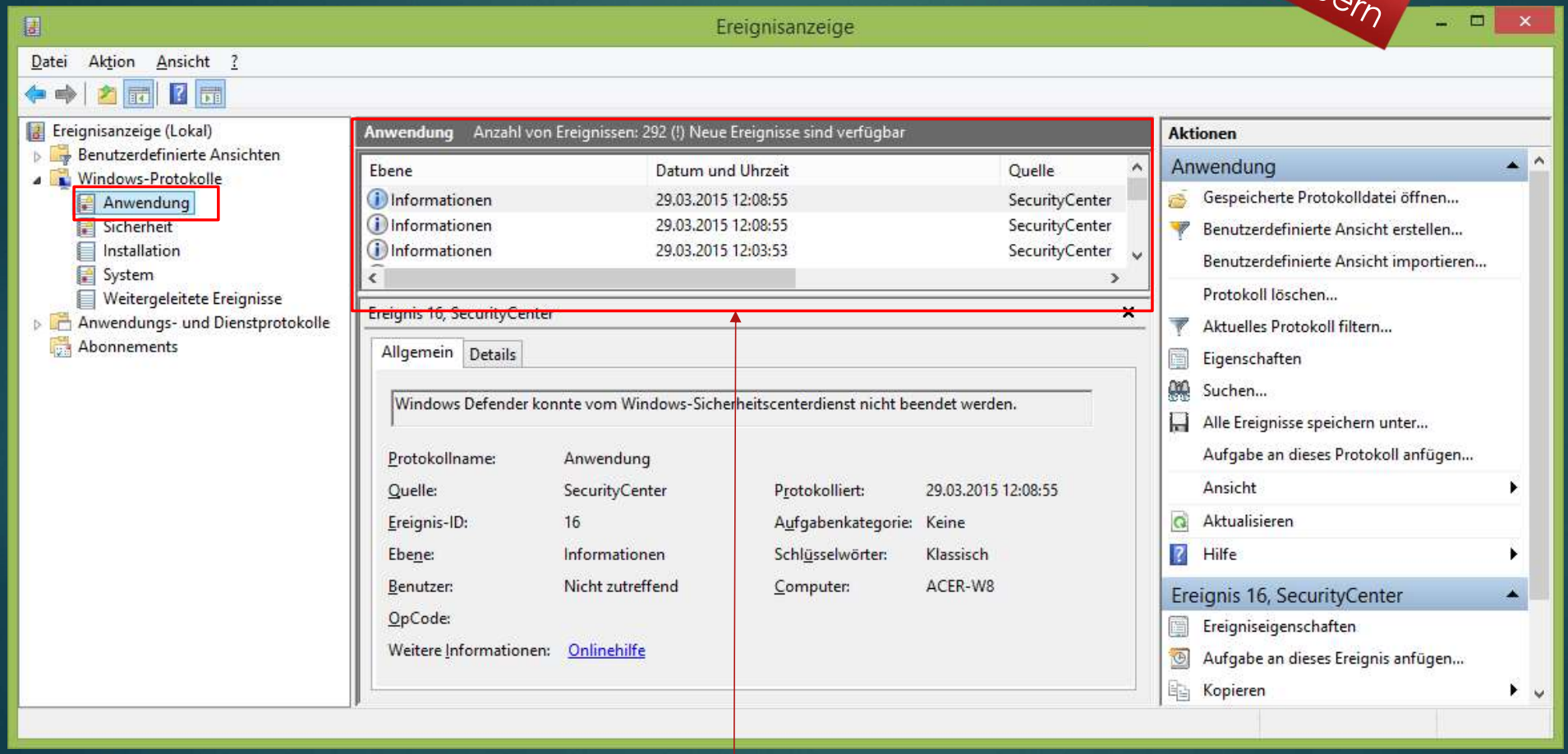
Installation
Alle Ereignisse, die beim Installieren von Programmen auftreten

System
Ereignisse, die von den Windows-Systemkomponenten Protokolliert wurden. Beispiel: Fehler beim Laden eines Gerätetreibers, Startfehler im Zusammenhang mit anderen Systemkomponenten

Weitergeleitete Ereignisse
Protokoll wird zum Speichern von Ereignissen bei Remote-Computer verwendet.

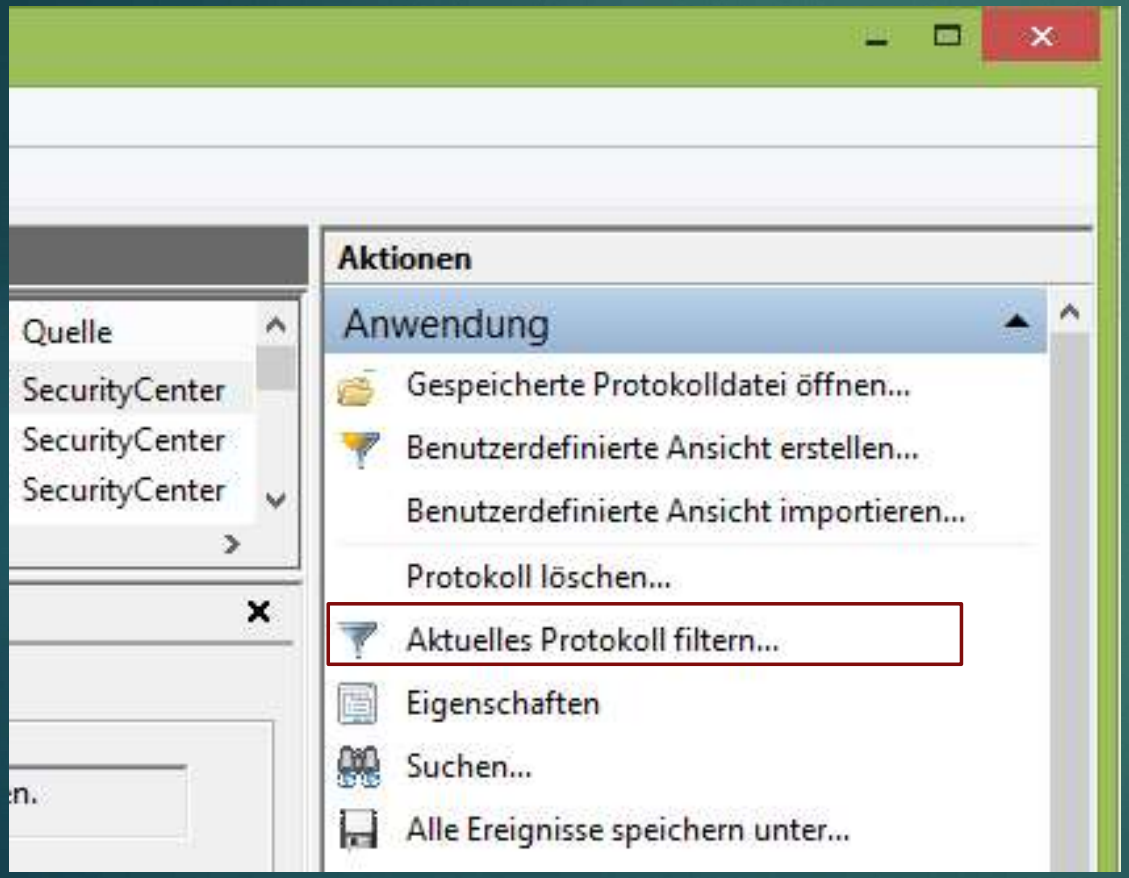
Klicken Sie auf **Anwendung**

Es kann etwas dauern



Windows listet nun alle Anwendungen auf

Aktuelles Protokoll filtern



Klicken Sie mit der **linken** Maustaste auf

Aktuelles Protokoll filtern…

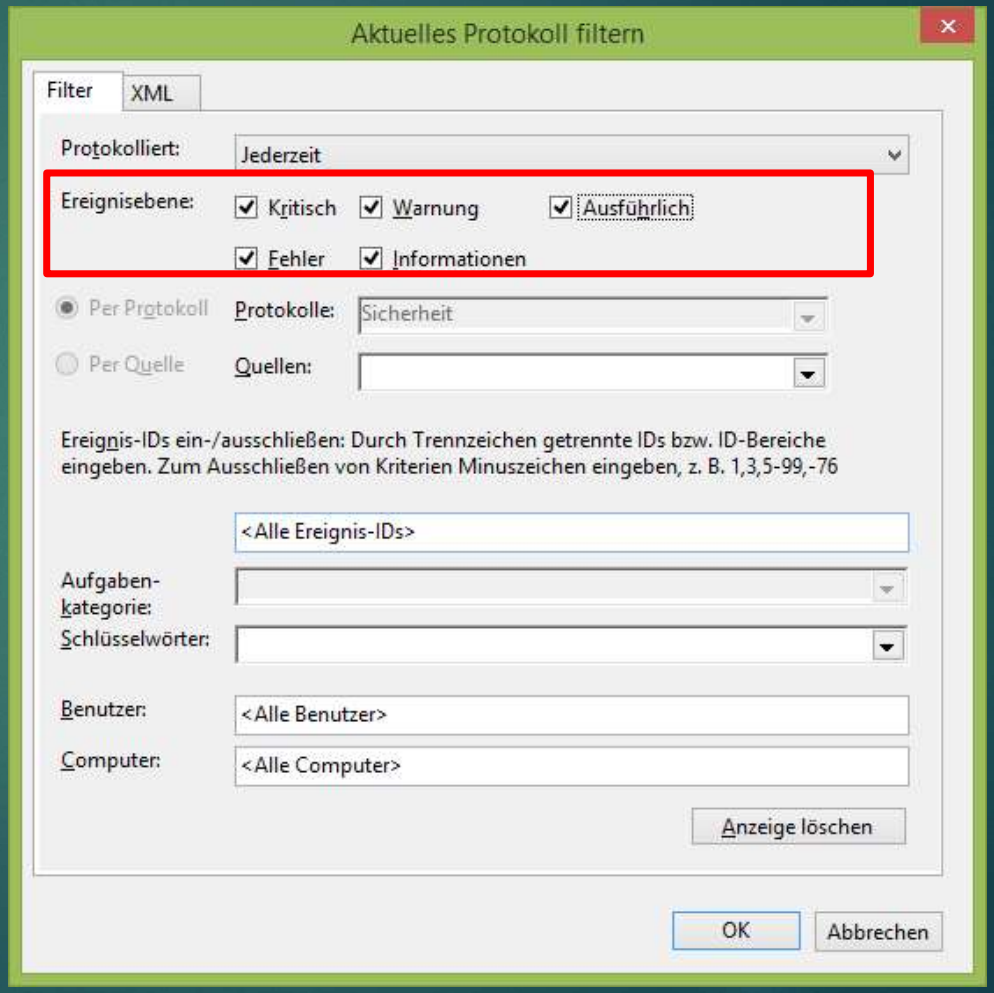
Das Protokoll unterscheidet 5 Ereignisebenen

Kritisch: Meldungen erhält man meist, wenn Windows abstürzt, einfach neu startet oder ein Hardware-Defekt vorliegt.

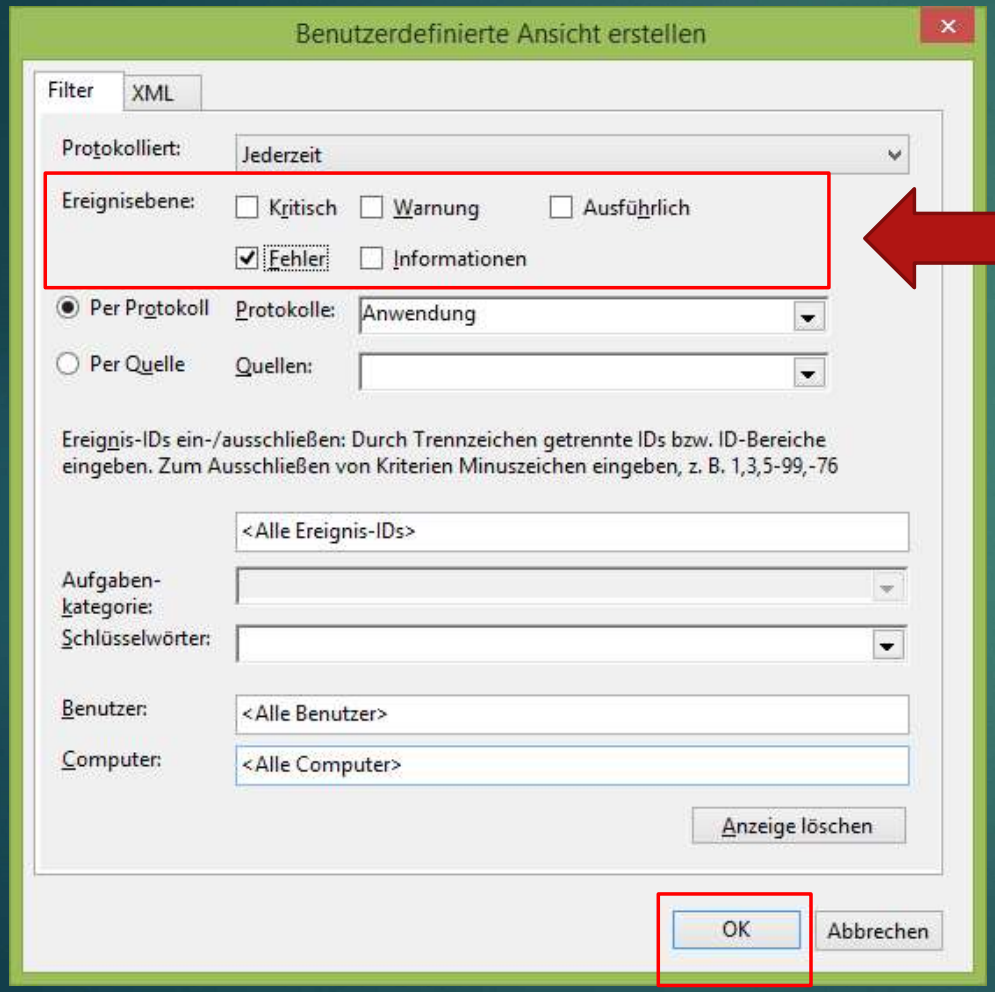
Fehler: Die Klassifizierung nimmt Windows vor, wenn beispielsweise ein Programm abstürzt, ein Dienst nicht geladen wird oder ein Hardware-Fehler vorliegt.

Warnung: Info über Probleme, etwa fehlgeschlagener Verbindungsaufbau, Datenverlust beim Schreibvorgang oder geringer Festplattenspeicher

Informationen: Reguläre Vorgänge – System- und Programmstart, Beendigung eines Dienstes, Abschluss einer Installation, Erfolgreiches Laden eines Netzwerktreibers



Aktuelles Protokoll filtern: Fehler



Aktivieren Sie unter **Ergebnisebene** nur **Fehler.**

Klicken Sie dann mit der **linken** Maustaste auf **OK**.

Es wurden 4 Fehler gefunden

Was sind das für Fehler?

Führen Sie einen Doppelklick auf eine Fehlermeldung auf.

Die Ereignis-ID kennzeichnet einen Vorgang unter Windows. Die ID ist eine Zahl bis 5 Stellen. Mit dieser ID-Zahl kann man die Fehlerquellen einkreisen.

Nach dem Doppelklick öffnet sich das Fenster Ereigniseigenschaften

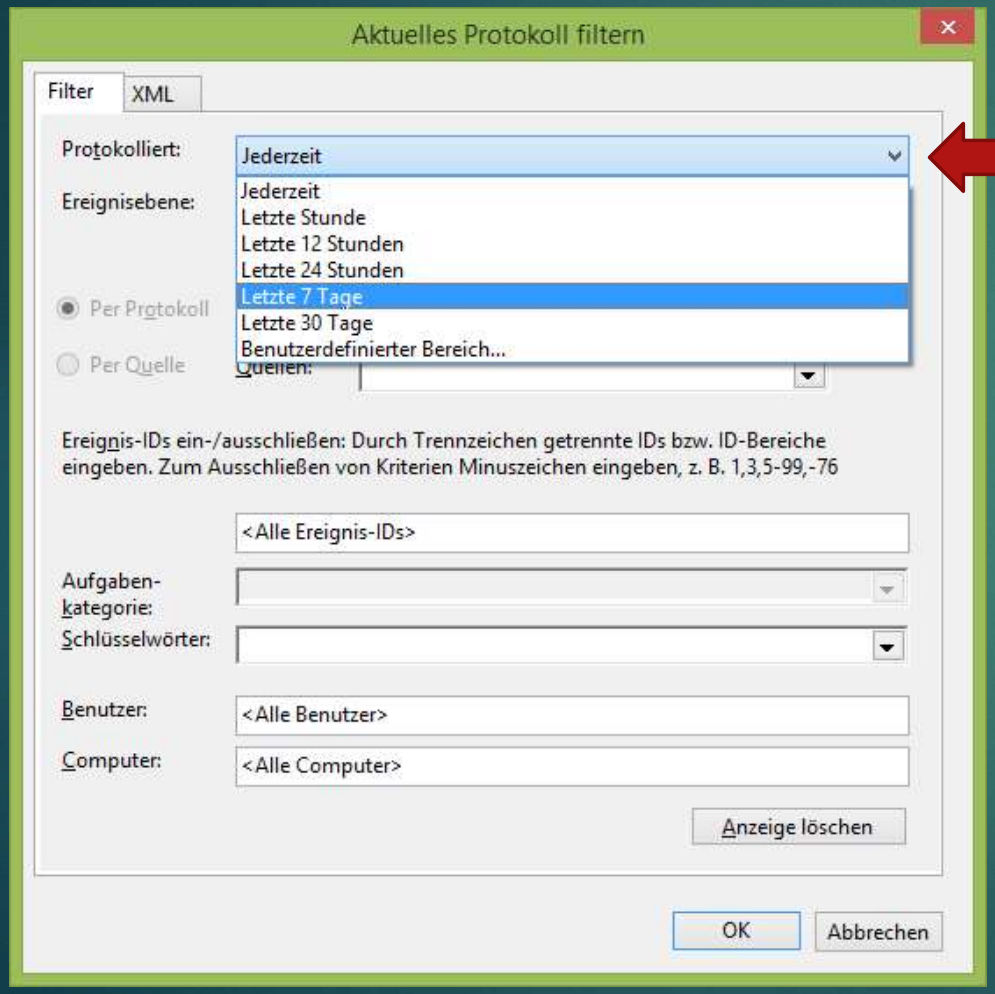
Hier finden Sie die Fehlerangaben

Später dazu mehr!

Windows-Protokoll Anwendung listet sehr viele Fehler auf > 50

Zeigt das Protokoll sehr viele Fehler an, dann sollten Sie den Protokoll-Zeitraum eingrenzen

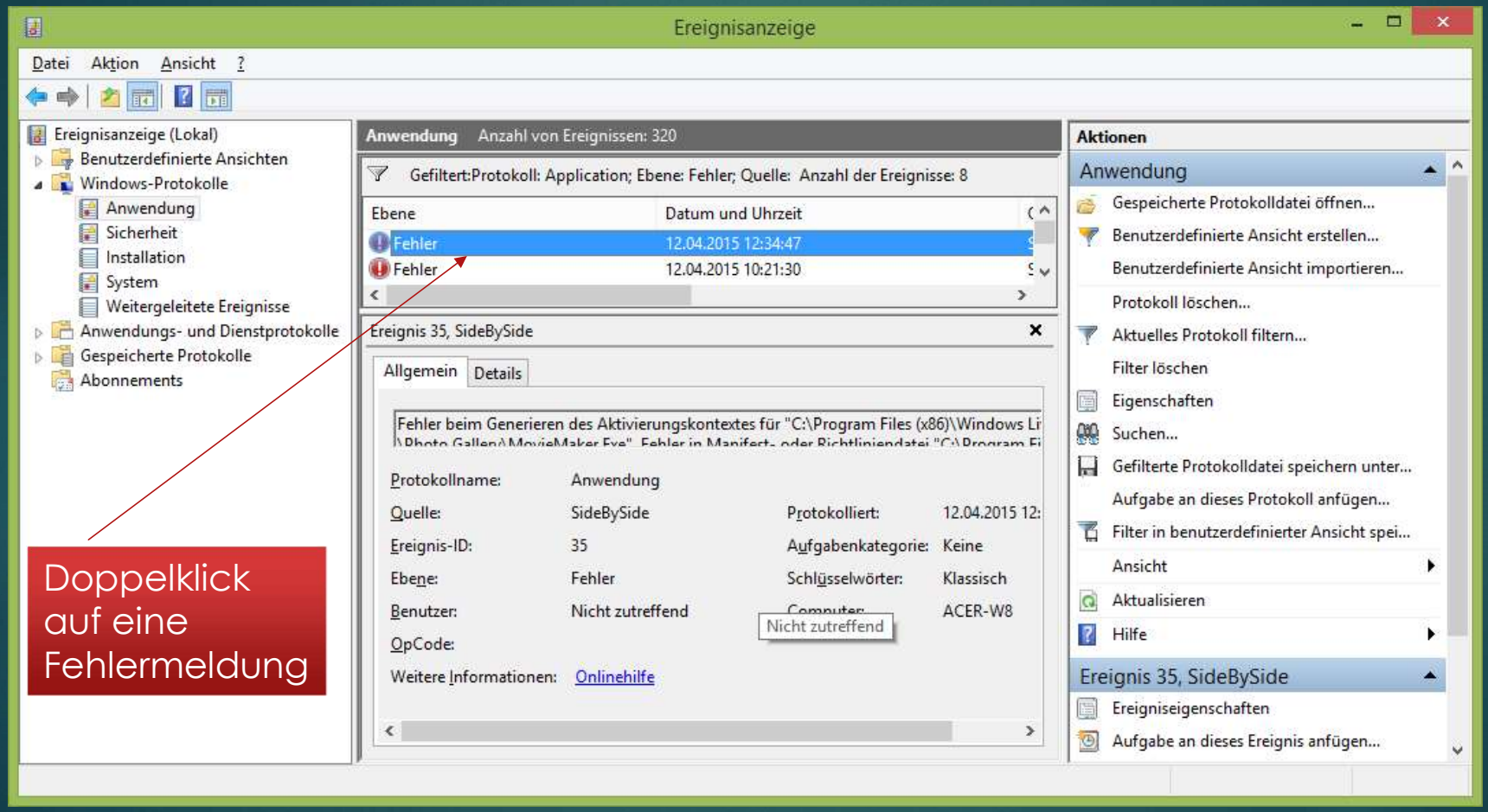
Aktuelles Protokoll filtern



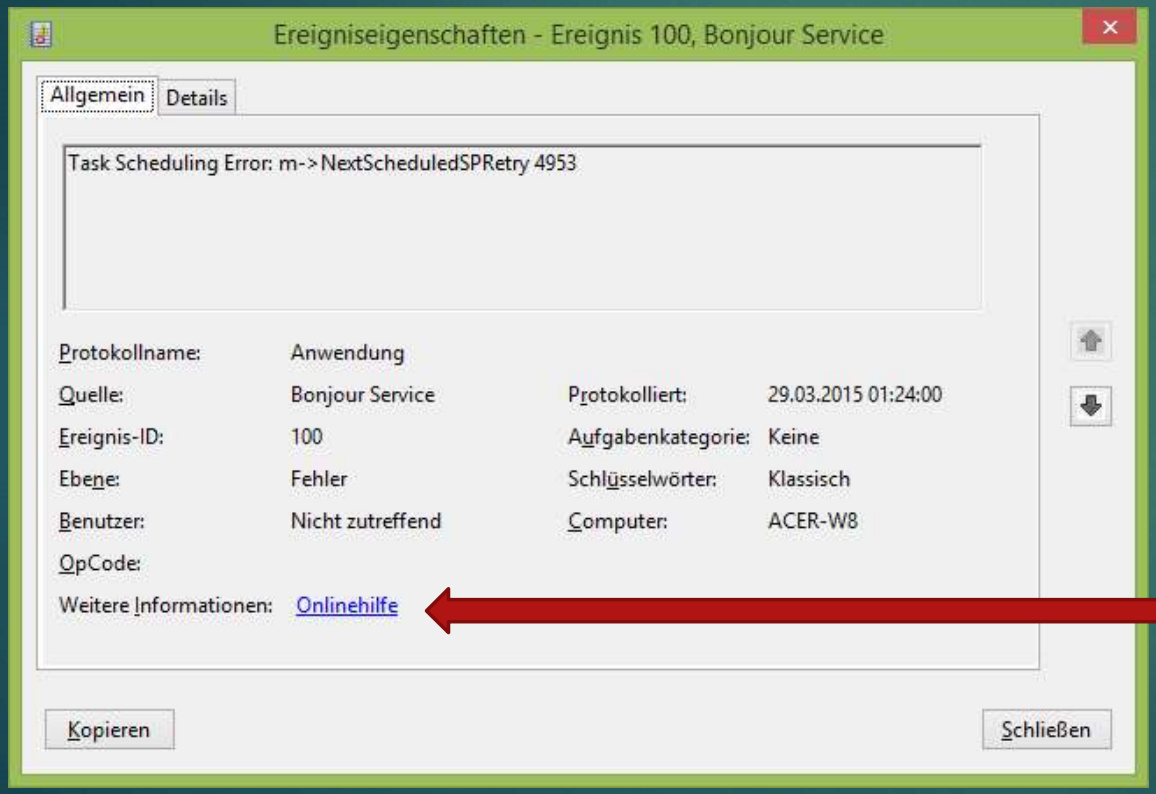
Stellen Sie hier den Zeitraum auf „**Letzte 7 Tage**“

Danach überprüfen Sie die Fehler.

Fehlerüberprüfung



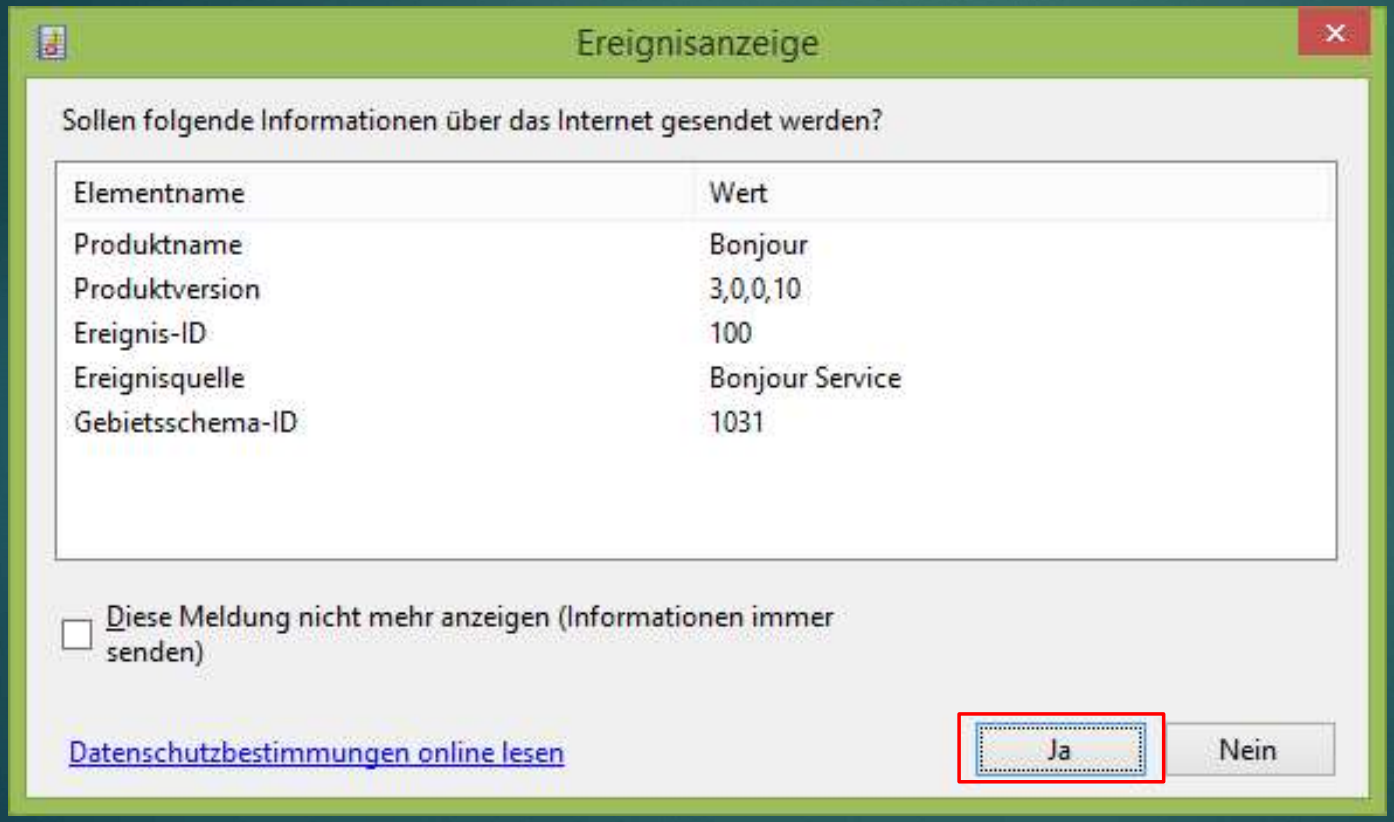
Fehlerbeispiel:
Ereignis-ID 100 Bonjour Service



Man kann die **Microsoft-Onlinehilfe** versuchen.

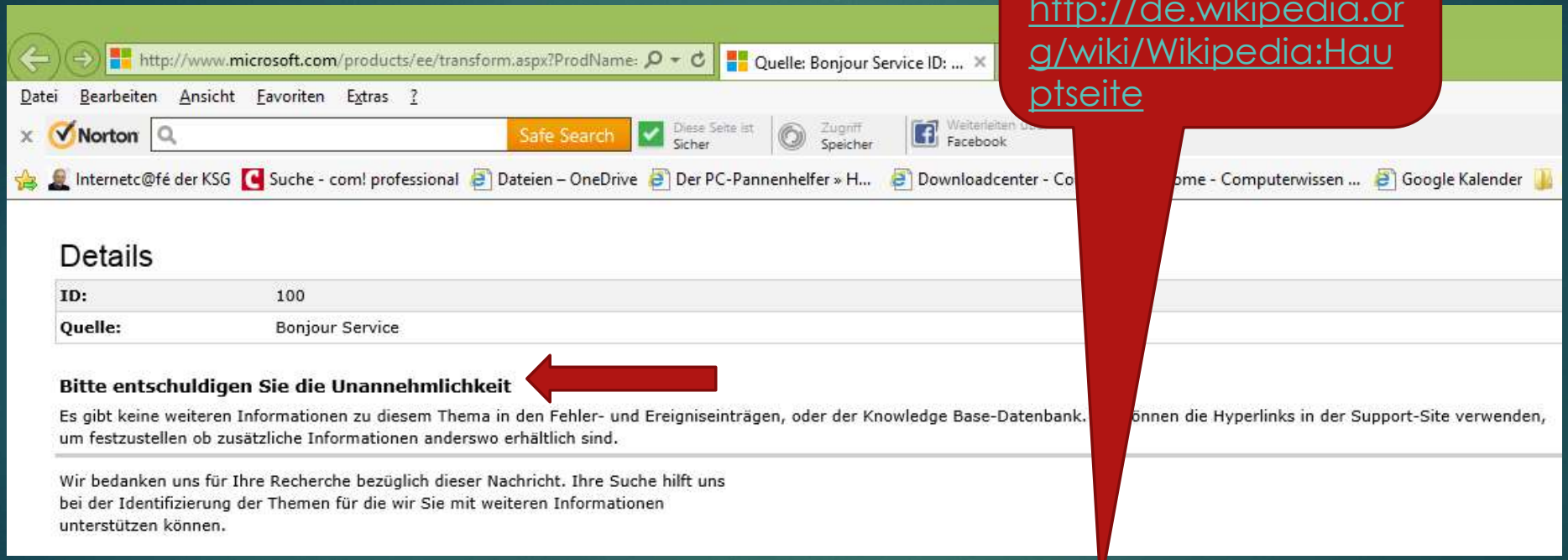
Klicken Sie mit der linken Maustaste auf **Onlinehilfe**.

Onlinehilfe anfordern



Klicken Sie auf **Ja**

Onlinehilfe
– hilft oft nicht weiter



Schauen Sie bei Wikipedia nach:

http://de.wikipedia.org/wiki/Wikipedia:Hauptseite

Versuchen Sie dann Hilfe im Internet zu finden.

Ergebnis der Suche bei Wikipedia

Bonjour (Apple)

Bonjour (franz. für „Guten Tag!“), ehemals Rendezvous (franz. für „das Treffen“), ist eine Technik, die die automatische Erkennung von Netzwerkdiensten in IP-Netzen bereitstellt.

Es handelt sich also um ein Programm von iTunes zum iPhone / iPad von Apple.

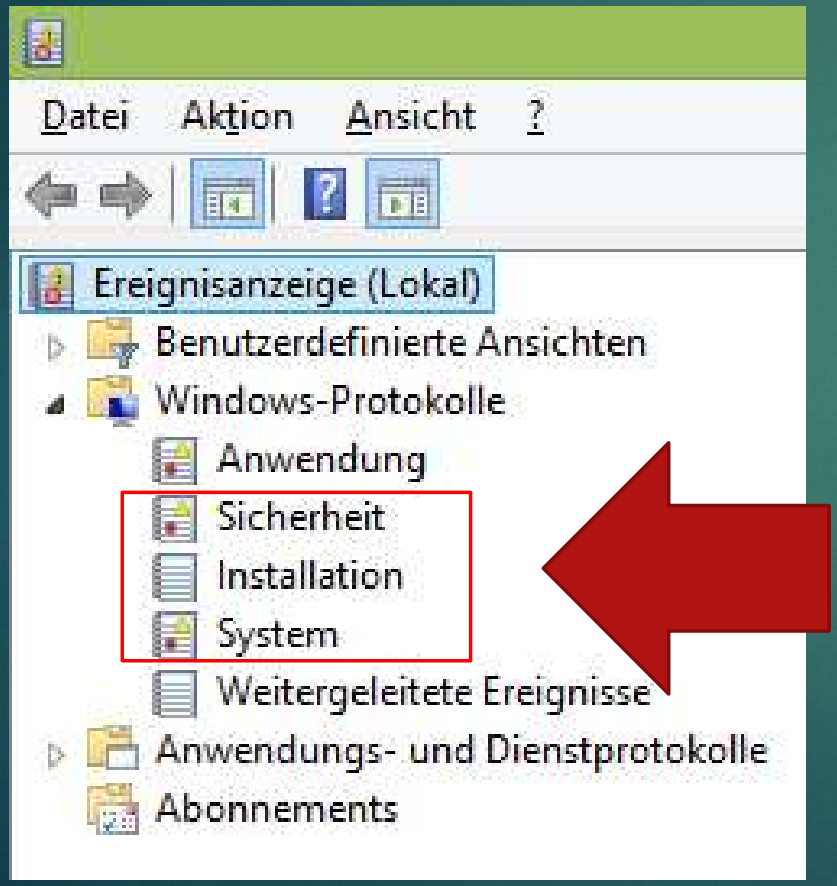
Lösung:
Einstellungen unter Dienste / Firewall prüfen evtl. Programm deinstallieren und dann wieder installieren

Eine Lösung zu finden ist nicht einfach und oft sehr zeitaufwendig.

Prüfen Sie nun die anderen Windows-Protokolle nach Fehlern

Prüfen Sie nun die Windows-Protokolle:

Sicherheit, Installation, System



Tipps & Tricks

Hier finden Sie Hilfe im Internet:

http://www.microsoft.com/technet/support/ee/ee_advanced.aspx

https://technet.microsoft.com/de-de/ms772425.aspx

http://support.microsoft.com

http://www.eventid.net/search.asp

http://www.fehlercodes.com

http://de.wikipedia.org/wiki/Wikipedia:Hauptseite

Bei Treiberfehler : Prüfen Sie beim Hersteller, ob es ein Update gibt.

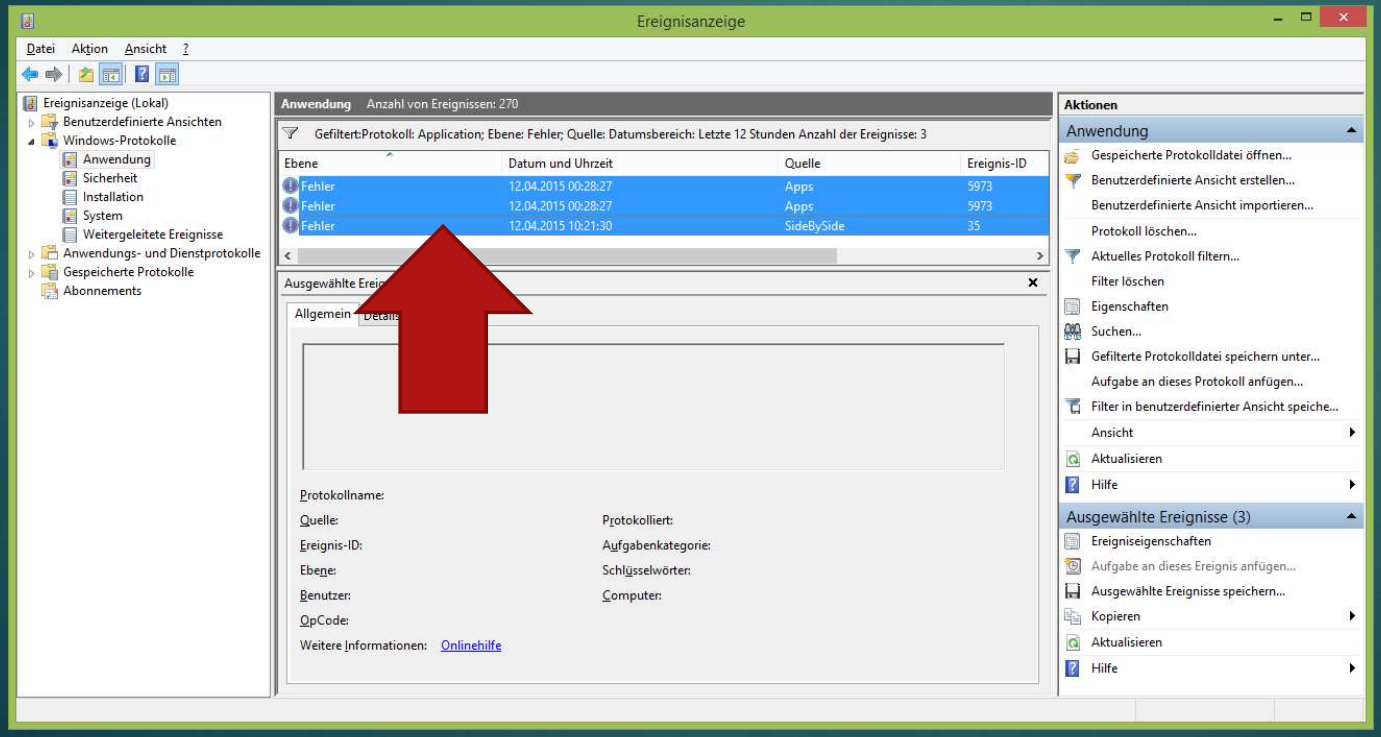
Fehlerprotokoll an einen Dritten senden

Tipps & Tricks

Senden Sie das Protokoll per E-Mail an einen Fachmann

So geht‘s:

Schritt 1: Markieren Sie mit der Shift-Taste und der Pfeil-Taste die Einträge



Tipps & Tricks

Senden Sie das Protokoll per E-Mail an einen Fachmann

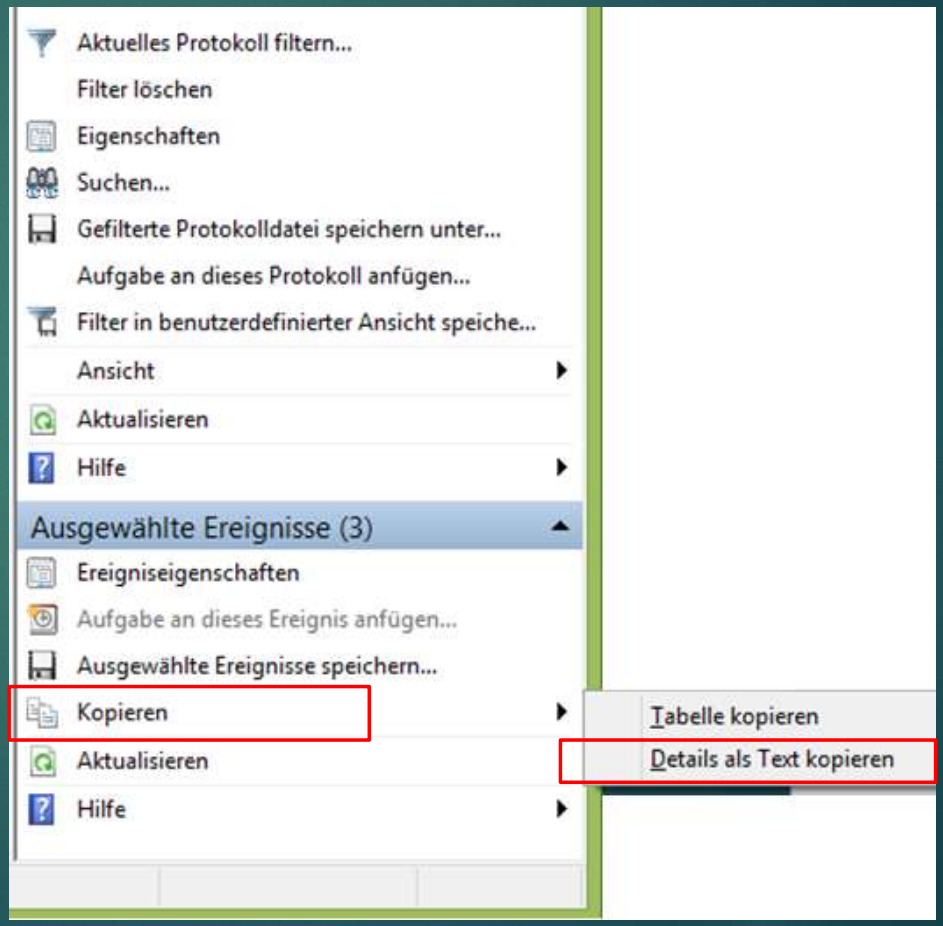
Schritt 2:

Klicken Sie nun mit der linken Maustaste auf:

Kopieren

und dann auf:

Details als Text kopieren



Tipps & Tricks

Senden Sie das Protokoll per E-Mail an einen Fachmann

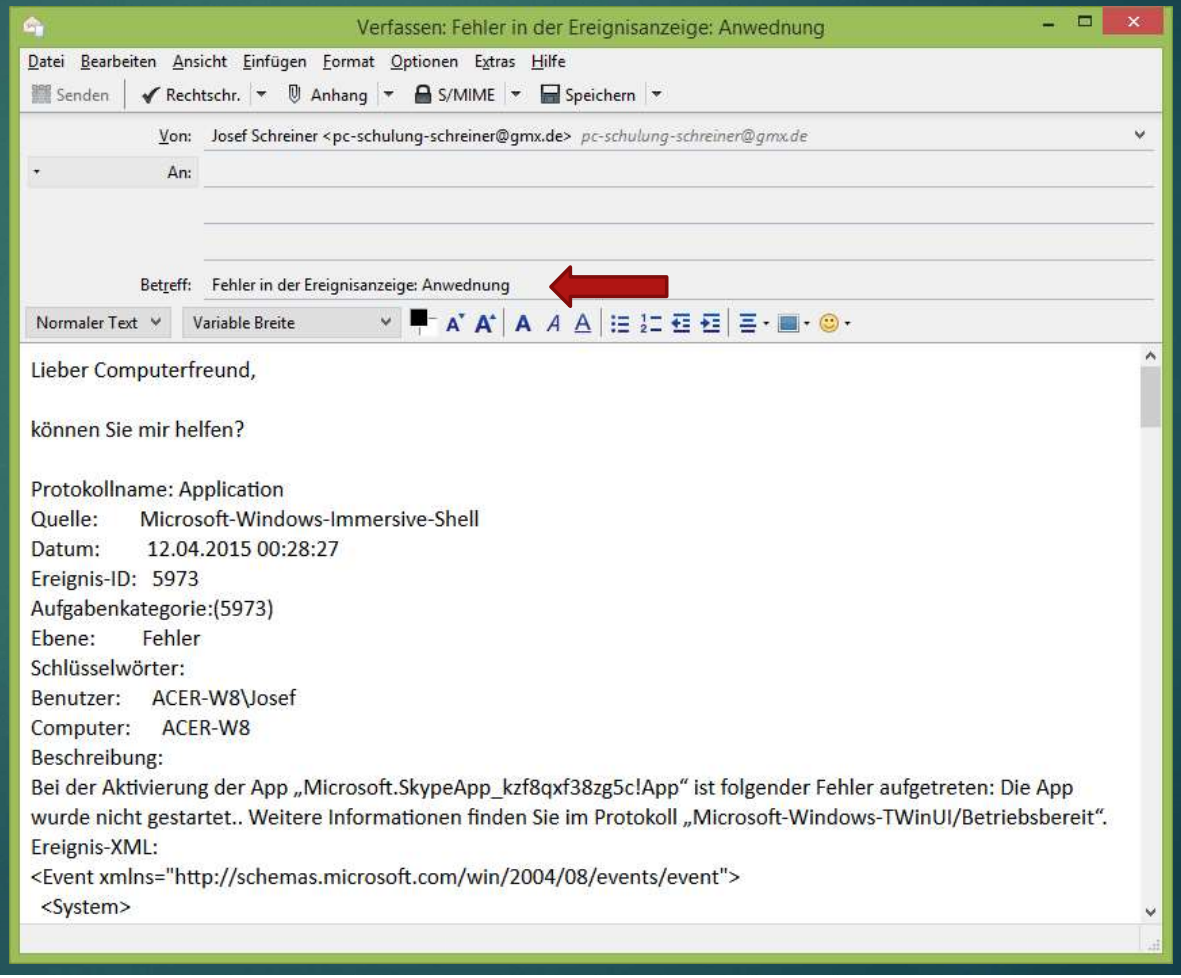
Schritt 3:
Starten Sie nun Ihr E-Mail-Programm und erstellen Sie eine neue E-Mail

Schritt 4:
Dann drücken Sie die Tastenkombination **[Windows-Taste + [C]**
und fügen die den zwischengespeicherten Text in die E-Mail ein.

Tipps & Tricks

Senden Sie das Protokoll per E-Mail an einen Fachmann

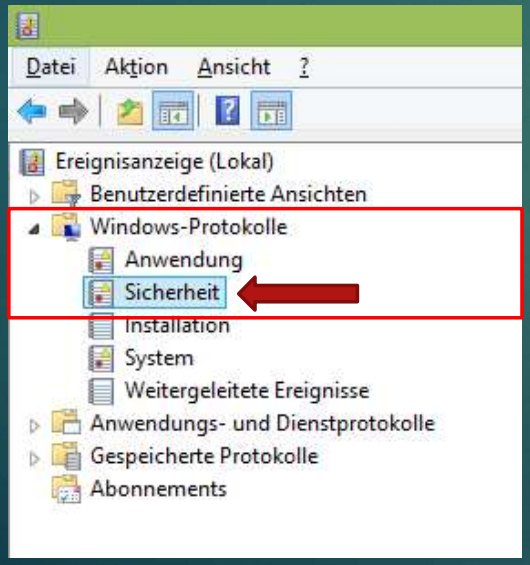
In der Betreffzeile müssen Sie das Protokoll bezeichnen
z. B. Anwendung

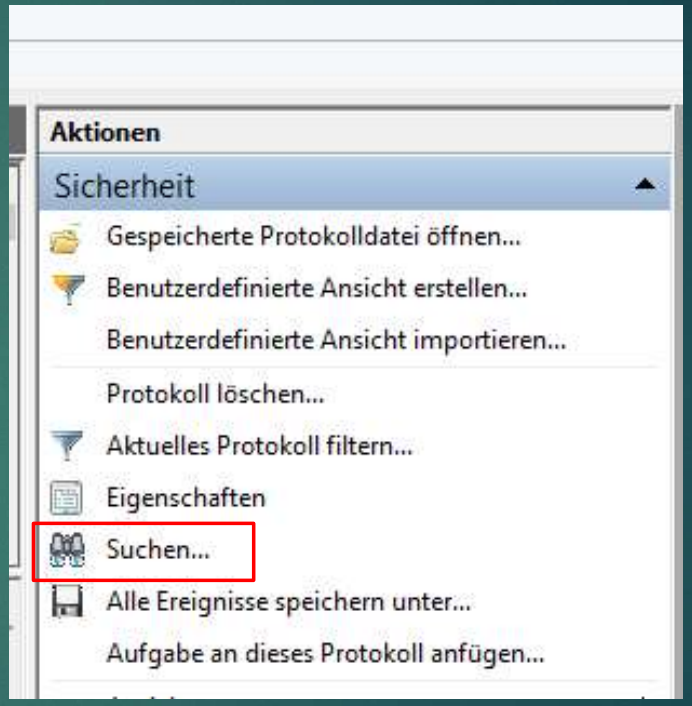


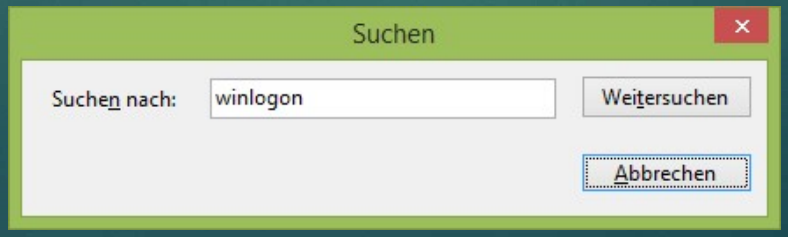
Tipp & Tricks

Wann wurde der PC zuletzt benutzt / angemeldet?

- Klicken Sie auf Windows-Protokolle
- Klicken Sie **Sicherheit**
- Wählen Sie rechts **Suchen**
- Geben Sie den Suchbegriff **Winlogon** ein
- Klicken Sie auf **Weitersuchen**

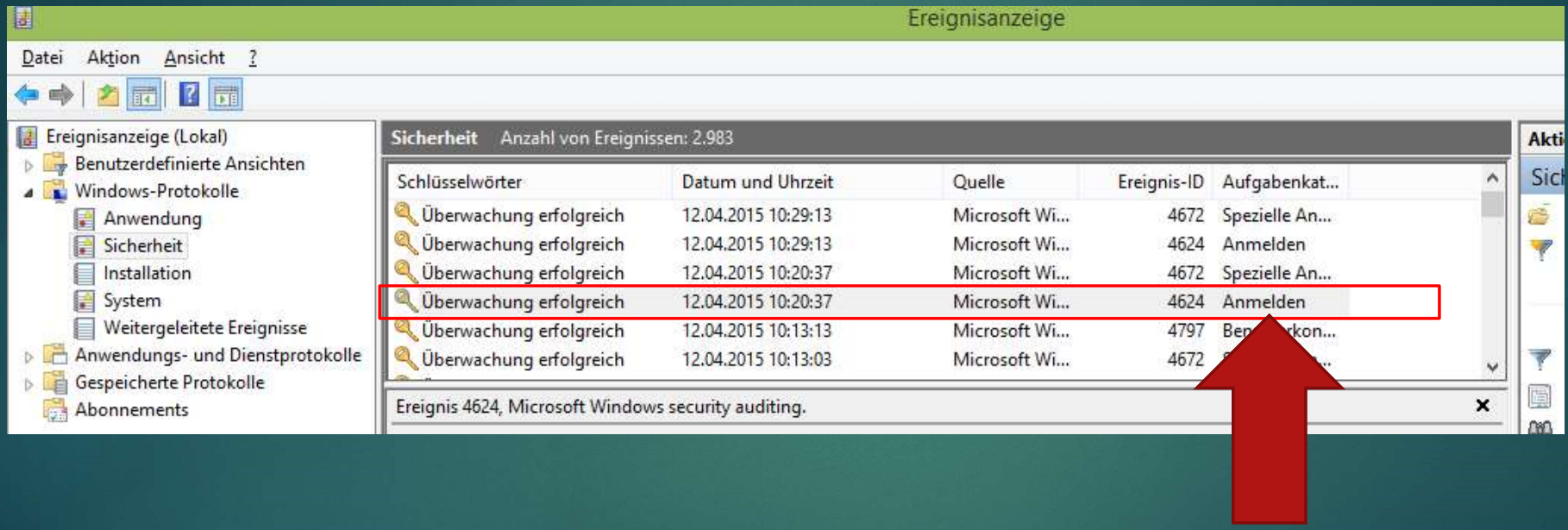






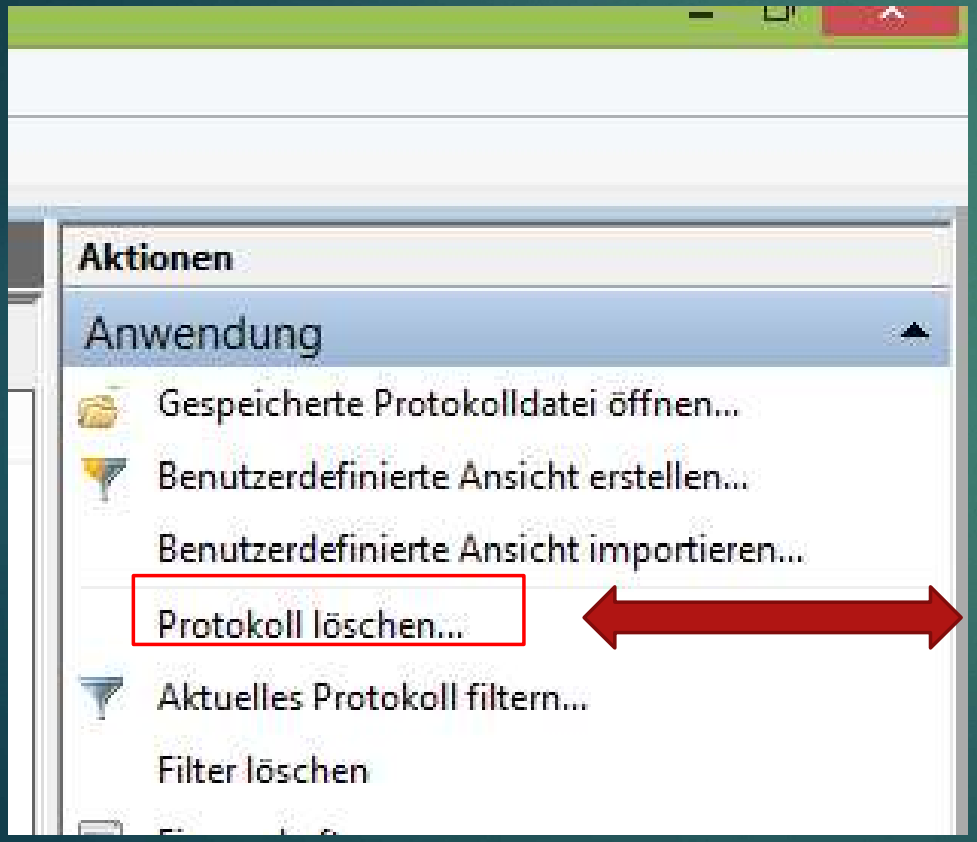
Tipp & Tricks

Wann wurde der PC zuletzt benutzt / angemeldet?



Sie erhalten dann den letzten Anmeldezeitpunkt
– unter Aufgabenkategorie steht „**Anmelden**“

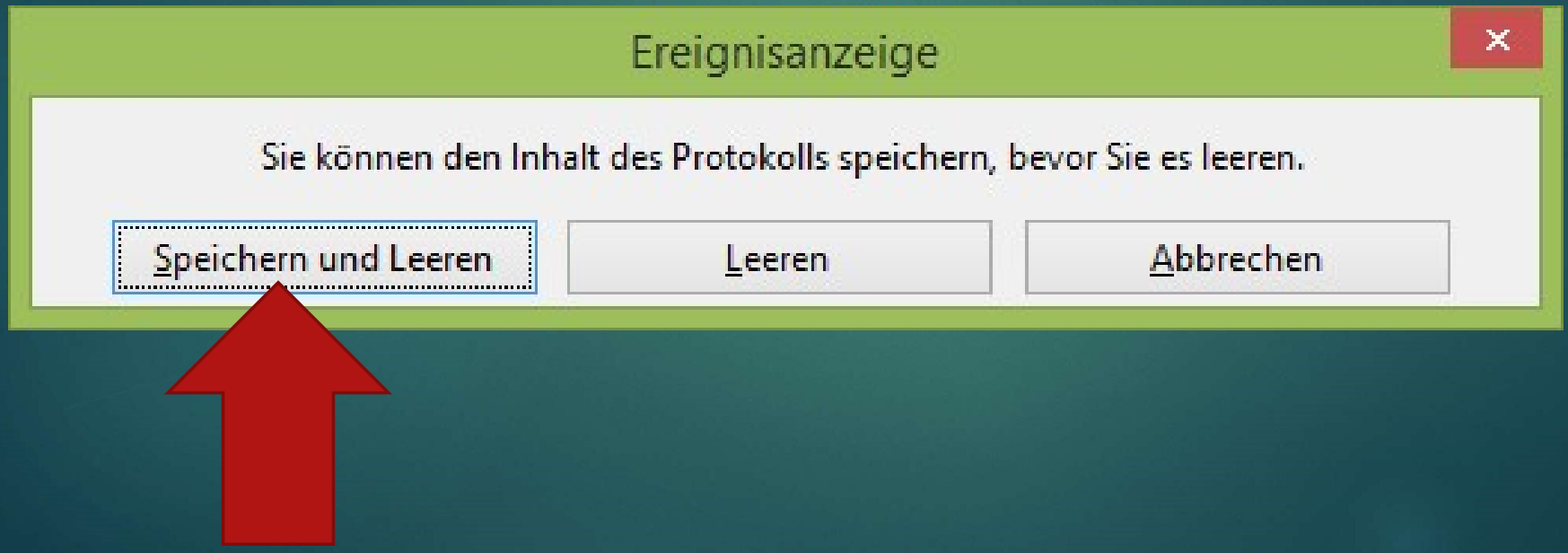
Tipps & Tricks
Protokoll Speichern und Leeren



Schritt 1: Klicken Sie mit der linken Maustaste auf **Protokoll löschen…**

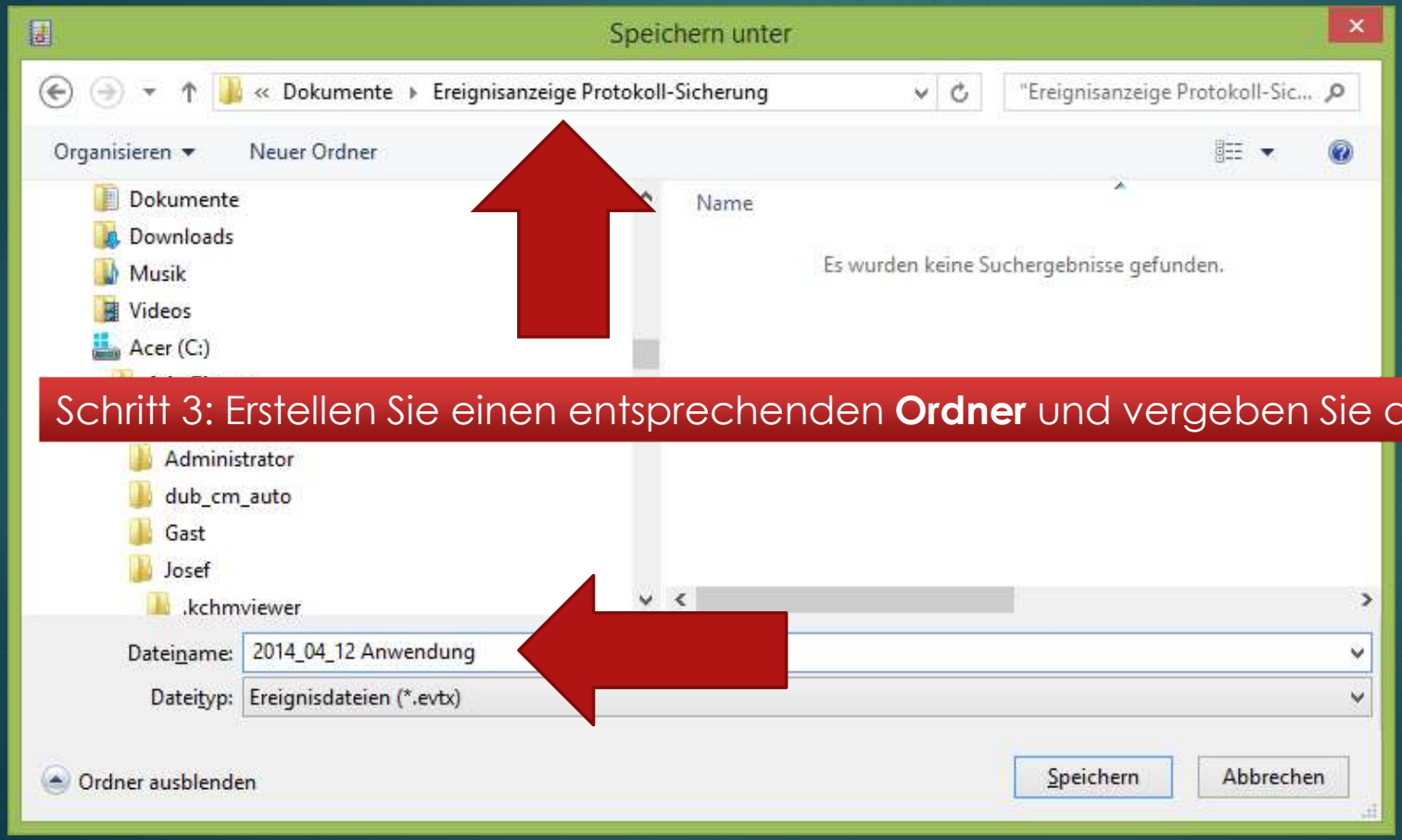
Tipps & Tricks
Protokoll Speichern und Leeren

Schritt 2: Klicken Sie mit der linken Maustaste auf **Speichern und Leeren**



Tipps & Tricks

Protokoll Speichern und Leeren



Schritt 3: Erstellen Sie einen entsprechenden **Ordner** und vergeben Sie den **Dateinamen**

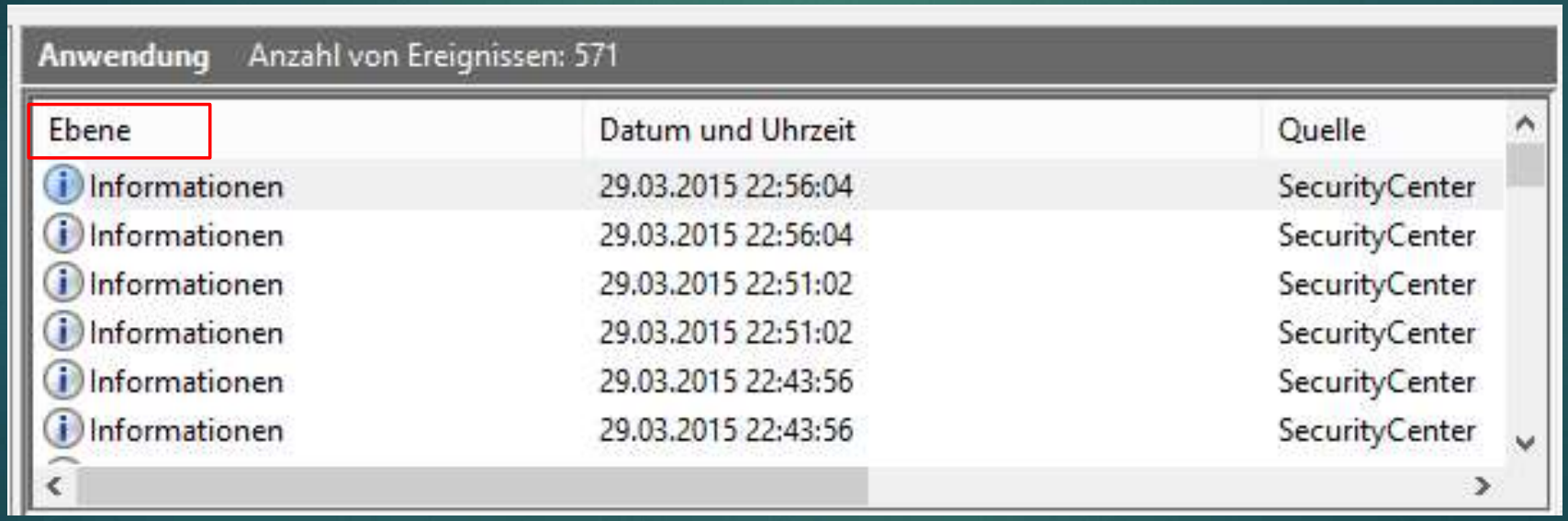
Nach einer Woche prüfen Sie wieder Ihren PC

Wenn nach einer Woche wieder Fehler protokolliert sind, so sollten Sie unbedingt die Fehlerursache abstellen.

Tipps & Tricks

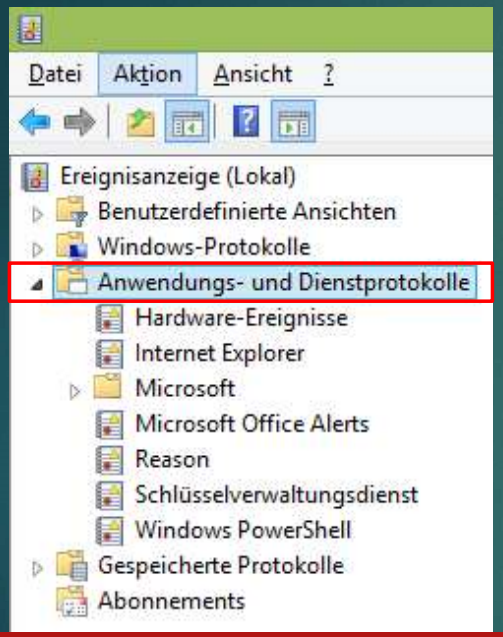
Ereignisse sortieren

Klicken Sie einfach auf die Spaltenüberschrift – z. B. Datum und Uhrzeit

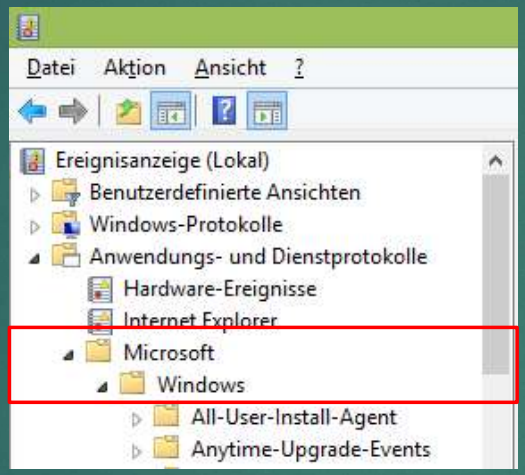


Anwendungs- und Dienstprotokolle

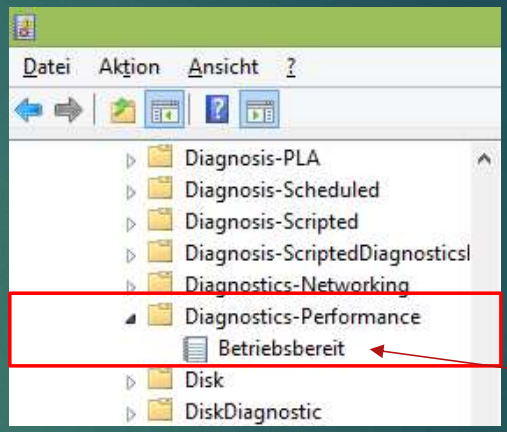
Klicken Sie nacheinander auf:



- Anwendungs- und Dienstprotokolle



- Microsoft
- dann auf Windows



- Diagnostic-Performance
- dann auf Betriebsbereit

In Windows-Vista Operational

Anwendungs- und Dienstprotokolle

Dienste und Programme im Hintergrund

Während Windows startet, werden viele Dienste und Programme automatisch im Hintergrund geladen

Filtern Sie die Einträge: z. B. Fehler

Einträge mit einer Ereignis-ID zwischen

- 100 und 199 beziehen sich auf den PC-Startvorgang