

Die Windows- Ereignisanzeige

© PC-SCHULUNG-SCHREINER

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?

3

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.

Ihr Windows-Tagebuch

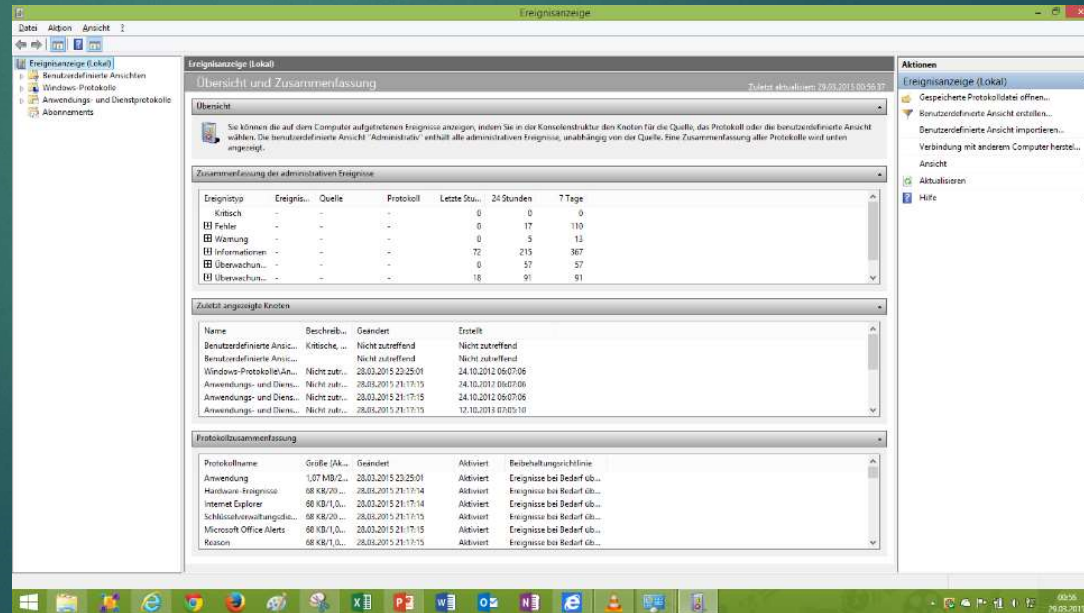
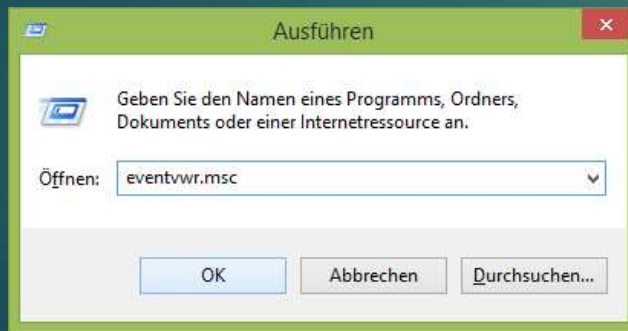
Wie wird die Ereignisanzeige gestartet?

4

Es geht auch mit der Tastenkombination:

Windows-Taste + [R]

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



Windows XP bis Windows 8.1

Ereignisanzeige

5

(c) PC-SCHULUNG-SCHREINER

Ereignisanzeige (Lokal)

- Benutzerdefinierte Ansichten
- Windows-Protokolle
- Anwendungs- und Dienstprotokolle
- Gespeicherte Protokolle
- Abonnements

Übersicht und Zusammenfassung Zuletzt aktualisiert: 12.04.2015 12:10:53

Übersicht

Sie können die auf dem Computer aufgetretenen Ereignisse anzeigen, indem Sie in der Konsolenstruktur den Knoten für die Quelle, das Protokoll oder die benutzerdefinierte Ansicht wählen. Die benutzerdefinierte Ansicht "Administrativ" enthält alle administrativen Ereignisse, unabhängig von der Quelle. Eine Zusammenfassung aller Protokolle wird unten angezeigt.

Zusammenfassung der administrativen Ereignisse

Ereignistyp	Ereignis...	Quelle	Protokoll	Letzte Stu...	24 Stunden	7 Tage
Kritisch	-	-	-	0	0	0
Fehler	-	-	-	0	12	48
Warnung	-	-	-	0	3	40

Zuletzt angezeigte Knoten

Name	Beschreib...	Geändert	Erstellt
Windows-Protokolle\An...	Nicht zutr...	11.04.2015 21:49:46	24.10.2012 06:07:06
Windows-Protokolle\Sic...	Nicht zutr...	11.04.2015 00:16:09	24.10.2012 06:07:06
Windows-Protokolle\Sys...	Nicht zutr...	12.04.2015 11:13:51	24.10.2012 06:07:05

Protokollzusammenfassung

Protokollname	Größe (Ak...	Geändert	Aktiviert	Beibehaltungsrichtlinie
Anwendung	1,07 MB/2...	11.04.2015 21:49:46	Aktiviert	Ereignisse bei Bedarf üb...
Hardware-Ereignisse	68 KB/20 ...	02.04.2015 00:00:58	Aktiviert	Ereignisse bei Bedarf üb...
Internet Explorer	68 KB/1,0...	02.04.2015 00:00:58	Aktiviert	Ereignisse bei Bedarf üb...

Aktionen

- Ereignisanzeige (Lokal)
- Gespeicherte Protokolldatei öffnen...
- Benutzerdefinierte Ansicht erstellen...
- Benutzerdefinierte Ansicht importieren...
- Verbindung mit anderem Computer herstel...
- Ansicht
- Aktualisieren
- Hilfe

Öffnen Sie die Windows-Protokolle

6

Klicken Sie auf den kleinen Pfeil vor Windows-Protokolle

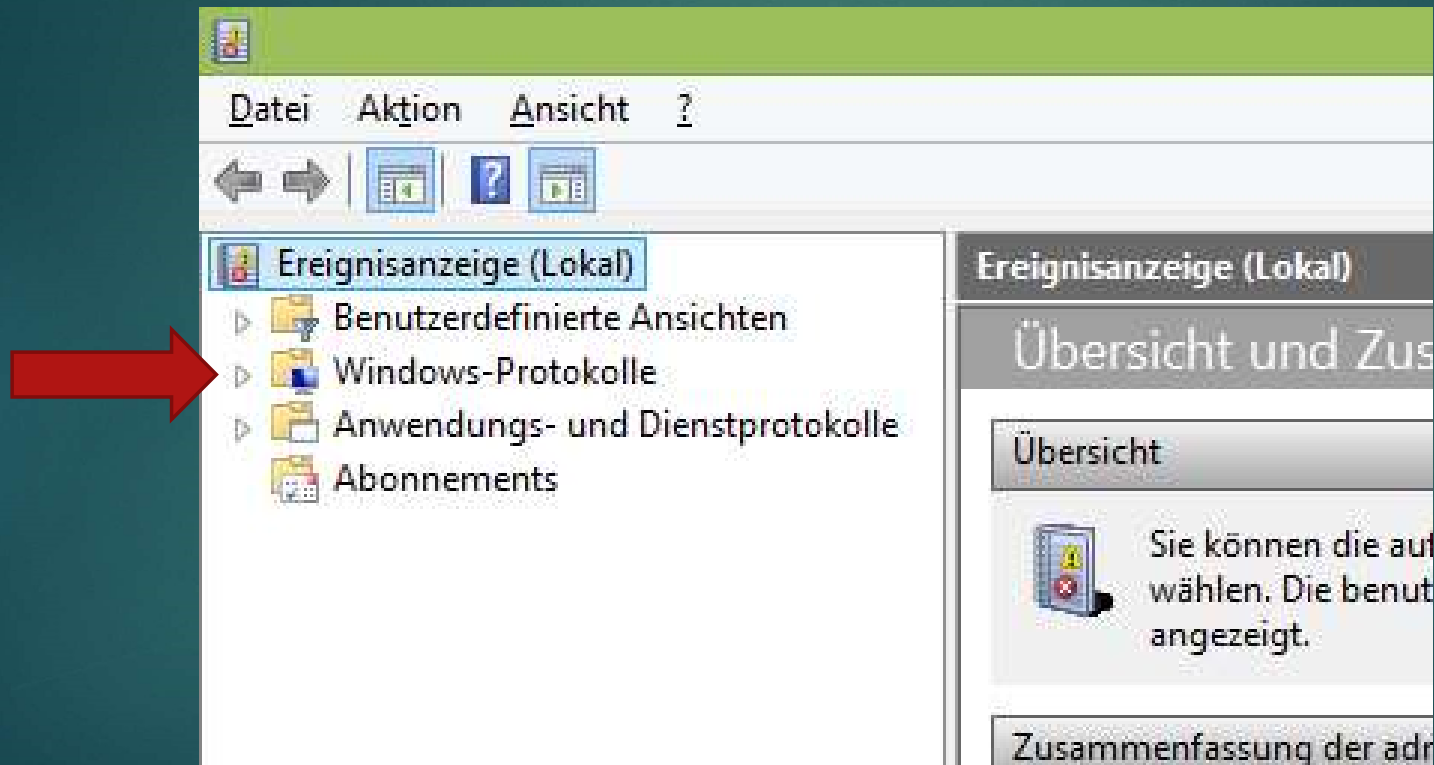
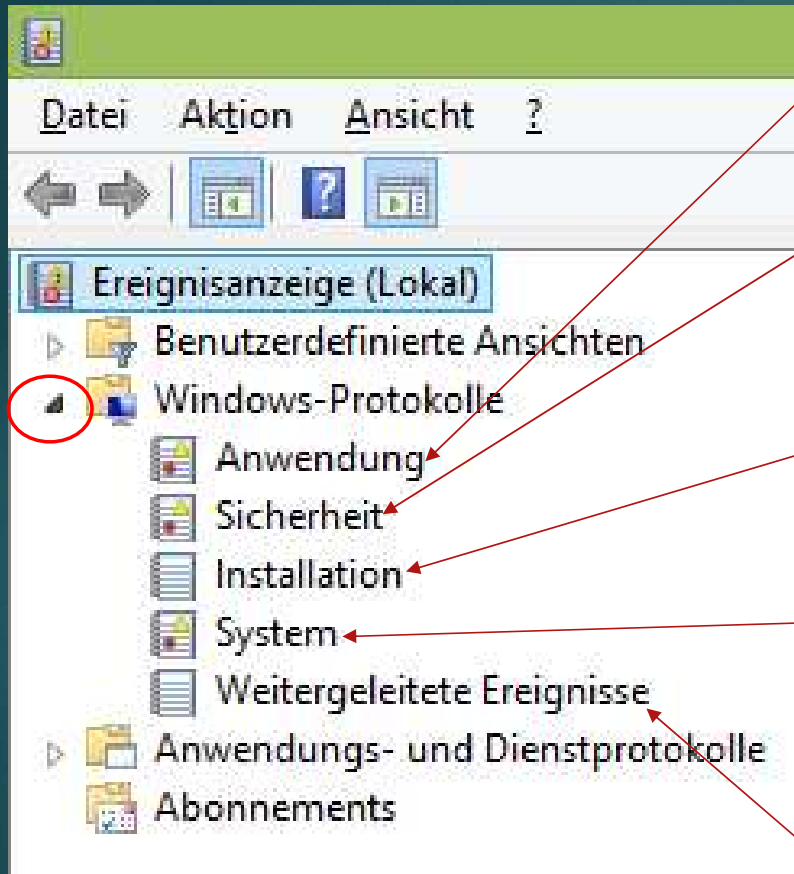


Abbildung: Windows Vista, Windows 7, Windows 8.1

Windows-Protokolle

7

(c) PC-SCHULUNG-SCHREINER



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

8

Ereignisanzeige Anzahl von Ereignissen: 292 (!) Neue Ereignisse sind verfügbar

Ebene	Datum und Uhrzeit	Quelle
Informationen	29.03.2015 12:08:55	SecurityCenter
Informationen	29.03.2015 12:08:55	SecurityCenter
Informationen	29.03.2015 12:03:53	SecurityCenter

Ereignis 16, SecurityCenter

Allgemein Details

Windows Defender konnte vom Windows-Sicherheitscenterdienst nicht beendet werden.

Protokollname:	Anwendung	Protokolliert:	29.03.2015 12:08:55
Quelle:	SecurityCenter	Aufgabenkategorie:	Keine
Ereignis-ID:	16	Schlüsselwörter:	Klassisch
Ebene:	Informationen	Computer:	ACER-W8
Benutzer:	Nicht zutreffend		
OpCode:			
Weitere Informationen:	Onlinehilfe		

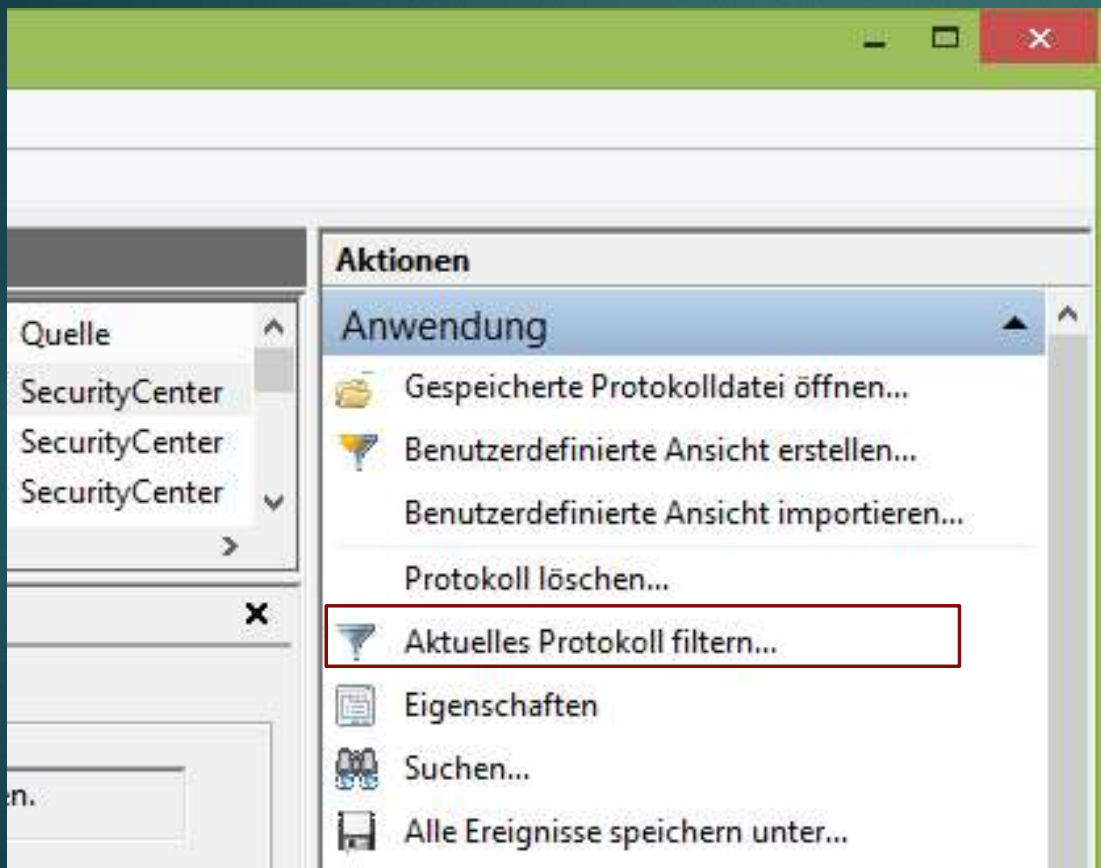
Windows listet nun alle Anwendungen auf

Aktuelles Protokoll filtern



9

(c) PC-SCHULUNG-SCHREINER



Klicken Sie mit der **linken** Maustaste auf

Aktuelles Protokoll filtern...

Das Protokoll unterscheidet 5 Ereignisebenen



10

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

Filter XML

Protokolliert: Jederzeit

Ereignisebene: Kritisch Warnung Ausführlich
 Fehler Informationen

Per Protokoll Protokolle: Sicherheit

Per Quelle Quellen:

Ereignis-IDs ein-/ausschließen: Durch Trennzeichen getrennte IDs bzw. ID-Bereiche eingeben. Zum Ausschließen von Kriterien Minuszeichen eingeben, z. B. 1,3,5-99,-76

<Alle Ereignis-IDs>

Aufgabenkategorie:

Schlüsselwörter:

Benutzer: <Alle Benutzer>

Computer: <Alle Computer>

Anzeige löschen

OK Abbrechen

Aktuelles Protokoll filtern: Fehler



11

(c) PC-SCHULUNG-SCHREINER

Benutzerdefinierte Ansicht erstellen

Filter XML

Protokolliert: Jederzeit

Ereignisebene: Kritisch Warnung Ausführlich
 Fehler Informationen

Per Protokoll Protokolle: Anwendung

Per Quelle Quellen:

Ereignis-IDs ein-/ausschließen: Durch Trennzeichen getrennte IDs bzw. ID-Bereiche eingeben. Zum Ausschließen von Kriterien Minuszeichen eingeben, z. B. 1,3,5-99,-76

<Alle Ereignis-IDs>

Aufgabenkategorie:

Schlüsselwörter:

Benutzer: <Alle Benutzer>

Computer: <Alle Computer>

Anzeige löschen

OK Abbrechen

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

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

Es wurden 4 Fehler gefunden



12

Ereignisanzeige

Anwendung Anzahl von Ereignissen: 425

Gefiltert: Protokoll: Application; Ebene: Fehler; Quelle: Anzahl der Ereignisse: 4

Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Fehler	29.03.2015 01:24:00	Bonjour Service	100	Keine
Fehler	29.03.2015 01:24:00	Bonjour Service	100	Keine
Fehler	29.03.2015 01:24:00	Bonjour Service	100	Keine
Fehler	28.03.2015 22:50:37	Application Hang	1002	(101)

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 Ereignisseigenschaften

13

(c) PC-SCHULUNG-SCHREINER



Hier finden Sie die Fehlerangaben
Später dazu mehr!

Windows-Protokoll Anwendung listet sehr viele Fehler auf > 50



14

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

Aktuelles Protokoll filtern



15

(c) PC-SCHULUNG-SCHREINER

Aktuelles Protokoll filtern

Filter XML

Protokolliert: Jederzeit

Ereignisebene: Jederzeit
Letzte Stunde
Letzte 12 Stunden
Letzte 24 Stunden
Letzte 7 Tage
Letzte 30 Tage
Benutzerdefinierter Bereich...

Per Protokoll
 Per Quelle

Quellen:

Ereignis-IDs ein-/ausschließen: Durch Trennzeichen getrennte IDs bzw. ID-Bereiche eingeben. Zum Ausschließen von Kriterien Minuszeichen eingeben, z. B. 1,3,5-99,-76

<Alle Ereignis-IDs>

Aufgaben-kategorie:

Schlüsselwörter:

Benutzer: <Alle Benutzer>

Computer: <Alle Computer>

Anzeige löschen

OK Abbrechen

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

Danach überprüfen Sie die Fehler.

Fehlerüberprüfung

16

The screenshot shows the Windows Event Viewer application. The left pane displays a tree view of event logs, with 'Anwendung' (Application) selected. The main pane shows a list of events filtered by 'Protokoll: Application; Ebene: Fehler; Quelle: Anzahl der Ereignisse: 8'. Two error events are visible, with the most recent one selected. A red arrow points from a text box to this selected error event. The right pane shows a list of actions available for the selected event.

Anwendung Anzahl von Ereignissen: 320

Gefiltert: Protokoll: Application; Ebene: Fehler; Quelle: Anzahl der Ereignisse: 8

Ebene	Datum und Uhrzeit
Fehler	12.04.2015 12:34:47
Fehler	12.04.2015 10:21:30

Ereignis 35, SideBySide

Allgemein Details

Fehler beim Generieren des Aktivierungskontextes für "C:\Program Files (x86)\Windows Li
Photo Gallen\MovieMaker Eye". Fehler in Manifest- oder Richtliniendatei "C:\Program Fi

Protokollname:	Anwendung	Protokolliert:	12.04.2015 12:
Quelle:	SideBySide	Aufgabenkategorie:	Keine
Ereignis-ID:	35	Schlüsselwörter:	Klassisch
Ebene:	Fehler	Computer:	ACER-W8
Benutzer:	Nicht zutreffend		
OpCode:			
Weitere Informationen:	Onlinehilfe		

Doppelklick auf eine Fehlermeldung

Aktionen

Anwendung

- Gespeicherte Protokolldatei öffnen...
- Benutzerdefinierte Ansicht erstellen...
- Benutzerdefinierte Ansicht importieren...
- Protokoll löschen...
- Aktuelles Protokoll filtern...
- Filter löschen
- Eigenschaften
- Suchen...
- Gefilterte Protokolldatei speichern unter...
- Aufgabe an dieses Protokoll anfügen...
- Filter in benutzerdefinierter Ansicht spei...

Ansicht

- Aktualisieren
- Hilfe

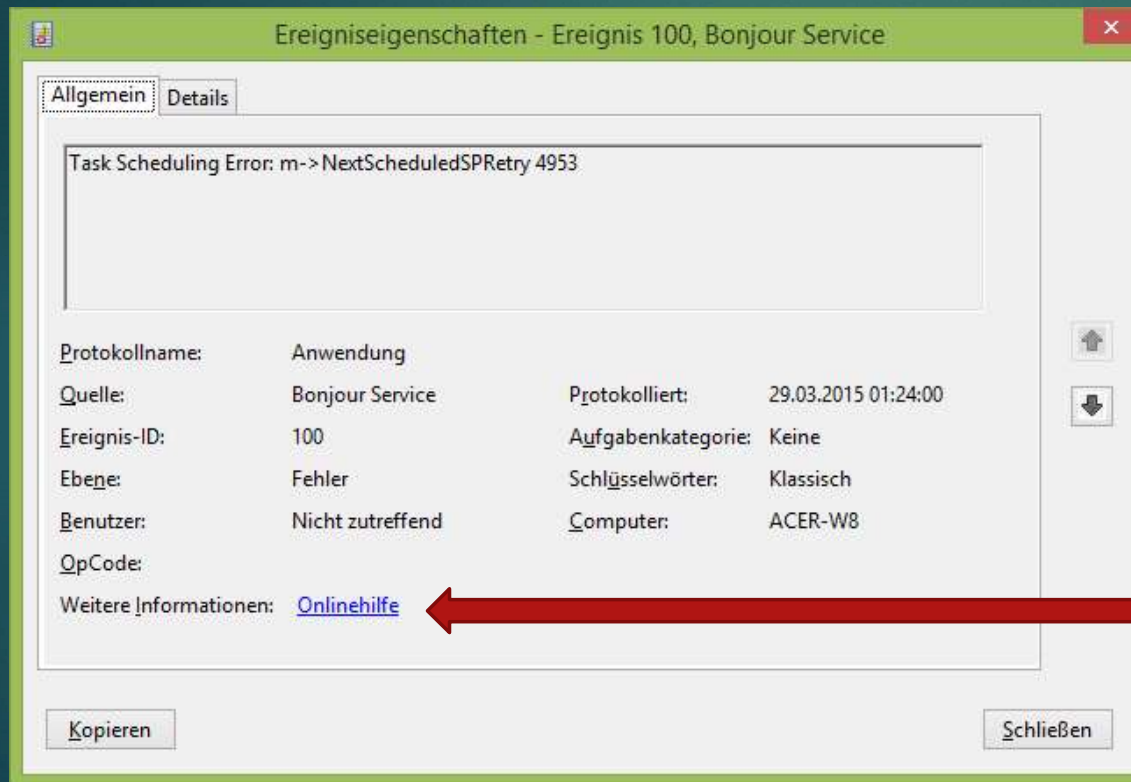
Ereignis 35, SideBySide

- Ereigniseigenschaften
- Aufgabe an dieses Ereignis anfügen...

Fehlerbeispiel: Ereignis-ID 100 Bonjour Service

17

(c) PC-SCHULUNG-SCHREINER



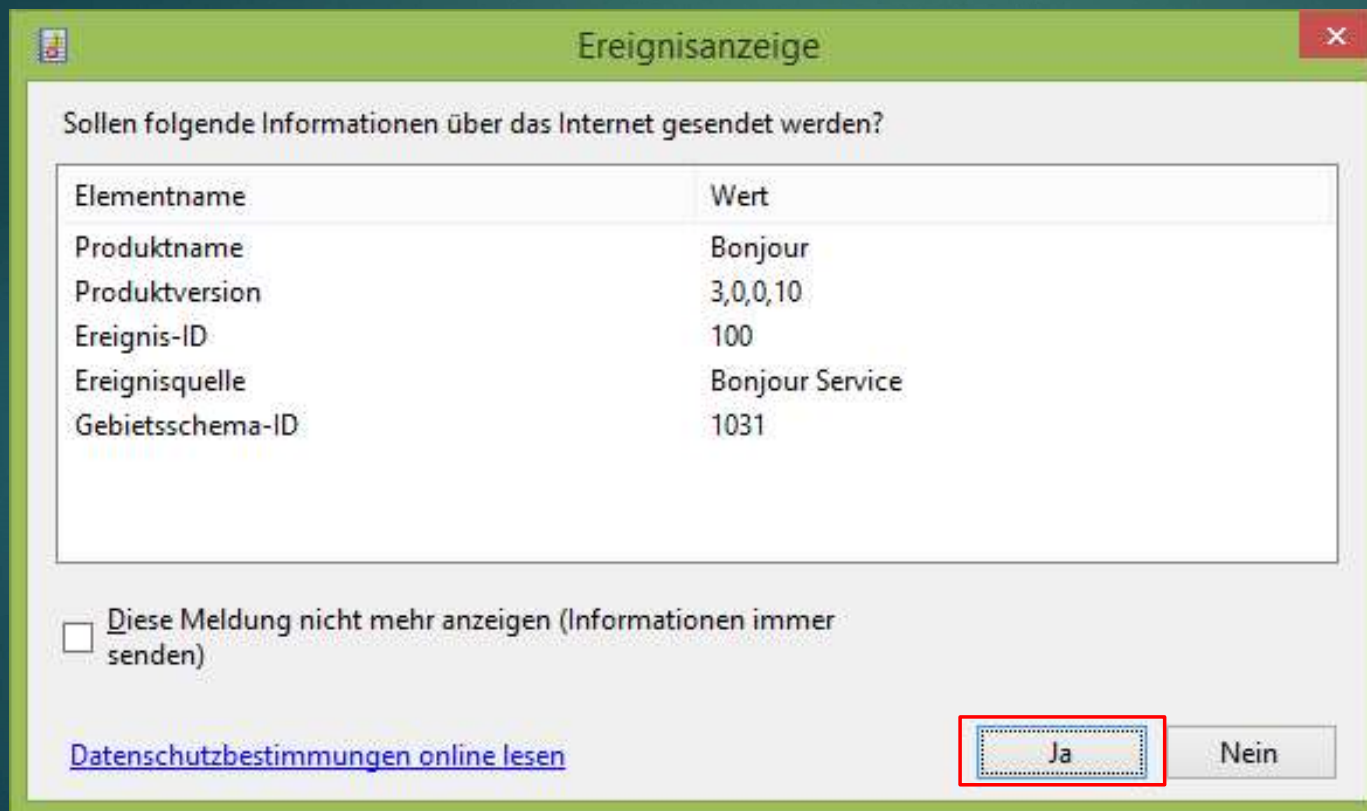
Man kann die **Microsoft-Onlinehilfe** versuchen.

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

Onlinehilfe anfordern

18

(c) PC-SCHULUNG-SCHREINER



Sollen folgende Informationen über das Internet gesendet werden?

Elementname	Wert
Produktname	Bonjour
Produktversion	3,0,0,10
Ereignis-ID	100
Ereignisquelle	Bonjour Service
Gebietsschema-ID	1031

Diese Meldung nicht mehr anzeigen (Informationen immer senden)

[Datenschutzbestimmungen online lesen](#)

Ja Nein

Klicken Sie auf **Ja**

Onlinehilfe – hilft oft nicht weiter

19

(c) PC-SCHULUNG-SCHREINER



The screenshot shows a Microsoft support page. The browser address bar displays the URL: <http://www.microsoft.com/products/ee/transform.aspx?ProdName:>. The page content includes a 'Details' section with the following information:

ID:	100
Quelle:	Bonjour Service

Below the table, a red arrow points to the text: **Bitte entschuldigen Sie die Unannehmlichkeit**. The text below the arrow reads: "Es gibt keine weiteren Informationen zu diesem Thema in den Fehler- und Ereigniseinträgen, oder der Knowledge Base-Datenbank. Sie können die Hyperlinks in der Support-Site verwenden, um festzustellen ob zusätzliche Informationen anderswo erhältlich sind."

At the bottom of the page, there is a paragraph: "Wir bedanken uns für Ihre Recherche bezüglich dieser Nachricht. Ihre Suche hilft uns bei der Identifizierung der Themen für die wir Sie mit weiteren Informationen unterstützen können."

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

20

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

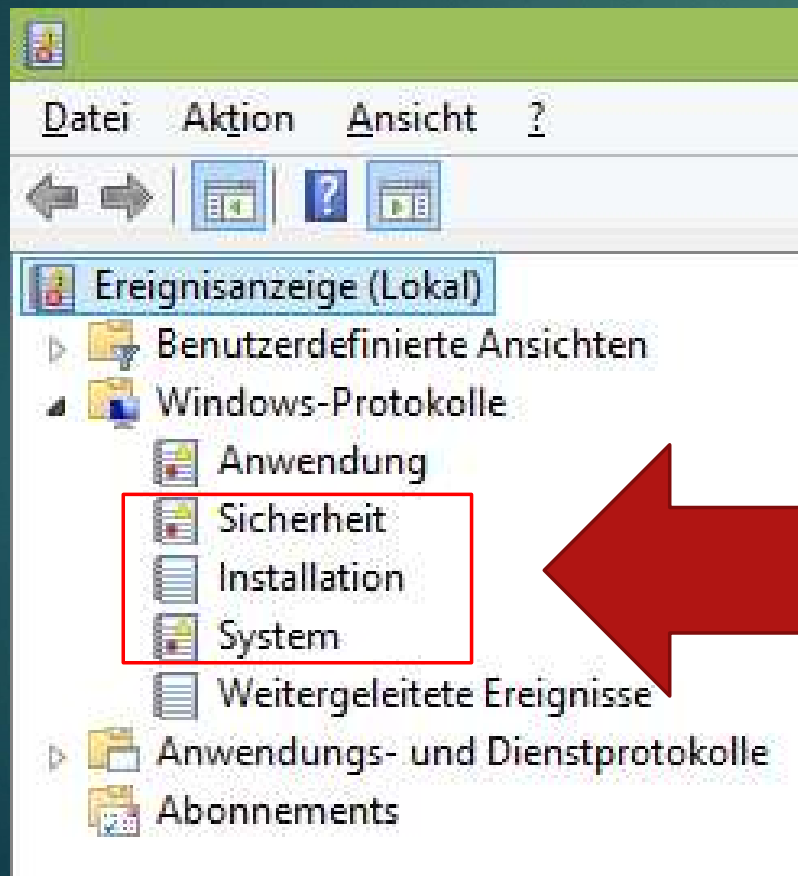
Eine Lösung zu finden ist nicht einfach und oft sehr zeitaufwendig.

**Prüfen Sie nun die anderen
Windows-Protokolle nach Fehlern**

Prüfen Sie nun die Windows-Protokolle: Sicherheit, Installation, System

23

(c) PC-SCHULUNG-SCHREINER



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

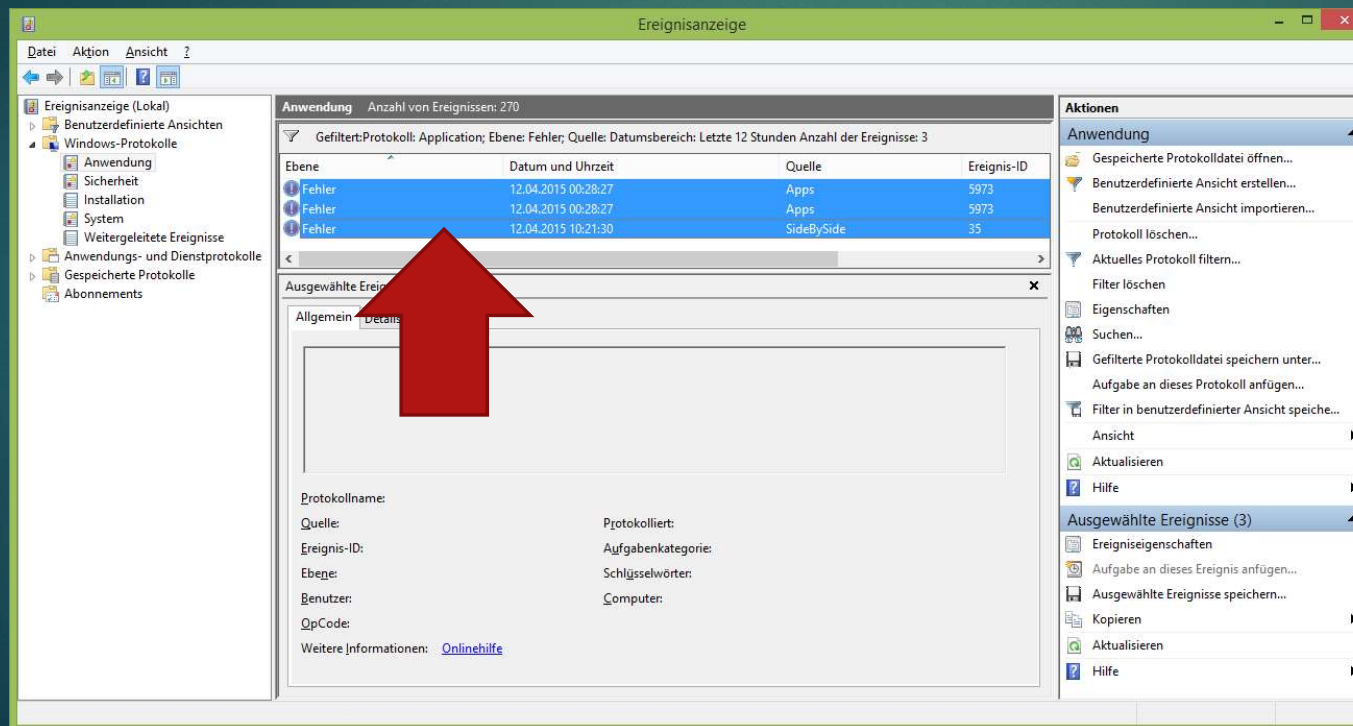
Tipps & Tricks

26

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

27

Senden Sie das Protokoll per E-Mail an einen Fachmann

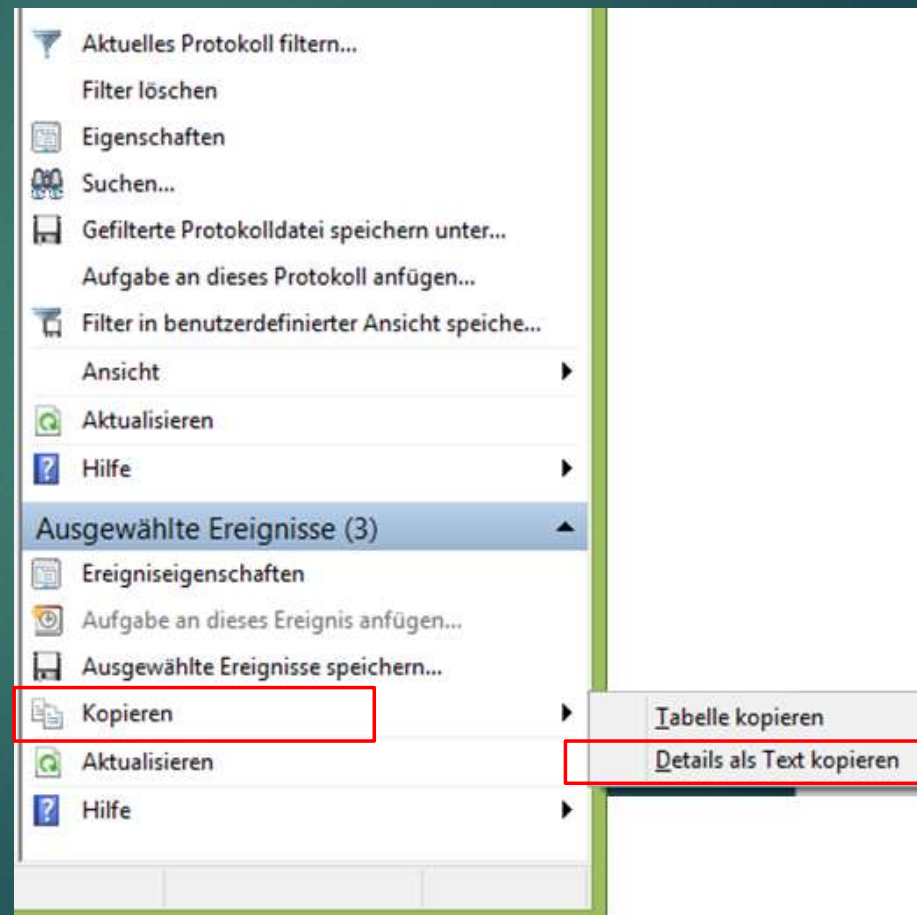
Schritt 2:

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

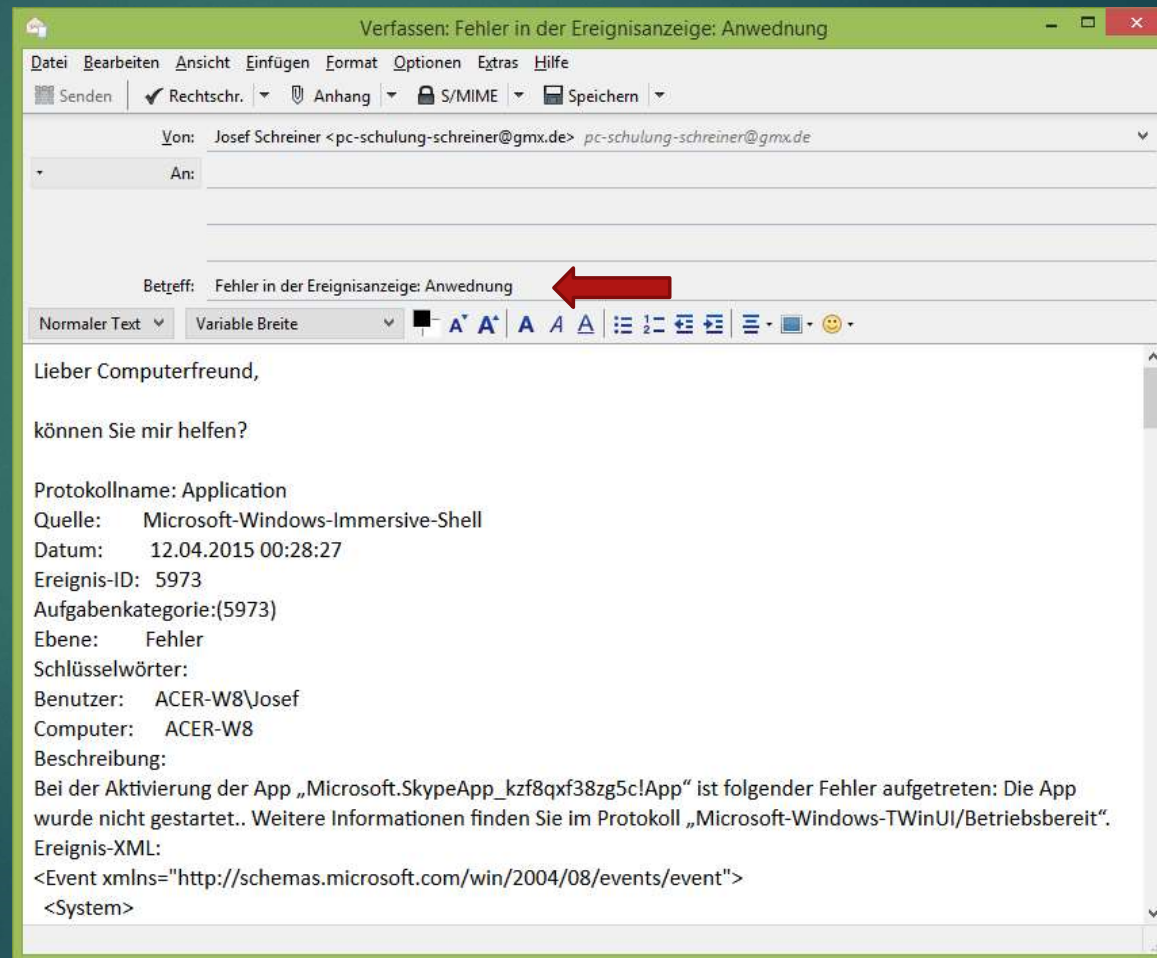
Schritt 4:

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

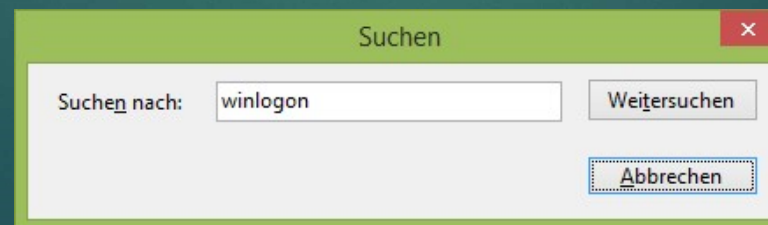
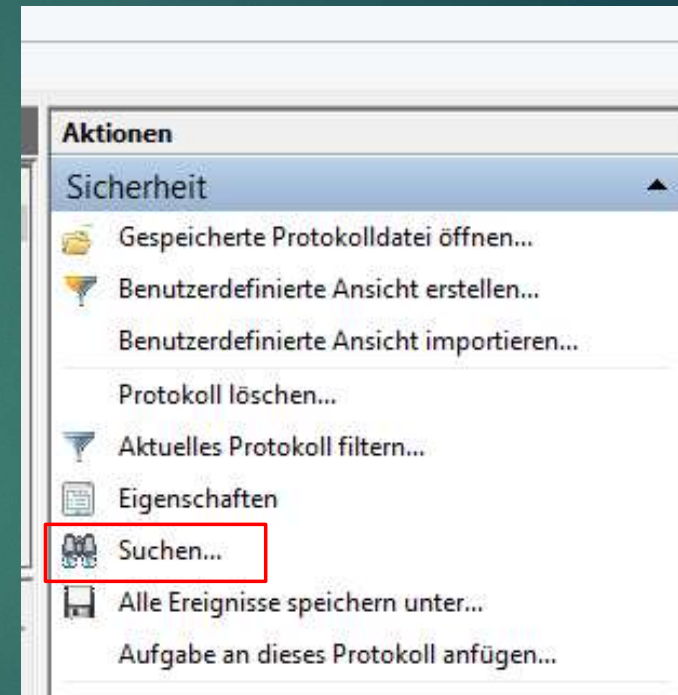
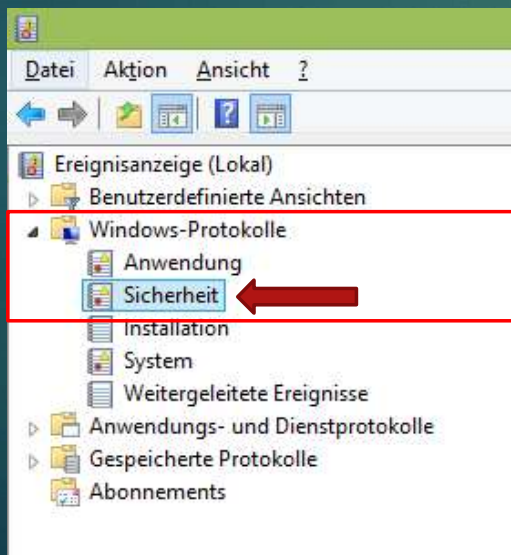


Tipp & Tricks

30

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?

31

(c) PC-SCHULUNG-SCHREINER

The screenshot shows the Windows Event Viewer window titled 'Ereignisanzeige'. The left pane shows the tree view with 'Sicherheit' selected under 'Windows-Protokolle'. The main pane displays a table of security events. The event 'Anmelden' (ID 4624) is highlighted with a red box, and a red arrow points to it from below. The table columns are: Schlüsselwörter, Datum und Uhrzeit, Quelle, Ereignis-ID, and Aufgabenkat... The event details pane at the bottom shows 'Ereignis 4624, Microsoft Windows security auditing.'

Schlüsselwörter	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkat...
Überwachung erfolgreich	12.04.2015 10:29:13	Microsoft Wi...	4672	Spezielle An...
Überwachung erfolgreich	12.04.2015 10:29:13	Microsoft Wi...	4624	Anmelden
Überwachung erfolgreich	12.04.2015 10:20:37	Microsoft Wi...	4672	Spezielle An...
Überwachung erfolgreich	12.04.2015 10:20:37	Microsoft Wi...	4624	Anmelden
Überwachung erfolgreich	12.04.2015 10:13:13	Microsoft Wi...	4797	Benutzerkon...
Überwachung erfolgreich	12.04.2015 10:13:03	Microsoft Wi...	4672	Spezielle An...

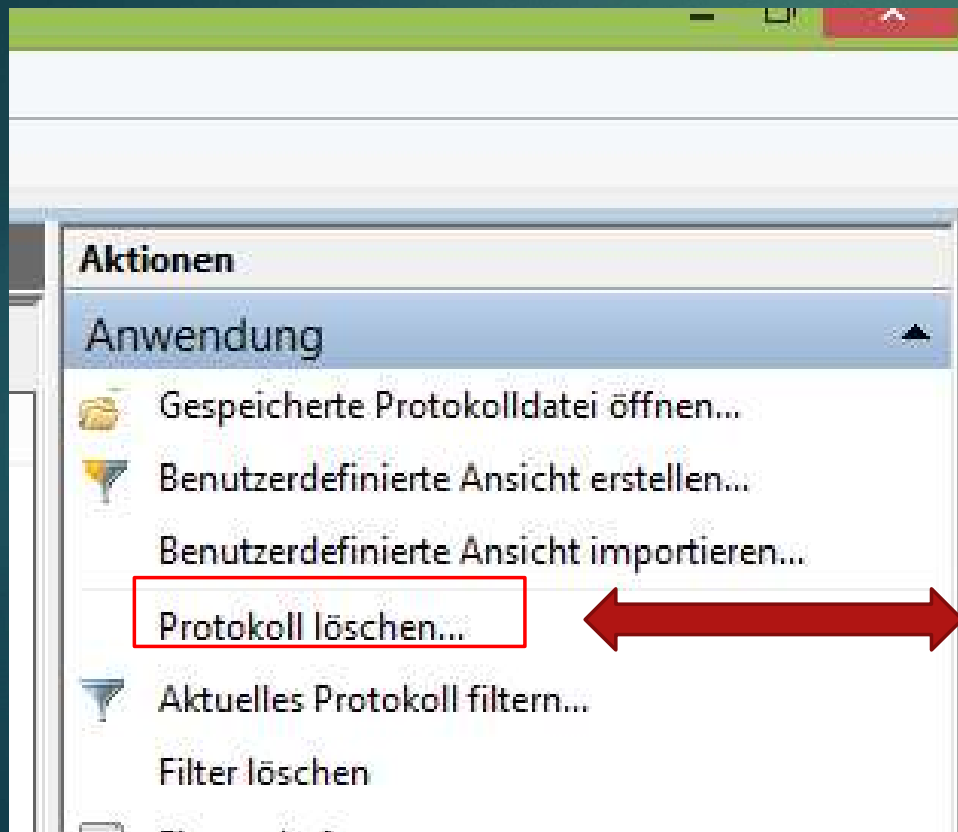
Sie erhalten dann den letzten Anmeldezeitpunkt
– unter Aufgabenkategorie steht „**Anmelden**“

Tipps & Tricks

Protokoll Speichern und Leeren

32

(c) PC-SCHULUNG-SCHREINER

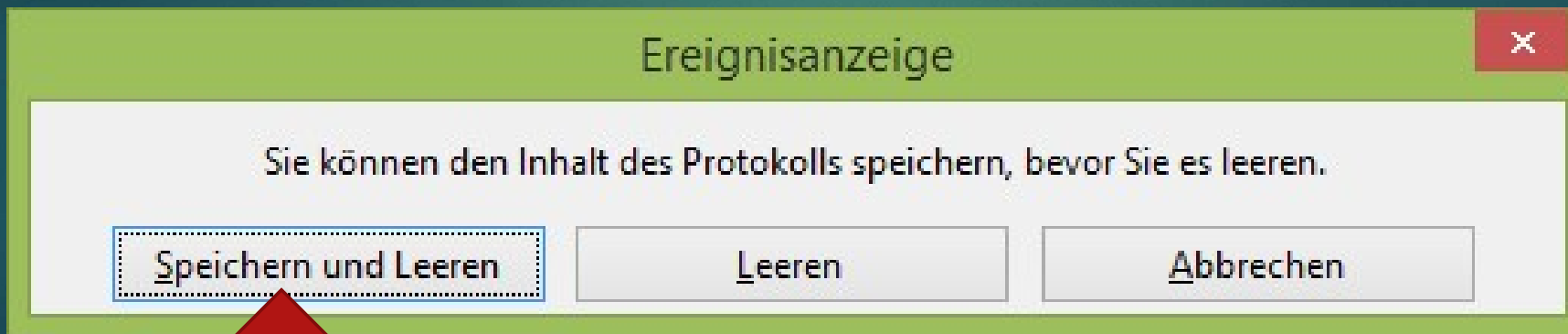


Schritt 1: Klicken Sie mit der linken Maustaste auf **Protokoll löschen...**

Tipps & Tricks

Protokoll Speichern und Leeren

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

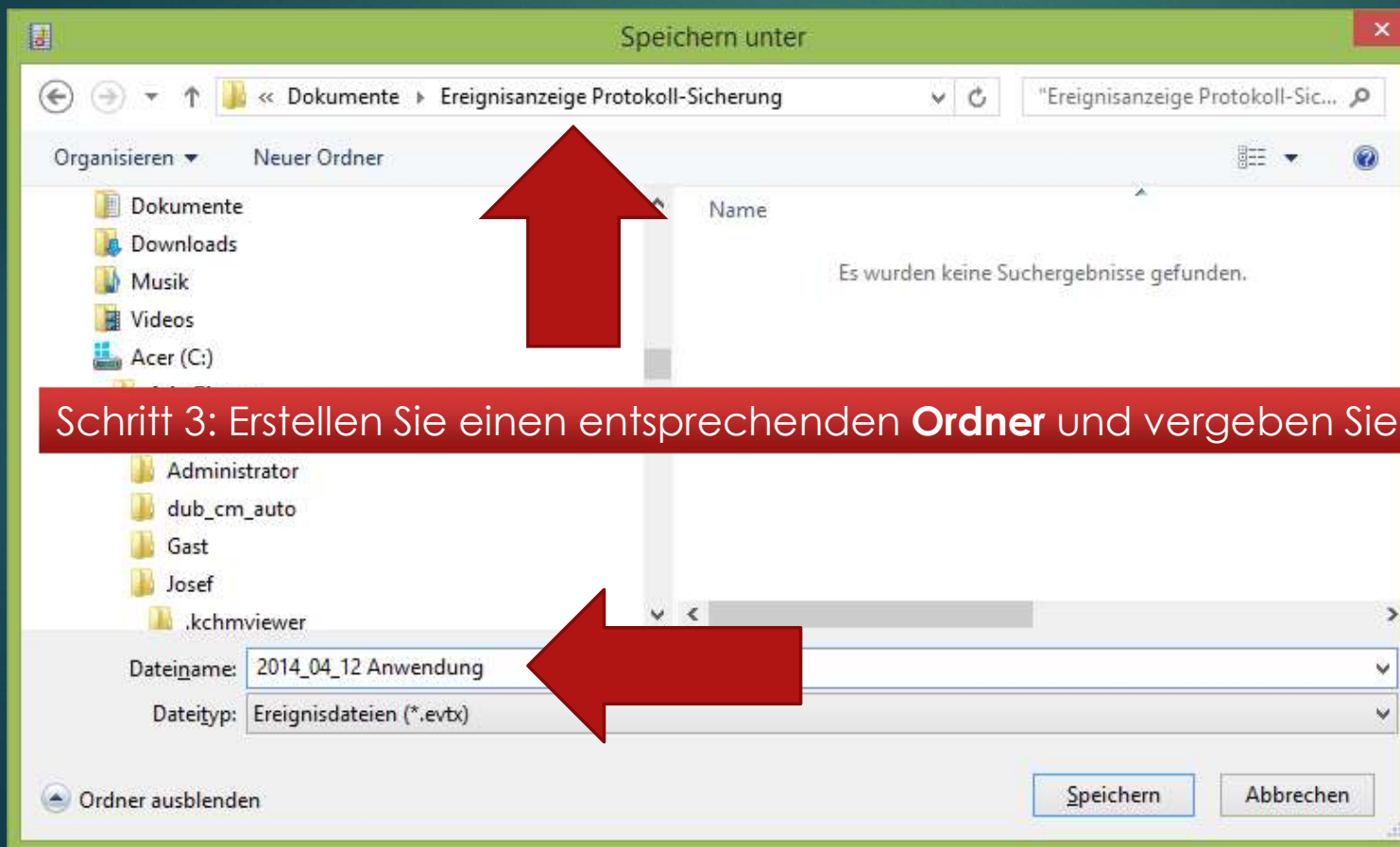


Tipps & Tricks

Protokoll Speichern und Leeren

34

(c) PC-SCHULUNG-SCHREINER



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

Nach einer Woche prüfen Sie wieder Ihren PC

35

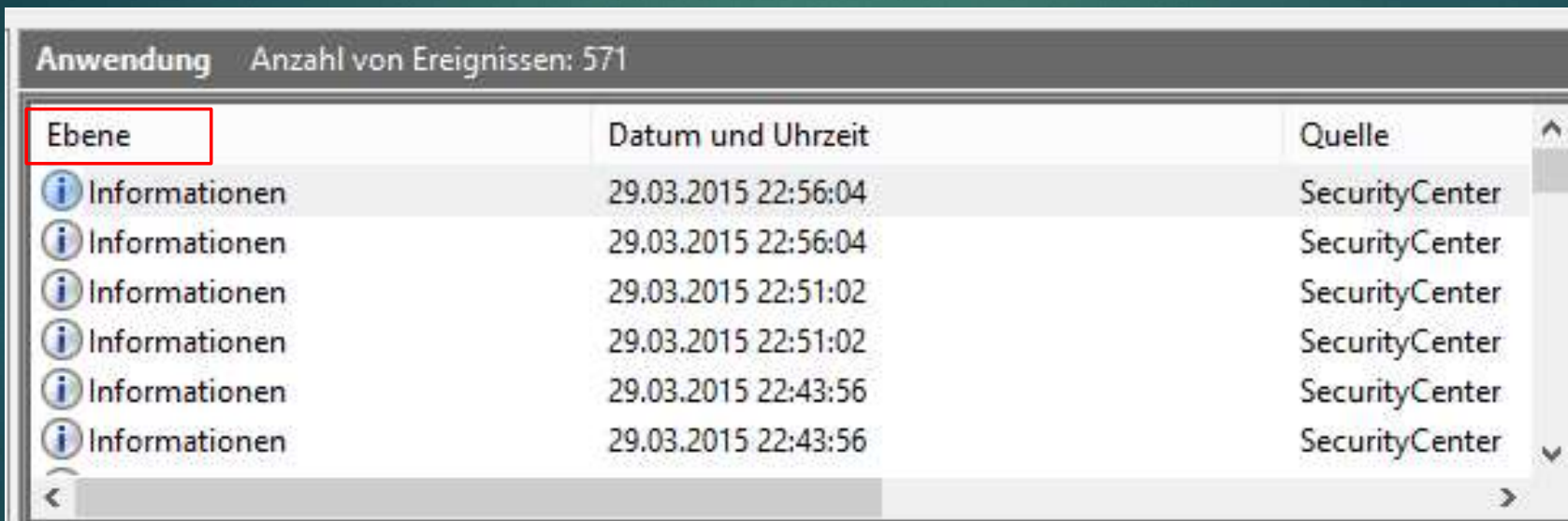
Wenn nach einer Woche wieder Fehler protokolliert sind, so sollten Sie unbedingt die Fehlerursache abstellen.

Tipps & Tricks

Ereignisse sortieren

36

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



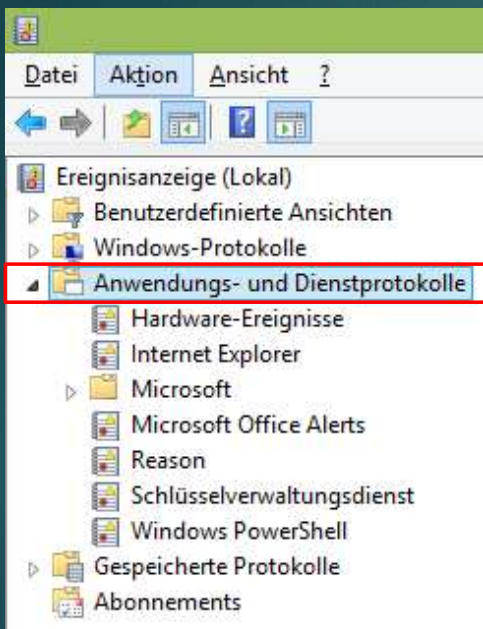
Ebene	Datum und Uhrzeit	Quelle
i Informationen	29.03.2015 22:56:04	SecurityCenter
i Informationen	29.03.2015 22:56:04	SecurityCenter
i Informationen	29.03.2015 22:51:02	SecurityCenter
i Informationen	29.03.2015 22:51:02	SecurityCenter
i Informationen	29.03.2015 22:43:56	SecurityCenter
i Informationen	29.03.2015 22:43:56	SecurityCenter

Anwendungs- und Dienstprotokolle

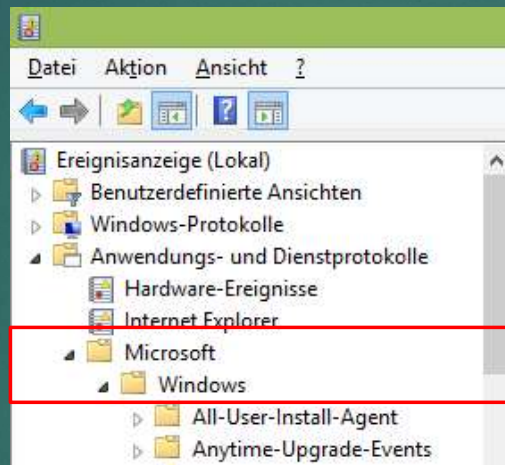
Klicken Sie nacheinander auf:

37

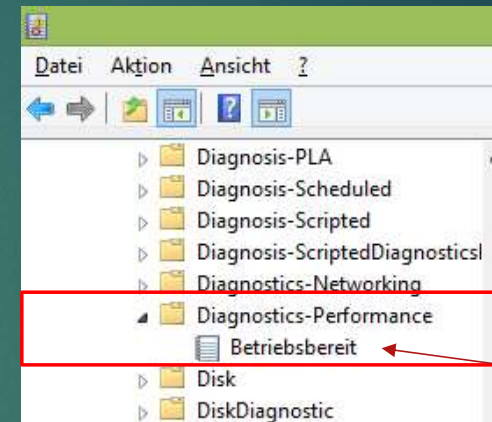
(c) PC-SCHULUNG-SCHREINER



▶ Anwendungs- und Dienstprotokolle



▶ Microsoft
▶ dann auf Windows



▶ Diagnostic-Performance
▶ dann auf Betriebsbereit

**In Windows-Vista
Operational**

Anwendungs- und Dienstprotokolle

Dienste und Programme im Hintergrund

38

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