Windows Ereignisanzeige

Autor: Moser Tobias

Datum: 20.01.2020

Typ: Information

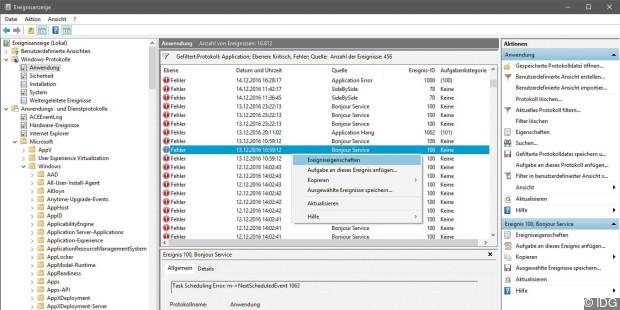
Version: 1.0

**Inhaltsverzeichnis**

|  |
| --- |
| **INHALT** |
| [1 Einleitung 3](#_Toc30662020)  [2 Mächtiges Systemprotokoll mit sperriger Handhabung 3](#_Toc30662021)  [2.1 Ereignisanzeige über das Windows-Kontextmenü öffnen 4](#_Toc30662022)  [2.2 So klassifiziert Windows die Einträge im Systemprotokoll 5](#_Toc30662023)  [3 So lesen Sie die Einträge im Windows-Logbuch richtig 6](#_Toc30662024)  [3.1 Ereignisprotokoll sichern und aufräumen 7](#_Toc30662025)  [3.2 Aufbau eines Protokolleintrags 8](#_Toc30662026)  [4 Ereignisanzeige auf einem Remote-PC öffnen 9](#_Toc30662027)  [4.1 Die Fehlercodes einzelner Ereigniseinträge entschlüsseln 9](#_Toc30662028)  [4.2 Ereigniseinträge sortieren, eigene Ansicht erstellen 10](#_Toc30662029)  [4.3 Ereignisbenachrichtigung erstellen 11](#_Toc30662030) |

# Einleitung

**In der Ereignisanzeige hält Windows alles fest, was im System passiert. Damit wird dieses Protokoll zu einem mächtigen Werkzeug, das Sie bei der Lösung von Hard-und Softwareproblemen unterstützt. Wir zeigen, wie Sie dabei am besten vorgehen.**

**Fehlersuche im Windows-Protokoll.**

Sowohl das Betriebssystem [Windows](https://www.pcwelt.de/handover/451?ws=1) als auch die installierten Programme nutzen das Ereignisprotokoll, um bestimmte Vorkommnisse und Informationen über den Zustand des Systems festzuhalten. Der Zugriff auf das Protokoll erfolgt über die Ereignisanzeige. Darin verzeichnen [Windows](https://www.pcwelt.de/handover/451?ws=1) und Systemdienste beispielsweise, wann das Betriebssystem gestartet wurde, welche Geräte nicht richtig funktionieren und wo Netzwerk- und Softwarefehler aufgetreten sind. Auch allerhand Sicherheitswarnungen werden von diesem Systemtool erfasst. Anhand des Logbuchs können Sie also präzise nachverfolgen, was Ihr System wann gemacht hat. Vor allem im Rahmen von Fehleranalysen können diese Informationen hilfreich sein.

# Mächtiges Systemprotokoll mit sperriger Handhabung

Die Ereignisanzeige geht auf Windows XP zurück und ist neben Windows 10 ebenfalls in Windows 7 und 8.1 enthalten. Durch die an die Serverbetriebssysteme angelehnte Aufmachung und Bedienung erscheint das Bordwerkzeug sperrig und wenig zugänglich. Dabei lohnt sich ein Blick in die vielen Datensätze der Ereignisanzeige nicht im Rahmen der Fehlerbehebung. Durch seine streng chronologische Aufmachung mit Angabe von Datum und Uhrzeit zu jedem Eintrag können Sie rückwirkend nachvollziehen, in welcher Reihenfolge Probleme aufgetreten sind und welche Folgeprobleme dadurch verursacht wurden. Der Funktionsumfang der Ereignisanzeige ist von Windows XP über Vista und Windows 7 hin zu Windows 8/8.1 und Windows 10 gewachsen. Wir beschreiben im Folgenden die Nutzung des Ereignisprotokolls in Windows 10, die identisch mit der Verwendung in Windows 8.1 ist.

## Ereignisanzeige über das Windows-Kontextmenü öffnen



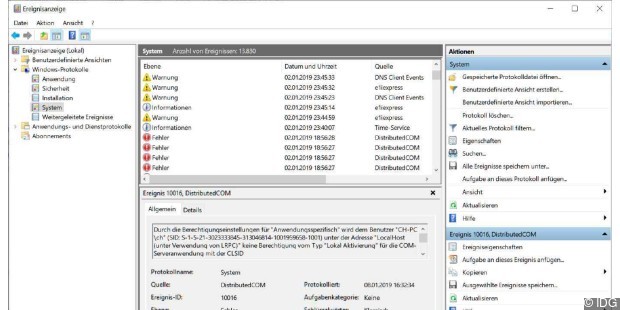
**Mit dem Befehl „Ereignisanzeige“ rufen Sie das Betriebssystemprotokoll auf.**

In [Windows 10](https://www.pcwelt.de/a/windows-fehlersuche-per-ereignisanzeige-so-geht-s,3404408) öffnen Sie die Ereignisanzeige am bequemsten durch einen Rechtsklick auf das Windows-Symbol und den Befehl „Ereignisanzeige“. In Windows 7, 8.1 und 10 können Sie das Logbuch auch über die Eingabe von Ereignisanzeige in die Windows- oder Startmenü-Suchzeile und einen Klick auf „Ereignisanzeige“ starten. Im Startmenü finden Sie die Ereignisanzeige im Untermenü „Windows-Verwaltungsprogramme“. Alternativ lässt sich das Protokoll über den Ausführen-Dialog aufrufen: Drücken Sie dafür die Tastenkombination Windows-R, tippen Sie in das Ausführen-Fenster den Befehl

eventvwr.exe

ein und bestätigen Sie mit „OK“. Daraufhin öffnet sich die Ereignisanzeige in einem neuen Fenster.

## So klassifiziert Windows die Einträge im Systemprotokoll

**Die Klassifikation der Protokolleinträge erfolgt in der ersten Spalte.**

Das wenig übersichtliche Fenster der Ereignisanzeige ist in drei grundlegende Bereiche unterteilt. Über die Leiste ganz links können Sie wie im Explorer auf die einzelnen Protokollbereiche mit den Anwendungsereignissen, Sicherheitsaktivitäten und Systemmeldungen zugreifen. Am wichtigsten sind die Kategorien in dem Bereich „Windows-Protokolle“, die Sie durch Ausklappen erreichen. In [Windows 10](https://www.pcwelt.de/a/windows-fehlersuche-per-ereignisanzeige-so-geht-s,3404408) finden Sie hier die Unterpunkte „Anwendungen“, Sicherheit“, „Installation“, „System“ und „Weitergeleitete Ereignisse“, die Sie regelmäßig überprüfen sollten. Ein Klick auf eines dieser Protokolle bringt Sie zur Liste mit den gespeicherten Protokolleinträgen.

Unter „Anwendungen“ erfassen sowohl Windows als auch verschiedene Anwendungen mehr oder minder wichtige Vorkommnisse. Die Einträge im Protokollordner „Sicherheit“ beschränken sich dabei normalerweise auf Angaben zum Vollzug von Überwachungsaufgaben und sind daher nicht allzu relevant. Auch unter „Installation“ sowie „Weitergeleitete Ereignisse“ findet sich in der Regel kaum Spannendes. Deutlich mehr Informationen lassen sich der Protokollkategorie „System“ entnehmen, die sämtliche im Zusammenhang mit den Systemkomponenten relevante Aktivitäten aufführt.

Auch die im Bereich „Anwendungs- und Dienstprotokolle“ aufgeführten Ereigniskategorien können im Rahmen der Fehlersuche oder beim Überprüfen der Systemsicherheit relevant sein. In diesen Kategorien protokolliert Windows Ereignisse, die keine systemweiten Auswirkungen haben, sondern einzelnen Anwendungen oder Komponenten zugeordnet sind. Ein Klick auf eine der Kategorien öffnet die korrespondierenden Protokolleinträge in der mittleren Spalte der Ereignisanzeige.

Ganz oben erscheinen in der Voreinstellung die neuesten Ereignisse, ältere Protokolleinträge finden Sie weiter unten. Die rechte Spalte des Ereignisanzeige-Fensters führt die jeweils verfügbaren Aktionen auf. Hier können Sie etwa eigene Protokollansichten definieren, zuvor gespeicherte Protokolldateien öffnen oder im Logbuch suchen.

Ein Klick auf einen der tabellarisch aufgeführten Protokolleinträge öffnet die Detailansicht im unteren Fensterbereich. Hier sehen Sie Informationen zur genauen Problemursache und bekommen Angaben dazu, welche Systemkomponenten, Software oder Treiber den betreffenden Eintrag verursacht haben.

# So lesen Sie die Einträge im Windows-Logbuch richtig

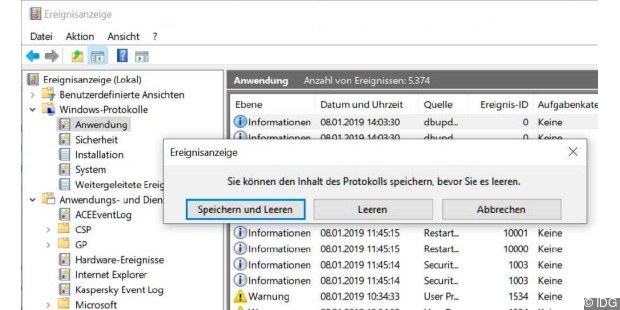
Wenn das Betriebssystem, eine Hardwarekomponente, ein Treiber oder eine systemnahe Anwendung Probleme machen, erscheint in der ersten Spalte der Ereignisliste eine Einstufung, die mit „Warnung“, „Fehler“ oder „Kritisch“ betitelt ist. Einträge mit der Klassifizierung „Information“ können Sie getrost überspringen. Sehen Sie die Liste nach Warnungen und Fehlern durch. Auch wenn viele Einträge erscheinen, ist das kein Grund zur Panik, denn „Fehler“ und „Warnung“ bedeuten anders als „Kritisch“ alleine noch nicht viel.

Welche Ereignisse relevant sind, hängt von verschiedenen Faktoren ab. Achten Sie auf die Spalte „Uhrzeit“. Wenn Ereigniseinträge zum selben Zeitpunkt wie offensichtliche Probleme (externes Gerät nicht ansprechbar, Absturz eines Programms, vorübergehend keine WLAN-Verbindung) auftreten, dann lohnen sich Recherchen anhand der Ereignisdetails, sofern die Probleme wie im Falle einer abgebrochenen WLAN-Verbindung nicht anderweitig einfach lösbar sind.

## Ereignisprotokoll sichern und aufräumen

Haben Sie sich einmal durch die Einträge des Ereignisprotokolls gekämpft, bietet es sich aus Gründen der Übersicht an, das bisherige Logbuch zu löschen.

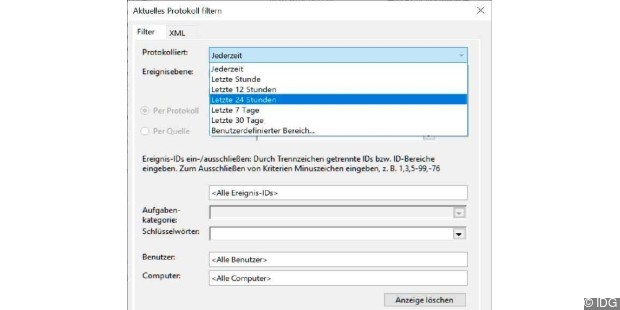
So brauchen Sie beim nächsten Mal nicht durch die Flut bereits bekannter Meldungen zu navigieren und können sich stattdessen auf Neueinträge konzentrieren. Die Löschfunktion hat [Microsoft](https://www.pcwelt.de/handover/380?ws=1) in das Kontextmenü der Protokollkategorien integriert, das nach einem Rechtsklick auf „Anwendungen“, „Sicherheit“, „Installation“ oder „System“ erscheint. Wählen Sie „Protokoll löschen“.



**Das Löschen nicht mehr benötigter Einträge aus dem Protokoll hält die Ereignisübersicht schlank.**

Windows bietet daraufhin in einem neuen Dialog an, das Protokoll zu löschen, indem Sie auf „Leeren“ klicken oder das Protokoll zunächst zu speichern und dann zu löschen. Wenn Sie das bisherige Protokoll etwa zu Vergleichs- oder Dokumentationszwecken vor dem endgültigen Entfernen sichern möchten, gehen Sie auf „Speichern und Leeren“. Wählen Sie nun einen Speicherordner sowie einen Dateinamen. Es empfiehlt sich ein Dateiname, an dem Sie später leicht erkennen können, um welchen Protokolltyp es sich handelt. Sinnvoll ist es, als Dateiname die jeweilige Protokollkategorie gefolgt von einer kurzen Problembeschreibung und dem Datum zu verwenden, beispielsweise „Büro-PC Anwendungen Netzwerkfehler 2017-Januar-13“. Die so gespeicherte Datei können Sie in der Ereignisanzeige jederzeit über den Befehl „Aktion –› Gespeicherte Protokolldatei öffnen“ laden und betrachten.

## Aufbau eines Protokolleintrags



**VDie Einträge im Ereignisprotokoll lassen sich über einen Filter zeitlich eingrenzen.**

Windows kennzeichnet die einzelnen Einträge in den Protokollen unter „Anwendung“, „Sicherheit“ und „System“ je nach Art und Wichtigkeit zusätzlich mit verschiedenen Symbolen. Einträge, die in der ersten Spalte als „Informationen“ gekennzeichnet sind, sind meist banaler Natur und daher mit einem grafischen „i“ für „Information“ markiert. So gibt es etwa bei jedem Windows-Start und beim Herunterfahren des PCs standardmäßig Einträge mit den Ereignisnummern 6005 und 6006, die lediglich festhalten, dass die Ereignisprotokollierung gestartet oder beendet wurde.

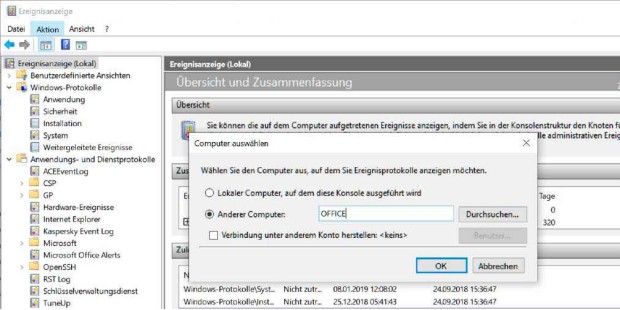
Warnungen mit einem gelben Dreiecksymbol und Fehler mit einem roten Kreis und weißem Ausrufezeichen sollten Sie genauer unter die Lupe nehmen, sie sind unter Umständen Hinweise auf schwerwiegende Probleme bis hin zu Datenverlust, allerdings sind sie längst nicht immer gravierend.

Mit einem Doppelklick auf eines der aufgeführten Protokollereignisse wechseln Sie zu den detaillierten Ereignisinformationen. Hier sind neben Datum und Zeit noch verschiedene Fakten festgehalten. Bei „Quelle“ steht der Name der Windows- oder Softwarekomponente, die das betreffende Ereignis ausgelöst hat. Außerdem enthält jeder Ereigniseintrag eine eigene Nummer – die so bezeichnete Event-ID –, die Sie hinter „Ereignis-ID“ ablesen können. Am aussagekräftigsten ist der Beschreibungstext, der normalerweise am meisten Platz beansprucht. Dort erläutert Windows je nach Ereignis mehr oder weniger ausführlich, was es mit dem Eintrag auf sich hat.

# Ereignisanzeige auf einem Remote-PC öffnen

Mithilfe der Ereignisanzeige können Sie nicht nur das Systemprotokoll Ihres eigenen Rechners einsehen, sondern auch einen Blick in die Warn- und Fehlermeldungen von anderen Rechnern im Heimnetzwerk werfen.

Um die Ereignisanzeige auf einem Remote-Computer zu öffnen, starten Sie das Systemtool zunächst wie gewohnt, etwa in [Windows 10](https://www.pcwelt.de/a/windows-fehlersuche-per-ereignisanzeige-so-geht-s,3404408) per Rechtsklick auf das Windows-Symbol, gefolgt von einem Klick auf „Ereignisanzeige“.



**Die Klassifikation der Protokolleinträge erfolgt in der ersten Spalte.**

Im Ereignisanzeige-Tool wählen Sie dann „Aktion –› Verbindung mit anderem Computer herstellen“. Es öffnet sich ein neuer Dialog, in dem Sie entweder den Namen des Computers im [Netzwerk](https://www.pcwelt.de/a/windows-fehlersuche-per-ereignisanzeige-so-geht-s,3404408) ohne vorangestellte „\\“ eingeben und mit „OK“ bestätigen oder auf „Durchsuchen“ klicken, um ihn im [Netzwerk](https://www.pcwelt.de/a/windows-fehlersuche-per-ereignisanzeige-so-geht-s,3404408) zu suchen. Haben Sie sich für „Durchsuchen“ entschieden, klicken Sie auf „Erweitert –› Jetzt suchen“ und warten, bis Windows unten im Fenster die im Netzwerk verfügbaren Computernamen anzeigt. Markieren Sie einen Computer und klicken Sie danach zwei Mal auf „OK“, um die Verbindung herzustellen und das Remote-Ereignisprotokoll anzuzeigen.

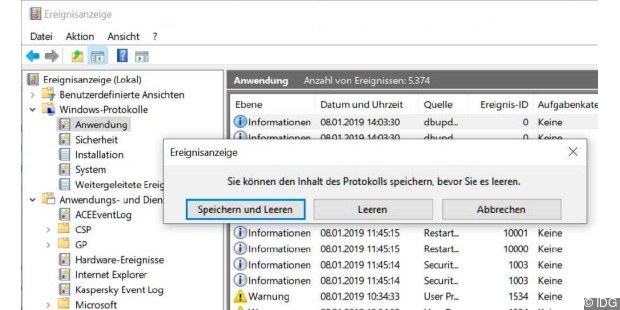
## Die Fehlercodes einzelner Ereigniseinträge entschlüsseln

Konkrete Hinweise über die Fehlerquelle liefert die Ereignis-ID. Die ID 4321 besagt beispielsweise, dass die für Ihren Rechner vorgesehene IP-Adresse nicht registriert werden konnte, weil sie etwa bereits von einem anderen Gerät im [Netzwerk](https://www.pcwelt.de/a/windows-fehlersuche-per-ereignisanzeige-so-geht-s,3404408) belegt ist. Aus dem Eintrag mit der ID 7023 erfahren Sie, dass Windows den angegebenen Dienst nicht ordnungsgemäß starten konnte oder der betreffende Dienst unvorhergesehen beendet wurde.

Weil sich niemand alle Ereignis-IDs merken kann, hat [Microsoft](https://www.pcwelt.de/handover/380?ws=1) hinter „Weitere Informationen“ eine Onlineverknüpfung zur Microsoft-Webseite eingebaut, die allerdings nur selten brauchbare Informationen liefert. Ein paar mehr Hinweise enthält die Webseite  [https://technet.microsoft.com/de-de/ms772425.aspx](https://www.pcwelt.de/handover/1222?redirect=http%3A//clkde.tradedoubler.com/click%3Fp%3D81561%26a%3D1573066%26g%3D0%26epi%3DPCW-LDB_microsoftstore.com%26url%3Dhttps%3A//technet.microsoft.com/de-de/ms772425.aspx) . Sie ist Bestandteil von [Microsoft](https://www.pcwelt.de/handover/380?ws=1) TechNet und ermöglicht Ihnen eine Überprüfung von Ereignis-IDs.

Wenn es um die genaue Bedeutung und Interpretation eines Protokolleintrags geht, liefern die Onlinedatenbanken  [www.eventid.net](http://www.eventid.net)  sowie  [www.ultimatewindowssecurity.com](http://www.ultimatewindowssecurity.com)  meist aussagekräftigere Angaben. Diese Datenbanken beinhalten neben passenden Fehlerbeschreibungen auch Tipps zur Problemlösung. Auch eine Websuche liefert in den meisten Fällen hilfreiche Ergebnisse. Suchen Sie beispielsweise bei Google mit den Stichwörtern „Ereignis ID xxxx“ oder „Event ID xxxx“, wobei Sie den Platzhalter xxxx durch die fragliche ID aus der Ereignisanzeige ersetzen. Verfeinern lässt sich die Suche, wenn Sie markante Teile der Beschreibung über die Zwischenablage mit dazu setzen. Öffnen Sie einen Eintrag in der Ereignisanzeige mithilfe eines Doppelklicks, markieren Sie mit der [Maus](https://www.pcwelt.de/a/windows-fehlersuche-per-ereignisanzeige-so-geht-s,3404408) einen Teil des Beschreibungstextes und drücken Sie als Nächstes Strg-C. Wechseln Sie daraufhin zum Browser und fügen Sie den kopierten Text mit Strg-V in das Suchfeld ein.

## Ereigniseinträge sortieren, eigene Ansicht erstellen



**Das Löschen nicht mehr benötigter Einträge aus dem Protokoll hält die Ereignisübersicht schlank.**

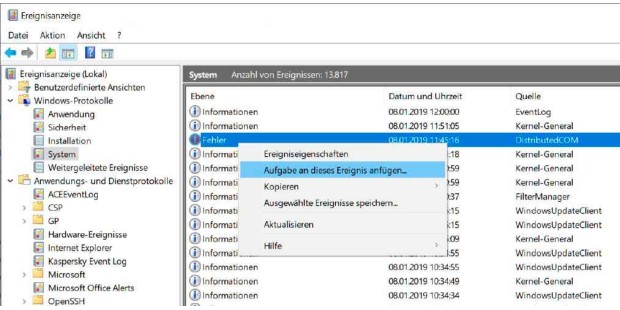
Haben Sie einen verdächtigen Eintrag gefunden, sollten Sie auch die zeitlich umliegenden Einträge in der Ereignisliste untersuchen. Oftmals wiederholt sich ein Fehler, beispielsweise bei jedem Systemstart oder beim Zugriff auf ein bestimmtes Laufwerk. Um sich einen schnellen Überblick über alle kritischen Fehler oder die Warnungen im Protokoll zu verschaffen, können Sie die Liste sortieren. Klicken Sie hierzu auf die Spaltenüberschrift „Ebene“. Windows zeigt die Einträge mit der Stufe „Warnung“ und „Fehler“ dann untereinander an.

Möchten Sie schnell einen Überblick über die in der Datenflut verborgenen wichtigen Einträge erhalten, können Sie die Inhalte der Ereignisanzeige filtern oder eine benutzerdefinierte Ansicht erstellen. Die beiden Funktionen finden sich in der Aktionsleiste rechts im Ereignisanzeigetool. Klicken Sie auf „Aktuelles Protokoll filtern“, um die Ansicht etwa auf Einträge der Kategorie „Kritisch“ oder „Fehler“ einzuschränken. Möchten Sie die Filterauswahl als eigene Ansicht speichern, die Sie zukünftig mithilfe eines Doppelklicks direkt aufrufen können, wählen Sie bitte den Befehl „Benutzerdefinierte Ansicht erstellen“.

In beiden Fällen gibt Ihnen der Filterauswahldialog die Möglichkeit, die Ereignisse über das Ausklappfeld „Protokolliert“ zeitlich einzuschränken. Voreingestellt ist „Jederzeit“ für sämtliche Einträge, Sie können stattdessen auch „Letzte Stunde“, „Letzte 12 Stunden“ oder „Letzte 7 Tage“ angeben. So können Sie gezielt den Zeitstempel von Fehlern und Warnungen mit dem Zeitpunkt eines PC-Absturzes oder einem fehlerhaften Gerätezugriff vergleichen und Rückschlüsse ziehen, was, aus welchem Grund nicht geklappt hat. Setzen Sie bei „Ereignisebene“ Häkchen vor die gewünschten Klassifizierungen und bestätigen Sie Ihre Wahl mittels „OK“. Wenn Sie eine neue Ansicht erstellen, müssen Sie nun noch den Namen eingeben, unter dem Windows Ihren neuen Filter speichert.

## Ereignisbenachrichtigung erstellen

Sollte Ihnen ein Eintrag in der Ereignisanzeige verdächtig erscheinen, etwa weil er auf einen defekten Treiber oder Zugriffsfehler auf ein bestimmtes Laufwerk hinweist, können Sie sich automatisch informieren lassen, falls das Problem erneut auftritt. Gehen Sie dazu in der Ereignisanzeige zur jeweiligen Protokollkategorie und klicken Sie in der Tabelle den gewünschten Eintrag mit der rechten Maustaste an. Wählen Sie „Aufgabe an dieses Ereignis anfügen“.



**Klicken Sie auf „Aktion –› Verbindung mit anderem Computer herstellen“, um übers Netzwerk Einblick ins Ereignisprotokoll eines Netzwerk-PCs zu erhalten.**

Im ersten Fenster des Assistenten ersetzen Sie die hinter „Name“ vorgeschlagene kryptische Bezeichnung durch einen aussagekräftigen Namen, zum Beispiel „Windows-Update geht nicht“. Klicken Sie auf „Weiter“ und überspringen Sie das nächste Fenster mit „Weiter“. Nun können Sie eine Benachrichtigungsaktion einstellen. Zur Auswahl steht unter anderem „Meldung anzeigen (veraltet“). Lassen Sie sich vom Zusatz „veraltet“ nicht irritieren: Für Ihre Zwecke ist diese Option bestens geeignet. Klicken Sie darauf, dann auf „Weiter“ und geben Sie den gewünschten Meldungstext ein. Mit „Weiter“ und „Fertig stellen“ speichern Sie die automatische Benachrichtigung, die danach aktiv ist.