



Windows Problemlöser

Analysieren

Probleme aufspüren und verstehen
Prozessen auf die Finger schauen



Absichern

Sofortmaßnahmen ergreifen
Windows radikal abdichten

Reparieren

Notfall-Windows bauen und einsetzen
Probleme beim Update beseitigen

Ausreizen

Gratis auf Windows 10 wechseln
Windows schnell mit der Tastatur bedienen



Hochsicherheits- Windows

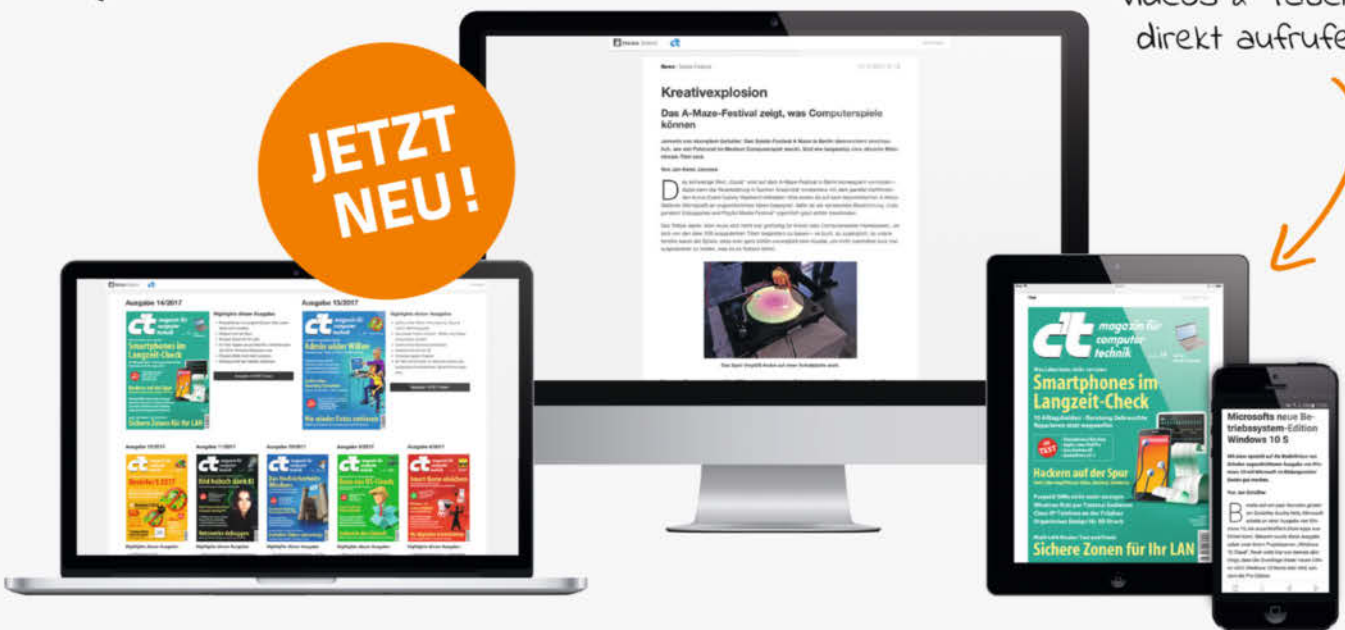
Mit diesen Bordmitteln bekommt Ihr Windows Profi-Schutz

UNABHÄNGIG IN JEDER HINSICHT: c't als Heft und digital auf jedem Gerät lesen

In jedem Browser &
auf jedem Gerät c't lesen

Videos & Tabellen
direkt aufrufen

**JETZT
NEU!**



Leesezeichen & Kommentare
synchronisieren


Optimale Darstellung für
mobile Endgeräte


Testen Sie jetzt c't online und stöbern Sie
3 Monate lang in allen verfügbaren Ausgaben.

Mit Willkommensgeschenk: z.B. ein Kino- und Snack-Gutschein

Zum Angebot: ct.de/digital-erleben

Bitte bei Bestellung über Telefon oder E-Mail angeben: 1CEA1713

 ct.de/digital-erleben

 +49 541/80 009 120

 leserservice@heise.de

**JETZT
TESTEN!**

Alle Jahre wieder

Einige von Ihnen haben in den letzten Wochen in unserer Redaktion angefragt, ob es denn bald wieder ein Sonderheft mit geballtem Windows-Wissen von uns geben wird – nun ist es da! Und anders als im vergangenen Jahr, in dem wir uns speziell dem neuen Windows 10 widmeten, ist dies wieder ein ganz klassisches Best-of der Artikel aus c't, die sich um Microsofts Betriebssysteme drehen.

Systemanalyse, Fehlersuche und -behebung sind schon lange Kernthemen unserer Windows-Sonderhefte. Dabei widmen wir uns diesmal nicht nur Windows-Bordmitteln wie Task-Manager und Ressourcenmonitor, sondern zeigen auch, wie man Windows wirklich präzise überwachen und jedem einzelnen Prozess auf die Finger schauen kann.

Ein Universalwerkzeug bei PC-Problemen ist seit Jahren das c't-Notfall-Windows – ein Baukasten für ein bootfähiges Notfallmedium, gespickt mit allerhand Hilfsmitteln. Es eignet sich nicht nur zur Behebung von Startproblemen, für die Viren-suche und ähnliches, sondern bietet auch Tools zur Hardware-Analyse. Selbstverständlich darf es in diesem Heft nicht fehlen.

Unser c't-Tool für ein Hochsicherheits-Windows ist ein Viren-schutz der eher ungewöhnlichen Art. Es eignet sich, um in

allen gängigen Windows-Versionen die bordeigene Blockier-funktion für unbekannte Programme scharfzuschalten: Mit den richtig gesetzten System Restriction Policies lässt sich selbst ein Windows 10 Home so undurchlässig gegen Trojaner abdichten, wie man es sonst eher auf speziell gesicherten Firmensystemen mit Enterprise-Windows erwarten würde.

Der Umstieg auf Windows 10 und der parallele Betrieb mit einer älteren Version ist nach wie vor ein Thema. Wir zeigen Wege zur Parallelinstallation sowie Tricks, um gängige Probleme von Anfang an zu umschiffen oder sie zu beheben, wenn sie doch einmal auftauchen.

Viel Spaß und gutes Gelingen!

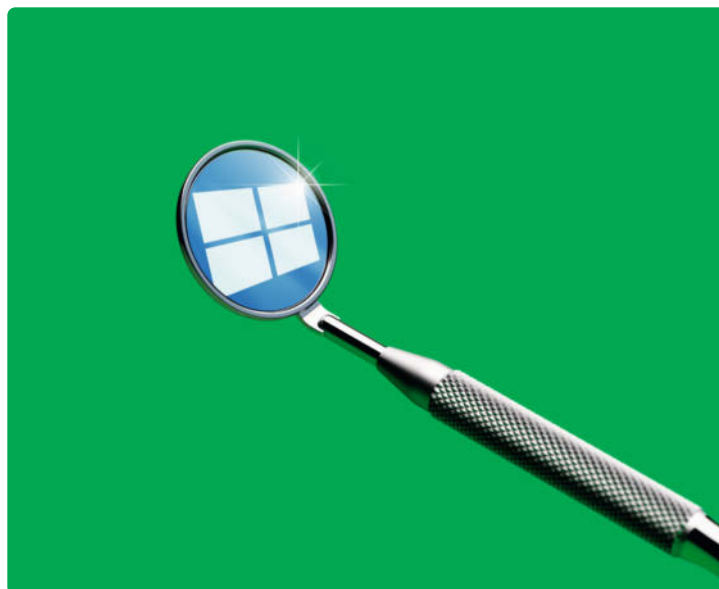


Jan Schüßler

Inhalt

Analysieren

- 7 Die besten Systemwerkzeuge professionell einsetzen
- 10 Windows mit Task-Manager & Co. ausforschen
- 15 Die Ereignisanzeige bei Windows-Problemen nutzen
- 16 Windows Analyse mit dem Process Monitor: Einführung
- 22 Windows Analyse mit dem Process Monitor: Funktionen
- 26 Windows Analyse mit dem Process Monitor: Spezialwissen



Analysieren

Windows tut nicht, was es soll? Lesen Sie, wie Sie Ihrem Betriebssystem mit den bordeigenen und anderen kostenlosen Werkzeugen auf den Zahn fühlen und als Königsdisziplin laufende Prozesse bis ins Detail überwachen können.

Seite 6

Absichern

- 31 c't-Tool aktiviert Profi-Schutz
- 36 Mit Restrictor zum sicheren Windows
- 42 Gefahren von Downloads abschätzen
- 46 Mehr Sicherheit durch gezieltes Deaktivieren unnötiger Funktionen
- 54 Browser und E-Mail gegen Angriffe absichern
- 58 Neuer Schutz im Windows 10 Fall Creators Update

Zum Heft

- 3 Editorial
- 121 Impressum



Absichern

Sie wollen Angriffe verhindern? Schon einfache Maßnahmen im System wappnen Windows gegen viele Attacken von außen. Mit sogenannten Software Restriction Policies können Sie es aber auch zur Hochsicherheitszone machen.

ab Seite 30



Reparieren und helfen

Der Schadensfall ist eingetreten? Oder Sie müssen ungeplant ein System administrieren? Wir helfen – mit unserem Bausatz für ein Notfall-Windows sowie Ratschlägen für Familien- und Aushilfs-Admins. Dazu gibt es Tipps gegen bockige Upgrades und Updates.

ab Seite 64



Ausreizen, optimieren, individualisieren

Sie reizt das riesige Potenzial von Windows? In unserer Auswahl zeigen wir, wie Sie virtuelle Festplatten für Parallelinstallationen nutzen und geben Tipps, wie Sie Ihr System an die eigenen Bedürfnisse anpassen.

ab Seite 108

Reparieren und helfen

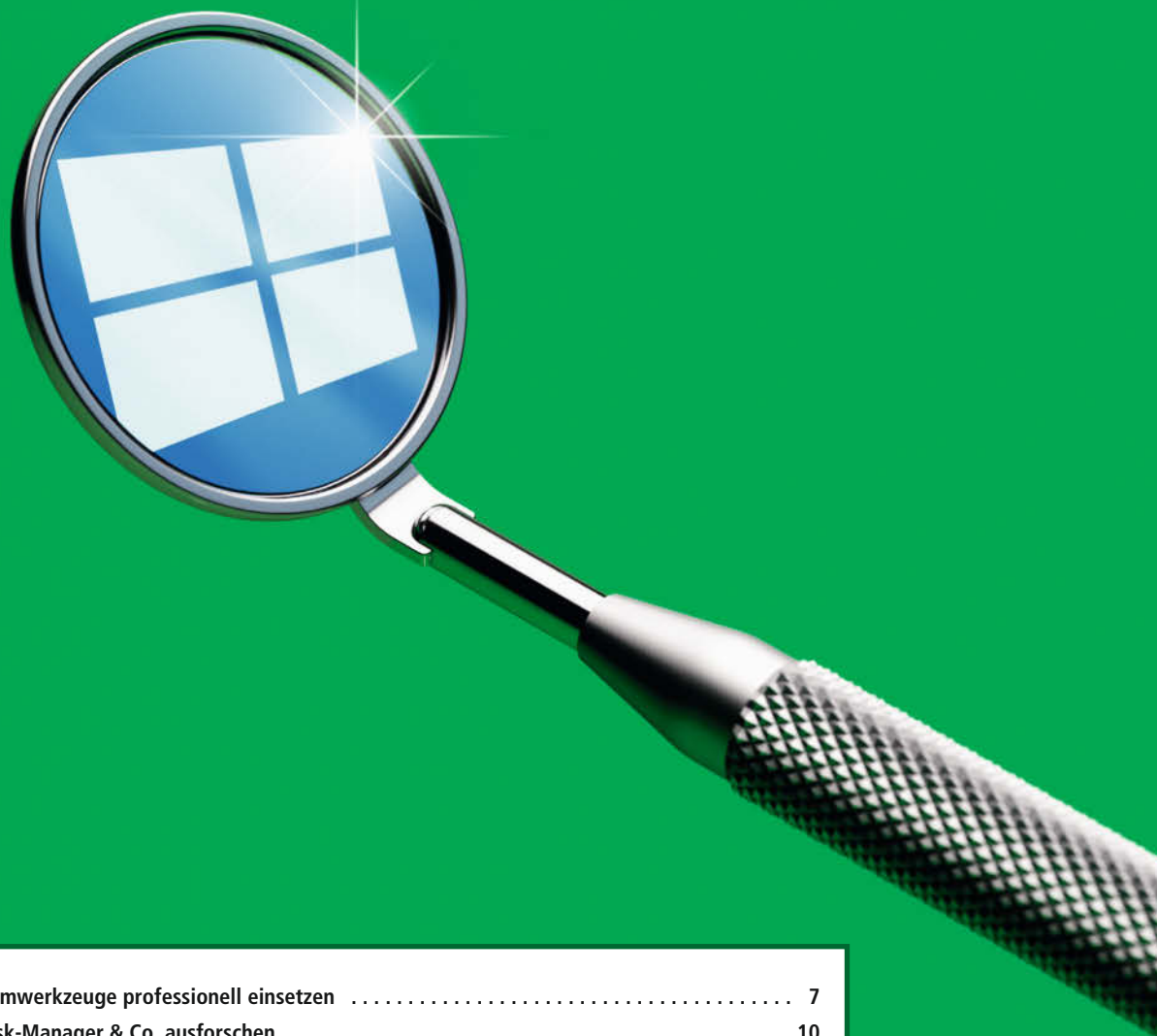
- 65 c't-Notfall-Windows 2018: Bausatz anwenden
- 68 Notfall-Windows: Viren-Alarme einordnen
- 70 Notfall-Windows: Tipps und Tricks
- 76 Notfall-Windows: Viren suchen
- 82 Hilfestellungen für (un-)freiwillige IT-Hausmeister
- 84 Tipps für Admins wider Willen
- 90 Fernwartungssoftware statt Turnschuh-Administration
- 96 Rechtliches für Freizeit- und Auftrags-Admins
- 100 Updates und Upgrades für Windows 10 beherrschen
- 104 Fragen und Antworten zum Windows-Alltag

Ausreizen, optimieren, individualisieren

- 109 Parallelinstallationen zum Testen, Experimentieren, Reinschnuppern
- 110 Zweit-Windows per Drag & Drop
- 116 Upgrade für Windows 10 in einer VHD durchführen
- 118 VHDs mit Snapshots einfrieren
- 122 Automatisierung mit der Windows-Aufgabenplanung
- 124 Tipps für Power-User
- 129 An Windows 10 mit PIN anmelden
- 130 Windows 7 neben Windows 10 installieren
- 134 Richtig umsteigen von Windows 7 auf Windows 10
- 141 Hochauflösende Monitore an Windows 10 betreiben
- 142 Windows-Benutzerkonten mit Sprachprofilen ausstatten
- 144 Mit Windows-Tastenkürzeln schneller ans Ziel
- 148 Fragen und Antworten zum Windows-Alltag

Analysieren

Windows tut nicht, was es soll? Lesen Sie, wie Sie Ihrem Betriebssystem mit den bordeigenen und anderen kostenlosen Werkzeugen auf den Zahn fühlen und als Königsdisziplin laufende Prozesse bis ins Detail überwachen können.



Die besten Systemwerkzeuge professionell einsetzen	7
Windows mit Task-Manager & Co. ausforschen	10
Die Ereignisanzeige bei Windows-Problemen nutzen	15
Windows Analyse mit dem Process Monitor: Einführung	16
Windows Analyse mit dem Process Monitor: Funktionen	22
Windows Analyse mit dem Process Monitor: Spezialwissen	26

Axel Vahldiek

Die besten Systemwerkzeuge professionell einsetzen

Wenn Windows zickt, ist das wie Zahnweh: Es bringt einen zwar nicht um, geht aber kolossal auf die Nerven, und die angeblichen Wundermittelchen vom Quacksalber aus der Seitengasse helfen nicht auf Dauer. Im realen Leben muss man dann zum Zahnarzt, in der Windows-Welt können Sie sich mit professionellem Werkzeug selbst helfen.

Windows-Problemen sowohl am eigenen als auch an fremden Rechnern rücken Sie am besten zielgerichtet und mit geeignetem Werkzeug zu Leibe. In diesem und den folgenden Artikeln zeigen wir, wann sich welche Programme empfehlen und wie Sie möglichst großen Nutzen daraus ziehen. Unterteilt haben wir die Artikel nach Aufgaben: Analyse laufender Prozesse, Auswerten der umfangreichen Windows-eigenen Protokolle sowie Anlegen und Auswerten zusätzlicher Protokolle über sämtliche Zugriffe auf die Festplatte und auf die Registry.

Doch nicht immer muss man gleich zu Spezialwerkzeugen greifen, denn viele Probleme lassen sich viel simpler lösen. Probieren Sie zunächst die in diesem Artikel genannten Tipps durch. Damit erfahren Sie zwar nicht immer, was eigentlich das Problem war, doch macht das ja erst mal nichts. Falls es später doch wieder auftreten sollte, kann man es ja immer noch genauer untersuchen.

Oh, ein Problem

Eines noch vorab: Wenn Sie mit den Werkzeugen aus den nachfolgenden Artikeln auf Windows losgehen, werden Sie auf haufenweise Fehlermeldungen stoßen – so viele, dass man glauben könnte, dass Windows nur aus purem Glück noch läuft. Doch dem ist

keineswegs so, denn Windows stuft alles Mögliche als „Fehler“ ein, was in Wirklichkeit gar kein Problem darstellt. Zum Beispiel prüft Windows beim Öffnen des Startmenüs, ob für diesen Vorgang vom Administrator Gruppenrichtlinien vorgegeben wurden. Falls nicht – was der Normalfall ist – sieht man im Process Monitor (siehe Seite 16) als Ergebnis ein „Not found“. Auch in der Ereignisanzeige werden Sie massenhaft auf angebliche Fehler stoßen. Wenn Windows beispielsweise beim nächsten Neustart Updates installiert, dauert das halt etwas. Windows notiert diese Verzögerung als Fehler, je nach Dauer sogar als „kritischen“, nachzulesen in der Ereignisanzeige unter „Anwendungs- und Dienstprotokolle/Microsoft/Windows/Diagnostics-Performance“. Mehr zur Ereignisanzeige lesen Sie auf Seite 15.

Daher das Allerwichtigste zur Windows-Analyse gleich vorab, denn so trivial und selbstverständlich es auch klingt, wird es doch allzu oft vergessen: Ein Problem haben Sie nur, wenn etwas nicht funktioniert. Ignorieren Sie also erst mal sämtliche Fehlermeldungen und Hinweise, die nicht offensichtlich mit dem Problem zusammenhängen, welches Sie gerade haben.

Ersthelfer

Nun zu den angesprochenen einfacheren Handgriffen: Manche davon sind so trivial, dass gerade Profis sie immer wieder vergessen, zum Beispiel einfach etwas noch mal zu versuchen – vielleicht hat man ja nur versehentlich einen Dialog weggeklickt oder so. Auch gern vergessen wird das Befolgen dieses schönen Spruchs: „Wenns nicht tut, hilft Reboot.“ Letzteres löst zum Beispiel viele Probleme, die auftreten, weil Windows Updates einspielen will, damit aber nur halb fertig geworden ist, weil eben der Neustart noch fehlt.

Des Weiteren bringt Windows einige Hausmittelchen mit, etwa die „Problembehandlung“. Tippen Sie diesen Begriff ins Suchfeld des Startmenüs, öffnen Sie den pas-

senden Suchtreffer und klicken dann oben links auf „Alle anzeigen“. Schauen Sie nach, ob eine Problembehandlung für Ihren akuten Fall vorhanden ist und wenn ja, lassen Sie Windows einfach mal selbst machen. Gute Erfahrungen damit haben wir vor allem bei vermurksten Einstellungen der Netzwerkkarte gesammelt. Details zur Problembehandlung finden Sie in [1].

Wenn der neue Hardware-Treiber zickt, kann man ihn ganz einfach wieder durch den alten ersetzen. Drücken Sie dazu Windows+Pause und klicken dann oben links auf „Geräte-Manager“. Im Kontextmenü der betreffenden Hardware klicken Sie auf „Eigenschaften“ und dort auf „Treiber“. Ein Klick auf den Knopf „Vorheriger Treiber“ restauriert den alten Treiber und nach einem Reboot geht hoffentlich wieder alles.

Ebenfalls als Bordmittel dabei ist die Option, zum letzten Systemwiederherstellungspunkt zurückzukehren. Dabei setzt Windows sich selbst auf einen älteren Stand zurück. Doch Vorsicht: Das bedeutet nicht nur, dass es bei der Rückkehr zu einem Wiederherstellungspunkt die seitdem überschriebenen Dateien restauriert, sondern eben auch die seitdem neu hinzugekommenen löscht. Ihre persönlichen Daten sind dabei zwar normalerweise nicht gefährdet, weil die üblichen Dokumententypen allesamt unangetastet bleiben. Selbst geschriebene Skripte allerdings können dabei verloren gehen, und dieses Schicksal droht auch selbst kreierte und exotischen Dateitypen. Daher ist vor der Rückkehr zu einem älteren Stand unbedingt ein Backup ratsam – aber das ist es ja sowieso immer. Zum Aufrufen der Systemwiederherstellung drücken Sie Windows+Pause, klicken dann links auf „Computerschutz“ und im folgenden Dialog auf „Systemwiederherstellung“. Nach einem Klick auf „Weiter“ werden Ihnen die letzten Wiederherstellungspunkte angeboten, mit einem Häkchen vor „Weitere Wiederherstellungspunkte ...“ alle vorhandenen. Weitere Details zur Systemwiederherstellung finden Sie in [1].

Time of Day	Process	PID	Operation	Path	Result
09:35:06.42110269	mmc.exe	2804	RegOpenKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\{C6037EAB-3A93-4236-8810-BE00A01D071C}\User\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	NAME NOT FOUND
09:35:06.42111606	mmc.exe	2804	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\{C6037EAB-3A93-4236-8810-BE00A01D071C}\User	SUCCESS
09:35:06.42112191	mmc.exe	2804	RegOpenKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\{C6037EAB-3A93-4236-8810-BE00A01D071C}\User\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	NAME NOT FOUND
09:35:06.4212357	mmc.exe	2804	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\{C6037EAB-3A93-4236-8810-BE00A01D071C}\User	SUCCESS
09:35:06.4212781	mmc.exe	2804	RegCreateKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\{C6037EAB-3A93-4236-8810-BE00A01D071C}\User\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	NAME NOT FOUND
09:35:06.4213533	mmc.exe	2804	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\{C6037EAB-3A93-4236-8810-BE00A01D071C}\User	SUCCESS
09:35:06.4213841	mmc.exe	2804	RegCreateKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\{C6037EAB-3A93-4236-8810-BE00A01D071C}\User\Software	SUCCESS
09:35:06.4215406	mmc.exe	2804	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\{C6037EAB-3A93-4236-8810-BE00A01D071C}\User\Software	SUCCESS
09:35:06.4215784	mmc.exe	2804	RegCreateKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\{C6037EAB-3A93-4236-8810-BE00A01D071C}\User\Software\Microsoft	SUCCESS
09:35:06.4216595	mmc.exe	2804	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\{C6037EAB-3A93-4236-8810-BE00A01D071C}\User\Software	SUCCESS
09:35:06.4216900	mmc.exe	2804	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\{C6037EAB-3A93-4236-8810-BE00A01D071C}\User\Software\Microsoft	SUCCESS
09:35:06.4217211	mmc.exe	2804	RegCreateKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\{C6037EAB-3A93-4236-8810-BE00A01D071C}\User\Software\Microsoft\Windows	SUCCESS
09:35:06.4218328	mmc.exe	2804	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\{C6037EAB-3A93-4236-8810-BE00A01D071C}\User\Software\Microsoft	SUCCESS
09:35:06.4218601	mmc.exe	2804	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\{C6037EAB-3A93-4236-8810-BE00A01D071C}\User\Software\Microsoft\Windows	SUCCESS
09:35:06.4219087	mmc.exe	2804	RegCreateKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\{C6037EAB-3A93-4236-8810-BE00A01D071C}\User\Software\Microsoft\Windows\CurrentVersion	SUCCESS
09:35:06.4219913	mmc.exe	2804	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\{C6037EAB-3A93-4236-8810-BE00A01D071C}\User\Software\Microsoft\Windows	SUCCESS
09:35:06.4220200	mmc.exe	2804	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\{C6037EAB-3A93-4236-8810-BE00A01D071C}\User\Software\Microsoft\Windows\CurrentVersion	SUCCESS
09:35:06.4220512	mmc.exe	2804	RegCreateKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\{C6037EAB-3A93-4236-8810-BE00A01D071C}\User\Software\Microsoft\Windows\CurrentVersion\Policies	SUCCESS
09:35:06.4221142	mmc.exe	2804	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\{C6037EAB-3A93-4236-8810-BE00A01D071C}\User\Software\Microsoft\Windows\CurrentVersion	SUCCESS
09:35:06.4221419	mmc.exe	2804	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\{C6037EAB-3A93-4236-8810-BE00A01D071C}\User\Software\Microsoft\Windows\CurrentVersion\Policies	SUCCESS
09:35:06.4221719	mmc.exe	2804	RegOpenKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\{C6037EAB-3A93-4236-8810-BE00A01D071C}\User\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	SUCCESS
09:35:06.4222338	mmc.exe	2804	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\{C6037EAB-3A93-4236-8810-BE00A01D071C}\User\Software\Microsoft\Windows\CurrentVersion\Policies	SUCCESS
09:35:06.4222814	mmc.exe	2804	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\{C6037EAB-3A93-4236-8810-BE00A01D071C}\User\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\LockTaskbar	SUCCESS
09:35:06.4223819	mmc.exe	2804	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy Objects\{C6037EAB-3A93-4236-8810-BE00A01D071C}\User\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	SUCCESS

Viele Fehlermeldungen weisen nicht etwa auf ein Problem hin, sondern auf ganz normale Vorgänge. Hier prüft Windows vor dem Anlegen eines neuen Registry-Schlüssels, ob es ihn schon gibt. Falls nicht – was der Normalfall ist –, meldet es „Name not found“.

Apropos Backup: So eines zurückzuspielen ist ein weiteres simples Mittel zur Lösung von Windows-Problemen. Unterscheiden Sie dabei zwischen dem täglichen Backup Ihrer persönlichen Daten (Tipps dazu standen in [2]) sowie dem Backup der kompletten Windows-Installation mitsamt allen Einstellungen und Anwendungen. Ab Windows 8.1 können Sie für letzteres c't-WImage einsetzen (siehe ct.de/wimage). Wer noch Windows 7 nutzt, kann stattdessen zu Drive Snapshot greifen; eine kostenlose, aber zeitlich beschränkte Vollversion der Software steckt im c't-Notfall-Windows (siehe S. 65).

Sparpotenzial

Wenn die simplen Handgriffe nichts bringen, ist es Zeit für eine Online-Recherche – vielleicht hatten andere das Problem ja auch und konnten es bereits lösen. Dabei werden Sie aber womöglich über Werbeanzeigen stolpern, die Ihnen das Blaue vom Himmel versprechen, gern verbunden mit dem Angebot, kostenlos Ihren PC zu scannen. Sparen Sie sich den Klick darauf: Selbst bei seriösen Angeboten ist nur der Scan kostenlos, die fällige Reparatur aber nicht. Denn von irgendwas muss der Anbieter ja die Anzeigen bezahlen. Und eine Garantie, dass die Reparatur wirklich klappt, gibt es auch nicht.

Sie werden bei der Web-Recherche außerdem viele Ratschläge finden, einfach mal irgendwelche Programme laufen zu lassen, beispielsweise die Freeware „CCleaner“. Doch Obacht: Dieses Tool ist eigentlich zum Entfernen von Datenmüll gedacht und keineswegs ein Universal-Problemlöser. Und die Registry-Optimierung des Programms macht erfahrungsgemäß sogar mehr kaputt als sie repariert [3]. Eine Zeitlang steckte

sogar eine Backdoor drin [4]. Seien Sie also besser vorsichtig sowohl mit diesem als auch mit allen anderen Programmen, die Ihr Problem irgendwie von alleine lösen sollen – je unspezifischer und unbegründeter ein Lösungsvorschlag ist, umso mehr Misstrauen ist angebracht.

Richtig googlen

Das Netz ist durchaus voll von sinnvollen Ratschlägen, man muss nur wissen, wie man sie findet. Dazu gehören zuerst mal die richtigen Suchbegriffe.

Sofern Fehlermeldungen erscheinen, tippt man deren Wortlaut daher kurzerhand eins zu eins ab, und zwar in Anführungsstrichen, damit nur Suchtreffer mit genau derselben Meldung gefunden werden. Viele

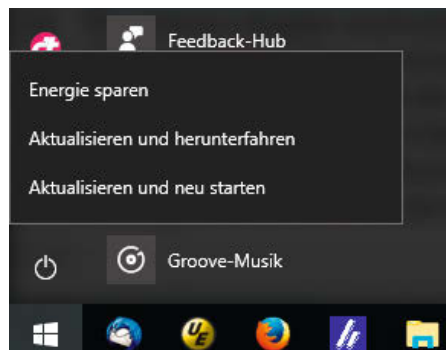
Fehlermeldungen lassen sich per Strg+C und Strg+V woanders einfügen, das vermeidet Tippfehler. Falls dabei chaotisch formatierter Text im Suchschlitz landet, fügen Sie den Text stattdessen in Notepad ein und kopieren dort die entscheidende Fehlermeldung heraus.

Sonst verwenden Sie möglichst präzise Begriffe und vermeiden dabei Umschreibungen. Tippen Sie die Namen der betroffenen Dialoge aus deren Titelzeilen ab. Sofern möglich, hilft auch eine Übersetzung der Frage ins Englische – dafür sind oft mehr Lösungsvorschläge im Netz zu finden als auf Deutsch.

Falls der PC gelegentlich unvermittelt neustartet oder gar in einer Neustart-Schleife hängt, deutet das auf einen Bluescreen hin, dessen Fehlercode ebenfalls bei der Recherche nützlich sein kann. Um den Bluescreen zu sehen, müssen Sie Windows allerdings erst anweisen, ihn auch anzuzeigen statt einfach neuzustarten. Drücken Sie dazu Windows+Pause, klicken dann auf „Erweiterte Systemeinstellungen“, unter „Starten und Wiederherstellen“ auf „Einstellungen“ und entfernen das Häkchen vor „Automatisch Neustart durchführen“.

Microsoft befragen

Noch zielgerichteter suchen Sie, wenn Sie an die Suchanfrage noch etwas anhängen. Denn Microsoft stellt selbst jede Menge Lösungen zum Nachlesen bereit, vor allem in seiner Knowledge Base oder als Antworten fachkundiger Mitarbeiter in den hauseigenen Foren. Bei letzteren muss man sich allerdings oft erst durch längere Threads lesen, daher zuerst zur Knowledge Base. Um die gezielt zu durchsuchen, hängen Sie hinter Ihre Suchanfrage mit einem Leerzeichen ge-



Nicht für jedes Windows-Problem braucht man schweres Gerät. Mitunter reicht stattdessen ein Neustart, etwa wenn sich Windows seltsam verhält, weil es Updates bereits teilweise eingespielt hat, damit aber noch nicht ganz fertig ist.

trennt noch „site:support.microsoft.com“ an. Die dort angebotenen Artikel sind meist im Original englischsprachig, und was Ihnen im Browser angezeigt wird, ist deren maschinelle Übersetzung. Die Qualität der Übersetzungen ist oft fragwürdig, aber wenn man den Mauszeiger über einen Satz hält, erscheint darüber wenigstens das englischsprachige Original.

Sollte in der Knowledge Base nichts zu finden sein, kürzen Sie den Anhang der Suchanfrage auf „site:microsoft.com“. Dann zeigt Google auch die Treffer aus den Microsoft-Foren (answer.microsoft.com). Sie werden hier zwar auch massenhaft unbeantwortete Fragen finden, doch lohnt es trotzdem, nach Antworten Ausschau zu halten. Einige Gruppen von Foren-Teilnehmern stechen dabei besonders heraus: Jene mit der Abkürzung „MSFT“ arbeiten genau wie jene mit dem Namen „Microsoft“ im Profil direkt für den Konzern. Die Wahrscheinlichkeit, dass deren Antwort stimmt, ist daher recht hoch. Die Abkürzung „MVP“ steht für „Most Valuable Professional“, was wiederum eine Auszeichnung von Microsoft für in der Community besonders engagierte Freiwillige ist. Diese Teilnehmer arbeiten also nicht direkt für Microsoft und können für den Konzern nicht sprechen, dafür sind deren Praxis-Tipps mitunter mehr wert als die mancher Microsoft-Mitarbeiter.

Suchtreffer aus den Technet- und MSDN-Bibliotheken von Microsoft (technet.microsoft.com/de-de/library und msdn.microsoft.com/de-de/library) bieten oft qualitativ hochwertige Artikel, die von Menschen ins Deutsche übersetzt wurden. Allerdings vermitteln die Artikel eher Hintergrundwissen und Anleitungen für bestimmte Handgriffe im Unternehmensumfeld sowie für Entwickler. Kon-

krete Lösungen für ein akutes Problem sind eher selten zu finden, dafür aber das Fachwissen, mit dem man das Problem vielleicht selbst lösen kann.

Erst wenn das alles nichts bringt, lohnt der Versuch ohne „site:microsoft.com“. Schließlich können Sie das Ganze noch mal ohne Anführungsstriche durchspielen.

Wenn partout keine Antwort zu finden ist, kann man auch einfach selbst eine Frage stellen. Voraussetzung ist ein Microsoft-Konto. Achten Sie beim Schreiben auf die üblichen Netiquette. Und auch wenn Ihnen Windows gerade furchtbar auf den Keks geht: Vermeiden Sie beleidigende Begriffe dafür. Wer Ihnen helfen soll, muss sich damit auskennen, und so mancher Kenner mag das fragliche Produkt halt auch und nimmt die Beleidigung des Produkts prompt persönlich.

Erst wenn das alles nichts bringt, schlägt die Stunde spezieller Systemwerkzeuge – dann aber richtig. (axv) **ct**

Literatur

- [1] Axel Vahldiek, Heilt von allein, Manchmal reichen für Windows die Hausmittelchen, c't 13/14, S. 84
- [2] Gerald Himmelein, Lutz Labs, Axel Vahldiek, Backup statt Lösegeld, Daten Trojaner-sicher speichern, c't 11/16, S. 102
- [3] Axel Vahldiek, Gezielt ausmisten, Platz schaffen auf der Windows-Partition, c't 12/16, S. 116
- [4] Axel Vahldiek, Olivia von Westernhagen, Schadsoftware vom Virenschutz-Hersteller, Wochenlang Backdoor in CCleaner, c't 21/2017, S. 47

Name	Beschreibung	Speich...	Kategorie	Herausgeber
Aufzeichnen von Audiodateien	Dient dem Erkennen und Behebe...	Lokal	Sound	Microsoft ...
Bluescreen	Probleme behandeln, durch die ...	Lokal	Windows	Microsoft ...
Drucker	Dient dem Erkennen und Behebe...	Lokal	Drucken	Microsoft ...
Eingehende Verbindungen	Dient dem Erkennen und Behebe...	Lokal	Netzwerk	Microsoft ...
Freigegebene Ordner	Dient dem Erkennen und Behebe...	Lokal	Netzwerk	Microsoft ...
Hardware und Geräte	Dient dem Erkennen und Behebe...	Lokal	Gerät	Microsoft ...
Heimnetzgruppe	Dient dem Erkennen und Behebe...	Lokal	Netzwerk	Microsoft ...
Intelligenter Hintergrundübertragungsdienst (Ba...	Probleme erkennen und beheben...	Lokal	Windows	Microsoft ...
Internet Explorer-Sicherheit	Dient dem Erkennen und Behebe...	Lokal	Webbrowser	Microsoft ...
Internetverbindungen	Dient dem Erkennen und Behebe...	Lokal	Netzwerk	Microsoft ...
Leistung von Internet Explorer	Dient dem Erkennen und Behebe...	Lokal	Webbrowser	Microsoft ...
Netzwerkadapter	Dient dem Erkennen und Behebe...	Lokal	Netzwerk	Microsoft ...
Problembehandlung bei der Programmkompati...	Dient dem Erkennen und Behebe...	Lokal	Programme	Microsoft ...
Spracherkennung	Bereiten Sie das Mikrofon vor, un...	Lokal	Windows	Microsoft ...
Stromversorgung	Dient dem Erkennen und Behebe...	Lokal	Stromvers...	Microsoft ...
Suche und Indizierung	Dient dem Erkennen und Behebe...	Lokal	Windows	Microsoft ...
Systemwartung	Dient dem Erkennen und Bereinig...	Lokal	System	Microsoft ...
Tastatur	Sucht und korrigiert Probleme mi...	Lokal	Windows	Microsoft ...
Videowiedergabe	Probleme mit der Wiedergabe vo...	Lokal	Windows	Microsoft ...
Wiedergeben von Audiodateien	Dient dem Erkennen und Behebe...	Lokal	Sound	Microsoft ...
Windows Media Player-Bibliothek	Dient dem Erkennen und Behebe...	Lokal	Medienwi...	Microsoft ...
Windows Media Player-DVD	Dient dem Erkennen und Behebe...	Lokal	Medienwi...	Microsoft ...
Windows Media Player-Einstellungen	Dient dem Erkennen und Behebe...	Lokal	Medienwi...	Microsoft ...
Windows Store-Apps	Probleme behandeln, die die ord...	Lokal	Windows	Microsoft ...
Windows Update	Lösen Sie Probleme, durch die ei...	Lokal	Windows	Microsoft ...

So manches Problem kann Windows selbst lösen, beispielsweise mit der bordeigenen „Problembehandlung“.

Mit Spaß ins neue Jahr!



Mit 12 der besten Cartoons aus **ct**

Alle aktuellen Zeitschriften, ausgewählte Fachbücher, eBooks und digitale Magazine für Heise Medien- oder Maker Media-Abonnenten oder ab einem Einkaufswert von 15 € versandkostenfrei.

Bestellen Sie ganz einfach online unter shop.heise.de/2018 oder per E-Mail: service@shop.heise.de

heise shop

shop.heise.de/2018



Hajo Schulz

Windows mit Task-Manager & Co. ausforschen

Der Task-Manager liefert durchaus brauchbare Informationen, wenn es darum geht herauszufinden, womit sich Windows gerade beschäftigt. Einige seiner Ausgaben sind aber interpretationsbedürftig. Wo er an seine Grenzen stößt, stehen weit mächtigere Werkzeuge zur Verfügung.

Der PC fühlt sich irgendwie langsam an, die Festplatte röhrt ständig vor sich hin, der Notebook-Akku ist schon nach der halben Zeit leer: Es gibt die unterschiedlichsten Gründe, warum man wissen will, was Windows so alles treibt. Ist das System mal wieder mit sich selbst beschäftigt, weil es gerade den Suchindex aktualisiert oder nach Updates sucht? Oder treibt womöglich eine Malware ihr Unwesen und versendet megabyteweise Spam?

Je nachdem, wie detailliert die Antworten auf diese Fragen ausfallen sollen und wie intensiv Sie sich überhaupt damit beschäftigen wollen, bieten sich unterschiedliche Diagnoswerkzeuge an. Schon in Windows selbst

sind brauchbare Messinstrumente enthalten, deren erweiterte Funktionen sich aber nicht auf den ersten Blick erschließen. Wer noch tiefer einsteigen will, findet im Internet häufig kostenlose Software, die den vollen Durchblick verspricht – wirklich empfehlenswert sind nur wenige Tools, und auch die guten brauchen Einarbeitung, wenn man sie voll ausnutzen will.

Task-Manager

Für einen ersten Überblick darüber, was gerade so alles läuft, ist der in Windows enthaltene Task-Manager das ideale Werkzeug. Mit der Tastenkombination Strg+Umschalt+Esc

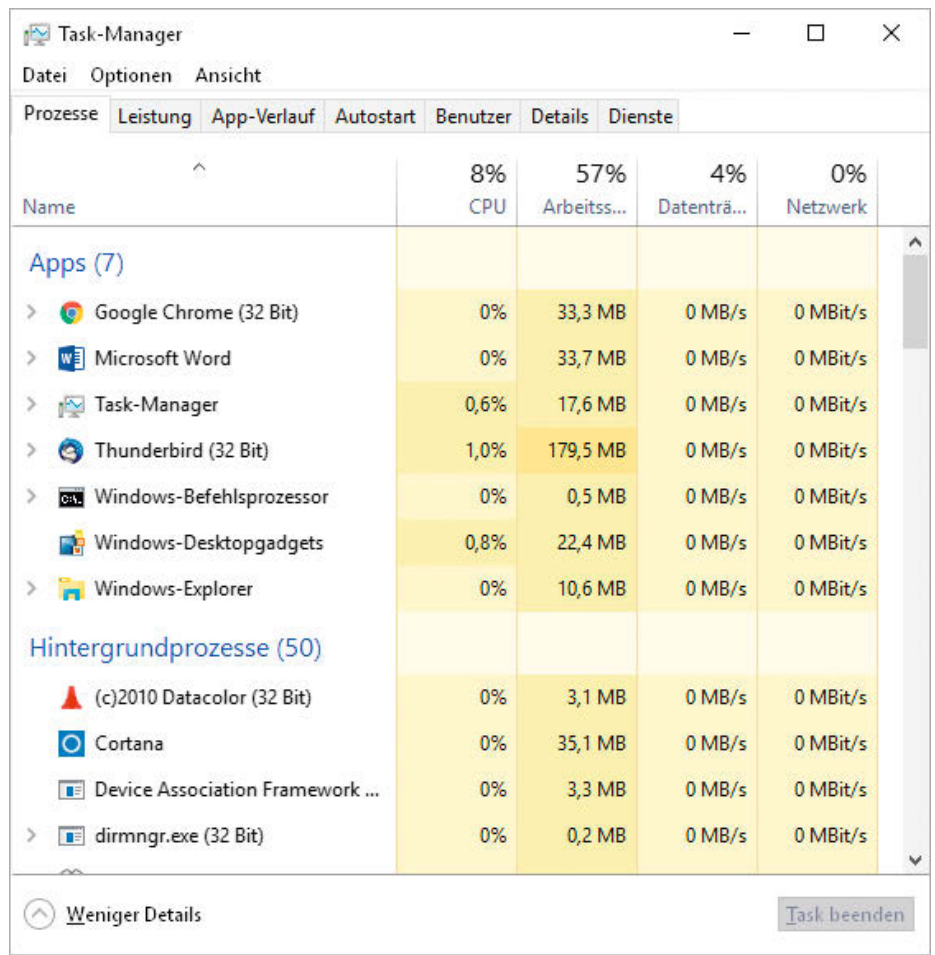
ist er schnell gestartet. Seit Windows 8 hat er gegenüber den Vorversionen deutlich hinzugelern. Beim ersten Aufruf präsentiert er sich allerdings erst einmal sehr reduziert: Man sieht lediglich eine Liste der gerade geladenen Apps und Programme; die Einträge besitzen ein kurzes Kontextmenü mit den wichtigsten Befehlen. Seinen vollen Funktionsumfang offenbart der Task-Manager nach einem Klick auf „Mehr Details“.

Schon das erste Register „Prozesse“ reicht häufig aus, um herauszufinden, womit der PC gerade seine Zeit vertröhelt: Die globale Auslastung von CPU, Hauptspeicher, Festplatte und Netzwerkanschluss steht in den Spaltenköpfen über den jeweiligen Einträgen der laufenden Prozesse. Ein Klick auf einen Spaltenkopf sortiert – wie bei allen tabellarischen Ansichten des Task-Managers – die Prozessliste nach diesem Kriterium, sodass das Programm, das aktuell beispielsweise die meiste Datenträgeraktivität verursacht, ganz oben erscheint. Ebenfalls wie bei allen Tabellen im Task-Manager lassen sich über einen Rechtsklick auf einen Spaltenkopf weitere Detail-Spalten ein- oder angezeigte ausblenden.

Praktisch ist die Kategorisierung der laufenden Prozesse in Apps, Hintergrund- und Windows-Prozesse, wobei sich die Unterscheidung der letzten beiden Kategorien nicht immer erschließt. Apps – und dazu gehören auch traditionelle Windows-Anwendungen, die sich mit einem Fenster auf dem Bildschirm zeigen – erscheinen nach einem Klick auf die Spaltenüberschrift „Name“ ganz oben in der Liste. Ein Klick auf den Pfeil vor einem Eintrag öföhnet die Liste der zum jeweiligen Prozess gehörenden Fenster, die sich über das Kontextmenü schließen („Task beenden“) oder in den Vordergrund holen lassen. Wem die Kategorisierung der Prozesse nicht gefällt, der kann sie über den Menübefehl „Ansicht/Nach Typ gruppieren“ ausschalten.

Etwas eigentümlich verhält sich die Spalte „Status“, wenn man sie einblendet: In der Grundeinstellung ist der Eintrag bei allen Prozessen leer. Erst wenn man sie mit dem Menübefehl „Ansicht/Statuswerte/Anhaltstatus anzeigen“ aktiviert, erscheint bei inaktiven Apps „Angehalten“.

Wer die Auslastung verschiedener Ressourcen im zeitlichen Verlauf beobachten



Der Windows-eigene Task-Manager hat mit Windows 8 viele Funktionen hinzugewonnen. Er zeigt sie aber erst nach einem Klick auf „Mehr Details“.

möchte, ist auf dem Task-Manager-Register „Leistung“ richtig: Für jede der Ressourcen Prozessor, Arbeitsspeicher, Datenträger und Netzwerk gibt es hier eine Kurve, die zeigt, wie stark das System und Anwendungen die jeweilige Komponente während der letzten Minute beansprucht haben. Ein Klick in die Liste auf der linken Seite ruft rechts eine vergrößerte Ansicht der jeweiligen Ressource mit Zusatzinformationen auf den Plan.

Hat man die CPU-Auslastung ausgewählt, kann man das Diagramm per Rechtsklick umschalten zwischen einer kumulierten Ansicht und einer, bei der jeder logische Prozessorkern eine eigene Grafik bekommt. Der Erkenntnisgewinn ist dabei aber nur gering: Eine unter Vollast arbeitende Single-Thread-Anwendung zeigt sich nur selten daran, dass ein einzelner Kern zu 100 Prozent beschäftigt ist.

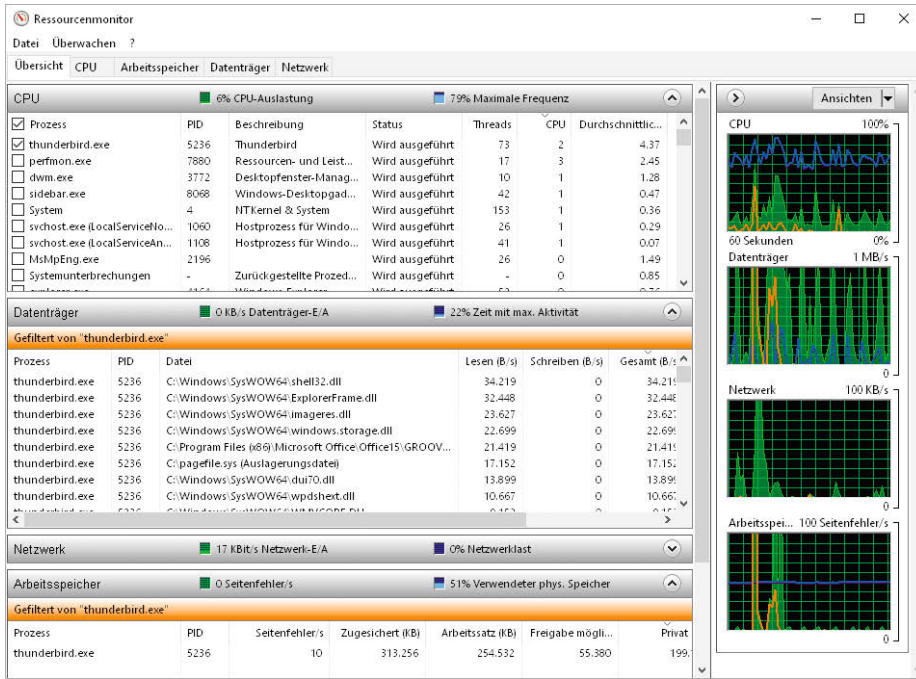
Um zu erkennen, dass ein Prozess einen CPU-Kern voll auslastet, zum Beispiel weil ein Bug ihn in eine Endlosschleife gestürzt hat, muss man also die Gesamtauslastung der CPU im Auge behalten: Sinkt die etwa auf einem Vierkerner mit Hyper-Threading dau-

erhaft nicht unter 12,5 Prozent, liegt der Verdacht nahe, dass ein Prozess einen Kern voll beschäftigt.

Bei der Analyse eines aktuellen Performance-Problems sind die Task-Manager-Register „App-Verlauf“ und „Benutzer“ meist von untergeordneter Bedeutung. Interessanter ist da schon der Tab „Autostart“: Auf ihm finden Sie möglicherweise die Antwort auf die Frage, warum ein bestimmtes Programm überhaupt gerade läuft. Außerdem liefert der Task-Manager eine Einschätzung, wie sehr die erkannten Autostart-Programme den Windows-Start verzögern. Die größten Zeitfresser lassen sich per Kontextmenü an Ort und Stelle deaktivieren. Allerdings wertet der Task-Manager bei Weitem nicht alle Mechanismen im Dateisystem und in der Registry aus, über die Windows Programme, Dienste und Treiber beim Systemstart lädt. Ein gründlicheres Werkzeug stellen wir weiter unten vor.

Die ausführlichsten Informationen über gerade laufende Prozesse liefert der Task-Manager auf seinem Register „Details“. Erwähnenswert ist hier vor allem der Befehl „Spalten

WERKZEUGE ZUR PROZESSANALYSE		
Programm	Quelle	Funktion
Task-Manager	Windows	schneller Überblick über laufende Prozesse und Systemlast
Ressourcenmonitor	Windows	Analyse der Auslastung von CPU, Festplatte und Netzwerk
Process Explorer	sysinternals.com	tiefgehende Analyse laufender Programme
Autoruns	sysinternals.com	Analyse und Konfiguration von Autostart-Programmen



Den Aktivitäten einzelner Programme kann man mit dem Ressourcenmonitor auf den Grund gehen. Die Grafiken geben aber Gelegenheit zu Fehlinterpretationen.

auswählen“ im Kontextmenü der Überschriften der Tabellenspalten. Darüber lässt sich unter anderem recht schnell herausfinden, ob ein bestimmtes Programm 32- oder 64-bittig ist (Spalte „Plattform“) und ob es mit Administratorrechten läuft („Heraufgestuft“). Trotzdem gilt auch für den „Details“-Tab: Wer wirklich alles über einen laufenden Prozess erfahren will, greift besser zu einem potenteren Werkzeug – dazu gleich mehr.

Auch das Register „Dienste“ dient eher der schnellen Übersicht als der ausführlichen Konfiguration und Diagnose. Immerhin lassen sich von hier aus einzelne Dienste über ihr Kontextmenü starten und beenden. Der Befehl „Dienste öffnen“ lädt das zuständige Snap-in der Computerverwaltung zur Dienste-Konfiguration. Um einen bestimmten Dienst hier wiederzufinden, sollte man eine Ungereimtheit kennen: Was die Computerverwaltung „Name“ nennt, heißt im Task-Manager „Beschreibung“; der „Name“ aus dem Task-Manager taucht in der Dienste-Konfiguration nur auf den Eigenschaften-Seiten auf.

Ressourcenmonitor

Das zweite wichtige Tool zur Performance-Diagnose aus dem Lieferumfang von Windows, der Ressourcenmonitor, spielt seine Stärken gegenüber dem Task-Manager vor allem dann aus, wenn es darum geht, die Aktivitäten einzelner Prozesse genauer zu untersuchen. Starten lässt er sich am einfachsten über einen Link unten auf der Seite „Leistung“ des Task-Managers, alternativ mit der

Eingabe `resmon` im „Ausführen“-Dialog (Win+R).

Ein frisch geöffnetes Ressourcenmonitor-Fenster zieren am rechten Rand vier Grafiken, deren Interpretation sich allerdings nicht auf den ersten Blick erschließt. Gemeinsam ist ihnen, dass sie die Systemaktivitäten der letzten 60 Sekunden darstellen und dabei jeweils zwei Graphen in einem gemeinsamen Fensterchen verwenden: eine grüne Fläche und eine blaue Linie. Im Falle der CPU-Auslastung ist der wichtigere Graph der grüne, denn er zeigt die Prozessorauslastung in Prozent. Die blaue Linie steigt umso mehr, je länger die CPU mit vollem Takt gelaufen ist; umgekehrt deutet ein tiefer Wert darauf hin, dass der Prozessor es sich leisten konnte, durch Heruntertakten Strom zu sparen.

Am missverständlichsten sind wahrscheinlich die Grafiken für den Datenverkehr mit Datenträgern und dem Netzwerk: „Alles grün“ bedeutet noch lange keine Volllast, denn die grüne Fläche skaliert sich jeweils automatisch so, dass die Spitzen nicht allzu weit aus der Anzeige herausragen. Die aktuelle Skalierung steht in der rechten Ecke über der Grafik. Sind hier bei den Datenträgern beispielsweise nur „100 KB/s“ angegeben, dreht sich die Festplatte praktisch im Leerlauf, selbst wenn sich die grüne Kurve im oberen Bereich bewegt. Aussagekräftiger ist die blaue Kurve, die stets die prozentuale Auslastung anzeigt. Beim Netzwerk hat aber auch sie nur beschränkte Aussagekraft: Ist der Rechner per Gigabit-Ethernet mit einem

Router verbunden, wertet der Ressourcenmonitor erst 1000 MBit/s als 100 Prozent, selbst wenn der Router Daten nur mit 20 MBit/s aus dem Internet saugen kann.

Beim Arbeitsspeicher gibt die blaue Linie die prozentuale Belegung des RAM an, die grüne Fläche die – skalierten – „Seitenfehler“ (seit Windows 10 1607: „Harte Fehler“) pro Sekunde. Trotz der Bezeichnung gibt ein Wert jenseits von null hier erst einmal keinen Anlass zur Besorgnis: Ein Seitenfehler – englisch „page fault“ – tritt immer dann auf, wenn ein Prozess versucht, auf eine Adresse im virtuellen Speicher zuzugreifen, der gegenwärtig kein physisches RAM zugeordnet ist. Das passiert, wenn Windows diesen Speicherbereich ausgelagert hat oder wenn ein Prozess zum ersten Mal auf einen Adressbereich im Programmcode zugreift. Dann muss Windows diesen Speicherbereich zunächst aus der Auslagerungsdatei oder aus einer EXE- oder DLL-Datei von der Festplatte füllen; das geschieht immer für eine komplette Speicherseite von üblicherweise 4 KByte Größe am Stück. Wenn Sie gerade eine größere Anwendung laden, ist eine hohe Zahl von Seitenfehlern also völlig normal. Erst wenn Sie hier im laufenden Betrieb ständig eine grüne Linie am Anschlag beobachten, steckt offenbar zu wenig RAM für die derzeitigen Aufgaben in Ihrem Rechner. Sie sollten dann darüber nachdenken, ihn aufzurüsten oder weniger Programme gleichzeitig zu betreiben.

Die Listen in der linken Seite des Ressourcenmonitors schlüsseln die Angaben der Graphen nach Prozessen auf. Die Tabellen für Datenträger- und Netzwerkzugriffe gehen sogar noch einen Schritt weiter und spendieren den Zugriffen auf einzelne Dateien beziehungsweise Netzwerk-Gegenstellen eigene Einträge. Ständige Lese- und Schreibzugriffe auf die Auslagerungsdatei `C:\pagefile.sys` ergeben so etwa einen weiteren Hinweis auf die Überlastung des Arbeitsspeichers. Alle Tabellen lassen sich durch Klicks auf Spaltenüberschriften neu sortieren; die Kontextmenüs der Spaltenköpfe enthalten Befehle zum Aus- und Einblenden von Detailangaben.

Mit den Kästchen vor den Einträgen der Prozessliste unter „CPU“ kann man die Zeilen der anderen Tabellen filtern, sodass dort nur noch die Daten der ausgewählten Prozesse zu sehen sind. Zu den globalen Graphen gesellt sich dann jeweils eine orangefarbene Linie, die den Anteil der markierten Prozesse an der grünen Fläche darstellt.

Der Filter bleibt auch bestehen, wenn man über die Karteireiter am oberen Fenster Rand auf eine der anderen Seiten des Ressourcenmonitors umschaltet, um sich weitere Details anzeigen zu lassen. Besonders erwähnenswert ist hier die Seite „CPU“: Sie hilft

bei der Jagd nach CPU-Zeit fressenden Diensten. Stellt sich nämlich in der Übersicht heraus, dass svchost.exe schuld an den unerklärlichen Systemaktivitäten ist, kann man damit zunächst meist nicht viel anfangen: Jede Instanz dieses Programms birgt in der Regel mehrere Dienste. Um herauszufinden, welcher davon gerade durchdreht, klappen Sie im Ressourcenmonitor einfach die Liste der Dienste auf und sortieren sie nach der Spalte „CPU“. Wie beim Task-Manager liefert die Spalte „Beschreibung“ die Namen, unter denen Sie die Dienste in der Computerverwaltung wiederfinden.

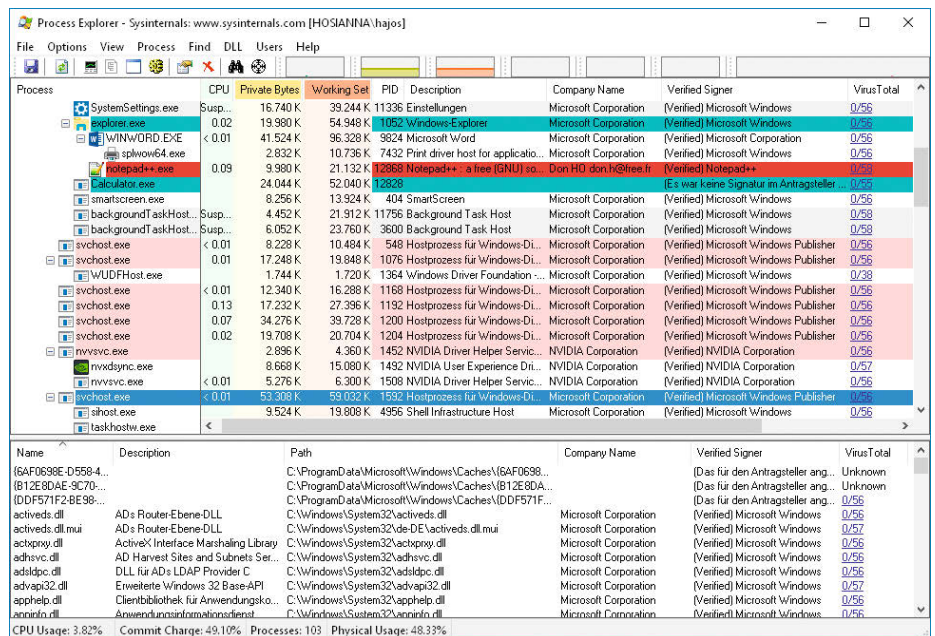
Process Explorer

Wo die Diagnose-Tools aus dem Windows-Lieferumfang an ihre Grenzen stoßen, müssen externe Werkzeuge her, allen voran die aus der Sysinternals-Serie. Sie lassen sich kostenlos herunterladen und laufen ohne besondere Installation (siehe ct.de/wgwb).

Eines der populärsten Werkzeuge aus dieser Reihe ist der Process Explorer. Eingefleischte Fans bezeichnen ihn gerne als Task-Manager auf Steroiden, aber das wird seinem Funktionsumfang nur teilweise gerecht: Er eignet sich unter anderem auch zur Malware-Jagd und steht Entwicklern bei der Fehlersuche zur Seite.

Beim ersten Start möchte der Process Explorer einmalig seine Lizenzbestimmungen bestätigt haben und präsentiert sich dann als zunächst ziemlich furchtneinflößende, unübersichtliche und bunte Liste der laufenden Prozesse. Die vermeintliche Unordnung röhrt daher, dass der Process Explorer die aktiven Prozesse in einer Baumstruktur anzeigt, bei der der „Vater“ eines Prozesses immer derjenige ist, der das „Kind“ gestartet hat. Top-Level-Einträge repräsentieren entweder Prozesse, die das System beim Start geladen hat, oder solche, deren Erzeuger nicht mehr läuft. Über einen Klick auf die Spaltenköpfe lässt sich die Liste ohne Einrückungen nach jedem angezeigten Merkmal sortieren; mehrfache Klicks auf die Überschrift „Process“ bringen die Strukturansicht zurück.

Die angezeigten Attribute lassen sich über den Befehl „Select Columns“ aus dem Kontextmenü der Spaltenköpfe oder dem View-Menü den eigenen Bedürfnissen anpassen. Dabei kann man aus insgesamt 117 Werten auswählen – zu viele, um ständig alle im Blick zu haben. Das muss man aber gar nicht: Der Process Explorer kann über Befehle aus dem View-Menü bis zu zehn „Column sets“ speichern und wieder laden. Man stellt sich also die angezeigten Spalten so ein, wie es für die anstehende Aufgabe gerade sinnvoll ist, und speichert diese Zusammenstellung dann unter einem Namen. Mit wenigen Klicks oder den Tastaturkürzeln Strg+1 bis



Nur nicht bange machen lassen: Die Detailfülle der Informationen, die der Process Explorer anzeigt, kann erschlagen, lässt sich aber bändigen.

Strg+0 lassen sich diese Konfigurationen jederzeit wiederherstellen.

Die Konfigurationen speichern nicht nur die in der Prozessliste angezeigten Spalten, sondern auch diejenigen, die die Tabelle in der unteren Fensterhälfte darstellt: Einschalten lässt sie sich mit dem Menübefehl „View/Show Lower Pane“ oder dem Tastenkürzel Strg+L. Sie kennt zwei Ansichten: In der ersten, auszuwählen mit Strg+D, listet sie alle DLLs, die der ausgewählte Prozess gerade geladen hat. Die zweite (Strg+H) bietet eine Übersicht über alle Handles des aktuellen Prozesses, also seine geöffneten Dateien, Registry-Schlüssel, Synchronisationsobjekte und so weiter. Mit dem Menübefehl „Find/Find Handle or DLL“ (Strg+F) kann man auch global über alle Prozesse nach solchen geöffneten Objekten suchen und sie über den Befehl „Close Handle“ aus ihrem Kontextmenü dem Eigentümer-Prozess entreißen. Aber Achtung: Damit bringen Sie unter Umständen das jeweilige Programm zum Absturz. Trotzdem kann der Befehl als letzte Rettung sinnvoll sein, etwa wenn sich eine Datei partout nicht löschen lässt, weil ein Prozess sie ständig in Benutzung hat.

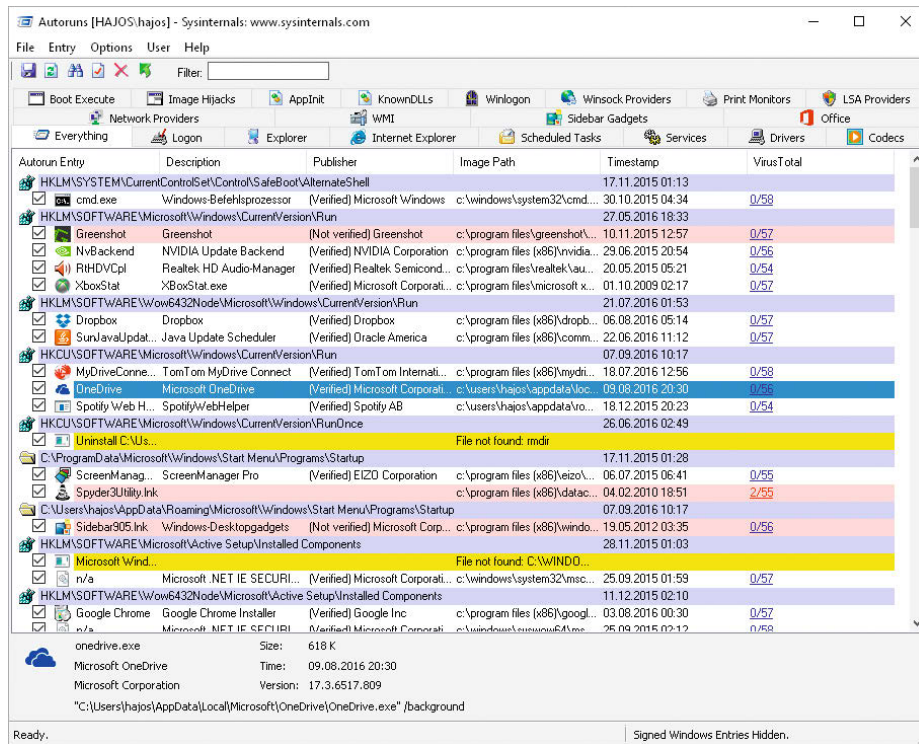
Viren-Schnellcheck

Zu den Spalten-Auswahlsätzen, die erfahrene Process-Explorer-Anwender in ihrer Sammlung haben, gehört einer, der dabei hilft, dem Verdacht auf Schädlinge im System nachzugehen. Zusätzlich zu den standardmäßig dargestellten Spalten zeigt er

mindestens die Attribute „Company Name“, „Verified Signer“ und „VirusTotal“; die zuständigen Schalter finden sich auf den Registern „Process Image“ und „DLL“ des „Select Columns“-Dialogs.

Damit die Spalte „Verified Signer“ sinnvolle Werte anzeigt, muss im Options-Menü der Eintrag „Verify Image Signatures“ eingeschaltet sein. Daraufhin erscheint bei jedem Prozess die Angabe, wer die dazugehörige ausführbare Datei digital signiert hat. Unsignierte Dateien oder solche, bei denen hier eine Fehlermeldung auftaucht, sind per se noch kein Sicherheitsrisiko. Erhöhtes Misstrauen ist aber angesagt, wenn eine unsignierte Datei in der Spalte „Company Name“ behauptet, von einem großen Hersteller wie Microsoft, Intel oder Nvidia zu stammen, oder wenn „Company Name“ und „Verified Signer“ nicht zusammenpassen.

Um die „VirusTotal“-Spalte mit Leben zu füllen, empfiehlt es sich, im Options-Menü unter „VirusTotal.com“ die Option „Check VirusTotal.com“ zu setzen; bei einer stabilen Internetverbindung ohne Volumenkosten sollte man auch „Submit Unknown Executables“ aktivieren. Das bewirkt, dass der Process Explorer die ausführbare Datei jedes laufenden Prozesses durch den Webdienst VirusTotal.com überprüfen lässt: Dort suchen derzeit 67 verschiedene Virens Scanner in den übermittelten Dateien nach Virensignaturen. Das Scan-Ergebnis merkt sich die Webseite mit einem SHA256-Hashes der Datei. Das nutzt der Process Explorer, indem er im ersten Anlauf nur die Hashes von EXE- und DLL-Dateien an VirusTotal.com übermittelt; erst



Wie der Process Explorer bietet das Programm Autoruns Funktionen an, die der Abwehr von Viren und anderen Schädlingen dienen.

wenn dabei ein „Unknown“ herauskommt, überträgt er die komplette Datei und lässt sie neu scannen.

Das Ergebnis in der Spalte „VirusTotal“ lautet im Idealfall bei allen Prozessen „0/n“ mit n zwischen 50 und 67. Kleine von 0 verschiedene Zahlen deuten meist auf Fehlalarme einiger der befragten Scanner hin; wer es genauer wissen will, klickt das Ergebnis im Process Explorer an und schickt damit seinen Browser auf die VirusTotal-Seite mit den ausführlichen Ergebnissen.

Hat man einen oder gar mehrere Prozesse als Malware identifiziert, ist es nur die zweitbeste Idee, sie über den Menübefehl „Process/Kill Process“ sofort zu beenden. Stattdessen empfiehlt es sich, sie erst einmal mit dem Menübefehl „Process/Suspend“ anzuhalten. Gegen das Abschießen schützen sich nämlich viele Schädlinge, indem sie mehrere Prozesse starten, die einander sofort neu laden, sobald einer verschwindet. Ein schlafender Prozess ist einerseits schwerer zu erkennen und kann andererseits seine Kumpagne nicht mehr schützen.

Unheil kann ein angehaltener Prozess vorläufig ebenso wenig anrichten wie ein beendeter. Er steckt aber noch im Speicher und man kann über seine Eigenschaften in Ruhe versuchen, Informationen zu sammeln, um den Infektionsweg oder mögliche Nebenwirkungen zu identifizieren. Besonders interessant sind unter anderem die Felder „Autostart Location“ und „Parent“ auf der Seite

„Image“ sowie die Seite „Strings“ des „Properties“-Dialogs. Beim Sammeln weiterer Hinweise kann auch der Befehl „Process/Search Online“ helfen, der den Standard-Browser öffnet und eine vorformulierte Anfrage an die dort konfigurierte Suchmaschine richtet.

Löschen kann man die infizierte EXE-Datei freilich nicht, solange sie noch als Prozess geöffnet ist. Aber das fällige Herunterfahren sowie eine gründliche Analyse und Reinigung des Systems mit einem externen Antivirenprogramm ersetzt der Process Explorer ohnehin nicht.

Autoruns

Ein weiteres beliebtes Sysinternals-Werkzeug hört auf den Namen Autoruns. Der Performance-Analyse dient es zwar nur indirekt, kann aber trotzdem wertvolle Hilfe leisten, wenn es darum geht herauszufinden, was gerade so alles im System läuft – und vor allem: warum. Dazu klappert Autoruns alle bekannten Stellen in der Registry und im Dateisystem ab, die dafür zuständig sind, dass Programme beim Systemstart, bei der Benutzeranmeldung und zu einigen anderen Gelegenheiten automatisch gestartet werden.

Das Programm präsentiert sich ähnlich bunt und auf den ersten Blick unübersichtlich wie der Process Explorer, die innere Logik erschließt sich aber recht schnell: Die hellblau hervorgehobenen Zeilen repräsentieren

die Registry-Schlüssel und Dateipfade, in denen das Tool nach Autostart-Programmen sucht, darunter zeigt es jeweils die dort gefundenen Einträge. Hellrot sind Einträge markiert, bei denen etwas mit der Signatur der zugehörigen Programmdatei nicht stimmt, gelb solche, die auf eine nicht existierende Datei verweisen.

Die Liste lässt sich auf verschiedene Arten filtern: Den größten Durchblick verschaffen die Karteireiter am oberen Fensterrand, die die Einträge nach dem Anlass des Startkategorisieren; die wichtigsten sind „Logon“ und „Services“. Über Befehle im Options-Menü lassen sich alle Einträge ausblenden, bei denen das Programm von Microsoft stammt, oder nur solche, die von Haus aus zu Windows gehören – an letzteren sollte man nicht ohne Not herumfummeln, um die Systemstabilität nicht zu gefährden.

Der Befehl „Options/Scan Options“ bietet Schalter für Funktionen, die denen des Process Explorer für den Malware-Check ähneln: Autoruns kann die Signaturen der automatisch gestarteten Programme überprüfen und sie von VirusTotal.com auf Viren checken lassen.

Dem Kampf gegen Malware dienen auch der Befehl „File/Analyse Offline System“ sowie die Einträge im „User“-Menü: Mit ihnen lassen sich die Autostarts eines gerade nicht laufenden, parallel installierten Windows beziehungsweise die eines anderen Benutzerkontos analysieren. Damit umgeht man wirksam Schutzmechanismen, die manche Schädlinge enthalten und die im laufenden Betrieb verschleiern, wer oder was sie startet.

Um den automatischen Start eines Programms oder Dienstes zu verhindern, klickt man einfach das Häkchen vor seinem Eintrag aus. Das löscht ihn nicht komplett, sondern deaktiviert ihn erst einmal nur. Wenn sich nach dem nächsten Systemstart herausstellt, dass man dadurch eine wichtige Funktion außer Betrieb gesetzt hat, kann man den Autostart an derselben Stelle wieder aktivieren.

Wer lieber von Hand in der Registry oder im Dateisystem herumfummeln möchte, findet im Kontextmenü von Autoruns-Einträgen den Befehl „Jump to Entry“, der den Explorer oder den Registry-Editor an der Stelle öffnet, wo der jeweilige Autostart konfiguriert ist. „Jump to Image“ schickt einen Explorer in den Ordner mit der ausführbaren Datei. Ist neben Autoruns auch der Process Explorer installiert, kann man letzteren mit dem gleichnamigen Kontextmenübefehl aufrufen und sich dort die Eigenschaften des laufenden Prozesses anzeigen lassen. (hos) **ct**

Sysinternals-Tools:
ct.de/wgby

Jan Schüßler

Die Ereignisanzeige bei Windows-Problemen nutzen

Wenn Windows rumzickt, kann ein Blick in die Ereignisanzeige erhellend sein. Allerdings ist nicht alles problematisch, was Windows einen Fehler nennt – es gilt, in der Masse der Ereignisse die tatsächlichen Warnsignale zu erkennen.

Windows protokolliert in der Ereignisanzeige, was es für erwähnenswert hält. Das sind nicht nur schwere Systemfehler, ungewöhnliche Neustarts und Ähnliches, sondern auch Hinweise auf unsauber konfigurierte Netzwerkschnittstellen, Erfolg oder Fehlschlag bei Windows-Updates, gestartete Dienste und ganz schlicht das Hoch- und Runterfahren.

Die allermeisten Ereignisse, die Windows auflisten kann, sind rein informativer Natur und allenfalls für statistische Zwecke oder für Entwickler zum Debugging von Interesse. Macht Windows Probleme, landen allerdings auch darüber oft Einträge in den Ereignisprotokollen.

Material sichten

Die Ereignisanzeige starten Sie am schnellsten per Tastatur (Windows-Taste, „ereig“, Eingabetaste) oder ab Windows 8 per Maus über das WinX-Menü (Rechtsklick in der linken unteren Bildecke, Klick auf Ereignisanzeige). Auf der Startseite präsentiert sie eine „Zusammenfassung der administrativen Ereignisse“ der letzten sieben Tage. Hier sind vor allem die Ereignistypen „Kritisch“ und „Fehler“ einen Blick wert. Ein Klick auf das Pluszeichen links neben dem Ereignistypnamen klappt die Kategorie auf und zeigt, welche Ereignis-IDs in der letzten Zeit protokolliert wurden, welche Quelle sie ausgelöst hat und in welchem Protokoll sie gelandet sind.

Apropos „in welchem Protokoll“: Protokolle gibts massenhaft; klappt man in einem Windows 10 Pro in der aktuellen Version 1709 die Kategorien „Windows-Protokolle“

und „Anwendungs- und Dienstprotokolle“ komplett auf, zählt man über 380 Stück.

Auch wenn Ihr PC absolut einwandfrei funktioniert, wird die Ereignisanzeige Sie trotzdem mit reichlich Einträgen zu Fehlern und Warnungen konfrontieren. Doch dabei gilt: locker bleiben, denn im Alltag fallen reichlich harmlose Ereignisse an, die Windows als Fehler oder Warnungen bezeichnet. Typisch sind etwa Warnungen zu Zeitüberschreitungen bei der Namensauflösung (Ereignis-ID 1014, Quelle DNS Client Events), wenn die Verbindung zum WLAN zwischen-drin abgerissen ist. Windows 10 erzeugt jedes Mal, wenn eine Kachel-App aktualisiert wird, einen Eintrag zu einem „Fehler beim Ändern des AppModel Runtime-Status“ (69, AppModel-Runtime). Solange alles stabil läuft, können Sie diese Einträge getrost ignorieren. Mehr noch: Sie sollten gar nicht erst in die Versuchung kommen, diese vermeintlichen Fehler zu beheben – effektiver lässt sich keine Lebenszeit vernichten.

Um bei tatsächlich instabil laufendem Windows nicht die Nadel im Heuhaufen suchen zu müssen, bieten sich zwei Ansätze an. Der erste ist ein Doppelklick auf die nach ID sortierten Ereigniseinträge in der „Zusammenfassung der administrativen Ereignisse“: Er listet alle Ereignisse dieses Typs chronologisch sortiert auf. Ein Klick auf ein Ereignis zeigt unterhalb der Liste Details an, die bei der Eingrenzung des Fehlers hilfreich sein könnten – zum Beispiel, welcher Treiber abgestürzt ist oder welche Festplatte zickt. Wie in einem Webbrowser gelangt man mit der Zurück-Schaltfläche oben links wieder auf die Zusammenfassungsseite.

Der zweite Ansatz ist vor allem bei Systemabstürzen sinnvoll: Unter „Windows-Protokolle/System“ landet das Gros der Ereignisse, die auf defekte Hardware hinweisen können. Hier finden sich Bluescreens (1001, Bug-Check) ebenso wieder wie völlig unkontrollierte Neustarts (41, Kernel-Power) und aussteigende Festplatten (beispielsweise 51, disk oder 157, disk oder 129, storahci).

Abgesehen von solchen typischen Fällen ist die Fülle an Ereignis-IDs schier unüber-

schaubar; dass die IDs je nach Quelle völlig unterschiedliche Bedeutungen haben, macht die Sache nur noch unübersichtlicher. Der kommerzielle Anbieter eventid.net pflegt eine umfangreiche und kostenlos nutzbare Datenbank von ID-/Quellen-Kombinationen (siehe ct.de/w9yw). Oft sind die dort gebotenen Informationen schon hilfreich; für eine Jahresmitgliedschaft ab 29 US-Dollar gibts Extraleistungen wie bevorzugte Analyse neuer Ereignisse, weiterführende Links zu Problemlösungen und Hintergrundinfos.

Frühwarner

Darüber hinaus lässt sich die Ereignisanzeige auch als Frühwarnsystem einsetzen. Komfortabel klappt das mit einem Eintrag in der Windows-Aufgabenplanung, der ein individuelles Skript zum Filtern der Ereignisflut startet, etwa das c't-EventWatch-Skript (siehe ct.de/w9yw). Das kann vor allem für die Früherkennung von Festplattenausfällen hilfreich sein, erfordert jedoch ein umfangreiches Blacklisting unbedenklicher Warnungen und Fehler. Eine ausführliche Anleitung dafür finden Sie in [1] und [2].

Auch dann, wenn Windows gar nicht zickt, kann die Ereignisanzeige hilfreich sein: Etwa um herauszufinden, wann sich welcher Benutzer am PC angemeldet hat (4624, Microsoft Windows Security Auditing), wann der PC in den Energiesparmodus ging (42, Kernel-Power) oder ob Windows in Abwesenheit des Besitzers hochgefahren wurde (12, Kernel-General). (jss) **ct**

Literatur

- [1] Peter Siering, Selbstüberwachung, Ereignisprotokolle im Blick, c't 10/12, S. 148
- [2] Peter Siering, Fehlerfrühwarnsystem, Windows-Ereignisse und -Protokolle, c't 13/14, S. 88

Ereignisdatenbank, EventWatch-Skript:
ct.de/w9yw



Axel Vahldiek

Windows-Analyse mit dem Process Monitor: Einführung

Wenn es um das Lösen von Windows-Problemen geht, kann mitunter nur noch der mächtige Process Monitor weiterhelfen. Sein Einsatz stellt zwar keinerlei Gefahr, jedoch selbst für Fortgeschrittene eine Herausforderung dar. Diese Einführung hilft bei den ersten Schritten.

Die Freeware Process Monitor protokolliert sämtliche Zugriffe von Windows und allen laufenden Anwendungen auf Dateien, Ordner und Registry-Schlüssel, außerdem Netzaktivitäten, Start und Ende von Prozessen und einiges mehr. Damit findet man beispielsweise heraus, an welcher Stelle eine Anwendung an fehlenden Rechten scheitert und wo genau in der Registry eine spezielle Einstellung gespeichert wird. Der Process Monitor kann sogar den kompletten Boot-Vorgang überwachen. Das Programm erfordert allerdings Einarbeitung, beispielsweise enthält die Symbolleiste abgesehen von „Öffnen“ und „Speichern“ nur

Symbole, die man nicht von anderen Programmen kennt. Des Weiteren passiert bei Windows und den laufenden Anwendungen unter der Haube dermaßen viel, dass der Process Monitor in jeder Sekunde Hunderte von Ereignissen protokolliert, selbst wenn sich auf dem Desktop gar nichts tut. Und wenn wirklich etwas los ist, kommen schnell mal Hunderttausende oder gar Millionen Ereignisse zusammen. Solche Massen lassen sich nicht durch bloßes Drüberschauen analysieren.

Die Ergebnisse bekommen Sie mit Filtern in den Griff. Bei Bedarf hilft eine Online-Recherche dabei herauszufinden, um was