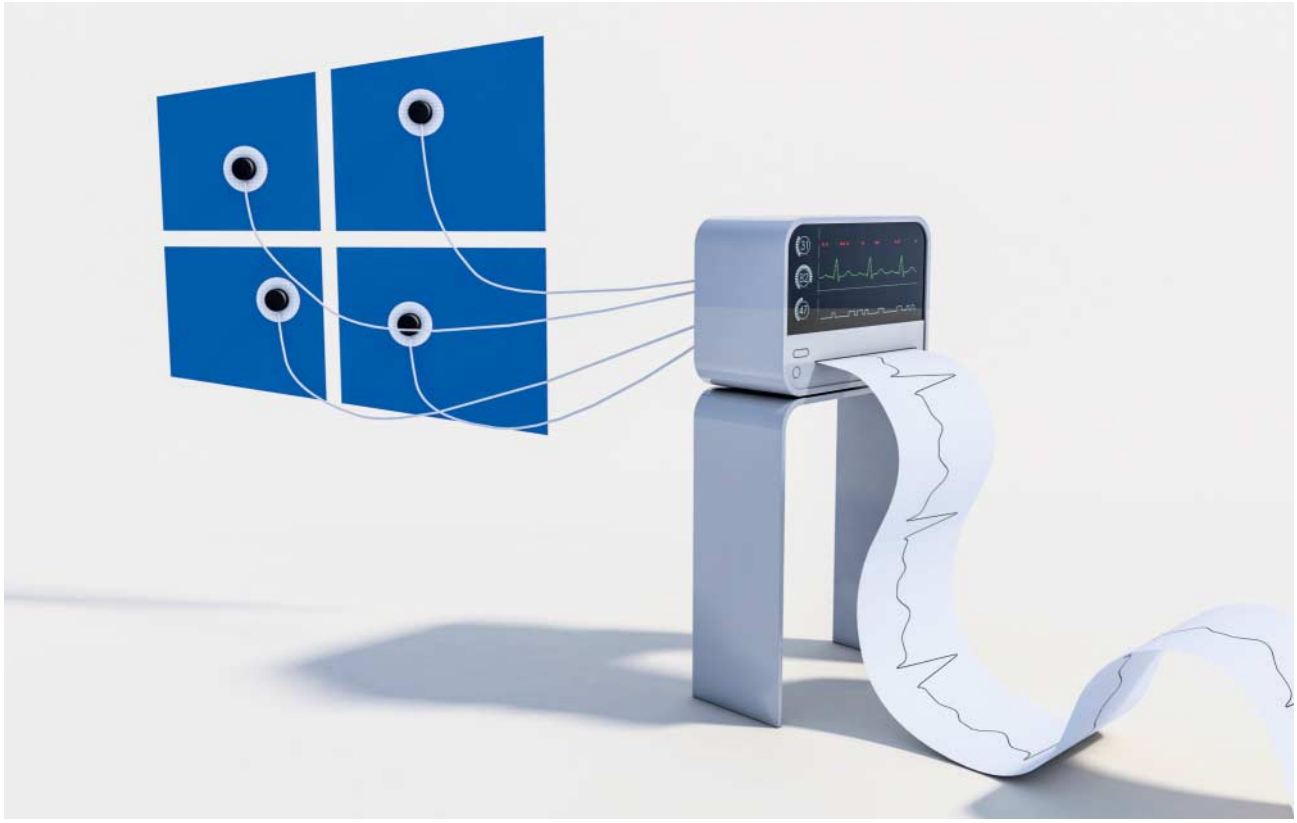


Introspektion

Systemdiagnose mit dem Windows Task-Manager

Mit dem Task-Manager hat Windows ein für viele Zwecke ausreichendes Tool zur Systemdiagnose an Bord. Trotzdem wird er gerne unterschätzt – nicht zuletzt deswegen, weil sich so manche seiner Funktionen erst auf den zweiten Blick erschließen.

Von Hajo Schulz

Warum reagiert mein Rechner auf meine Klicks so langsam? Was treibt Windows da im Hintergrund auf der Festplatte, dass ihr Lämpchen ständig blinkt? Wieso dreht der Lüfter auf Hochtouren, obwohl ich doch gerade nur Mail lese? Um diesen und ähnlichen Fragen nachzuspüren, braucht es keine teure Diagnose-Software: Die Antworten gibt Windows selbst – wenn man weiß, wo man nachsehen muss.

Das Programm, das in solchen Fällen zum Einsatz kommt, ist der Task-Manager. Er hat in den letzten Windows-Ausgaben einiges dazugelernt, versteckt sein Wissen aber zunächst vor dem Anwender. Grund genug, sich mit aktuellen Stand mal etwas eingehender zu beschäftigen.

Erster Eindruck

Gestartet wird der Task-Manager am schnellsten mit der Tastenkombination Strg+Umschalt+Esc. Wer sich die nicht merken mag, findet ihn auch im Kontextmenü der Taskleiste und der Uhr sowie in dem Menü, das sich seit Windows 8 mit einem Rechtsklick auf das Windows-Logo links unten auf dem Bildschirm oder mit Win+X öffnen lässt. Außerdem ist er eine der Optionen auf der Seite, die der klassische „Klammergriff“ Strg+Alt+Entf anzeigt.

In der Grundeinstellung besteht der Task-Manager lediglich aus einer minimalistischen Liste der gerade geöffneten Programme und Apps. Nicht einmal vollständig ist sie – Explorer-Fenster fehlen zum Beispiel. Über die Schaltfläche „Task beenden“ kann man Programme schließen; ein Kontextmenü bietet ein paar zusätzliche Funktionen.

Seine Leistungsfähigkeit offenbart der Task-Manager erst, wenn man unten auf „Mehr Details“ klickt: Dann erscheint seine vollständige Oberfläche mit Hauptmenü und insgesamt sieben Seiten, zwischen denen man über Karteireiter am oberen Rand wechseln kann.

Die erste – „Prozesse“ – zeigt im oberen Abschnitt dieselbe Liste wie zuvor, hier aber vollständig und mit einigen Zusatzinformationen: Zu jeder Anwendung informiert der Task-Manager darüber, wie stark sie gerade die CPU belastet, wie viel Arbeitsspeicher sie belegt und mit welcher Geschwindigkeit sie aktuell Daten mit lokalen Datenträgern und dem Netzwerk austauscht. Oft reicht schon ein Blick auf diese Liste, um zu sehen, weshalb ein bestimmtes Programm gerade träge reagiert: Ein besonders hoher Wert in der Spalte „Datenträger“ identifiziert etwa die Festplatte als den Flaschenhals.

Die laufenden Prozesse sortiert der Task-Manager in dieser Ansicht zunächst in drei Kategorien ein: Unter „Apps“ stehen alle Programme, die als Fenster auf dem Desktop in Erscheinung treten. Alles, was Windows sonst noch so im Verborgenen ausführt, steckt in den Kategorien „Hintergrundprozesse“ und „Windows-Prozesse“, wobei nicht so recht klar wird, worauf die Unterteilung beruht. Mit einem Klick auf einen der anderen Spaltenköpfe als „Name“ lässt sich diese Kategorisierung aufheben und die Liste stattdessen nach der gewählten Spalte sortieren. So identifiziert man schnell diejenigen Prozesse, die gerade die CPU, den Hauptspeicher, die Festplatte oder die Netzwerkschnittstelle besonders stark beanspruchen.

Auf eine Spaltenüberschrift zu klicken, um die angezeigten Daten nach dieser Spalte zu sortieren, funktioniert in allen tabellarischen Ansichten des Task-Managers. Außerdem besitzen alle Spaltenköpfe ein Rechtsklick-Menü, über das sich entweder direkt oder mit Hilfe des Befehls „Spalten auswählen“ weitere Details ein- und überflüssige Angaben ausblenden lassen.

Eine Eigentümlichkeit ist bei der optionalen Spalte „Status“ der Prozesse-Seite zu beachten: Sie füllt sich erst mit Leben, wenn man im Menü die Option „Ansicht/Statuswerte/Anhaltestatus anzeigen“ aktiviert. Dann zeigt sie bei minimierten oder in den Hintergrund geklickten Apps gegebenenfalls „Angehalten“ an; für herkömmliche Windows-Anwendungen hat sie keine Bedeutung.

Eine zweite Besonderheit teilt sich das Spalten-Kontextmenü der Seite „Prozesse“ mit dem auf der Seite „Benutzer“: Die Angaben in den Spalten Arbeitsspeicher, Datenträger und Netzwerk lassen sich hier im Untermenü „Ressourcewerte“ bei Bedarf von absoluten auf Prozentwerte umschalten.

Überblick

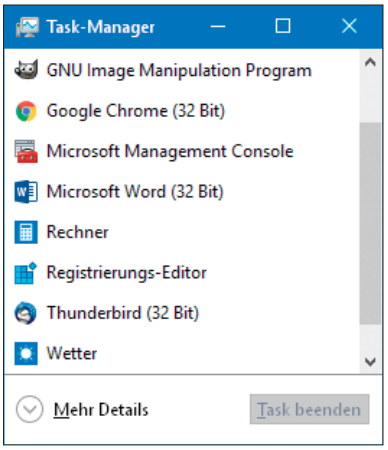
Ist die Seite „Prozesse“ eher dazu gedacht, den Ressourcenverbrauch einzelner Programme zu begutachten, findet sich eine übersichtliche Darstellung der Gesamtauslastung des Systems auf der Seite „Leistung“. Auf der linken Seite zeigen kleine Diagramme die Auslastung der wichtigsten Ressourcen im zeitlichen Verlauf, ihre Beschriftungen geben den aktuellen Wert wieder. Durch einen Klick auf eine Ressource ruft man weitere Details auf.

Auf einigen der Detail-Seiten verbergen sich weitere Informationen in Kontextmenüs. So kann man die Grafik der CPU-Auslastung per Rechtsklick in Einzeldiagramme ändern, die jeweils den Durchsatz eines logischen Prozessorkerns darstellen. Besonders aussagekräftig ist das heutzutage aber nicht mehr: Auf modernen CPUs verschiebt Windows die Last sehr dynamisch zwischen den verfügbaren Kernen hin und her, unter anderem um möglichst viel Rechenpower pro Watt verheizter elektrischer Leistung zu erreichen. Dass sich eine Single-Thread-Anwendung in eine Endlosschleife verrannt hat, erkennt man also nicht mehr unbedingt daran, dass ein Kern unter Volllast läuft. Auf einer Quad-Core-CPU sorgt sie vielmehr für eine mehr oder weniger gleichmäßige Auslastung aller vier Kerne zu etwa 25 Prozent; kommt noch Hyperthreading ins Spiel, drehen die acht logischen Kerne mit je circa 12,5 Prozent.

Eine Besonderheit gilt es bei der Interpretation der Auslastung von Netzwerkanschlüssen zu beachten: Diese Diagramme ändern ihren Maßstab dynamisch. Wenn eine Zeitlang kein nennenswerter Netzwerkverkehr stattfindet, sorgen bereits durch die Leitung tröpfelnde 100 KBit/s für Vollausschlag. Um zu beurteilen, ob die Netzwerkkarte wirklich am Anschlag arbeitet, muss man also immer den Maximalwert im Blick haben, der rechts oben am Diagramm steht.

Im Kontextmenü von Netzwerk-Diagrammen verbirgt sich übrigens noch der Befehl „Netzwerkdetails anzeigen“, der eine nicht gerade hübsche, aber sehr detaillierte Statistik der gesendeten und empfangenen Daten auf den Schirm ruft. Die Summen geben dabei die Werte seit dem Start der aktuellen Task-Manager-Sitzung an.

Jede der Detail-Grafiken lässt sich per Doppelklick oder über den Kontextmenübefehl „Diagrammübersichtsansicht“ auf eine kompakte Darstellung reduzieren, die das gesamte Drumherum des Task-Managers ausblendet. Das Fenster lässt sich dann beispielsweise platzsparend in eine Ecke des Bildschirms verschieben. Das ist recht praktisch, wenn man eine Grafik im Blick behalten will, während man ein neues Programm oder eine Eigenentwicklung testet. Ähnlich kompakt ist die „Zusammenfassungsansicht“, die sich mit dem gleichnamigen Befehl aus dem Kontextmenü der linken Spalte oder einem Doppelklick dorthin anzeigen lässt.



Beim ersten Aufruf präsentiert sich der Task-Manager als ziemlich unspektakuläre Liste der laufenden Programme. Erst ein Klick auf „Mehr Details“ schaltet seinen vollen Funktionsumfang frei.

Brot und Butter

Die Seiten „App-Verlauf“, „Autostart“ und „Benutzer“ bergen keine großen Geheimnisse. Bei ersterer verwendet Microsoft den Begriff „App“ ausnahmsweise mal konsequent: Die Seite listet nur den Ressourcenverbrauch von Store-Apps und ignoriert den der klassischen Windows-Anwendungen.

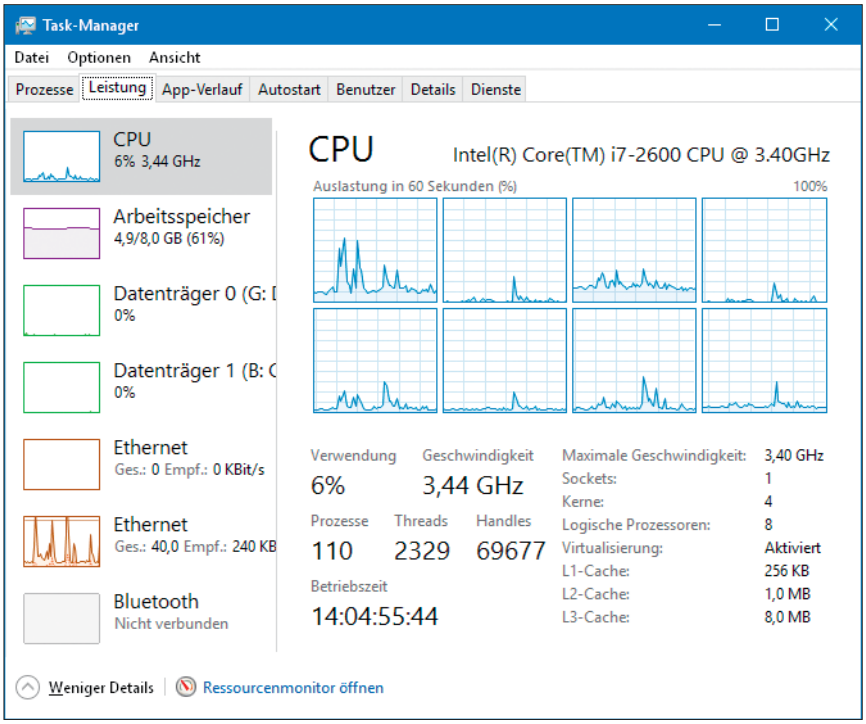
Bei den Autostarts ist der interessanteste Befehl im Kontextmenü der Einträge „Online suchen“: Er öffnet den als Standard eingerichteten Browser und sendet eine Anfrage an die Microsoftsche Suchmaschine Bing. Als Schlagwörter werden die Namen des Austostart-Eintrags und der EXE-Datei übergeben. Die Antworten sollen dabei helfen, unbekannte Einträge einer Anwendung oder einem Hersteller zuzuordnen. Meist finden sich unter den ersten paar Suchergebnissen auch ein oder mehrere Links zu Seiten mit Beurteilungen, ob die angefragte Datei harmlos oder womöglich ein Virus ist. Sehr vertrauenswürdig sind solche Aussagen allerdings oft nicht, vor allem dann nicht, wenn sie aus einem Diskussionsforum stammen. Wer bei unbekannten Autostarts sicher gehen will, dass sich keine Malware eingenistet hat, verwendet besser den Kontextmenübefehl „Dateipfad öffnen“ und schickt die ausführbare Datei an die Internetseite www.virustotal.com: Hier scannen sie bis zu 60 Virenscanner und stellen so ein ziemlich zuverlässiges Zeugnis aus.

Die Seite „Benutzer“ zeigt dieselben Einträge und Zusatzinformationen wie „Prozesse“, ordnet und summiert sie aber nach den beteiligten Benutzerkonten. Im Kontextmenü von Konten sind vielleicht noch die Befehle erwähnenswert, die den dazugehörigen Benutzer abmelden, seine Sitzung trennen oder ihm eine Nachricht senden.

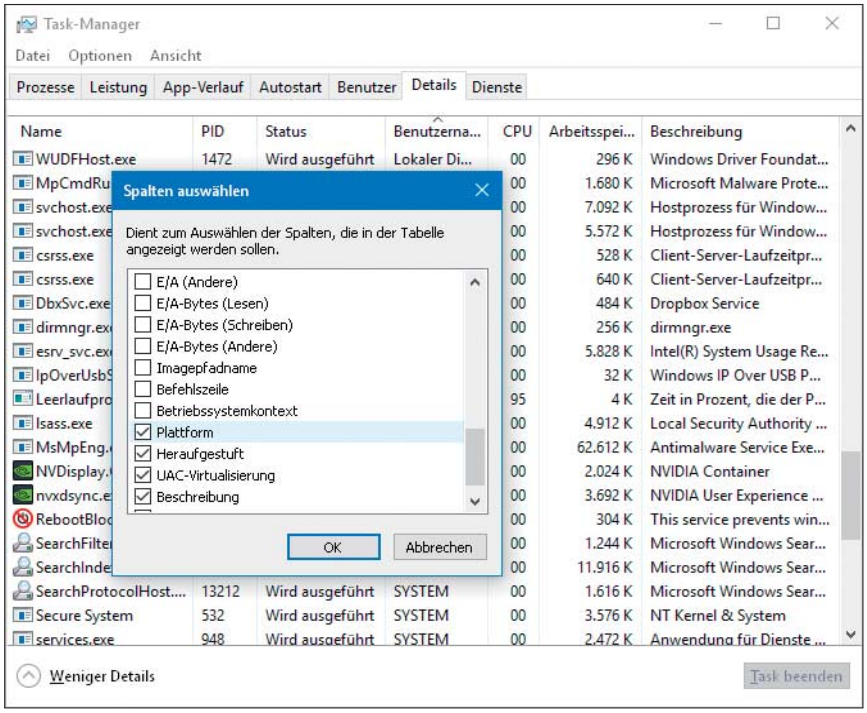
Mikroskop

Die Task-Manager-Seite, die unbedarften Benutzern wahrscheinlich am meisten Respekt einflößt, ist „Details“. Relativ schmucklos präsentiert sie eine tabellarische Liste aller laufenden Prozesse mit ihren wichtigsten Eigenschaften. Der spröde Charme dieser Liste lässt ihre Mächtigkeit kaum erahnen.

Über den Befehl „Spalten auswählen“ aus dem Kontextmenü der Spaltenköpfe lassen sich bis zu 38 Informationshäpp-



Wie stark verschiedene Ressourcen des Rechners im Verlauf der letzten Minute ausgelastet waren, zeigt der Task-Manager auf der Seite „Leistung“.



Auf der Seite „Details“ lassen sich bis zu 38 Eigenschaften der laufenden Prozesse übersichtlich auflisten. Ein Klick auf einen Spaltenkopf sortiert nach jeder beliebigen.

chen pro Prozess anzeigen. Etliche davon sind selbsterklärend, andere so exotisch, dass selbst Power-User sie wohl nur selten brauchen. Einige verdienen aber ein paar Erläuterungen.

Zur letzten Kategorie gehören die Spalten „Seitenfehler“ und „Ändern der Seitenfehler“: Anders, als man vielleicht meinen könnte, handelt es sich dabei nicht um Fehlfunktionen von Programmen. Vielmehr bedeutet ein Seitenfehler, dass ein Prozess versucht hat, auf eine Speicheradresse zuzugreifen, der zu diesem Zeitpunkt kein physisches RAM zugeordnet war. Windows musste den Speicherinhalt zunächst aus der Auslagerungsdatei oder dem ausführbaren Code – etwa einer EXE- oder DLL-Datei – laden. Eine große Zahl an Seitenfehlern ist also zunächst kein Grund zur Panik: Wenn ein großes Programm lange läuft und intensiv genutzt wird, muss es währenddessen eben auch viel Code nachladen. Besorgniserregend ist allerdings, wenn „Ändern der Seitenfehler“ dauerhaft und bei mehreren Programmen einen hohen Wert – deutlich über 500 – anzeigt. Dann treten nämlich ständig Seitenfehler auf. Das ist ein sicheres Zeichen dafür, dass der Rechner für die gerade anstehenden Aufgaben zu wenig RAM besitzt und mehr mit dem Ein- und Auslagern von Daten als mit dem Abarbeiten von Benutzercode beschäftigt ist. Abhilfe schaffen zusätzliche RAM-Riegel oder der Verzicht auf den gleichzeitigen Betrieb mehrerer speicherhungriger Anwendungen.

Interessant sind auch die Spalten „Heraufgestuft“ und – auf 64-bittigen Windows-Installationen – „Plattform“: Erstere enthält ein „Ja“ bei allen Prozessen, denen die Benutzerkontensteuerung Administratorrechte verliehen hat; diese Prozesse haben also unter anderem Schreibzugriff im Systemordner und im Schlüssel `HKEY_LOCAL_MACHINE` in der Registry. Unter „Plattform“ steht, ob es sich bei dem Prozess um ein 32- oder ein 64-Bit-Programm handelt.

Im Kontextmenü der Prozess-Einträge selbst finden sich etliche Befehle, die Entwicklern beim Testen ihrer Anwendungen helfen, in Einzelfällen aber auch zum Optimieren des Systems dienen können. So kann man etwa über „Priorität festlegen“ weniger wichtigen Prozessen CPU-Zeit entziehen, die dann Anwendungen im Vordergrund zugutekommt; mit ein bisschen Glück lassen sich ruckelnde Spiele oder Mediaplayer damit noch um ein paar Prozent beschleunigen. Auch wild gewordene Programme, die die CPU auslasten und den Rechner unbedienbar machen, kann man so einbremsen. Andersherum kann man versuchen, über „Zugehörigkeit festlegen“ die Rechenzeit fressenden Hintergrundaktivitäten auf einen CPU-Kern zu konzentrieren, und hoffen, dass die anderen Kerne dadurch mehr Zeit für die Programme im Vordergrund haben. Allerdings beziehen sich beide Befehle immer nur auf die laufenden Prozesse und werden nicht gespeichert. Startet man die Programme neu, erhalten sie wieder ihre Standardwerte zugewiesen.

Ähnlich schmucklos wie die Liste der Prozesse kommt die Seite „Dienste“ daher. Praktisch ist sie dennoch, erspart ihr Kontextmenü dem Anwender doch für einfache Aufgaben wie das Starten und Anhalten von Diensten, die Computerverwaltung zu öffnen und sich zur Dienst-Verwaltung durchzuklicken. Wer beide Werkzeuge im Wechsel benutzt, sollte wissen, dass die Spalte, die die Computerverwaltung „Name“ nennt, im Task-Manager „Beschreibung“ heißt.

Die Spalte „PID“ enthält die Prozess-IDs laufender Programme, mehr oder weniger nichtssagende Zahlen. Ihren Sinn bekommen sie, wenn man über die Seite „Details“ herausgefunden hat, dass eine der Instanzen von svchost.exe die CPU unter Dauerlast hält: Dann sucht man deren PID bei den Diensten und kann damit den Kreis der verdächtigen Aktivitäten schon ziemlich eingrenzen. Bei Windows 10 ab Version 1703 („Creators Update“) läuft sogar jeder Dienst in seiner eigenen svchost-Instanz und hat damit eine eigene Prozess-ID.

Wie weiter

Der Task-Manager ist ein ziemlich ernst zu nehmendes Diagnose-Tool, das allen Windows-Anwendern mit wenigen Mausklicks oder Tastendrücken zur Verfügung steht. Allerdings hat er seine Grenzen: Abhängigkeiten von Prozessen untereinander verrät er ebenso wenig wie die Namen von Dateien, die ein bestimmter Prozess gerade geöffnet hat. Wer Antworten auf diese Fragen braucht, muss sich dann doch ein erweitertes Tool besorgen. Als besonders praxistauglich hat sich dabei der Process Explorer von Microsoft Sysinternals erwiesen. Über ct.de/yn98 gelangen Sie an den kostenlosen Download.

(hos@ct.de) c't

Alternative Task-Manager: ***ct.de/yn98***