Totalüberwachung

Windows mit dem Sysinternals Process Monitor auf die Finger schauen

Eines der mächtigsten Werkzeuge zur Windows-Analyse ist der Process Monitor. Er erstellt geradezu gigantische Protokolle, die auf den ersten Blick unübersichtlich sind – doch dank sinnvoller Filterfunktionen lässt sich damit exakt nachvollziehen, welcher Prozess was treibt.

Von Jan Schüßler

Will man Vorgängen in Windows wirklich genau auf den Grund gehen, braucht man ein Tool, das über alles, was im System passiert, in Echtzeit ein Protokoll anlegt. Ein solches Hilfsmittel ist der Process Monitor. Er ist Teil der Sysinternals-Suite, ein umfangreicher Werkzeugkasten für Windows.

Der Process Monitor führt penibel Protokoll: Er registriert Zugriffe aller Prozesse und jeglicher Art auf Dateien, Ordner und Registry-Schlüssel. Damit lässt sich exakt nachvollziehen, was eigentlich in den Tiefen des Systems vor sich geht. Fehlerberichte oder gar fertige Problemlösungen gibt das Programm hingegen nicht aus – sondern einen Berg an Rohdaten, die es erlauben, Fehlerursachen zu ergründen. Ein solches Monitor-Tool ist nichts für zwischendurch, denn pro Sekunde fallen ein paar hundert bis zigtausend Zugriffe an, je nachdem, ob das System im Leerlauf steht oder man gerade damit arbeitet. Dank sinnvoller Filterfunktionen bekommt man die Flut an Einträgen aber gut in den Griff.

Um sich einen Eindruck zu verschaffen, laden Sie den Process Monitor herunter (siehe c't-Link), entpacken das Zip-Archiv und starten daraus das Programm procmon.exe. Nach dem Abnicken der Lizenzbedingungen protokolliert der Process Monitor sofort drauflos. Das frisst Ressourcen – stoppen Sie die Aufzeichnung mit einem Klick auf das Lupen-Icon in der Symbolleiste.

Der Process Monitor listet für jede Aktion den genauen Zeitpunkt (Time of Day), den Namen des Prozesses und seine ID (Process Name und PID), die Art des Zugriffs (Operation), das Ziel (Path), das Ergebnis (Result) und Details der Operation auf – also etwa, welcher Wert aus einem Registry-Schlüssel gelesen oder in ihn hineingeschrieben wurde.

Die „Operation“ kann beispielsweise ein Zugriff aufs Dateisystem sein (Create File, CloseFile, ReadFile, ...), Information über einen gestarteten oder beendeten Thread (Thread Create, Thread Exit) oder Registry-Zugriffe (zum Beispiel RegOpen Key, RegQueryValue und RegCreateKey).

Nadel im Heuhaufen

Die wichtigste Filterfunktion lässt sich per Rechtsklick auf einen Eintrag mit den Optionen „Include“ und „Exclude“ aufrufen. Um das Vorgehen zu veranschaulichen, haben wir ein Beispiel aus der Praxis gewählt: Ein Windows-10-Notebook, das den Bildschirm niemals in den Energiesparmodus schicken soll, so lange ein Benutzer angemeldet ist – speziell dann, wenn es im Netzbetrieb läuft. Die Dauer des Timeouts ist in den Energie-Einstellungen deshalb auf „Nie“ gesetzt, springt aber aus unerfindlichen Gründen früher oder später – nach ein paar Stunden bis ein paar Tagen – immer wieder auf Microsofts Standardwert „20 Minuten“ zurück.

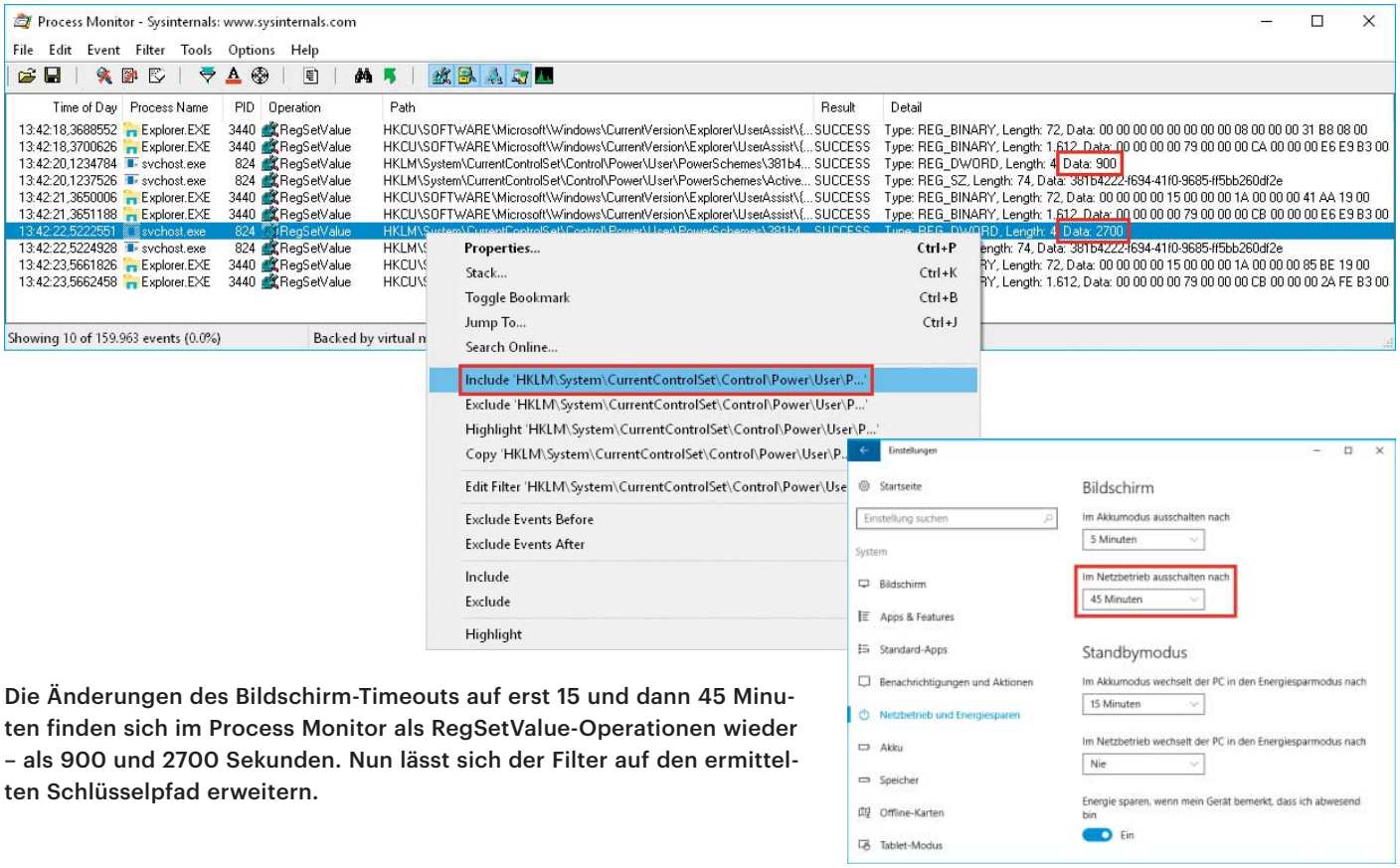
Werte für Energiespar-Timeouts (und viele andere Systemeinstellungen) werden über Registry-Schlüssel gesteuert. Um das seltsame Verhalten zu unterbinden, muss man also zunächst wissen, welcher Registry-Schlüssel eigentlich angefasst wird, wenn man den Timeout in der Systemsteuerung ändert.

Da das Protokoll rasend schnell anwächst, ist es ratsam, die Überwachung zunächst mit einem Klick auf das Lupen-Icon in der Symbolleiste abzuschalten und die bisherige Aufzeichnung mit dem Radiergummi-Icon (zwei Schaltflächen weiter rechts) zu löschen, um danach die Windows-10-Einstellungen zu öffnen und in „System“ die Funktion „Netzbetrieb und Energiesparen“ aufzurufen. Danach sollte es zügig gehen: die Aufzeichnung im Process Monitor starten, die Option „Bildschirm im Netzbetrieb ausschalten nach“ nacheinander auf zwei verschiedene Werte setzen, etwa 15 Minuten und 45 Minuten, und die Aufzeichnung im Process Monitor gleich wieder beenden.

Gefunden!

Das Ergebnis ist ein Protokoll mit ein paar hunderttausend Einträgen, daher gehts nun ans Filtern. Da irgendwo in der Liste auch die durchgeführten Änderungen am gesuchten Registry-Schlüssel für den Bildschirm-Timeout versteckt sein müssen, hilft nun das Fernglas-Icon in der Symbolleiste weiter. Es öffnet die Volltextsuche, die in diesem Beispiel nach dem Begriff „RegSetValue“ suchen soll. Das ist der Operationstyp, der zwangsläufig geloggt wird, wenn ein Wert in der Registry geändert wird.

Sobald die Suche einen solchen Eintrag gefunden hat, markiert sie ihn in der Liste. Ein Klick mit der rechten Maustaste auf die Operation „RegSetValue“ öffnet ein Kontextmenü mit Filtermöglichkeiten; die gewünschte heißt „Include 'RegSet Value'“. Die Liste der Ereignisse sollte



Die Änderungen des Bildschirm-Timeouts auf erst 15 und dann 45 Minuten finden sich im Process Monitor als RegSetValue-Operationen wieder – als 900 und 2700 Sekunden. Nun lässt sich der Filter auf den ermittelten Schlüsselpfad erweitern.

damit von ein paar hunderttausend auf vielleicht zehn bis zwanzig Einträge zusammenschrumpfen – eben all jene, die einen „RegSetValue"-Vorgang beschreiben.

Um aus dieser Liste den relevanten Key zu ermitteln, hilft nun ein Blick in die Spalte „Detail": Dort sollten sich zwei Einträge mit dem Wortlaut „Type: REG_DWORD, Length: 4, Data: 2700" und „Type: REG_DWORD, Length: 4, Data: 900" finden. Dies sind die gesuchten Einstellungen – die Data-Werte 900 und 2700 entsprechen dem jeweils neu gesetzten Bildschirm-Timeout in Sekunden.

In flagranti

Mit einem Rechtsklick in der Spalte „Path" auf den Registry-Pfad und dann auf „Include 'HKLM\System\CurrentControlSet\...'" lässt sich der Filter zusätzlich auf genau diesen Schlüssel einengen, sodass die Liste in diesem Beispiel nur noch zwei Einträge anzeigt. Mit diesem Filter kann man den Process Monitor nun einfach im Hintergrund weiterloggen lassen.

Weil das auf Dauer viele Ressourcen frisst – irgendwann ist der Hauptspeicher mit einem gigantischen Protokoll gefüllt –, sollte im Menü „Filter" auf jeden Fall die Option „Drop Filtered Events" eingeschaltet werden. Sie bewirkt, dass alles, was durch das Filterraster fällt, nicht bloß ausgeblendet, sondern komplett verworfen wird und somit nicht den RAM vollmüllt. Sobald der Registry-Wert für den Monitor-Timeout wieder einmal angefasst wurde, entsteht ein zusätzlicher Eintrag im Process Monitor. Der zeigt dann auch an, welcher Prozess sich unerwünschter Weise an der Timeout-Einstellung vergriffen hat.

Das weitere Vorgehen hängt ein wenig davon ab, welcher Prozess den Zugriff veranlasst. Möglichkeiten, den Registry-Wert auf den gewünschten Wert festzunageln, gibt es mehrere: etwa eine Aufgabe in der Windows-Aufgabenplanung, die den Wert alle 15 Minuten wieder auf 0 setzt oder das Ausklammern des fraglichen Prozesses vom Systemstart (zum Beispiel mit Sysinternals Autoruns). Ein radikalerer Weg ist es, dem System im Registry-Editor die Schreibrechte für den Schlüssel zu entziehen.

Da geht mehr

Besteht der Verdacht, dass die Energiespar-Einstellung schon während des Systemstarts zurückgesetzt wird, kann man unter „Options" die Funktion „Enable Boot Logging" starten. Beim Aufruf des Process Monitor nach einem Neustart lässt sich das Protokoll einsehen und filtern.

Ähnlich lässt sich mit dem Process Monitor beispielsweise analysieren, was genau eigentlich Zusatz-Software anstellt, die die Datenschutzeinstellungen von Windows 10 mit einem Handgriff optimieren soll, welche Prozesse im Leerlauf des Systems auf sensible Dateien zugreifen und so weiter. Weiß man nicht genau, wonach man eigentlich sucht, ist die Filterfunktion der Wahl oft nicht „include", sondern „exclude"; sie wirft nur Ereignisse mit dem gewählten Attribut aus der Liste. Das kann dauern, daher sollten Sie sich für den Einsatz des Process Monitor auf jeden Fall Zeit nehmen.

(jss@ct.de) c't

Process Monitor: ct.de/yc7g