Dem Fehler auf der Spur

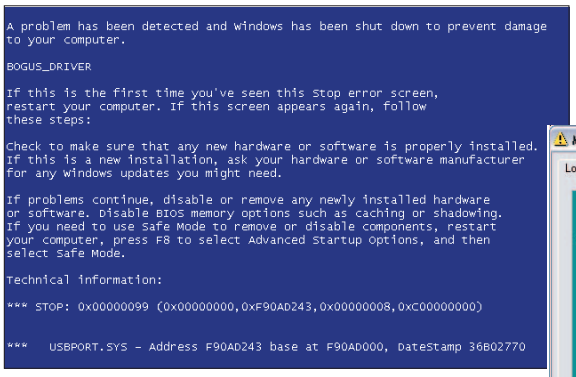
Wenn Windows XP abstürzt, ist meist ein fehlerhafter Treiber im Spiel. Dieser Tech Talk erklärt, was Bluescreens über das System verraten.

Oliver Ibelshäuser

Führt ein Mausklick in der laufenden Bildbearbeitung oder im Mail-Client zum plötzlichen Bluescreen of Death (BSOD), suchen die Benutzer die Fehlerursache fast immer in den Anwendungen selbst. Das ist der falsche Ansatz. Applikationen können keinen »blauen« Crash verursachen. Anwendungen, aber auch einige Windows-Routinen wie der Anmeldeprozess laufen im User-Mode. Dieser arbeitet in einem abgeschlossenen Adressraum und gewährt keinen Zugriff auf die Hardware. Der Vorteil: Fehler bringen das OS nicht zum Absturz oder Stillstand, sondern legen nur die betreffende Anwendung lahm – der so genannte Operation-Error. Andere Programme bleiben jedoch davon unbeeinflusst, da der User-Mode jeder Anwendung einen eigenen Adressraum zuweist.

Gravierende Systemfehler entstehen im Kernel-Mode. Dort werden Management-Dienste (Hardware-Verwaltung, Systemdienste), die Gerätetreiber, der HAL (Hardware Abstraction Layer) und der Microkernel ausgeführt. Nur der Kernel kommuniziert direkt mit der Hardware und verwaltet den Speicher.

Tritt ein Fehler auf, protokollieren die Kernel-Mode-Komponenten den Bug im günstigsten Fall und setzen die Arbeit fort. Dann bemerkt der Anwender das Problem gar nicht. Verhindert der Fehler jedoch die Fortsetzung eines Kernel-Prozesses, lädt das System als letzten Ausweg den Trap-Mechanismus KeBugCheckEx *(msdn.microsoft.com/library/default.asp?url=/library/en-us/kmarch/hh/kmarch/k105_9kfm.asp)*. Dieser sorgt für den kontrollierten Shutdown des Systems. Im Gegensatz zur landläufigen Meinung, der »Bluescreen of Death« sei ein plötzlicher Knock-out, handelt es sich um eine systematische Schutzmaßnahme. Der Speicherinhalt geht nicht verloren.



▲ Der Bluescreen kennzeichnet den **Urheber des Crashs** in verschlüsselten Zeichenketten.

Botschaften im Bluescreen

Abhängig vom Betriebssystem, vom aufgezeichneten Fehler sowie den Systemeinstellungen, variiert der Aufbau eines Bluescreens. Ist beispielsweise der Debug-Modus in der Datei *boot.ini* aktiviert, werden mehr Informationen dargestellt. Immer aber liefert die Routine KeBugCheckEx mit Hilfe mehrerer Parameter einige brauchbare Hinweise auf das eigentliche Problem.

Grundsätzlich ist der BSOD fünfgeteilt. Je nach Ursache nennt die Tafel zunächst eine Fehlerkategorie – im einfachsten Fall den problematischen Treiber. Darunter folgen allgemeine Anweisungen und Mitteilungen zum Fehlercode.

Die kryptisch anmutenden Zeichenketten der Bug-Check-Information werden von der Stop-Zeile eingeleitet. Diese bezeichnet den Fehlertyp und den -code. Der erste String – etwa Stop 0x0000001E – beschreibt den Typ, etwa Zugriffsverletzungen im Kernel. In der Klammer folgen drei oder vier hexadezimale Parameter, wobei die erste Nummernfolge klare Aussagen zur Ursache des Zusammenbruchs machen kann.

Eine Liste der häufigsten Stop-Meldungen samt Interpretation der Codes und einer Erläuterung der Ursachen finden Anwender in den ausführlichen Technet-Beiträgen:

▲ Das kostenlose Tool Error-Message **entschlüsselt die häufigsten Fehlercodes**.

www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000pro/reskit/part7/proch33.asp

Das Freeware-Tool Windows Error Messages kennt überdies die Bedeutung der häufigsten Fehlercodes *(www.pqtuning-downloads.de/system.htm)*.

Die zweite Zeichenkette stellt die Speicheradresse dar, in der der Fehler aufgetreten ist. Die weiteren beiden Codes spezifizieren den Fehler und sind kontextabhängig. Weiterhin folgen je nach System Informationen zum Prozessor. In den darunter aufgeführten Blöcken stehen Treiber- und DLL-Informationen samt Basisadressen und Zeitstempel (Datestamp). Ein Stack-Ausschnitt folgt im vierten Block. Dieser ist sehr wichtig, lässt sich aber nur mit speziellen Werkzeugen dechiffrieren (siehe »Quer-Treiber entlarven«, Seite 178). OIB

KOMPAKT

- Bluescreens sind keine plötzlichen Systemabstürze, sondern kontrollierte Schutzmaßnahmen des Systems.
- Mit dem aktuellen Windows-Debugger bietet Microsoft das beste Analysewerkzeug zum kostenlosen Download an.
- Das versteckte Windows-Tool Verifier spürt faule Treiber im System auf und hilft bei der Fehlerbekämpfung.