





Windows-Crashdumps auswerten

von  Nils Kaczinski  30. Oktober 2009, 08:40 Uhr

 Kategorie: Tools, Troubleshooting, Windows

(Dieser Text entstammt leicht modifiziert dem Buch "Windows XP – Die Expertentipps" von Microsoft Press. Wir publizieren ihn hier mit freundlicher Genehmigung des Verlags.)

Immer, wenn Windows feststellt, dass ein illegaler Vorgang eine für das System kritische Situation hervorgerufen hat, beendet es sich selbst und zeigt einen Bluescreen an. Doch das ist nicht alles: Es protokolliert in diesem Moment auch noch, was direkt vor dem Bluescreen passiert ist, damit eine Chance besteht, das Problem zu beheben.

Grundsätzlich gilt: Wenn Sie nur einmal nach langer Zeit einen Bluescreen erhalten, kann es durchaus sinnvoll sein, den Computer einfach neu zu starten. Wenn danach alles wieder zuverlässig läuft, sind Sie zwar vermutlich Opfer einer Programmfehlens in einem Gerätetreiber oder einer direkten Hardware-Fehlfunktion geworden. Manche Fehler wirken sich aber so selten aus, dass es praktisch nie zu einem Systemabsturz kommt. Hier können Sie abwägen, ob es die Mühe lohnt, das Problem zu analysieren.

Ein Speicherabbild sichern

Wenn der Fehler aber häufiger zutage tritt, sollten Sie ihm nachgehen. Dazu müssen Sie zunächst sicherstellen, dass Windows überhaupt genügend Daten sammelt. So gehen Sie vor:

1. Öffnen Sie die Systemeigenschaften (am schnellsten geht es, wenn Sie *Windows+R* drücken, dann *sysdm.cpl* eintippen und abschließend *Eingabe* drücken).
2. Öffnen Sie die Registerkarte *Erweitert*. Klicken Sie dort im unteren Abschnitt *Starten und Wiederherstellen* auf die Schaltfläche *Einstellungen*.
3. Stellen Sie sicher, dass das Kontrollkästchen *Automatisch Neustart durchführen* deaktiviert ist.
4. Wählen Sie im Listenfeld *Debuginformationen* speichern den Eintrag *Kernelspeicherabbild* aus. Der Eintrag *Kleines Speicherabbild (xx KB)* erzeugt zu wenige Daten, während der Wert *Vollständiges Speicherabbild* für den Zweck der Fehleranalyse unnötig viele Daten produziert.
5. Stellen Sie sicher, dass das Kontrollkästchen *Vorhandene Datei überschreiben* aktiviert ist – andernfalls wird nämlich keine neue Datei geschrieben, wenn der gewählte Name schon vergeben ist, sondern es findet gar keine Protokollierung statt.

Wenn künftig ein Fehler im Kernelmodus auftritt, wird Ihnen Ihr System einen Bluescreen präsentieren und eine Kopie des Kernelspeichers aus dem Arbeitsspeicher in eine Datei schreiben. Diese Datei trägt den Namen *memory.dmp* und liegt direkt im Systemverzeichnis (normalerweise *C:\Windows*). Achten Sie darauf, dass Sie diese Datei nach einem Systemabsturz in einen anderen Ordner verschieben, denn sonst wird sie beim nächsten Bluescreen überschrieben, und Sie können keine Diagnose mehr durchführen.

Den STOP-Fehler nachschlagen

Als einfachste (und durchaus Erfolg versprechende) Maßnahme können Sie sich die Fehlernummer notieren, die Windows auf dem Bluescreen selbst angibt. Sie steht direkt nach dem Wort »STOP« recht weit unten auf dem

Bluescreen und ist im hexadezimalen Format angegeben. Nach dieser Nummer können Sie auf der englischsprachigen Webseite des MVP-Kollegen James A. Eshelman suchen, der eine sehr umfassende Artikelsammlung zu Stop-Fehlermeldungen zusammengetragen hat. Sie finden seine Seite unter <http://aumha.org/win5/kbestop.htm>.

Das Speicherabbild analysieren

Falls die Stop-Fehlernummer Sie nicht weiterbringt oder falls Sie den Dingen selbst auf den Grund gehen wollen, können Sie das Kernspeicherabbild analysieren, das Windows angelegt hat. Hierzu allerdings müssen Sie zunächst ein geeignetes Programm installieren. Microsoft bietet Ihnen den Debugger *WinDbg* an, der zwar nur in englischer Sprache, aber kostenlos erhältlich ist. Es ist Teil der »Debugging Tools for Windows«, die Sie von folgender Webseite herunterladen können:

[Debugging Tools for Windows - Overview]

<http://www.microsoft.com/whdc/DevTools/Debugging/default.mspix>

Sie können das Werkzeug auf einem beliebigen Windows-Rechner installieren, es muss sich dabei nicht um den Computer handeln, auf dem der Bluescreen aufgetreten ist. Auch unter Windows 7 läuft das Programm.

Nach der Installation muss *WinDbg* noch konfiguriert werden. Um nämlich ein Speicherabbild analysieren zu können, muss der Debugger so genannte »Symboldateien« vorfinden, die zusätzliche Informationen zu den Analysedaten enthalten. Am einfachsten ist es dabei, wenn Sie während der Analyse auf das Internet zugreifen können, denn dann besorgt sich *WinDbg* immer gezielt die Symboldateien, die es tatsächlich braucht. Ein vollständiger Download hingegen würde je nach Betriebssystem über 200 MB auf einen Schlag erfordern. Die Downloads finden Sie bei Bedarf auch über den obigen Link.

So richten Sie *WinDbg* für den Internet-Download ein:

1. Legen Sie auf Ihrer Festplatte einen Ordner an, in dem die Symboldateien gespeichert werden sollen. Der Pfad zu diesem Ordner sollte kurz sein und darf keine Leerzeichen enthalten. Ein sinnvoller Name wäre *C:\symbole*.
2. Starten Sie *WinDbg*. Öffnen Sie das Menü *File* und wählen Sie dort den Befehl *Symbol File Path*. Tragen Sie in das Dialogfeld *Symbol Search Path* im Textfeld *Symbol path* folgenden Text ein:
`SRV*C:\symbole*http://msdl.microsoft.com/download/symbols`
Dabei entspricht *C:\symbole* dem Pfad des Ordners, den Sie in Schritt 1 angelegt haben.
3. Stellen Sie sicher, dass während der Arbeit mit *WinDbg* eine HTTP-Verbindung ins Internet möglich ist.

Mit dem Menübefehl *File/Open Crash Dump* können Sie nun die Datei *memory.dmp* öffnen, die beim letzten Bluescreen erzeugt wurde. *WinDbg* präsentiert Ihnen dann ein Fenster mit dem Titel *Command*, in dem eine Menge Text erscheint. Wenn die Symboldateien korrekt heruntergeladen wurden, sollte nach der Meldung »Loading Kernel Symbols« eine Reihe mit Punkten erscheinen.



Nach kurzer Denkpause gibt *WinDbg* dann den ersten Tipp ab, welches Modul den Fehler im System verursacht haben könnte. In einer Zeile, die mit den Worten beginnt: »Probably caused by« (zu Deutsch: »Vermutlich verursacht durch«) steht der Name einer Datei, die wahrscheinlich an dem Problem Schuld ist. Da *WinDbg* zu

diesem Zeitpunkt nur eine Kurzanalyse durchgeführt hat, ist die Aussage noch nicht zwingend, aber doch in den meisten Fällen bereits zutreffend.

```
Microsoft (R) Windows Debugger Version 6.3.0017.0
Copyright (c) Microsoft Corporation. All rights reserved.
Loading Dump File [D:\temp\MEMORY.DMP]
Kernel Summary Dump File: Only kernel address space is available
Symbol search path is:
SRV*D:\temp\Symbols*http://msdl.microsoft.com/download/symbols
Executable search path is:
Windows XP Kernel Version 2600 (Service Pack 1) UP Free x86 compatible
Product: WinNt, suite: TerminalServer SingleUserTS Personal
Built by: 2600.xpsp2.030422-1633
Kernel base = 0x804d0000 PsLoadedModuleList = 0x8053f530
Debug session time: Sun May 23 22:13:38 2004
System Uptime: 0 days 0:08:10.140
Loading Kernel Symbols
.....
Loading unloaded module list
..
Loading User Symbols
*****
* *
* Bugcheck Analysis *
* *
*****
Use !analyze -v to get detailed debugging information.
BugCheck E2, {0, 0, 0, 0}
Probably caused by : i8042prt.sys ( i8042prt!I8xProcessCrashDump+235 )
Followup: MachineOwner
_____
```

In den meisten Fällen kann die Auswertung nach dieser Kurzanalyse eigentlich schon beendet werden, weil das Ergebnis schon auf die richtige Datei hinweist. Um den Dingen jedoch weiter auf die Spur zu kommen, können noch zwei weitere Schritte gemacht werden:

1. Tippen Sie im unteren Teil des *Command*-Fensters von *WinDbg* hinter der Eingabeaufforderung `kd>` folgenden Befehl ein:
`!analyze -v`
2. *WinDbg* gibt nun zahlreiche weitere Informationen aus. Gleich die erste Zeile ist hier von Interesse. Sie besteht aus einer Zeichenkette in Großbuchstaben, die mit Unterstrichen getrennt ist. Hierbei handelt es sich um den symbolischen Namen des Fehlers, z. B. *NTFS_FILE_SYSTEM*. Sie können versuchen herauszufinden, ob *WinDbg* zu diesem Fehler selbst etwas weiß. Geben Sie wiederum im unteren Teil des *Command*-Fensters den Befehl `.hh NTFS_FILE_SYSTEM` ein, also `.hh` gefolgt von dem Fehlernamen, den Sie einfach aus dem Text kopieren können. Mit etwas Glück enthält die Online-Hilfe, die *WinDbg* jetzt öffnet, bereits Hinweise zur Behebung des Problems.

Doch auch der weitere Ausgabertext des Befehls `!analyze -v` enthält noch einige verwertbare Informationen. Zur Verdeutlichung finden Sie hier ein Beispiel, wie die Ausgabe aussehen könnte.

```
kd> !analyze -v
*****
* *
* Bugcheck Analysis *
* *
*****
MANUALLY_INITIATED_CRASH (e2)
The user manually initiated this crash dump.
Arguments:
Arg1: 00000000
Arg2: 00000000
Arg3: 00000000
Arg4: 00000000
```

Debugging Details:

```
BUGCHECK_STR: MANUALLY_INITIATED_CRASH
DEFAULT_BUCKET_ID: DRIVER_FAULT
LAST_CONTROL_TRANSFER: from f9aed681 to 804f0103
STACK_TEXT:
80535448 f9aed681 000000e2 00000000 00000000 nt!KeBugCheckEx+0x19
80535464 f9aecefb 002d9cc0 01644dc6 00000000 i8042prt!I8xProcessCrashDump+0x235
805354ac 8052d17d 81261d98 812d9c08 00010009 i8042prt!
I8042KeyboardInterruptSrv+0x21c
805354ac 806aefaa 81261d98 812d9c08 00010009 nt!KiInterruptDispatch+0x3d
80535540 80514023 8053dda0 ffdffc50 ffdff980 hal!HalProcessorIdle+0x2
80535550 8052d70c 00000000 0000000e 00000000 nt!PopIdle0+0x47
FOLLOWUP_IP:
i8042prt!I8xProcessCrashDump+235
f9aed681 5d pop ebp
SYMBOL_STACK_INDEX: 1
FOLLOWUP_NAME: MachineOwner
SYMBOL_NAME: i8042prt!I8xProcessCrashDump+235
MODULE_NAME: i8042prt
IMAGE_NAME: i8042prt.sys
DEBUG_FLR_IMAGE_TIMESTAMP: 3d6de41d
STACK_COMMAND: kb
BUCKET_ID: MANUALLY_INITIATED_CRASH_i8042prt!I8xProcessCrashDump+235
Followup: MachineOwner
```

In diesem Beispiel ist die Ursache überdeutlich, denn sie basiert auf einem zu Testzwecken manuell ausgelösten Bluescreen. Leider ist die Sachlage in realen Problemfällen nicht immer so eindeutig. Hier hilft Ihnen aber ein Blick auf den Abschnitt *STACK_TEXT*. Dort listet *WinDbg* den Inhalt des so genannten »Stack« auf, das ist ein Befehlsspeicher, der vom Prozessor abgearbeitet wird. Sie finden dort die zuletzt aufgerufenen Funktionen (das sind die Hexadezimalwerte) und daneben (in der letzten Spalte) die Namen der beteiligten Treiber und Systemdateien: Der Eintrag vor dem Ausrufezeichen ist die entsprechende Datei, an deren Namen meist ein *.sys* anzuhängen ist. Die im Stack aufgelisteten Dateien kommen in den Kreis der Verdächtigen, sofern ihr Name nicht *nt* ist.

An dieser Stelle erhalten Sie bereits eine Reihe von Dateinamen angezeigt, die als Übeltäter für den Systemabsturz in Frage kommen. Der nächste Schritt sollte nun darin bestehen, den Hersteller der jeweiligen Dateien ausfindig zu machen. Ein einfacher, aber zeitaufwändiger Weg besteht darin, mit der Suchfunktion des Windows-Explorer die Datei auf der Festplatte zu lokalisieren. Ist sie gefunden, gibt es zwei Möglichkeiten:

1. Klicken Sie mit der rechten Maustaste auf die gefundene Datei. Wählen Sie im Kontextmenü den Befehl *Eigenschaften*. Im Eigenschaftenfenster wird unter *Ort* der Speicherpfad der Datei angegeben. Manchmal taucht hier der Name des Herstellers als Ordnername auf.
2. Falls das Kontextmenü auch eine Registerkarte *Version* enthält (das ist nicht immer der Fall), sollten Sie auch dort nachsehen, ob in einem der Einträge der Name des Herstellers auftaucht.

Wenn Sie den Hersteller einer verdächtigen Datei identifizieren konnten, sollten Sie auf dessen Webseite nachsehen, ob es dort Informationen zu dem Problem gibt. Vielleicht existiert auch bereits eine neue Version des fraglichen Treibers.

Falls Ihre Nachforschungen nach dem Hersteller oder einer Problemlösung erfolglos waren, bleibt Ihnen immer noch die Internetrecherche. Übergeben Sie die gefundenen Dateinamen und den symbolischen Fehlernamen an Ihre bevorzugte Suchmaschine. Auch in der Microsoft Knowledge Base lohnt die Suche, ebenso natürlich in den technischen Newsgroups. Es ist gut möglich, dass Ihr Problem bereits bekannt ist und es eine Lösung oder einen Workaround dafür gibt.

Verwandte Beiträge:

1. [Installation von NT4-Druckertreibern auf Windows Server 2003](#)

Für die meisten Drucker gibt es auf der Windows Server 2003-CD keinen entsprechenden Druckertreiber mehr für Windows NT 4.0. Somit...

2. [Wo erhalte ich Informationen zu einem Stop-Fehler \(Bluescreen\)?](#)

Ein "Blue Screen of Death" (BSOD oder schlicht Bluescreen) zeigt an, dass Windows einen Systemfehler festgestellt und sich deshalb heruntergefahren...

3. [Werdig v2 \(English version\): Online data recovery for Active Directory](#)

This is the English version of my Active Directory recovery tool Werdig v2. Find the original German version here on...

4. [KMS-Aktivierung mit Windows 7 und Windows Server 2008 R2](#)

Bei der Produktaktivierung von Windows Server 2008 R2 und Windows 7 mit einem KMS unter Windows Server 2003 bestehen Probleme....

5. [Wie Windows mit großem Hauptspeicher umgeht](#)

Da es immer wieder Unklarheiten zum Umgang von Windows-Betriebssystemen mit großen Speichermengen (RAM) gibt, fasse ich die wichtigsten Punkte noch...