

# 9 Systemanalyse mit Fehlersuchbäumen

An einem üblichen PC lässt sich aufgrund seines modularen Aufbaus weit mehr reparieren und austauschen als bei Smartphones oder Tablets, was aber nicht bedeutet, dass nicht auch bei diesen Geräten eigene Reparaturversuche unternommen werden können. Wildes Herumexperimentieren führt dabei selten zum Erfolg, sondern eine strukturierte besonnene Vorgehensweise, bei der sich nicht selten herausstellt, dass die Ursache eher trivial war und sich ohne großen Aufwand beheben ließ.

Als äußerst hilfreich für eine strukturierte Fehlersuche erweisen sich Fehlersuchbäume, damit auch der nicht so technisch versierte Anwender den Überblick behält und relativ schnell die Ursache des Problems ermitteln kann. Auf dem Einleger zu diesem Buch sind eine ganze Reihe von Fehlersuchbäumen zu finden, die hier teilweise aus dem Text hergeleitet werden, sofern die dazu wichtigen Informationen nicht an anderer Stelle im Buch zu finden sind, was entsprechend kenntlich gemacht ist.

## 9.1 Hardware- oder Softwarefehler?

Diese entscheidende Frage ist mitunter nur schwer zu beantworten, wenn das Gerät nicht »komplett tot« ist. Was in solch einem Fall zu tun ist, wird in Abschnitt 9.6 näher erläutert. Wichtig ist für diese grundlegende Analyse, was mit dem Gerät seit dem letzten Mal, als es einwandfrei funktioniert hat, passiert ist. Oftmals hat man in Erinnerung, dass das Gerät ohne eigenes Zutun plötzlich und völlig unerwartet nicht mehr richtig funktioniert. Nicht selten stellt sich am Ende einer Fehlersuche heraus, dass zwischenzeitlich sehr wohl etwas am Gerät verändert wurde, nur hat man nicht die Verbindung zwischen den beiden Ereignissen gesehen. Typischerweise ist neue Software installiert worden, was nicht unbedingt durch den Anwender selbst, sondern auch per automatischer Updatefunktion passiert sein kann.

Für alle Betriebssysteme sind verschiedene Testprogramme erhältlich, die eine mehr oder weniger ausführliche Überprüfung des Systems ermöglichen. Tools wie *Tune Up Utilities* oder *WinOptimizer* versprechen darüber hinaus ein optimales und schnelleres Windows. In echten Problemfällen sind sie jedoch keine Hilfe, sondern können die Situation sogar noch verschlimmern, weil eben zusätzliche Software installiert wird. Generell sollte im Problemfall zunächst keinerlei Software installiert werden, sondern es sollte versucht werden, mit den jeweiligen »Bordmitteln« des Betriebssystems genauere Kenntnisse über die mögliche Ursache zu erlangen, wie es noch genauer erläutert wird.

### 9.1.1 Virenbefall?

Ein Virenbefall ist natürlich auch möglich, was bei Linux, iOS und Android eher unwahrscheinlich ist, bei Windows-Systemen jedoch bei ungewohntem merkwürdigen PC-Verhalten stets mit ins Kalkül zu ziehen ist. Ein Virens Scanner mit automatischer,

mindestens täglicher Updatefunktion muss bei Geräten mit Windows auf jeden Fall installiert sein. Auch wenn meist von einem Virens Scanner gesprochen wird, erkennt die Software typischerweise verschiedene Schädlinge (wie Trojaner, Rootkits und Malware), und der Begriff *Virus* wird allgemein (wie hier auch) als Synonym für Schadsoftware verwendet. Normalerweise sollte der im Hintergrund laufende Wächter bei einem auftretenden Virus Alarm schlagen. Hin und wieder sollte dennoch ein manueller Virens Scan eingeleitet werden, und wenn dann Schadsoftware detektiert wird, liegt bereits etwas im Argen und der PC kann bereits seit längerer Zeit befallen sein.

Schadsoftware wird allerdings auch dann nicht immer erkannt, weil sie als normale Software erscheint, jedoch als Malware einzustufen ist und möglicherweise den Windows-PC blockiert, was dann ein ganz offensichtliches Problem darstellt. Besonders verbreitet sind Schädlinge, die als System-Tools vermelden, dass auf dem PC Viren und/oder Spyware erkannt worden ist und der PC aus Sicherheitsgründen blockiert wird. Zur Aufhebung ist laut Anzeige eine kostenpflichtige Schutzsoftware zu installieren. Möglicherweise wird auch vermeldet, dass angeblich illegale Software aus dem Netz bezogen wurde, was als GEMA-, GVV- oder BKA-Trojaner bekannt ist. Üblicher Virens Scanner Software entzieht sich dieser Schädlingstyp oftmals, sodass dessen Beseitigung zwar etwas aufwendiger ist, keinesfalls sollte aber Geld – letztlich an den Verursacher – für eine vermeintliche Lösung des Problems gezahlt werden.

**BUNDESPOLIZEI** Es ist die ungesetzliche Tätigkeit enthüllt!

**Achtung!!!**  
 Ein Vorgang illegaler Aktivitäten wurde erkannt.  
 Das Betriebssystem wurde im Zusammenhang mit Verstößen gegen die Gesetze der Bundesrepublik Deutschland gesperrt! Es wurde folgender Verstoß festgestellt: Ihre IP Adresse lautet: "" mit dieser IP wurden Seiten mit pornografischen Inhalten, Kinderpornographie, Sodomie und Gewalt gegen Kinder aufgerufen  
 Auf Ihrem Computer wurden ebenfalls Videodateien mit pornografischen Inhalten, Elementen von Gewalt und Kinderpornografie festgestellt! Es wurden auch Emails in Form von Spam, mit terroristischen Hintergründen, verschickt. Diese Sperre des Computers dient dazu, Ihre illegalen Aktivitäten zu unterbinden.

**Ihre Angaben:** IP: Browser: Internet Explorer 7.0 OS: Windows XP Country: City: ISP:

Um die Sperre des Computers aufzuheben, sind Sie dazu verpflichtet eine Strafe von 100 Euro zu zahlen. Sie haben zwei Möglichkeiten die Zahlung von 100 Euro zu leisten.  
 1) Die Zahlung per Ukash begleichen:  
 Dazu geben Sie bitte den erworbenen Code in das Zahlungsfeld ein und drücken Sie anschließend auf OK (haben Sie mehrere Codes, so geben Sie diese einfach nacheinander ein und drücken Sie anschließend auf OK)  
 Sollte das System Fehler melden, so müssen Sie den Code per Email (einzahlung@landes-kriminal.net) versenden.  
 2) Die Zahlung per Paysafecard begleichen:  
 Dazu geben Sie bitte den erworbenen Code (gegebenfalls inkl. Passwort) in das Zahlungsfeld ein und drücken Sie anschließend auf OK (haben Sie mehrere Codes, so geben Sie diese einfach nacheinander ein und drücken Sie anschließend auf OK) Sollte das System Fehler melden, so müssen Sie den Code per Email (einzahlung@landes-kriminal.net) versenden.

**Ukash**

**Wo kann ich Ukash kaufen?**  
 Es gibt unzählige Möglichkeiten, Ukash zu erwerben, z. B. in Geschäften, Kosken, per Geldautomat, online oder über eine E-Wallet (elektronische Geldbörse). Nachstehend finden Sie eine Liste, aus der hervorgeht, wo Sie in Ihrem Land Ukash erwerben können

**Tankstellen** - Jetzt auch erhältlich bei folgenden Tankstellen: Agip, Avia, Esso, OMV, Q1 und Westfalen.

**epay** - Kaufen Sie Ukash in vielen tausend Supermärkten oder Call-Shops, in denen Sie dieses Logo sehen.

**paysafecard**

Abb. 9-1 Nicht immer ist Schadsoftware so auffällig.

Für die Beseitigung eines derartigen Schädlingstyps ist – wenn möglich – im abgesicherten Modus (siehe Abschnitt 9.4) zu starten und sind die Programme unter `SYSTEMKONFIGURATION – SYSTEMSTART (msconfig)`, die automatisch beim Boot geladen werden, zu kontrollieren. Außerdem ist die Registry (`regedit`) nach entsprechenden Einträgen zu durchsuchen und ggf. zu löschen. Mittlerweile stellen bekannte Virensicherhersteller (z. B. Avira, Kaspersky) für die Beseitigung dieses speziellen Schädlingstypus eigene Boot-Images zum Download für die Anfertigung einer Boot-CD zur Verfügung (siehe auch Abschnitt 7.3.2). Gleichwohl taucht fast täglich neue Schadsoftware auf, für die es noch keine befriedigende automatische Beseitigungsmethode gibt, sodass die Systemwiederherstellung (siehe Abschnitt 7.1.4) ein probates Mittel ist, um den Computer wieder in einen früheren Zustand zurücksetzen zu können.

## 9.2 Hardware und Gerätetreiber

Für die Computerhardware sind spezielle Softwaretreiber notwendig. Bei jedem aktuellen Betriebssystem gibt es hierfür eine Instanz, die die entsprechende Verwaltung vornimmt und verschiedene Werkzeuge für die Installation und Konfiguration vorsieht.

### 9.2.1 Windows-Gerätmanager

Bei Windows ist dies der `GERÄTEMANAGER` (Systemsteuerung – Hardware und Sound), der die einzelnen Komponenten in einer Baumstruktur darstellt. Über die `EIGENSCHAFTEN` lassen sich zu jeder Komponente detaillierte Informationen (wie die Belegung von PC-Ressourcen) anzeigen, wozu auch die Version der Treibersoftware zählt. Wenn die Treiber an dieser Stelle ohne Warnung oder Fehler ausgewiesen sind, kann man davon ausgehen, dass die Komponenten softwaretechnisch korrekt im System implementiert sind. An dieser Stelle lassen sich einzelne Komponenten bei Bedarf auch deaktivieren und der dazugehörige Treiber wechseln oder aktualisieren. Das (vorübergehende) Deaktivieren einer Komponente ist immer dann sinnvoll, wenn ein Gerätekonflikt auftritt oder ein bestimmtes Gerät bewusst nicht verwendet werden soll, etwa das WLAN-Interface bei einem Desktop-PC, der stattdessen den kabelgebundenen Ethernet-Anschluss zu verwenden hat. Ein aktivierter WLAN-Adapter versucht standardmäßig, eine IP-Adresse per DHCP zu beziehen und eine Verbindung aufzubauen, was zu Verzögerungen beim Netzwerkzugriff und letztlich auch zu Sicherheitsproblemen führen kann.

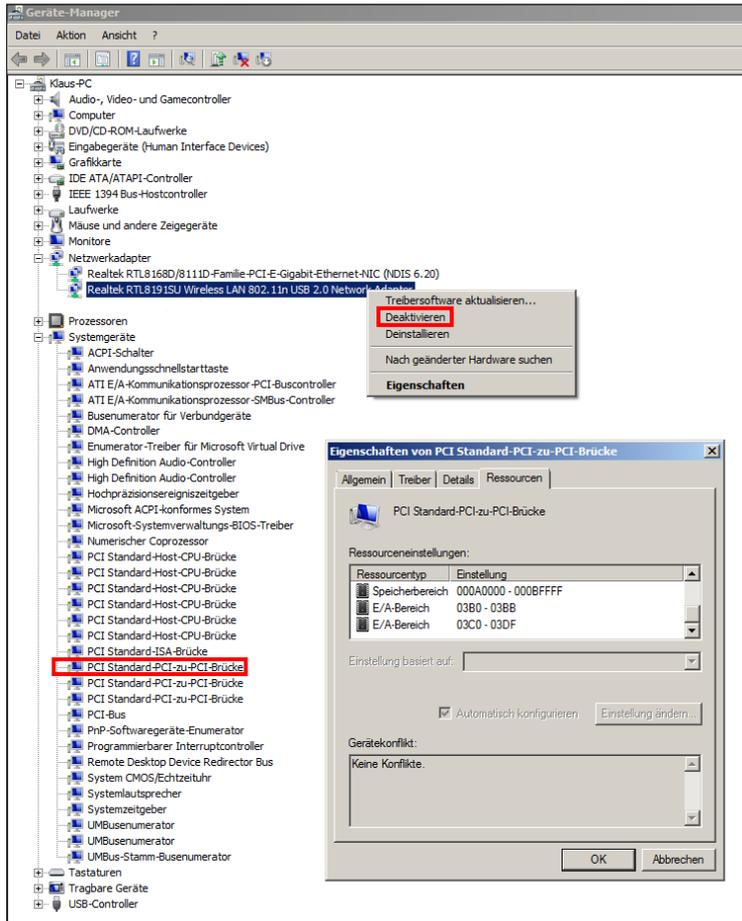


Abb. 9–2 Dem Windows-Geräte-Manager gilt bei einem vermuteten Problemfall mit einer Hardwarekomponente stets der erste Blick. Hier lassen sich Einheiten auch abschalten und die jeweilige Ressourcenbelegung einsehen.

Ein Gerätekonflikt liegt dann vor, wenn zwei Komponenten die gleichen PC-Ressourcen (E/A-Bereich, Speicherbereich, Interrupt-, DMA-Kanal) für sich beanspruchen, was in früheren Zeiten fast regelmäßig auftrat, heutzutage jedoch aufgrund der automatischen Mechanismen (Plug & Play) bei PCI, PCIe, SATA und dem USB kaum noch passiert. Da man die PC-Ressourcen für eine Komponente nicht mehr mit Jumpern festlegt, muss man sich darauf verlassen, dass das Betriebssystem und der Gerätetreiber die passenden Parameter untereinander aushandeln. Wenn dies nicht korrekt funktioniert, sollte ein neuer Gerätetreiber das Problem beseitigen.

### 9.2.2 Linux-Kontrollzentrum

Bei Linux sind die Hardwareeinstellungen in verschiedenen Dateien und Verzeichnissen (`/proc`, `/var`) zu finden (siehe Abschnitt 7.3), die sich mit einem üblichen Editor lesen und auch verändern lassen. In Abhängigkeit von der Distribution ist möglicherweise eine Gerätemanager-ähnliche Software (z. B. Hardwarekontrollzentrum) gleich mit dabei, die sich natürlich auch nachinstallieren lässt, wie beispielsweise *Hardinfo* oder *Sysinfo*. Standardmäßig bietet SUSE-Linux mit dem YaST-Kontrollzentrum immer noch eine der besten Lösungen für die Analyse und die Konfiguration von Hard- und Software, weil hiermit eine zentrale Anlaufstelle auch für Problemfälle zur Verfügung steht. Ubuntu hat hier im Laufe der Zeit jedoch aufgeholt, sodass hier ebenfalls eine komfortable und logisch organisierte System- und Einstellungsverwaltung implementiert ist.

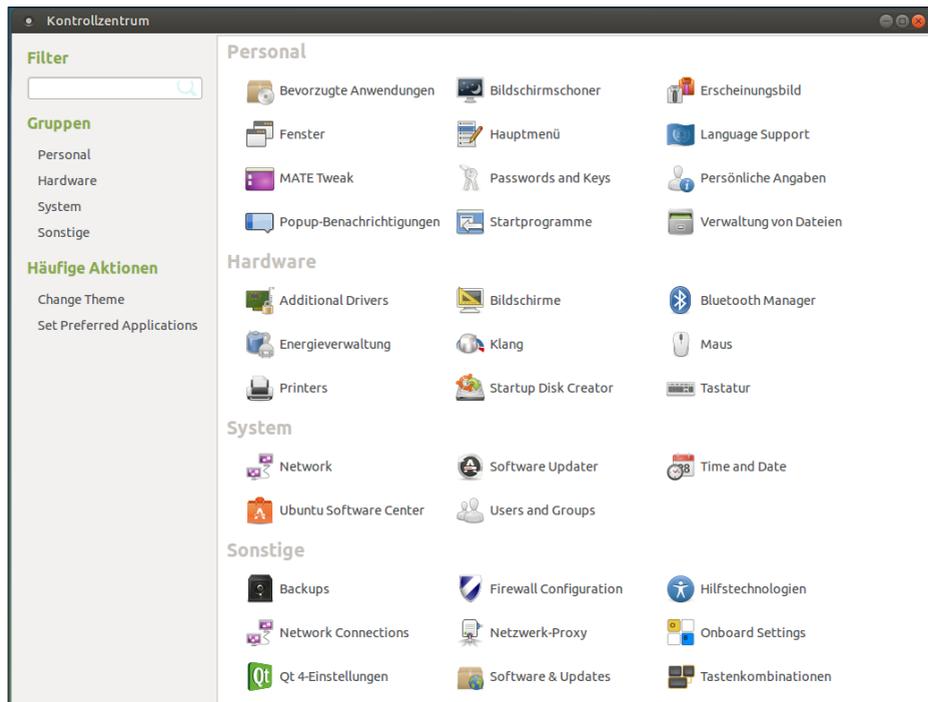


Abb. 9–3 Das Kontrollzentrum bei Ubuntu-Mate

Mithilfe der Kommandozeilenbefehle `lsusb` und `lspci` lassen sich die USB- und die PCI-Geräte anzeigen, was üblicherweise mit jeder aktuellen Distribution standardmäßig funktioniert. Dasselbe gilt für das Programm `lshw`, das sehr detaillierte Informationen über die Computerausstattung anzeigen kann und mit Root-Rechten ausgeführt wird. Für einen schnellen Überblick gibt man ein:

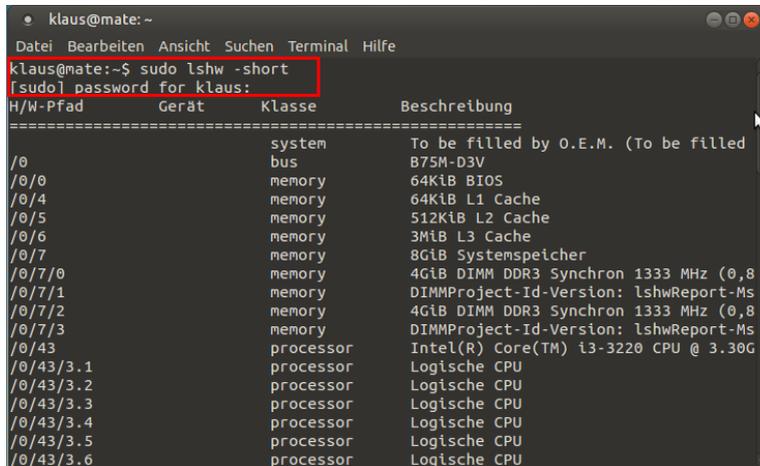
```
sudo lshw -short
```

Ausführlich kann die Ausgabe mit

```
sudo lshw > hardware.txt
```

in eine Textdatei gelenkt werden – oder in eine HTML-Datei mit:

```
sudo lshw -html > hardware.html
```



```

klaus@mate:~$ sudo lshw -short
[sudo] password for klaus:
H/W-Pfad      Gerät      Klasse      Beschreibung
-----
/0            system     To be filled by O.E.M. (To be filled
/0/0         bus        B75M-D3V
/0/0         memory     64KiB BIOS
/0/4         memory     64KiB L1 Cache
/0/5         memory     512KiB L2 Cache
/0/6         memory     3MiB L3 Cache
/0/7         memory     8GiB Systemspeicher
/0/7/0       memory     4GiB DIMM DDR3 Synchron 1333 MHz (0,8
/0/7/1       memory     DIMMProject-Id-Version: lshwReport-Ms
/0/7/2       memory     4GiB DIMM DDR3 Synchron 1333 MHz (0,8
/0/7/3       memory     DIMMProject-Id-Version: lshwReport-Ms
/0/43        processor  Intel(R) Core(TM) i3-3220 CPU @ 3.30G
/0/43/3.1    processor  Logische CPU
/0/43/3.2    processor  Logische CPU
/0/43/3.3    processor  Logische CPU
/0/43/3.4    processor  Logische CPU
/0/43/3.5    processor  Logische CPU
/0/43/3.6    processor  Logische CPU

```

Abb. 9–4 Anzeige der erkannten Hardware mit Lshw, wofür Root-Rechte und die (nochmalige) Angabe des Passworts notwendig sind.

### 9.2.3 Android-Einstellungen

Bei Android finden sich unter *Einstellungen* auch einige Angaben zur Hardware und zu Einstellungsmöglichkeiten etwa für Bluetooth, WLAN, zum Speicher und zum Akku. Aufgrund der Linux-Verwandtschaft lassen sich in den Verzeichnissen `/dev` und `/etc` verschiedene Gerädateien (Treiber) und Konfigurationsdateien finden, die sich jedoch nur mühsam dem Benutzer erschließen. Deshalb ist man bei Android zunächst auf die Möglichkeiten unter *Einstellungen* (Speicher, Akku) angewiesen, wo typischerweise unter *TELEFONINFO* – *HARDWAREINFORMATIONEN* oder auch unter *Geräteinformationen* noch Details zur jeweiligen Hardware zu finden sind, was von der jeweiligen Android-Version und dem jeweiligen Gerät abhängig ist.