10. Ist mein PC befallen?

Wenn Sie diesen Verdacht haben, sollten Sie den PC sofort vom Internet trennen. Es gibt die Gefahr, dass Ihr PC gerade ferngesteuert oder ausspioniert wird oder dass der Virus versucht, Spam zu versenden. Schlimmer noch: Der Virus könnte versuchen, andere PCs in Ihrem Netzwerk zu infizieren. Die Firewall des Routers schützt vor Angriffen aus dem Internet, doch das innere Netzwerk schützt sie nicht. Wenn ein Virus den Router überwunden und den ersten PC im Netzwerk befallen hat, sind die anderen Rechner stark gefährdet.

10.1. Symptome

10.1.1. Falsche Antivirus-Meldungen

Wissen Sie, wie eine Warnmeldung Ihres installierten Schutzprogramms aussieht? Wenn Sie plötzlich eine anders aussehende Warnmeldung eines unbekannten Virenscanners sehen, ist das ein sicheres Anzeichen dafür, dass das System infiziert wurde.

Eine Unmenge von Viren, die das Programm angeblich gefunden hat, soll Sie verleiten, Ihrem installierten Sicherheitsprogramm zu misstrauen und dieses neue Antivirenprogramm zu erwerben. Wenn Sie auf den angebotenen Link klicken, gelangen Sie auf eine professionell aussehende Website voller Auszeichnungen und Kundenbewertungen (und fangen sich dabei vielleicht einen Drive-by-Virus ein). Dann wird die Kreditkartennummer abgefragt – und viel zu viele Nutzer fallen darauf herein.

Was tun: In Bearbeitung befindliche Dateien speichern und den PC schnell herunterfahren. Dann den PC im „Abgesicherten Modus ohne Netzwerk“ neu starten und die verdächtige Software deinstallieren. Wenn das nicht gelingt, das System auf einen früheren Zustand zurücksetzen.

10.1.2. Häufige Popup-Fenster

Wenn Sie auf oft besuchten, vertrauten Webseiten plötzlich mit aufpoppender Werbung konfrontiert werden, ist Ihr Browser vielleicht unterwandert.

Versuchen Sie, Toolbars und unbekannte Software zu deinstallieren, eventuell im abgesicherten Modus.

10.1.3. Unerwünschte Browser-Toolbars

Plötzlich hat der Browser ein(ig)e neue Toolbars, die Sie nicht installiert haben? Die meisten Browser zeigen unter Ansicht → Symbolleisten die installierten Symbolleisten an. Entfernen Sie die Haken vor allen Toolbars, die Sie nicht unbedingt behalten möchten. Wird die verdächtige Toolbar nicht angezeigt oder lässt sie sich nicht deinstallieren, versuchen Sie den Browser auf Standardeinstellungen zurückzusetzen. Wenn auch das nichts bringt, gehen Sie so vor wie bei „Falsche Antivirus-Meldungen“.

Achten Sie bei der Installation jeglicher Software stets darauf, was alles mitinstalliert werden soll.

10.1.4. Unerwünschte Suchmaschinen

Egal wonach Sie suchen, Sie finden hauptsächlich kostenpflichtige Abo-Angebote und Kaufangebote? Das ist typisch für die Ask-„Suchmaschine“. Die ist vermutlich zusammen mit der Ask-Toolbar installiert worden, aber auch bei der Installation mehrerer Freeware-Programme kann Ihnen diese Toolbar aufgedrängt worden sein. Selbst beim Download von zweifellos nützlichen Programmen wie Java oder Nero wird Ask mitinstalliert, wenn Sie nicht aufpassen.

Wer verdient daran, die Suchergebnisse zu manipulieren? „Suchmaschinen“ wie z. B. Ask leiten zusätzliche potenzielle Interessenten auf ausgewählte Seiten. Ask zählt mit, wie viele Nutzer auf welche Seiten geleitet wurden. Deren Besitzer zahlen für den Traffic. Von diesen Einnahmen zahlt Ask „Kopfprämien“ an Softwareanbieter, denen es gelungen ist, ihren Nutzern die Ask-Suchmaschine zu installieren.

10.1.5. Freunde empfangen merkwürdige Mails mit Ihrem Absender

Es gibt mehrere Möglichkeiten, wie die Hacker an die Adressen Ihrer Freunde gekommen sind: Aus abgefangenen E-Mails oder aus einem gehackten Facebook-Konto. Aber vielleicht hat sich ein Trojaner eingenistet und Ihren PC erfolgreich nach Adressen durchsucht.

Was tun? Prüfen Sie, ob Sie sich noch an Ihrem Mailkonto anmelden können. Wenn ja, das Passwort ändern. Unerwünschte Toolbars und andere Software entfernen. Den PC mit dem eigenen Schutzprogramm und einigen Online-Virenscannern überprüfen, auch im abgesicherten Modus.

10.1.6. Online-Passwörter stimmen nicht mehr

Sie können Ihre E-Mails nicht mehr abrufen und das E-Mail-Programm behauptet, das Passwort stimmt nicht? Oder die Anmeldung bei Amazon, Ebay oder Facebook funktioniert nicht mehr? Es könnte sein, dass Ihre Accounts gekapert worden sind, vorzugsweise alle diejenigen, für welche Sie ein identisches Password benutzt haben.

Haben Sie vielleicht vor kurzem auf eine authentisch anmutende Phishing-Mail reagiert, die um die Erneuerung des Passworts für einen Online-Dienst gebeten hat? Und nun wundern Sie sich, dass Ihr Passwort nochmals geändert wurde und dass in Ihrem Namen Einkäufe getätigt oder Verträge abgeschlossen werden?

Was tun? Informieren Sie sofort alle Kontakte, um den Schaden für Andere zu verringern. Melden Sie dem betroffenen Online-Dienst die Kompromittierung. Die meisten Provider helfen Ihnen mit einem neuen Passwort, manche haben diesen Vorgang bereits automatisiert.

Werden die gleichen Anmeldedaten auch auf anderen Webseiten genutzt, sollten sie auch dort schnellstens geändert werden. Kontrollieren Sie alle ihre Internetshops, ob dort etwas in Ihrem Namen bestellt wurde und ob die Lieferung noch storniert werden kann.

10.1.7. Security-Software, Taskmanager, Registry-Editor sind deaktiviert

Ihre Security-Software ist deaktiviert, obwohl sie noch nicht abgelaufen ist? Ein Update ändert daran nichts oder gelingt nicht? Vermutlich ist das System infiziert. Ganz besonders gilt das, wenn der Taskmanager nicht mehr startet. Versuchen Sie, die Schutzsoftware zu deinstallieren und nach einem Neustart erneut zu installieren. Funktioniert sie nach dem nächsten Neustart und der Aktualisierung wie immer? Wenn nicht, ist eine Neuinstallation von Windows ratsam. Im Internet gefundene Ideen funktionieren nicht oft.

10.1.8. Software installiert sich selbstständig

Mitten am Tag werden Sie aufgefordert, einer Installation zuzustimmen? Das Programm behauptet, ein Update des Antivirenprogramms o. ä. zu sein? Ungewollte und unerwartete Installationsprozesse, die aus dem Nichts starten, sind ebenfalls ein starkes Anzeichen dafür, dass das System gehackt wurde.

Sie haben ein Programm – nur **ein** Programm – heruntergeladen und werden **zwei**mal gefragt, ob Sie einer Installation zustimmen? Malware versucht oft, sich wie jede x-beliebige Software mit einer Installationsroutine auf dem Rechner zu installieren. Häufig kommen die Schädlinge als „Huckepack“ mit sauberen Programmen. Oft hilft es, Lizenzvereinbarungen zu lesen, bevor Sie ein Programm herunterladen. In vielen dieser Texte, die leider niemand liest, wird haarklein aufgeführt, welche Programme wie mitkommen.

10.1.9. Der Mauszeiger bewegt sich von allein

Sie kehren nach einer Pause zum PC zurück und sehen, dass sich der Mauszeiger zielstrebig bewegt? Wird Ihr PC gerade ferngesteuert? Wenn die Maus einen Wackelkontakt hätte, würde sie sich nicht zielstrebig bewegen.

Was tun? Fotografieren oder filmen Sie den Bildschirm mit der Digitalkamera zu Beweiszwecken. Trennen Sie dann den PC vom Internet. Suchen Sie einen „sauberen“ PC und ändern Sie alle wichtigen Passwörter, angefangen mit Online-Banking und E-Mail-Konten. Sprechen Sie mit Ihrer Bank: Vielleicht sollten Sie ein Limit für Online-Überweisungen setzen? Manche Banken bieten eine E-Mail-Benachrichtigung bei Lastschriften an.

Stellen Sie Strafanzeige bei der Polizei. Banken ersetzen einen eventuellen Schaden nicht, wenn Sie leichtsinnig gewesen sind. Es ist gut, wenn Sie nachweisen können, dass es sich um einen Angriff gehandelt hat, z. B. mit Bildschirmfotos. Lassen Sie von einem IT-Forensiker eine komplette Kopie Ihrer Festplatte anfertigen. Die Kopie kann gegebenfalls später genau untersucht werden kann, um die Art des Schadens zu beweisen. Vielleicht sollten Sie die infizierte Festplatte einfach ausbauen und durch eine neu gekaufte Festplatte ersetzen, das kommt Sie billiger als ein Forensiker. Eine Windows-Neuinstallation sollten Sie auf jeden Fall vornehmen.

10.1.10. Der PC ist sehr langsam

Es könnte sein, dass die Festplatte zu voll ist (C: sollte nicht mehr als 80 % voll sein) oder „im Sterben liegt". Klicken Sie auf Start und tippen Sie in das Suchfeld „Programme/Dateien durchsuchen" den Befehl „eventvwr.msc" ein. In der Ereignisanzeige wählen Sie „Windows-Protokolle" → „System". Wenn Sie mehrere „Fehler" von der Quelle „Disk" finden können, sollten Sie Ihre Daten sichern und eine neue Festplatte kaufen.

Wenn Sie die Tasten „Strg" und „Alt" (beide in der unteren linken Ecke der Tastatur) gleichzeitig gedrückt halten und zusätzlich die Taste „Entf" drücken, muss sich ein bildschirmfüllendes Menü öffnen. Klicken Sie auf „Task-Manager starten". Auf den Registerkarten „Leistung" und „Netzwerk" können Sie die Auslastung des PCs kontrollieren. Die LAN-Verbindung sollte inaktiv sein und selbst während des Surfens sollten die Auslastungsspitzen unter 1 % liegen. Die CPU-Auslastung im Ruhezustand darf einige Spitzenwerte unter 10 % haben (Windows beschäftigt sich mit sich selbst). Auf der Registerkarte „Prozesse" kann man sehen, welches Programm wie viel Prozessorzeit belegt. Machen Sie das Taskmanager-Fenster breit genug, damit Sie den Programmnamen und die Beschreibung sehen können. Vielleicht finden Sie so das Programm, welches die hohe Auslastung verursacht.

10.1.11. Die Startseite des Browsers hat sich geändert

Manchmal reicht es aus, einfach die Startseite des Browsers richtig einzustellen. Wie geht das?

Beim Internet Explorer:

- Taste F10 drücken, um die Menüleiste einzublenden,
- „Extras" → „Internetoptionen" → Registerkarte „Allgemein"
- Tragen Sie Ihre Wunschseite ein oder klicken Sie auf „Aktuelle Seite", damit alle in diesem Moment geöffneten Webseiten zu Startseiten werden.
- Übernehmen, OK.

Beim Mozilla Firefox:

- Über den Menü-Button zu „Einstellungen", → Registerkarte „Allgemein"

Beim „Chrome":

- Menü-Button → „Einstellungen".
- Beim Start „Bestimmte Seite oder Seiten öffnen" → „Seiten festlegen".

Schließen Sie den Browser und starten Sie ihn erneut. Ist die Startseite immer noch falsch?

Klicken Sie mit der rechten Maustaste auf das Icon bzw. den Startmenüeintrag, mit dem Sie üblicherweise den Browser starten, und dann auf „Eigenschaften".

Die Zeile „Ziel" sollte mit dem Namen des Browsers enden, z. B. „iexplore.exe" oder „firefox.exe", meist gefolgt von einem Anführungszeichen. Wenn dahinter die Webadresse der lästigen Seite steht, löschen Sie diese heraus!

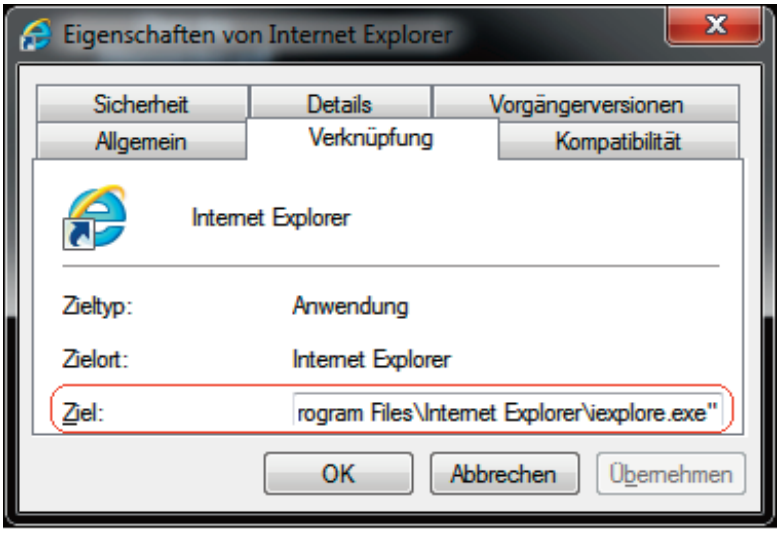

Abb 10.1: Intakte Verknüpfung mit Internet Explorer

10.2. PC säubern oder neu installieren?

In leichten Fällen (der Virenscanner hat eine oder wenige infizierte Dateien gefunden) ist eine Reparatur sinnvoll. In schweren Fällen kann es sinnvoll sein, die Daten zu sichern, die Festplatte zu formatieren und das Betriebssystem von Grund auf neu zu installieren.

Woran erkennt man einen derart schweren Fall, dass eine Neuinstallation sinnvoll ist?

- Eine einfache Reparatur führt nicht zum Erfolg.
- Das installierte Antivirenprogramm meldet, den Schaden nicht reparieren zu können, und ein Online-Scanner kann es auch nicht.
- Nach einer scheinbar gelungenen Reparatur ist nach einiger Zeit der Schädling wieder da.
- Nach einer „einfachen Reparatur“ ist das Betriebssystem instabil oder offensichtlich beschädigt.
- Multiple Probleme: Mehrere Arten von Schädlingen gleichzeitig. Systemsteuerung oder einige Programme lassen sich nicht starten, System ist ausgelastet, Festplatte ist im Dauerbetrieb.
- Ihr PC verschickt E-Mails ohne Ihr Wissen.
- Sie haben das Gefühl, dass jemand Ihren PC manipuliert.

Die Entscheidung zwischen Reparatur und Neuinstallation ist nicht einfach. Eine Neuinstallation dauert einen Tag, aber eine Reparatur kann ebenfalls mehrere Stunden dauern (und am Ende fehlschlagen). Nach einer akkurat durchgeführten Neuinstallation kann man 100 % sicher sein, dass das System wieder sauber ist. Falls Ihr Windows bereits vor dem Befall nicht im Bestzustand war, ist eine Reparatur vorzuziehen.

Falls Sie noch Windows Vista oder gar Windows XP installiert hatten, sollten Sie gleich auf Windows 7 wechseln. Meiden Sie Windows 8 – der Riesenaufwand zum Erlernen des neuen Bedienkonzepts ist einfach zu groß.

Bei den meisten befallenen PCs konnten wir drei und mehr **verschiedene** Schädlinge finden, die sich auf mehrere dutzend Dateien verteilten. Dass ein PC von nur einem Schädling befallen ist, war selten. Aus Sicht der Hacker ist das logisch: Wenn man einen PC geknackt hat, nutzt man das voll aus und installiert auch noch das restliche Sortiment der eigenen Malware. Und wenn der Nutzer endlich einen der Schädlinge entfernt hat und den PC neu startet, installiert einer der verbliebenen Schädlinge seinen „Kollegen“ erneut.

Einigermaßen sicher können Sie nur sein, wenn Sie

- entweder die Festplatte aus dem infizierten PC ausgebaut und als Zweitplatte an einem sauberen PC durchgecheckt haben
- oder wenn Sie den PC von einer Live-CD gebootet und mit einem Antivirenprogramm durchsucht haben, das sich vor dem Virenscan die aktuellsten Virenkennungen heruntergeladen hat.

Ein installiertes Antivirenprogramm ist in der Regel korrumpiert. Vergessen Sie nicht, auf dem gesäuberten PC das Antivirenprogramm zu deinstallieren und nach einem Neustart erneut zu installieren.

Aber wundern Sie sich nicht, wenn die Viren einige Wochen später wieder da sind. Tarnkappenviren und Rootkits lassen sich schwer entdecken und entfernen. Außerdem gibt es einige Stellen, wo Schadcode schwer aufzufinden ist, z. B. in fälschlich als defekt deklarierten Sektoren der Festplatte.

Ein Virus könnte die Einstellungen des PC verändert haben, einen Port geöffnet und Ordner für den Fernzugriff freigegeben haben. Er könnte ein Huckepack-Programm installiert haben, z. B. ein legales Fernsteuerprogramm. Auch wenn der Virus restlos entfernt ist, bleiben dessen Änderungen bestehen.

Auch wenn es sehr aufwändig ist: Die sicherere Methode ist: Daten sichern, alle Partitionen oder zumindest die Systempartition löschen, Windows und Anwendungen von Grund auf neu installieren, Daten zurückkopieren und bei alle dem keinen Fehler machen.

In seltenen Fällen reicht es nicht einmal, die Festplatte bzw. Partition zu formatieren. Moderne Viren (z.B. Bootviren) bleiben möglicherweise erhalten. Entweder Sie kaufen eine neue Festplatte oder Sie benutzen ein Programm, welches die Festplatte mit einem Muster überschreibt (einschließlich der kompletten Spur Null).

Fakt ist: Auch wenn eine Säuberung scheinbar perfekt gelungen ist – **wenn ein Rechner einmal unterwandert gewesen ist, darf ihm nie wieder vollständig vertraut werden.**

10.3. DESINFEKTIONSMETHODEN

Falls Sie sich entschlossen haben, auf eine Neuinstallation zu verzichten, folgen hier einige Anleitungen, wie Sie die Malware hoffentlich entfernen können.

10.3.1. Der PC startet nicht mehr

Die Reparatur ist vielleicht mit der Windows-Installations-DVD möglich. Wenn Sie diese nicht haben, können Sie rechtzeitig vorher einen „Systemreparaturdatenträger“ erstellen:

„Start → Alle Programme → Wartung → Systemreparaturdatenträger erstellen“. Legen Sie einen CD-Rohling ein und klicken Sie auf „Datenträger erstellen“. Beschriften Sie die fertige CD mit „Reparaturdatenträger“ und heben Sie ihn gut auf.

Wenn Windows nicht mehr startet, booten Sie vom Reparaturdatenträger oder der Windows-Installations-DVD.

- „Press any key to boot from CD or DVD“
- Windows is loading files ...
- Bestätigen Sie die Spracheinstellung, dann „Weiter“ zu den „Computerreparaturoptionen“. Sie müssen das zu reparierende Betriebssystem auswählen, dann „Weiter“.
- Nun können Sie im Fenster „Systemwiederherstellungsoptionen“ ein geeignetes Tool auswählen, z. B.
  - mit der „Systemstartreparatur“ die Startdateien des Systems reparieren,
  - mit der „Systemwiederherstellung“ das System auf einen früheren Zustand zurücksetzen, siehe dazu 10.3.5. „Rückkehr zum letzten Systemwiederherstellungspunkt“,
  - das „Eingabeaufforderungsfenster“ öffnen. Das Systemlaufwerk hat den Laufwerksbuchstaben D: Sie können z. B. mit dem Befehl
    `robocopy d:\ f:\ *.doc* *.xls* /s /r:0` (wobei `f:` die externe Festplatte ist)
    alle Word- und Excel-Dateien retten. Wie Sie die Eingabeaufforderung sonst noch nutzen können, sehen Sie nächste Seite unter: „10.3.2. Reparaturmöglichkeiten an der Eingabeaufforderung“.

10.3.2. Malware im „Abgesicherten Modus“ entfernen

Der abgesicherte Modus ist ein Minimalbetriebsmodus, bei dem nur die unverzichtbaren Treiber geladen und nur unverzichtbare Dienste gestartet werden. Es besteht eine gute Chance, dass Malware im abgesicherten Modus nicht aktiv wird und sich nicht tarnen kann.

Wie kommt man in den abgesicherten Modus?

Drücken Sie die Funktionstaste F8 genau im Moment, wenn der PC mit dem BIOS-Test fertig ist und Windows zu starten beginnt (wenn „Windows wird gestartet“ angezeigt wird). Achtung! Sie müssen schnell sein! Sie können auch rechtzeitig vorher beginnen, die Taste F8 im Viertelsekundenabstand zu drücken, um den richtigen Zeitpunkt nicht zu verpassen.

Bei manchen PCs wird die Taste F8 vom BIOS benutzt, um ein Bootmenü anzuzeigen, in dem Sie wählen können, ob Sie von DVD, Festplatte, USB-Stick o. Ä. booten wollen. Bewegen Sie den Kursor auf „Booten von der Festplatte“. Drücken Sie dann Enter und **sofort** wieder auf F8.

Wählen Sie nun einen der „Abgesicherten Modi“ unter den Startoptionen aus.

Der Start im abgesicherten Modus gelingt mir nicht

Falls Windows hartnäckig normal hochfährt, gibt es noch eine Möglichkeit, im abgesicherten Modus zu starten. Starten Sie die Eingabeaufforderung und tippen Sie den Befehl „msconfig“ ein. Auf der Registerkarte „Start“ aktivieren Sie unten links „Abgesicherter Start“ und wählen Sie die Optionen aus, die Sie benötigen. Nach dem OK starten Sie neu. Nun sollte Ihr PC im abgesicherten Modus starten.

Wenn Sie mit Ihren Arbeiten im abgesicherten Modus fertig sind, den Haken im Kästchen „Abgesicherter Start“ wieder entfernen, damit der Rechner zukünftig wieder normal hochfährt.

Falls auch das nicht klappt, hat vielleicht der BKA-Trojaner o. ä. den abgesicherten Modus lahmgelegt. Dann brauchen Sie die Windows-Installations-DVD.

- Starten Sie den PC von dieser DVD (vorher müssen Sie vielleicht die Boot-Reihenfolge im BIOS ändern oder die Taste drücken, mit der man beim Start die Bootsequenz einmalig ändern kann, z. B. F12).
- Im Installationsfenster wählen Sie „Computerreparaturoptionen“.

Drei Arten des Abgesicherten Modus

- „Abgesicherter Modus mit Netzwerktreibern“ ermöglicht das Herunterladen von Reparaturprogrammen, Treiber–Updates und Online-Antivirenprogrammen.
- „Abgesicherter Modus“ verzichtet auf Netzwerktreiber.
- „Eingabeaufforderung“ stellt die geringsten Anforderungen an Windows und ist manchmal die letzte Rettung, wenn die beiden anderen abgesicherten Modi nicht starten. Die grafische Bedienoberfläche ist nicht verfügbar, es steht nur die Eingabeaufforderung zur Verfügung.

Reparaturmöglichkeiten im abgesicherten Modus (mit oder ohne Netzwerkfunktionen)

- Vielleicht findet Ihr Antivirenprogramm den Übeltäter.
- Nutzen Sie einen Online-Virenscanner.
- Versuchen Sie mit der Systemsteuerung → Software, unerwünschte Programme oder Toolbars zu entfernen. Es sind Programme dabei, die Sie nicht kennen? Entfernen Sie im Zweifel lieber einige Programme zu viel als zu wenig. Der PC wird sich schon melden, wenn ein wichtiges Unterprogramm fehlt.
- Im Fenster „Reparaturkonsole“ können Sie Windows mit der Systemwiederherstellung auf einen früheren Zeitpunkt zurücksetzen, an dem der abgesicherte Modus noch funktionierte.
- Ihre Daten bleiben unverändert. Das bedeutet aber auch, dass ein eventuell eingefangener Virus oder Trojaner noch auf dem PC existiert. Obwohl er wahrscheinlich deaktiviert ist, sollte er noch entfernt werden.

Reparaturmöglichkeiten an der Eingabeaufforderung

Falls der Start nur mit der „Eingabeaufforderung“ gelingt, können die folgenden Befehle nützlich sein:

- `explorer` bringt Ihnen den Desktop zurück, und Sie können beispielsweise mit dem Windows–Explorer Ihre Daten sichern oder verdächtige Dateien löschen.
- `eventvwr` (die Ereignisanzeige) zeigt Ihnen mögliche Probleme. Suchen Sie unter „System“ und „Anwendungen“ nach Auffälligkeiten.
- Mit `regedit` können Sie Korrekturen an der Registry vornehmen.
- Mit `control` kann die Systemsteuerung geöffnet werden, die Konfigurationszentrale des Systems. Hier können Sie verdächtige Programme entfernen, Treiber aktualisieren und vieles andere.
- Mit `msconfig` kann man verdächtige Programme vom Systemstart ausschließen.
- Mit `rstrui.exe` starten Sie die Systemwiederherstellung. Sie können auswählen, bis zu welchem Wiederherstellungspunkt Sie Windows zurücksetzen wollen.
- Mit den Befehlen `xcopy` oder `robocopy` können Sie Daten auf eine externe Festplatte kopieren.

Anmerkung: Wenn der Start nur mit der „Eingabeaufforderung“ gelingt, besteht ein geringes Restrisiko, dass im Hintergrund ein ungewöhnlich cleverer Schädling aktiv ist. Starten Sie besser den PC vom Reparaturdatenträger oder der Windows-Installations-DVD, wie eine Seite vorher unter „10.3.1. Der PC startet nicht mehr“ beschrieben.

10.3.3. Online-Virenscanner

Falls der PC infiziert ist, muss man damit rechnen, dass ein installierter Virenscanner nicht mehr funktioniert. Wenn Windows noch startet, kann man den PC mit einem Online-Scanner untersuchen. Doch schalten Sie Ihre anderen PCs aus oder trennen Sie diese vom Router, bevor Sie den verdächtigen PC an den Router anstecken.

Der Scanner hat nichts gefunden? Das heißt nicht, dass Sie aufatmen können. Online-Scanner können einige Arten von Schädlingen prinzipbedingt nicht finden. Starten Sie den Scanner noch einmal, und zwar im „abgesicherten Modus mit Netzwerktreibern". Doch auch im abgesicherten Modus könnte ein getarnter Schädling unentdeckt bleiben. Es ist grundsätzlich besser, den PC von einer Rettungs-CD zu booten.

10.3.4. Virencheck mit einer Antivirus-Rettungs-CD

Wenn der PC nicht mehr normal startet, können Sie es mit einer Antiviren-Rettungs-CD versuchen. Wenn Sie ein Antivirenprogramm mit beiliegender Installations-CD gekauft haben, ist vielleicht diese CD bootfähig. Andernfalls können Sie mit einem „sauberen" PC eine geeignete Rettungs-CD herunterladen und auf CD brennen.

Beispiel: Rettung mit der „Avira-AntiVir-Rettungs-CD"

Lassen Sie eine Suchmaschine nach „Avira-AntiVir-Rettungs-CD" suchen. Sie finden das Programm auf der Seite `http://www.avira.com/de/download/product/avira-rescue-system` in zwei Versionen: Als ISO-Image, welches Sie mit Ihrem Brennprogramm auf eine bootfähige CD brennen müssen, und als EXE-Version mit integriertem Brennprogramm. Außerdem gibt es eine deutschsprachige Anleitung zum Download. Wenn Sie nicht sicher sind, dass Ihr Brennprogramm eine ISO-Datei brennen kann, dann wählen Sie die .EXE-Version. Legen Sie einen CD-Rohling ein und starten Sie die heruntergeladene „rescue-system.exe". Nach der Sicherheitsabfrage (.exe-Dateien sind potenziell gefährlich) startet Ihr Brenner.

Booten Sie von der erstellten Rettungs-CD. Wählen Sie im Startbildschirm den Menüpunkt „Boot AntiVir Rescue System (default)" aus und drücken Sie Enter. Wählen Sie „Deutsch" als Sprache. Wenn eine Internetverbindung besteht, erneuert ein Klick auf „Update" die Virensignaturen. Klicken Sie dann auf „Virenscanner" und „Scanner starten", um das Betriebssystem zu untersuchen.

Nach dem Scan finden Sie unter „Sonstiges" die „Logdatei" mit der Liste der gefundenen und der behobenen Probleme. Mit dem Dateimanager können Sie verdächtige Dateien löschen und unter „Extras" gibt es „Regedit", mit dem ein Fachmann die Registry bereinigen kann. Die Rettungs-CD enthält den Firefox-Browser, damit Sie im Internet nach Lösungsvorschlägen suchen können.

Beispiel: Rettung mit Windows Defender Offline

Diese Software wird von Microsoft kostenlos zur Verfügung gestellt. Suchen Sie mit Google nach „defender offline" und gehen Sie zur Seite „windows.microsoft.com/de-de/...". Entscheiden Sie sich für die 32- oder 64-Bit-Version, sie muss mit der Windows-Version auf dem infizierten PC übereinstimmen. Wenn Sie eine leere CD einlegen, wird die Rettungs-CD gebrannt.

Booten Sie von der Rettungs-CD. Wählen Sie den Startmodus (üblicherweise den „normalen Windows-Start"). Nach einem langdauernden „Windows wird geladen" untersucht das Rettungsprogramm den Computer und bietet je nach erkanntem Problem die Reparaturmöglichkeiten an. Die kurze Überprüfung dauert einige Minuten, die vollständige Überprüfung mehr als eine Stunde.

10.3.5. Rückkehr zum letzten Systemwiederherstellungspunkt

Wenn der PC noch startet, können Sie mit der „Systemwiederherstellung“ das System auf einen früheren Zustand zurücksetzen. Das Programm finden Sie auf „Start → Alle Programme → Zubehör → Systemprogramme“. Wählen Sie einen Zeitpunkt aus, an dem das System vermutlich noch in Ordnung war.

Was tun, wenn der älteste Systemwiederherstellungspunkt nicht weit genug zurückreicht? Vielleicht hilft Ihnen „AwayVir“.

10.3.6. Alle potenziell schädlichen Prozesse stoppen

Von `http://www.langmeier-software.com/awayvir-download.php` können Sie ein kostenloses Programm „AwayVir“ herunterladen. Installieren Sie das Programm im abgesicherten Modus oder starten Sie die portable Version von einem USB-Stick. AwayVir deaktiviert alle Prozesse, die nicht zum Betriebssystem gehören. Das Betriebssystem wird auf einen Zusand ähnlich wie nach der Neuinstallation zurückgesetzt. Mit hoher Wahrscheinlichkeit werden alle schädlichen Prozesse deaktiviert. Anschließend kann ein Antivirenprogramm die inaktiven Reste beseitigen.

10.4. PC neu installieren

10.4.1. Daten von einem verseuchten PC retten und säubern

Schadsoftware kann sich nur verbreiten und Schaden anrichten, wenn sie ausgeführt wird. Auch wenn es sich merkwürdig liest: Eine verseuchte Festplatte ist ungefährlich, solange Sie keine auf dieser Festplatte gespeicherten Programme starten und keine Dateien öffnen. Das Betrachten der Ordner mit dem Windows Explorer oder einem anderen Dateimanager ist ungefährlich, das Sortieren, Kopieren oder Löschen von Dateien auch.

Welche Dateien sind gefährlich? Alle ausführbaren Dateien, vor allem Dateien mit `.exe`, `.com` und `.dll`, seltener `.hta`, `.pif`, `.scr`, `.scf` (komplette Liste siehe 4.2.2. E-Mail-Versand mit SMTP).

Daraus folgen die ersten drei Vorsichtsmaßnahmen:

- Kopieren Sie keine Programmordner. Kopierte Programme funktionieren ohnehin nicht, Sie müssen auf dem neuen System jedes benötigte Programm von Grund auf neu installieren.
- Kopieren Sie nur Dateitypen, von denen Sie wissen, dass es sich um Daten handelt, vorzugsweise um Ihre selbst erstellten Daten.

Verhindern Sie, dass ein Virus aktiv ist, während Sie Daten kopieren! Ausführbarer Programmcode kann auch im Master Boot Record der Festplatte oder im Startprogramm eines USB-Sticks stecken. Deshalb dürfen Sie einen infizierten PC nicht mit seinem eigenen, infizierten Betriebssystem starten. Das könnte dazu führen, dass jeder Datenträger, den Sie anstecken, augenblicklich infiziert wird. Entweder Sie starten ein Betriebssystem von einer Live-CD oder Sie stecken die verseuchte Festplatte an einen „sauberen“ PC mit einem aktuellen Antivirenprogramm. Verhindern Sie aber unbedingt, dass der saubere PC versehentlich von der infizierten Festplatte startet! Überprüfen Sie die Boot-Reihenfolge im BIOS!

Vielleicht wollen Sie den Befehl ROBOCOPY zum Kopieren verwenden, der in meinem Buch „Datensicherung für Anfänger“ ausführlich vorgestellt wurde? Kopieren Sie die Datei `robocopy.exe` aus den Ordner `C:\Windows\System\` ins Hauptverzeichnis der Ziel-Festplatte. Geben Sie dann in der „Eingabeaufforderung“ den folgenden Befehl ein:

```
Z:\robocopy Q:\ Z:\retten\ /s /r:0 /xd c:\windows c:\programme* /xf *.exe *.com *.dll
```

Statt **Q** (Quelle) und **Z** (Ziel) müssen Sie die bei Ihnen gültigen Laufwerksbuchstaben einsetzen.

Mit dem obigen Befehl werden alle Dateien kopiert, außer Dateien vom Typ `*.exe *.com *.dll` und auch die Dateien aus den Verzeichnissen `C:\Windows` und `C:\Programme` werden nicht mitkopiert.

Leider versteckt Robocopy den soeben erstellten Ordner `Z:\retten` mit allen Dateien. Vielleicht, um Manipulationen am Backup zu erschweren? Sie müssen einen weiteren Befehl an der Eingabeaufforderung eintippen:

```
attrib Z:\retten\ -s -h -r
```

Auch hier müssen Sie `Z:` durch die Bezeichnung des Ziellaufwerks ersetzen. Mit dem Befehl werden die Kennzeichnungen **S**ystem, **H**idden (versteckt) und **R**ead-Only (nur Lesen) aufgehoben und die Daten sind zugänglich.

Wenn Sie einen Dateimanager verwenden wollen bzw. müssen, genügt es vermutlich, Ihre Ordner „Desktop“, „Eigene Bilder“, „Eigene Dokumente“, „Eigene Musik“, „Eigene Videos“ und „Favoriten“ zu kopieren. Achten Sie darauf – besonders beim Desktop-Ordner – keine ausführbaren Dateien mitzukopieren, die möglicherweise verseucht sein könnten. Sie können die ausführbaren Dateien vor dem Kopieren mit einem Kommandozeilenbefehl sehr effektiv löschen: Starten Sie die „Eingabeaufforderung“, am besten mit Administratorrechten:

- „Start → Alle Programme → Zubehör“
- Klicken Sie mit der rechten Maustaste auf „Eingabeaufforderung“ und mit der linken Maustaste auf „Als Administrator ausführen“.
- Geben Sie das Administrator-Kennwort ein und klicken Sie auf „Ja“ bzw. „OK“.
- Tippen Sie „`del Q:\*.exe /s /q`“ in das Fenster ein und bestätigen Sie mit der Enter-Taste.

Wiederholen Sie den Befehl, wobei für `*.exe` nacheinander `*.dll` und `*.com` eingesetzt werden, eventuell auch für weitere Dateitypen.

10.4.2. Regeln für eine sicherheitsbewusste Neuinstallation

- Daten sichern.
- Die Festplatte partitionieren. Es ist sehr empfehlenswert, unterschiedliche Partitionen für Betriebssystem und Daten vorzusehen. Dann braucht man beim nächsten Störfall nur Laufwerk C: mit dem Betriebssystem neu zu installieren, während die Daten auf D: erhalten bleiben.
- Windows in einer leeren Partition installieren. Niemals über ein vorhandenes System darüberinstallieren!
- Die unverzichtbaren Treiber installieren.

Sie sind gerade fertig geworden, Windows neu zu installieren? Beginnen Sie nicht damit, Ihre Daten auf den neu eingerichteten PC zu kopieren – es könnten infizierte Dateien darunter sein. Zuerst sollten Sie die Sicherheitslücken des Betriebssystem schließen, indem Sie alle angebotenen Updates ausführen. Dann sollten Sie ein Antivirenprogramm installieren und ebenfalls auf den neuesten Stand bringen. Erst jetzt können Sie die benötigten Anwendungsprogramme installieren und zunächst nur die allerwichtigsten Daten zurückkopieren.

- Neuestes Service Pack installieren.
- Aktuelle Sicherheitsupdates installieren (möglichst ohne Internetverbindung, also z.B. von CD!)
- Restliche Treiber wie Grafikkarte, Sound, Maus, Drucker usw. installieren (Natürlich als Administrator).
- Virenscanner (möglichst von CD) installieren und einrichten.
- Ein eingeschränktes Benutzerkonto einrichten.
- Erst jetzt zum ersten Mal die Internet Verbindung herstellen! (Im Schutz eines DSL-Routers)
- Vom Virenscanner die neuesten Signaturen/Updates herunterladen.
- Die restlichen Daten zurücksichern. Beachten Sie, dass in den gesicherten Daten noch Schädlinge enthalten sein können. Daher sollten die Daten nicht sofort nach der Neuinstallation neu aufgespielt werden, sondern (falls Sie so lange warten können) erst eine Woche später. Wenn das Antivirenprogrammen Signaturen hat, die eine Woche neuer sind als der Schädling, steigt die Erkennungsrate bei eine Woche alten Dateien auf 100 %, hat der Test einer Computerzeitschrift ergeben.