

Anleitung: Neuaufsetzen des Systems und anschliessende Absicherung!

Wenn auf einem System eine **Malware** [☞](#), wie z.B. ein Backdoor Trojaner oder ein Wurm mit Backdoor Funktionalität installiert und diese auch aktiv wurde, dann spricht man von einer **Kompromittierung (Bloßstellung) des Systems** [☞](#). Dies hat zur Folge, dass alle Dateien (insbesondere AV Anwendungen) manipuliert werden können und somit die sensiblen Daten des Benutzers bzw. Systems als bekannt anzusehen sind. Das System als solches ist folglich nicht mehr vertrauenswürdig, da die Möglichkeit des Fernzugriffs durch Dritte besteht.

Die einzig sichere Möglichkeit um wieder einen vertrauenswürdigen Zustand herzustellen wäre ein Neuaufsetzen des System mit anschliessender Absicherung.

Was Backdoor Trojaner können:

[Trojaner-Info](#) [☞](#)

[Wikipedia-Backdoor](#) [☞](#)

[Wikipedia-Trojaner](#) [☞](#)

Q: Warum ist eine Bereinigung des kompromittierten Systems durch Removal-Tools und AV Scanner nicht sinnvoll?

A: [Entfernung von Schädlingen](#) [☞](#)

[Was tun bei Kompromittierung des Systems?](#) [☞](#)

[Ich habe einen Virus / Dialer / „Trojaner“ / wurde „gehackt“. Was soll ich tun?](#) [☞](#)

[Cobra \(MOD TB\)](#) [☞](#) und [Cidre \(MOD d - b\)](#) [☞](#)

[Help: I Got Hacked. Now What Do I Do?](#) [☞](#)

Q: Was bedeutet Neuaufsetzen?

A: Es sollte mindestens die System-Partition (i.d. Regel C:), besser aber alle befindlichen Partitionen der Festplatte, gelöscht werden. Anschliessend wird die Festplatte bei der Installation des Betriebssystems neu partitioniert und das System gemäss der nachfolgenden Anleitung abgesichert.

[FAQ - Partitionieren unter Windows 2000 und XP](#) [☞](#)

[Windows neu oder erstmalig installieren \(Screenshotguide\)](#) [☞](#)

Nach dem Neuaufsetzen und VOR der ersten Internet Verbindung solltest du folgende Punkte abarbeiten:

1. [Eingeschränktes Benutzerkonto](#) [☞](#) erstellen und zum Surfen benutzen
2. Die [Windows "Firewall" \(Win XP SP2/3\)](#) [☞](#) aktivieren
3. Das [System updaten](#) [☞](#)[1] und stets aktuell halten
4. NT-Dienste sicher konfigurieren [ntsvcfg.de](#) [☞](#) oder [dingens.org](#) [☞](#)
5. [IE sicherer konfigurieren](#) [☞](#) und nur noch für das Windows Update benutzen (Alternativ: [blafusel.de](#) [☞](#))
6. Sichere und komfortablere Browser wie z.B. die [Mozilla Suite oder Firefox](#) [☞](#) verwenden
7. MS Outlook und MS Outlook Express [sicherer konfigurieren](#) [☞](#).
8. Besser wäre es, sichere eMail Clients wie [Thunderbird](#) [☞](#) einzusetzen
9. Deine [Passwörter](#) [☞](#) ändern
10. Image der Systempartition erstellen mit z.B. Acronis True Image 8
11. Surf-, Patch- und Downloadverhalten überdenken
12. AV Anwendung installieren, AV Guard aktivieren und aktuell halten

[1] Bezugsmöglichkeiten von Service Pack 3 für XP -> [Download](#) oder [CD-Bestellung](#)
Bezugsmöglichkeiten von Service Pack 1 für Vista -> [Download](#) oder [CD-Bestellung](#)

Zusätzlich sollten folgende Einstellungen am System vorgenommen werden:

- a) Den [Windows Nachrichtendienst](#) deaktivieren
- b) Dateinamenerweiterung bei bekannten Dateitypen wieder einblenden: Win-Taste + E -> Extras -> Ordneroptionen -> Reiter "Ansicht" -> Haken bei "Erweiterungen bei bekannten Dateitypen ausblenden" **entfernen**.
- c) ["Geschützte Systemdateien ausblenden \(empfohlen\)" und "Alle Dateien und Ordner anzeigen"](#)

Wichtig!

- Bei Win 2000 entfällt Punkt 2! Punkt 1, 3 und 4 sind vor der ersten I-net Verbindung abzuarbeiten.

Ebenso empfehlenswert diese Patches offline auszuführen [MS03-039](#) und [KB835732](#)

- Bei Win ME entfällt Punkt 1, 2 und 4. Die [Datei- und Druckerfreigabe](#) sollte deaktiviert werden.

Infos zur Installation von Win ME, 2000, XP und Vista findest du hier:

[Windows Vista Installation](#) und [Windows Vista FAQ](#)
[Windows XP Installation](#) und [Windows XP FAQ](#)
[Windows 2000 Installation](#) und [Windows 2000 FAQ](#)
[Windows ME Installation](#) und [Windows ME FAQ](#)
[Windows 98 Installation](#) und [Windows 98 FAQ](#)

Lesenswerte Lektüre für die Zukunft:

[Kompromittierung unvermeidbar?](#)
[Wie kann ich mein System vernünftig absichern?](#)
[Der Link-Block](#)
[Security through Obscurity](#)
[PE-Builder...der Retter!](#)
[\(Un\)Sicheres Windows am Heim-PC](#)
[Tutorials des dedies-boards](#)
[Bundesamt für Sicherheit in der Informationstechnik](#)
[Sicher im Internet](#)

Aktuelle Sicherheits- und Malware News:

[Heise](#)
[Golem](#)
[Virenticker.de](#)
[Scip - Sicherheitslücken](#)
[tecchannel](#)
[SecurityFocus](#)
[testticker](#)
[Infos zu Patches für MS-Produkte](#)

To be continued...

Eine ausführliche Anleitung von MobyDuck kannst Du hier nachlesen ->
[Windows XP richtig aufsetzen](#)

Damit Ihr die Anleitung auch offline betrachten könnt', steht diese, ab sofort zum [Download](#) im PDF Format zur Verfügung!