

Windows sicher einrichten in 15 Schritten

erstellt am 13. November 2004 von

COBRA

Dies ist eine einfache Schritt-für-Schritt-Anleitung, um einen Windows 2000- oder XP-Rechner sicherer einzurichten. Sie wurde geschrieben, da sich viele von uns bereits bei der Installation von Windows Würmer einhandeln und oft nur wenig später Trojaner und Backdoors, die das System vollständig **kompromittieren**. Wir wollen mit dieser einfachen Anleitung einen Weg aufzeigen, ein sichereres Windows-System zu installieren und zu administrieren. Auf kostenpflichtige Komponenten weist das €-Symbol hin.

1. Optional, aber sehr empfehlenswert: den Rechner an einen Hardwarerouter (50 €) anschließen.
2. Partitionierung nach Einschieben der Windows CD. Empfehlenswert, und hier am Beispiel einer 60 GB-Platte (GB hier behandelt wie von den Plattenherstellern: 1000 MB = 1 GB):

Partition	Name	Größe (GB)	Dateisystem
c:\	system	6.0	NTFS
d:\	swap	0.5	NTFS
e:\	programs	10.0	NTFS
f:\	data	43.5	NTFS

Diese einfache Partitionierung hat viele Vorteile gegenüber einer einzelnen 60 GB Partition. Die Trennung von Betriebssystem (system) und Programmen (programs) erspart Defragmentieren. Die Einrichtung eines fixen virtuellen Speichers auf d:\ (swap) dient dem gleichen Zweck und beschleunigt langfristig das Betriebssystem. Die Trennung von Daten und dem übrigen System schließlich erleichtert die Wiedereinrichtung des Betriebssystems ungemein: die Daten auf f:\ bleiben auch bei der Formatierung von c:\ und e:\ unangetastet. Natürlich kann die Partitionierung auch beliebig feiner sein, als hier angedeutet. Man beachte aber: bei einem Backup des Systems mittels einer Image-Software (siehe Punkt

15) müssen die Partitionen c:\ und e:\ bei jeder (Teil-) Sicherung zeitgleich gesichert werden, da ansonsten die Registry auf c:\ möglicherweise (falls zwischenzeitlich weitere Programme installiert werden) nicht mehr den tatsächlich installierten Programmen auf e:\ entspricht.

3. Installieren von Windows 2000/Windows XP auf c:\. Danach leite man zunächst den virtuellen Speicher von Windows auf die oben eingerichtete Partition d:\ um. Ferner sollte man die Möglichkeit einschalten, die Erweiterungen aller Dateien zu sehen (Explorer). Kosmetische Änderungen bei Windows XP sind je nach Bedarf vorzunehmen.

4. Mit einem **anderen** Rechner entweder **diese** oder **jene** Seite besuchen, und den Anweisungen Folge leisten.

Es empfiehlt sich wegen Wurmern wie Blaster (aka Lovsan) nicht, vor **Beenden** der Netzwerkdienste online zu gehen, es sei denn, der Rechner ist mit einem Hardwarerouter verbunden.

Alternativ kann in diesem Stadium auch temporär eine PersonalFireWall von CD installiert werden (siehe Punkt 12), oder, bei Windows XP, die integrierte Firewall aktiviert werden.

5. Aktivieren der Onlineverbindung.
6. ActiveX, active Scripting und JScript in den Sicherheitseinstellungen der Internetzone des IE deaktivieren. windowsupdate.microsoft.com zu den vertrauenswürdigen Seiten hinzufügen. Diese Zone auf „mittel“ stellen. Anschließend sämtliche verfügbaren Security-Fixes und den neuesten Service-Pack installieren (Windows Update im Startmenü).

7. Installation eines vernünftigen Virencanners. Zu empfehlen: Kaspersky Antivirus (KAV), den man **hier** (€) erhält. Eine in der Erkennungsleistung zwar schwächere, jedoch durchaus brauchbare Alternative ist der Freeware-Scanner **AntiVir**. Nach der Installation bitte den Guard aktivieren. Täglich updaten. Man beachte die automatische Systemwiederherstellung: Würmer, Viren und Trojaner, die den Rechner infizieren, werden nach dem Löschen automatisch in das betreffende Verzeichnis kopiert und sorgen somit für einen immer wiederkehrenden Alarm des Wächters. Zum endgültigen Löschen muß die Systemwiederherstellung zumindest temporär **außer Kraft** gesetzt werden!

8. Installation eines Spyware-Scanners, wie z. B. **Spybot** oder **AdAware**. Beide sind frei erhältlich. Oft updaten!
9. Falls der Rechner auch oder gar ausschließlich über einen ISDN- oder Modem-Zugang zum Internet verfügt, sollte man einen Dialer-Warner und -Scanner installieren. Eine gute Wahl ist hierbei die Freeware **A² Personal**.
10. Installation eines vernünftigen Browsers. Zu empfehlen: **Opera** oder **Firefox**. Den Internet-Explorer sollte man in Zukunft nur noch für die unerläßlichen Windowsupdates einsetzen.
11. Installation eines vernünftigen Mailclients. Es gibt viele, aber zu empfehlen sind sicher **TheBat! (€)**, **Thunderbird** oder **Pegasus**. In jedem Fall sollte man einkommende HTML-Mails als reinen Text anzeigen lassen. Verschicken sollte man ebenfalls reinen Text, gegebenenfalls mit Anhang.
12. Optional, und nur in Einzelfällen empfehlenswert: Installation einer Personal-Firewall, wie z. B. **Sygate Personal** oder **Kerio**. Beide Programme sind für Privatnutzer kostenlos.
13. Falls etwas nicht so funktioniert, wie es sollte: die benötigten, in Punkt 2 aber möglicherweise irrtümlich deaktivierten Dienste wieder aktivieren.
14. Useraccount(s) mit eingeschränkten Rechten anlegen. Vertrauliche Dateien verschlüsseln, falls möglich (nicht bei Windows XP Home).
15. Nach dem Installieren aller notwendigen Software empfiehlt es sich, den gegenwärtigen Installationsstand mithilfe einer Image-Software zu sichern. Die prominentesten Beispiele hierfür sind **Norton Ghost (€)** und **TrueImage (€)**, aber auch hier sind kostenlose Alternativen vorhanden, wie z. B. **Partition Saving**. Diese Sicherung erlaubt eine bequeme Wiederherstellung der sauberen Installation.

In Zukunft: als User und *nicht* als Administrator anmelden. Regelmäßige Updates nicht vergessen oder automatischen Hinweis aktivieren. Regelmäßige Backups eines **sauberen** Systems erleichtern die Wiederherstellung eines aktuell gepatchten Systems ungem.

Dateianhänge nicht öffnen, ohne sie zu scannen (auch von Bekannten, da die Absenderadresse leicht gefälscht werden kann). Auch Updates sollte man so behandeln, falls der Guard nicht aktiv ist. Software sollte man grundsätzlich nur von vertrauenswürdigen

Quellen installieren, also von deren Ursprungsseiten oder von Seiten, die von vielen nachweislich erfolgreich benutzt wurden. Von „Geheimtips“ wie Kaazaa und dergleichen ist absolut abzuraten.