

Wie vermeide ich Zwangsupgrade zu Windows 10?

Nach Studium dieser Angelegenheit in den vergangenen Monaten ist mein Rat wie folgt:

- Deinstalliere alle unten angeführte Aufdatierungen = Updates (sofern vorhanden).
- Aufdatiere dein Windows 7 oder 8 nur manuell und vermeide dabei verdächtige Updates.
- Installiere GWX Control Panel und lasse es autostarten, sodass dein Computer bei jedem Start geprüft wird. Prüfe auch ab und zu, ob diese Anwendung selbst ein Update hat. Entdeckst du zum Beispiel eines Tages, dass bei "Are Windows Update OS Upgrades enabled" ein "yes" steht, kannst du dies sofort bereinigen. Siehe hier.
- Immunisiere dein System gegen Telemetrie (Datenfernübertragung) mit Spybot Anti-Beacon. Siehe hier.
- **VORSICHT!** KB3161608 vom 20. Juni 2016 scheint mir so weit verdächtig. Siehe diese Beschreibung <https://support.microsoft.com/en-us/kb/3161608>. **Betreffend spätere Rollups, siehe unten.**

Nachtrag 24.6.2016: Ein neues Problem!

Neuerdings wird man beim Installieren eines Updates echt genervt, weil es eine Ewigkeit dauert, bis der Computer (jedenfalls in Windows 7) die Liste der bereits installierten Updates durchsucht hat. Erst nach diesem Durchsuchen kann die Installation fortgesetzt werden. Siehe hierzu die folgenden Artikel:

[KB3161664 ersetzt KB3153199](#)

[Windows 7 update scans taking forever?](#)

[Microsoft releases KB 3161647, KB 3161608 to fix slow Windows 7 update scans](#)

Dies ist nicht nur ein Problem, wenn man direkt aus dem Internet aufdatiert, was ich aber nicht tue, sondern erweist sich nunmehr (seit April oder Mai 2016) auch als ein Problem beim manuellen Aufdatieren. Auch hier wird das Update im Schneckentempo installiert, wenn man ohne Neustart (außer am Ende) nach einander mehrere auf einmal installieren will. Es betrifft dann nur das zweite und weitere Updates, aber nicht das erste in der Reihe. Deshalb gibt es ein Workaround: Wenn man nach *jedem* Update den Computer neu startet, geht es gut, also: jedes Mal nur einzeln installieren. Gemäß der Empfehlung im erstgenannten Artikel habe ich KB3135445 von Februar 2016 installiert (aber keine weitere der in jenen Artikeln genannten Updates). Danach ging es wieder ohne diese lästige Verzögerung. Ich zögere aber, immer wieder neue Aufdatierungen von Windows Update zu installieren, weil ich nicht weiß, wie sich das auf die Immunität gegen Windows 10 auswirkt. Sollte das Problem später wieder auftreten, werde ich wohl auch eine spätere Aufdatierung von Windows Update installieren müssen.

Weil frühere Updates dieses Problem nicht verursachen, wird das wohl bedeuten, dass Microsoft nun etwas im Format der Updates geändert hat, wodurch eine neuere Version von Windows Update verlangt wird.

Nachtrag 16.7.2016

In der Liste unten mit Updates, die du besser nicht haben solltest, habe ich nur einige wenige weitere aus einer anderen Quelle in rotbrauner Farbe hinzugefügt. Wahrscheinlich nicht sehr wichtig, beurteile nach deinem Bauchgefühl ...

Nachtrag 23.7.2016

VORSICHT! Der "update rollup" KB3172605 vom 21.7.2016 für Windows 7 ist könnte eigentlich eine „nette“ Weise, um alle die Updates hineinzuschleichen, die du versucht hast, von deinem Computer fernzuhalten ... Aber: **ENTWARNUNG?** Angeblich soll das Rollup sicher sein und eine ganze Reihe von einzelnen Dateien beinhalten und keine vergangenen Updates. Eine Auflistung des Inhalts ist hier zu haben: <http://download.microsoft.com/download/7/7/5/775C786B-D9C1-41DF-AAFD-155FF28EA0A1/3172605.csv>. Vgl. <https://support.microsoft.com/en-us/kb/3172605>. **Nein! Keine Entwarnung, siehe unten.**

Nachtrag 24.7.2016

Ein paar Verbesserungen in der Liste über unerwünschte Updates sowie Ergänzungen zur Liste über Einträge in der *hosts* Datei, am Ende.

Nachtrag 10.8.2016

Unter den Updates vom August 2016 kommt mir KB3167679 etwas merkwürdig vor, da es Authentifizierungsmethoden betrifft und sich erst nicht mit Firefox herunterladen ließ. Es ging aber mit dem Internet Explorer (den ich sonst nie verwende) – und am nächsten Tag doch mit Firefox ... Jedoch: Um welche Authentifizierung handelt es sich hier? Dies mag schon überverdachtsam sein, jedoch hat Microsoft schon früher mit Tricks versucht, um das Leben mit Windows 7 schwer zu machen, zum Beispiel mit dem berüchtigten Update KB3133977. Siehe hierzu: [“Microsoft Windows Update KB3133977 Is Deadly”](#) und [After installing Microsoft Update KB3133977 for Windows 7, some users may encounter a “Secure Boot Violation”](#). Nach dem “red screen alarm” kam die freche Aufforderung, zu Windows 10 zu wechseln, „um das Problem zu lösen“ ...

Nachtrag 18.8.2016

Leider muss ich die ENTWARNUNG? oben vom 23.7.16 zurücknehmen! Das neue Vorgehen von Microsoft, monatlich sogenannte „Rollups“ herauszugeben, ist doch der Sicherheit deines Windows 7 oder 8 gar nicht so zuträglich, wie man es scheinen lassen will. Rollup KB3172605 von Juli 2016 enthält (wie inzwischen herausgefunden) doch Kleinigkeiten, die mit Telemetrie zu tun haben. Das Gleiche kann dann sehr wohl dem Rollup KB3179573 von August 2016 gelten. Vgl. den Artikel [Win7 and 8.1 to get cumulative updates – you no longer control your Win7 or 8.1 machine](#). Die neue Taktik scheint zu sein, Windows 7 und 8 in Hinsicht auf Privatsphäre und Spionage dem Windows 10 immer näher zu bringen! *Deshalb werde ich vorläufig keine solche Rollups installieren ...* [Fortgesetzt 20.8.] Dieser Artikel erklärt die Pläne: [Further simplifying servicing models for Windows 7 and Windows 8.1](#), worin die Aussage: „Mit der Zeit wird Windows proaktiv auch Updates zum monatlichen Rollup hinzufügen, die bereits in der Vergangenheit herausgegeben wurden. Unser Ziel ist schließlich, *alle Updates mit einzubringen, die wir in der Vergangenheit* seit der letzten Grundlinie *herausgaben*, sodass der monatliche Rollup völlig kumulativ wird und Sie nur den letzten einzelnen Rollup installieren müssen, um auf dem aktuellen Stand zu sein. Wir empfehlen, zu dem Model des monatlichen Rollups überzugehen, um Zuverlässigkeit und Qualität der Aufdatierung aller Versionen von Windows zu verbessern“ (meine Hervorhebung). **Das sagt so ziemlich alles ...**

Nachtrag 29.-30.9.2016

KB3184122 verlangt scheinbar ein Update KB3185319 für Internet Explorer Version 11, wenn du ihn hast, aber nicht für andere Versionen. Es ist aber ratsam, keine höhere Version als 9 zu haben und ihn nur ausnahmsweise zu gebrauchen. Aus oben erwähnten Gründen habe ich September rollup KB 3185278 ausgelassen. Update KB3184143 entfernt Get Windows 10 App und andere Software, die mit der am 29. Juli 2016 abgelaufenen Gratisaufdatierung auf Windows 10 verbunden sind – die du ohnehin nicht haben solltest... und es kann nach der Installation von diesem Update passieren, dass der Computer nicht mehr startet ...

Nachtrag 12.10.2016

Es ist geschehen! Microsoft hat nun einen bösen Schritt unternommen, um unabhängiges Aufdatieren von Windows 7 und 8 zu stoppen! Mit den Updates im Oktober haben sie endgültig ein neues Aufdatierungsverfahren eingeführt, siehe [Simplifying updates for Windows 7 and 8.1](#), [Further simplifying servicing models for Windows 7 and Windows 8.1](#) und [More on Windows 7 and Windows 8.1 servicing changes](#). „Simplifying“ („vereinfachend“) bedeutet hier *verkomplizierend* für Anwender, die selbst wählen wollen, welches Update er/sie vertraut und installieren will. Die neuen in Wahrheit *unbequemen* „Bequemlichkeits“-Rollups lassen uns keine Wahl, außer zwischen Sicherheitsaufdatierung und Gesamtaufdatierung. Das Letztere beinhaltet auch Updates, die nicht speziell der Sicherheit dienen. Aber beide werden zweifellos auch Updates beinhalten, die manche von uns nicht sehr vertrauen, da sie mit Telemetrie oder anderen Funktionen zum Spionieren zu tun haben könnten, und sie können auch mit etwas älteren Updates „aufrollen“, die wir bereits weggewählt und deshalb nicht installiert haben. Das wird die offensichtliche Motivation für diese „Vereinfachung“ sein. Es gibt jedoch die Hoffnung, dass man Wege findet, um das herumzugehen und doch eine Wahl für die Privatsphäre zu wahren. Ich werde verfolgen, was darüber im Netz erscheint. In der Zwischenzeit werde ich nicht mehr aufdatieren und mich ein wenig mehr mit Linux Mint befassen ...

Nachtrag 13.10.2016

Man lese: [Say good-bye to individual patches on Windows 7 and 8](#) und [Microsoft is changing the way it patches Windows 7 and 8.1. Here's what we know -- and what to do to keep having Windows your way](#). Es ist die Rede von einer "Patchocalypse"...

Microsoft behauptet, dass der Zirkus eingerichtet wurde, sodass man das System mithilfe von *unfreiwilligem* "Feedback" verbessern könne, Aber es ist ja völlig klar, dass dies ein weiterer Schritt in Richtung Totalüberwachung vom Internet und ihren Anwendern ist.

Hiermit ist vieles von dem, was unten steht, bereits überholt ...

Vermeide KB3170735 und alle anderen Updates zu Windows Journal. Windows Journal sollte nicht verwendet werden, da das Programm ein massives Sicherheitsloch in Windows ist.

Bisher hat man immer für die neue Version bezahlen müssen, und nun sollen sie alle gratis bekommen? Diese „Großzügigkeit“ ist ja schon verdächtig ... Ist es Windows 10 oder Windows NSA?

Deshalb werden sehr viele Computer ab dem 29. Juli, die mit Windows 7 oder 8 liefen, ungefragt zu Windows 10 aufgradiert worden sein. Wenn nämlich das folgende Update installiert ist (oder war), das seit Anfang Juli 2015 angeboten und bei vielen Anwendern automatisch installiert (eingeschmuggelt) wurde: KB3035583, zunächst als optional erklärt, später als „wichtig“. Dann wird wahrscheinlich am 29.7.2015 oder ziemlich bald danach dein Windows automatisch zu Windows 10 aufgradiert sein. Wolltest du das nicht, hättest du rechtzeitig dieses Update entfernen müssen (und nun wird es wohl zu spät sein).

Unten sind Updates aufgeführt, die du nicht haben solltest, wenn du Windows 10 nicht haben willst und auch *keine zusätzlichen Spionagefunktionen in Windows 7 oder 8*, die denen entsprechen, die Windows 10 hat. Die Liste ist aus verschiedenen Quellen zusammengestellt.

Updates, die du nicht haben solltest (Stand September 2016)

Allgemeine Updates (für Windows 7, oder sowohl für Windows 7 wie auch 8)

(Beschreibungen sind in Englisch belassen)

KB971033 Update that describes Windows Activation Technologies. License validation check

KB2505438 Tracks performance, breaks some fonts

KB2506928 Problem with links in Outlook, may spy

KB2545698 Fixes some blurry fonts in IE9, may spy

KB2574819 For Remote Desktop Services – unless needed!

KB2592687 For Remote Desktop Services – unless needed!

KB2660075 Problem with Samoa time zone, may spy

KB2670838 Updates platform for Windows 7 SP1 (seems suspicious). Breaks AERO functionality and can blur some fonts

KB2726535 Adds South Sudan to list of countries, may spy

KB2830477 For Remote Desktop Services – unless needed!

KB2876229 Unless you use Skype (Skype spies, too!)

KB2882822 Update for adding itracerelogger interface support

KB2902907 For MS Security Essentials, that should not be used anyway!

KB2922324 Telemetry

KB2923545 Update for the Remote Desktop Protocol

KB2938066 Probably update to Update Client

KB2952664 Compatibility update for upgrading Windows 7. Nags about Windows 10

KB2966583 Improves the Update Readiness Tool so that it can be executed *without user interaction*

KB2970228 New currency symbol for Russian ruble

KB2977759 Compatibility update for Windows 7 RTM = W10 Diagnostics Compatibility telemetry

KB2990214 Aids in transitioning from Windows 7 to 10

KB2996978 No description found

KB2994023 RDP 8.1 client for Windows 7 disconnects, may spy

KB2999116 Windows 10 universal C Runtime in Windows 7

KB3008273 Update rollup for Windows 8 and for an issue with Windows 7

KB3012973 Upgrade to Windows 10 Pro

KB3014460 Windows 10 Insider preview install

KB3015249 Adds telemetry points to consent.exe

KB3021917 Update to Windows 7 SP1 that determines if performance issues may be encountered when 10 is installed.

Sends telemetry back to Microsoft

KB3022345 Telemetry
 KB3035583 Creates the annoying “Get Windows 10 App” notification in your taskbar
 KB3042058 Contains Winlogon spying
 KB3046480 For a .NET Framework issue when upgrading Windows 7 or 8
 KB3050265 Update to the Windows Update client for Windows 7. Also states that there are “general improvements that are made to support upgrades to later version of Windows.” WU service updated to accept upgrade to W10 + other fixes
 KB3065987 Makes “improvements” to Windows Update Client for Windows 7, pushing of Windows 10
 KB3065987-v2 Cf. above
 KB3065988-v2 For Windows Update Client
 KB3068707 Telemetry
 KB3068708 Telemetry
 KB3074677 Windows 10 Upgrade preparation
 KB3075249 Adds telemetry points to consent.exe
 KB3075851 Makes “improvements” to Windows Update Client for Windows 7, pushing of Windows 10
 KB3075853 For Windows Update Client
 KB3079821 Enables Windows 7 to activate Windows 10
 KB3080079 Supports a TLS function that may not be needed
 KB3080149 Telemetry
 KB3081437 Windows 10 Upgrade preparation
 KB3081954 Prepares Upgrade and adds telemetry
 KB3083324 New update client (may ease upgrade to Windows 10)
 KB3083710 New update client (may ease upgrade to Windows 10)
 KB3086255 Update for the graphics component in windows (breaks safedisc)
 KB3088195 Has a key logger on the Kernel Level
 KB3090045 Windows 10 Upgrade Update for Windows 7/8
 KB3093983 Contains IE spying
 KB3094176 Aids upgrade to Windows 10 (Siehe [unten](#))
 KB3095649 Actually for Windows 8 and not needed for Windows 7
 KB3102810 Fixes issue with Windows Update, but also preparers for Windows 10 in Windows 7
 KB3123862 Updated capabilities to upgrade windows 7 and windows 8.1
 KB3112343 Enables additional upgrade scenarios from Windows 7 to Windows 10
KB3125574 Telemetry for Windows 7
 KB3135445 For Windows Update, probably preparing for upgrade
 KB3138612 A new version of KB3135445
 KB3139929 Security update for internet explorer and upgrade to Windows 10
KB3146449 Windows 10 upgrade
 KB3150513 Compatibility update for windows
 KB3170735 Windows Journal update
KB3172605 Update rollup
KB3173040 Windows 10 Upgrade notice
KB3179573 Update rollup
KB3181988 Fixes an error that is caused by rollup KB3125574 that should, however, not be installed
KB3184143 removes the Get Windows 10 app and other related software
KB3185278 Update rollup

Updates für Windows 8:
 KB2976978 Compatibility update, , prepares for Windows 10
 KB3008273 Update rollup for Windows 8 and for an issue with Windows 7
 KB3015249 Adds telemetry points to consent.exe
 KB3035583 Creates the annoying “Get Windows 10 App” notification in your taskbar
 KB3044374 Aids in transitioning to 10
 KB3046480 For a .NET Framework issue when upgrading Windows 7 or 8
 KB3050267 Update to the Windows Update client for Windows 8.1. Also states that there are “general improvements” that are made to support upgrades to Windows 10
 KB3058168 Activates Windows 10 from Windows 8 or Windows 8.1
 KB3064683 For OOB modifications to reserve Windows 10 in Windows 8.1
 KB3065988 For Windows Update Client
 KB3065988-v2 For Windows Update Client
 KB3072318 Windows 10 Upgrade preparation for Windows 8
 KB3075249 Adds telemetry points to consent.exe
 KB3081454 Windows 10 Upgrade preparation
 KB3083325 Telemetry - Windows 10 Upgrade preparation
 KB3083711 Update for Windows Update Client for windows 8.1

KB3090045 Windows 10 Upgrade Update for Windows 7/8
 KB3065988 For Windows Update Client
 KB3112336 Enables additional upgrade scenarios from Windows 8.1 to Windows 10
 KB3102812 Fixes issue with Windows Update, but also preparers for Windows 10 in Windows 8
 KB3135449 For Windows Update, probably preparing for upgrade
 KB3138615 A new version of KB3135449
 KB3146449 Updated internet explorer 11 capabilities to upgrade windows 8.1 and windows 7
[KB3172614 Update rollup](#)
[KB3179574 Update rollup](#)
[KB3185279 Update rollup](#)

Über **KB3094176** = Windows Management Framework 5.0 beinhaltet Aufdatierungen von Windows PowerShell: Konfiguration vom *erwünschten Zustand*, *Fremdkontrolle* und *Kontrollinstrumentarium*. *Wie wenn dafür gemacht, um über den Computer die Kontrolle zu übernehmen!* Ähnlich könnte "Application Compatibility Toolkit 5.6" (Toolkit-Sammlung für Anwendungscompatibilität) möglicherweise darüber die Kontrolle übernehmen wollen, welche Anwendung du haben darfst oder nicht haben sollst. Installiere dieses Toolkit nicht! Es wurde bereits berichtet, dass Microsoft in Windows 10 bestimmte Anwendungen blockieren oder deinstallieren möchte, und man will sicher aus Windows 7 oder 8 eventuelle Vorsichtsmaßnahmen gegen Zwangsaufgradierung aus dem Weg räumen.

Über **KB3050267**: Bereitet vor für Windows 10 Upgrade, aber fügt auch eine Option in GPEDIT ein, womit Windows 10 Upgrade blockiert werden kann. Deshalb mag man dieses Update gleichwohl erst installieren und dann wieder entfernen ...

Es wird empfohlen, den Internet Explorer nicht zu verwenden, aber wenn es sein muss, dann IE9 und keine höhere Version. Wenn man IE10 und IE11 installiert, installiert man automatisch auch KB2670838, das unerwünscht ist. Um das zu verhindern, installiert man besser [IE10 BlockerToolkit](#) und [IE11 BlockerToolkit](#).

Und wie entfernt man ein Update manuell? Gehe zur *Systemsteuerung* und klicke auf *Programme* und dann unter *Programme und Funktionen* auf *Installierte Updates anzeigen*. Man kann da ein Update KBxxxxxxx ins Suchfeld oben rechts eintragen. Ist es installiert, wird es angezeigt. Klicke in dem Fall rechts auf die Datei und dann auf *Deinstallieren*. Starte darauf den Computer neu.

Bringt nunmehr Microsoft zusätzliche Schleichupdates, die nicht der Sicherheit dienen, sondern eher der Überwachung in Windows 7 und 8, neben der Win10-Vorbereitung? Das ist eher wahrscheinlich und wäre nicht erstaunlich ... *Die Tatsache, dass Windows 10 nach dem 31 Juli 2016 nicht mehr gratis sein wird, hat aus guten Gründen vielen zur Spekulation geführt, dass dann Windows 7 und Windows 8 bereits so weit aufdatiert sein werden, dass sie viele neue Spionagefunktionen haben werden, ähnlich wie in Windows 10.*

Aufdatierungen sind da, um funktionelle Probleme zu beseitigen und „Schlupflöcher“ in der Software zu stopfen. Aber theoretisch könnte Microsoft mit einem „Update“ ein Schlupfloch *herstellen*, um etwas hineinschleichen zu lassen.

Installiere nie ein Update, das mit Telemetrie (Datenfernübertragung) zu tun hat! Es wird heute besser sein, Windows 7 und 8 nicht mehr sofort aufzudatieren, und jedenfalls nicht automatisch! Nicht bevor man im Internet die Erfahrungen Anderer mit dem aktuellen Update abgeklärt hat. Eine dafür hilfreiche Webseite ist <http://forums.mydigitallife.info/printthread.php?t=64561&pp=10&page=1> (registriere dich dort, um zu allen Informationen Zugang zu haben).

Nach einem versehentlichen Upgrade zu Windows 10 kann man zur früheren Version „zurückrollen“. Das geht aber nur innerhalb von 30 Tagen, und nur wenn das frühere System nicht gelöscht ist – und wie viele Spionagefunktionen von Windows 10 bleiben dann doch noch?

- Um das zu tun, gehe zum Startmenü von Windows 10 und wähle „Einstellungen“.
- Wähle „Update und Sicherheit“.
- Klicke „Wiederherstellung“ und wähle „Zu Windows 7 [bzw. 8] zurückkehren“. Klicke „Los geht's“ bzw. „Zu früherem Build zurückkehren“.

[GWX Control Panel](#) ist eine Anwendung, welche die Datei GWX.exe sucht und für Löschen meldet, und den Computer so einstellt, dass das Herunterladen von Dateien verhindert wird, welche die Installation von Windows 10 vorbereiten. GWX.exe ist eine sehr große Installationsdatei für Windows 10.

Ich habe den Control Panel im Autostart, sodass ich nach jedem Start meines Windows 7 sofort sehen kann, ob im System etwas in diesem Sinne geändert wurde, oder das System immer noch gegen Windows 10 immun ist. Ich lasse das Programm im „monitoring mode“ (Überwachungsmodus) laufen, sodass es alarmiert, sollte während dem Betrieb des Systems etwas diesbezüglich geändert werden. Die unerwünschte Datei GWX.exe kann auch mit dem [GWX Removal Tool](#) entfernt werden.

Windows 7 und höher haben (in C:\Windows\system32\SnippingTool.exe) auch ein „Snipping Tool“, das Bildschirmfotos machen kann. Dieses Tool ist (wenn fernaktiviert) auch brauchbar für Spionagezwecke. Es kann abgestellt werden:

- Schreibe *gpedit.msc* im Suchfeld des Startmenüs (nur in Windows Professional, Ultimate oder Enterprise möglich) und öffne diese.
- Gehe zu den Richtlinien *Computerkonfiguration* [oder *Benutzerkonfiguration*] > *Administrative Vorlagen* > *Windows-Komponenten* > *Tablet PC* > *Zubehör*.
- Hebe die Richtlinien zum Blockieren des Snipping Tools („*Ausführen des Snipping Tools nicht zulassen*“) auf und starte Windows neu. Teste dann, ob das Programm nun startet.

Windows 10 enthält eine hübsche Auswahl an Spion- und Kontrollfunktionen, siehe: [Windows 10 vernichtet deine Privatsphäre](#). Die Kontrollfunktionen können außerdem in deinen Computer eingreifen, um darin zu ändern, was dem Großen Bruder nicht gefällt. Möglicherweise ist auch ein sogenannter Killswitch (Todesschalter) eingebaut, wodurch man von Microsoft (oder von irgendwoher) deinen Computer (oder bestimmte Funktionen darin) lahmlegen kann.

Zu den vordersten Überwachungsfunktionen gehören (und das sind sicher nicht alle ...):

- Information über dein Gerät und seine Anwendungen.
- Überwachung deiner Internetaktivitäten.
- Information über Spracheingabefunktionen wie Sprache-zu-Text sammeln.
- Information über eine geöffnete Datei – über die Datei selbst, über die Anwendung, womit du sie öffnest und darüber, wie lange das dauert.
- Information darüber, wenn du einen Text einfügst, wobei die Schriftzeichen aufgenommen werden können (key logging).

Windows 10 wird zwangsmäßig aufdatiert. Du kannst das automatische Updaten (fast) nicht verhindern, also [die automatische Aufdatierung nicht abstellen](#) und [Windows 10: Automatische Updates verursachen schon Probleme](#). Es gibt allerdings (noch) gewisse Möglichkeiten, das automatische Aufdatieren mit Tricks zu verhindern – bis Microsoft dem wohl ein Ende macht. Dadurch kann Microsoft in deinen Computer alles hineinschmuggeln, was man dort haben will. Die schöne Ausrede ist natürlich, dass dies nur für dein Bestes sei. Schön wär's, wenn es nur für deine Sicherheit wäre, aber es wird in manchen Fällen viel mehr für die „sichere Funktion“ des Überwachungssystems sein, nämlich noch mehr ausgereifte Spion- und Kontrollfunktionen.

Siehe [Windows 10 und Privatsphäre](#), eine umfassende Übersicht darüber, was du in Windows 10 tun musst, um zumindest einiges von seiner Schnüffelwut einzudämmen. [DoNotSpy10](#) ist ein Programmchen, das dies für dich tun kann, aber Vorsicht: Es mag Adware installieren, wenn du das nicht wegklickst. Ein anderes Programm, das interessant zu sein scheint, ist [Destroy Windows 10 Spying](#), (mit wenig Beschreibung auf der [Seite des Verfassers](#)). Es fügt in deiner hosts-Datei viele Internetadressen hinzu, die blockiert werden sollen, weil sie für Berichte an Microsoft verwendet werden, direkt oder indirekt. Diese Internetadressen werden auch im Link angegeben und du kannst sie auch selbst [in deine hosts-Datei eintragen](#), wenn du weißt, wie. Das Tool tut wahrscheinlich noch mehr und wird nicht nur für Windows 10 empfohlen, sondern auch für Windows 7 und 8, weil auch darin neue Updates sehr wahrscheinlich Spionagefunktionen eintragen. Microsoft warnt gegen solche Tools, aber wer ist naiv genug, um das ernst zu nehmen? O&O Software ist eine kleine Firma, die von Scientology betrieben wird, aber gleichwohl einige gute Softwareprodukte hat. Sie haben ein kostenloses Antispy-tool herausgegeben, das Windows 10 zum Schweigen bringen soll: [O&OShutUp10](#). Noch einige Tools zum Zähmen von Windows 10 sind [Disable Windows 10 Tracking](#) und [Win10Privacy](#) (kann angeblich auch Zwangsaufdatierung deaktivieren). Aber man

kann wohl davon ausgehen, dass kein solches Tool 100%-ig schützt: [Windows 10 ruft immer noch nach Hause, unabhängig von Einstellungen zum Bewahren der Privatsphäre](#) und [Auch wenn man es ihm sagt, kann Windows 10 nicht aufhören, Microsoft zu informieren](#).

Einige solche Tools werden in [diesem Video](#) verglichen.

Ein neueres und scheinbar besseres Tool für Windows 7, 8 und 10 für den gleichen Zweck ist [Spybot Anti-Beacon](#) (Forum [hier](#)). Ich habe es erfolgreich verwendet, aber es ist ratsam, vorher einen Wiederherstellungspunkt zu setzen.

Es gibt allerdings einige Tricks, um das automatische Aufdatieren von Windows 10 zu stoppen, auf die man gekommen ist: [How to Prevent Windows 10 From Automatically Downloading Updates](#), [A workaround to Turn Off Windows Update in Windows 10](#), [Disable/Turn Off Automatic Updates In Windows 10, Here's How](#) und [Windows 10 Hack: 3 Ways To Stop Forced Updates](#). Es bleibt nun übrig, eine Quelle für das Herunterladen der Updates für manuelle Installation zu finden. Da ich Windows 10 nicht habe und nicht haben will, habe ich das (noch) nicht untersucht. Vgl. [How to Check for and Install Windows Updates in Windows 10](#). (Eine Möglichkeit könnte [Portable Update](#) sein.)

Es wäre keineswegs erstaunlich, wenn Microsoft gelegentlich ein Update einschleichen lässt, das diese Einstellungen rückgängig macht oder zu einem neuen Spionageweg „aufdatiert“. Deshalb: Überprüfe sie regelmäßig!

Dass Big Brother allen Windows 10 unterjubeln will, sodass sie besser überwacht- und manipulierbar sind, ist so offensichtlich, dass man eine ordentliche Portion von Naivität und Leichtgläubigkeit braucht, um das nicht erkennen zu wollen. Dass Microsoft nun auch durch gezielte Werbung Geld machen möchte, wozu sie alles über dich wissen will, kommt wohl eher an die 2. Stelle.

Kein Wunder, dass immer mehr Menschen sich mit Linux befassen, um früher oder später darauf umzusteigen. Auch kein Wunder, dass nun auch Microsoft Linux unter seinen Fittichen haben will und deshalb bereits seit 2003 heimlich daran arbeitet (siehe [hier](#), [hier](#) und [hier](#)). Man will natürlich ein Linux im gleichen Sinne haben, wie Windows 10, ganz im Dienste des Großen Bruders. Aber versucht Microsoft nun, mit Spionageabsichten auch [Linux-Systeme zu infiltrieren](#)? Möge kein Linux-Anwender je ein Microsoft-„Tool“ installieren!

Alles nur „Konspirationstheorie“? Oder Konspirationsfakten? Warte ab, du wirst es mit der Zeit selbst erleben ...

Nun wär es ja keineswegs erstaunlich, wenn Microsoft bald ein neues Update in deinen Computer einschleichen lassen will, das ungefähr dasselbe tut, wie KB3035583. Um sich dagegen so gut es geht abzusichern, empfehle ich, das automatische Aufdatieren abzustellen und nur manuell aufzudatieren. Natürlich auch, um so viele Spionagefunktionen wie möglich von deinem System fernzuhalten.

[Schütze deinen Computer gegen unerwünschte Updates](#). *Installiere nie ein Update, das mit Telemetrie zu tun hat!*

WARNUNG!!! Zu allem Übel mit Microsofts neuem Spionagesystem ist nun auch ein Erpresservirus im Internet los. **Öffne nie eine E-Mail, die dir das Herunterladen einer Installationsdatei für Windows 10 anbietet!** Siehe [Jenes Aufdatierungsangebot für Windows 10 kann ein maskiertes Erpressungsvirus sein](#). Ein Virus, das den Zugang zu deinen Dateien blockiert, wenn du nicht erst einen größeren Betrag bezahlst, um sie freizubekommen. Siehe auch [CTB-Locker Erpresservirus wird durch gefälschte Windows 10 Update E-Mails verbreitet](#).

Kill Windows 10 (permanently)

Dieses interessante Tool wird [hier](#) gefunden und beschrieben. Neben einigen anderen Dingen entfernt es auch viele unerwünschte Updates aus Windows 7 und 8. Lade auch eine Readme-Datei [hier](#) herunter. Eine cmd-Datei ist [hier](#) zu haben. Bevor du sie herunterlädst, solltest du die Markierung “Download with Secured Download manager” entfernen. Ein alternativer Link ist [hier](#). **Vorschlag: Setze einen Wiederherstellungspunkt, bevor du dieses Programm laufen lässt.**

Ich habe dieses Tool ohne Probleme laufen lassen. Zuerst überprüfte ich, dass kein hier erwähntes Update installiert ist. Wenn KILLWindows10.cmd einmal hängte, war es vermutlich, weil es versuchte, ein bereits deinstalliertes Update zu deinstallieren. Nach einem Neustart lief alles durch. Es versteckt auch unerwünschte Updates vor Windows Updates und es deaktiviert unerwünschte "scheduled tasks" (geplante Aufgaben).

Zusätzliche Information: [New Intel CPUs Have NSA Exploitable Secret Hidden Backdoor](#): Neue Intel-Prozessoren haben eine versteckte Hintertür, durch die Hacker oder die NSA deinen Computer fernsteuern können, auch wenn er ausgeschaltet ist.

Wie du deinen Computer gegen Installation vor unerwünschten Aufdatierungen schüttest.

Semi-manuelle Aufdatierung

Zuerst:

1. Klicke das Startmenü und schreibe „Dienste“ in das Suchfeld.
2. Es erscheint eine Liste der Dienste. Gehe darin zu „Windows update“ hinunter, klicke rechts und gehe zu „Eigenschaften“. Wenn da etwas anderes steht, ändere zu „Manuell“ und klicke „OK“. Klick dann wieder rechts und klicke „Start“.

Dann:

3. Systemsteuerung > Windows Update > Einstellung ändern. Kommt man nicht direkt zu Windows Update: Erst zu System und Sicherheit gehen und dann findet man es dort.
4. Wähle „Nach Updates suchen, aber Zeitpunkt zum Herunterladen und Installieren manuell festlegen“.
5. Gehe zurück zum vorigen Fenster (<) und wähle „Nach Updates suchen“.
6. Es erscheint eine Liste der verfügbaren Updates. Gehe in dieser Liste die „wichtigen“ und „optionalen“ Updates durch. Entferne die Markierung bei Updates, die du nicht haben willst und klicke rechts auf jene, die du nie installieren willst, um „Update ausblenden“ zu markieren.
7. Markiere nur jene Updates, die du herunterladen und installieren willst. Gehe dann zurück zum vorigen Fenster und klicke „Installieren“. Du kannst erst eine Beschreibung des Updates einsehen.
8. Hattest du vorher eine andere Einstellung unter „Einstellung ändern“, gehe zurück und wähle die frühere Einstellung.

Falls du sonst nie in dieser Weise aufdatierst, sondern nur völlig manuell (siehe unten), gehe zurück zu 1. und 2., stoppe den „Windows Update“-Dienst und ändere die Eigenschaft zu „Deaktiviert“. Auch wenn du manchmal doch wieder in dieser Weise aufdatieren willst, ist es eine gute Idee, den Service in der Zwischenzeit bei „Deaktiviert“ zu halten. Es scheint nämlich möglich zu sein, dass der Service sonst durch einen externen Eingriff gestartet werden kann. Aus dem gleichen Grund ist es auch ratsam, die Update-Einstellung bei „Nie nach Updates suchen (nicht empfohlen)“ zu behalten.

- Finde hier sowohl wichtige wie optionale Updates:
<http://www.microsoft.com/de-de/search/DownloadResults.aspx?q=%22windows%207%22%20updates&sortby=-availabledate>.
 Wähle „Nach alter (aufsteigend)“ bei „Sortieren nach“, wenn da etwas anderes steht.

Und/oder hier:

- <https://technet.microsoft.com/de-de/library/security/ms16-jun> – für Juni 2016. Entsprechend für andere Monate: ms16-may für Mai 2016, usw. Diese Seite erscheint erst am offiziellen Update-Tag, aber bleibt dann lange verfügbar. Sie zeigt nur wichtige Updates.

Ändere nun den Windows Update Dienst zu „Manuell“ und starte ihn, wie oben beschrieben (1. und 2.), weil Updates nur dann installiert werden können, wenn dieser Dienst läuft. Installiere die Updates und ändere die Einstellung des Dienstes zurück zu „Deaktiviert“ und stoppe den Service.

Überprüfe die Aufdatierung

Installiere für diesen Zweck MBSA = [Microsoft Baseline Security Analyzer](#). Starte ihn und führe einen Scan von deinem Computer durch. Das dauert eine ganze Weile und am Ende zeigt er alle „fehlenden“ Updates (auch die, welche du nicht haben willst ...). Aber entdeckst du hier ein Update, das du wirklich übersehen hast, merke es dir um es nachher herunterzuladen. Um es zu finden, schreibe „KBxxxxxxx“ im Suchfeld deines Browser, wo xxxxxxx die Nummer des Updates ist. MBSA funktioniert nur, wenn der Windows Update Dienst läuft.

INSTALLIERE NIE EIN UPDATE, DAS MIT TELEMETRIE (DATENFERNÜBERTRAGUNG) ZU TUN HAT! Und sei skeptisch, wenn von [Customer-Experience](#) bzw. Kundenerfahrung die Rede ist – es könnte eine nicht sehr positive „Erfahrung“ werden ...

In Windows 7/8.1 Pro/Ultimate/Enterprise das Aufgradieren blockieren

1. Öffne *gpedit.msc* mit administrativen Rechten.
2. Gehe zu *Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Windows-Update*.
3. Finde *Turn off the upgrade to the latest version of Windows through Windows Update* (die Richtlinie ist aktuell noch nicht lokalisiert) klicke doppelt daran.
4. Im dadurch geöffneten Fenster *Aktivieren* und dann *OK* klicken.

Dann sollte das Herunterladen des Windows 10 Upgrades als Windows-Update verhindert sein. Die Richtlinie ist aber nur vorhanden, wenn die entsprechenden Vorbereitungsupdates auch installiert sind.

Aufgradieren in Windows 7 Home/8.1 Core Blockieren

Hier gibt es keinen Gruppenrichtlinien-Editor. Man muss den Registrierungs-Editor einsetzen.

1. Starte den Registrierungs-Editor *als Administrator*.
2. Gehe zum folgenden Zweig: *HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate*
3. Unter *WindowsUpdate* den DWORD-Wert (32 Bit) *DisableOSUpgrade* einfügen und auf 1 setzen.

Das blockiert auch das Herunterladen von Windows 10.

Get Windows 10-App loswerden

Sind Updates installiert, die für Windows 10 vorbereiten, erscheint das Symbol links in der Taskleiste.



Um auch dieses loszuwerden, greifen wir zum Registrier-Editor,

1. Starte den Registrier-Editor *als Administrator*.
2. Gehe zu *HKLM\Software\Microsoft\Windows\CurrentVersion\WindowsUpdate\OSUpgrade*
3. Ändere im Schlüssel *OSUpgrade* DWORD-Wert (32 Bit) *ReservationsAllowed* von 2 zu 0.

Sind dort der Schlüssel oder der Wert nicht vorhanden, sind entsprechende Updates nicht installiert.

Ergänzung 1: Es gibt noch einen Weg, um GWX zu blockieren. Gehe in der Registry zu *HKLM\SOFTWARE\Policies\Microsoft\Windows* und füge den Unterschlüssel *Gwx* ein. Schreibe den DWORD-Eintrag *DisableGwx* im Unterschlüssel hinzu und setze den Wert auf 1. Nach Neustart von Windows sollte das Symbol nicht mehr da sein.

Ergänzung 2: Probiere den [folgenden Script](#) aus, um Registereinträge mit reg-Dateien zu erzeugen, die Windows 10 blockieren:

Schließe alle offene Anwendungen.

1. Drücke **Windowstaste + R**.
3. Schreibe **notepad** und klicke **OK**.
4. Kopiere das Folgende in den Notepad:
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\GWX]
"DisableGWX"=dword:00000001

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate]
"DisableOSUpgrade"=dword:00000001
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\OSUpgrade]
```

"AllowOSUpgrade"=dword:00000000
 "ReservationsAllowed"=dword:00000000

5. Speichere dies als **Upgrade.reg**.
6. Starte **Upgrade.reg** mit einem Doppelklick. Bestätige mit Yes bzw. Ja und dann OK.
7. Starte den Computer neu.
8. Prüfe sein Verhalten.

Bevor man Einträge in der Registry durchführt, ist es ratsam, zuerst ein Backup von der Registry anzulegen, sodass man die frühere Version bei Bedarf wieder herstellen kann. Ein gutes Backup-Programm ist [Registry Backup](#).

Die wichtigsten Web-Links, die in deiner hosts-Datei blockiert sein sollten:

a.ads1.msn.com	oca.telemetry.microsoft.com.nsatc.net
a.ads2.msn.com	pre.footprintpredict.com
a-0001.a.msedge.net	preview.msn.com
ad.doubleclick.net	rad.msn.com
adnexus.net	redir.metaservices.microsoft.com
adnxs.com	reports.wes.df.telemetry.microsoft.com
ads.msn.com	services.wes.df.telemetry.microsoft.com
ads1.msads.net	settings-sandbox.data.microsoft.com
ads1.msn.com	sls.update.microsoft.com.akadns.net
az361816.vo.msecnd.net	sqm.df.telemetry.microsoft.com
az512334.vo.msecnd.net	sqm.telemetry.microsoft.com
choice.microsoft.com	sqm.telemetry.microsoft.com.nsatc.net
choice.microsoft.com.nsatc.net	statsfe1.ws.microsoft.com
compaexchange.cloudapp.net	statsfe2.update.microsoft.com.akadns.net
corp.sts.microsoft.com	statsfe2.ws.microsoft.com
corpext.msitadfs.glbdns2.microsoft.com	survey.watson.microsoft.com
cs1.wpc.v0cdn.net	telecommand.telemetry.microsoft.com
df.telemetry.microsoft.com	telecommand.telemetry.microsoft.com.nsatc.net
diagnostics.support.microsoft.com	telemetry.appex.bing.net
fe2.update.microsoft.com.akadns.net	telemetry.appex.bing.net:443
feedback.microsoft-hohm.com	telemetry.microsoft.com
feedback.search.microsoft.com	telemetry.urs.microsoft.com
feedback.windows.com	vortex.data.microsoft.com
i1.services.social.microsoft.com	vortex-sandbox.data.microsoft.com
i1.services.social.microsoft.com.nsatc.net	vortex-win.data.microsoft.com
oca.telemetry.microsoft.com	watson.live.com

[Diese interessante Webseite](#) schlägt auch die folgenden Einträge vor, wobei die mit opencandy besonders schlecht sind:

a.ads2.msads.net	softonic.com
adsmockarc.azurewebsites.net	sourceforge.net
api.opencandy.com	spynet2.microsoft.com
b.ads1.msn.com	spynetalt.microsoft.com
b.ads2.msads.net	sqm.microsoft.com
bi.bisrv.com	tracking.opencandy.com
bingads.microsoft.com	tracking.opencandy.com.s3.amazonaws.com
cdn.opencandy.com	watson.ppe.telemetry.microsoft.com
dl.delivery.mp.microsoft.com	watson.telemetry.microsoft.com
image.online-convert.com/convert-to-ico	watson.telemetry.microsoft.com.nsatc.net
media.opencandy.com	wes.df.telemetry.microsoft.com
offer.alibaba.com	www.bestvistadownloads.com
sb.scorecardresearch.com	www.softonic.com

Softonic ist eine nicht sehr vertrauenswürdige Downloadseite, aber für meinen Eindruck ist hingegen sourceforge in Ordnung. Alibaba ist eine chinesische e-commerce-Seite. Ich würde auch [www.brothersoft.com](#) mitnehmen, die wie softonic einen eigenen Downloader hat, und das ist mir ein bisschen verdächtig.