W10 GPO (1)

Windows 10: Datenschutzeinstellungen für Admins

*von* [*Thomas Joos*](http://www.zdnet.de/autor/thomas-joos/) *am* [*3. Februar 2016*](http://www.zdnet.de/date/2016/02/03/)*, 16:10 Uhr*

**Die Datenschutzeinstellungen von Windows 10 stehen nicht nur bei Privatanwendern in der Kritik. Auch in Unternehmen ist das ein Problem. Admins können allerdings für die Konfiguration von Unternehmens-PCs zahlreiche Möglichkeiten nutzen, um das Sammeln von Daten zu unterbinden.**

Administratoren, die Windows-10-Clients in Unternehmen bereitstellen, sollten sich darüber Gedanken machen, wie der Datenschutz im neuen System optimiert werden kann. Zwar stehen für [Privatanwender Tools zur Verfügung](http://www.zdnet.de/88258284/mehr-datenschutz-fuer-windows-10-xp-antispy-w10privacy-und-co/), die auch in Firmen ihren Dienst verrichten, allerdings ist das in produktiven Umgebungen aus verschiedenen Gründen selten sinnvoll. Windows 10 bietet auch interne Einstellungen, die Anwender und Administratoren selbst anpassen können. Außerdem gibt es Vorlagen für Gruppenrichtlinien und Möglichkeiten, bestimmte [Microsoft](http://www.zdnet.de/unternehmen/microsoft/)-Server in der Firewall des Unternehmens zu blockieren.

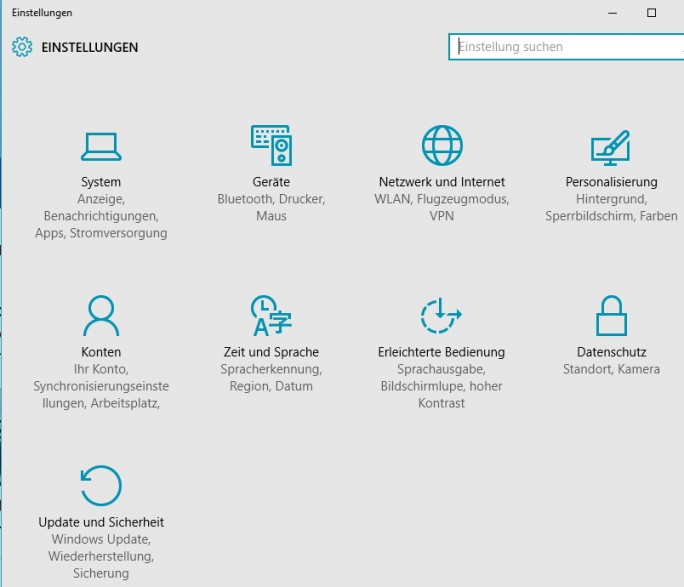
Administratoren, die Windows 10 für den Unternehmenseinsatz vorbereiten, sollten sich darüber hinaus folgende Artikel in der Microsoft-TechNet ansehen:

[Konfiguration von Telemetriedaten und andere Einstellungen in Ihrem Unternehmen](https://technet.microsoft.com/library/mt577208.aspx)

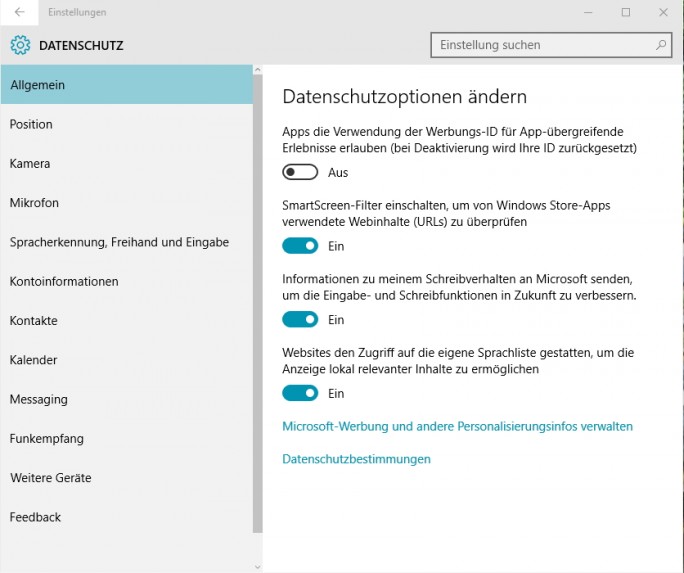
[Festlegen von Voreinstellungen für Windows 10-Dienste](http://windows.microsoft.com/de-de/windows-10/services-setting-preferences)

**Datenschutz-Einstellungen anpassen**

Um den Datenschutz in Windows 10 zu optimieren, sollte nach der Installation ein erster Blick in die Einstellungen gehen. Diese sind am schnellsten zu finden, wenn im Suchfeld nach „Datenschutz“ gesucht wird. Grundsätzlich ist es also sinnvoll, wenn vor der Erstellung eines Images für die Bereitstellung von Windows 10 die Datenschutzoptionen angepasst werden.

[[](http://www.zdnet.de/wp-content/uploads/2016/02/schutz-01.jpg)](http://www.zdnet.de/wp-content/uploads/2016/02/schutz-01.jpg)Die neuen PC-Einstellungen wurden von Microsoft deutlich vereinfacht und übersichtlicher gestaltet. Der Bereich soll die Systemsteuerung auf Dauer ersetzen (Screenshot: Thomas Joos).

Die wichtigsten Einstellungen für den Datenschutz sind im Bereich „Datenschutz“ zusammengefasst. Hier sollten zunächst die Einstellungen vorgenommen werden, die auch später bei den Rechnern der Anwender gelten sollen. Natürlich taugen die Einstellungen an dieser Stelle nicht für die Automatisierung. Viele dieser Einstellungen lassen sich auch über Gruppenrichtlinien-Einstellungen vorgeben.

[](http://www.zdnet.de/wp-content/uploads/2016/02/schutz-02.jpg)In den Datenschutz-Einstellungen lassen sich mit Schiebereglern viele Verbesserungen bezüglich der Sicherheit in Windows 10 erreichen (Screenshot: Thomas Joos).

**Einstellungen mit Skript anpassen**

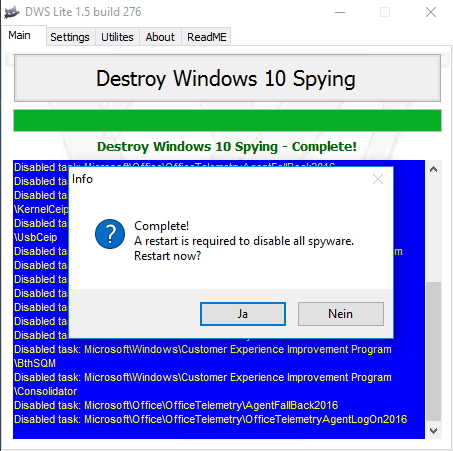
Wer sich etwas mit Skripting auseinandersetzt, kann viele Datenschutzeinstellungen in Windows 10 auch über Batch- oder Skripts durch Registry-Änderungen vornehmen. Eine Vorlage dafür ist zum Beispiel auf der Seite [Pastebin](http://pastebin.com/K8Ww4j8z) zu finden. Hier können entweder alle Einstellungen auf Test-Rechner übernommen werden oder sie werden an die eigenen Anforderungen angepasst.

Wer das Ganze über die PowerShell erledigen will, findet auf [Github](https://github.com/MichiMunich/Windows10-Privacy) ein weiteres Skript dazu. Allerdings gilt bei beiden Skripten, dass diese nicht einfach übernommen werden sollten, zumindest nicht auf produktiven Arbeitsstationen, sondern nur als Vorlage dienen. Dadurch können im Unternehmen effizient Skriptdateien entwickelt werden, die unabhängig von den Möglichkeiten in Windows 10 den Datenschutz verbessern.

In diesem Bereich kann auch die HOSTS-Datei im Verzeichnis „C:\Windows\System32\drivers\etc“ eine Rolle spielen. Hier lassen sich Namensauflösungen unabhängig von DNS konfigurieren. Viele der in Windows 10 integrierten Diagnosefunktionen leiten ihre Informationen direkt zu Microsoft-Servern weiter. Über die Hosts-Datei lassen sich diese Anfragen auch an die lokale IP-Adresse des Rechners umleiten. Dadurch versendet Windows 10 zwar Daten, diese kommen aber nicht bei Microsoft an, sondern landen auf dem eigenen Rechner. Alternativ können die entsprechenden Server auch direkt in der Unternehmensfirewall blockiert werden. Die am häufigsten verwendeten Serveradressen sind folgende:

* 2mdn.net
* a-0001.a-msedge.net
* adnxs.com
* ads1.msn.com
* ads2.msads.net
* ads2.msn.com
* aka-cdn-ns.adtech.de
* ams9.msecn.net
* appex.bing.net
* appex.bing.net:443
* atdmt.com
* cloudapp.net
* data.microsoft.com
* df.telemetry.microsoft.com
* flashtalking.com
* footprintpredict.com
* gateway.messenger.live.com
* hotmail.com
* live.com
* metaservices.microsoft.com
* microsoft.com.nsatc.net
* microsoft-hohm.com
* msads.net
* msftncsi.com
* msitadfs.glbdns2.microsoft.com
* msn.comppe.telemetry.microsoft.com
* rad.msn.comrads.msn.com
* search.microsoft.com
* services.social.microsoft.com
* services.social.microsoft.com.nsatc.net
* serving-sys.com
* settings-sandbox.data.microsoft.com
* sts.microsoft.com
* support.microsoft.com
* telemetry.microsoft.com
* telemetry.microsoft.com.nsatc.net
* update.microsoft.com.akadns.net
* urs.microsoft.com
* vo.msecnd.net
* vortex-sandbox.data.microsoft.com
* vortex-win.data.microsoft.com
* watson.microsoft.com
* wes.df.telemetry.microsoft.com
* windows.comwpc.v0cdn.net
* ws.microsoft.com

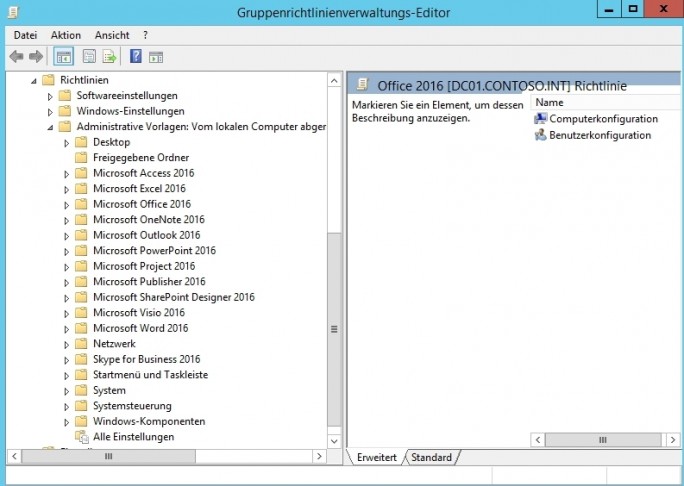
Die Daten können Administratoren auch über das kostenlose Tool [Destroy Windows 10 Spying](http://filepony.de/download-destroywindowsspying/get-mirror-server.html) auf einem Testrechner einspielen lassen. Das Tool muss nicht installiert werden, es erweitert die Hosts-Datei und nimmt Anpassungen an der Registry vor. Die angepasste Host-Datei kann durchaus als Vorlage für die Bereitstellung im Unternehmen dienen. In jedem Fall erhalten Administratoren dadurch schon einen Überblick, welche Daten wohin übertragen werden und was unter Umständen an der Firewall und an anderer Stelle blockiert werden kann.

[](http://www.zdnet.de/wp-content/uploads/2016/02/schutz-05.jpg)Mit einem kostenlosen Tool lassen sich Hosts-Einträge für besseren Datenschutz in Windows 10 erstellen (Screenshot: Thomas Joos).

**Gruppenrichtlinieneinstellungen für besseren Datenschutz integrieren**

Beim Einsatz von Windows 10 im Unternehmen spielen natürlich die Gruppenrichtlinien eine besonders wichtige Rolle. Hier können Administratoren zentral Einstellungen vorgeben. Da aktuell Windows Server 2016 noch nicht zur Verfügung steht, und in Windows Server 2012 R2 die passenden Einstellungen noch nicht verfügbar sind, müssen die Vorlagendaten (\*.admx) manuell auf den Domänencontrollern eingespielt werden. Microsoft stellt diese kostenlos zum [Download](https://www.microsoft.com/de-DE/download/details.aspx?id=48257) zur Verfügung. Zusätzlich bietet Microsoft eine [Excel-Tabelle](http://download.microsoft.com/download/8/F/B/8FBD2E85-8852-45EC-8465-92756EBD9365/Windows%2010%20ADMX%20spreadsheet.xlsx) mit Erläuterungen für die einzelnen Einstellungen zum Download an. Die [Gruppenrichtlinienvorlagen für Office 2016](https://www.microsoft.com/en-us/download/details.aspx?id=49030) stellt Microsoft ebenfalls kostenlos zur Verfügung .

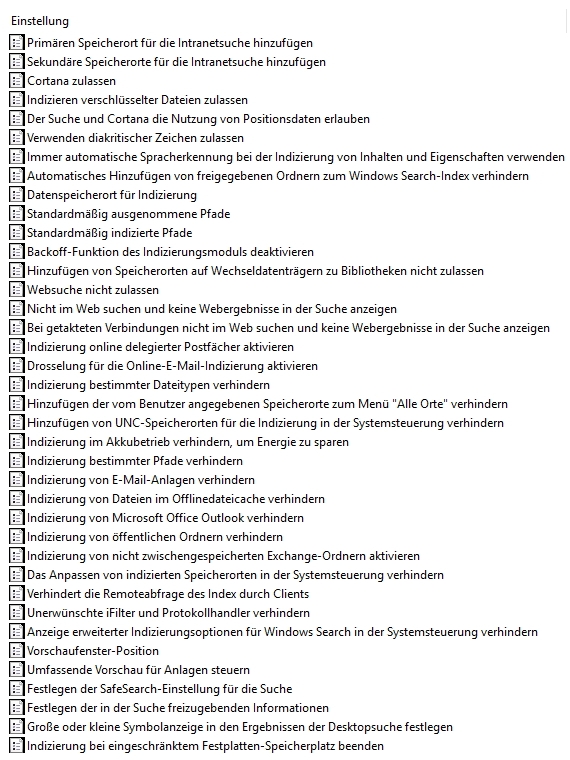
Nach dem Download werden die ADMX-Dateien in das Verzeichnis *C:\PolicyDefinitions* auf den Domänencontrollern im Netzwerk kopiert. Die ADML-Dateien werden wiederum in das entsprechende Sprachverzeichnis in *C:\PolicyDefinitions* kopiert, zum Beispiel in das Verzeichnis *de-de*. Auf den Domänencontrollern befinden sich danach also alle ADMX-Dateien zur Erstellung von Gruppenrichtlinien, und alle notwendige ADML-Dateien, für die jeweilige Sprache. Die Vorgehensweise ist also identisch mit der Integration der Gruppenrichtlinienvorlagen für Windows 10 und Windows Server 2016. Setzen Unternehmen auf eine zentrale Ablage aller Gruppenrichtlinieneinstellungen, dann werden diese natürlich an die entsprechende Stelle kopiert.

[](http://www.zdnet.de/wp-content/uploads/2016/02/schutz-03.jpg)Nachdem die Gruppenrichtlinienvorlagen importiert sind, können Administratoren zentral Sicherheit-Einstellungen für Windows 10, aber auch für [Office](http://www.zdnet.de/themen/office-2013/) 2016 vorgeben (Screenshot: Thomas Joos).

Generell ist es empfehlenswert, für die Steuerung von Windows 10 und Office 2016 eine neue Gruppenrichtlinie erstellen, über die ausschließlich Einstellungen für das Betriebssystem oder Office vorgenommen werden. Tauchen Probleme auf, müssen Administratoren nur in dieser Richtlinie suchen, oder können die Richtlinie deaktivieren. Alle anderen Richtlinien bleiben dagegen weiterhin aktiv.

**Sicherheits-Einstellungen über Gruppenrichtlinien steuern**

Sobald die Gruppenrichtlinien-Vorlagen in der Domäne verfügbar sind, können Administratoren zentral die Einstellungen für Windows 10 und Office 2016 verbessern. Neben den Datenschutz-Einstellungen, spielen hier natürlich auch die Einstellungen für den neuen Sprachassistenten Cortana eine wichtige Rolle. Denn dieser Sprachassistent kann einige Daten in das Internet übertragen, die Unternehmen aus Datenschutzgründen besser blockieren sollten. Die Einstellung für Cortana sind im Bereich „Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Suche“ zu finden.

[](http://www.zdnet.de/wp-content/uploads/2016/02/schutz-04.jpg)Der Sprachassistent Cortana lässt sich in den Gruppenrichtlinien von Windows 10 und Windows Server 2016 steuern oder ganz deaktivieren (Screenshot: Thomas Joos).

Durch die Option „Nicht im Web suchen und keine Webergebnisse in der Suche anzeigen“ lässt sich verhindern, dass Anwender Cortana aktivieren und im Internet nach Informationen suchen. Cortana zeigt an dieser Stelle in Windows 10 auch an, dass die Option mit Richtlinien deaktiviert wurde. Darüber finden sich hier weitere Einstellungen, zum Beispiel die Deaktivierung von Positionsdaten, was vor allem auf mobilen Rechnern interessant ist, die zum Beispiel über DirectAccess mit dem Firmennetzwerk verbunden sind.

Mit der Richtlinieneinstellung „Cortana zulassen“ können Administratoren durch Setzen der Option „Deaktivieren“ Cortana auf allen Rechnern im Unternehmen generell ausschalten. Natürlich funktioniert die Standard-Suche in Windows weiter, nur die erweiterten Funktionen von Cortana werden dadurch deaktiviert.

Auch Microsoft Edge lässt sich über Gruppenrichtlinien steuern. Zu finden sind die Einstellungsmöglichkeiten über „Computerkonfiguration\Richtlinien\Administrative Vorlagen\Windows-Komponenten\Microsoft Edge“. Hier lassen sich Cookies verbieten, oder die Skriptausführung in Edge blocken. Hier sollten sich Administratoren vor allem die Einstellung „Sendet den gesamten Intranetdatenverkehr an Internet Explorer“ ansehen. Sinnvoll ist das, wenn interne Webseiten im Einsatz sind.

**Office 2016 absichern und überwachen**

Die Konfiguration von Sicherheitseinstellungen für Office-Programme sind über „Computerkonfiguration\Richtlinien\Administrative Vorlagen“ und „Benutzerkonfiguration\Richtlinien\Administrative Vorlagen\[Microsoft Office](http://www.zdnet.de/themen/office-2013/) 2016\Sicherheitseinstellungen“ sowie bei „Benutzerkonfiguration\Richtlinien\Administrative Vorlagen“ und „Benutzerkonfiguration\Richtlinien\Administrative Vorlagen\Microsoft Office 2016\Datenschutz\Trust Center“ zu finden.

Setzen Unternehmen Office 2016 Professional Plus ein, können Administratoren über eine Excel-Tabelle, zusammen mit einer SQL-Datenbank eine Telemetrieumgebung für Office 2016 aufbauen. Der dazu notwendige Client ist in Office 2016 integriert. Die Gruppenrichtlinieneinstellungen für den Telemetrieclient sind über „Benutzerkonfiguration\Richtlinien\Administrative Vorlagen\Microsoft Office 2016\Telemetriedashboard“ zu finden.

**Spezielle Richtlinien für Windows 10 Enterprise und Unternehmensrechnung**

Unternehmen die auf Windows 10 Enterprise setzen, können zum Beispiel die Richtlinieneinstellung „Computerkonfiguration / Richtlinien / Administrative Vorlagen / Windows-Komponenten / Datensammlung und Vorabversionen“ nutzen, um den Datenschutz zu verbessern. Hierlassen sich die wertvollen Nutzungsdaten blockieren, was in anderen Editionen von Windows 10 ohne Zusatztools nicht möglich ist.

Unternehmen, die zur Bereitstellung von Updates auf WSUS setzen, können die P2P-Verteilung von Updates über Windows 10 deaktivieren. Diese Einstellung ist auch in anderen Editionen verfügbar. Die entsprechenden Einstellungen dazu sind über „Computerkonfiguration / Richtlinien / Administrative Vorlagen / Windows-Komponenten / Delivery Optimization“ zu finden. Zwar lädt Windows 10 beim Einsatz in Active Directory die Updates nur von Domänenrechnern herunter, dennoch ist es beim Einsatz von Tools wie WSUS sinnvoll alle Updates zentral herunterladen zu lassen.

Soll verhindert werden, dass Anwender die Einstellungen ihrer Rechner mit anderen Rechnern synchronisieren, kann das ebenfalls per Gruppenrichtlinie erfolgen. Diese Funktion war bereits Bestandteil von [Windows 8](http://www.zdnet.de/themen/windows-8/)/8.1. Da viele Unternehmen aber diese Version übersprungen haben, oder die Einstellung nicht gesetzt haben, macht es beim Einsatz von Windows 10 sind, diese Synchronisierung-Richtlinie einzustellen. In den Gruppenrichtlinien ist diese Konfiguration über „Computerkonfiguration / Richtlinien / Administrative Vorlagen / Windows-Komponenten / Einstellung synchronisieren“ zu finden.

Zwar ist der Cloudspeicher OneDrive bereits in Windows 7 nutzbar und in Windows 8/8.1 fest integriert, dennoch sollte bei der Migration zu Windows 10 überprüft werden, ob dieser Speicher auf Unternehmens-Rechnern genutzt werden darf. Die Einstellungen sind in den Gruppenrichtlinien über „Computerkonfiguration / Richtlinien / Administrative Vorlagen / Windows-Komponenten / OneDrive“ konfigurierbar.

Vor allem bei Gruppenrichtlinien, die auf Notebooks von mobilen Anwendern umgesetzt werden, sollte die Einstellung „Computerkonfiguration / Richtlinien / Administrative Vorlagen / Windows-Komponenten / Position und Sensoren / Windows-Positionssuche“ überprüft werden.

Seit Windows 10 lassen sich auch Datenübertragungen der integrierten Windows-Spiele besser steuern. Dazu wird die Einstellung „Computerkonfiguration / Richtlinien / Administrative Vorlagen / Windows-Komponenten / Windows Game Recording and Broadcasting“ genutzt.

Eine weitere Einstellung für den besseren Datenschutz ist das Aktivieren der Einstellung „Werbe-ID deaktivieren“ unter „Computerkonfiguration / Richtlinien / Administrative Vorlagen / System / Benutzerprofile“.

**Fazit**

Mit Windows 10 überträgt Microsoft einige Daten zu den eigenen Servern, die Administratoren häufig gerne blockieren wollen. Zwar lassen sich mit Bordmitteln bereits einige Einstellungen verbessern, IT-Manager sollten aber frühzeitig bei der Planung der Bereitstellung von Windows 10 auch den Datenschutz miteinbeziehen. Mit Gruppenrichtlinien, angepassten Images und Einträgen in den Firewalls sowie einigen Skripten lässt sich der Datenschutz erheblich verbessern. Welche Mittel eingesetzt werden, ist schlussendlich Sache des jeweiligen Unternehmens.

Wie bei allen neuen Windows-Betriebssystem ist es aber empfehlenswert, die Gruppenrichtlinien-Einstellung für mehr Sicherheit und Datenschutz in jedem Fall zu verwenden. Natürlich sollten sich Administratoren auch Gedanken darüber machen, ob die Einstellungsänderungen auf Kosten der Produktivität der Anwendern gehen. Sind aber Funktionen für die tägliche Arbeit nicht notwendig, dann spricht auch nichts dagegen diese zu deaktivieren.