Arbeitskreis Informationssicherheit
der deutschen Forschungseinrichtungen (AKIF)

Orientierungshilfe zur datenarmen Konfiguration von Windows 10

AKIF-Arbeitsgruppe „Windows 10“:
Dr. Robert Formanek – Universität Hohenheim
Jens Syckor, Raffael Kozerski, Dr. Erasmus Scholz – TU Dresden
Willem Wahlen – Helmholtz-Zentrum Geesthacht
Joachim S. Müller – Fraunhofer ZV
Susanne Weinmann – Max-Planck-Gesellschaft

Kontakt:
Dr. Robert Formanek
robert.formanek@uni-hohenheim.de

Version:	Datum	Änderungshistorie
2.0	06.12.2016	• Allgemeines • Datenschutz • Cortana & Websuche • Gruppenrichtlinien • WLAN-Optimierung • Windows Defender • Sonstiges
1.0	13.05.2016	Initiale Version

Inhalt

Vorwort

Vorwort zur 2. Auflage

Die Nachfrage nach dieser Orientierungshilfe – auch außerhalb von Forschung und Lehre – war deutlich größer als erwartet. Dies hat uns gezeigt, dass das Projekt vieles richtig gemacht hat. Die meisten Anregungen wurden in diese zweite Auflage aufgenommen. Jetzt wird das Update 1607 (Anniversary Update) berücksichtigt.

Der Trend scheint eindeutig. Je weniger Geld man für eine Windows 10 Edition bezahlt, umso mehr Daten muss die Nutzerin oder der Nutzer liefern. Dies muss zu der Empfehlung führen, dass in Hochschulen, Universitäten und Forschungseinrichtungen nur die Education bzw. Enterprise Edition eingesetzt werden sollten: zu viele Einstellungen fehlen in der Home und Professional Edition.

Ab 1. Januar 2017 wird Dr. Robert Formanek, IT-Sicherheitsbeauftragter der Universität Hohenheim, die Federführung in dem Projekt übernehmen. Vielen Dank für die Bereitschaft. Vielen Dank auch an Frau Susanne Weinmann, dass sie das Projekt so weit gebracht hat. Neue Aufgaben in der Max-Planck-Gesellschaft lassen ihr keine Zeit mehr für dieses Projekt.

München, im November 2016

Rainer W. Gerling
Vorsitzender des Sprecherkreises des AKIF

Vorwort zur 1. Auflage

Von Windows 7 zu Windows 10 ist es ein gewaltiger Wechsel. Deshalb haben sich Forschungseinrichtungen und Hochschulen auch immer wieder gefragt, kann man es guten Gewissens verantworten diesen Wechsel zu vollziehen oder bleiben Datenschutz und IT-Sicherheit dabei auf der Strecke?

Aus dem anfänglichen Versuch zusammenzutragen, was an Konfigurationsempfehlungen existiert, ist ein größeres Projekt geworden. Hierzu haben etliche Forschungseinrichtungen und Hochschulen beigetragen. Ihnen allen gilt unser Dank.

Herausgekommen ist dabei keine „Anleitung zur sicheren Konfiguration von Windows 10". Aber wir sind uns sicher, auf dem Weg zu einer sicheren Konfiguration einige Schritte in die richtige Richtung gegangen zu sein. Letztendlich haben wir das Dokument „Orientierungshilfe für eine datenarme Konfiguration von Windows 10" erstellen können. Unnötige Funktionalitäten werden abgeschaltet, die Kommunikation nach Hause wird eingeschränkt. Das Papier erhebt keinen Anspruch auf Vollständigkeit. Von daher sind wir für entsprechende Hinweise dankbar.

Microsoft wird Windows 10 ein- bis zweimal im Jahr aktualisieren. Dann muss untersucht werden, was sich in Bezug auf diese Orientierungshilfe verändert hat. Insofern wird dies ein lebendes Dokument sein. Wie wir die dafür erforderlichen personellen Ressourcen aufbringen, ist noch unklar.

Es kam auch schon die Frage nach einer entsprechenden Orientierungshilfe für Office 365. Hier muss sich ein Team finden, das es schreibt.

Über ein Feedback - wie über Verbesserungsvorschläge - würden wir uns freuen.

München, im Juni 2016

Rainer W. Gerling
Vorsitzender des Sprecherkreises des AKIF

Präambel

Die Orientierungshilfe erklärt und dokumentiert die wichtigsten Funktionen und Einstellungen von Windows 10 für eine maximal sichere Konfiguration des Betriebssystems.

Es handelt sich hierbei ausschließlich um Empfehlungen und Hinweise, welche nicht einfach ungesehen übernommen werden sollen. Vielmehr sollten die lokalen Administratoren und Verantwortlichen für IT-Sicherheit die Anforderungen sowie die vorhandene Infrastruktur vor Ort überprüfen und bei der Planung des Einsatzes von Windows 10 berücksichtigen.

Die Orientierungshilfe wird fortlaufend aktualisiert, um dem neuen Konzept, welches Microsoft mit Windows 10 verfolgt, gerecht zu werden. Neue und geänderte Funktionen und Dienste werden dazu möglichst zeitnah eingepflegt.

Hinweise und Erläuterungen zum Datenschutz bei Windows 10 und dessen Diensten finden sich in der von der DFN Forschungsstelle Recht veröffentlichten Handlungsempfehlung „Datenschutzrechtliche Probleme bei der Einführung neuer Betriebssysteme - Eine Untersuchung am Beispiel Windows 10“[1].

[1] https://www.dfn.de/fileadmin/3Beratung/Recht/handlungsempfehlungen/Datenschutzrechtliche_Probleme_bei_der_Einfuehrung_neuer_Betriebssysteme.pdf (Abrufdatum: 25.08.2016)

Allgemeines

Mit Windows 10 beschreitet Microsoft neue Wege. Neben neuen Funktionen, wie z.B. der digitalen Assistentin Cortana und dem neuen Browser Edge, steht vor allem das gesamte Konzept „Windows as a Service" im Fokus. Damit unterscheidet es sich von den bisherigen, klassischen Betriebssystemen wie Windows XP, Windows 7 oder Windows 8.1. Während größere Updates und neue Funktionen bisher in Form einer neuen Betriebssystem-Version oder eines Service-Packs veröffentlicht wurden, werden diese zukünftig als kontinuierliche Updates geliefert und stehen sofort allen Nutzern zur Verfügung. Das Betriebssystem wird also laufend weiterentwickelt.

Das derzeit aktuelle Update ist das Anniversary Update (Build 1607, auch Redstone1 genannt) und wurde am 2. August 2016 veröffentlicht.

Für berechtigt lizensierte Geräte mit Windows 7 und Windows 8/8.1 (ausgenommen Education- und Enterprise-Editionen) wurde das Upgrade bisher kostenlos angeboten. Damit sollten möglichst viele Kunden zum Umstieg bewegt werden. Diese Phase wurde am 29. Juli 2016 wie angekündigt beendet, Windows 10 wird dementsprechend auch nicht mehr als empfohlenes Update angeboten. Ein kostenloses Upgrade ist derzeit nur noch für Geräte mit Assistive Technology (barrierefreie Geräte für Seh- und Hörgeschädigte) möglich. Wie die Anwendung dieser Technologie auf einem Endgerät festgestellt wird ist jedoch nicht bekannt. Weiterhin verfügbar ist das Media Creation Tool. Um über dieses Tool Windows 10 installieren zu können oder ein ISO-Image zu erstellen muss jedoch ein gültiger Windows 10-Lizenzschlüssel vorliegen.

Warum geht Microsoft diesen Schritt? Sein künftiges Geschäft sieht Microsoft nicht mehr im Verkauf von Betriebssystemen, sondern in der Bereitstellung von Dienstleistungen wie Office 365 („Software as a Service"), Cloud-Anwendungen („Storage as a Service"), Spielen, Apps etc. Windows 10 wird hierbei als Plattform betrachtet, welche die Inanspruchnahme der Dienste erst ermöglicht.

Eine weitere Einnahmequelle verspricht sich Microsoft aus der Platzierung von Werbung, welche auf den Verbraucher zugeschnitten ist. Hersteller wie Apple oder Google verfolgen einen sehr ähnlichen Weg bereits seit Jahren. Informationen für diese personalisierte Werbung sammelt Microsoft aus verschiedenen Quellen beim Nutzer direkt. Viele der Dienste, welche Daten sammeln, sind standardmäßig in Windows 10 aktiviert, also NICHT „Privacy by default". Häufig kennen die Nutzer den Umfang des Datensammelns auch gar nicht. Microsoft wird aus diesem Grund häufig als „Datenkrake" bezeichnet, welche Endgeräte mit Windows 10 in eine „private Abhöranlage" verwandelt. Eine Verbesserung in Windows 10 ist in diesem Fall jedoch die Möglichkeit über zahlreiche Optionen in den Einstellungen den Datenschutz zu erhöhen und Datenübertragungen zu unterbinden oder einzuschränken.

Installation

Von Microsoft wird für den einfachen Umstieg auf Windows 10 für bestimmte Editionen (Home, Pro) ein Upgrade angeboten. Um Windows 10 jedoch von Beginn an optimal zu konfigurieren wird eine Neuinstallation empfohlen. Hierbei ist darauf zu achten, dass die Installation mit benutzerdefinierten Einstellungen durchgeführt wird.

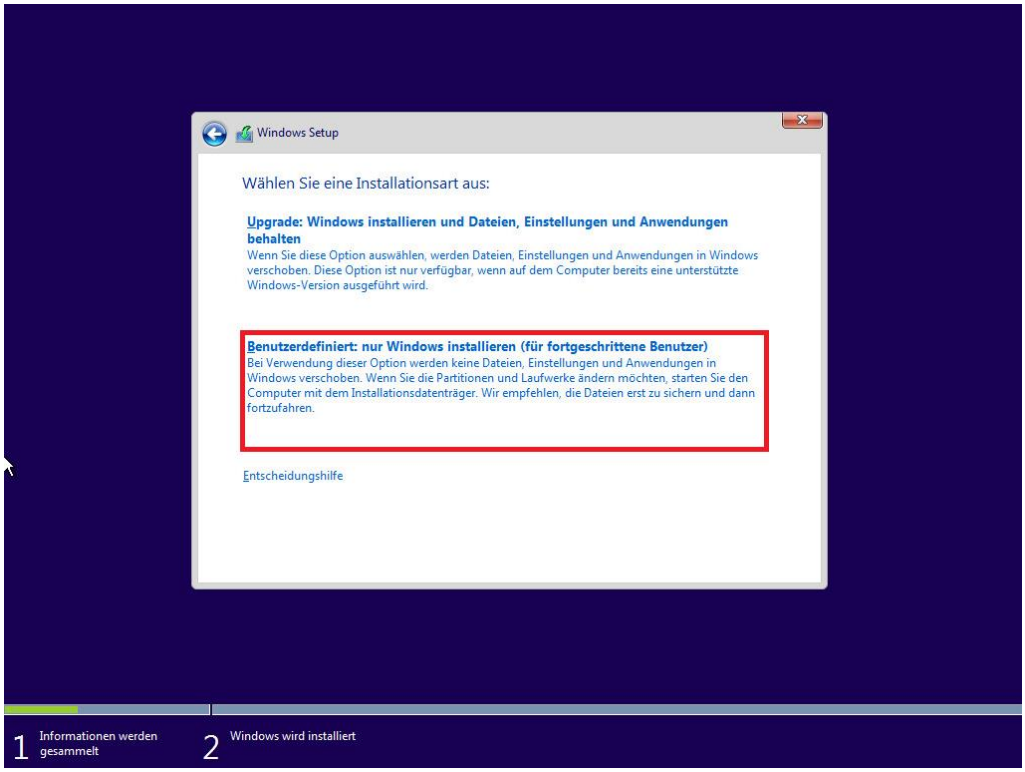

Abbildung 1: Benutzerdefinierte Installation

Von der Verwendung der Express-Einstellungen wird dringend abgeraten. Durch die so übernommene Vorkonfiguration von Windows werden Microsoft zahlreiche Zugriffsmöglichkeiten auf die Daten der Anwender eingeräumt, was nachfolgend auch zu einer übermäßigen Datenübermittlung an Microsoft führt. Windows 10 verfolgt nicht das „Privacy by default"-Prinzip, d.h. datenübermittelnde Funktionen müssen explizit deaktiviert werden.

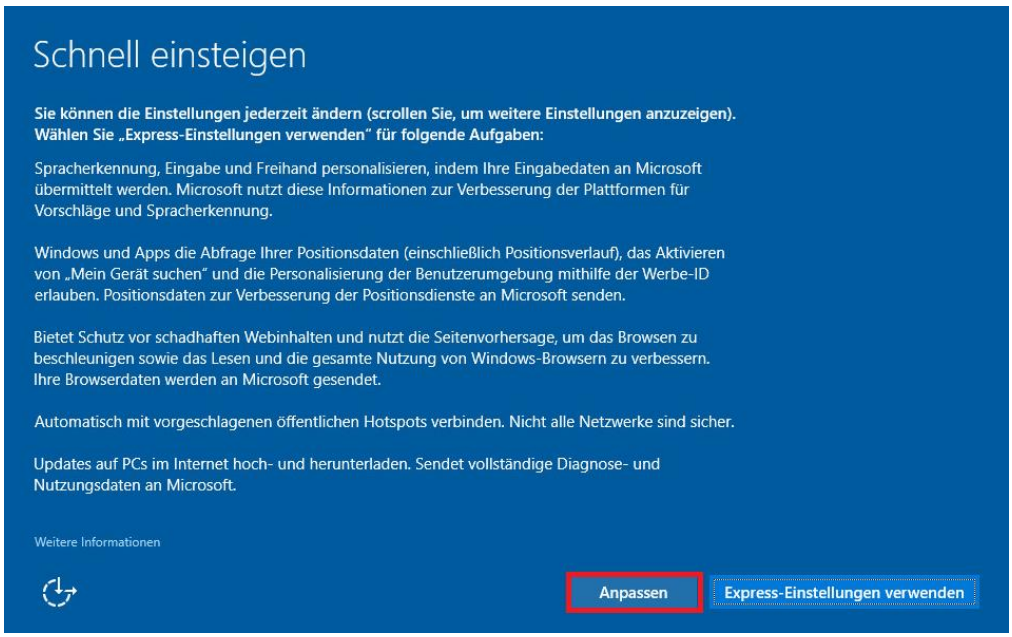

Abbildung 2: Einstellungen anpassen

Auf den folgenden Seiten sind alle Schieberegler standardmäßig eingeschaltet (siehe Abbildung 3).

Abbildung 3: Einstellungen anpassen - Standardeinstellung von Microsoft

Diese sollten nach links verschoben werden um die Dienste zu deaktivieren.

Auf dieser Seite befindet sich seit dem Anniversary Update ein neuer Schieberegler für Skype.

Zudem sollte man darauf achten, im Fenster nach unten zu scrollen, um auch die Einstellungen für die Position zu setzen.

Abbildung 4: Einstellungen anpassen (Teil 1) - empfohlene Einstellungen

Zudem sollte man in diesem Fenster darauf nach unten zu scrollen, um auch die Einstellungen für die Position zu setzen.

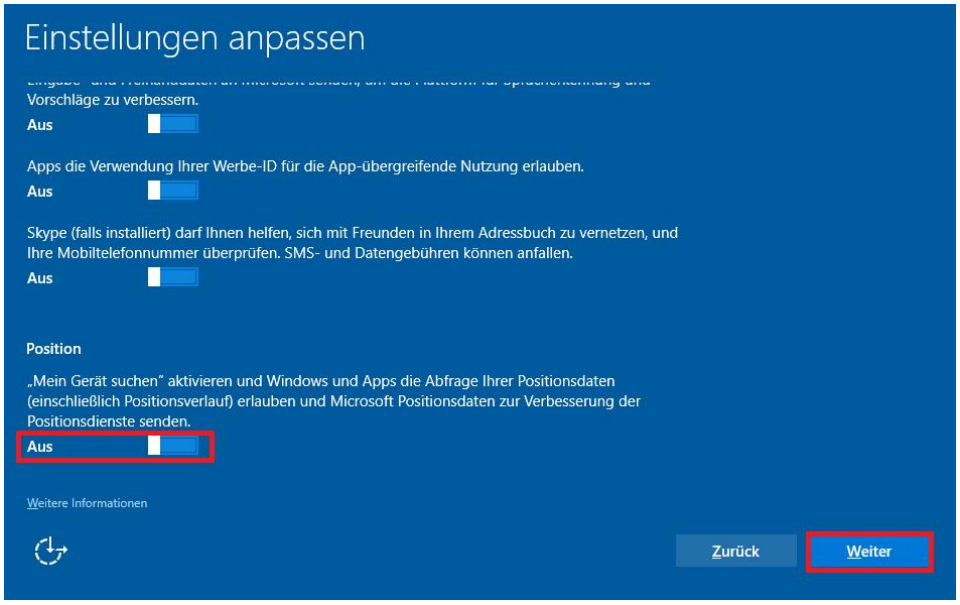

Abbildung 5: Einstellungen anpassen (Teil 2) - empfohlene Einstellungen

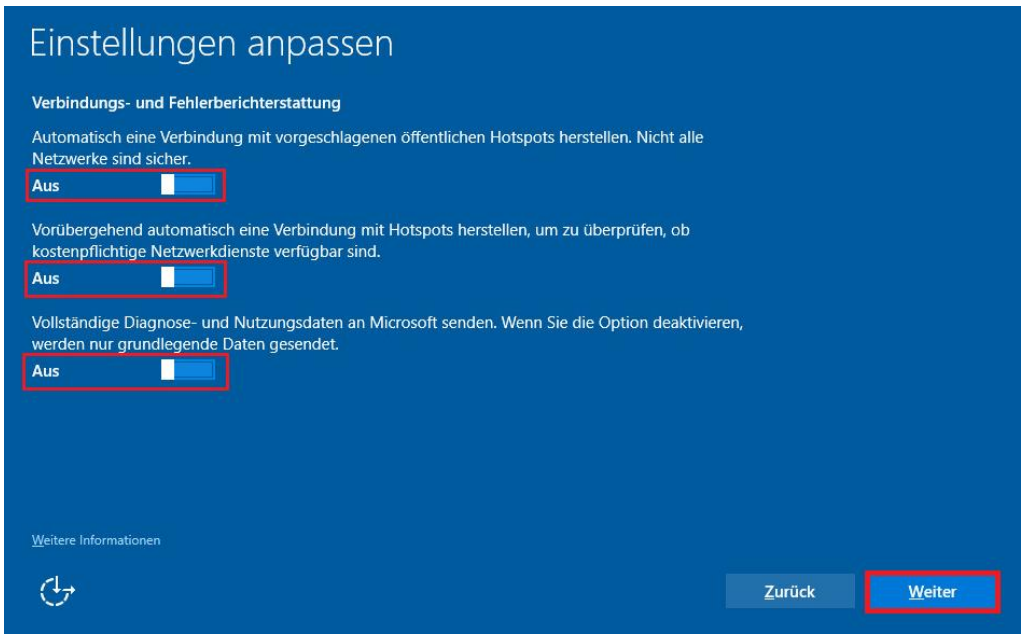

Abbildung 6: Einstellungen anpassen (Teil 3) - empfohlene Einstellungen

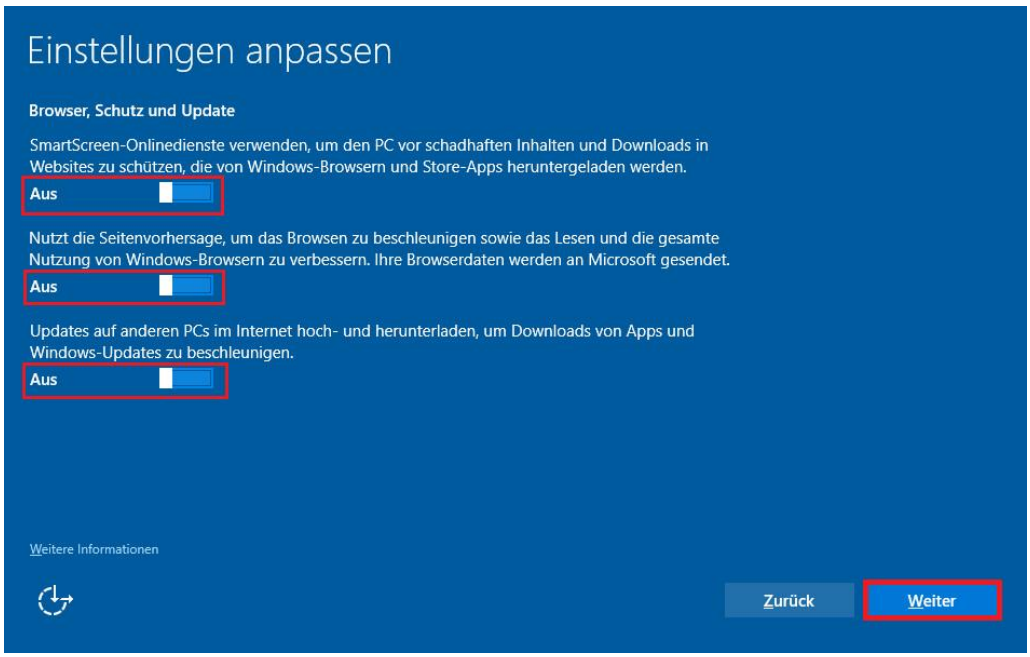

Abbildung 7: Einstellungen anpassen (Teil 4) - empfohlene Einstellungen

Ebenfalls mit dem Anniversary Update wird die Aktivierung bzw. Deaktivierung (empfohlen) von Cortana bereits im Installationskontext nachgefragt.

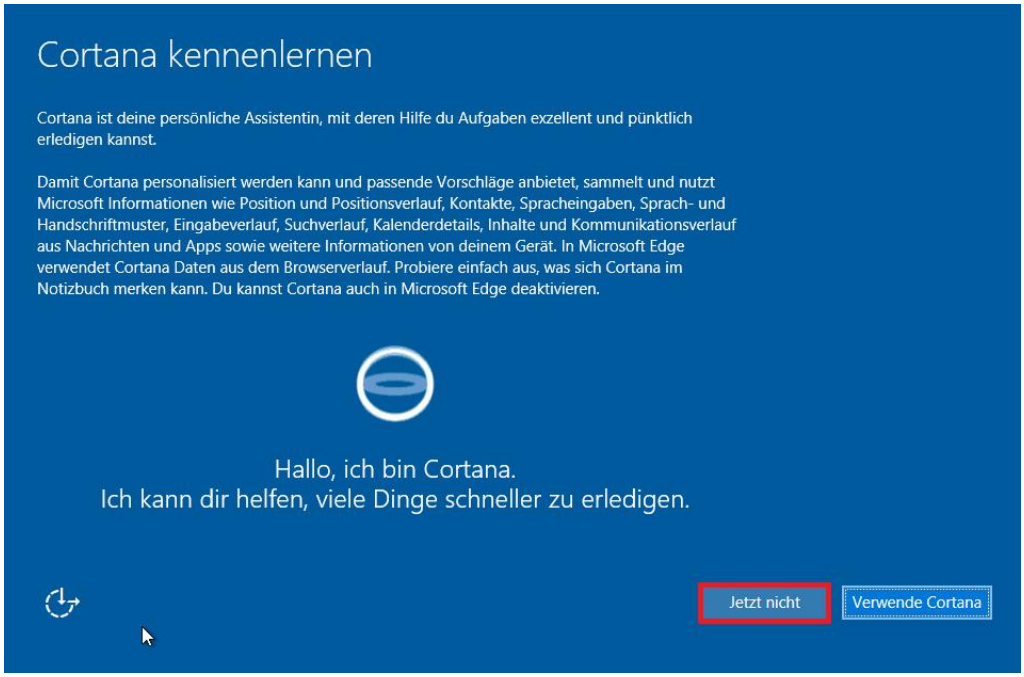

Abbildung 8: Aktivierung bzw. Deaktivierung (empfohlen) von Cortana im Installationskontext

Anmeldung/Konto

Für die Anmeldung an Windows 10 wird die Verwendung eines lokalen Benutzerkontos empfohlen.

Für Geräte, welche in einer Domäne betrieben werden, wird die Verwendung eines Domänen-Kontos empfohlen.

Von einer Verknüpfung mit einem Microsoft-Konto (Outlook.com, MSN, Hotmail), auch für die bloße Verwendung im Windows Store, wird grundsätzlich abgeraten. Durch diese ist die Vorkonfiguration von Windows 10 am wenigsten restriktiv und es werden die meisten Daten gesammelt und an Microsoft übermittelt.

Die Verwendung eines Microsoft-Geschäftskontos sollte lediglich zur Anmeldung im Windows 10 Store for Business dienen. Die Verwendung als Benutzerkonto ist derzeit nicht empfehlenswert.

Einige Funktionen, z.B. die Synchronisation von Einstellungen oder auch Cortana, sind nur bei der Verwendung eines Microsoft-Kontos verfügbar (siehe Abbildung 7).

Weitere Informationen zur Anmeldung mit einem Microsoft-Konto finden sich in der Handlungsempfehlung „Datenschutzrechtliche Probleme bei der Einführung neuer Betriebssysteme - Eine Untersuchung am Beispiel Windows 10" von der DFN Forschungsstelle Recht.

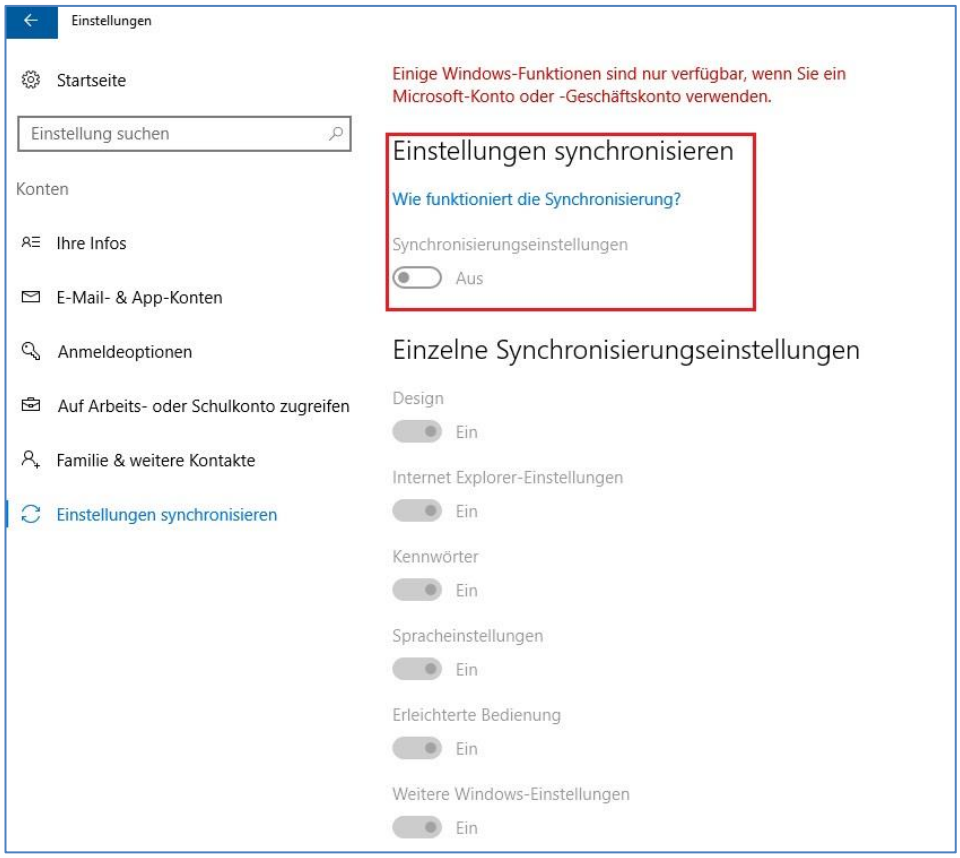

Abbildung 9: Synchronisierung der Einstellung nur mit Microsoft-Konto möglich

Unter dem Punkt „Anmeldeoptionen" gibt es zudem die Möglichkeit, Windows Hello einzurichten. Dabei handelt es sich um eine Methode zur biometrischen Authentifizierung. Dies ist

sowohl für das Gerät möglich als auch für einzelne Apps und Dienste. Für die Authentifizierung werden Fingerabdrücke, das Gesicht oder die Iris einer Person verwendet. Jedoch werden keine Bilder dieser gespeichert, sondern lediglich einzelne Merkmale. Diese werden auch nur auf dem Gerät gespeichert und nicht zu Microsoft transferiert.

Außerdem gibt es unter „Anmeldeoptionen" die neue Einstellung „Datenschutz". Hier können Details zum Benutzerkonto auf dem Anmeldebildschirm ausgeblendet werden.

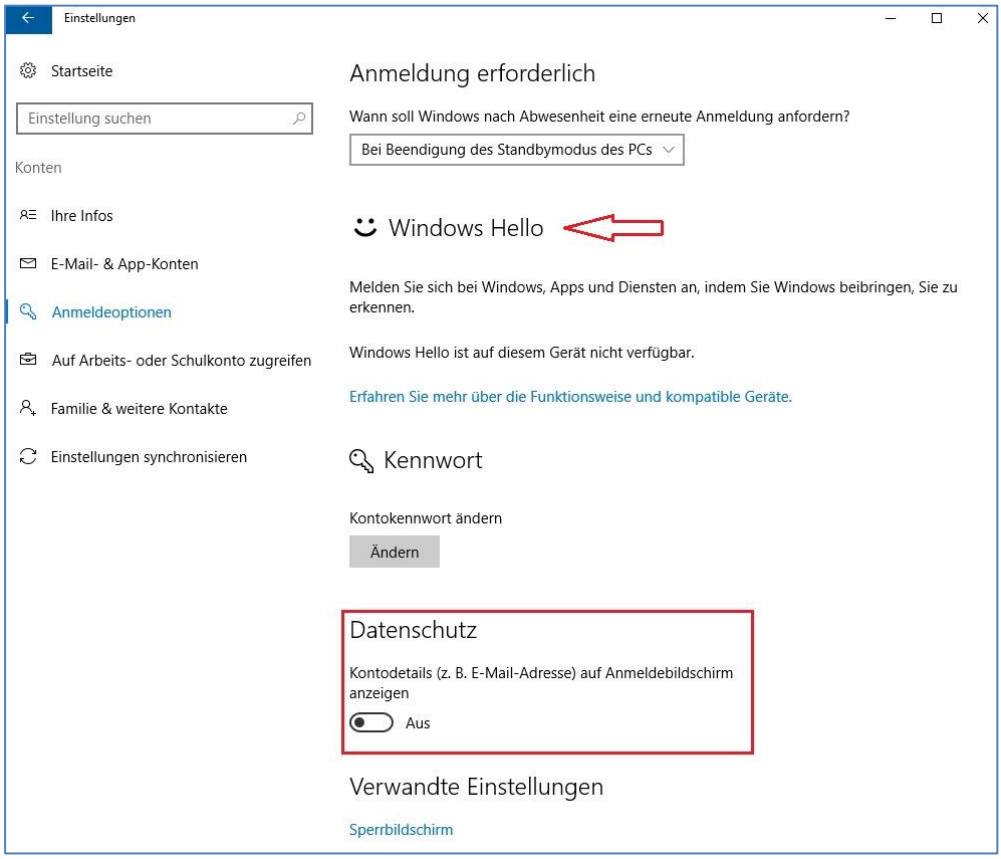

Abbildung 10: Anmeldeoptionen

Konfiguration

Viele Funktionen und Dienste von Windows 10 lassen sich mittels Gruppenrichtlinien und/oder PowerShell-Scripten verwalten. Die Wichtigsten hinsichtlich einer maximal sicheren Konfiguration von Windows 10 finden sich als lose Sammlung im Anhang 1.

Es ist jedoch u.U. nicht möglich, alle Einstellungen auf diesem Wege zu verwalten. Einige Einstellungen lassen sich nur über die Benutzeroberfläche konfigurieren (jedoch auch abhängig davon, wie und wo ein betroffenes Gerät eingesetzt werden soll). Prinzipiell lassen sich alle Einstellungen über Gruppenrichtlinien verwalten, insofern es einen Eintrag in der Registrierung hierfür gibt.

Für Stand-Alone-Geräte und/oder für Geräte mit Home- oder Pro-Editionen von Windows 10 ist es u.U. erforderlich, die Einstellungen über die Benutzeroberfläche vorzunehmen. Auch für Bring-your-own-Device-Geräte kann die nachfolgende Dokumentation der wichtigsten Einstellung in der Benutzeroberfläche eine wichtige Hilfestellung sein.

Datenschutz-Einstellungen

Allgemein

Folgende Funktionen sollten **ausgeschaltet** werden:

- Verwendung der Werbe-ID. (siehe Hinweis-Kasten Seite 9)
- Das Senden von Informationen zum Schreibverhalten an Microsoft.
- Der Zugriff auf die Sprachliste.
- SmartScreen-Filter. (siehe Hinweise-Kasten Seite 9)
- Neu: Öffnen und Benutzen von Apps durch Apps auf anderen Geräten
- Neu: Öffnen und Benutzen von Apps durch Apps auf anderen Geräten über Bluetooth

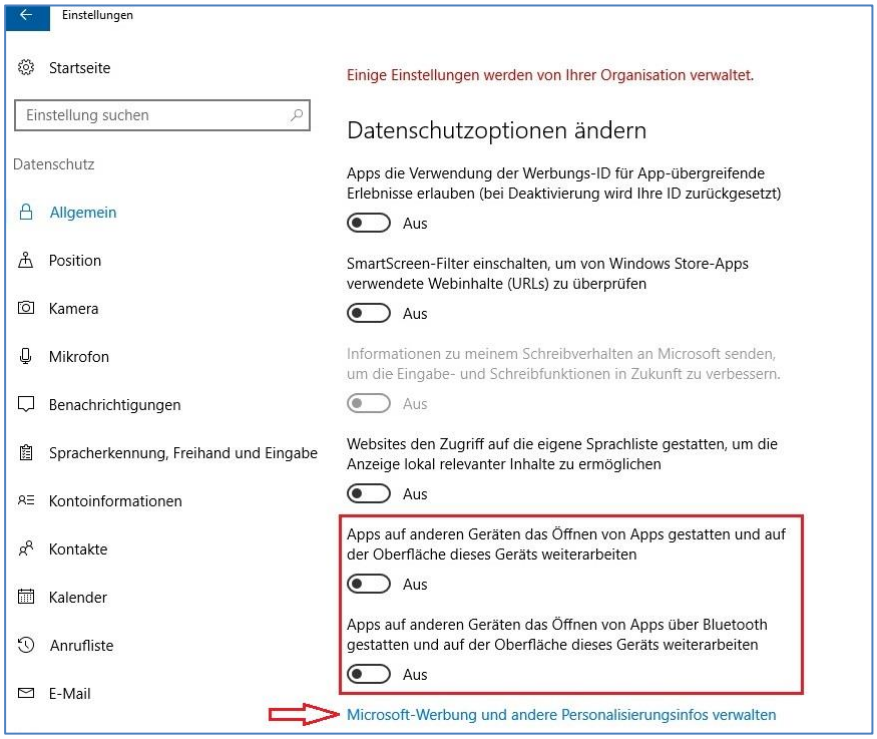

Abbildung 11: Datenschutzeinstellungen - Allgemein

Diese Punkte können auch mittels Gruppenrichtlinie bzw. PowerShell-Script deaktiviert werden. Informationen dazu sind im Anhang 1 zu finden.

Zusätzlich ist der Link „Microsoft-Werbung und andere Personalisierungsinfos verwalten" anzuklicken.

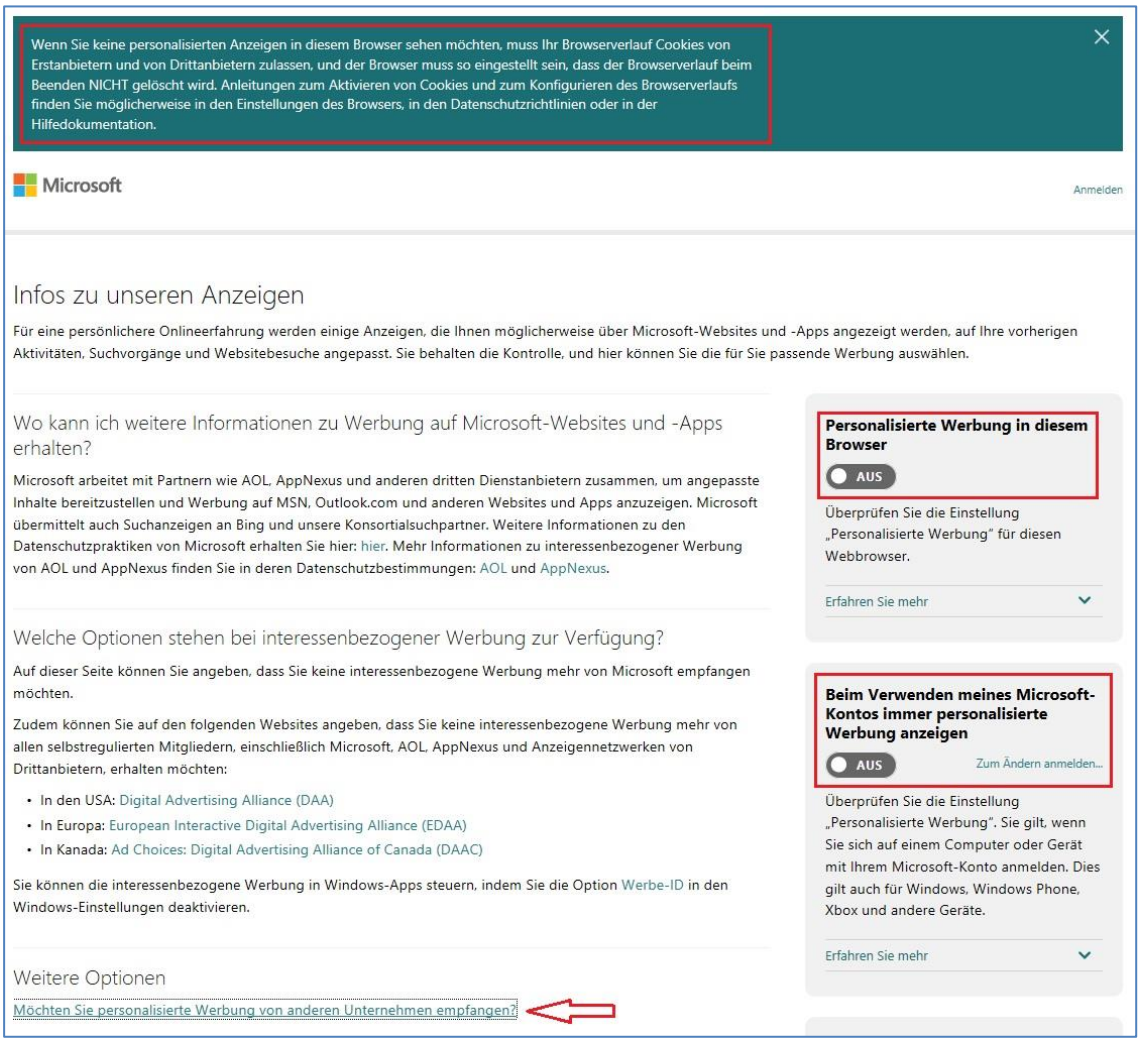

Abbildung 12: Werbungs-ID - Startseite

Auf der sich öffnenden Homepage finden sich auf der rechten Seite zwei Einstellungsmöglichkeiten. Hier kann die personalisierte Werbung von Microsoft deaktiviert werden. Die ersten Einstellung ist für den aktuell verwendeten Browser: dort wird ein Cookie gesetzt, welcher die Werbung verhindert (verwendeter Browser in Abbildungen 9-11: Microsoft Edge). Für weitere verwendete Browser muss der Vorgang wiederholt werden. Werden die Cookies in einem Browser gelöscht, werden auch die vorgenommenen Einstellungen für die personalisierte Werbung gelöscht.

Die zweite Einstellung gilt für den Fall einer Anmeldung mit einem Microsoft-Account. In diesem Fall wird die Einstellung für alle Geräte, welche mit diesem Microsoft-Konto verwendet werden, übernommen.

Unter „Weitere Optionen" findet sich der Link „Möchten Sie personalisierte Werbung von anderen Unternehmen erhalten?". Folgt man diesem, so landet man auf einer Seite auf der sich auch personalisierte Werbung von Dritten ausschalten lässt. Zuerst wird der Browser dahingehend überprüft, ob Cookies von Drittanbietern erlaubt sind. Anschließen wird in der

Übersicht angezeigt, welche Firmen personalisierte Werbung anbieten (Tab 1), welche Firmen diese für den verwendeten Browser anbieten (Tab 2) und für welche Firmen diese bereits deaktiviert ist (Tab 3, Abbildung 13).

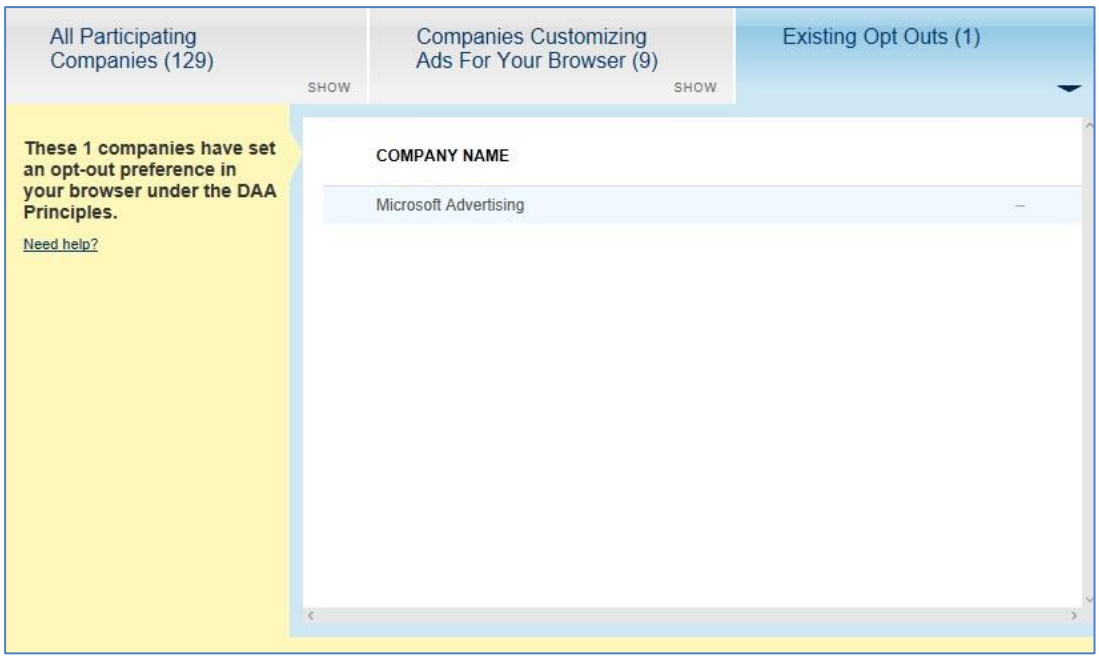

Abbildung 13: Werbungs-ID – personalisierte Werbung von Microsoft deaktivieren

Es wird empfohlen, die personalisierte Werbung für alle teilnehmenden Unternehmen zu deaktivieren. Dies ist auf dem ersten Tab der Anzeige möglich. Es können über „Select all shown" alle ausgewählt werden (natürlich ist es auch möglich, nur einzelne Unternehmen auszuwählen) und über den Button „Submit your choices" deaktiviert werden.

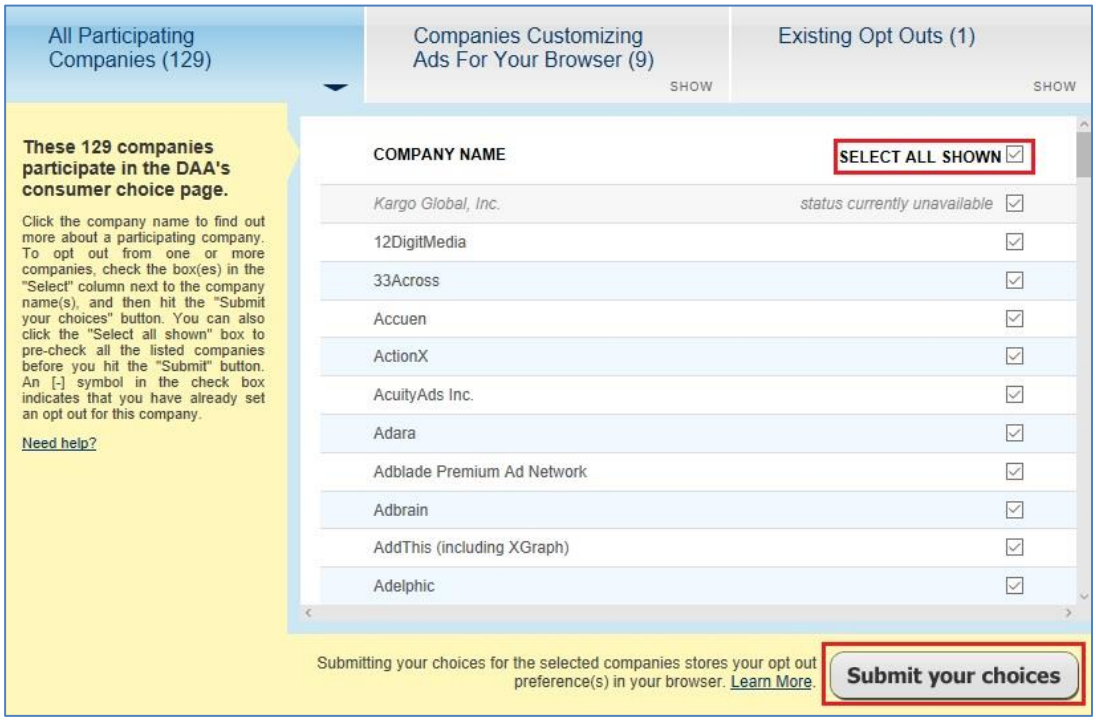

Abbildung 14: Werbungs-ID - personalisierte Werbung von Drittanbietern deaktivieren

Hinweis „Werbe-ID"

Dient der personalisierten Anzeigen-Einblendung im Webbrowser. Es werden bspw. Standorte, angesehene Inhalte und Suchanfragen an Microsoft übermittelt und verarbeitet. Für die Verwendung der Werbe-ID ist die Anmeldung mit einem Microsoft-Benutzerkonto nötig. Dieses wird automatisch mit der ID verknüpft.

Hinweis „SmartScreen-Filter"

Der SmartScreen-Filter dient der Überprüfung von Web-Inhalten und Downloads bspw. mittels Phishing-Filter oder Malwareschutz zur Vorbeugung gegen Betrug und zur Abwehr von Schadsoftware. Dazu werden Daten über die verwendeten Webinhalte an Microsoft sendet, wo diese mit einer Datenbank abgeglichen, aber nicht gespeichert werden. Diese Schutzfunktion des Browsers wird üblicherweise durch die verwendete Antivirensoftware übernommen, kann also problemlos deaktiviert werden.

Position

Die Standortbestimmung (über GPS und/oder IP-Adresse) sollte deaktiviert werden, da die Standorte an Microsoft übermittelt werden und genaue Standortverläufe erstellt werden. Jedoch kann dies nicht umfassend verhindert werden, da auch Daten von WLAN-Hotspots, Mobilfunkmasten und Bluetooth-Adaptern verwendet werden. Zudem können Apps von Drittanbietern weiterhin auf den Standort zugreifen, der Zugriff dieser Apps kann am Ende der Seite jedoch einzeln verwaltet werden. Dies sollte beispielsweise beim Einsatz von Apps und Diensten, für deren Funktionalität Standortdaten benötigt werden (z.B. Navigation), angewendet werden. Ein neues Feature bei dieser Einstellung ist die Verwendung des ungefähren Standorts, dies kann z.B. der Internet-Einwahlknoten sein. Zudem gibt es hier die Möglichkeit, einen Standardort festzulegen, wenn die automatischen Erkennungsdienste deaktiviert sind. Am Ende der Seite wird zusätzlich auf Apps hingewiesen, die Geofencing verwenden. D.h. ob sich interessante Orte innerhalb eines definierten Umkreises zum festgestellten Standort befinden. Dieses Feature ist nur in Verbindung mit der Positionserkennung möglich.

Die Einstellung kann auch mittels Gruppenrichtlinie bzw. PowerShell-Script deaktiviert werden. Informationen dazu sind im Anhang 1 zu finden.

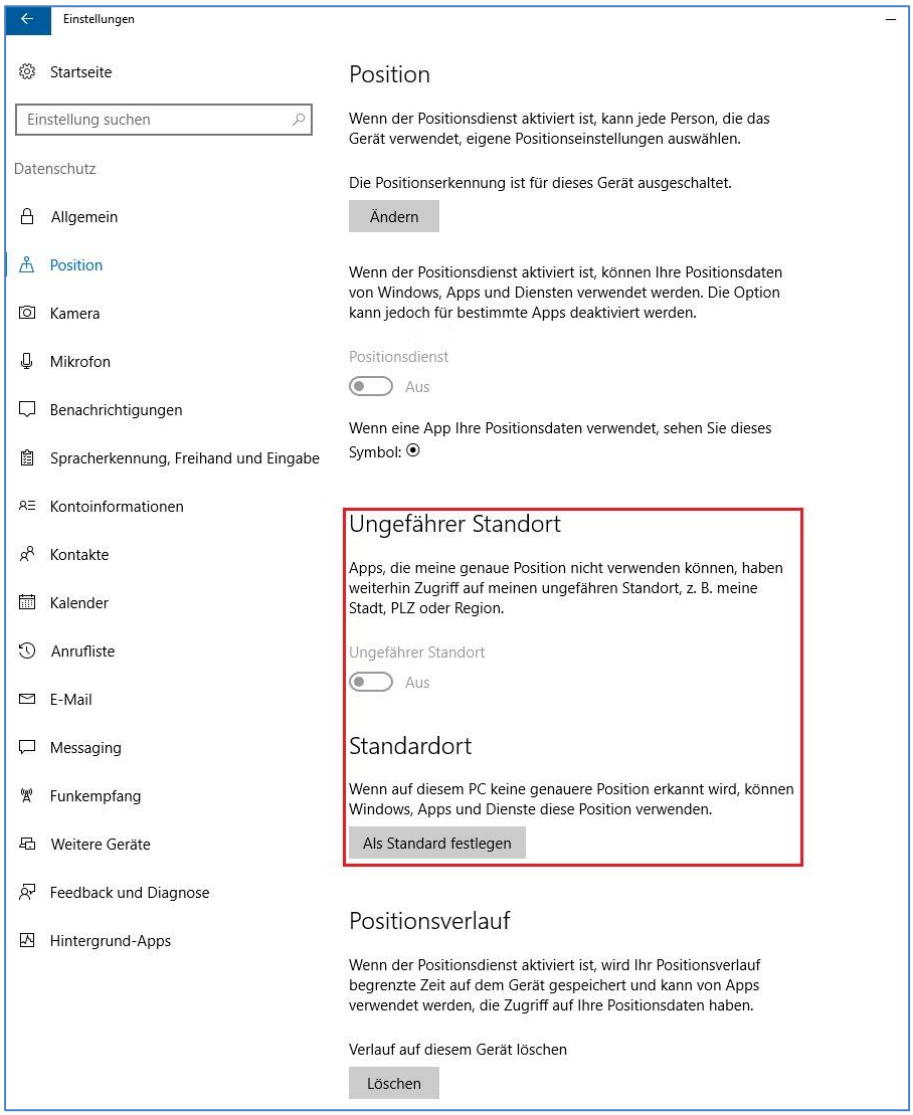

Abbildung 15: Datenschutzeinstellungen - Position

Kamera und Mikrofon

Hier kann einzelnen (am Ende der Seite) oder allen Apps (Schieberegler ganz oben) der Zugriff auf die Kamera und das Mikrofon erlaubt oder entzogen werden. Hierbei ist zu überlegen, welche Apps für ihre Funktionalität tatsächlich den Zugriff benötigen. Sinnvoll ist es z.B. bei Skype oder anderen Videotelefonie-Diensten. Die App „Verbinden", welche sich u.U. auf der Einstellungsseite „Kamera" befindet, dient der Verbindung zu Miracast (wenn das Gerät dies unterstützt).

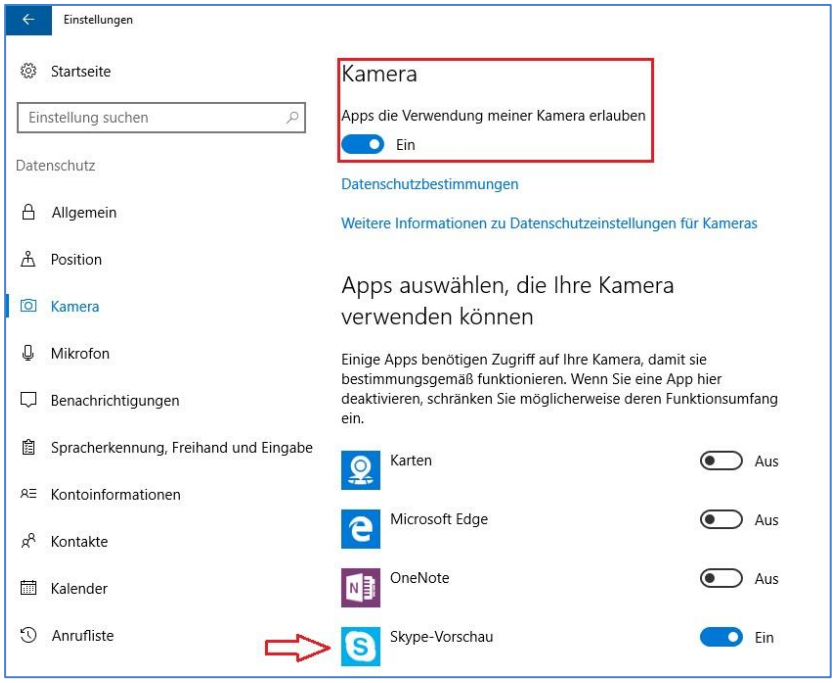

Abbildung 16: Datenschutzeinstellungen – Kamera

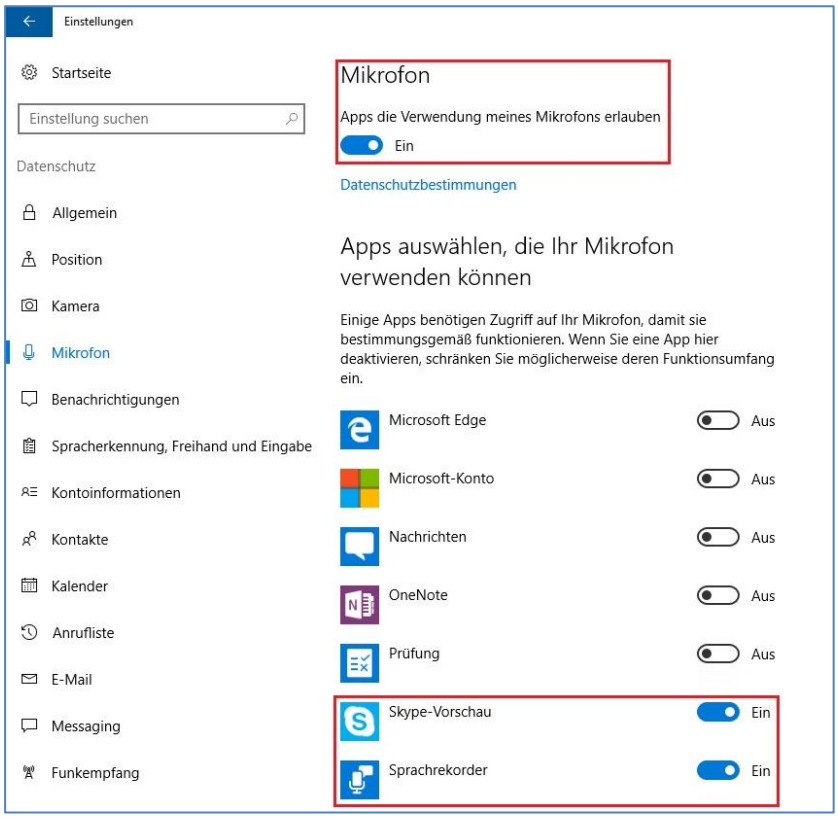

Abbildung 17: Datenschutzeinstellungen - Mikrofon

Benachrichtigungen

Diese Registerkarte unter den Datenschutz-Einstellungen ist neu nach dem Anniversary-Update. Hier verbirgt sich ein neues Feature, welches unter Android- oder iOS-Betriebssystemen schon längst gängig ist. Es ermöglicht z.B. anderen Geräten wie Smart-watches den Zugriff auf Benachrichtigungen des Action Centers.

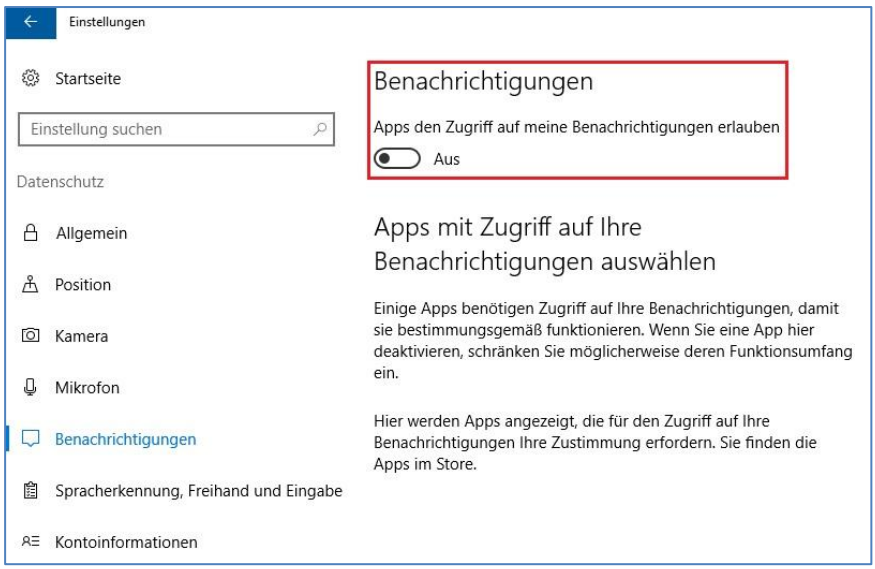

Abbildung 18: Apps den Zugriff auf Benachrichtigungen erlauben

Spracherkennung, Freihand und Eingabe

Hinter diesen drei Begriffen versteckt sich nichts Anderes als der digitale Assistent Cortana. Dieser ist bei einer Neuinstallation seit dem Anniversary-Update standardmäßig aktiviert, wenn er im Installationsvorgang nicht explizit deaktiviert wurde

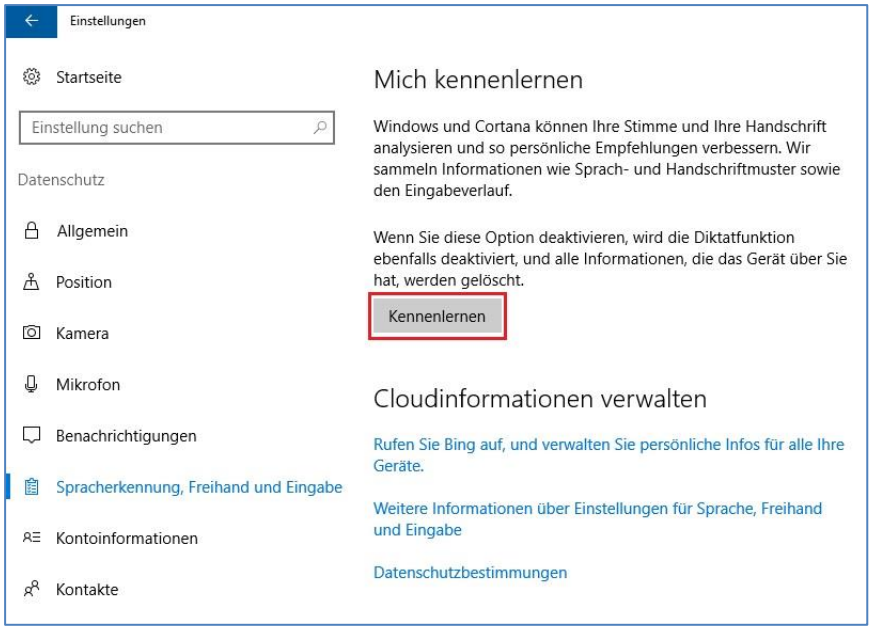

Abbildung 19: Datenschutzeinstellungen - Spracherkennung, Freihand und Eingabe

Sollte der Dienst aktiviert worden sein, so kann man ihn unter diesem Punkt wieder komplett deaktivieren („Kennenlernen beenden"). Dadurch wird jedoch auch die Diktierfunktion deaktiviert.

Die normale Sprach- und Texterkennung (wenn das Endgerät dazu geeignet ist) ist weiterhin verfügbar, auch offline. Es werden keine Daten an Microsoft übermittelt, „Lernen" ist dennoch möglich indem neue Wörter auf dem Gerät gespeichert werden.

Klickt man auf den Link „Rufen Sie Bing auf, und verwalten Sie persönliche Infos für alle ihre Geräte" gelangt man auf die Seite https://www.bing.com/account/personalization. Dort können die während der Nutzung von Cortana gesammelten und gespeicherten Informationen verwaltet und auch gelöscht werden.

Weitere Informationen zu Cortana finden sich unter dem Punkt „Cortana".

Kontoinformationen

An dieser Stelle besteht die Möglichkeit, Apps den Zugriff auf das eigene Konto zu erlauben oder zu verbieten. Dies bezieht sich auf den Fall, dass ein Microsoft-Konto verknüpft ist. Grundsätzlich wird empfohlen, den Zugriff auf Kontoinformationen auszuschalten.

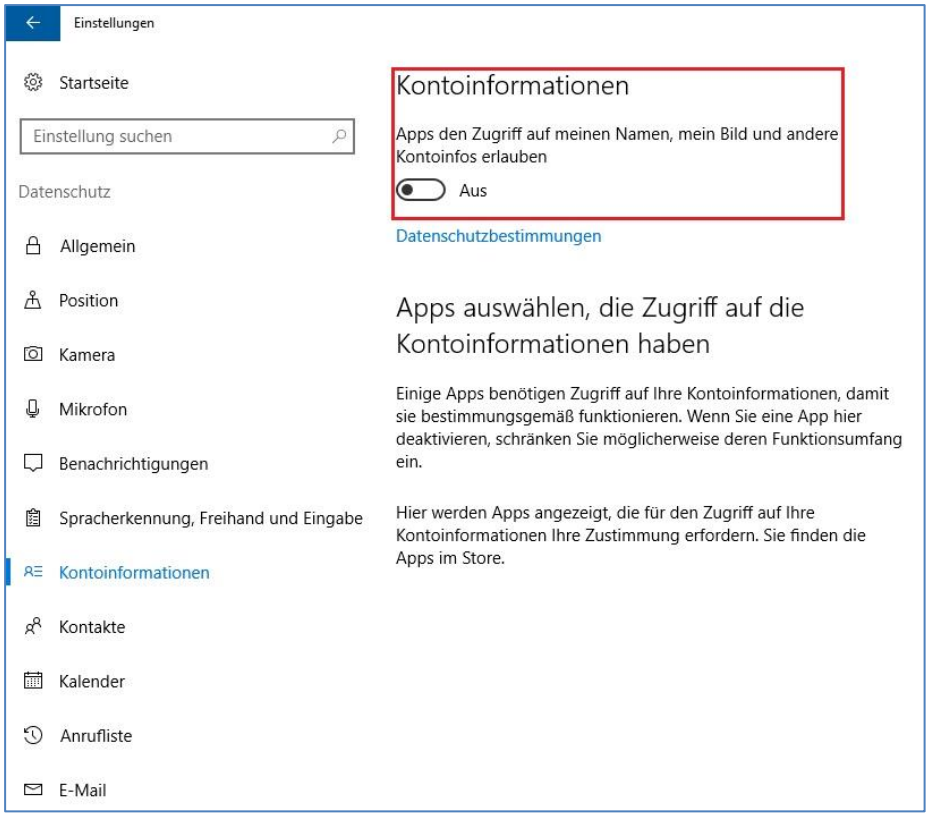

Abbildung 20: Datenschutzeinstellungen - Kontoinformationen

Kontakte und Kalender

An dieser Stelle besteht die Möglichkeit einzelnen oder allen Apps den Zugriff auf die Kontakte und Kalender zu erlauben oder zu verbieten. Hierbei ist zu überlegen, welche Apps für ihre Funktionalität tatsächlich den Zugriff benötigen.

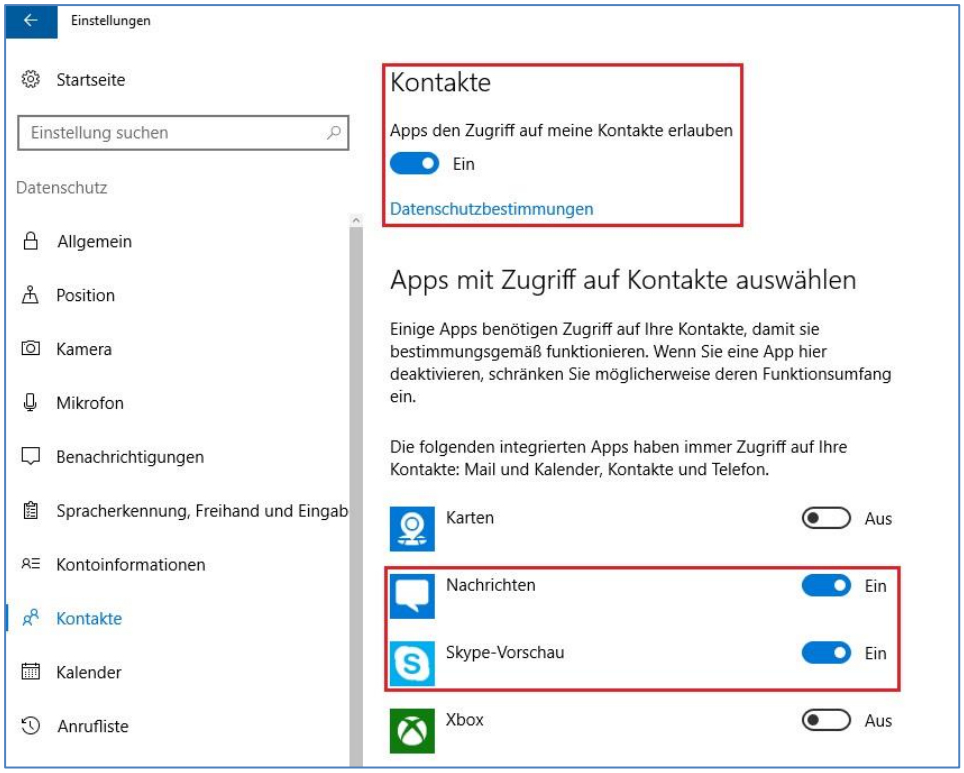

Abbildung 21: Datenschutzeinstellungen - Kontakte

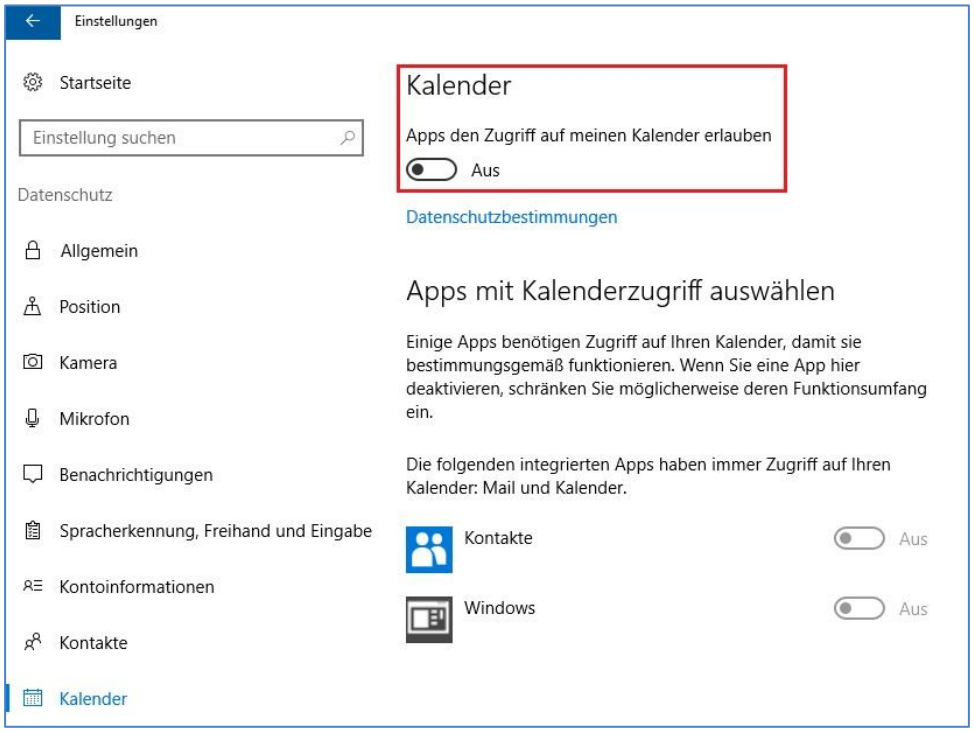

Abbildung 22: Datenschutzeinstellungen - Kalender

Anrufliste

Ist es möglich, mit einem Endgerät zu telefonieren, kann man unter dieser Einstellung einzelnen oder allen Apps den Zugriff auf die Anrufliste erlauben. Hierbei ist zu überlegen, welche Apps für ihre Funktionalität tatsächlich den Zugriff benötigen.

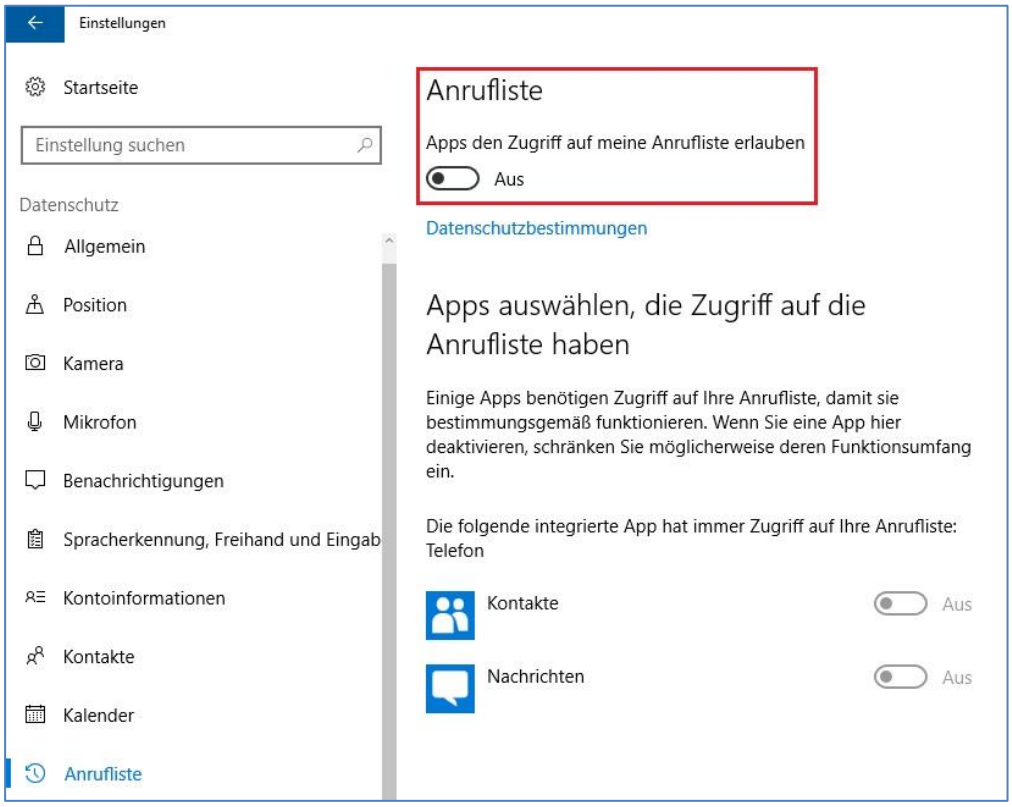

Abbildung 23: Datenschutzeinstellungen - Anrufliste

E-Mail

An dieser Stelle besteht die Möglichkeit einzelnen oder allen Apps den Zugriff und das Senden von E-Mails zu erlauben oder zu verbieten. Hierbei ist zu überlegen, welche Apps für ihre Funktionalität tatsächlich den Zugriff benötigen.

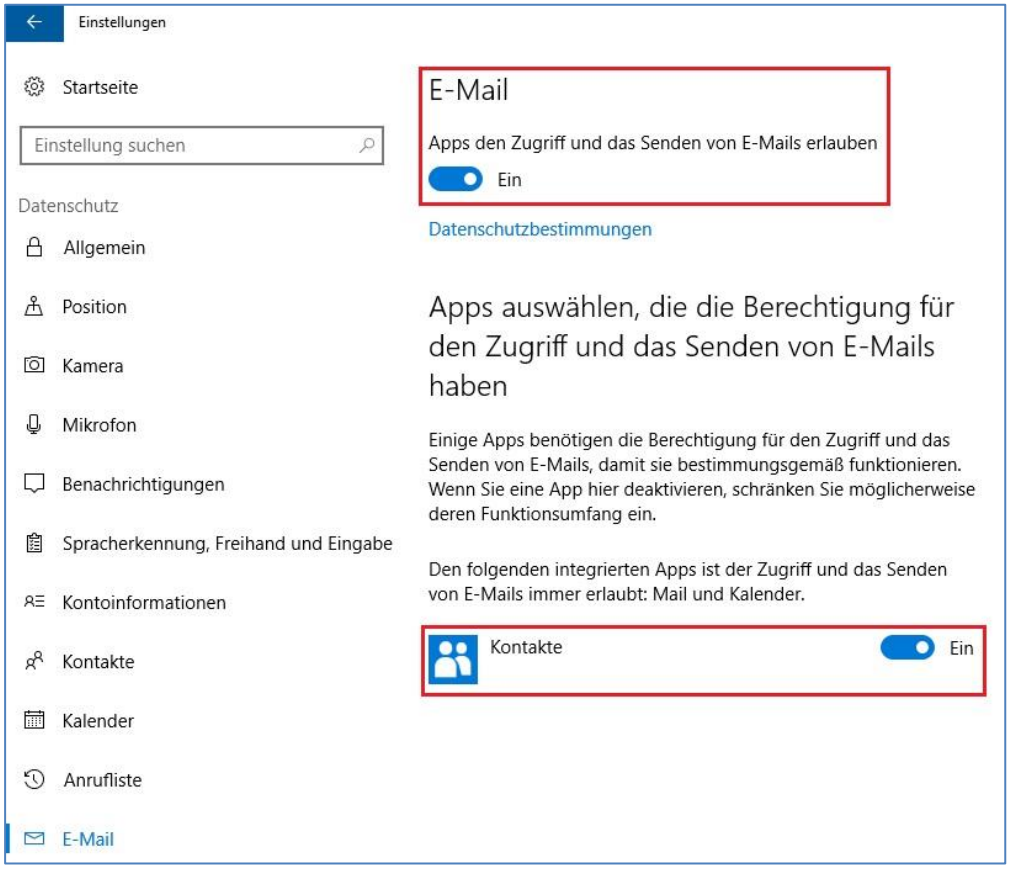

Abbildung 24: Datenschutzeinstellungen - E-Mail

Messaging und Funkempfang

An dieser Stelle besteht die Möglichkeit einzelnen oder allen Apps den Zugriff zur Messaging-Funktion und zur Funksteuerung zu erlauben oder zu verbieten. Hierbei ist zu überlegen, welche Apps für ihre Funktionalität tatsächlich den Zugriff benötigen. Es wird jedoch empfohlen, diese Funktionen abzuschalten.

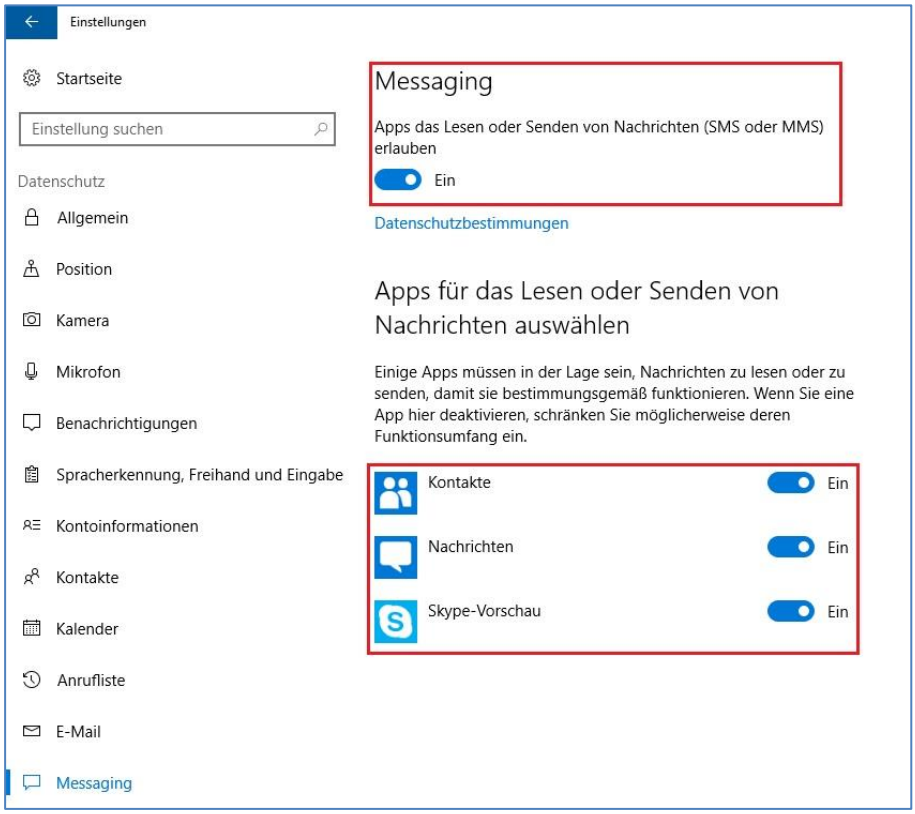

Abbildung 25: Datenschutzeinstellungen - Messaging

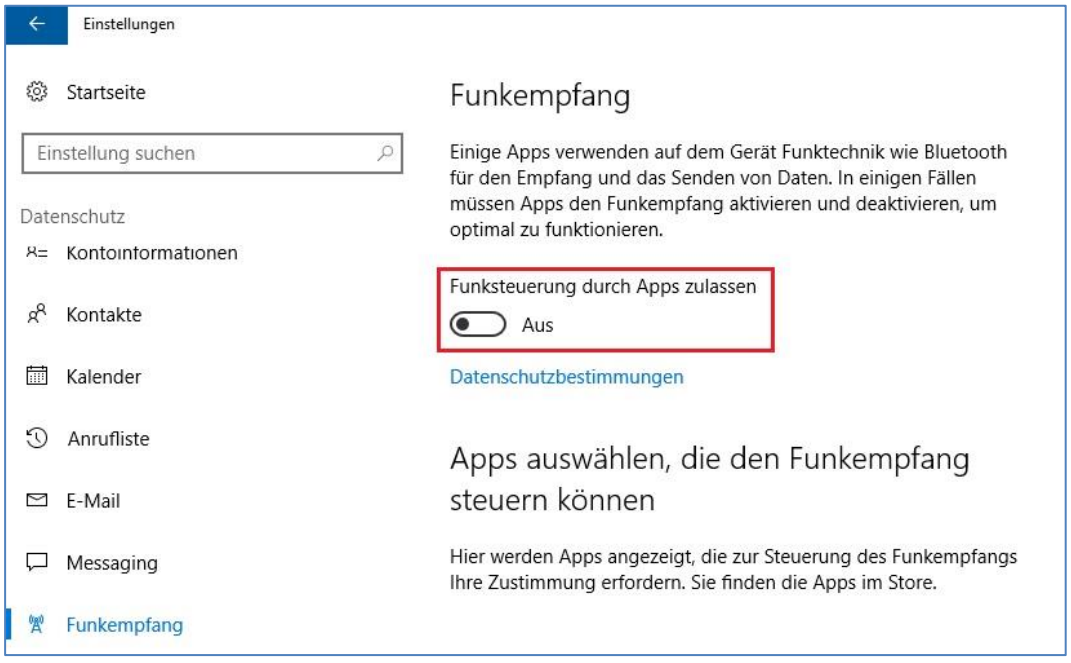

Abbildung 26: Datenschutzeinstellungen - Funkempfang

Weitere Geräte

Dieser Punkt ist nur relevant, wenn Windows 10 mit einem Microsoft-Konto verknüpft wird (NICHT empfohlen). Hier sollte die Synchronisation mit anderen Geräten deaktiviert werden, da so z.B. auch WLAN-Passwörter auf den Servern von Microsoft abgelegt werden.

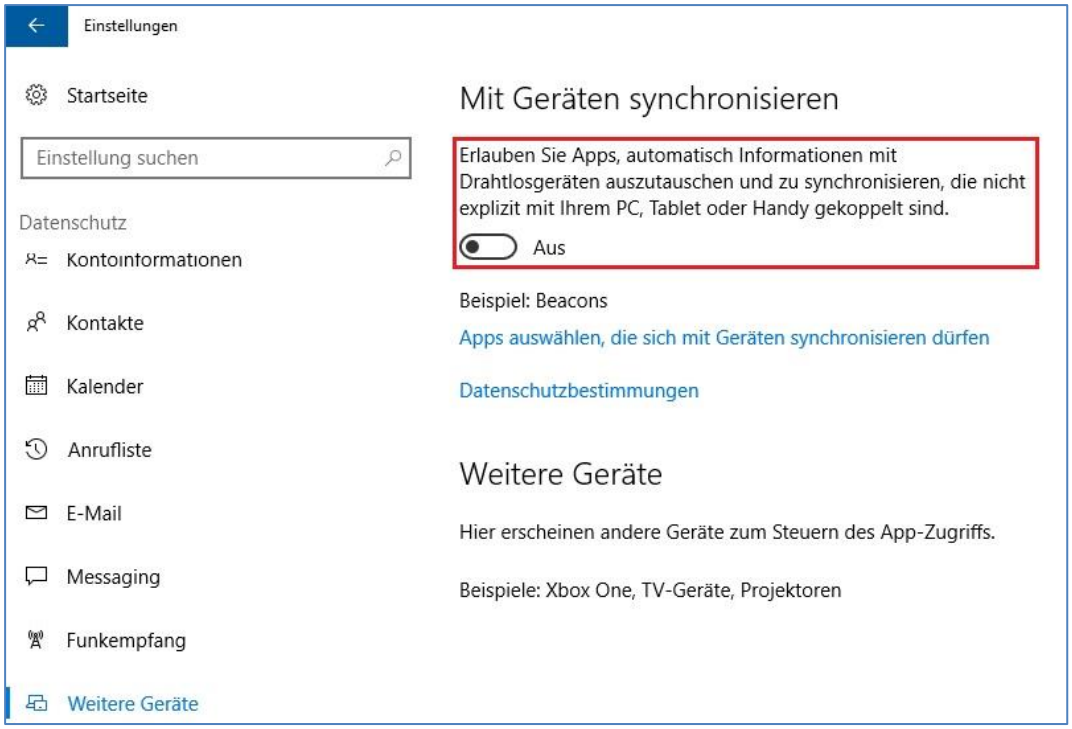

Abbildung 27: Datenschutzeinstellungen - weitere Geräte

Feedback und Diagnose

Dieser Abschnitt behandelt Telemetrie-Daten welche an Microsoft gesendet werden und anhand derer Microsoft dann z.B. Fehleranalysen durchführt. Informationen hierzu finden Sie im Kapitel „Telemetriedaten“.

WLAN-Optimierung

Die WLAN-Optimierung erlaubt es dem Anwender, sich automatisch mit in der Nähe befindlichen, bekannten und unverschlüsselten WLAN-Netzwerken zu verbinden. Diese bekannten Netzwerke verfügen nicht über einen Passwortschutz. Dazu zählen bspw. öffentliche Hotspots, welche mittels Crowdsourcing-Netzwerken einer breiten Masse bekannt gemacht werden. Die WLAN-Optimierung sammelt zudem Informationen über diese Netzwerke, bspw. ob diese über eine stabile Internetverbindung verfügen. Es ist jedoch zu beachten, dass die Nutzung der WLAN-Optimierung eine Anmeldung am verwendeten Gerät mit einem Microsoft-Benutzerkonto voraussetzt.

Diese Funktion von Windows 10 sollte in den Einstellungen deaktiviert werden. Bei zentral verwalteten Endgeräten, welche ins Unternehmensnetzwerk eingebunden sind, kann die WLAN-Optimierung mittels Gruppenrichtlinie deaktiviert werden.

Werden jedoch private Geräte verwendet (BYOD – Bring your own Device) sollte die WLAN-Optimierung explizit deaktiviert werden. Bei der Benutzung von WLAN 802.1X-Authentifizierung ist Wi-Fi-Sense grundsätzlich nicht nutzbar. Dies gilt ebenso für das Eduroam-Netzwerk.

Um zu verhindern, dass Dritte ein organisationseigenes, offenes Netzwerk automatisch mit der WLAN-Optimierung nutzen können, wird von Microsoft empfohlen „_optout“ an den Netzwerknamen des WLAN anzuhängen.

Weitere Hinweise zur WLAN-Optimierung finden sich in der Handlungsempfehlung „Datenschutzrechtliche Probleme bei der Einführung neuer Betriebssysteme - Eine Untersuchung am Beispiel Windows 10“ der Forschungsstelle Recht des DFN.

Hinweis „WLAN-Optimierung“

Seit dem „Anniversary Update“ (Windows 10 Version 1607) im Juli 2016, ist die Funktion zum Teilen sensibler Zugangsdaten für verschlüsselte WLANs mit Facebook-, Skype- und outlook.com-Kontakten nicht mehr verfügbar.

Cortana

Bei Cortana handelt es sich um den digitalen Assistenten, welcher in Windows 10 integriert ist und mit Siri (Apple) und Google Now (Google) verglichen werden kann. Im Gegensatz zu diesen Diensten ist Cortana aber auch auf Desktops und sogar für iPhone/iPad und Android-Smartphones verfügbar. Durch Synchronisation können Informationen auf mehreren Geräten abgerufen werden. Der Dienst kann per Text- und Spracheingabe gesteuert werden und liefert kontextabhängige und nutzerspezifische Informationen. Die Funktionalitäten von Cortana lassen sich durch die Installation weiterer Apps auch erweitern. So können bspw. Sprachgesteuerte Notizen erstellt werden (standardmäßig ist das diktieren von Texten noch nicht möglich) oder durch spezielle Fitness-Apps kann der Dienst auch als „Ernährungsberater" genutzt werden.

Cortana ist sehr tief in das System integriert und sammelt Daten aus verschiedenen Quellen und Diensten, speichert diese und wertet sie aus. So z.B. Sucherergebnisse (aus Bing), Kontakt- und Kalenderdaten, Inhalte von E-Mails, Browserverlauf, Sprach-Eingaben, Standorte, Daten aus Verzeichnissen (Bilder, Dokumente) u.a. Die Speicherung und Auswertung der Daten findet in der Microsoft-Cloud statt. Dies bedeutet, dass auch eine ständige Datenverbindung zu den Microsoft-Servern notwendig ist. Dabei muss davon ausgegangen werden, dass persönliche Daten übertragen und gespeichert werden. Bei Verwendung eines Code-Wortes zum „Wecken" von Cortana, hört dieser Dienst sogar ständig mit.

Cortana ist seit dem Anniversary-Update im Sommer 2015 standardmäßig aktiviert. Die Deaktivierung von Cortana (und auch der Websuche) ist nur noch über Umwege möglich (Windows 10 Home). Bereits in Betrieb gegangene Systeme sollten noch einmal dahin gehend geprüft werden, dass Cortana weiterhin deaktiviert ist.

Für die Nutzung von Cortana ist die Anmeldung mit einem Microsoft-Benutzerkonto nötig.

Weitere Hinweise zu Cortana finden sich in der Handlungsempfehlung „Datenschutzrechtliche Probleme bei der Einführung neuer Betriebssysteme - Eine Untersuchung am Beispiel Windows 10" der Forschungsstelle Recht des DFN.

Cortana in Unternehmen

Cortana ist auch für den Einsatz in Unternehmen konzipiert. Mit der Cortana Analytics Suite stellt Microsoft ein Business-Intelligence-Tool zur Verfügung, welches mit verschiedenen Daten-Quellen, auch in der Cloud, zusammenarbeitet und die Informationen den Anwendern bereitstellt. U.a. gibt es die Möglichkeit, Cortana Analytics mit Microsoft Azure oder Office 365 zu verbinden. Vor allem mit der Anbindung an Office 365 eröffnen sich neue Wege. Neben der Analyse von E-Mails und Kalendereinträgen, wird Cortana durch den Einsatz von Power BI für Office 365 zur Big Data-Lösung.

Für Anwender im Unternehmensbereich kann Cortana so u.a. bei der Planung von Reisen helfen, Termine des Tages anzeigen und auch benötigte Dokumente bereitstellen.

Die Steuerung von Cortana ist im Unternehmenskontext auch über Gruppenrichtlinien möglich. Hier lässt sich die Nutzung von Cortana auch direkt unterbinden.

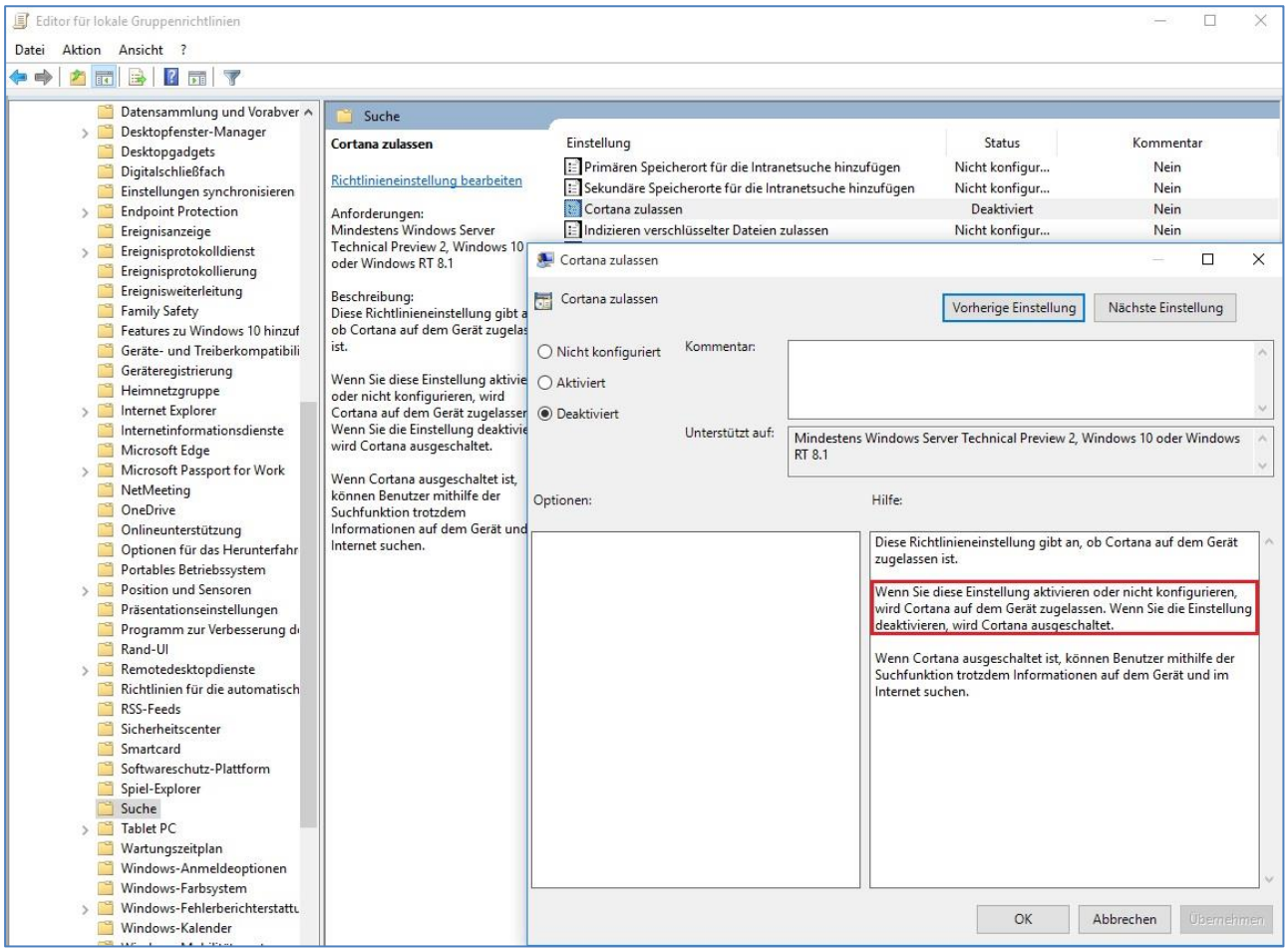

Abbildung 28: Gruppenrichtlinie - Deaktivierung Cortana

Nach der Ausführung von gpedit.msc findet man die Einstellungsoptionen unter *Computer-konfiguration\Administrative Vorlagen\Windows-Komponenten\Suche.*

Um Cortana vollständig auszuschalten muss es unter „Cortana zulassen" deaktiviert werden. Die Option „Nicht konfiguriert" ist nicht ausreichend, da mit dieser Einstellung noch Daten an Microsoft gesendet werden können.

Websuche

Windows 10 besitzt in der Taskleiste ein Suchfeld.

Bei Verwendung von Cortana ist dieses das Hauptwerkzeug des digitalen Assistenten.

Ist Cortana deaktiviert, besteht dennoch die Möglichkeit die Suche zu verwenden. Man kann sowohl den Rechner lokal durchsuchen nach Dateien oder Programmen als auch das Internet.

Für die Websuche wird die Suchmaschine Bing verwendet. Eine alternative Suchmaschine ist nicht einstellbar. Da nicht ausgeschlossen werden kann, dass die Suchverläufe an Microsoft übermittelt werden, wird empfohlen, die Websuche zu deaktivieren.

Dazu klickt man in das Suchfeld, woraufhin sich ein Fenster öffnet. Am linken Rand findet sich ein Zahnrad, welches die Einstellungen signalisiert. Dort hat man die Möglichkeit, die Funktion zu deaktivieren. Auch Cortana kann man auf diesem Weg aktivieren/deaktivieren.

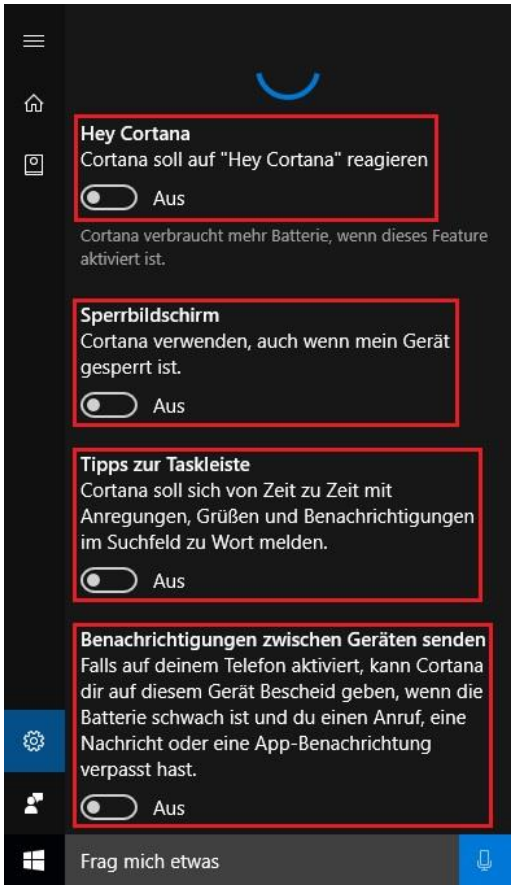

Abbildung 29: Websuche / Cortana (Übersicht 1)

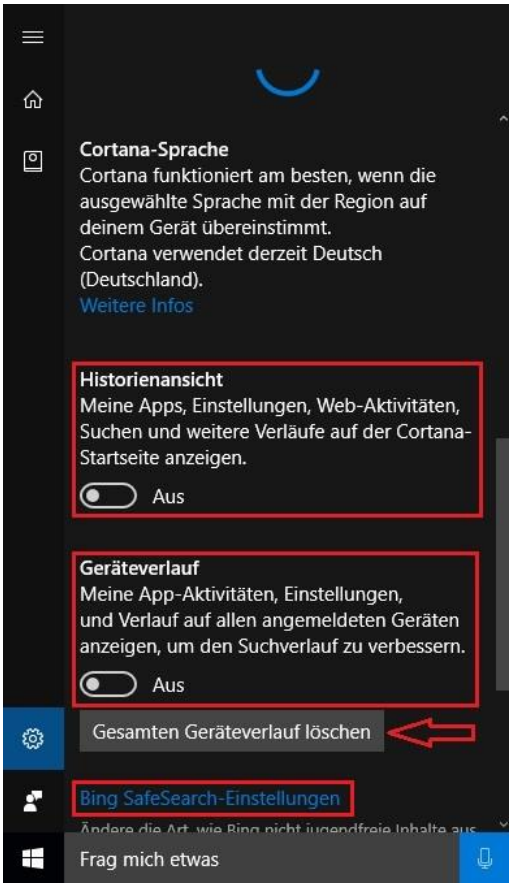

Abbildung 30: Websuche / Cortana (Übersicht 2)

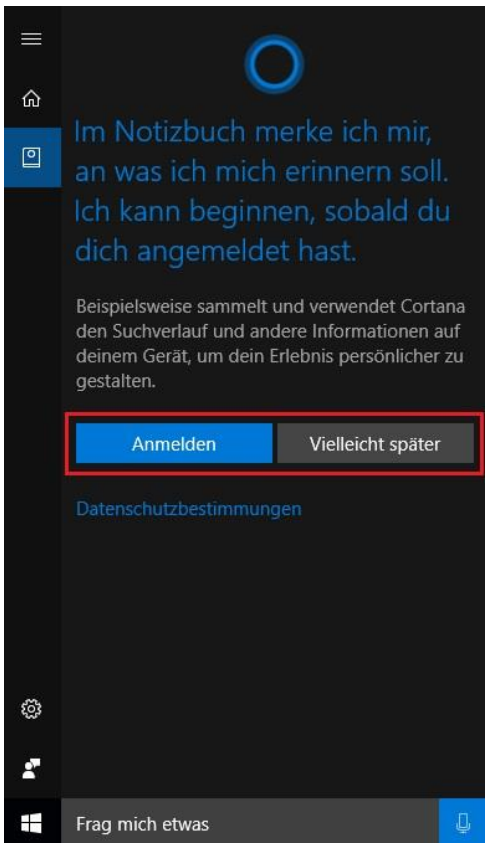

Abbildung 31: Websuche / Cortana (Übersicht 3)

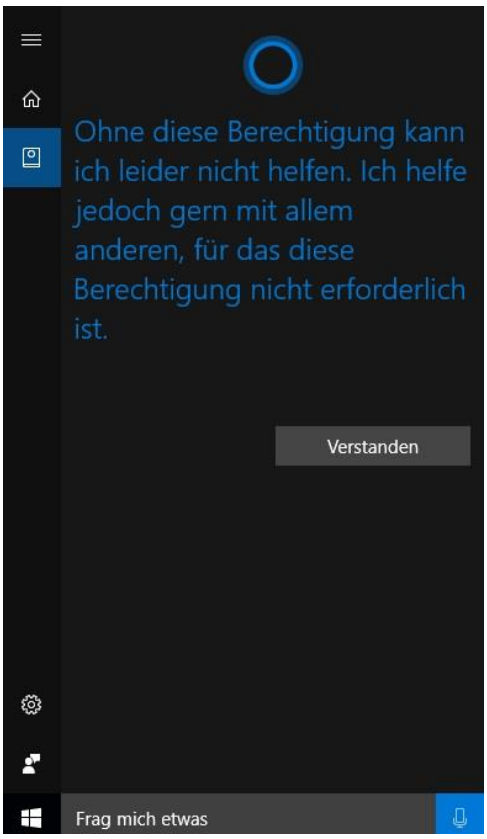

Abbildung 32: Websuche / Cortana (Übersicht 4)

In den ersten 4 Übersichten (Abbildung 29 – 32) sieht man das Konfigurationsmenü der Websuche, wenn Cortana aktiviert ist.

In der Übersicht 5 (Abbildung 33) ist Cortana deaktiviert.

Abbildung 33: Websuche / Cortana (Übersicht 5)

OneDrive

Bei OneDrive handelt es sich um den Microsoft-eigenen Cloud-Speicher, ähnlich der iCloud, Dropbox und GoogleDrive. Eine Verwendung als Client-Anwendung setzt die Anmeldung am Endgerät mit einem Microsoft-Benutzerkonto voraus. Als Web-Anwendung kann der Dienst aber ebenfalls genutzt werden.

Daten, welche in OneDrive abgelegt werden, werden weltweit in Microsoft-Rechenzentren gespeichert.

Während Privat-Anwender nicht über den Speicherort der Daten entscheiden können, ist es Unternehmens-Kunden möglich, die Speicherung von Daten in OneDrive Business auf europäischen Servern (Irland, Amsterdam) vertraglich zu vereinbaren. Für das 2. Halbjahr 2016 hat Microsoft zudem die Inbetriebnahme einer Deutschland-Cloud angekündigt. Dann ist es deutschen Unternehmens-Kunden auch möglich, die Speicherung der Daten in der deutschen Cloud vertraglich zu vereinbaren.

Wenn die Verwendung von OneDrive nicht vorgesehen ist, sollte die Anwendung in Windows 10 deaktiviert werden.

- Folgen Sie dem Pfad *Computerkonfiguration* > *Administrative Vorlagen* > *Windows-Komponenten* > *OneDrive;* Doppelklick auf *Verwendung von OneDrive für die Dateispeicherung* verhindern → **Aktivieren** und auf „Übernehmen" klicken

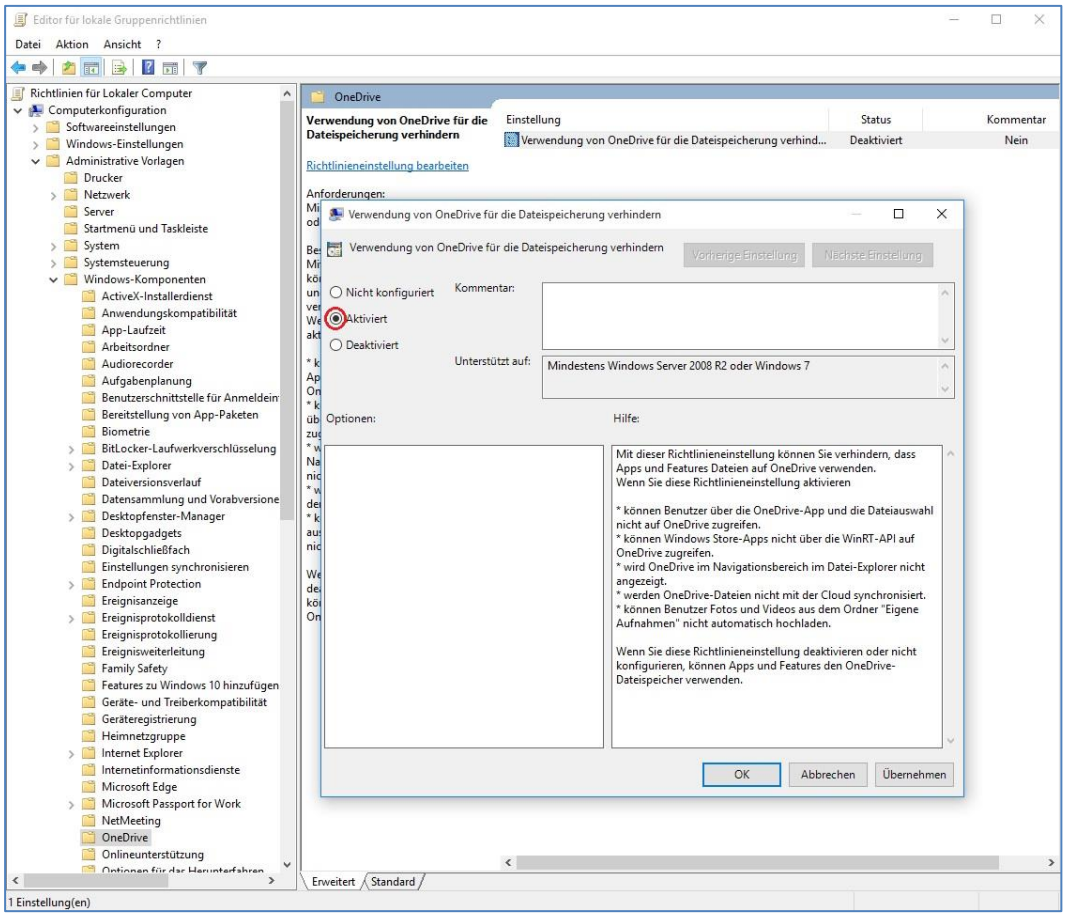

Abbildung 34: Gruppenrichtlinie - Verwendung von OneDrive für Dateispeicherung verhindern

Edge

In Windows 10 veröffentlicht Microsoft seinen neuen Browser Edge. Dieser ist der Nachfolger des bisher verwendeten Internet Explorers (aktuell: Version 11), wobei in Windows 10 beide parallel genutzt werden können. Gerade in der Anfangszeit sind noch nicht alle Webseiten Edge-kompatibel, weshalb man direkt aus dem neuen Browser heraus Seiten auch im Internet Explorer öffnen kann. Der Internet Explorer wird von Microsoft jedoch nicht mehr aktiv weiterentwickelt, der Support soll aber bis voraussichtlich Mitte 2020 aufrechterhalten werden. Edge ist der zukünftige Browser von Microsoft, dessen Entwicklung auch vorangetrieben wird. Bei einer Neuinstallation ist Edge bereits als Standard-Browser aktiviert. Bei Benutzung dieses Browsers sollten zu Beginn einige Änderungen in den Einstellungen vorgenommen werden. Über die drei Punkte im oberen Bereich des Browser können die Einstellungen aufgerufen werden. In dieser ersten Menü-Übersicht findet sich auch die Möglichkeit, direkt aus Edge heraus eine Webseite mit dem Internet Explorer zu öffnen.

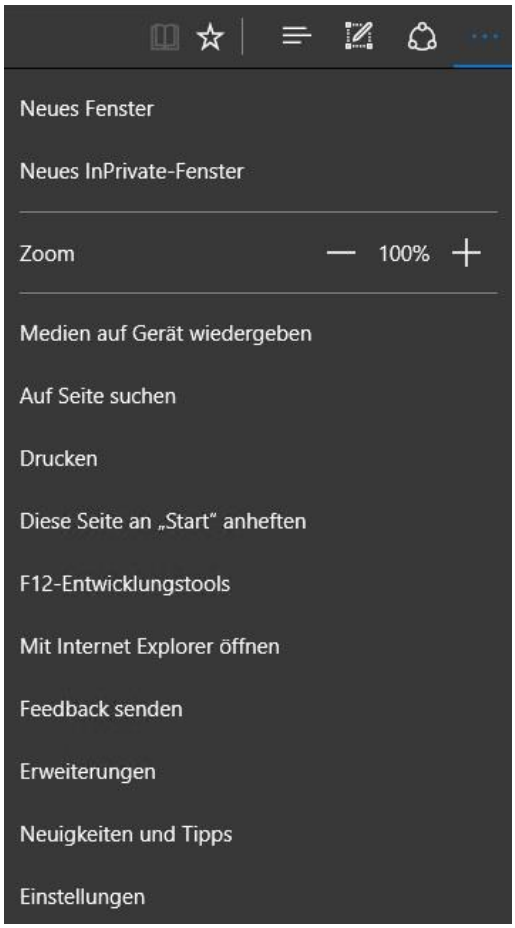

Abbildung 35: Edge - Menü

Im ersten Menü der Einstellungen können allgemeine Konfigurationen vorgenommen werden. Design (Farbe, Favoritenleiste) und Startverhalten (Startseite, neue Tabs) können nach eigenen Bedürfnissen gestaltet werden.

Bei der Konfiguration der Anzeige neuer Tabs gibt es verschiedene Auswahlmöglichkeiten. Empfohlen wird die Einstellung *Leere Seite.* Bei der Möglichkeit *Beste Websites* werden beliebte und häufig geklickte Websites, z.B. Amazon, Youtube oder Wikipedia, in Form eines Icons auf dem neuen Tab eingeblendet. Wird *Beste Websites und empfohlener Inhalt* ausgewählt, werden zusätzlich zu den Icons noch ausgewählte Inhalte von MSN, dem Microsoft-eigenen Nachrichten-Portal, eingeblendet. Diese werden von Microsoft an die eigenen Interessen angepasst indem das Browserverhalten analysiert wird. Dazu wird bspw. der Browserverlauf an Microsoft übermittelt. Ein wichtiger Punkt in diesem ersten Menü ist *„Browserdaten löschen" (siehe Unterpunkt „Browserdaten löschen).*

Durch einen Klick auf *Erweiterte Einstellungen anzeigen* gelangt man in ein weiteres Menü.

In diesem finden sich die für den Browser Edge wichtigsten Einstellungen zu Datenschutz und IT-Sicherheit.

Unter Punkt 1 (siehe Abbildung auf der nächsten Seite) sollte der Schieberegler auf „Ein" gestellt werden um Popups im Browser zu blockieren.

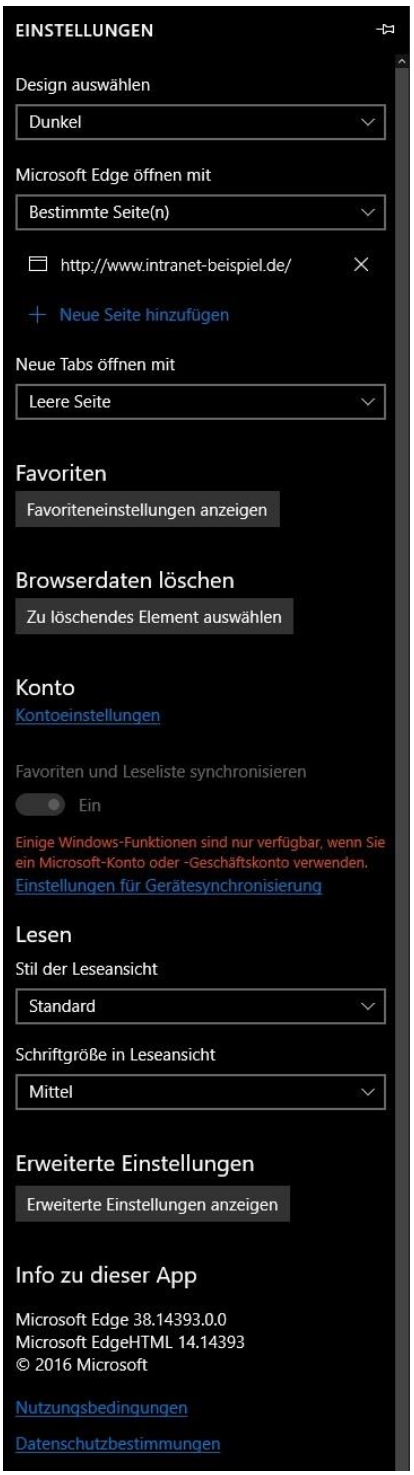

Abbildung 36: Edge - Übersicht der allgemeinen Einstellungen

Browserdaten löschen

Hier können Anwender Cookies, den Browserverlauf, den Browsercache aber auch den Downloadverlauf, Kennwörter und Formulardaten aus dem Browser löschen. Durch einen Klick auf „Mehr anzeigen" lassen sich weitere Daten auswählen, die gelöscht werden sollen. Zusätzlich gibt es die Möglichkeit, diese Daten nach jeder Sitzung zu löschen, indem man den Schieberegler auf „Ein" stellt.

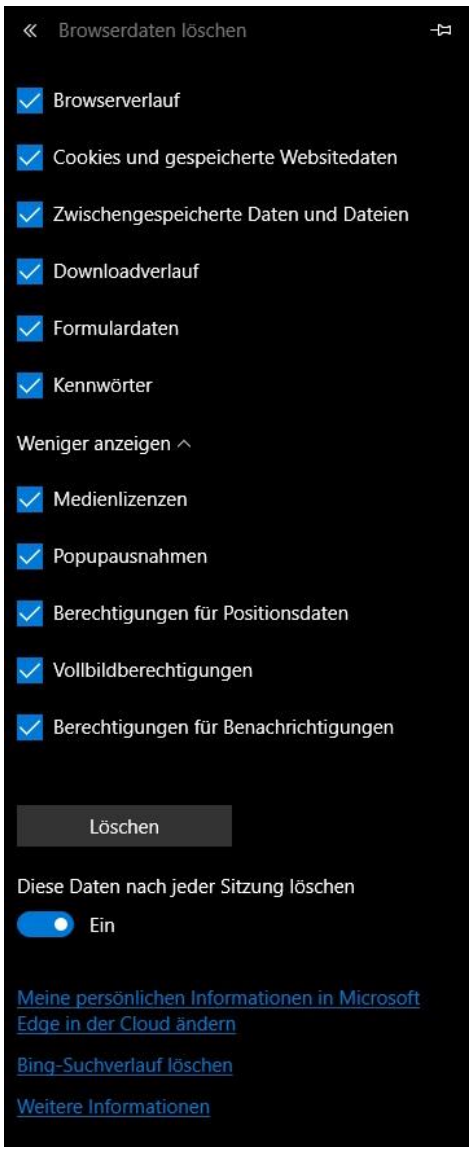

Abbildung 37: Edge - Browserdaten löschen

Aufgrund der ständig wiederkehrenden Probleme mit Sicherheitslücken im Adobe Flash Player sollte die Verwendung von diesem im Browser deaktiviert werden. Sollte er dennoch einmal benötigt werden, kann er temporär aktiviert werden.

Grundsätzlich nicht im Browser gespeichert werden sollten Kennwörter aller Art. Im Abschnitt *Datenschutz und Dienste* hat man die Möglichkeit, das Speichern von Kennwörtern und, ebenfalls empfohlen,von Formulareinträgen zu deaktivieren. Außerdem findet sich hier ein Link, über welchen bereits gespeicherte Einträge wieder gelöscht werden können.

Ebenso sollte die „Do-Not-Track"-Funktion aktiviert werden (Achtung: siehe weitere Infos unter dem Hinweis „Do-Not-Track-Funktion"). Dadurch wird besuchten Webseiten mitgeteilt, dass man zu Zwecken von personalisierter Werbung von Dritten nicht verfolgt werden möchte.

Cookies, zumindest von Drittanbietern, sollten blockiert werden. Normalerweise enthalten Cookies Informationen darüber, welche Webseiten ein Nutzer besucht hat. Es gibt jedoch auch Cookies, welche sehr tiefgehend das Internetverhalten protokollieren und die sehr willkürlich von Webseiten gesetzt wurden. Das Zulassen von Cookies sollte dementsprechend kritisch betrachtet werden. Einige Dienste jedoch, wie bspw. Do-Not-Track oder das Blockieren von personalisierter Werbung benötigen bzw. setzen jedoch Cookies für ihre Funktionalität.

Bei den weiteren Optionen ist besonders die Deaktivierung der Seitenvorhersage wichtig, da bei dieser sehr ausführlich das Internetverhalten analysiert wird. Die Aktivierung/Deaktivierung der beiden anderen ist optional.

Hinweis „Do-Not-Track"-Funktion

Bei Aktivierung der Do-Not-Track-Funktion wird im Browser ein Cookie gesetzt, welcher signalisiert, dass Aktivitäten nicht von Webseiten nachverfolgt werden sollen. Aus diesem Grund müssen Cookies (mit Ausnahme der Cookies von Drittanbietern) im Browser aktiviert werden.

Jedoch ist zu beachten, dass Microsoft ebenso wie viele andere Anbieter von Webseiten diese Funktion zur Zeit noch nicht unterstützt, da es bisher noch keine Einigung über die standardmäßige Interpretation des DNT-Signals gibt.

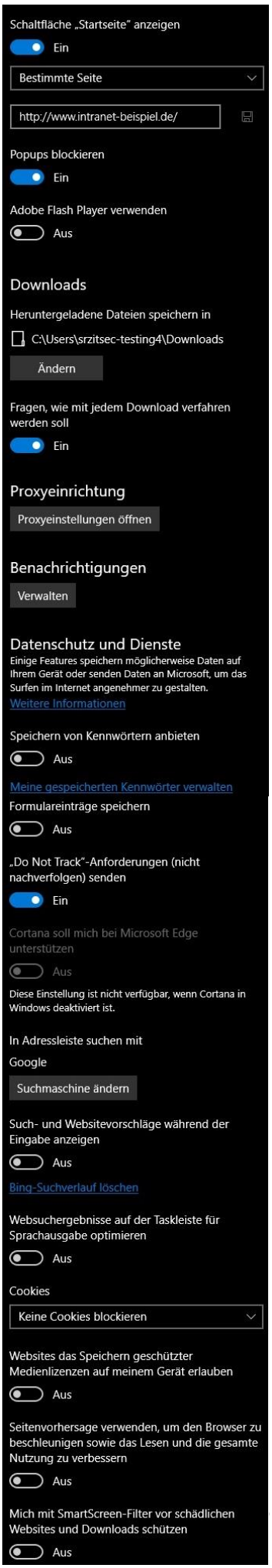

Abbildung 38: Edge - Übersicht der erweiterten Einstellungen

Suche in Edge

Eine weitere Neuerung im Browser Edge ist, dass es kein separates Suchfeld in der Menüleiste gibt. Die Suche erfolgt über die Adressleiste des Browsers.

Standardmäßig ist in Edge die Microsoft-eigene Suchmaschine Bing eingestellt. Da Bing jedoch auch Daten, z.B. Suchanfragen, an Microsoft übermittelt wird empfohlen, eine andere Suchmaschine auszuwählen. Es ist grundsätzlich empfehlenswert eine alternative Suchmaschine anzubieten.

Im Gegensatz zu anderen Browsern, auch dem alten Internet Explorer, sind jedoch keine weiteren Suchmaschinen verfügbar. Diese müssen erst angelegt werden.

Dazu sollte im Browser die entsprechende Suchmaschine (Google, DuckDuckGo, etc.) aufgerufen werden. In den erweiterten Einstellungen findet sich der Punkt „In Adressleiste suchen mit". Unter „Suchmaschine ändern" öffnet sich ein weiteres Untermenü. Dort ist nun die zuvor normal in Browser geöffnete Suchmaschine gelistet und kann als Standard ausgewählt werden.

Abbildung 39: Edge - Suchmaschine ändern 1

Erweiterungen (Add-ons) für Edge

Seit dem Anniversary Update gibt es ebenso wie für andere Browser auch für Edge verschiedene Erweiterungen. Diese müssen aus dem Windows Store heruntergeladen werden, was aber direkt aus dem Browser heraus geschehen kann.
Über das Edge-Menü gelangt man zu dem Punkt Erweiterungen. Dort kann man einsehen, ob bereits Erweiterungen installiert sind. Ebenso gibt es an dieser Stelle die Möglichkeit, neue Erweiterungen herunterzuladen. Dazu wird man zum Windows Store weitergeleitet. In diesem Fall ist keine Anmeldung am Store mit einem Microsoft-Konto nötig. Die Erweiterungen werden anschließend direkt im Browser installiert und können ggf. noch konfiguriert werden.

Abbildung 40: Edge - Erweiterungen

Änderung des Standard-Browsers

Wie auch bei der Suchmaschine, sollte dem Nutzer mindestens 1 alternativer Browser angeboten werden (weitere Hinweise zum Browser Edge finden sich in der Handlungsempfehlung „Datenschutzrechtliche Probleme bei der Einführung neuer Betriebssysteme - Eine Untersuchung am Beispiel Windows 10" der Forschungsstelle Recht des DFN).

Die Möglichkeit, einen alternativen Browser als Standardbrowser auszuwählen findet sich in den Einstellungen der Standardprogramme.

Durch Eingabe des Begriffes *Standardprogramme* in das Suchfeld der Taskleiste (schon beim Eintippen wird eine Liste von Vorschlägen angezeigt, aus der man auswählen kann), gelangt man zur entsprechenden Konfigurationsseite.

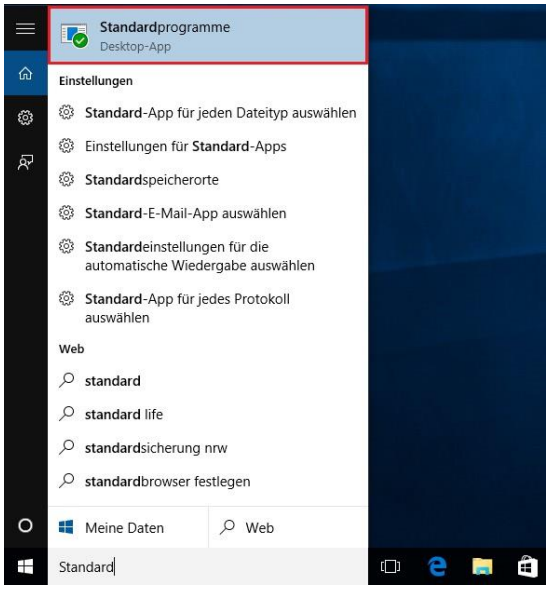

Abbildung 41: Edge - Standardbrowser ändern 1

Als nächstes wählt man den Punkt *Standardprogramme festlegen* aus.

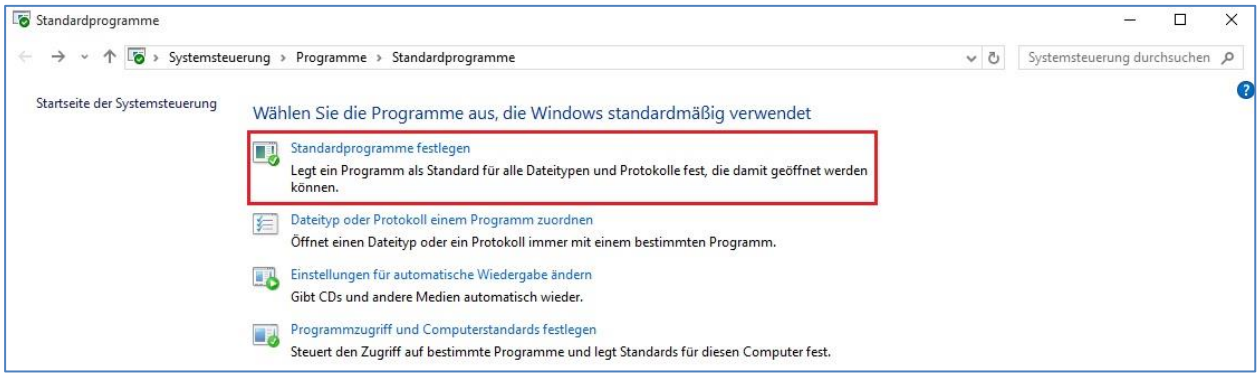

Abbildung 42: Edge - Standardbrowser ändern 2

Links in der Programmliste wählt man den Browser aus, der als Standard eingesetzt werden soll, und klickt auf *Dieses Programm als Standard festlegen.* Anschließend bestätigt man durch einen Klick auf *OK* worauf sich die Ansicht wieder schließt.

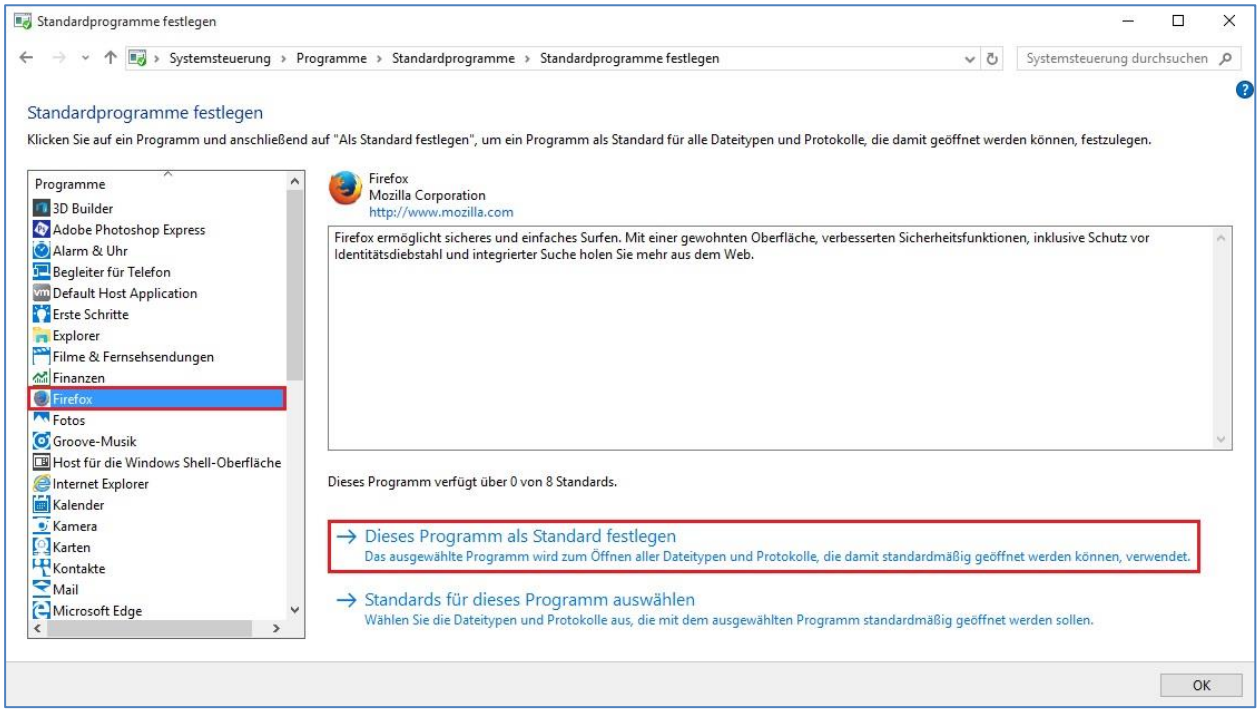

Abbildung 43: Edge - Standard-Browser ändern 3

Apps / Windows Store

Die Anmeldung im Store ist derzeit nur mit einem Microsoft-Benutzerkonto möglich. Dies ist auch nur im Store möglich, ohne direkte Anmeldung mit einem Microsoft-Benutzerkonto am Gerät.

Seit Ende 2015 gibt es neben dem Windows Store auch einen Windows Store for Business für Unternehmenskunden. Hier ist sowohl die Anmeldung mit einem Microsoft-Benutzerkonto als auch mit einem Microsoft-Geschäftskonto möglich.

Microsoft hat für den Business Store eine Offline Lizenzierung angekündigt, die es unter anderem ermöglichen soll, Volumenlizenzen für Apps zu erwerben.

Zum jetzigen Zeitpunkt ist dieses Modell jedoch noch nicht verfügbar.

Wenn im Unternehmen der Windows Store und Apps eingesetzt werden sollen, ist der Business Store mit Offline Lizenzierung aus Datenschutzgründen am ehesten zu empfehlen.

Bei der Verwendung von Apps können diesen über die Benutzeroberfläche Zugriffsrechte gegeben und entzogen werden. Dies kann in den Datenschutz-Einstellungen unter den jeweiligen Unterpunkten für jede einzelne App verwaltet werden, z.B. ob Zugriff auf Kontakte, Kalender, Mikrofon, Standort usw. gestattet werden soll.

Des Weiteren kann man einstellen, ob Apps Benachrichtigungen schicken können und ob diese bspw. auf dem Sperrbildschirm angezeigt werden können. Empfohlen wird, diese Funktionalitäten zu deaktivieren.

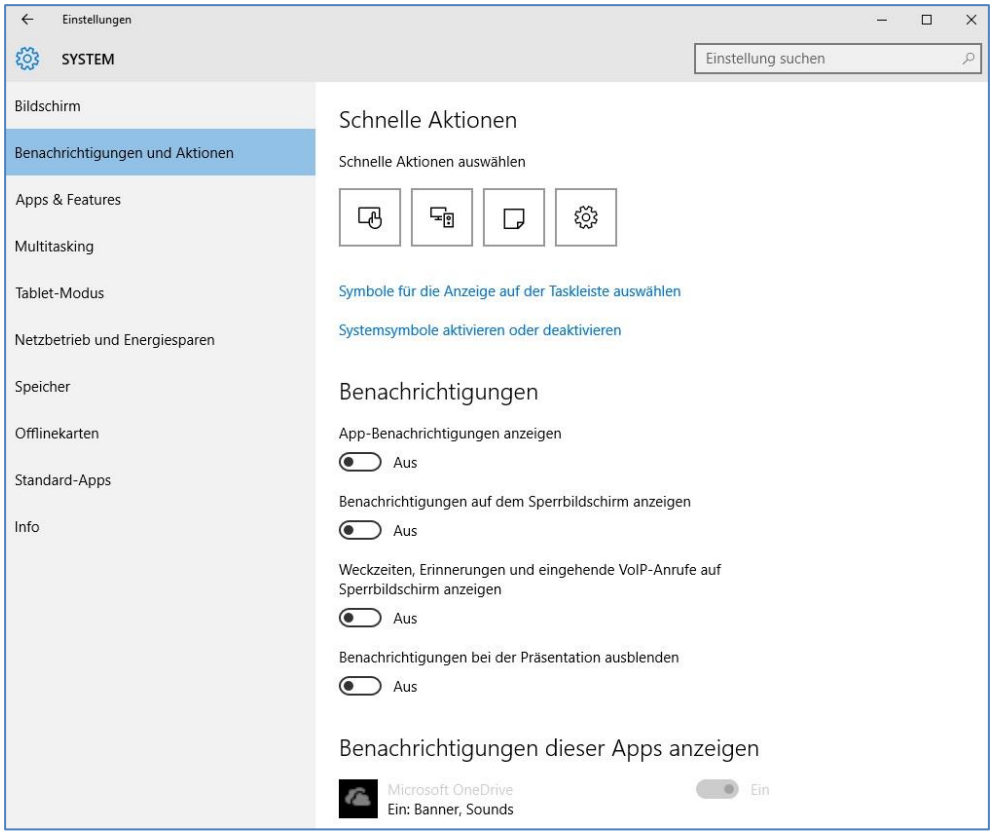

Abbildung 44: App-Benachrichtigungen deaktivieren

Windows Update

Dass Microsoft mit Windows 10 ein neues Betriebssystem-Konzept verfolgt, spiegelt sich auch beim Thema Updates wieder.

Nichts geändert hat sich bei den Sicherheitspatches, welche nach wie vor einmal monatlich erscheinen. Neu dagegen ist, dass neue Funktionalitäten und Dienste mit ihrer Fertigstellung veröffentlicht werden und sofort verfügbar sind. Während „große" Updates früher in Form von Service Packs oder komplett neuen Windows-Versionen veröffentlicht wurden, wird dies nun regelmäßig zwei- bis dreimal jährlich geschehen in Form von Funktions-Updates. Das erste dieser Updates für Windows 10 erschien im November 2015 unter dem Namen „Treshold".

Außerdem gibt es Neuerungen in der Update-Politik. Häufig wird damit das sognannte „Zwangsupdate" in Verbindung gebracht. Alle Windows 10-Installationen werden nun regelmäßig automatisch upgedatet. Allerdings unterscheiden sich die verschiedenen Windows-Editionen im Hinblick auf die Beeinflussung des Update-Zeitpunkts recht stark voneinander. Damit verfolgt Microsoft das Ziel, dass alle Endgeräte sich auf der gleichen, aktuellsten Version und dem gleichen, aktuellen Update-Level befinden. Aus Sicht der IT-Sicherheit ist dies eine recht gute Maßnahme.

Es ist wichtig zu wissen, dass zumindest ein Updated im „Current Branch"-Ring, bereits einige Monate im Umlauf ist und ausgiebig getestet wurde, so dass die Fehleranfälligkeit nur noch sehr gering ist. In der folgenden Abbildung ist die Windows 10-Update-Verteilung von Microsoft dargestellt. Anhand dieser soll verdeutlicht werden welche Windows 10-Nutzer zu welchem Zeitpunkt Updates bekommen.

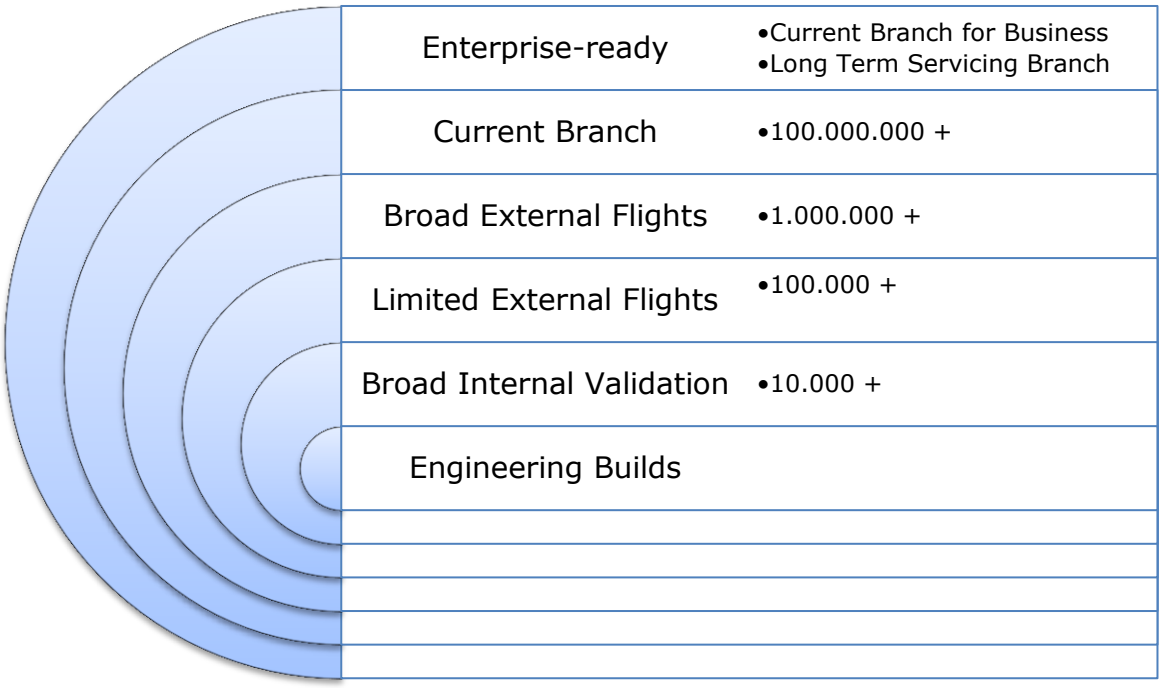

Abbildung 45: Update-Verteilringe

Im ersten und zweiten Ring („Engineering Builds" und „Broad Internal Validation") werden neue Funktionsupdates direkt nach ihrer Fertigstellung Microsoft-Intern verteilt und getestet, d.h. zuerst die Entwickler, anschließend alle Mitarbeiter von Microsoft. Der dritte und vierte Ring („Limited External Flights" und „Broad External Flights") entspricht dem

Windows-Insider-Progamm. Das Update ist dann bereits seit ca. 4 bis 6 Monaten im Umlauf, bevor es diese Ringe erreichen. Erst dann, im 5. Ring („Current Branch") und somit frühestens 4 Monate nach Veröffentlichung, wird das Update an Nutzer von Windows 10 Home sowie Pro verteilt. Während Home-Nutzer den Update-Vorgang kaum beeinflussen können, haben die Nutzer der Pro-Edition wenigstens die Möglichkeit, den Update-Zeitpunkt auf einen bestimmten Wochentag und eine bestimmte Uhrzeit zu legen.

In der Unternehmens-Infrastruktur jedoch, in der Betriebssysteme häufig in stabilen Umgebungen laufen müssen, kann dieses Windows-Update-Modell zu Problemen führen, insbesondere bei fehlerhaften Updates. Hier gibt es zum einen die Möglichkeit, lokale Verteilringe zu definieren und das Update zeitverzögert zu installieren. So kann der erste Verteilring auch als Testumgebung fungieren um dort das Update zuerst auszurollen. Wichtig in diesem Zusammenhang ist, die betroffenen Rechner zu kategorisieren und ggf. zu priorisieren (Beispielkriterien: ein Rechner mit hoher benötigter Verfügbarkeit sollte in einen der letzten Verteilringe/ Rechner zum Recherchieren in der Bibliothek können in einen der ersten Verteilringe). Rechner gleicher Kategorie/Priorität sind in einem Verteilring zusammenzufassen. Eine weitere Möglichkeit, die sich Nutzern von Pro-, Education- und Enterprise-Editionen von Windows 10 bietet, ist die optionale Verwendung des Current Branch for Business. Die Funktions-Updates werden hier nochmals ca. vier Monate später ausgeliefert als beim einfachen Current Branch. Während hier für Nutzer der Pro-Edition die gleichen Bedingungen für den Installationszeitraum gelten wie beim Current Branch, können Enterprise- und Education-Nutzer statt des Windows Updates die Windows Server Update Services (WSUS) nutzen. Dies ermöglicht eine zeitliche Verzögerung des Updates um weitere 8 Monate (d.h. in dieser Variante kann man ein Update bis zu 16 Monate hinauszögern, wenn man am Insiderprogramm teilnimmt und das Update entsprechend eher bekommt).

Besonders kritische Bereiche sollten mit Windows 10 Enterprise LTSB (Long Term Servicing Branch) betrieben werden. Dort gibt es zwar ebenfalls regelmäßig Sicherheitsupdates und auch die Funktionsupdates sind verfügbar, letztere müssen jedoch erst spätestens nach 10 Jahren eingespielt werden. Microsoft wird aber regelmäßig nach großen Funktions-Updates ein neues LTSB-Build, d.h. einen jeweils aktuellen Snapshot für diese Version bereitstellen. Einige Dienste, wie Cortana, OneDrive oder der Windows Store sind für diese Version nicht verfügbar. Der garantierte Support für Windows 10 Enterprise LTSB beträgt 10 Jahre.

Was alle Editionen gemeinsam haben, ist, dass bei versäumtem Einspielen der Updates innerhalb der Maximalgrenzen der Support von Microsoft für die Windows 10-Installation eingestellt wird.

In den nachfolgenden Abbildungen (Testsystem: Windows 10 Enterprise, Stand-Alone-Installation) ist die Konfiguration des Windows Updates in der Benutzeroberfläche dokumentiert.

Auf der ersten Seite kann der Neustart-Zeitpunkt nach dem Update angegeben werden. Außerdem bekommt man Informationen, welche Updates verfügbar sind.

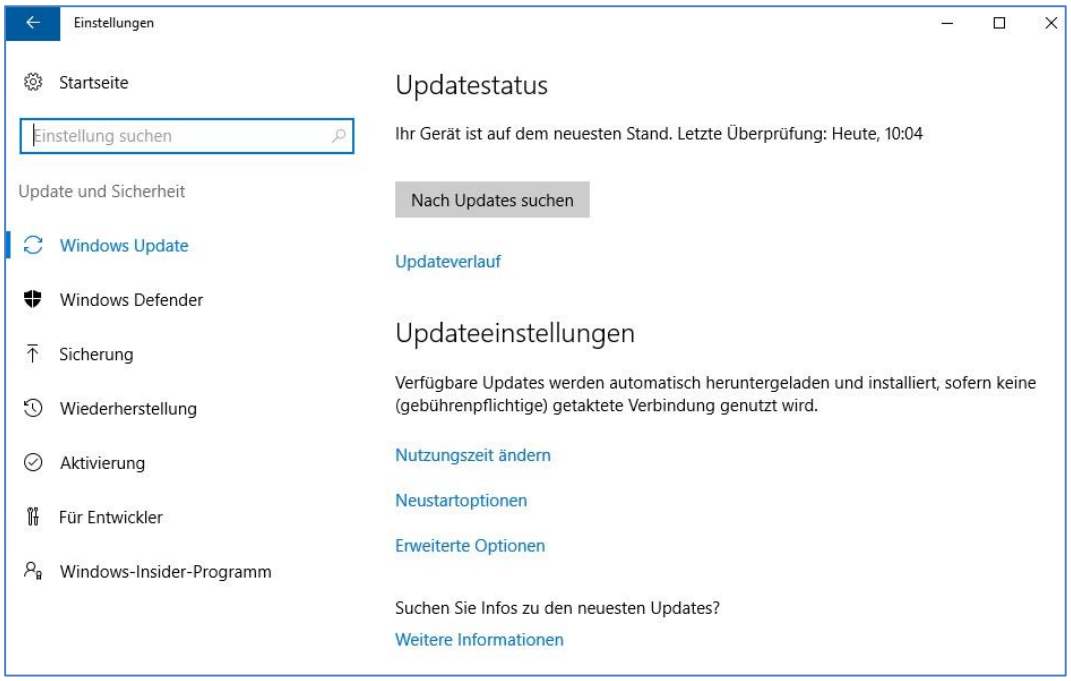

Abbildung 46: Windows-Update - allgemein

Am Ende der Seite gelangt man über einen Link zu den Erweiterten Optionen.

Dort gibt es die Möglichkeit, Updates für weitere Microsoft-Produkte, wie z.B. Office zu laden oder bestimmte Upgrades für einige Zeit zurückzustellen (falls es bspw. Probleme bei der Installation gab und diese rückgängig gemacht wurde). Für weitere Microsoft-Produkte kann diese Funktion deaktiviert werden, da es sich in der Regel nicht um sicherheitsrelevante Updates handelt. Der zweite Punkt ist optional wählbar.

Des Weiteren kann man sich an dieser Stelle für das Windows Insider Programm anmelden.

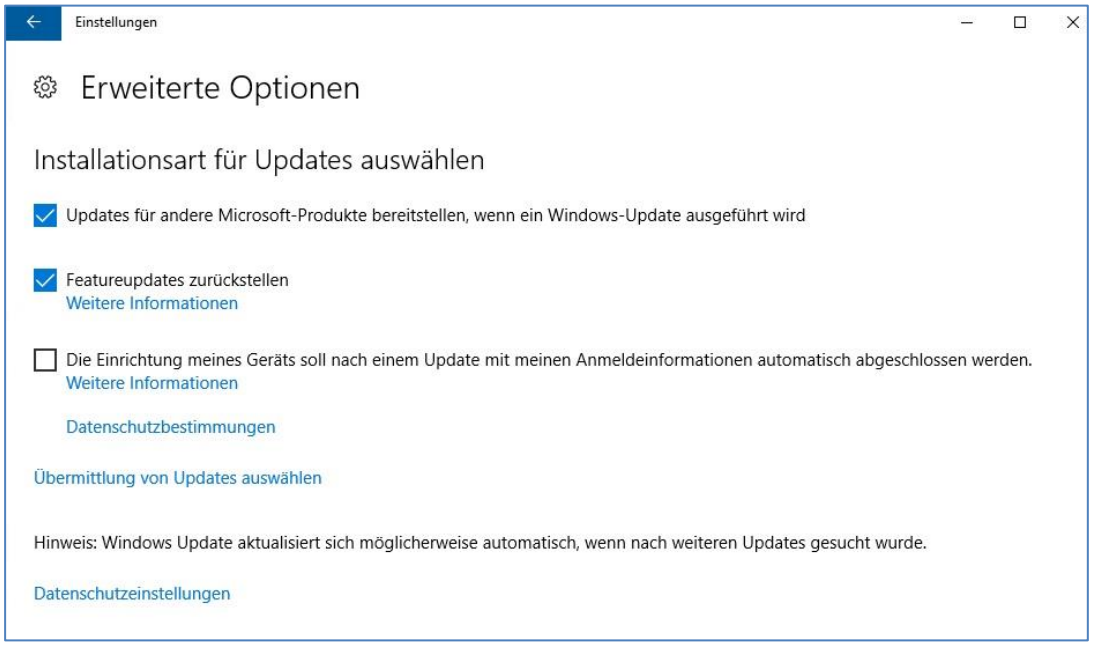

Abbildung 47: Windows Update - erweiterte Optionen

Hinter dem Link „Übermittlung von Updates auswählen“ verbirgt sich noch eine wichtige Einstellung.

Updates können, um die Server von Microsoft zu entlasten, auch von anderen Geräten, welche das Update bereits erhalten haben, heruntergeladen werden. Dabei handelt es sich um Geräte, welche in einem lokalen Netzwerk oder übers Internet über eine P2P-Verbindung verfügen. Hier liegt die Gefahr, dass bspw. manipulierte Updates geladen werden. Diese Option sollte umgehend deaktiviert werden.

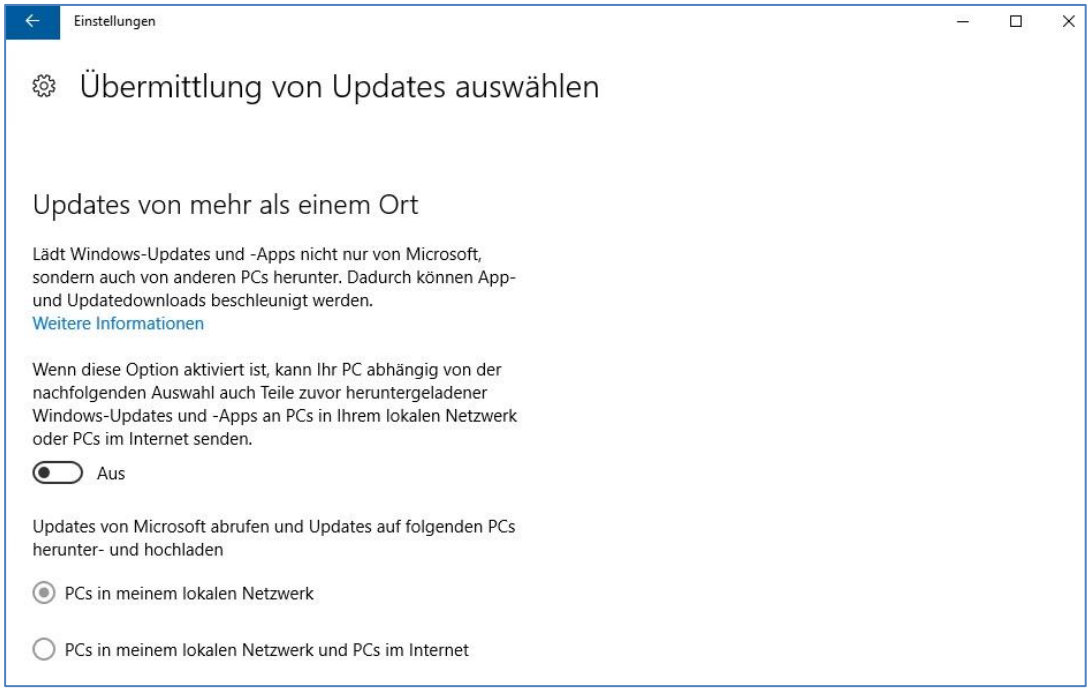

Abbildung 48: Windows Update - Updates von anderen Orten

Windows Defender

Für den Fall, dass ein Anwender keinen separaten Virenschutz installiert hat, sollte der Echtzeitschutz des Windows Defenders aktiviert werden.

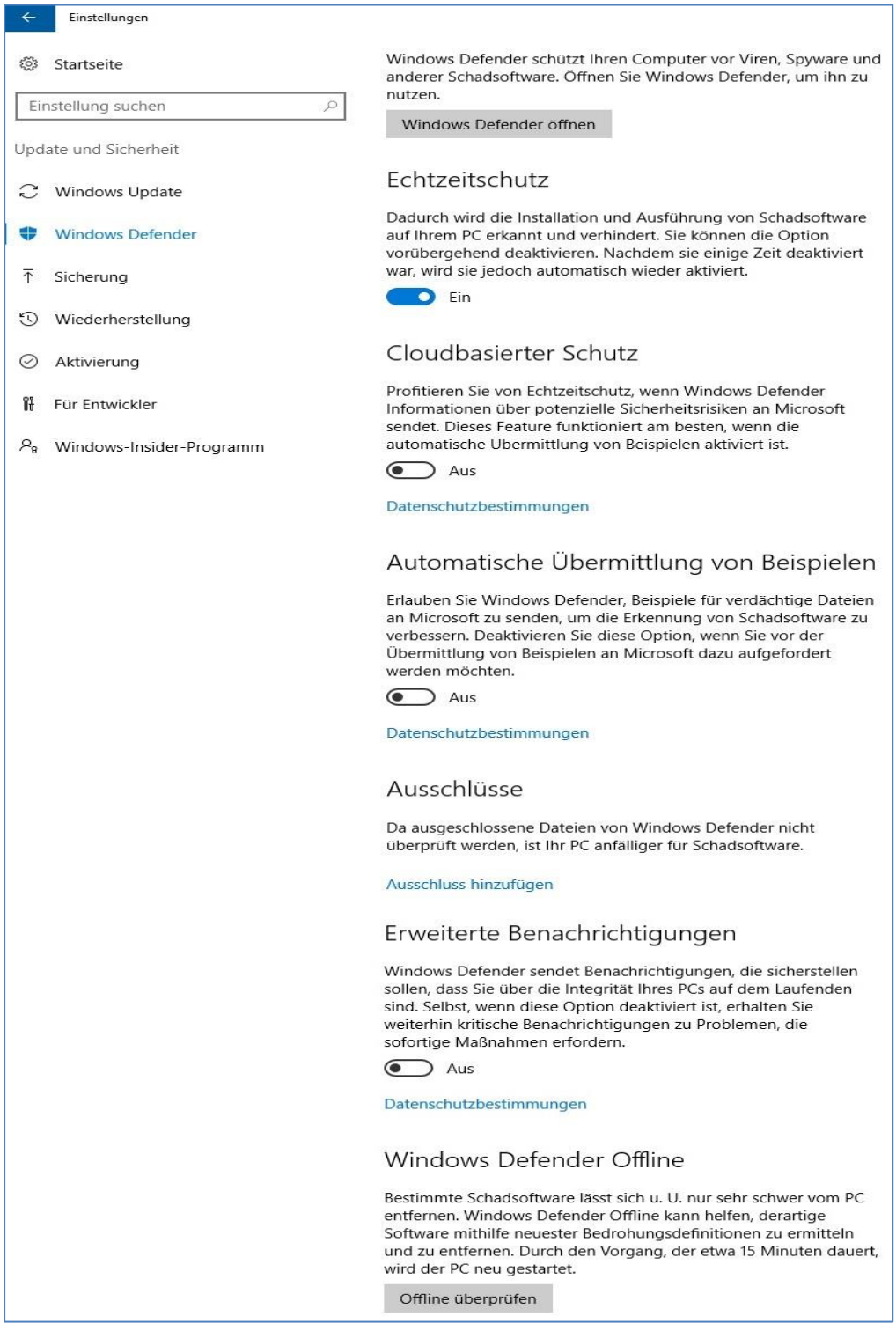

Abbildung 49: Einstellungen Windows Defender

Die Aktivierung des Cloudbasierten Schutzes ist optional. Eine Übermittlung von gefundenen Sicherheitsproblemen an Microsoft kann bei der Weiterentwicklung und Optimierung des Windows Defenders hilfreich sein.

Die Aktivierung des SmartScreen-Filters wäre in diesem Fall ebenso empfehlenswert.

Dennoch wird der Einsatz eines separaten Virenscanners empfohlen. Der Einsatz des Windows Defender ist nur im privaten Gebrauch von Windows 10-Geräten vertretbar.

Neuerungen ab Windows 10 Version 1607 – Anniversary Update

Der Windows Defender wurde mit dem Anniversary Update erweitert. Für die Enterprise-, Education- und Pro-Editionen gibt es nun auch eine Advanced Thread Protection. Diese dient dem verhaltensbasierten, cloud-gestützten Erkennen von fortschrittlichen Angriffen und Schadsoftware.

Zusätzlich ist der Defender nun auch mit einem Offline-Modus ausgestattet, so dass ein Gerät auch ohne Netzwerkverbindung gescannt werden kann.

Eine weitere Neuerung ist die Windows Information Protection, welche ebenfalls nur den oben genannten Editionen zur Verfügung steht. Diese dient dem Schutz vor unbeabsichtigtem Datenverlust. Sie ermöglicht es

Telemetriedaten

Um zu unterbinden, dass Microsoft regelmäßig Feedback anfordert und Diagnose- und Nutzungsdaten auswertet, müssen unter diesem Punkt die Einstellungen angepasst werden. Die Feedback-Anforderung sollte auf „Nie" gesetzt werden. Bei den Diagnose- und Nutzungsdaten ist dies in der Home-Edition von Windows 10 nicht möglich. Hier sollte dafür die Einstellung auf „einfach" gesetzt werden.

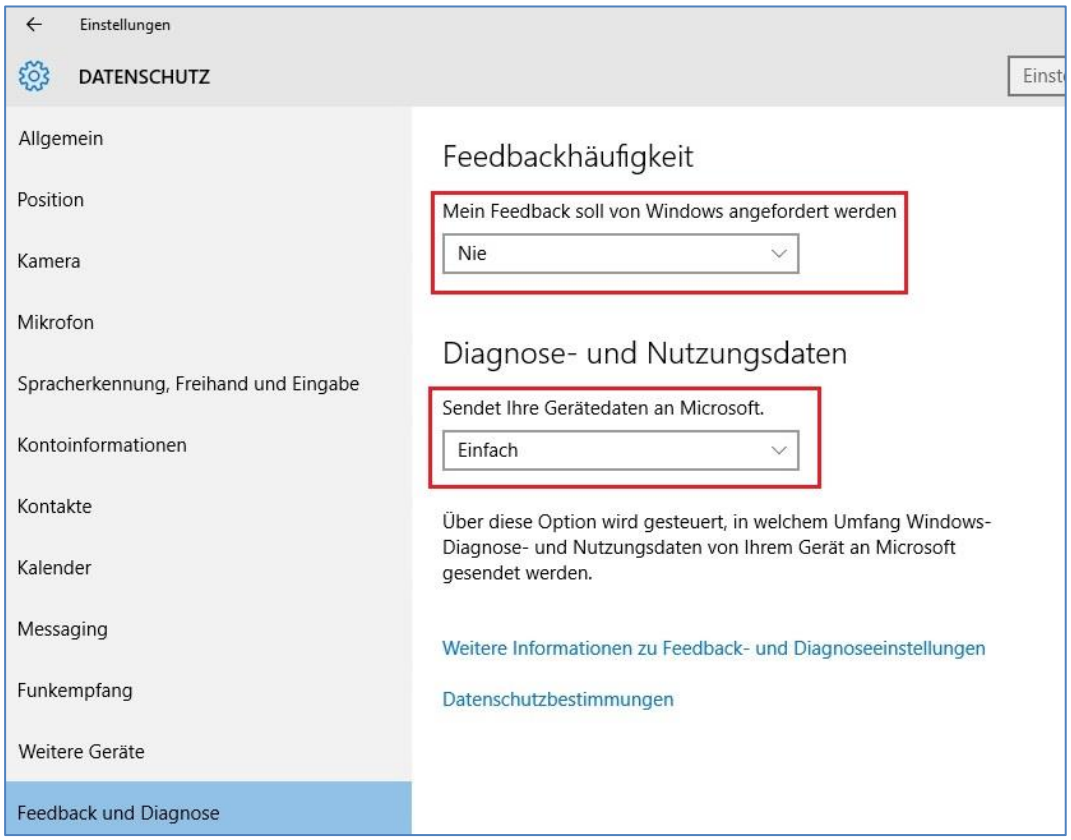

Abbildung 50: Datenschutzeinstellungen - Feedback und Diagnose

Durch das Setzen der Einstellung auf „NIE" bei den Diagnose- und Nutzungsdaten wird das Senden von Telemetriedaten an Microsoft weitestgehend abgeschaltet (dies ist jedoch nur in der Enterprise-Edition ab Windows 10 Build 1511 möglich). Die Einstellung „Nie" bedeutet, dass ein Security Level eingestellt ist. Somit wird dennoch ein minimaler Satz mit Betriebssystem-notwendigen Daten wird an Microsoft gesendet. Dazu gehören bspw. die verwendete Windows-Version, die Maschinenkennung und die Geräteklasse. Daten, welche Rückschlüsse auf die Nutzer zulassen könnten, werden nicht an Microsoft übertragen. Für Geräte, welche in einer Domäne betrieben werden, ist es jedoch möglich, diese Daten an einen lokalen Administrator umzuleiten.

Weitere Hinweise zu den Telemetriedaten finden sich in der Handlungsempfehlung „Datenschutzrechtliche Probleme bei der Einführung neuer Betriebssysteme - Eine Untersuchung am Beispiel Windows 10" der Forschungsstelle Recht des DFN.

Anleitung:

- Öffnen Sie die Eingabeaufforderung (**cmd**, als Administrator ausführen) und geben Sie Folgendes ein:

```
sc delete DiagTrack
sc delete dmwappushservice
echo "" > C:\ProgramData\Microsoft\Diagnosis\ETLLogs\AutoLogger\AutoLogger-
Diagtrack-Listener.etl
```

- Öffnen Sie den Editor für Gruppenrichtlinien (**gpedit.msc**, als Administrator ausführen)
  - Folgen Sie dem Pfad *Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Datensammlung und Vorabversionen;* Doppelklick auf *Telemetrie zulassen* → **Deaktivieren** und auf „Übernehmen" klicken

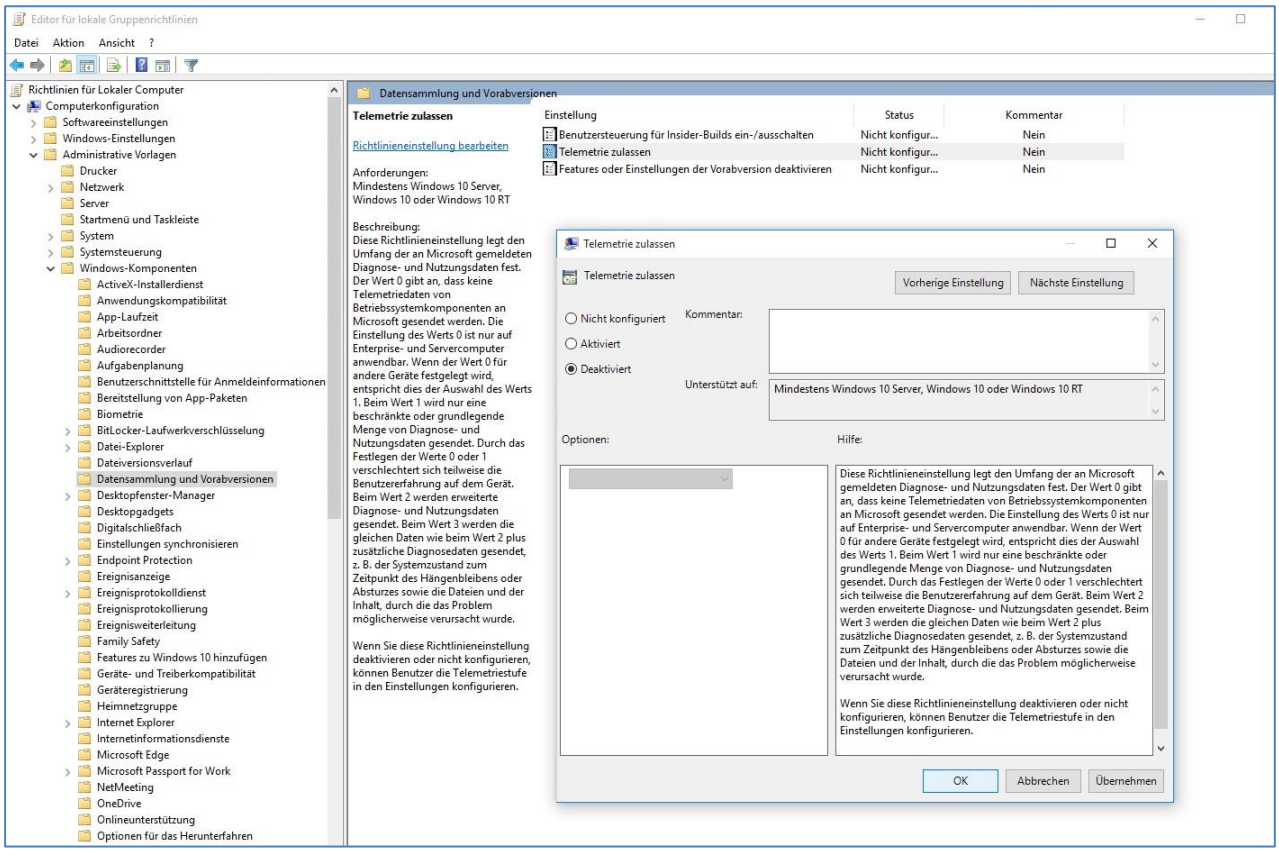

Abbildung 51: Gruppenrichtlinie - Telemetrie deaktivieren

- Öffnen Sie den Registry Editor (**regedit**, als Administrator ausführen)
  - Folgen Sie dem Pfad *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\DataCollection;* ändern Sie den Wert bei *AllowTelemetry* von 1 auf 0, dann bestätigen Sie mit OK

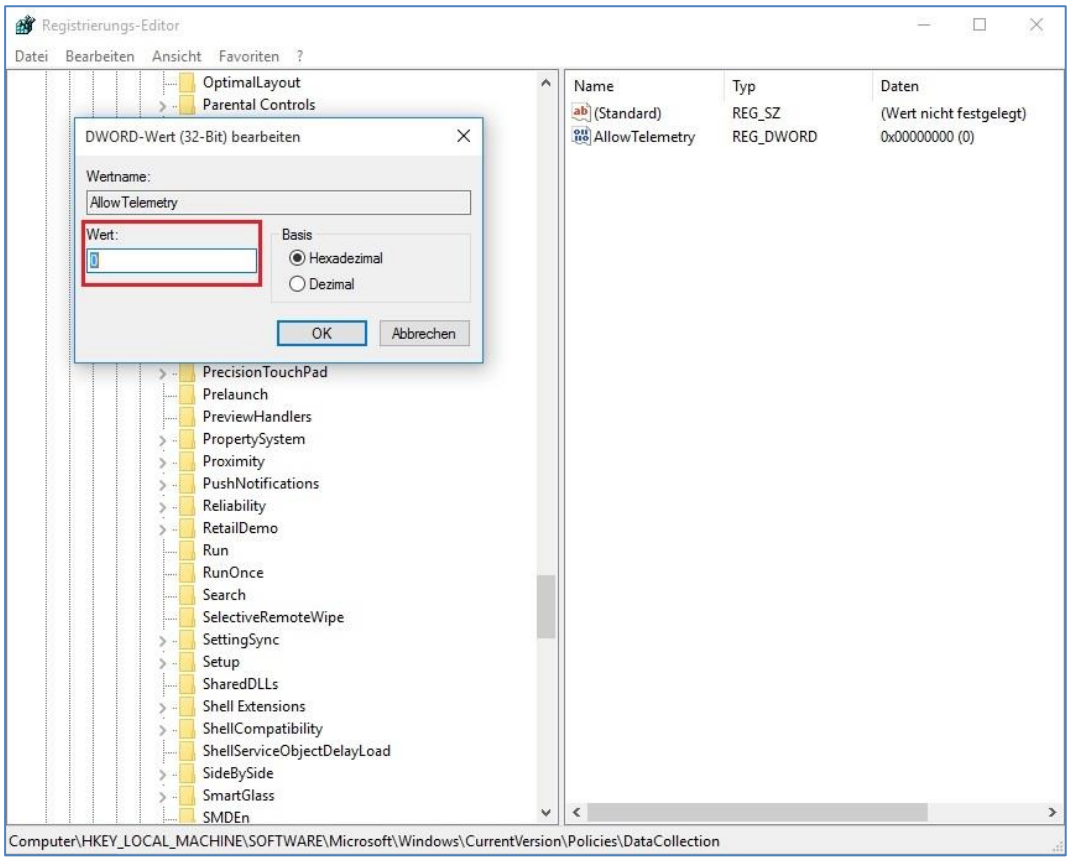

Abbildung 52: Registry - Telemetrie deaktivieren

Test-Monitoring von Telemetrie-Daten[2]:

Das Traffic-Monitoring von Testinstallationen hat ergeben, dass auch mit optimaler Einstellung zur datenarmen Konfiguration von Windows 10 – und damit der vollständigen Deaktivierung der Telemetriedaten – noch Kommunikation mit entsprechenden Microsoft-Servern stattgefunden hat.

Testumgebung:

- Verwendung von Windows 10 Edu und Enterprise LTSB
- Betrachtung des Betriebssystems als Black-Box
- Installation und Konfiguration mit verschiedenen Einstellungen zur datenarmen Konfiguration von Windows 10 (Szenarien)
- Einsatz einer Firewall vor dem Windows-10 Datennetz
- Konfiguration eines Benutzers
- Auswertung das Kommunikationsverhaltens ohne Benutzerinteraktion
- Installation ohne Internetzugang
- Installation einer Virenschutzsoftware (Sophos)
- Installation eines zusätzlichen Browsers (Mozilla Firefox)
- Deaktivierung von OneDrive
- Deaktivierung der Tunneling-Interfaces
    - Teredo
    - 6to4
    - Protokoll 41 (IPv6 in IPv4)

[2] Testumgebung an der TU Dresden

Die in Abbildung 41 dargestellten Ergebnisse stammen von einer Windows 10 Enterprise LTSB-Testinstallation mit den oben genannten Einstellungen. Die Konfiguration erfolgte anhand der Empfehlungen aus diesem Dokument.

Der Test fand zudem vor dem Update 1511 (Treshold) statt.

UDP	141.76.24.xx	141.30.66.135	53		DNS TU Dresden
TCP	141.76.24.xx	23.37.42.235	80	a23-37-42-235.deploy.static.akamaitechnologies.com	
TCP	141.76.24.xx	65.55.113.12	80	CloudFare ohne DNS-Namen	Microsoft Hosting
TCP	141.76.24.xx	204.79.197.200	443	bing.com, www.bing.com, *.platform.bing.com, *.bing.com, ieonline.microsoft.com, *.windowssearch.com, cn.ieonline.microsoft.com, *.origin.bing.com, *.mm.bing.net, *.api.bing.com, ecn.dev.virtualearth.net, *.cn.bing.net, *.cn.bing.com, *.ssl.bing.com, *.appex.bing.com, *.platform.cn.bing.com, ssl-api.bing.com, ssl-api.bing.net, *.api.bing.net, bingsandbox.com, www.bingsandbox.com, *.bingapis.com, *.working-bingapis-int.com, *.staging-bingapis-int.com, *.working-bingapis-int.net, *.staging-bingapis-int.net, feedback.microsoft.com, feedback-int.microsoft.com, insertmedia.bing.office.net, *.r.bing.com	
TCP	141.76.24.xx	65.55.252.92	443	*.big.telemetry.microsoft.com, *.telemetry.microsoft.com, telemetry.microsoft.com, *.phx.gbl	
TCP	141.76.24.xx	191.232.139.253	443	settings.data.microsoft.com, groups.data.microsoft.com	
TCP	141.76.24.xx	191.237.208.126	443	spynet2.microsoft.com, spynetalt.microsoft.com, spynet.microsoft.com, SpyNetFrontEnd-DC1-TiP.cloudapp.net, SpyNetFrontEnd-DC2-TiP.cloudapp.net, SpyNetFrontEnd-EAS-TiP.cloudapp.net, SpyNetFrontEnd-SAS-TiP.cloudapp.net, SpyNetFrontEnd-NEU-TiP.cloudapp.net, SpyNetFrontEnd-WEU-TiP.cloudapp.net, SpyNetFrontEnd-BRA-TiP.cloudapp.net, SpyNetFrontEnd-JPE-TiP.cloudapp.net, SpyNetFrontEnd-JPW-TiP.cloudapp.net, SpyNetFrontEnd-AUE-TiP.cloudapp.net, SpyNetFrontEnd-AUS-TiP.cloudapp.net	
TCP	141.76.24.xx	134.170.53.30	443	fe2.update.microsoft.com	
TCP	141.76.24.xx	212.201.100.142	80	a212-201-100-142.deploy.akamaitechnologies.com	
TCP	141.76.24.xx	23.37.45.183	443	cp201-prod.do.dsp.mp.microsoft.com, disc201-prod.do.dsp.mp.microsoft.com, geover-prod.do.dsp.mp.microsoft.com, kv201-prod.do.dsp.mp.microsoft.com	
TCP	141.76.24.xx	65.52.108.135	443	array102-prod.do.dsp.mp.microsoft.com, geo-prod.do.dsp.mp.microsoft.com, geover-prod.do.dsp.mp.microsoft.com, orgeover-prod.do.dsp.mp.microsoft.com	
TCP	141.76.24.xx	95.101.46.117	443	cp101-prod.do.dsp.mp.microsoft.com, kv101-prod.do.dsp.mp.microsoft.com, disc101-prod.do.dsp.mp.microsoft.com, geover-prod.do.dsp.mp.microsoft.com	
TCP	141.76.24.xx	191.234.4.50	80	c-0001.c-msedge.net	Microsoft Bing
TCP	141.76.24.xx	157.55.133.204	443	sls.update.microsoft.com	

Abbildung 53: Logfile mit aufgebauten und abgelehnten Verbindungen/Anfragen (Screenshot: TU Dresden)

Ergebnisse:

- Übermittlung von Daten an Microsoft bereits während der Installation
- Privacy-by-Default findet keine Berücksichtigung (Opt-Out Verfahren)
- Datenschutzkonforme Einstellungen auf Anwenderebene („Schieberegler“) sind nicht ausreichend
- Telemetrie ist nicht komplett abschaltbar
- Datenschutzkonforme Ausgestaltung ist nicht über eine Firewall zu erreichen (Mobilität)
- Edition Education erzeugt deutlich erhöhtes Kommunikationsverhalten mit Microsoft,
- auch bei datenschutzvertretbarer Einstellung (Anzahl der Ziele: 49)
- Edition LTSB mit sehr geringen Kommunikationsverhalten (Anzahl Ziele: 14)
- Es ist ungeklärt, welche Daten zu welchen Zwecken an Microsoft übermittelt werden

Sonstiges

Editionen

Edition	Beschreibung
Windows 10 Home	Basis-Edition für Privatanwender, enthält alle an den Verbraucher gerichtete Funktionen und Dienste
Windows 10 Pro	Baut auf Windows 10 Home auf und enthält zusätzliche Funktionen für den Geschäftsbetrieb, z.B. die Möglichkeit der Anbindung an eine Unternehmensinfrastruktur, Bit Locker-Verschlüsselung und die Administration über Gruppenrichtlinien
Windows 10 Pro Education	Windows 10 Pro für akademische Nutzer; erhältlich nur für berechtigte Lizenznehmer in Verbindung mit neuer Hardware von ausgewählten Partnern; einige Funktionen und Dienste sind nicht enthalten, z.B. Cortana, Vorschläge im Windows Store sowie Tipps und Tricks zu Windows
Windows 10 Enterprise	Voller Funktionsumfang speziell für den Betrieb in Unternehmen, nur Volumenlizenzierung möglich, erhältlich als E3 (klassische Enterprise-Edition) oder E5 (E3 + Windows Defender ATP)
Windows 10 Enterprise LTSB	LTSB → Long Term Servicing Branch, Enterprise-Edition mit verringertem Funktionsumfang (ohne Cortana und Edge) sowie erweiterter Kontrolle über Updates (Feature-Updates können bis zu 10 Jahre zurückgestellt werden) für Umgebungen die besonders sensibel sind oder stabil sein müssen, die Edition N (speziell für Europa) wird zudem ohne medienrelevante Technologien ausgeliefert (z.B. ohne Windows Media Player, ohne Skype, ohne Kamera und Sprachrekorder; das hat zur Folge, dass dadurch einige Funktionen und Dienste nicht oder nur eingeschränkt zur Verfügung stehen)
Windows 10 Education	Entspricht der Enterprise-Edition (ohne Cortana und LTSB), speziell für Nutzer aus dem akademischen Bereich

Information Protection

Information Protection ist ein neuer Dienst für Unternehmen, welcher auf der Cloud-Plattform Azure angeboten wird. Dieser dient dem Schutz vor unbeabsichtigtem Datenverlust. Der Dienst hilft, Daten (sowohl in der Cloud als auch in lokalen Infrastrukturen) zu klassifizieren, zu trennen und zu schützen.

Vorinstallierte Apps

In Windows 10 gibt es eine Reihe vorinstallierter Apps, die u.U. nicht benötigt werden. Diese werden mit jedem Funktions-Update neu installiert.

In der folgenden Übersicht findet sich eine Liste der Apps sowie PowerShell-Befehle zum Löschen dieser (Administrator-Berechtigung erforderlich).

Vorinstallierte App	**PowerShell-Befehl**
3D Builder	Get-AppxPackage *3dbuilder* | Remove-AppxPackage
Alarm und Uhr	Get-AppxPackage *windowsalarms* | Remove-AppxPackage
Begleiter für Telefon	Get-AppxPackage *windowsphone* | Remove-AppxPackage
Erste Schritte	Get-AppxPackage *getstarted* | Remove-AppxPackage
Filme & TV	Get-AppxPackage *zunevideo* | Remove-AppxPackage
Finanzen	Get-AppxPackage *bingfinance* | Remove-AppxPackage
Fotos	Get-AppxPackage *photos* | Remove-AppxPackage
Groove-Musik	Get-AppxPackage *zunemusic* | Remove-AppxPackage
Kamera	Get-AppxPackage *windowscamera* | Remove-AppxPackage
Karten	Get-AppxPackage *windowsmaps* | Remove-AppxPackage
Kontakte	Get-AppxPackage *people* | Remove-AppxPackage
Mail & Kalender	Get-AppxPackage *windowscommunicationsapps* | Remove-AppxPackage
Microsoft Solitaire Collection	Get-AppxPackage *solitairecollection* | Remove-AppxPackage
Nachrichten	Get-AppxPackage *bingnews* | Remove-AppxPackage
Office holen	Get-AppxPackage *officehub* | Remove-AppxPackage
OneNote	Get-AppxPackage *onenote* | Remove-AppxPackage
Rechner	Get-AppxPackage *windowscalculator* | Remove-AppxPackage
Skype-Vorschau	Get-AppxPackage *skypeapp* | Remove-AppxPackage
Sport	Get-AppxPackage *bingsports* | Remove-AppxPackage
Sprachrekorder	Get-AppxPackage *soundrecorder* | Remove-AppxPackage
Xbox Identity Provider	Get-AppxPackage *xboxIdentityprovider* | Remove-AppxPackage
Xbox	Get-AppxPackage *xboxapp* | Remove-AppxPackage
Alle vorinstallierten Apps wieder installieren	Get-AppxPackage –allusers | foreach {Add-AppxPackage –register "$($_.InstallLocation)\appxmanifest.xml" -DisableDevelopmentMod

Abbildungsverzeichnis

Anlage 1: Gruppenrichtlinien und PowerShell Scripte

Es ist zu beachten, dass nicht jede Edition von Windows 10 über Gruppenrichtlinien (GPO) konfigurierbar ist. Ebenso gibt es nicht für jede Einstellung eine Gruppenrichtlinie, stattdessen ist diese aber meist auch über einen Registry-Eintrag konfigurierbar.

Hier einige Hinweise:

- Tipps und Tricks zu Windows sowie Empfehlungen aus dem Store lass sich in der Pro-Edition nicht mehr vollständig per GPO deaktivieren, dies ist nur noch in der Benutzeroberfläche möglich.
- Der Sperrbildschirm lässt sich bei der Pro-Edition nicht mehr deaktivieren.
- Der Umweg über Registry-Einträge soll bei einigen Einstellungen in der Pro-Edition nicht mehr möglich sein (nicht geprüft).
- App-Vorschläge lass sich in der Pro-Edition nicht mehr per GPO abschalten, dies muss manuell auf jedem Gerät geschehen.

Telemetrie deaktivieren

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows Komponenten > Datensammlung und Vorabversionen
Einstellung	Telemetrie zulassen
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Data Collection and Preview Builds > Allow Telemetry
Wert	Aktiviert (0 – Aus [Nur Enterprise])
Script (Powershell)	`New-ItemProperty -path "HKLM\SOFTWARE\Policies\Microsoft\Windows\DataCollection" -name "AllowTelemetry" -value "0" -propertyType dword -force`
Beschreibung (GPO)	Diese Richtlinieneinstellung legt den Umfang der an Microsoft gemeldeten Diagnose- und Nutzungsdaten fest. Der Wert 0 gibt an, dass keine Telemetriedaten von Betriebssystemkomponenten an Microsoft gesendet werden. Die Einstellung des Werts 0 ist nur auf Enterprise- und Servercomputer anwendbar. Wenn der Wert 0 für andere Geräte festgelegt wird, entspricht dies der Auswahl des Werts 1. Beim Wert 1 wird nur eine beschränkte oder grundlegende Menge von Diagnose- und Nutzungsdaten gesendet. Durch das Festlegen der Werte 0 oder 1 verschlechtert sich teilweise die Benutzererfahrung auf dem Gerät. Beim Wert 2 werden erweiterte Diagnose- und Nutzungsdaten gesendet. Beim Wert 3 werden die gleichen Daten wie beim Wert 2 plus zusätzliche Diagnosedaten gesendet, z. B. der Systemzustand zum Zeitpunkt des Hängenbleibens oder Absturzes sowie die Dateien und der Inhalt, durch die das Problem möglicherweise verursacht wurde.Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, können Benutzer die Telemetriestufe in den Einstellungen konfigurieren.
Hinweise	GPO Win10 Enterprise Build 10240 (vor Update 1511)

OneDrive deaktivieren

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows Komponenten > OneDrive
Einstellung	Verwendung von OneDrive für die Dateispeicherung verhindern
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > OneDrive > Prevent the usage of OneDrive for file storage
Wert	Aktiviert
Script (Powershell)	`New-ItemProperty -path "HKLM\SOFTWARE\Policies\Microsoft\Windows\OneDrive" -name "DisableFileSyncNGSC" -value "1" -propertyType dword -force`
Beschreibung (GPO)	Mit dieser Richtlinieneinstellung können Sie verhindern, dass Apps und Features Dateien auf OneDrive verwenden. Wenn Sie diese Richtlinieneinstellung aktivieren: • können Benutzer über die OneDrive-App und die Dateiauswahl nicht auf OneDrive zugreifen. • können Benutzer über die OneDrive-App und die Dateiauswahl nicht auf OneDrive zugreifen. • können Windows Store-Apps nicht über die WinRT-API auf OneDrive zugreifen. • wird OneDrive im Navigationsbereich im Datei-Explorer nicht angezeigt. • werden OneDrive-Dateien nicht mit der Cloud synchronisiert. • können Benutzer Fotos und Videos aus dem Ordner "Eigene Aufnahmen" nicht automatisch hochladen. Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, können Apps und Features den OneDrive-Dateispeicher verwenden.
Hinweise	./.

Ortung deaktivieren

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows Komponenten > Position und Sensoren > Windows-Positionssuche
Einstellung	Windows-Positionssuche deaktivieren
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Location and Sensors > Windows Location Provider > Turn off Windows Location Provider
Wert	Aktiviert
Script (Powershell)	`New-ItemProperty -path "HKLM\SOFTWARE\Policies\Microsoft\Windows\LocationAndSensors" -name "DisableWindowsLocationProvider" -value "1" -propertyType dword -force`
Beschreibung (GPO)	Mit dieser Richtlinieneinstellung wird die Windows-Positionssuche für diesen Computer deaktiviert. Wenn Sie diese Richtlinieneinstellung aktivieren, wird die Windows-Positionssuche deaktiviert und kann von keinem Programm auf diesem Computer verwendet werden. Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, kann die Windows-Positionssuche von allen Programmen auf diesem Computer verwendet werden.
Hinweise	Sollten Apps verwendet werden müssen, die ohne Abrufen von Positionsdaten nicht funktionsfähig sind, sollte das Deaktivieren dieser Funktion nicht erzwungen werden.

Cortana deaktivieren

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows Komponenten > Suche
Einstellung	Cortana zulassen
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Search > Allow Cortana
Wert	./.
Script (Powershell)	`New-ItemProperty -path "HKLM\SOFTWARE\Policies\Microsoft\Windows\Windows Search" -name "AllowCortana" -value "0" -propertyType dword -force`
Beschreibung (GPO)	Diese Richtlinieneinstellung gibt an, ob Cortana auf dem Gerät zugelassen ist. Wenn Sie diese Einstellung aktivieren oder nicht konfigurieren, wird Cortana auf dem Gerät zugelassen. Wenn Sie die Einstellung deaktivieren, wird Cortana ausgeschaltet. Wenn Cortana ausgeschaltet ist, können Benutzer mithilfe der Suchfunktion trotzdem Informationen auf dem Gerät und im Internet suchen.
Hinweise	Cortana

Senden und Abrufen von Hardwaremetadaten verhindern

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > System > Geräteinstallation
Einstellung	Abrufen von Gerätemetadaten aus dem Internet verhindern
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > System > Device Installation > Prevent device metadata retrieval from the Internet
Wert	Aktiviert
Script (Powershell)	`New-ItemProperty -path "HKLM\SOFTWARE\Policies\Microsoft\Windows\Device Metadata" -name "PreventDeviceMetadataFromNetwork" -value "1" -propertyType dword -force`
Beschreibung (GPO)	Mit dieser Richtlinieneinstellung können Sie verhindern, dass Gerätemetadaten aus dem Internet abgerufen werden.Wenn Sie diese Richtlinieneinstellung aktivieren, werden keine Gerätemetadaten für installierte Geräte aus dem Internet abgerufen. Diese Richtlinieneinstellung überschreibt die Einstellung im Dialogfeld "Geräteinstallationseinstellungen" (Systemsteuerung > System und Sicherheit > System > Erweiterte Systemeinstellungen > Registerkarte "Hardware"). Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird durch die Einstellung im Dialogfeld "Geräteinstallationseinstellungen" gesteuert, ob Gerätemetadaten aus dem Internet abgerufen werden.
Hinweise	./.

Windows MRT und ggf. Hochladen verdächtiger Daten unterbinden

Gruppenrichtlinie ./.

Einstellung
1.) DontOfferThroughWUAU
2.) DontReportInfectionInformation

Gruppenrichtlinie (englisch) ./.

Wert
1.) 1
2.) 1

Script (Powershell)
1)
```
New-ItemProperty -path
"HKLM\SOFTWARE\Policies\Microsoft\MRT" -name
"DontOfferThroughWUAU" -value "1" -propertyType dword
–force
```
2)
```
New-ItemProperty -path
"HKLM\SOFTWARE\Policies\Microsoft\MRT" -name "
DontReportInfectionInformation " -value "1" -propertyType
dword -force
```

Beschreibung (GPO) ./.

Hinweise Jeden zweiten Dienstag im Monat ist Microsofts „Patch Day", zu dem das Unternehmen gebündelt Software-Updates für Windows, Office & Co über die Windows-Update-Funktion ausliefert. Mit dabei ist immer auch eine neue Version des „Microsoft Windows-Tool zum Entfernen bösartiger Software", kurz „MRT". Dabei handelt es sich um einen Virenscanner ohne Wächter-Funktion, der beim Aufruf den PC nach einigen speziellen Viren, Würmern und Trojanern durchsucht und diese entfernt. ES ERSETZT KEIN ANTIVIRUS-PROGRAMM! Das automatische Windows-Update lädt das aktuelle MRT nicht nur herunter, sondern startet auch gleich einen Scan-Vorgang. Der Registry-Eintrag 1) unterbindet diesen Vorgang. Der Registry-Eintrag 2) sorgt dafür, dass kein Report an Microsoft gesendet wird, wenn dennoch ein Scan gestartet wurde.

Windows Defender und ggf. Hochladen verdächtiger Daten bestätigen

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows Komponenten > Endpoint Protection > MAPS
Einstellung	Dateibeispiele senden, wenn eine weitere Analyse erforderlich ist
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Windows Defender > MAPS > Send file samples when further analysis is required
Wert	Aktiviert – Immer auffordern
Script (Powershell)	`New-ItemProperty -path "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet" -name " SubmitSamplesConsent" -value "0" -propertyType dword -force`
Beschreibung (GPO)	./.
Hinweise	In einigen Einrichtungen wird auf allen verwalteten Windows Client eine Security- und Antivirus-Suite eines Drittherstellers eingesetzt. Der in Windows 10 integrierte Windows Defender ist in diesem Fall deaktiviert. Es gibt jedoch einige wenige Ausnahmen, wo bestimmte Messanlagen und –software nicht kompatibel zu der Dritthersteller Sicherheitssoftware ist. Diese Systeme werden in einem zusätzlich abgesicherten Netzwerkbereich betrieben und der Windows Defender ist aktiviert. Für diese Clients greift die hier aufgeführte Konfiguration. Die Einstellung „Aktiviert – Immer senden" ist gleichzusetzen mit „deaktiviert". Der Group Policy Editor ändert diese Einstellung automatisch auf „deaktiviert" ab.

Windows Defender Cloudbasierter Schutz deaktivieren

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows Komponenten > Endpoint Protection > MAPS
Einstellung	Beitritt zu Microsoft MAPS
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Windows Defender > MAPS > Join Microsoft MAPS
Wert	Deaktiviert
Script (Powershell)	`New-ItemProperty -path "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet" -name "SpyNetReporting" -value "0" -propertyType dword -force`
Beschreibung (GPO)	./.
Hinweise	In einigen Einrichtungen wird auf allen verwalteten Windows Client eine Security- und Antivirus-Suite eines Drittherstellers eingesetzt. Der in Windows 10 integrierte Windows Defender ist in diesem Fall deaktiviert. Es gibt jedoch einige wenige Ausnahmen, wo bestimmte Messanlagen und –software nicht kompatibel zu der Dritthersteller Sicherheitssoftware ist. Diese Systeme werden in einem zusätzlich abgesicherten Netzwerkbereich betrieben und der Windows Defender ist aktiviert. Für diese Clients greift die hier aufgeführte Konfiguration.

Unterbinden der Teilnahme am Windows Customer Experience Improvement program

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > System > Internet-kommunikations-verwaltung > Internet-kommunikations-einstellungen
Einstellung	Programm zur Verbesserung der Benutzerfreundlichkeit deaktivieren
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > System > Internet Communication Management > Internet Communication Settings > Turn off the Windows Messenger Customer Experience Improvement Program
Wert	Aktiviert
Script (Powershell)	`New-ItemProperty -path "HKLM\SOFTWARE\Policies\Microsoft\SQMClient\Windows" -name "CEIPEnable" -value "0" -propertyType dword -force`
Beschreibung (GPO)	Diese Richtlinieneinstellung deaktiviert das Programm zur Verbesserung der Benutzerfreundlichkeit. Das Programm zur Verbesserung der Benutzerfreundlichkeit sammelt Informationen über die Hardwarekonfiguration sowie darüber, wie Sie unsere Software und unsere Dienste verwenden, um Trends und Verwendungsmuster zu erkennen. Ihr Name, Ihre Adresse und jegliche anderen persönlichen Informationen werden von Microsoft nicht erfasst. Sie müssen keine Fragebögen ausfüllen, und kein Vertreter wird mit Ihnen Kontakt aufnehmen. Sie können einfach ohne Unterbrechung weiterarbeiten. Das Programm ist einfach und benutzerfreundlich. Wenn Sie diese Richtlinieneinstellung aktivieren, nimmt kein Benutzer am Programm zur Verbesserung der Benutzerfreundlichkeit teil. Wenn Sie diese Richtlinieneinstellung deaktivieren, nehmen alle Benutzer am Programm zur Verbesserung der Benutzerfreundlichkeit teil. Wenn Sie diese Richtlinieneinstellung nicht konfigurieren, kann der Administrator mithilfe der Komponente "Problemberichte und -lösungen" in der Systemsteuerung das Programm zur Verbesserung der Benutzerfreundlichkeit für alle Benutzer aktivieren.
Hinweise	./.

Anwendungstelemetrie deaktivieren

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows Komponenten > Anwendungs-kompatibilität
Einstellung	Anwendungstelemetrie deaktivieren
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Application Compatibility > Turn off Application Telemetry
Wert	Aktiviert
Script (Powershell)	`New-ItemProperty -path "HKLM\SOFTWARE\Policies\Microsoft\Windows\AppCompat" -name "AITEnable" -value "0" -propertyType dword -force`
Beschreibung (GPO)	Die Richtlinieneinstellung steuert den Zustand der Anwendungstelemetrie-Komponente im System. Die Anwendungstelemetrie ist ein Mechanismus, mit dem die anonyme Nutzung bestimmter Windows-Systemkomponenten durch Anwendungen nachverfolgt wird. Wenn Sie die Anwendungstelemetrie durch Auswahl von "Aktivieren" deaktivieren, wird die Sammlung von Nutzungsdaten gestoppt. Wenn das Programm zur Verbesserung der Benutzerfreundlichkeit deaktiviert ist, wird die Anwendungstelemetrie unabhängig von der Einstellung dieser Richtlinie deaktiviert. Das Deaktivieren der Telemetrie wird mit jedem Start einer neuen Anwendung wirksam. Führen Sie einen Neustart durch, um sicherzustellen, dass die Sammlung von Telemetriedaten für alle Anwendungen gestoppt wurde.
Hinweise	./.

Inventory Collector deaktivieren

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows Komponenten > Anwendungs-kompatibilität
Einstellung	Inventory Collector deaktivieren
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Application Compatibility > Turn off Inventory Collector
Wert	Aktiviert
Script (Powershell)	`New-ItemProperty -path "HKLM\SOFTWARE\Policies\Microsoft\Windows\AppCompat" -name " DisableInventory" -value "1" -propertyType dword -force`
Beschreibung (GPO)	Diese Richtlinieneinstellung steuert den Status von Inventory Collector. Inventory Collector nimmt Anwendungen, Dateien, Geräte und Treiber im System auf und übermittelt die Informationen an Microsoft. Diese Informationen werden zur Diagnose von Kompatibilitätsproblemen verwendet. Wenn Sie diese Richtlinieneinstellung aktivieren, wird Inventory Collector deaktiviert, und es werden keine Informationen an Microsoft gesendet. Die Sammlung von Installationsdaten durch den Programmkompatibilitäts-Assistenten wird ebenfalls deaktiviert. Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird Inventory Collector aktiviert. Hinweis: Diese Richtlinieneinstellung bleibt ohne Wirkung, wenn das Programm zur Verbesserung der Benutzerfreundlichkeit deaktiviert ist. Inventory Collector ist dann deaktiviert.
Hinweise	./.

Diagnose Tracking Dienst deaktivieren

Gruppenrichtlinie	./.
Einstellung	Benutzererfahrung und Telemetrie
Gruppenrichtlinie (englisch)	Connected User Experiences and Telemetry
Wert	Startup: Disable
Script (Powershell)	`Get-Service DiagTrack | Set-Service -StartupType Disabled`
Beschreibung (GPO)	Der Diagnosenachverfolgungsdienst ermöglicht die Datenerfassung zu Funktionsproblemen in Windows-Komponenten.
Hinweise	Dieses Tool muss bei den Diensten deaktiviert werden. (services.msc)

WAP Push-Nachrichtenroutingdienst deaktivieren

Gruppenrichtlinie	./.
Einstellung	dmwappushsvc
Gruppenrichtlinie (englisch)	dmwappushsvc
Wert	Startup: Disable
Script (Powershell)	`Get-Service dmwappushsvc | Set-Service -StartupType Disabled`
Beschreibung (GPO)	WAP Push-Nachrichtenroutingdienst
Hinweise	Dieses Tool muss bei den Diensten deaktiviert werden. (services.msc)

Werbe-ID deaktivieren

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > System > Benutzerprofile
Einstellung	Werbe-ID deaktivieren
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > System > User Profiles > Turn off the advertising ID
Wert	Aktiviert
Script (Powershell)	`New-ItemProperty -path "HKLM\SOFTWARE\Policies\Microsoft\Windows\AdvertisingInfo" -name "DisabledbyGroupPolicy" -value "1" -propertyType dword -force`
Beschreibung (GPO)	Mit dieser Richtlinieneinstellung wird die Werbe-ID deaktiviert und damit verhindert, dass Apps die ID App-übergreifend verwenden. Wenn Sie diese Richtlinieneinstellung aktivieren, wird die Werbe-ID deaktiviert. Apps können die ID nicht App-übergreifend verwenden. Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, können Benutzer steuern, ob Apps die Werbe-ID App-übergreifend verwenden können.
Hinweise	./.

Smartscreen-Filter ausschalten

Gruppenrichtlinie
Computerkonfiguration
> Administrative Vorlagen
> Windows-Komponenten
> Datei-Explorer

Einstellung
Windows SmartScreen konfigurieren

Gruppenrichtlinie (englisch)
Computer Configuration
> Administrative Templates
> Windows Components
> File Explorer
> Configure Windows SmartScreen

Wert
Aktiviert – Smartscreen deaktivieren

Script (Powershell)
```
New-ItemProperty -path
"HKLM\SOFTWARE\Policies\Microsoft\Windows\System" -name
"EnableSmartScreen" -value "0" -propertyType dword -force
```

Beschreibung (GPO)
Diese Richtlinieneinstellung ermöglicht Ihnen das Verwalten des Verhaltens von Windows SmartScreen. Windows SmartScreen trägt dazu bei, die Sicherheit von PCs zu gewährleisten, indem Benutzer vor dem Ausführen unbekannter, aus dem Internet heruntergeladener Programme gewarnt werden. Wenn dieses Feature aktiviert ist, werden einige Informationen zu Dateien und auf PCs ausgeführten Programmen an Microsoft gesendet.
Wenn Sie diese Richtlinieneinstellung aktivieren, kann das Verhalten von Windows SmartScreen durch das Festlegen einer der folgenden Optionen gesteuert werden:

- Vor dem Ausführen einer heruntergeladenen unbekannten Software Genehmigung eines Administrators anfordern
- Benutzer vor dem Ausführen einer heruntergeladenen unbekannten Software warnen
- SmartScreen deaktivieren
- Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird das Verhalten von Windows SmartScreen von den Administratoren mithilfe der Windows SmartScreen-Einstellungen in "Sicherheit und Wartung" auf dem PC verwaltet.
- Optionen:
- Vor dem Ausführen einer heruntergeladenen unbekannten Software Genehmigung eines Administrators anfordern
- Benutzer vor dem Ausführen einer heruntergeladenen unbekannten Software warnen
- SmartScreen deaktivieren

Hinweise
In dem Menüpunkt unter „Einstellungen – Datenschutz – Allgemein" ist die Option nicht ausgegraut, obwohl sie per GPO erzwungen wird.
Der SmartScreen-Filter sollte ausgeschaltet werden, um z.B. von Windows Store-Apps verwendete Webinhalte (URLs) zu überprüfen.

Smartscreen-Filter ausschalten

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Microsoft Edge
Einstellung	Ermöglicht die SmartScreen-Konfiguration
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Microsoft Edge > Allows you to configure SmartScreen
Wert	Deaktiviert
Script (Powershell)	`New-ItemProperty -path "HKLM\SOFTWARE\Policies\Microsoft\MicrosoftEdge\PhishingFilter" -name "EnabledV9" -value "0" -propertyType dword -force`
Beschreibung (GPO)	Mit dieser Einstellung legen Sie fest, ob SmartScreen eingeschaltet wird. Die Einstellung ist standardmäßig aktiviert. Wenn Sie diese Einstellung aktivieren, ist SmartScreen für alle Computer eingeschaltet. Wenn Sie diese Einstellung deaktivieren, ist SmartScreen ausgeschaltet.
Hinweise	Microsoft Edge Hier scheint es noch einen Bug oder Übersetzungsfehler zu geben. Mit dem Wert „Deaktiviert" wird der SmartSreen-Filter in Edge abgeschaltet. Der SmartScreen-Filter sollte ausgeschaltet werden, um z.B. von Windows Store-Apps verwendete Webinhalte (URLs) zu überprüfen.

Senden von Informationen zum Schreibverhalten deaktivieren

Gruppenrichtlinie	./.
Einstellung	./.
Gruppenrichtlinie (englisch)	./.
Wert	./.
Script (Powershell)	`New-ItemProperty -path "HKCU\SOFTWARE\Microsoft\Input\TIPC" -name "Enabled" -value "0" -propertyType dword -force`
Beschreibung (GPO)	Informationen zum Schreibverhalten an Microsoft senden, um Eingabe- und Schreibfunktionen in Zukunft zu verbessern.
Hinweise	Wenn die Telemetriestufe auf Einfach oder Sicherheit eingestellt ist, wird diese Option automatisch deaktiviert. Diese Einstellung ist nicht als GPO verfügbar. Es ist derzeit lediglich möglich, mittels eines Registrierungsschlüssels im Userkontext eine Vorgabe dieser Einstellung zu bewirken.

Websites Zugriff auf Sprachliste deaktivieren

Gruppenrichtlinie	./.
Einstellung	./.
Gruppenrichtlinie (englisch)	./.
Wert	./.
Script (Powershell)	`New-ItemProperty -path "HKCU\Control Panel\International\User Profile" -name "HttpAcceptLanguageOptOut" -value "1" -propertyType dword -force`
Beschreibung (GPO)	Websites den Zugriff auf die eigene Sprachliste gestatten, um die Anzeige lokal relevanter Inhalte zu ermöglichen.
Hinweise	Diese Einstellung ist nicht als GPO verfügbar. Es ist derzeit lediglich möglich, mittels eines Registrierungsschlüssels im Userkontext eine Vorgabe dieser Einstellung zu bewirken.

Zugriff von Apps auf Benutzerdaten deaktivieren

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > System > Benutzerprofile
Einstellung	Benutzerverwaltung für die Freigabe von Informationen zum Benutzernamen, Kontobild und zur Domäne für Apps (keine Desktop-Apps)
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > System > User Profiles > User management of sharing user name account picture and domain information with apps (not desktop apps)
Wert	Aktiviert – Immer deaktiviert

Script (Powershell)	1)
	`New-ItemProperty -path "HKLM\SOFTWARE\Policies\Microsoft\Windows\System" -name "AllowUserInfoAccess" -value "2" -propertyType dword –force`
	2)
	`New-ItemProperty -path "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\DeviceAccess\Global\{C1D23ACC-752B-43E5-8448-8D0E519CD6D6}" -name "Value" -value "Deny" -propertyType string –force`

Beschreibung (GPO)	Durch diese Einstellung wird verhindert, dass Benutzer die Zugriffsmöglichkeit von Apps auf Informationen zum Benutzernamen, Kontobild und zur Domäne verwalten können. Wenn Sie diese Richtlinieneinstellung aktivieren, kann die Freigabe von Informationen zum Benutzernamen, Bild und zur Domäne durch Festlegen einer der folgenden Optionen gesteuert werden: "Immer aktiviert" - Benutzer können diese Einstellung nicht ändern, und der Name sowie das Kontobild des Benutzers werden für Apps (keine Desktop-Apps) freigegeben. Zudem können Apps (keine Desktop-Apps), die über die Enterprise-Authentifizierungsoption verfügen, auch die UPN, SIP/URI und DNS von Benutzern abrufen. "Immer deaktiviert" - Benutzer können diese Einstellung nicht ändern, und der Benutzername und das Kontobild werden nicht für Apps (keine Desktop-Apps) freigegeben. Zudem können Apps (keine Desktop-Apps), die über die Enterprise-Authentifizierungsoption verfügen, die UPN, SIP/URI und DNS von Benutzern nicht abrufen. Die Auswahl dieser Option kann sich negativ auf bestimmte Unternehmenssoftware und/oder Branchen-Apps auswirken, die zum Herstellen einer Verbindung mit Netzwerkressourcen von den durch diese Einstellung geschützten Domäneninformationen abhängig sind. Wenn Sie diese Richtlinie nicht konfigurieren oder deaktivieren, hat der Benutzer Vollzugriff auf diese Einstellung, und er kann sie aktivieren und deaktivieren. Die Auswahl dieser Option kann sich negativ auf bestimmte Unternehmenssoftware und/oder Branchen-Apps auswirken, die zum Herstellen einer Verbindung mit Netzwerkressourcen von den durch diese Einstellung geschützten Domäneninformationen abhängig sind. Dies ist insbesondere dann der Fall, wenn die Benutzer die Einstellung

deaktivieren.

Hinweise

Die GPO funktioniert nicht. Die Option wird nicht konfiguriert und kann durch den User verändert werden. Mittels des zweiten Registrierungseintrags kann eine Voreinstellung der Option getroffen werden.

Apps verbieten, den Funkempfang zu steuern

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Datenschutzbestimmungen für die App
Einstellung	Zugriff auf Funksteuerung durch Windows-Apps zulassen
Gruppenrichtlinie (englisch)	Allow access to radio control by Windows Apps
Wert	Legen Sie das Feld "Eine Einstellung wählen" als "Force Deny" fest
Script (Powershell)	`New-ItemProperty -path "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\DeviceAccess\Global\{A8804298-2D5F-42E3-9531-9C8C39EB29CE}" -name "Value" -value "Deny" -propertyType string -force`
Beschreibung (GPO)	Einige Apps verwenden auf dem Gerät Funktechnik wie Bluetooth für den Empfang und das Senden von Daten. In einigen Fällen müssen Apps den Funkempfang aktivieren und deaktivieren, um optimal zu funktionieren.
Hinweise	Einstellung auch auf Benutzeroberfläche "Einstellungen > Datenschutz" optionale Einstellung, in Benutzeroberfläche auch nur für einzelne Apps auswählbar

Apps verbieten, mit Geräten zu synchronisieren

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Datenschutzbestimmungen für die App
Einstellung	Zugriff auf vertrauenswürdige Geräte durch Windows-Apps zulassen
Gruppenrichtlinie (englisch)	Allow access to trusted devices by Windows Apps
Wert	Legen Sie das Feld "Eine Einstellung wählen" als "Force Deny" fest
Script (Powershell)	`New-ItemProperty -path "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\ DeviceAccess\Global\LooselyCoupled” -name "Value" -value "Deny" -propertyType string -force`
Beschreibung (GPO)	Erlauben Sie Apps, automatisch Informationen mit Drahtlosgeräten auszutauschen und zu synchronisieren, die nicht explizit mit Ihrem PC, Tablet oder Handy gekoppelt sind.
Hinweise	Einstellung auch auf Benutzeroberfläche "Einstellungen > Datenschutz" optionale Einstellung, in Benutzeroberfläche auch nur für einzelne Apps auswählbar

Feedbackhäufigkeit auf „Nie“ konfigurieren / Benachrichtigung nicht mehr anzeigen

Gruppenrichtlinie	./.
Einstellung	1.) PeriodInNanoSeconds 2.) NumberOfSIUFInPeriod
Gruppenrichtlinie (englisch)	1.) PeriodInNanoSeconds 2.) NumberOfSIUFInPeriod
Wert	1.) 0 2.) 0

Script (Powershell)	1.)
	`New-ItemProperty -path "HKCU\SOFTWARE\Microsoft\Siuf\Rules" -name " PeriodInNanoSeconds " -value "0" -propertyType dword –force`
	2.)
	`New-ItemProperty -path "HKCU\SOFTWARE\Microsoft\Siuf\Rules" -name "NumberOfSIUFInPeriod " -value "0" -propertyType dword -force`

Beschreibung (GPO)	Feedback soll von Windows angefordert werden: Nie.
Hinweise	Diese Einstellung bezieht sich nur auf das Benutzer-Feedback, und nicht auf die Telemetrie Daten. Diese Einstellung ist nicht als GPO verfügbar. Es ist derzeit lediglich möglich, mittels eines Registrierungsschlüssels im Userkontext eine Vorgabe dieser Einstellung zu bewirken.

Windows Fehlerberichterstattung deaktivieren

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Windows-Fehlerberichterstattung
Einstellung	Windows-Fehlerberichterstattung deaktivieren
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Windows Error Reporting > Disable Windows Error Reporting
Wert	Aktiviert
Script (Powershell)	`New-ItemProperty -path "HKLM\SOFTWARE\Policies\Microsoft\Windows\Windows Error Reporting" -name "Disabled" -value "1" -propertyType dword -force`
Beschreibung (GPO)	Durch diese Richtlinieneinstellung wird die Windows-Fehlerberichterstattung deaktiviert, sodass keine Berichtsdaten gesammelt oder an Microsoft oder interne Server innerhalb Ihres Unternehmens gesendet werden, wenn die Software unerwartet beendet wird oder ausfällt. Wenn Sie diese Richtlinieneinstellung aktivieren, sendet die Windows-Fehlerberichterstattung keine Probleminformationen an Microsoft. Darüber hinaus sind in der Systemsteuerung unter "Sicherheit und Wartung" auch keine Informationen zur Problemlösung verfügbar. Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, hat die Richtlinieneinstellung "Fehlerberichterstattung deaktivieren" unter "Computerkonfiguration/Administrative Vorlagen/System/Internetkommunikationsverwaltung/Internetkommunikationseinstellungen" Vorrang. Wenn "Fehlerberichterstattung deaktivieren" ebenfalls deaktiviert oder nicht konfiguriert ist, werden die Benutzereinstellungen in der Systemsteuerung unter "Windows-Fehlerberichterstattung" angewendet.
Hinweise	./.

WiFi-Sense deaktivieren

Gruppenrichtlinie	./.
Einstellung	./.
Gruppenrichtlinie (englisch)	./.
Wert	./.
Script (Powershell)	`New-ItemProperty -path "HKLM\SOFTWARE\Microsoft\WcmSvc\wifinetworkmanager\config" -name "AutoConnectAllowedOEM" -value "0" -propertyType dword -force`
Beschreibung (GPO)	Bei der WLAN-Optimierung werden Geräte automatisch mit bekannten Hotspots und den WLAN-Netzwerken verbunden, welche die Kontakte für die Person freigegeben haben.
Hinweise	WiFi-Sense ist nur auf Geräten mit WLAN Adapter verfügbar. Wird der Registrierungsschlüssel gesetzt, sind alle WiFi-Sense Optionen ausgegraut, und können auch von Anwendern mit administrativen Rechten nicht mehr über das Menü verändert werden. Man kann diese Einstellung als einmalige GPO Preference setzen, so dass bei Notwendigkeit der Registrierungsschlüssel lokal auf dem Client entfernt werden kann.

Nutzung von Positionsdaten deaktivieren

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows Komponenten > Suche
Einstellung	Der Suche und Cortana die Nutzung von Positionsdaten verbieten
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Search > Allow search and Cortana to use location
Wert	Deaktiviert
Script (Powershell)	./.
Beschreibung (GPO)	Diese Richtlinieneinstellung gibt an, ob von der Suche und Cortana standortabhängige Such- und Cortana-Ergebnisse bereitgestellt werden können. Wenn diese Option aktiviert ist, können die Suche und Cortana auf Positionsdaten zugreifen.
Hinweise	Cortana

Websuche für Desktopsuche deaktivieren

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows Komponenten > Suche
Einstellung	Websuche nicht zulassen
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Search > Do not allow web search
Wert	Aktiviert
Script (Powershell)	./.
Beschreibung (GPO)	Wenn diese Richtlinie aktiviert ist, wird die Option zum Durchsuchen des Webs aus der Windows-Desktopsuche entfernt. Wenn diese Richtlinie deaktiviert oder nicht konfiguriert ist, ist die Weboption verfügbar, und die Benutzer können das Web mithilfe des standardmäßigen Browsersuchmoduls durchsuchen.
Hinweise	Cortana

Websuche mit Cortana deaktivieren

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows Komponenten > Suche
Einstellung	Nicht im Web suchen und keine Webergebnisse in der Suche anzeigen
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Search > Don't search the web or display web results in Search
Wert	Aktiviert
Script (Powershell)	./.
Beschreibung (GPO)	Mit dieser Richtlinieneinstellung können Sie steuern, ob in der Suche Abfragen im Web durchgeführt werden können, und ob die Webergebnisse in der Suche angezeigt werden. Wenn Sie diese Richtlinieneinstellung aktivieren, werden keine Abfragen im Web durchgeführt, und es werden keine Webergebnisse angezeigt, wenn ein Benutzer in der Suche eine Abfrage durchführt. Wenn Sie diese Richtlinieneinstellung deaktivieren, werden Abfragen im Web durchgeführt, und es werden Webergebnisse angezeigt, wenn ein Benutzer in der Suche eine Abfrage durchführt. Wenn Sie diese Richtlinieneinstellung nicht konfigurieren, können Benutzer festlegen, ob bei der Suche Abfragen im Web durchgeführt werden können, und ob die Webergebnisse in der Suche angezeigt werden.
Hinweise	Cortana Hinweis von Microsoft: Es könnte dennoch ein wenig Netzwerkverkehr mit Bing.com bestehen, um zu bewerten, ob bestimmte Komponenten von Cortana auf dem neuesten Stand sind. Um diese Netzwerkaktivität vollständig zu deaktivieren, können Sie eine Windows Firewall-Regel erstellen, um ausgehenden Datenverkehr zu verhindern: Computerkonfiguration > Windows-Einstellungen > Sicherheitseinstellungen > Windows-Firewall mit erweiterter Sicherheit > Windows-Firewall mit erweiterter Sicherheit - <LDAP-Name> > ausgehende Regeln; Rechtsklick > neue Regel; im Assistenten: Seite "Regeltyp" > "Programm" wählen > weiter > Seite "Programm" > Programmpfad eingeben: %windir%\systemapps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe > weiter Seite "Aktion" > "Verbindung blockieren " wählen > weiter > Seite "Profil" > Kontrollkästchen "Domäne", "Privat" und "Öffentlich" aktivieren > weiter > Seite "Name" > Name eingeben, bspw. Cortana-Firewallkonfiguration > Fertig stellen > Rechtsklick auf die erstellte Regel > Eigenschaften > Reiter "Protokolle und Ports" > folgende Informationen wählen: - Protokolltyp: TCP - Lokaler Port: Alle Ports

- Remote-Port: Alle Ports
> mit OK bestätigen

Weitergabe von Informationen im Suchvorgang an Bing deaktivieren

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows Komponenten > Suche
Einstellung	Festlegen der in der Suche freizugebenden Informationen
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Search > Set what information is shared in Search
Wert	Aktiviert - Anonyme Informationen
Script (Powershell)	./.
Beschreibung (GPO)	Mit dieser Richtlinieneinstellung können Sie steuern, welche Informationen in der Suche für Bing freigegeben werden. Wenn Sie diese Richtlinieneinstellung aktivieren, können Sie eine von vier Einstellungen festlegen, die von Benutzern nicht geändert werden kann: • Benutzerinformationen und Standort: Freigabe des Suchverlaufs, eines Teils der Microsoft-Kontoinformationen und des genauen Standorts des Benutzers, um die Suche und weitere Microsoft-Funktionen zu personalisieren. • Nur Benutzerinformationen: Freigabe des Suchverlaufs und eines Teils der Microsoft-Kontoinformationen des Benutzers, um die Suche und weitere Microsoft-Funktionen zu personalisieren. • Anonyme Informationen: Freigabe von Nutzungsinformationen, aber keine Freigabe des Suchverlaufs, der Microsoft-Kontoinformationen oder des genauen Standorts. Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, können die Benutzer wählen, welche Informationen bei der Suche freigegeben werden.
Hinweise	Cortana

Insider Builds deaktivieren

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows Komponenten > Datensammlung und Vorabversionen
Einstellung	Benutzersteuerung für Insider-Builds ein-/ausschalten
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Data Collection and Preview Builds > Toggle user control over Insider builds
Wert	Deaktiviert
Script (Powershell)	./.
Beschreibung (GPO)	This policy setting determines whether users can access the Insider build controls in the Advanced Options for Windows Update. These controls are located under "Get Insider builds," and enable users to make their devices available for downloading and installing Windows preview software. If you enable or do not configure this policy setting, users can download and install Windows preview software on their devices. If you disable this policy setting, the item "Get Insider builds" will be unavailable. Note: This policy setting applies only to devices running the Pro, Enterprise, or Server editions of Windows 10.
Hinweise	./.

Seitenvorschläge im Internet Explorer deaktivieren

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows Komponenten > Internet Explorer
Einstellung	"Vorgeschlagene Sites" aktivieren
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Turn on Suggested Sites
Wert	Deaktiviert
Script (Powershell)	./.
Beschreibung (GPO)	Diese Richtlinieneinstellung steuert das Feature "Vorgeschlagene Sites" auf Grundlage der Browseraktivität des Benutzers. "Vorgeschlagene Sites" meldet den Browserverlauf eines Benutzers an Microsoft, um Sites vorzuschlagen, die für den Benutzer möglicherweise interessant sind. Wenn Sie diese Richtlinieneinstellung aktivieren, wird der Benutzer nicht zur Aktivierung des Feature "Vorgeschlagene Sites" aufgefordert. Der Browserverlauf des Benutzers wird an Microsoft gesendet, um Vorschläge zu erzeugen. Wenn Sie diese Richtlinieneinstellung deaktivieren, werden die diesem Feature zugeordneten Einstiegspunkte und Funktionen deaktiviert. Wenn Sie diese Richtlinieneinstellung nicht konfigurieren, kann der Benutzer das Feature "Vorgeschlagene Sites" aktivieren oder deaktivieren.
Hinweise	Internet Explorer

Suchvorschläge für Microsoftdienste deaktivieren

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows Komponenten > Internet Explorer
Einstellung	Für Microsoft-Dienste das Bereitstellen von erweiterten Vorschlägen zulassen, wenn Benutzer Text in die Adressleiste eingeben
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Allow Microsoft services to provide enhanced suggestions as the user types in the Address bar
Wert	Deaktiviert
Script (Powershell)	./.
Beschreibung (GPO)	Mit dieser Richtlinieneinstellung wird Internet Explorer in die Lage versetzt, erweiterte Vorschläge bereitzustellen, wenn Benutzer Text in die Adressleiste eingeben. Zum Bereitstellen der erweiterten Vorschläge werden die Tastenanschläge des Benutzers über Microsoft-Dienste an Microsoft gesendet. Wenn Sie diese Richtlinieneinstellung aktivieren, erhalten Benutzer beim Eingeben von Text in die Adressleiste erweiterte Vorschläge. Außerdem können Benutzer im Charm "Einstellungen" dann nicht die Einstellung "Vorschläge" ändern. Wenn Sie diese Richtlinieneinstellung deaktivieren, erhalten Benutzer beim Eingeben von Text in die Adressleiste keine erweiterten Vorschläge. Außerdem können Benutzer im Charm "Einstellungen" dann nicht die Einstellung "Vorschläge" ändern. Wenn Sie diese Richtlinieneinstellung nicht konfigurieren, können Benutzer im Charm "Einstellungen" die Einstellung "Vorschläge" ändern.
Hinweise	Internet Explorer

Autovervollständigung für Webadressen

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows Komponenten > Internet Explorer
Einstellung	AutoVervollständigen für Webadressen deaktivieren
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Turn off the auto-complete feature for web addresses
Wert	Aktiviert
Script (Powershell)	./.
Beschreibung (GPO)	Diese AutoVervollständigen-Funktion schlägt passende Ergänzungen vor, wenn Benutzer Webadressen in die Adressleiste des Browsers eingeben. Wenn Sie diese Richtlinieneinstellung aktivieren, werden den Benutzern beim Eingeben von Webadressen keine Vorschläge gemacht. Benutzer können die Einstellungen für das AutoVervollständigen von Webadressen nicht ändern. Wenn Sie diese Richtlinieneinstellung deaktivieren, werden den Benutzern beim Eingeben von Webadressen Vorschläge gemacht. Benutzer können die Einstellungen für das AutoVervollständigen von Webadressen nicht ändern. Wenn Sie diese Richtlinieneinstellung nicht konfigurieren, können die Benutzer entscheiden, ob sie die AutoVervollständigen-Funktion für Webadressen ein- oder ausschalten möchten.
Hinweise	Internet Explorer optionale Einstellung

Periodische Suche nach Browser-Updates

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows Komponenten > Internet Explorer
Einstellung	Periodische Überprüfungen auf Internet Explorer-Softwareupdates deaktivieren
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Disable Periodic Check for Internet Explorer software updates
Wert	Aktiviert
Script (Powershell)	./.
Beschreibung (GPO)	Verhindert, dass Internet Explorer überprüft, ob eine neue Version des Browsers verfügbar ist. Wenn Sie diese Richtlinie aktivieren, überprüft Internet Explorer nicht, ob eine neuere Version des Browsers bereitsteht, und informiert die Benutzer nicht darüber. Wenn Sie diese Richtlinie deaktivieren oder nicht konfigurieren, überprüft Internet Explorer dies alle 30 Tage und benachrichtigt die Benutzer, wenn eine neue Version zur Verfügung steht. Mit dieser Richtlinie können Administratoren steuern, welche Version von Internet Explorer verwendet wird, da die Benutzer nicht benachrichtigt werden, wenn es eine neue Version des Browsers gibt.
Hinweise	Internet Explorer optionale Einstellung

von Webseiten angeforderte Positionsdaten vom Browser

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows Komponenten > Internet Explorer
Einstellung	Browser-Geolocation deaktivieren
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Turn off browser geolocation
Wert	Aktiviert
Script (Powershell)	./.
Beschreibung (GPO)	Mit dieser Richtlinieneinstellung können Sie die Unterstützung für Browser-Geolocation deaktivieren. So wird verhindert, dass Websites Standortdaten über den Benutzer anfordern. Wenn Sie diese Richtlinieneinstellung aktivieren, wird die Unterstützung für Browser-Geolocation deaktiviert. Wenn Sie diese Richtlinieneinstellung deaktivieren, wird die Unterstützung für Browser-Geolocation aktiviert. Wenn Sie diese Richtlinieneinstellung nicht konfigurieren, kann die Unterstützung für Browser-Geolocation unter "Internetoptionen" auf der Registerkarte "Datenschutz" aktiviert oder deaktiviert werden.
Hinweise	Internet Explorer optionale Einstellung

Blockierte ActiveX-Steuerelementen - Download von aktualisierten Listen deaktivieren

Gruppenrichtlinie	./.
Einstellung	./.
Gruppenrichtlinie (englisch)	./.
Wert	./.
Script (Powershell)	`bitte ergänzen falls vorhanden`
Beschreibung (GPO)	Wenn ActiveX-Steuerelemente blockiert werden, wird in regelmäßigen Abständen eine aktualisierte Liste der veralteten ActiveX-Steuerelemente heruntergeladen, die blockiert werden sollen. Der Download kann mit einer Registrierungseinstellung deaktiviert werden.
Hinweise	Internet Explorer REG_DWORD-Registrierungseinstellung: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\VersionManager\DownloadVersionList > Wert auf "0" stellen

Autoausfüllen-Funktion auf Webseiten

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows Komponenten > Microsoft Edge
Einstellung	Ermöglicht Ihnen, Benutzern die Verwendung von AutoAusfüllen auf Websites zu erlauben
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Microsoft Edge > Allows you to let people use autofill on websites
Wert	Deaktiviert
Script (Powershell)	./.
Beschreibung (GPO)	Mit dieser Einstellung legen Sie fest, ob Benutzer AutoAusfüllen auf Websites verwenden dürfen. Die Einstellung ist standardmäßig aktiviert. Wenn Sie diese Einstellung aktivieren, können Benutzer AutoAusfüllen auf Websites verwenden und Informationen lokal zwischenspeichern. Wenn Sie diese Einstellung deaktivieren, können die Benutzer AutoAusfüllen nicht verwenden.
Hinweise	Microsoft Edge optionale Einstellung

"Do Not Track"-Anforderung an Webseiten senden

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows Komponenten > Microsoft Edge
Einstellung	Ermöglicht Ihnen, Benutzern das Senden von DNT-Kopfzeilen zu erlauben
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Microsoft Edge > Allows you to let people send Do Not Track headers
Wert	Aktiviert
Script (Powershell)	`./.`
Beschreibung (GPO)	Mit dieser Einstellung legen Sie fest, ob Benutzer DNT-Kopfzeilen senden dürfen. Die Einstellung ist standardmäßig deaktiviert. Wenn Sie diese Einstellung aktivieren, können Benutzer DNT-Kopfzeilen von jedem Computer der Organisation senden. Wenn Sie diese Einstellung deaktivieren, können Benutzer keine DNT-Kopfzeilen senden.
Hinweise	Microsoft Edge

Passwort-Manager im Browser

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows Komponenten > Microsoft Edge
Einstellung	Ermöglicht das Konfigurieren des Kennwort-Managers
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Microsoft Edge > Allows you to configure password manager
Wert	Deaktiviert
Script (Powershell)	./.
Beschreibung (GPO)	Mit dieser Einstellung legen Sie fest, ob Benutzer Kennwörter lokal auf ihren Computern speichern können. Die Einstellung ist standardmäßig aktiviert. Wenn Sie diese Einstellung aktivieren, ist der Kennwort-Manager eingeschaltet, und Benutzer können Kennwörter lokal auf ihren Computern speichern. Wenn Sie diese Einstellung deaktivieren, ist der Kennwort-Manager ausgeschaltet, und die Benutzer können Kennwörter nicht lokal speichern.
Hinweise	Microsoft Edge

Suchvorschläge auf Adressleiste anzeigen

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows Komponenten > Microsoft Edge
Einstellung	Blockiert die Anzeige von Suchvorschlägen auf der Adressleiste
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Microsoft Edge > Stops address bar from showing search suggestions
Wert	Deaktiviert
Script (Powershell)	./.
Beschreibung (GPO)	Mit dieser Einstellung legen Sie fest, ob Suchvorschläge auf der Adressleiste angezeigt werden. Die Einstellung ist standardmäßig aktiviert. Wenn Sie diese Einstellung aktivieren, werden den Benutzern Suchvorschläge in der Adressleiste angezeigt. Wenn Sie diese Einstellung deaktivieren, werden in der Adressleiste keine Suchergebnisse angezeigt.
Hinweise	Microsoft Edge optionale Einstellung

Experimentiermodus abschalten

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows Komponenten > Datensammlung und Vorabversionen
Einstellung	Features oder Einstellungen der Vorabversion deaktivieren
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Data Collection and Preview Builds > Disable pre-release features or settings
Wert	Deaktiviert
Script (Powershell)	./.
Beschreibung (GPO)	Durch diese Richtlinie wird festgelegt, in welchem Umfang Microsoft mit dem Produkt experimentieren kann, um die Benutzereinstellungen oder das Geräteverhalten zu untersuchen. Beim Wert 1 ist Microsoft nur berechtigt, Geräteeinstellungen zu konfigurieren. Beim Wert 2 darf Microsoft den vollständigen Experimentiermodus nutzen. Wenn Sie diese Richtlinieneinstellung deaktivieren, wird der Experimentiermodus vollständig ausgeschaltet. Wenn Sie diese Richtlinieneinstellung nicht konfigurieren, können Benutzer die Option "Microsoft das Testen von Features in diesem Build gestatten" in den Einstellungen konfigurieren.
Hinweise	./.

Speicherort für Postition deaktivieren

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Position und Sensoren
Einstellung	Speicherort deaktivieren
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Location and Sensors > Turn off location
Wert	Aktiviert
Script (Powershell)	./.
Beschreibung (GPO)	Mit dieser Richtlinieneinstellung wird das Positionsfeature für den Computer deaktiviert. Wenn Sie diese Richtlinieneinstellung aktivieren, wird das Positionsfeature deaktiviert, und keines der auf dem Computer ausgeführten Programme kann Standortinformationen aus dem Positionsfeature verwenden. Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, können alle auf diesem Computer ausgeführten Programme Standortinformationen aus dem Positionsfeature verwenden.
Hinweise	Sollten Apps verwendet werden müssen, die ohne Abrufen von Positionsdaten nicht funktionsfähig sind, sollte das Deaktivieren dieser Funktion nicht erzwungen werden.

Sensorfeature deaktivieren

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Position und Sensoren
Einstellung	Sensoren deaktivieren
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Location and Sensors > Turn off sensors
Wert	Aktiviert
Script (Powershell)	./.
Beschreibung (GPO)	Mit dieser Richtlinieneinstellung wird das Sensorfeature für den Computer deaktiviert. Wenn Sie diese Richtlinieneinstellung aktivieren, wird das Sensorfeature deaktiviert und kann von keinem der auf dem Computer ausgeführten Programme verwendet werden. Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, können alle auf diesem Computer ausgeführten Programme das Sensorfeature verwenden.
Hinweise	Sollten Apps verwendet werden müssen, die ohne Abrufen von Positionsdaten oder Umgebungsdaten nicht funktionsfähig sind, sollte das Deaktivieren dieser Funktion nicht erzwungen werden. (Bsp. Lichtsensoren für automatische Einstellung der Bildschirmhelligkeit)

Positionsskripting von Programmen unterbinden

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Position und Sensoren
Einstellung	Positionsskripting deaktivieren
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Location and Sensors > Turn off location scripting
Wert	Aktiviert
Script (Powershell)	./.
Beschreibung (GPO)	Mit dieser Richtlinieneinstellung wird das Skripting für das Positionsfeature deaktiviert. Wenn Sie diese Richtlinieneinstellung aktivieren, werden keine Skripts für das Positionsfeature ausgeführt. Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, werden alle Positionsskripts ausgeführt.
Hinweise	Sollten Apps verwendet werden müssen, die ohne Abrufen von Positionsdaten nicht funktionsfähig sind, sollte das Deaktivieren dieser Funktion nicht erzwungen werden.

Handschrifterkennung deaktivieren

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Systemsteuerung > Regions- und Sprachoptionen > Handschriftanpassung
Einstellung	Automatisches Lernen deaktivieren
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Control Panel > Regional and Language Options > Handwriting personalization > Turn off automatic learning
Wert	Aktiviert
Script (Powershell)	./.
Beschreibung (GPO)	Diese Richtlinieneinstellung deaktiviert die Komponente für das automatischen Lernen der Handschrifterkennungsanpassung. Automatisches Lernen ermöglicht dem Benutzer das Sammeln und Speichern von Text und Freihandeingaben, um die Handschrifterkennung an das Vokabular und die Handschrift des Benutzers anzupassen. Zu den gesammelten Texten gehören alle ausgehenden Nachrichten in Windows Mail und in MAPI-E-Mail-Clients sowie die URLs aus dem Browserverlauf von Internet Explorer. Gespeichert werden Informationen wie Worthäufigkeit und Wörter, die den Handschrifterkennungsmodulen noch unbekannt sind (beispielsweise Eigennamen und Akronyme). Durch das Löschen von E-Mail-Inhalten oder des Browserverlaufs werden die gespeicherten Anpassungsdaten nicht gelöscht. Über den Eingabebereich vorgenommene Freihandeingaben werden gesammelt und gespeichert. Hinweis: Möglicherweise ist das automatische Lernen von Text und Freihandeingaben nicht für alle Sprachen verfügbar, selbst wenn die Handschriftanpassung verfügbar ist. Weitere Informationen finden Sie in der Tablet PC-Hilfe. Wenn diese Richtlinieneinstellung aktiviert wird, wird das automatische Lernen beendet, und alle gespeicherten Daten werden gelöscht. Benutzer können diese Richtlinieneinstellung nicht in der Systemsteuerung konfigurieren. Wenn Sie diese Richtlinie deaktivieren, wird das automatische Lernen aktiviert. Benutzer können diese Richtlinieneinstellung nicht in der Systemsteuerung konfigurieren. Gesammelte Daten werden nur bei aktivierter Handschriftanpassung für die Handschrifterkennung verwendet. Wenn diese Richtlinie nicht konfiguriert wird, können Benutzer wählen, ob sie das automatische Lernen aktivieren oder deaktivieren möchten. Dies kann entweder in der Systemsteuerung unter den Tablet-Einstellungen auf der Registerkarte "Handschrift" erfolgen oder im Anmeldedialog. Diese Richtlinieneinstellung ist mit der Richtlinieneinstellung "Handschriftanpassung deaktivieren" verwandt. Hinweis: Der für Freihandeingaben reservierte Speicherplatz ist auf 50

MB begrenzt, der für Textinformationen auf ungefähr 5 MB. Werden diese Grenzwerte erreicht und neue Daten gesammelt, werden alte Daten gelöscht, um Platz für die neueren Daten zu schaffen. Die Handschriftanpassung funktioniert nur mit Handschrifterkennungen von Microsoft, nicht mit Erkennungen von Drittanbietern.

Hinweise ./.

Synchronisation der Einstellungen unterbinden

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Einstellungen synchronisieren
Einstellung	Nicht synchronisieren
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Sync your settings > Do not sync
Wert	Aktiviert
Script (Powershell)	./.
Beschreibung (GPO)	Verhindert die Beteiligung dieses PCs an der Synchronisierung. Hierdurch wird in den PC-Einstellungen auf der Seite "Einstellungen synchronisieren" die Option "Einstellungen synchronisieren" ausgeschaltet und deaktiviert. Wenn Sie diese Richtlinieneinstellung aktivieren, wird "Einstellungen synchronisieren" ausgeschaltet, und auf dem PC wird keine der Gruppen vom Typ "Einstellungen synchronisieren" synchronisiert. Bei Verwendung der Option "Benutzern das Einschalten der Synchronisierung ermöglichen" ist die Synchronisierung standardmäßig ausgeschaltet, aber nicht deaktiviert. Wenn Sie diese Einstellung nicht festlegen oder deaktivieren, ist die Option "Einstellungen synchronisieren" standardmäßig eingeschaltet und kann vom Benutzer konfiguriert werden.
Hinweise	Relevant nur bei Anmeldung mit Microsoft-Konto oder -Geschäftskonto.

Deaktivierung Windows-Store

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Store
Einstellung	Alle Apps aus Windows Store deaktivieren
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > System > Internet Communication Management > Internet Communication settings > Turn off access to the Store
Wert	./.
Script (Powershell)	./.
Beschreibung (GPO)	./.
Hinweise	Nutzung des Windows Store nur mit Microsoft-Konto Möglichkeit, das Starten vorinstallierter oder heruntergeladener Apps zu deaktivieren automatische Aktualisierung von Apps wird ausgeschaltet und der Windows Store deaktiviert

Updates aus anderen Quellen deaktivieren

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Übermittlungsoptimierung
Einstellung	Downloadmodus
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Windows Update > Do not connect to any Windows Update Internet locations
Wert	Option: Keine
Script (Powershell)	./.
Beschreibung (GPO)	Über die Optionen können Sie auswählen, wo Updates und Apps im Rahmen der Übermittlungsoptimierung empfangen oder wohin sie gesendet werden. • Keine: Deaktiviert die Übermittlungsoptimierung • Gruppe: Übermittelt Updates und Apps zwischen PCs innerhalb derselben lokalen Netzwerkdomäne • Internet: Ruft Updates und Apps von PCs im Internet ab bzw. sendet sie an diese PCs • LAN: Übermittelt Updates und Apps nur zwischen PCs mit derselben NAT
Hinweise	Weitere Informationen finden sich im Empfehlungspapier unter Abschnitt "Windows Update"

internen Microsoft Updatedienst aktivieren

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Windows Update
Einstellung	Internen Pfad für den Microsoft Updatedienst angeben
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Windows Components > Windows Update > Specify intranet Microsoft update service location
Wert	Aktivier URL des internen Updatedienstes eingeben
Script (Powershell)	./.
Beschreibung (GPO)	Gibt einen Intranetserver an, der als Host für die Updates von Microsoft Update fungiert. Mit diesem Updatedienst können Sie dann die Computer in Ihrem Netzwerk automatisch aktualisieren. Mit dieser Einstellung können Sie einen Server im Netzwerk als Host für einen internen Updatedienst bestimmen. Der Client für automatische Updates durchsucht diesen Dienst nach Updates, die auf die Computer in Ihrem Netzwerk angewendet werden können. Wenn Sie diese Einstellung verwenden möchten, müssen Sie zwei Servernamen festlegen: den Server, auf dem der Client für automatische Updates die Updates erkennt und von dem er sie herunterlädt, und den Server, auf den die aktualisierten Arbeitssstationen die Statistiken hochladen. Sie können für beide Werte den gleichen Server festlegen. Wenn der Status auf "Aktiviert" festgelegt ist, stellt der Client für automatische Updates eine Verbindung mit dem angegebenen Microsoft Updatedienst im Intranet und nicht mit Windows Update her, um nach Downloads zu suchen und herunterzuladen. Durch Aktivieren dieser Einstellung müssen Endbenutzer in Ihrer Organisation die Updates nicht über eine Firewall herunterladen. Außerdem können Sie auf diese Weise die Updates vor der Bereitstellung testen. Wenn der Status auf "Deaktiviert" oder "Nicht konfiguriert" festgelegt ist und "Automatische Updates" nicht durch eine Richtlinie oder benutzerdefinierte Einstellung deaktiviert sind, stellt der Client für automatische Updates direkt eine Verbindung mit der Windows Update-Website im Internet her. Hinweis: Diese Richtlinie hat keine Auswirkung, falls die Richtlinie "Automatische Updates konfigurieren" deaktiviert ist. Hinweis: Diese Richtlinie wird unter Windows RT nicht unterstützt. Das Aktivieren dieser Richtlinie auf PCs, auf denen Windows RT ausgeführt wird, hat keinerlei Auswirkung
Hinweise	REG_DWORD-Registrierungseinstellung: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\DoNotConnectToWindowsUpdateInternetLocations > Wert auf "1" stellen

Benachrichtigungen auf Sperrbildschirm deaktivieren

Gruppenrichtlinie	Computerkonfiguration > Administrative Vorlagen > Systemsteuerung > Anpassung
Einstellung	Ein bestimmtes Standardbild für den Sperrbildschirm erzwingen
Gruppenrichtlinie (englisch)	Computer Configuration > Administrative Templates > Control Panel > Personalization > Force a specific default lock screen image
Wert	Aktiviert Häkchen bei "Unterhaltung Tipps, Tricks und mehr auf dem Sperrbildschirm" entfernen
Script (Powershell)	./.
Beschreibung (GPO)	diese Funktion verhindert die Anzeige von Benachrichtigungen auf dem Sperrbildschirm
Hinweise	./.