12 Gruppenrichtlinien in Windows 10

In diesem Kapitel werden folgende Themen behandelt:

- Wichtige Änderungen in Windows 10
- Startmenü, Taskleiste und Dateiverknüpfungen anpassen
- Windows Update anpassen
- Privatsphäre-Einstellungen konfigurieren
- Virtualisierungsbasierte Sicherheit in Windows 10
- Der Edge-Browser

12.1 Windows 10 – Software as a Service

Bevor wir in das Thema Gruppenrichtlinien in Windows 10 einsteigen, möchte ich hier einige grundlegende Konzepte von Windows 10 klären, die für das Verständnis einiger Funktionen wichtig sind.

Microsoft hat bei Erscheinen Windows 10 als das letzte Client-Windowssystem bezeichnet und bekanntgegeben, dass es kein Windows 11 geben wird. Wie Sie vermutlich schon gemerkt haben, heißt das aber keinesfalls, dass Microsoft Windows nicht mehr weiterentwickelt, sondern Windows 10 ist jetzt einfach ein Synonym für Windows geworden, und die Version verbirgt sich in der Feature-Release-Nummer.

Feature Releases oder kurz FR sind zweimal im Jahr erscheinende Upgrades, die das alte Feature Release vollständig ersetzen. Für den Upgrade-Vorgang wird das neue Feature Release im Hintergrund heruntergeladen und nach dem nächsten Neustart durch Windows PE installiert. Bei PE handelt es sich um ein Mini-Windows, das seit Windows Vista den Installationsprozess steuert, sich aber auch für Wartungszwecke einsetzen lässt.

Während des Upgrade-Vorgangs wird der Windows-Ordner in Windows.old umbenannt. Anschließend wird das neue Feature Release in einem neuen Windows-Ordner bereitgestellt und die Daten aus dem alten Windows-Ordner werden in der neuen Installation übernommen. Man spricht auch von einem In-Place-Upgrade. Genau genommen ist die Installation eines Feature Release also immer eine Neuinstallation.

Zur Drucklegung trägt das aktuelle Feature Release den Namen 20H2. Er setzt sich aus dem Jahr und dem Halbjahr zusammen, zu dem das Release bei Microsoft veröffentlicht wurde. Bis zum Frühjahr 2020 wurde noch das alte Namensschema verwendet, das statt dem Halbjahr die Nummer des Monats trug, in dem das FR bei Microsoft offiziell freigegeben wurde, was aber nicht zwingend auch dem Verfügbarkeitstermin entsprach. Die Version 1803 wurde z. B. erst Ende April an Endkunden verteilt. Microsoft hat es aus Gründen der Qualitätssicherung jetzt zum Glück aufgegeben, pünktlich alle 6 Monate ein neues Release zu veröffentlichen und die Namen der FR entsprechend angepasst. Dementsprechend können wir aktuell auf folgende Releases zurückblicken:

Tabelle 12.1 Windows 10 Releases bis Herbst 2020
Quelle: *https://en.wikipedia.org/wiki/Windows_10_version_history*

Release	Code-Name	Marketing-Name	Erscheinungsdatum	auch LSTB
1507	Threshold 1	–	29.07.2015	X
1511	Threshold 2	November Update	20.11.2015	
1607	Redstone 1	Anniversary Update	2.08.2016	X
1703	Redstone 2	Creators Update	5.04.2017	
1709	Redstone 3	Fall Creators Update	17.10.2017	
1803	Redstone 4	April 2018 Update	20.04.2018	
1809	Redstone 5	October 2018 Update	2.10.2018	X
1903	19H1	May 2019 Update	21.05.2019	
1909	19H2	November 2019 Update	12.11.2019	
2004	20H1	May 2020 Update	27.05.2020	
20H2	20H2	October 2020 Update	20.10.2020	

Neben der FR-Nummer hat Microsoft noch ein paar zusätzliche Namen eingeführt. So gibt es noch einen internen Code-Namen, der bereits seit 2019 aus dem Schema Release-Jahr und Release-Halbjahr besteht. Zusätzlich gibt es noch einen Marketingnamen, der sich auf den Release-Monat bezieht. Zum Glück hat Microsoft die Namen vereinheitlicht, da es selbst Experten manchmal schwer fiel noch nachzuvollziehen, von welcher Version die Rede war. Ich beziehe mich im Buch immer auf die FR-Nummer, weil diese einfach zu merken und eindeutig ist.

Mit den Feature Releases hat Microsoft auch den Support-Zeitraum mehrfach geändert. Im Gegensatz zu vorherigen Versionen von Windows, für die es immer zehn Jahre lang Sicherheitsupdates gab, sind es für Windows 10, je nach Version und halbjährlichem Release, maximal 30 Monate. Maximal heißt, dass dieser Zeitraum (Stand November 2020) nur die Enterprise Edition von Windows 10 betrifft, während alle anderen Versionen (Professional, Home) nur 18 Monate mit den sogenannten Quality-Updates versorgt werden. Mit der Ver-

sion 1809 hat Microsoft den Support-Zeitraum für die Enterprise-Edition noch einmal angepasst. Für die H2-Versionen ist er nun 30 Monate, für die Frühjahrs-Versionen dagegen nur 18 Monate. Die Supportzeiträume sind unterschiedlich, da Microsoft aktuell nur noch kleine Änderungen in das H2-Update einpflegt, während die großen Änderungen in das H1-Update einfließen. Das führt erstmals auch dazu, dass ein Update von einem H1 auf das nachfolgende H2-FR keine komplette Neuinstallation mehr erfordert, sondern nur noch ein einfaches Update.

Es gibt allerdings eine Ausnahme von dieser Regel, und das ist der sogenannte Long-Term Servicing Channel (LTSC). Diese speziellen Versionen von Windows, die es nur als Enterprise Edition gibt, werden zehn Jahre lang von Microsoft mit Updates versorgt. Das hat allerdings einen Preis, denn den LTSC-Versionen fehlen alle Features, die regelmäßig aktualisiert werden oder auf Cloud-Dienste zugreifen, also Cortana (die Windows-Sprachsteuerung), Windows Apps und der Edge-Browser.

Semi-Annual Updates und der Long-Term Servicing Channel

Die Feature Releases von Microsoft erscheinen seit April 2017 in halbjährlichem Abstand. Bis zur Version 2004 versuchte Microsoft, alle sechs Monate ein komplett neues Release herauszubringen. Ganz offensichtlich war es aber nicht möglich, im Vorfeld alle neuen Funktionen ausreichend zu testen, was mit jedem neuen FR zu massiven Fehlern und Stabilitätsproblemen führte. Seit der 20H1 hält sich Microsoft daher nicht mehr sklavisch an den 6-monatigen Release-Zeitraum mit Releases im März und September, sondern veröffentlicht ein FR erst dann, wenn diese ausreichend stabil ist. Außerdem ist nur noch das Frühjahrs-Update ein großes Update, während das Herbst-Update eher ein Stabilitäts-Update mit kleinen Änderungen, aber dafür 30 Monaten Support, ist.

Für spezielle Einsatzzwecke wie Geldautomaten oder Kassensysteme stellt Microsoft außerdem in unregelmäßigen Abständen für bestimmte Feature-Releases der Enterprise-Edition eine Version mit zehnjährigem Support bereit. Diese werden als Long-Term Service Channel (LTSC) – bis 2016 Long-Term Service Branch – bezeichnet und müssen gesondert lizenziert werden – man kann sie also nicht auf normalem Weg kaufen. Aktuell sind das die Feature-Release 1507, 1607 und 1809. Die nächste Version im LTSC wird voraussichtlich im Herbst 2021 erscheinen.

Alte Bezeichnung	umbenannt in
Current Branch	Semi-Annual Update (Targetted)
Current Branch for Business	Semi-Annual Update
Long-Term Service Branch	Long-Term Servicing Channel

12.1.1 Windows Updates verteilen

Neben den Feature-Updates hat Microsoft aber auch Änderungen an der Art und Weise vorgenommen, wie Sicherheitsupdates und Fehlerbereinigungen, jetzt als Quality Updates bezeichnet, verteilt werden. Quality Updates kommen nur noch in Form sogenannter kumulativer Updates (CU). Ein CU beinhaltet jeweils alle Updates, die seit Erscheinen eines Release veröffentlicht wurden, also auch alle Updates, die ein Computer bereits erhalten hat. Dadurch wird sichergestellt, dass ein Computer immer alle verfügbaren Updates installiert hat – man kann kein Update mehr auslassen. Da die CUs sehr schnell sehr groß werden (größer als 1 GB), hat Microsoft Express-Updates eingeführt. Mit ihrer Hilfe kann der Client die Updates ermitteln und installieren, die er wirklich benötigt. Express-Updates lösen Delta-Updates ab, die nur die Differenz zum jeweiligen vorhergehenden CU enthielten. Mehr zum Thema finden Sie unter *https://techcommunity.microsoft.com/t5/Windows-IT-Pro-Blog/Windows-10-quality-updates-explained-amp-the-end-of-delta/ba-p/214426* oder kurz *https://bit.ly/2LwMMYd*. Wenn Sie zur Update-Verteilung WSUS einsetzen, müssen Sie die Verteilung von Express-Updates explizit aktivieren, da Sie bis zu achtmal mehr Speicherplatz auf dem Server benötigen.

Zusammengefasst verteilt Microsoft also zwei[1] unterschiedliche Typen von Updates – Feature-Updates, die das Betriebssystem auf eine neue Version hieven, und Quality-Updates in Form von kumulativen Updates, die Fehler bereinigen. Beide Typen von Updates lassen sich nach wie vor über einen Windows Update Server (WSUS) bereitstellen. Sie benötigen für die Bereitstellung von Feature Releases mindestens WSUS 4.0. Wenn Sie Windows Server 2012 oder neuer als Betriebssystem für Ihren WSUS verwenden, aktualisiert sich der WSUS selbst auf die aktuellste Version. Windows Server 2008 R2 wird nicht mehr unterstützt.

Mehr zum Thema Servicing Channels von Microsoft direkt finden Sie unter *https://docs.microsoft.com/en-us/windows/deployment/update/waas-overview* oder kurz *https://bit.ly/2rKZI26*.

12.1.2 Windows Update for Business

Windows Update for Business ist ein alternatives Bereitstellungsverfahren für Updates, das Microsoft mit Windows 10 eingeführt hat. Genau genommen ist Windows Update for Business eigentlich gar nicht neu, sondern ein aufgebohrter Windows Update-Client, der bessere Steuerungsmöglichkeiten mit sich bringt.

Sie beziehen mit Windows Update for Business Ihre Updates nicht über einen zentralen Update-Server wie den WSUS, sondern über einen von Microsofts Update Servern oder alternativ andere Clients, die das Update bereits heruntergeladen haben (Peer-to-Peer). Das zweite Feature wird auch Delivery Optimization genannt und ähnelt dem BitTorrent-Verfahren, das früher auch gerne zum Teilen von Daten über das Internet verwendet wurde.

Das, was Windows Update for Business vom klassischen Windows Update unterscheidet, ist die Möglichkeit zu steuern, wann Updates zur Verfügung gestellt werden sollen, und zwar

[1] Genau genommen ist das nicht ganz korrekt, denn es gibt noch eine Reihe von zusätzlichen Update-Typen wie Servicing-Stack Updates, die den Windows Update Client aktualisieren, Windows Defender Updates sowie Treiber-Updates. Servicing-Stack Updates werden inzwischen ins CU integriert.

über einen Satz von einfachen Regeln. Das hat den Vorteil, dass Sie sich um die Freigabe von Updates nicht mehr kümmern müssen, sondern nur noch definieren, wann und wie ein Update zur Verfügung gestellt werden soll. Die Bereitstellung wird dann zeitgesteuert und automatisch vorgenommen. Das Konzept geht davon aus, dass es keine Einzelupdates mehr gibt, sondern nur noch kumulative Updates und Features, die eh eingespielt werden müssen. Warum also noch manuell freischalten? Wenn es wirklich zum Worst Case kommt und ein Update bei Ihnen nicht funktioniert, können Sie manuell eingreifen und das Bereitstellen von Updates für einen Zeitraum von bis zu 35 Tagen komplett aussetzen. Feature-Updates können nach der Installation für standardmäßig 10 Tage wieder deinstalliert werden

Das Windows Update for Business kann lokal in den Windows 10-Einstellungen über **Update und Sicherheit – Windows Update – Erweiterte Optionen** konfiguriert werden. Unter Windows 10 Home können Sie nur Anpassungen an der Übermittlungsoptimierung vornehmen, alle anderen Funktionen sind der Pro, Enterprise und Education Edition vorbehalten.

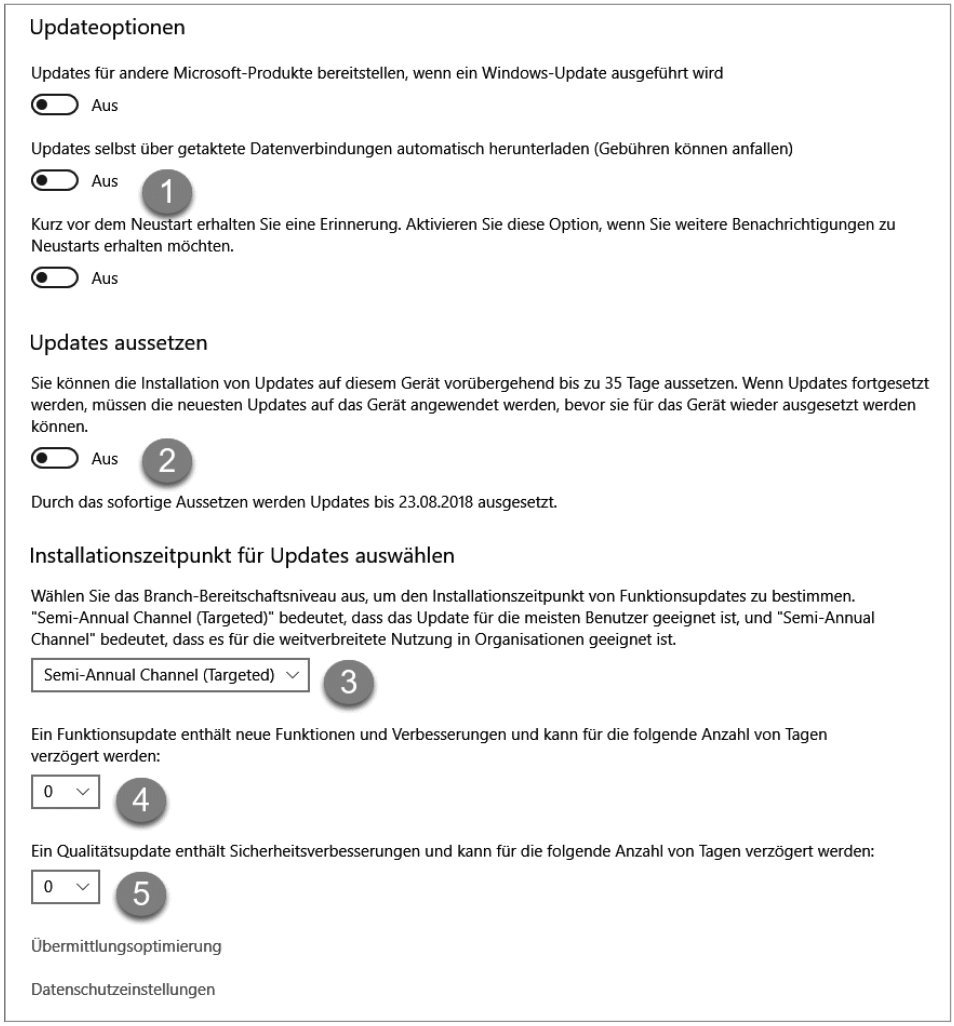


Bild 12.1 Die Updateoptionen von Windows 10 1909

In Bild 12.1 sehen Sie die lokalen Einstellungsmöglichkeiten von Windows 10 1909. Über „Updates selbst über getaktete Datenverbindungen herunterladen“ (1) können Sie festlegen, ob ein Update auch über Mobilverbindungen heruntergeladen werden soll. Mit „Updates aussetzen“ (2) können Sie Updates für bis zu 35 Tage deaktivieren – geben Sie hierzu in der Drop-Down-Liste an, bis wann die Updateprüfung ausgeschaltet sein soll. Achten Sie darauf, dass Sie nach dem Reaktivieren immer einen Updatedurchlauf starten müssen, bevor Sie Updates wieder deaktivieren können. Unter der Option „Installationszeitpunkt für Updates auswählen“ legen Sie fest, wann Updates bezogen auf ihr Erscheinungsdatum installiert werden sollen. Funktionsupdates können bis zu 365 Tage verzögert werden (3), Qualitätsupdates bis zu 30 Tage (4).

Ab Windows 10 2004 hat Microsoft die Konfigurationsmöglichkeiten zur Updateverzögerung aus den Einstellungen entfernt – sie können über Gruppenrichtlinien aber weiterhin konfiguriert werden (s. u.). Der Grund ist ein seit 2019 geändertes Installationsverhalten für Feature-Updates. Windows installiert Feature-Updates seitdem standardmäßig nicht mehr mit dem Release, sondern erst ein paar Monate bevor das FR aus dem Support läuft, aktualisiert dann aber auf das jeweils aktuelle FR[2]. Wenn die Update-Verzögerung konfiguriert ist, installiert Windows allerdings automatisch jedes Feature-Release lediglich mit der angegebenen Verzögerung. Dafür können Sie mit dem 2004-FR über eine Gruppenrichtlinie oder einen Registry-Key Windows auf ein spezifisches FR „festnageln“ (s. u.).

Unter „Übermittlungsoptimierung“ (Bild 12.2) können Sie konfigurieren, ob Sie die neue Übermittlungsoptimierung nutzen wollen und von woher der Client die Updates beziehen darf.

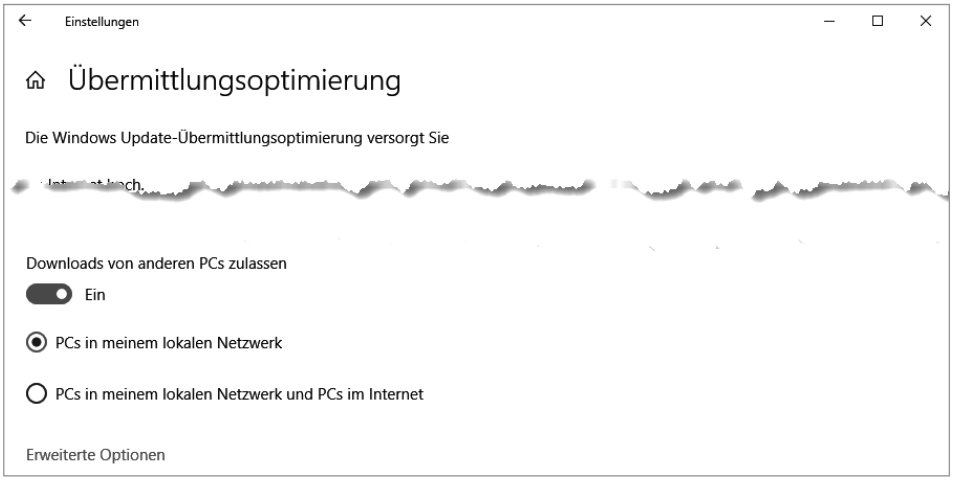


Bild 12.2 Zusätzlich zu BITS können Sie auch mit Delivery Optimization Updates beziehen.

Ab Windows 10 1709 können Sie in den erweiterten Optionen der Übermittlungsoptimierung auch steuern, wie viel von der Netzwerkbandbreite des Clients für den Up- und Down-

[2] Zumindest ist das die offizielle Aussage, auch wenn es offenbar Fälle gibt, in denen das nicht korrekt funktioniert. Siehe hierzu auch *https://www.askwoody.com/2020/patch-lady-anyone-else-getting-2004/* oder kurz *https://bit.ly/2JGddOQ*.

load von Updates verwendet werden darf. Hier können Sie auch sehen, wie viele Daten im laufenden Monat bereits wieder zu anderen Clients hochgeladen wurden.

Mit Windows 10 1607 hat Microsoft zusätzlich die Nutzungszeit eingeführt. Sie kann direkt im Hauptfenster der Windows Update-Einstellungen konfiguriert werden. Die Nutzungszeit kann ab 1703 bis zu 18 Stunden abdecken. Mit ihr wird bestimmt, in welchem Zeitraum weder Update-Benachrichtigungen noch automatische Neustarts ausgeführt werden dürfen. Das ist notwendig, um Geräte wie Tablets aktualisieren zu können, die normalerweise nie heruntergefahren, sondern nur in den Stromsparmodus versetzt werden. Seit FR 1903 kann Windows die Nutzungszeit auch automatisch bestimmen. Dieses Feature muss explizit aktiviert werden, da es sich letztlich um eine Nutzer-Überwachung handelt.

Alle diese Einstellungen können natürlich auch über eine Gruppenrichtlinie zentral gesteuert werden. Sie finden sich in den Einstellungen des Computers: **Administrative Vorlagen – Windows-Komponenten – Windows Update**:

Einstellung	Auswirkung
Automatischen Neustart nach Updates während der Nutzungszeit deaktivieren	Ist diese Einstellung aktiviert, kann Windows trotz aktivierter Nutzungszeit jederzeit neu starten.
Automatisches Herunterladen von Updates über getaktete Verbindungen zulassen	Erlaubt das Herunterladen von Updates über Mobilfunkverbindungen. Entspricht dem Button (1) in Bild 12.1
Benachrichtigungen für den automatischen Neustart zur Updateinstallation deaktivieren	Schaltet jegliche Update-Benachrichtigungen aus.
Energierichtlinie für den Neustart nach einem Update, die für Geräte in der Ladevorrichtung gilt	
Erforderliche Benachrichtigung für automatischen Neustart zur Updateinstallation konfigurieren	Sie können hier festlegen, ob für einen Neustart eine manuelle Bestätigung des Benutzers notwendig ist oder ob der Computer selbstständig neu starten kann.
Erinnerungsbenachrichtigungen über den automatischen Neustart zur Updateinstallation konfigurieren	Hier können Sie festlegen, wie lange vor einem geplanten Neustart eine Benachrichtigung an den Benutzer ausgegeben wird. Mit dieser Benachrichtigung kann der Benutzer den Neustart auch verschieben. Aktivieren Sie diese Richtlinie nicht, gilt der Standardwert von fünf Minuten.
Frist angeben, nach der ein automatischer Neustart zur Updateinstallation ausgeführt wird	Ist diese Option aktiviert, wird nach der angegebenen Zahl von Tagen (maximal 14) automatisch außerhalb der Nutzungszeit ein Neustart ausgeführt. Diese Option wird nicht wirksam, wenn die Richtlinie „Keinen automatischen Neustart für geplante Installationen automatischer Updates durchführen, wenn Benutzer angemeldet ist“ oder „Neustart immer automatisch zur geplanten Zeit durchführen“ aktiviert ist.
Keine Richtlinien für Updaterückstellungen zulassen, durch die Windows Update überprüft wird	Dieser etwas irreführende Name schaltet ab Windows 1703 (mit aktuellem CU) den Dual-Scan-Betrieb ab. Dual Scan (s. u.) heißt, dass Windows sowohl WSUS als auch Windows Update for Business zum Aktualisieren verwendet, was in den wenigsten Fällen erwünscht ist.

(Fortsetzung nächste Seite)

Einstellung	Auswirkung
Keine Treiber in Windows-Updates einschließen	Microsoft aktualisiert auch Treiber über Windows Update, was gerade bei neuen Geräten enorm praktisch ist. Aktivieren Sie diese Option, werden Treiber nicht mehr über Windows Update verteilt. Das hat auch Auswirkungen auf die Druckerinstallation, da seit dem Druckmodell 4.0 (mit Windows 8 eingeführt) der Client seine Druckertreiber für Druckerfreigaben nicht mehr vom Server bezieht (auch als Point and Print bezeichnet), sondern über Windows Update. Bis Windows 10 1607 und Windows Server 2016 muss das Übermitteln von Telemetriedaten erlaubt sein (s. u.), um Treiber herunterzuladen, ab Windows 10 1703 ist das nicht mehr notwendig.
Keine Verbindungen mit Windows Update-Internetadressen herstellen	Diese Funktion wird nur angewendet, wenn Windows Update konfiguriert und ein WSUS-Server angegeben ist. Sie verhindert, dass der Client sich neben dem lokalen Update-Server auch noch mit Servern im Internet verbindet. Im Gegensatz zu „Keine Richtlinie für Updaterückstellungen zulassen, durch die Windows Update überprüft wird“ verhindert diese Richtlinie nicht nur den Dual Scan, sondern unterbindet auch das Herunterladen aus dem Windows Store. Im Gegensatz zur Richtlinie „Microsoft Anwenderfeatures deaktivieren“ unter **Computerkonfiguration – Administrative Vorlagen – Windows-Komponenten – Cloudinhalt** werden beim ersten Anmelden die Download-Apps im Startmenü angezeigt, aber sie werden nicht heruntergeladen und ein manueller Download führt zu einer Fehlermeldung „Es ist keine Installation möglich, der Vorgang wird in Kürze wiederholt“. Effektiv wird der Windows Store also deaktiviert. Diese Einstellung funktioniert auch unter Windows 10 Professional! **Achtung:** Bei mir hat das Zurücksetzen dieser Einstellung auf „nicht konfiguriert“ weiterhin den Windows Store geblockt. Erst nachdem „deaktivieren“ konfiguriert war, konnte der Store wieder verwendet werden!
Keinen automatischen Neustart für geplante Installationen automatischer Updates durchführen, wenn Benutzer angemeldet ist	Für das Installieren des Updates muss der Benutzer den Computer manuell herunterfahren bzw. neu starten. Der Benutzer erhält hierüber eine Benachrichtigung. Diese Richtlinie ist nur gültig in Verbindung mit der Richtlinie „Automatische Updates konfigurieren“.
Neustart immer automatisch zur geplanten Zeit durchführen	Diese Richtlinie ist sehr missverständlich. Statt eine feste Zeit für das Aktualisieren des Computers angeben zu können, werden Updates im Hintergrund installiert und der Benutzer erhält eine Neustartbenachrichtigung. Mit dieser Option wird konfiguriert, wie lange der Benutzer Zeit hat, seine Daten zu speichern, bevor der Computer automatisch neu startet. Die mögliche „Gnadenfrist“ für den Benutzer kann zwischen 15 und 180 Minuten konfiguriert werden.

Einstellung	Auswirkung
Nutzungszeitbereich für automatische Neustarts angeben	Mit dieser Einstellung legen Sie fest, wie lang der Nutzungszeitbereich sein darf, wenn der Benutzer ihn individuell einstellt. Achten Sie darauf, dass Sie sich auch hier an die maximal unterstützten Zeitbereiche halten müssen und die Version 1607 nur zwölf Stunden unterstützt. Arbeiten Sie im Zweifelsfall mit WMI-Filtern und mehreren Richtlinien.
Stichtage für automatische Updates und Neustarts angeben	Hier können Sie einen Zeitrahmen festlegen, in dem die Installation und notwendige Neustarts vom Benutzer ausgeführt werden müssen, bevor sie vom System erzwungen werden. Für Qualitäts- und Funktionsupdates kann ein Zeitraum von 2 – 30 Tagen definiert werden, für den notwendigen Neustart eine Karenzzeit von 7 Tagen. Diese Einstellung soll ab FR 1709 anstatt der Einstellung *Beim Empfang von Qualitätsupdates auswählen* verwendet werden.
Warnbenachrichtigungszeitplan für den automatischen Neustart zur Updateinstallation konfigurieren	Wenn ein erzwungener Neustart aktiviert wurde, können Sie hier festlegen, ab wann der Benutzer über den Neustart informiert wird. Sie können die Frist für eine Informationsmeldung über den Neustart festlegen sowie die Frist für das Warnfenster, das den Benutzer direkt vor dem bestehenden Neustart warnt und zum Speichern seiner Daten anhält.
Wechsel zum erzwungenen Neustart und Benachrichtigungszeitplan für Updates festlegen	Mit dieser Einstellung können Sie festlegen, ab wann der Benutzer ein Update nicht mehr zurückstellen kann, sondern einen Neustart planen muss. Der Neustart muss nicht sofort ausgeführt werden, aber der Nutzer muss nach Ablauf der Benachrichtigungszeit einen Zeitpunkt für den Neustart definieren.
Zugriff auf alle Windows-Update-Funktionen entfernen	Blendet die Konfigurationsmöglichkeiten für das Windows Update auf dem Client aus. Diese Konfiguration ist empfehlenswert, da Windows per Dual Scan sowohl Windows Update als auch WSUS parallel verwenden kann (s. u.).
Zugriff auf Feature „Updates aussetzen“ entfernen	Verhindert, dass der Benutzer das Aktualisieren von Windows aussetzen kann. Das Feld **Anhalten bis** (s. Bild 12.1) wird deaktiviert.

Um den Installationszeitplan für Feature Releases und Quality-Updates festzulegen, öffnen Sie den Knoten **Computerkonfiguration – Administrative Vorlagen – Windows-Komponenten – Windows Update – Windows Update für Unternehmen** bzw. bis Windows 10 1703 **Windows Updates zurückstellen**. Hier finden Sie je nach Version aktuell bis zu fünf Einstellungen:

Einstellung	Auswirkung
Beim Empfang von Qualitätsupdates auswählen	Hier legen Sie fest, nach wie vielen Tagen ein neues Qualitätsupdate installiert werden soll. Ich empfehle, neue Qualitätsupdates immer mindestens eine Woche zu verschieben, da Microsoft schon mehrfach problematische Updates veröffentlicht hat. Sollte ein Update zu Problemen führen, kann man die Qualitätsupdates über „Qualitätsupdates aussetzen ab“ noch bis zu 35 Tage deaktivieren. Danach wird ein Zwangsupdate durchgeführt.
Deaktivieren von Sicherheitsvorkehrungen für Feature-Updates (ab FR 1903)	Microsoft pflegt eine Liste von Hard- und Softwarekonfigurationen, die bei einem Feature-Release zu Problemen führen können. Vor der Installation prüft das Setup, ob das Gerät kompatibel ist und führt die Installation nicht aus, wenn eine der aufgelisteten Konfigurationen erkannt wird. Wenn Sie diese Richtlinie aktivieren, setzen Sie die Prüfung aus. Diese Einstellung ist nur für das Testen von neuen Feature-Releases empfehlenswert, oder wenn Sie 100 % sicher sind, dass Ihre Systeme mit dem FR Problemfrei laufen.
Vorabversionen verwalten	Vorabversionen sind Beta-Versionen von Windows, die über den Eintrag **Update und Sicherheit – Windows-Insider-Programm** in den Windows-Einstellungen aktiviert werden können. Das Windows Insider-Programm ist nicht für Produktivsysteme gedacht. Um zu verhindern, dass Benutzer ihre Rechner eigenmächtig für das Windows Insider-Programm registrieren, wählen Sie in diesem Eintrag „Vorabversion deaktivieren“. Ist ein Rechner bereits im Insider-Programm, wählen Sie „Vorabversion deaktivieren, sobald die nächste Version veröffentlicht wurde“, damit der Rechner nach dem Update auf das Semi-Annual Update (Targetted) nicht wieder Teil des Insider-Programms wird.
Zeitpunkt für den Empfang von Vorabversionen und Funktionsupdates auswählen	Hier stellen Sie die Einstellungen aus Bild 1.1 (3) und (4) ein, also ab wann ein Feature-Update automatisch installiert werden soll. Mithilfe des Feldes „Vorabversionen oder Funktionsupdates aussetzen ab“ können Sie zentral alle Updates deaktivieren. Diese Funktionalität erlaubt es Ihnen, ein als problematisch erkanntes Update zu verschieben (s. Bild 1.1 (2), Updates aussetzen).
Zielversion des Funktionsupdates auswählen (ab FR 2004)	Hier können Sie Windows auf ein Feature-Release „festnageln“. Ist der von der Richtlinie betroffene Client noch nicht auf der angegebenen FR-Version, aktualisiert er sich. Danach bleibt er auf der Version, bis eine andere Version eingegeben ist. In das Zielversions-Feld geben Sie die FR-Bezeichnung ein, also z. B. 2004.

Weitere Informationen zu Windows Update for Business-Einstellungen finden Sie in den Microsoft-Dokumentationen unter *https://docs.microsoft.com/de-de/windows/deployment/update/waas-configure-wufb* oder kurz *https://bit.ly/2A9sjaP*.

12.1.3 Übermittlungsoptimierung/Delivery Optimization

Übermittlungsoptimierung oder Delivery Optimization (DO) ist ein neues Feature, das Microsoft mit Windows 10 eingeführt hat und das die Menge an Daten, die von Windows Update und dem Windows Store heruntergeladen werden, massiv reduziert. Das Verfahren basiert auf Peer-to-Peer-Technologie, Clients teilen bereits heruntergeladene Daten also mit anderen Clients (Peers) im gleichen Netzwerk (oder auch über das Internet). Dafür werden Dateien in Blöcke aufgeteilt, gehashed – es wird eine eindeutige ID erzeugt – und dann blockweise anstatt als monolithische Datei verteilt. Damit ein Client tatsächlich nur Originaldaten erhält, sind die Dateien digital signiert, der Client kann also nach Empfang der kompletten Datei prüfen, ob er ein unverändertes Update erhalten hat.

Wenn ein Client ein Update von einem Update-Server herunterladen möchte und die Übermittlungsoptimierung aktiviert ist, erhält er über die URL *.do.dsp.mp.microsoft.com eine Liste von Rechnern, die bereits Blöcke der Update-Datei bezogen haben. Auf Windows 10 Pro und Enterprise ist die Einstellung dabei standardmäßig so konfiguriert, dass ein PC Daten nur von Peers aus seinem eigenen lokalen Netzwerk empfängt (s. Bild 12.2). Der Update-Service ermittelt über die IP des sich verbindenden Rechners (normalerweise die öffentliche IP des Routers oder Proxys, über den der Client sich verbindet), mit welchen Peers er Daten austauschen darf. Man kann diese automatische Gruppierung aber auch überschreiben und manuell festlegen, welche Clients miteinander Daten austauschen dürfen, indem man eine Group-ID festlegt. Die Group-ID wird dann als einziges Kriterium verwendet, um zu ermitteln, welche Clients Daten austauschen dürfen. Alternativ kann man den AD-Standort oder die Domäne verwenden oder über DHCP oder DNS eine Gruppenzuordnung festlegen. Das ist wichtig, wenn man bereits mit IPv6 arbeitet (alle Clients haben eine öffentliche IP-Adresse) oder der Zugriff nach außen über Proxy-Arrays oder Load-Balancing stattfindet, sodass ein Standort nicht über eine eindeutige ID verfügt. Die Group-ID ist eine GUID (Globally Unique Identifier), die man z. B. mit dem PowerShell-Cmdlet `New-GUID` zufällig generieren kann.

Die Übermittlungsoptimierung arbeitet höchst effizient und teilt Daten deutlich schneller als die Alternative BranchCache. Sind die Daten erst einmal im lokalen Netzwerk, dauert es nur Sekunden, bis Clients lokale Peers als Quelle verwenden können. Die Daten werden dann mit voller lokaler Netzwerkgeschwindigkeit geteilt. Der Übermittlungsoptimierungsdienst verwendet hierfür Port 7680 im lokalen Netzwerk, für den Datentausch mit Internet-Peers Port 3544 (Teredo-Protokoll, eine IPv6-Übergangstechnologie).

Übermittlungsoptimierung ist vor allem für große Dateien effektiv und kostet Client-Ressourcen, weshalb sie standardmäßig erst aktiviert wird, wenn der Client mindestens über 4 GB RAM und 32 GB freien Speicherplatz auf dem Cache-Laufwerk verfügt. Diese Konfigurationen können über Gruppenrichtlinien angepasst werden, die Sie in der Computerkonfiguration unter **Administrative Vorlagen – Windows-Komponenten – Übermittlungsoptimierung** finden.

Die Übermittlungsoptimierung funktioniert übrigens genauso mit WSUS und dem Windows Store. Downloads aus dem Windows Store sind normalerweise benutzerinitiiert und werden als Vordergrundprozesse bezeichnet. Für Office 365 Apps müssen eine Reihe von Voraussetzungen erfüllt sein, die Microsoft unter *https://docs.microsoft.com/en-us/deployoffice/delivery-optimization* oder kurz *https://bit.ly/3ogx1HH* zusammengefasst hat.

Einstellung	Auswirkung	FR
Absolute max. Cachegröße (in GB)	Hier können Sie einen absoluten Wert für den Cache eingeben. Wird diese Option aktiviert, wird die maximale Cachegröße in Prozent ignoriert.	Ab 1607
Cachelaufwerk ändern	Hier können Sie den Ablageort für den Cache anpassen. Ab Version 1709 ist der Standardpfad C:\Windows\DeliveryOptimization.	Ab 1607
Cache Server Hostname	Seit System Center Configuration Manager 1906 (SCCM) stellt Microsoft den Connected Cache zur Verfügung, der Updates für Clients von den Microsoft Update Servern herunterladen und dann zwischenspeichern kann. Wenn Sie einen Connected Cache Server installiert haben, können Sie ihn über diese Einstellung oder DHCP (s. Richtlinie *Quelle des Cacheserver-Hostnamens*) den Clients bekannt machen. Mehr zum Microsoft Connected Cache erfahren Sie unter *https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/hierarchy/microsoft-connected-cache* oder kurz *https://bit.ly/3fY2ziM.*	Ab 2004
DownloadModus	Mit dem Downloadmodus legen Sie fest, mit welchen Methoden der Windows Update Client einen Download durchführen darf. **0: Nur HTTP:** Hiermit wird der Peer-to-Peer-Datenaustausch deaktiviert, die Übermittlungsoptimierung kann aber trotzdem Daten vom Update-Server abrufen und per HTTP Daten von Peers beziehen. Welche Daten hier bezogen werden, ist leider an keiner mir bekannten Stelle dokumentiert. HTTP bedeutet, dass der Client den BITS-Dienst für den Download verwendet (das ist das Standardverhalten voriger Windows-Versionen). **1: LAN:** Der Client benutzt HTTP (BITS) und Peer-to-Peer mit Clients im gleichen Netzwerk. **2: Gruppe:** Der Client benutzt HTTP (BITS) und Peer-to-Peer mit Clients der gleichen Gruppe. **3: Internet:** Der Client benutzt HTTP (BITS) und Peer-to-Peer mit beliebigen Clients. **99: Einfach:** Mit dieser Einstellung wird die Übermittlungsoptimierung komplett deaktiviert, der Client holt Updates nur per HTTP (BITS). **100: Überbrückung:** Verwendet BITS in Verbindung mit BranchCache. Übermittlungsoptimierung ist auch hier deaktiviert. Mehr zu den Übermittlungsmodi finden Sie unter *https://2pintsoftware.com/delivery-optimization-dl-mode/* und *https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization* oder kurz *https://bit.ly/2mD0Iot.*	Ab 1511
Geschäftszeiten festlegen, um die Bandbreite von Hintergrunddownloads zu begrenzen	Mit dieser Option können Sie unterschiedliche Bandbreiten für Tages- und Nachtzeiten festlegen. Dadurch wird es möglich, die Updates tagsüber zu begrenzen, aber nachts die volle (oder eine höhere) Bandbreite zur aktivieren. Hintergrunddownloads sind Prozesse, die vom System ausgeführt werden.	Ab 1803

Einstellung	Auswirkung	FR
Geschäftszeiten festlegen, um die Bandbreite von Vordergrunddownloads zu begrenzen	Wie „Geschäftszeiten festlegen, um die Bandbreite von Hintergrunddownloads zu begrenzen“, aber es werden Benutzerprozesse optimiert, also Downloads aus dem Microsoft Store.	Ab 1803
Gruppen-ID	Hier können Sie selbst bestimmen, welche Clients als Peers fungieren können, indem alle Peers die gleiche Gruppen-ID bekommen. Die Gruppen-ID ist ein GUID-Wert, den Sie mit dem PowerShell-Cmdlet `New-GUID` selbstständig erstellen können. Alternativ können Sie die Gruppen-ID auch über einen Netzwerkdienst vergeben. Dann konfigurieren Sie stattdessen die Richtlinie „Quelle von Gruppen-IDs auswählen“.	Ab 1511
Hintergrunddownloads von HTTP verzögern (sek)	Wenn Peer-to-Peer-Download aktiviert ist, können Sie mit dieser Option den Download per HTTP für mehrere Sekunden verzögern. Normalerweise versucht der Client, HTTP und Peer-to-Peer parallel zu nutzen, durch diese Option wird Peer-to-Peer bevorzugt.	Ab 1803
Max. Cachealter (in Sekunden)	Hier können Sie angeben, wie lange Updates lokal für andere Peers vorgehalten werden. Der Standard ist drei Tage. 0 bedeutet, dass Dateien nur bei Bedarf gelöscht werden.	Ab 1511
Max. Cachegröße (in Prozent)	Gibt an, wie viel Speicherplatz in Prozent vom Datenträger für den Cache verwendet werden darf. Der Windows-Standardwert ist 20%.	Ab 1511
Maximale Bandbreite für Downloads im Hintergrund (in KB/s)	Die Bandbreite, die für alle Downloads der Übermittlungsoptimierung in Summe von der verfügbaren Bandbreite verwendet werden darf in KB. Der Standardwert von Null lässt Delivery-Optimization die Bandbreite dynamisch bestimmen.	2004
Maximale Bandbreite für Downloads im Hintergrund (Prozent)	Die Bandbreite, die für alle Downloads der Übermittlungsoptimierung in Summe von der verfügbaren Bandbreite verwendet werden darf. Ersetzt „Maximale Downloadbandbreite“ (in Prozent). Hintergrund bezieht sich auf automatische Prozesse wie das Windows Update.	Ab 1803
Maximale Bandbreite für Downloads im Vordergrund (Prozent)	Wie „Maximale Bandbreite für Download im Hintergrund (Prozent)“, begrenzt aber auch User-Prozesse, aktuell also den Windows Store.	Ab 1803
Maximale Downloadbandbreite im Vordergrund (in KB/s)	Wie „Maximale Bandbreite für Download im Hintergrund (in KB/S)“, begrenzt aber auch User-Prozesse, aktuell also den Windows Store.	Ab 2004
Maximale Downloadbandbreite (in KB/s)	Wie viel KB/s (absolut) der verfügbaren Netzwerkbandbreite der lokalen Netzwerkkarte von der Übermittlungsoptimierung für den Download verwendet werden darf. Diese Einstellung kann ab der Version 1709 auch lokal in den erweiterten Einstellungen der Übermittlungsoptimierung gesetzt werden.	von 1607 bis 2004
Maximale Downloadbandbreite (in Prozent)	Ab 1803 ersetzt durch „Maximale Bandbreite für Downloads im Hintergrund“	von 1607 bis 2004

(Fortsetzung nächste Seite)

Einstellung	Auswirkung	FR
Methode zum Einschränken der Peerauswahl	Ab dem Feature Release 1803 kann man jetzt die Einstellungen des Download-Modes weiter einschränken, indem man hier vorgibt, dass Clients Daten nur aus dem eigenen Subnetz beziehen können.	Ab 1803
Maximale Uploadbandbreite (in KB/s)	Gibt die Bandbreite an, die verwendet werden kann, um anderen Clients Daten zur Verfügung zu stellen. Da ein Upload immer ein Hintergrundprozess ist, gibt es hier anders als bei der Downloadbandbreite keine Unterscheidung zwischen Hintergrund- und Vordergrundverarbeitung.	Ab 1607
Maximale Uploadbandbreite (in KB/s) – ab 1703	Wie viel KB/s (absolut) der verfügbaren Netzwerkbandbreite der lokalen Netzwerkkarte von der Übermittlungsoptimierung für den Upload verwendet werden darf. Diese Einstellung kann ab der Version 1709 auch lokal in den erweiterten Einstellungen der Übermittlungsoptimierung gesetzt werden.	Ab 1703
Minimale Datenträgergröße, die zur Verwendung des Peercaching zulässig ist (in GB)	Legt fest, wie viel freier Speicherplatz auf dem Datenträger verfügbar sein muss, damit der Host Updates zum Upload zur Verfügung stellt. Empfohlene Werte sind 64 – 256 GB, standardmäßig sind 32 GB eingestellt. Die Einstellung bezieht sich auf das Cachelaufwerk, dass über *Cachelaufwerk ändern* angepasst werden kann.	Ab 1703
Minimale Größe der Inhaltsdatei für das Peercaching (in MB)	Gibt an, wie groß eine Datei mindestens sein muss, damit die Übermittlungsoptimierung verwendet wird. Der auf dem Client gesetzte Standardwert ist 100 MB.	Ab 1703
Minimale RAM-Kapazität (einschließlich), die zur Verwendung des Peercaching erforderlich ist	Hier kann angegeben werden, wie viel GB RAM dem Client zur Verfügung stehen müssen, damit er die Übermittlungsoptimierung nutzt. Der Standardwert sind 4 GB, Sie können den Wert hier aber zwischen 1 GB und 4 GB anpassen.	Ab 1703
Minimaler Hintergrund-QoS-Wert (in KB/s)	Der QoS-Wert (Quality of Service) legt fest, wie viel Bandbreite für den Download von Windows Update reserviert werden. Wenn Windows die minimale Bandbreite durch lokale Peers nicht abdecken kann, wird versucht, die restliche Bandbreite über Update-Server zu bedienen. Je höher dieser Wert, desto mehr Daten werden also direkt von den Updateservern bezogen.	Ab 1607
Monatliche Obergrenze für Uploaddaten (in GB)	Dieser Wert kann auch auf dem Client in den erweiterten Einstellungen der Übermittlungsoptimierung konfiguriert werden und limitiert die Datenmenge, die pro Monat anderen Clients bereitgestellt werden kann. Sinnvoll ist diese Option nur, wenn man Daten auch mit Clients im Internet teilt.	Ab 1607
Peercaching aktivieren, während das Gerät über ein VPN verbunden ist	Deaktiviert die Übermittlungsoptimierung, wenn der Client per VPN verbunden ist.	Ab 1709

Einstellung	Auswirkung	FR
Quelle des Cacheserver-Hostnamens	Ein Cacheserver kann entweder manuell angegeben (Option Cacheserver-Hostname) oder per DHCP bestimmt werden. Wenn Sie diese Option aktivieren, holt sich der Client den Cacheserver einmalig aus der DHCP-Option 235. Stellen Sie *Erzwingen der DHCP-Option 235* ein, überschreibt der Client den Cache-Server mit jeder DHCP-Abfrage erneut durch den angegebenen Server.	Ab 2004
Quelle von Gruppen-IDs auswählen	Wenn Sie als Download-Modus Gruppe (2) gewählt haben, können Sie die Gruppen-ID auch über einen Netzwerkdienst verteilen. Die ID kann entweder über den AD-Standort (AD-Site), die Windows-Domäne (authentifizierte Domänen-SID) oder das DNS-Suffix gebunden werden. Alternativ können Sie eine Gruppen-ID über DHCP (DHCP-Options-ID) verteilen. Hierzu müssen Sie die Gruppen-ID über Option 234 verteilen. Eine Anleitung zur Konfiguration Ihres DHCP-Servers finden Sie unter *https://oliverkieselbach.com/2018/01/27/configure-delivery-optimization-with-intune-for-windows-update-for-business/* oder kurz *https://bit.ly/2OGbaIJ*.	Ab 1803
Uploads zulassen, während das Gerät im Akkubetrieb läuft und der minimale Akkustand (in Prozent) nicht erreicht ist.	Legen Sie einen Akkustand fest, ab dem kein Upload mehr stattfinden soll. Microsoft empfiehlt als Minimalwert 40%. Ist diese Richtlinie nicht gesetzt, ist der Upload auf mobilen Geräten deaktiviert, es findet also standardmäßig im Akkubetrieb gar kein Upload statt.	Ab 1709
Verzögerter Cacheserver-Fallback für Hintergrund-Download (in Sekunden)	Wenn ein Client den konfigurierten Cache-Server nicht erreichen kann, versucht er nach dem hier angegebenen Zeitraum stattdessen, die Updates per http (BIT-Dienst) zu beziehen. Diese Einstellung gilt für Hintergrunddienste wie Windows Update, deren Downloads vom Betriebssystem gesteuert werden.	1903
Verzögerter Cacheserver-Fallback für Vordergrund-Download (in Sekunden)	Wie *Verzögerter Cacheserver-Fallback für Hintergrund-Download*, bezieht sich aber auf vom Benutzer initiierte Downloads wie Apps aus dem Windows Store.	1903
Vordergrunddownloads von HTTP verzögern (sek)	Wenn Peer-to-Peer-Download aktiviert ist, können Sie mit dieser Option den Download per HTTP für mehrere Sekunden verzögern. Normalerweise versucht der Client, HTTP und Peer-to-Peer parallel zu nutzen, durch diese Option wird Peer-to-Peer bevorzugt. Beachten Sie, dass für den Endbenutzer während der reinen Peer-to-Peer-Verbindung kein Downloadfortschritt sichtbar ist.	Ab 1803

Alle Übermittlungsoptimierungseinstellungen finden Sie unter *https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization-reference* oder kurz *https://bit.ly/33EjTEt*.

Viele weitere Informationen zur Übermittlungsoptimierung finden Sie im Video „Delivery Optimization – a deep dive“ von der Ignite 2017 unter *https://channel9.msdn.com/Events/Ignite/Microsoft-Ignite-Orlando-2017/BRK2048* oder kurz *https://bit.ly/2uFsYv6*.

12.1.4 Bereitstellungsringe verwenden

Da Windows als Feature Release regelmäßig neu bereitgestellt werden muss – ca. einmal pro Jahr, wenn Sie jeweils ein Feature Release auslassen wollen – brauchen Sie einen Plan, wie Sie die Kompatibilität der Feature-Updates mit Ihren bestehenden Anwendungen testen. Im Gegensatz zur Migration von Windows XP auf Windows 7 steht Ihnen für die Migration auf ein neues Feature Release ja nur ein relativ kurzer Zeitraum zur Verfügung. Hier stelle ich Ihnen vor, wie Microsofts Vorschlag aussieht.

12.1.4.1 Das Konzept der Bereitstellungsringe

Für das Testen und Bereitstellen von Windows 10 sieht Microsoft sogenannte Bereitstellungsringe vor. Ein Bereitstellungsring definiert zwei Dinge: die Zielgruppe (Computer bzw. Benutzer), die das Update erhalten, und den Zeitrahmen, in dem das Update ausgerollt werden soll. In Microsofts Standardmodell gibt es vier von diesen Bereitstellungsringen.

Im innersten oder ersten Ring befindet sich eine Reihe von Testrechnern, die an der Windows Insider Preview teilnehmen, also Beta-Updates bekommen. Diese Maschinen sollten in etwa Ihrem Standardclient entsprechen und werden dafür verwendet, schon einmal erste Kompatibilitätstests durchzuführen, bevor Microsofts neues Feature Release veröffentlicht wird.

Der zweite Ring besteht aus einer Reihe von ausgewählten Computern bzw. Benutzern in den unterschiedlichen Abteilungen, die mit der Veröffentlichung des neuen Feature Release sehr zeitnah ein Update bekommen. Die Benutzer des zweiten Rings sollten „Technikaffin“ sein, was bedeutet, dass sie nicht gleich beim Helpdesk anrufen, wenn ein Knopf im neuen Build ein bisschen weiter nach rechts gerückt ist. Diese Benutzer sind dafür zuständig, die Fachanwendungen ausführlich zu testen und bei Problemen Rückmeldung an das Bereitstellungsteam zu machen. Das Bereitstellungsteam sollte grundsätzlich regen Kontakt zu diesen Benutzern halten und sie auch ständig über neue Release-Pläne auf dem Laufenden halten.

Nach einer ausführlichen Testphase bekommt der dritte Ring, das Gros der Clients, das Feature-Update. Der dritte Ring wird nach ca. 3 – 4 Monaten aktualisiert. Für diese Clients werden auch die Qualitätsupdates um eine Woche verschoben, um sicherzustellen, dass ein fehlerhaftes Update nicht gleich alle Unternehmensrechner in den Abgrund reißt.

Der vierte Ring ist der Ring, auf dem unternehmenskritische Anwendungen laufen. Das können z. B. alte Anwendungen sein, die eigentlich nicht mehr mit Windows 10 kompatibel sind und nur noch mit Tricks zum Laufen gebracht werden können, für die es aber keine Alternative gibt, oder Systeme, die nicht ausfallen dürfen. Dieser Ring bekommt seine Updates noch einmal später, und Qualitätsupdates werden noch weiter hinausgezögert.

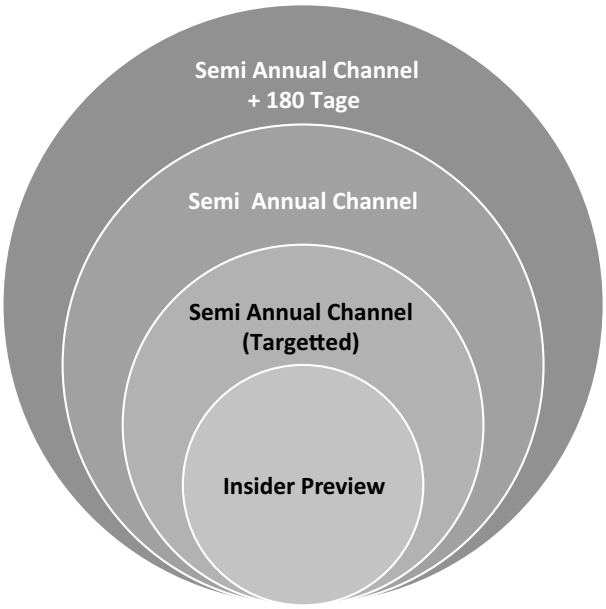


Bild 12.3 Windows-Bereitstellung in Wellen oder Ringen

Das Konzept finden Sie in Microsofts eigenen Worten unter *https://docs.microsoft.com/de-de/windows/deployment/update/waas-deployment-rings-windows-10-updates* oder kurz *https://bit.ly/2LHtpeW*.

Wenn Sie die Bereitstellung über Update-Ringe planen, ist meine persönliche Empfehlung, noch zwei weitere Ringe mit einzuschließen. Bevor Sie die Updates in dem eben beschriebenen zweiten Ring, also für technikaffine Benutzer freigeben, sollten Sie das neue Feature Release erst einmal ausführlich auf den Arbeitsplatzrechnern der Administration und des User Helpdesk nutzen – der muss die Probleme ja hinterher eh ausbaden und sollte sich insofern sowieso am besten mit den neuen Clients auskennen. Lassen Sie sich auf jeden Fall zwei bis drei Monate (ersetzen Sie Monate mit „kumulative Updates“) Zeit, bevor Sie ein Feature Release auf Produktivsysteme loslassen. Die Qualität der Feature-Releases ist seit FR 1909 zwar besser geworden, aber niemand garantiert, dass das auch in Zukunft so bleibt oder dass Sie von den Fehlern verschont bleiben, die trotzdem übersehen worden sind. Das Gleiche gilt für kumulative Updates – ich kann Ihnen aufgrund der Erfahrungen mit der Qualität von Updates nicht empfehlen, ein CU sofort nach Erscheinen auszurollen. Verzögern Sie die Updates um eine Woche und lesen Sie in dieser Zeit die einschlägigen Newsseiten wie Heise.de, Golem.de oder Borncity.com von Günther Born. Wenn es zu größeren Problemen kommt, werden Sie das hier vermutlich frühzeitig erfahren und können im Zweifel die Updates einfach aussetzen.

Für sehr kritische Systeme bietet es sich eventuell an, die LTSC-Version von Windows in Betracht zu ziehen. Microsoft sieht die LTSC-Version zwar nicht gerne auf Anwenderrechnern, sondern empfiehlt sie nur für Bank- oder Kassensysteme, aber letztlich ist auch die LTSC-Version nur ein Windows 10 ohne Cortana, Apps und Edge.

12.1.4.2 Windows per Gruppenrichtlinie auf ein FR festlegen

Seit FR 2004 kann man Windows per Gruppenrichtlinie auf ein Feature-Release festlegen. Windows versucht dann nur noch sich zu aktualisieren, wenn Sie die Gruppenrichtlinie auf ein neues FR anpassen. Über diese Option ist es auch möglich, komplette Feature-Releases einfach zu überspringen. Außerdem gewinnen Sie wieder mehr Kontrolle darüber, wann ein FR ausgerollt wird. Trotzdem müssen Sie FRs natürlich über Updateringe testen.

Zum Festlegen einer Zielversion wechseln Sie in den Computerrichtlinien zu **Administrative Vorlagen – Windows-Komponenten – Windows Update – Windows Update für Unternehmen**. Hier finden Sie eine Richtlinie **Zielversion des Funktionsupdates auswählen**. Tragen Sie hier den Namen der Version ein (z. B. 2004), installiert Windows das entsprechende Feature-Update und aktualisiert es nur, wenn Sie die Zielversion ändern. Ein Downgrade auf ein älteres FR ist explizit nicht möglich – ein aktualisierter Client kann nur auf eine höhere Version angehoben werden. Wählen Sie am besten immer das Release der zweiten Jahreshälfte aus, da es gut getestet und stabil sein sollte, und außerdem in der Enterprise-Version 30 statt 18 Monate Support hat. Dieser Stand bezieht sich auf November 2020 – Gerüchteweise soll 21H1 auch nur ein kleines Update sein, was dann eventuell auch Auswirkungen auf den Supportzeitraum hat.

12.1.4.3 Bereitstellungsringe implementieren (WSUS)

Wenn Sie Updates mit dem WSUS verteilen, legen Sie für jeden Bereitstellungsring, den Sie benötigen, eine Computergruppe auf dem WSUS an. Sie können die Gruppen von Hand zuweisen, oder Sie erstellen für jede Computergruppe auch ein GPO und weisen die Computer dann über das GPO zu. Neue Feature Releases geben Sie dann von Hand für die jeweilige Computergruppe frei.

12.1.4.4 Bereitstellungsringe implementieren – Update for Business

Wenn Sie mit Windows Update for Business arbeiten, erstellen Sie für jeden Ring ein eigenes GPO. Wenn Sie die Computer der einzelnen Update-Ringe in eigene OUs verschieben können, verknüpfen Sie die GPOs mit den zugehörigen OUs. Ansonsten wäre eine Variante, die GPOs relativ weit oben in ihrer AD-Struktur aufzuhängen und für jeden Ring auch eine globale Gruppe anzulegen. Richten Sie nun Sicherheitsfilter ein, die das GPO nur auf den Computern anwenden, die sich in der zugehörigen Sicherheitsgruppe befinden. Sie können die Computer dann Ringen zuweisen, indem Sie sie einfach in die entsprechende Sicherheitsgruppe aufnehmen. Achten Sie aber darauf, den frühesten Ring mit der niedrigsten Priorität zu verknüpfen und den spätesten Ring mit der höchsten, damit Ihnen bei einer falsch zugewiesenen Maschine nicht plötzlich die Updates um die Ohren fliegen.

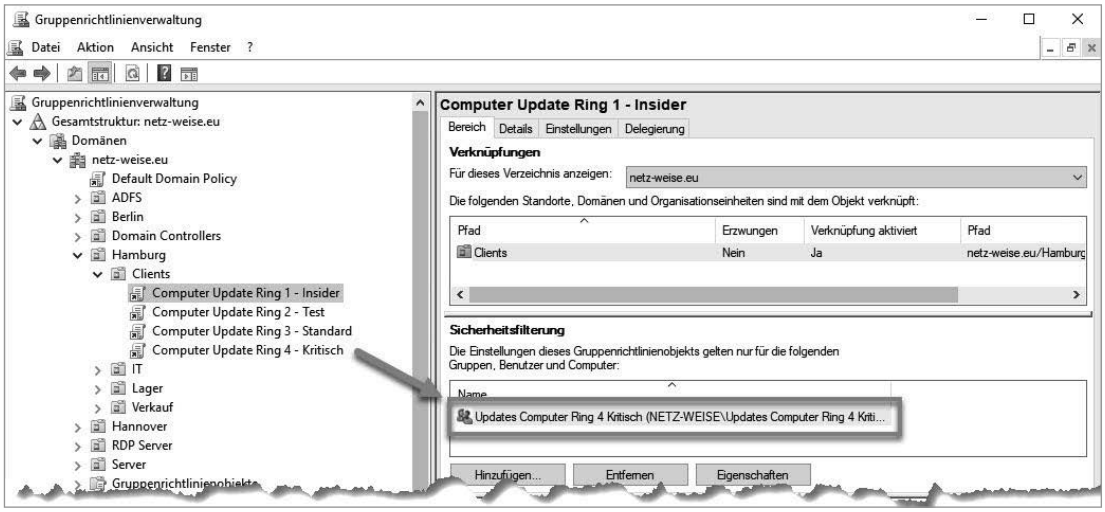


Bild 12.4 Für jeden Ring gibt es ein GPO und eine Gruppe, auf die gefiltert wird.

Bild 12.5 Achten Sie darauf, die kritischste Gruppe in der Verknüpfungsreihenfolge ganz nach oben zu schieben.

Nun können Sie die Windows Update for Business-Einstellungen in den einzelnen GPOs vornehmen.

12.2 Windows 10 und die Privatsphäre

Windows 10 hat neben den vielen Neuerungen auch einige, die man eigentlich gar nicht haben möchte, z. B. die automatische Übertragung verschiedener Daten ins Internet. Diese Daten werden oft auch als Privatsphäre-Einstellungen bezeichnet. Dabei unterscheidet Microsoft zwei verschiedene Typen von Daten, nämlich Telemetriedaten und Funktionsdaten. Telemetriedaten sind Daten, die von Microsoft über die Funktionsweise von Windows gesammelt werden, wie installierte Programme, installierte Updates, installierte Hardware usw., aber auch und vor allem Daten über die Zuverlässigkeit von Windows wie Programmabstürze. Funktionsdaten sind Daten, die vornehmlich von Apps an den App-Hersteller übertragen werden, weil die Funktion der App eigentlich von einem Dienst irgendwo im

Internet zur Verfügung gestellt wird und die App nur als Front-End fungiert. Was nach der Verwendung der Daten danach beim Hersteller passiert, ist für den Kunden normalerweise nur schwer nachvollziehbar, gelöscht werden die Daten nur in den seltensten Fällen.

12.2.1 Windows-Telemetrie

Telemetriedaten sind für Microsoft extrem wichtig, seit Windows in Form von Feature Releases ausgerollt wird. Während früher jeder neuen Windows-Version eine ziemlich lange Beta-Phase vorausging, stehen Microsoft jetzt vom Beginn eines neuen Entwicklungszyklus bis zum Release nur sechs Monate zur Verfügung. Im Vorfeld finden die Tests durch freiwillige Beta-Tester statt, die Updates durch die Insider Preview beziehen. Wenn ein neues Feature Release erscheint, sind die neuen Funktionen damit nicht wirklich ausreichend getestet. Das betrifft nicht nur Fehler, sondern auch die Anwenderfreundlichkeit. Um schnell an Nutzungsdaten zu kommen, wird die Windows Home Edition quasi zwangsaktualisiert, und die Verwendungs- und Fehlerinformationen werden dann automatisch im Hintergrund an Microsoft übermittelt. Die Telemetriedaten sollten nicht anwenderspezifisch ausgewertet werden, da es Microsoft letztlich nicht darum geht, Daten über einen einzelnen Benutzer zu sammeln, sondern Windows möglichst schnell (innerhalb von vier Monaten, bis das aktuelle Feature Release zum Semi-Annual Update gereift ist) in ein für Unternehmenskunden ausreichend stabiles Release zu bringen. Ich habe hier absichtlich „sollten“ geschrieben, denn die Telemetriedaten werden verschlüsselt im Hintergrund übertragen. Seit der Version 1803 bietet Microsoft die Möglichkeit, mithilfe einer App aus dem Windows Store die gesammelten Telemetriedaten anzuzeigen, den Diagnostic Data Viewer (s. u.).

Wie viele Telemetriedaten Microsoft sammeln darf, kann man anpassen, wobei es Unterschiede in den einzelnen Windows-Versionen gibt. Die Einstellungen sind lokal auf dem Client in den Einstellungen unter **Datenschutz – Diagnose und Feedback** konfigurierbar – s. Bild 12.6. Hier können Sie zwischen „Erforderlichen Diagnosedaten“ und „Optionalen Diagnosedaten“ (Stand 20H2 – manchmal ändern sich die Bezeichnungen) auswählen – ein vollständiges Deaktivieren der Datensammlung ist nicht vorgesehen! Über Gruppenrichtlinien haben Sie in der Enterprise Edition die Möglichkeit, die Sammlung noch weiter einzuschränken, aber komplett verhindern können Sie die Übermittlung nur, wenn Sie die Telemetrie-Server durch Ihre Firewall blocken lassen. Einen interessanten Artikel, wie Sie das mit der Windows Firewall erreichen können, finden Sie bei WinAero unter *https://winaero.com/blog/stop-windows-10-spying-on-you-using-just-windows-firewall/* oder kurz *https://bit.ly/2OrO2NZ*. Microsoft hat ebenfalls eine vollständige Liste aller URLs unter *https://docs.microsoft.com/en-us/windows/privacy/manage-windows-2004-endpoints* oder kurz *https://bit.ly/39CnQgL* veröffentlicht. Da sich die Endpoints ab und zu vermehren, sollten Sie auf der Seite vor dem Ausrollen von neuen FRs vorbeischauen. In der dazugehörigen Kategorie *Manage Windows 10 connection Endpoints*, die man leider nicht direkt verlinken kann, pflegt Microsoft für jedes FR eine Liste mit Endpoints, für deren Vollständigkeit ich nicht garantiere. Wenn Sie auf Nummer sicher gehen wollen, prüfen Sie zusätzlich auf Ihrer Firewall oder mit dem Web-Debug-Proxy Fiddler, den Sie kostenlos unter *https://www.telerik.com/fiddler* herunterladen können, ob Ihre Clients noch weitere Microsoft-Server ansprechen.

Telemetriedaten unter Datenschutzgesichtspunkten

Angela Merkel hat Daten als „Rohstoff des 21. Jahrhunderts“ bezeichnet. Microsoft sieht das ähnlich und sammelt daher ungefragt jede Menge Nutzungsdaten unter Windows 10 und Office, Diese Daten werden als Telemetriedaten bezeichnet und von Microsoft ausgewertet, um sowohl die Stabilität der Windows-Dienste als auch deren Akzeptanz beim Nutzer zu ermitteln. Das ist kein Microsoft-spezifisches Problem – seit Software „agil“ entwickelt wird (mehr zu dem Thema finden Sie unter *https://de.wikipedia.org/wiki/Agile_Softwareentwicklung*), sammelt eigentlich jede Anwendung Nutzungsdaten. Das gewinnt unter Windows 10 besondere Brisanz, da zum einen nicht bekannt ist, was Microsoft genau mit den Daten macht, und die Daten zum anderen auf amerikanischen Servern gespeichert werden. Spätestens seit Kippen des Privacy Shield am 16. Juli 2020 ist das Speichern von Daten europäischer Benutzer auf den Servern amerikanischer Unternehmen damit eigentlich nicht mehr erlaubt. Obwohl das Urteil nicht unerwartet kam, war niemand wirklich darauf vorbereitet, und bis heute (November 2020) gibt es keine eindeutige rechtliche Position zu der Problematik, da einfach zu viele Daten europäischer Nutzer auf amerikanischen Severn gespeichert sind. Dazu kommt, dass man nicht jede problematische Anwendung durch eine datenschutzkonforme ersetzen kann – beim Betriebssystem wird das mindestens sehr schwierig und kostenintensiv, in den meisten Fällen aufgrund der betriebskritischen Anwendungen, die nur unter Windows laufen, praktisch unmöglich.

Grundsätzlich enthalten Telemetriedaten keine Benutzerdaten, sondern Verhaltensdaten über die Nutzung von Funktionen, die verwendete Hardware und Applikationsverhalten. Diese Daten werden (laut Microsoft) nicht individuell ausgewertet, sondern mit anderen Daten zusammengeführt und sollen größtenteils nach 30 Tagen gelöscht werden. Zusätzlich werden Programme, die ein auffälliges Verhalten an den Tag legen, von Windows Defender an Microsoft übertragen, um so Malware frühzeitig erkennen und die Defender-Antivirensignaturen entsprechend anpassen zu können.

Die Telemetriedaten können außerdem dazu verwendet werden, Features wie Windows Update for Business zu überwachen. Microsoft stellt hierfür mit den Azure-Cloud-Diensten eine Funktion namens Desktop Analytics (ehemals Windows Analytics) zur Verfügung, die die Funktion eines WSUS-Reporting-Servers übernehmen kann und anzeigt, welche Clients auf welchen Update-Ständen sind oder schon lange keine Updates mehr bezogen haben. Dafür muss auf den Clients eine Customer-ID hinterlegt werden, über die Microsoft die Clients dann einem spezifischen Kunden zuweisen kann. Hierfür muss die Telemetrie aber aktiviert sein, da Daten über den Update-Stand sonst nicht übertragen werden können. Außerdem müssen die Telemetriedaten auf Clients, die an der Insider-Preview teilnehmen, auf „Vollständig“ bzw. „Optionale Diagnosedaten“ (gleiche Funktionalität, neuer Name) eingestellt sein.

Microsoft hat auf Druck diverser deutscher und anderer europäischer Behörden datenschutztechnisch inzwischen stark nachgeregelt. In der Enterprise-Edition (und nur hier!) können Sie die Übermittlung von Telemetrie-Daten in den Feature-Releases ab der 1903 praktisch vollständig unterbinden, und das sollten Sie auch tun, wenn Sie nicht auf Clouddienste wie Desktop Analytics angewiesen sind.

Mehr zum Privacy-Shield finden Sie unter *https://www.heise.de/ratgeber/FAQ-Das-Ende-des-Privacy-Shields-4906737.html* oder kurz *https://bit.ly/2JlOtvP*

Für die manuelle Konfiguration der Telemetrie-Einstellungen stehen zwei Optionen zur Wahl – *Erforderliche Diagnosedaten* oder *Optionale Diagnosedaten*. Unter Windows 10 Professional ist standardmäßig *Optionale Diagnosedaten* aktiviert, unter Windows 10 Enterprise *Erforderliche.* Wenn der Client Updates über die Insider Preview erhält, ist *Optionale Diagnosedaten* Pflicht und kann nicht umgestellt werden.

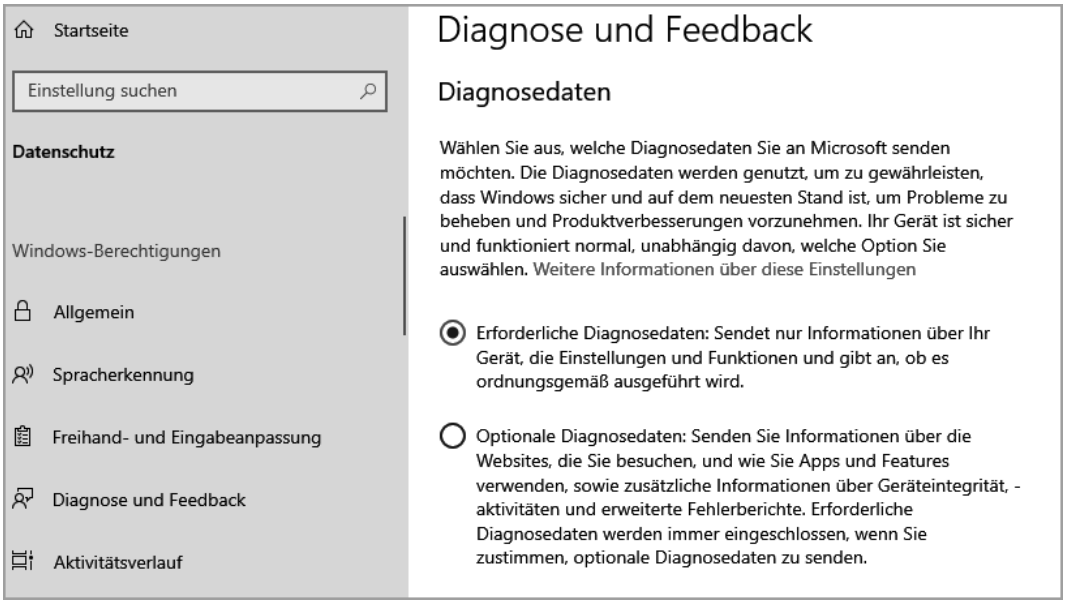


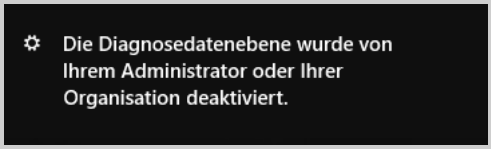
Bild 12.6 Sie können Diagnosedaten nur auf „Erforderlich“ stellen, sie aber nicht deaktivieren.

In den GPOs finden Sie die Telemetrie-Einstellungen in der Computerkonfiguration unter **Administrative Vorlagen – Windows-Komponenten – Datensammlung und Vorabversionen**. Unter **Telemetrie Zulassen** können Sie anpassen, wie viele Daten an Microsoft übertragen werden. Ihnen stehen hier vier Stufen zur Verfügung.

Stufe	Bedeutung
0 – Sicherheit (Nur Enterprise)	Diese Einstellung sammelt nur Informationen über das Malicious Software Removal Tool (MSRT), Windows Defender und System Center Endpoint Protection sowie einige wenige Basisdaten für die Konfiguration der Telemetrie-Dienste selbst. Die Antimalwaredaten werden nicht übermittelt, wenn Sie MSRT abschalten und eine Fremdhersteller-Antiviruslösung verwenden. Laut einer Untersuchung des BSI und des BayLDA werden hier seit der Version 1909 keine Telemetriedaten mehr übertragen, wenn gleichzeitig die *Windows Restricted Traffic Limited Functionality Baseline* aktiviert ist. Mehr zur Baseline erfahren Sie weiter unten. Diese Einstellung wird nur von Windows 10 Enterprise ausgewertet. Alle anderen Windows-Versionen ignorieren diese Einstellung.
1 – Einfach (entspricht ab 1903 „Erforderlich“)	Zu den Daten aus Stufe 0 werden Geräteinformationen gesammelt (Prozessor, Speicher, OS-Daten, Internet-Explorer-Version usw.), Informationen über Abstürze und Anwendungsfehler, Kompatibilitätsdaten und den Microsoft Store.
2 – Erweitert	**Microsoft hat diese Diagnosestufe mit FR 1903 abgeschafft! Ab 1903 entspricht diese Stufe Einfach bzw. Erforderlich** Zu den Daten aus Stufe 0 und 1 werden Ereignisse (aus dem Ereignisprotokoll) gesammelt, die über Windows-Komponenten, Microsoft-Apps und -Geräte protokolliert wurden, sowie Absturz-Diagnosedaten. Diese Stufe lässt sich nicht in den Windows-Einstellungen manuell konfigurieren, sondern nur über Gruppenrichtlinien!
2 – Erweiterte Diagnosedaten auf die von Windows Analytics erforderlichen Daten beschränken	**Microsoft hat diese Diagnosestufe mit FR 1903 abgeschafft! Ab 1903 entspricht diese Stufe Einfach bzw. Erforderlich** Diesen Level aktivieren Sie über die Stufe 2 und die zusätzliche Richtlinie „Erweiterte Diagnosedaten auf die von Windows Analytics erforderlichen Daten beschränken“. Sie können den Clouddienst Desktop Analytics (früher Windows Analytics) verwenden, um die Daten Ihrer Clients zentral auszuwerten. Durch Desktop Analytics ist es z. B. möglich, die Windows Update for Business-Daten zentral zu sammeln. Desktop Analytics benötigt für die Datensammlung mehr Informationen, als die Stufe Basis zur Verfügung stellt. Mit dieser Richtlinie schränken Sie die Einstellung „Erweitert“ auf das Minimum ein, das für Analytics notwendig ist. Diese Richtlinie steht ab Feature Release 1709 zur Verfügung.
3 – Vollständig (entspricht ab 1903 „Optionale Diagnosedaten“)	Die vollständige Telemetrie sammelt neben den Stufen 0 bis 2 noch Daten zu Pre-Release-Apps von Windows, die im Windows Insider-Ring ausgerollt werden. Außerdem kann Microsoft vom Client zusätzliche Daten wie Registry-Keys, vollständige Absturz-Diagnosedaten und Reports von msinfo32.exe, dxdiag.exe und powercfg.exe bei Bedarf anfordern, um Windows Fehler zu analysieren. Dies ist die Standardeinstellung in Windows 10 Pro.

Eine vollständige Auflistung, wie Microsoft die Daten auswertet und welche Daten genau übertragen werden, finden Sie unter *https://docs.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization* oder kurz *https://bit.ly/2LZbf8N* sowie *https://docs.microsoft.com/de-de/windows/privacy/changes-to-windows-diagnostic-data-collection* oder kurz *https://bit.ly/39tZWDO* für die Änderungen ab FR 1903.

Unter Datensammlung und Vorabversion gibt es noch eine Reihe von weiteren interessanten Einstellungen zur Telemetrie.

Einstellung	Auswirkungen	FR
Benutzersteuerung für Insider-Builds ein-/ausschalten	Wenn Sie diese Einstellung auf deaktiviert setzen, können Benutzer Windows 10 nicht mehr selbstständig in die Insider Preview aufnehmen. Diese Einstellung wird ab Feature Release 1709 über die Einstellung „Vorabversionen verwalten“ unter **Computerkonfiguration – Administrative Vorlagen – Windows-Komponenten – Windows Update – Windows Update für Unternehmen** konfiguriert.	Bis 1703
Übermitteln des Gerätenamens in Windows-Diagnosedaten zulassen	Hiermit können Sie aktivieren, dass der Name des Windows-Gerätes in den Telemetriedaten übermittelt werden darf. Standardmäßig wird er **nicht** übermittelt!	Ab 1803
Organisations-ID konfigurieren	Wenn Sie Windows Analytics verwenden, werden über die Organisations-ID Ihre Windows-Geräte Ihrer Organisation zugeordnet. Mehr dazu finden Sie unter *https://docs.microsoft.com/en-us/windows/deployment/update/windows-analytics-get-started* oder kurz *https://bit.ly/2NT67Dz* und *https://docs.microsoft.com/en-us/windows/deployment/update/windows-analytics-privacy* oder kurz *https://bit.ly/2AlDhtN*.	
Konfigurieren von Telemetrie-Opt-In-Änderungsbenachrichtigungen	Seit Feature Release 1803 gibt der Client bei der ersten Anmeldung eine Benachrichtigung aus, wenn die Telemetrie deaktiviert ist (Level 0). Das Gleiche macht er bei jeder Änderung. Mit dieser Richtlinie schalten Sie die Benachrichtigungen aus. 	Ab 1803
Konfigurieren der Benutzeroberfläche der Telemetrie-Opt-In-Einstellung	Diese Einstellung legt fest, ob Benutzer ihre Telemetriedaten in den Windows-Einstellungen unter **Datenschutz – Diagnose und Feedback** selber einstellen können.	Ab 1803
Verwendung des authentifizierten Proxys für den Dienst „Benutzererfahrung und Telemetrie im verbundenen Modus“	Hiermit können Sie festlegen, ob die Telemetriedienste unter Verwendung der Benutzer-Anmeldedaten eine Verbindung über einen Proxyserver mit Authentifizierungszwang herstellen dürfen. Standardmäßig ist dieses Feature deaktiviert. Alternativ können Sie für den Telemetriedienst unter „Benutzererfahrung und Telemetrie im verbundenen Modus konfigurieren“ einen eigenen Proxy hinterlegen.	Ab 1511 mit CU

Einstellung	Auswirkungen	FR
Benutzererfahrung und Telemetrie im verbundenen Modus konfigurieren	Hier können Sie den Proxyserver und den Port im Format *IP:Port* eingeben, der vom Telemetriedienst verwendet werden soll. Diese Einstellung wird verwendet, wenn „Verwendung des authentifizierten Proxys für den Dienst Benutzererfahrung und Telemetrie im verbundenen Modus“ deaktiviert ist. Ausführliche Informationen hierzu finden Sie unter *https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/configure-proxy-internet-windows-defender-advanced-threat-protection* oder kurz *https://bit.ly/2Ah8TRm*.	1507
Feedbackbenachrichtigungen nicht mehr anzeigen	Die Windows Feedback-App fordert den Benutzer regelmäßig zur Abgabe von Feedbacks auf, wenn er mit einem Windows Live-ID-Konto angemeldet ist. Mit dieser Einstellung können Sie die Benachrichtigung deaktivieren.	1507
Diagnosedatenanzeige deaktivieren	Verhindert, dass der Benutzer die Diagnosedatenanzeige konfigurieren kann. Die Diagnosedatenanzeige wird im Anschluss beschrieben.	1809
Deaktivieren Sie das Löschen der Diagnosedaten	Blockiert den Zugriff auf den Löschen-Button in den Einstellungen der Diagnosedaten in den Windows-Einstellungen.	1809

Achten Sie bei den Einstellungen darauf, dass die Option **Deaktiviert** meistens keine Auswirkung hat, sondern die Funktionen über ein Drop-down-Fenster festgelegt werden, wenn Sie eine Einstellung deaktivieren wollen. Diese unangenehme Eigenheit scheint sich bei Microsoft langsam einzubürgern, ist aber absolut kontraintuitiv.

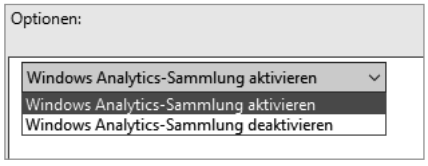


Bild 12.7
Einstellungen werden über Drop-down-Menüs im Aktivieren-Menü abgeschaltet.

Um zu prüfen, welche Daten Windows nach Hause übermittelt, können Sie den Diagnostic Data Viewer aus dem Windows Store herunterladen. Zuerst müssen Sie allerdings in den Windows-Einstellungen unter **Datenschutz – Diagnose und Feedback** die Diagnosedatenanzeige aktivieren. Diese Funktion steht Ihnen ab Feature Release 1803 zur Verfügung.

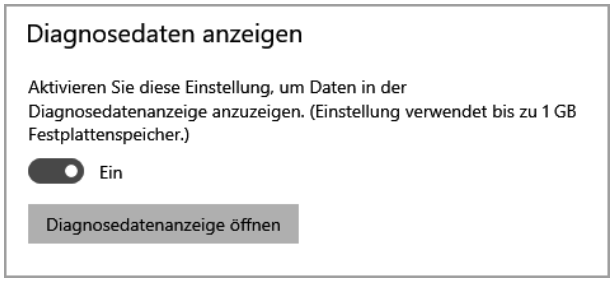


Bild 12.8
Diagnosedatenanzeige aktivieren und den Viewer direkt herunterladen

Anschließend können Sie direkt über den Windows Store oder über Auswahl des Buttons **Diagnose Datenviewer** die Diagnosedatenanzeige herunterladen. Sie können die Auswertung auch mit Hilfe von PowerShell automatisieren. Den dazu passenden Artikel finden Sie unter *https://docs.microsoft.com/en-us/windows/privacy/microsoft-diagnosticdataviewer* oder kurz *https://bit.ly/3mzCxF9*.

Bild 12.9 Die Diagnosedatenanzeige zeigt die gesammelten Informationen im JSON-Format an.

Die App zeigt die Daten in drei Spalten an. Ganz links können Sie filtern, welche Datenkategorien angezeigt werden sollen, in der mittleren Spalte sehen Sie die einzelnen Sammlungsdaten nach Uhrzeit und rechts sehen Sie gesammelten Daten im JSON-Format. Hier kann man sehr deutlich erkennen, dass Windows eine Menge an Daten zusammenträgt.

Microsoft hat zur Interpretation der Daten inzwischen eine Menge Informationen zusammengestellt. Sie finden Sie unter *https://docs.microsoft.com/en-us/windows/privacy/basic-level-windows-diagnostic-events-and-fields* oder kurz *https://bit.ly/2LAuhq1* für die Basisdaten und *https://docs.microsoft.com/en-us/windows/privacy/windows-diagnostic-data* oder kurz *https://bit.ly/2uX79HK* für die vollständige Telemetrie.

Achten Sie darauf, die Datensammlung nicht dauerhaft zu aktivieren, da die Datensammlung Last auf dem Datenträger erzeugen kann und erhebliche Mengen an Daten auf die Festplatte schreibt.

12.2.2 Funktionsdaten

Als Funktionsdaten bezeichnet Microsoft Daten, die von Apps an den Hersteller übertragen werden können. Viele Apps wie Cortana müssen Daten schon deshalb übertragen, weil die Hauptfunktion, nämlich die Spracherkennung, gar nicht durch die App, sondern durch einen Cloudservice (Bing) durchgeführt wird. Funktionsdaten sind von den Einschränkungen der Telemetrie nicht betroffen und müssen extra deaktiviert werden.

12.2.2.1 Cortana

Cortana ist Microsofts Sprachassistentin, benannt nach der künstlichen Intelligenz aus dem Xbox-Spiel Halo. Sie steht in direkter Konkurrenz zu Amazons Alexa, Apples Siri, Googles Assistant und wie sie noch alle heißen. Cortana ist seit der ersten Version von Windows 10 Bestandteil des Betriebssystems und soll es dem Benutzer erlauben, den Computer durch Sprachbefehle zu steuern. Seitdem hat Microsoft Cortana stetig zu einem Unternehmensassistenten weiterentwickelt, der sich in Office 365 und andere Microsoft-Dienste wie LinkedIn integrieren und dort auf Benutzerdaten zugreifen kann. Das erlaubt es Cortana, an Termine zu erinnern, Personendaten aus LinkedIn abzurufen, Termine zu erstellen, Websuchen durchzuführen usw.

Cortana und die Windows-Suche waren anfangs in der Suche integriert, inzwischen hat Microsoft die beiden Funktionen aber getrennt – Cortana kann jetzt über einen eigenen Button mit einem Kreis als Symbol aufgerufen werden. Sie benutzt ausschließlich Bing für die Websuche. Bei Bing werden auch die Benutzerdaten gespeichert, die Cortana sammelt. Was Cortana bzw. Bing über Sie gespeichert hat, können Sie auf der Website *https://account.microsoft.com/privacy* nachlesen und löschen. Sie finden hier z. B. Ihre Browsing-Historie oder Ihre Standortdaten wieder, soweit diese von Cortana aufgezeichnet wurden.

Bild 12.10
Richten Sie Cortana ein, werden automatisch Ihre Benutzerdaten gescannt

Um Cortana einzuschränken oder sie zu deaktivieren, stellt Ihnen Windows einige Einstellungen zur Verfügung, über die konfiguriert werden kann, welche Funktionen Cortana nutzen darf. Die meisten Einstellungen finden Sie in der Computerkonfiguration unter **Administrative Vorlagen – Windows-Komponenten – Suche**.

Einstellung	Auswirkungen
Cortana zulassen	Mit dieser Einstellung können Sie Cortana komplett deaktivieren. Die Suche im Startmenü funktioniert auch ohne Cortana einwandfrei.
Nicht im Web suchen und keine Webergebnisse in der Suche anzeigen	Legt fest, ob die Windows-Suche auch Webabfragen stellen und in den Suchergebnissen anzeigen darf. Diese Einstellung wird aber von dem Feature Release 1803 der Professional Edition ignoriert. Da Cortana auf die Verbindung mit Bing angewiesen ist, wird in der Enterprise Edition Cortana mit dieser Einstellung effektiv abgeschaltet. Der Unterschied zu „Cortana zulassen“ ist, dass das Deaktivieren von Cortana der Suche immer noch die Option lässt, Bing zu nutzen. Diese Einstellung ist also restriktiver als „Cortana zulassen“.
Cloudsuche zulassen	Mit dieser Einstellung können Sie verhindern, dass die Windows-Suche auch auf Ergebnisse aus Online-Diensten wie OneDrive oder SharePoint Online zugreifen darf. Dies ist keine Cortana-spezifische Einstellung, sondern bezieht sich auf die Windows-Suche.
Cortana auf Sperrbildschirm zulassen	Ist diese Einstellung aktiviert, kann Cortana auch dann Sprachbefehle empfangen und verarbeiten, wenn der Sperrbildschirm aktiviert ist. Aus Sicherheitsgründen ist es besser, diese Option zu deaktivieren, da sie schon zum Umgehen der Windows-Sicherheitsmaßnahmen verwendet wurde. Diese Funktion wird von Cortana ab FR 2004 aktuell nicht mehr unterstützt!
Der Suche und Cortana die Nutzung von Positionsdaten erlauben	Legt fest, ob Cortana für Webanfragen auf die aktuellen Ortsdaten zugreifen darf. Die Ortsdaten werden in regelmäßigen Abständen aus verschiedenen Datenquellen wie Wi-Fi-Netzwerken und GPS-Daten ermittelt. Mehr dazu, wie Windows Standortdaten ermittelt und verwendet, finden Sie unter *https://privacy.microsoft.com/en-us/windows-10-location-and-privacy* oder kurz *https://bit.ly/2LPFd2f*.

In der **Computerkonfiguration** unter **Administrative Vorlagen – Systemsteuerung – Regions- und Sprachoptionen** finden Sie noch folgende Einstellungen:

Einstellung	Auswirkungen
Aktivierung von Online-Spracherkennungsdiensten durch Benutzer zulassen früher: Eingabeanpassung zulassen	Wenn Sie diese Einstellung deaktivieren, verhindern Sie die Sprach- und Handschrifterkennung. Bis zur Version 1511 hat das Deaktivieren dazu geführt, dass Cortana gar nicht mehr verwendet werden konnte. Aber 1607 wird einfach nur die Sprachsteuerung von Cortana deaktiviert.

In der Computerkonfiguration unter **Administrative Vorlagen – Windows Komponenten – App-Datenschutz** können Sie außerdem festlegen, ob Apps über ein Weck-Wort aktiviert werden können.

Einstellung	Auswirkungen
Aktivieren von Windows-App mit Sprachbefehlen zulassen (ab 2004)	Ein Dropdown-Fenster (!) bestimmt, ob der Benutzer die Sprachsteuerung aktivieren kann oder die Sprachsteuerung grundsätzlich verweigert oder zugelassen wird. Das Deaktivieren der Richtlinie hat keine Auswirkungen.
Windows-App-Zugriff auf das Mikrofon zulassen (ab 2004)	Hier können Sie einzelnen Apps den Zugriff auf das Mikrofon erlauben oder verweigern (entspricht den App-Berechtigungen in den Windows-Einstellungen unter Datenschutz). Um Cortana den Zugriff auf das Mikrofon zu erlauben oder zu verweigern geben Sie den Namen der Paket-Familie ein: *Microsoft.549981C3F5F10_8wekyb3d8bbwe* Zum Bestimmen der Paketfamilie können Sie auch das PowerShell-Skript aus 12.2.4.2 – App-Datenschutz verwenden. Verweigern Sie Cortana den Zugriff auf das Mikrofon, werden die Spracheingabe-Funktionen von Cortana automatisch deaktiviert.

In der **Benutzerkonfiguration** unter **Administrative Vorlagen – Windows Komponenten – Datei-Explorer** können Sie auch noch weitere Einstellungen setzen:

Einstellung	Auswirkungen
Anzeige der letzten Sucheinträge im Datei-Explorer-Suchfeld deaktivieren	Verhindert, dass Suchanfragen gespeichert und bei späteren Anfragen als Vorschläge angezeigt werden.

Alle Einstellungen von Cortana finden Sie unter *https://docs.microsoft.com/en-us/windows/configuration/cortana-at-work/cortana-at-work-policy-settings* oder kurz *https://bit.ly/2MaWekf*. Die Richtlinien sollten hier auch für neuere Windows Releases aktualisiert werden.

Aus meiner Sicht ist Cortana hauptsächlich für mobile Geräte geeignet, also Smartphones und Tablets, und für Benutzer mit Einschränkungen. Stationäre Geräte werden seltener zur Terminplanung gebraucht und außerdem ist es ziemlich hinderlich, wenn in einem Büro mehrere Kollegen gleichzeitig versuchen, sich mit Cortana zu verständigen. Für diese Szenarien deaktivieren Sie Cortana besser.

12.2.3 Weitere Datenschutzoptionen

Neben der Windows-Telemetrie gibt es noch eine ganze Reihe von anderen Apps und Features, die Daten übertragen oder eine Benutzeridentifizierung ermöglichen. Hier möchte ich Ihnen nur einen Überblick über die wichtigsten Einstellungen geben.

12.2.3.1 Werbe-ID deaktivieren

Computerkonfiguration – Administrative Vorlagen – System – Benutzerprofile

Die Werbe-ID wird dazu verwendet, Benutzer anwendungsübergreifend wiederzuerkennen, ohne Personendaten zwischen den Anwendungen zu teilen. Damit wird es möglich, dass die

Daten, die ein Onlineshop über Benutzer gesammelt hat, genutzt werden können, um in der nächsten Anwendung wieder Werbung genau dieses Onlineshops anzeigen zu können. Microsoft bezeichnet das als relevante Werbung, weil beworben werden kann, wofür der Benutzer sich interessiert. Während dem Benutzer vermittelt wird, dass er nicht mehr mit uninteressanter Werbung zugespammt wird, ist es für werbende Unternehmen natürlich viel zielführender, wenn Sie dem Benutzer das Produkt bewerben können, das wirklich seinen Interessen entspricht.

Prinzipiell sollte die Werbe-ID ungefährlich sein, da sie anonymisiert ist, um auf Nummer sicher zu gehen, sollte man die ID aber trotzdem deaktivieren.

12.2.4 Windows Defender Smartscreen konfigurieren

Computerkonfiguration – Administrative Vorlagen – Windows-Komponenten – Datei Explorer

Smartscreen prüft beim Ausführen von Programmen, die aus dem Internet heruntergeladen wurden, ob diese potenziell schädlich sind. Dazu werden Programminformationen an einen Microsoft Webserver weitergeleitet, der die Datei identifiziert. Sie kennen vermutlich den Dialog „Der Computer wurde durch Windows geschützt“. Problematisch ist, dass Microsoft nicht dokumentiert hat, welche Daten hier übertragen werden.

Mit dieser Einstellung können Sie Smartscreen deaktivieren, um den Upload von Programmdaten zu verhindern. Es ist allerdings empfohlen, Smartscreen aktiviert zu lassen. Sie können Smartscreen über „Aktivieren“ auch so konfigurieren, dass Smartscreen das Ausführen von Programmen komplett verhindert und nicht nur warnt. Setzen Sie die Richtlinie dafür auf „Warnen und Umgehung verhindern“.

12.2.4.1 Feedbackbenachrichtigungen nicht mehr anzeigen

Computerkonfiguration – Administrative Vorlagen – Windows-Komponenten – Datensammlung und Vorabversionen

Die Windows Feedback-App gehört zu den Standard-Apps, die mit Windows geliefert werden. Die Feedback-App zeigt Informationen zu neuen Feature Releases an und kann auch genutzt werden, um Feedback zu Windows 10 an Microsoft zu liefern, wie Bugs oder Feature-Anfragen. Die Feedback-App kann selbstständig Feedback anfragen. Mit dieser Einstellung unterdrücken Sie Meldungen der Feedback-App.

12.2.4.2 App-Datenschutz

Computerkonfiguration – Administrative Vorlagen – Windows-Komponenten – App-Datenschutz

Unter App-Datenschutz können Sie konfigurieren, auf welche Geräte und Daten Windows-Apps zugreifen können. Sie konfigurieren hier einen Teil der Einstellungen, die unter Windows in den Einstellungen unter Datenschutz zu finden sind. Diese Einstellungen, die Sie hier vornehmen, gelten ausschließlich für Apps und werden von klassischen Anwendungen ignoriert. Zum Erlauben oder Verbieten von Apps müssen Sie die App-Paketfamilie ermitteln. Dabei hilft Ihnen das folgende PowerShell-Skript:

```
( Get-AppxPackage | Out-GridView -PassThru ).Packagefamilyname |
   Set-Clipboard
```

Wenn Sie das Skript in der PowerShell ausführen, öffnet sich ein Fenster mit allen im Benutzerkontext installierten Apps. Sie können die Apps nach Namen filtern – das Skript kopiert Ihnen dann die IDs der Paketfamilien in die Zwischenablage.

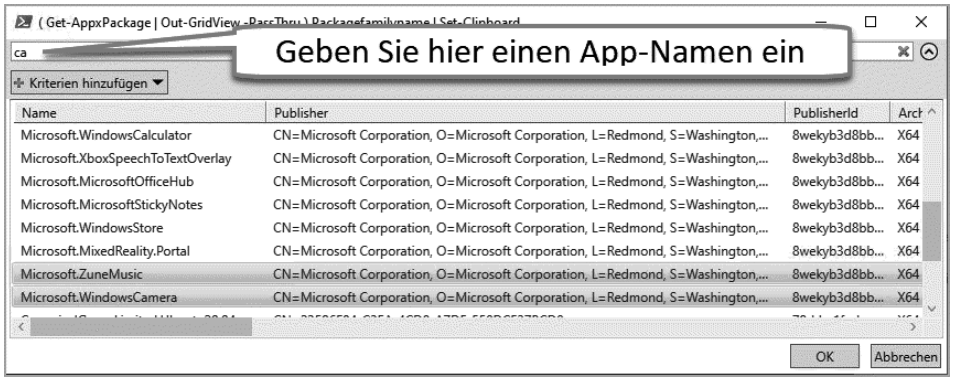


Bild 12.11 Filtern Sie im Suchen-Fenster die Apps nach Namen

12.2.4.3 Verwendung von OneDrive für die Datenspeicherung verhindern

Computerkonfiguration – Administrative Vorlagen – Windows-Komponenten – OneDrive

Wenn Sie Office 365 und OneDrive nicht verwenden, können Sie über diese Einstellung das Speichern in OneDrive verhindern und OneDrive auf dem Navigationsbereich des Explorers ausblenden.

12.2.4.4 Einstellungen synchronisieren

Computerkonfiguration – Administrative Vorlagen – Windows-Komponenten – Einstellungen synchronisieren

Hier können Sie für verschiedene Optionen wie Kennwörter, Konfigurationseinstellungen und App-Einstellungen festlegen, ob diese zentral über alle Ihre Geräte synchronisiert werden sollen.

12.2.4.5 Beitritt zu Microsoft MAPS

Computerkonfiguration – Administrative Vorlagen – Windows-Komponenten – Microsoft Defender Antivirus – MAPS

Das Microsoft MAPS-Programm wertet Daten des Windows Defender aus. Windows Defender kann auffälliges Verhalten oder erkannte Malware an Microsoft zur weiteren Analyse schicken, wenn Sie am MAPS-Programm teilnehmen. Deaktivieren Sie diese Einstellung, oder geben Sie an, ob Sie nur Basisinformationen an Microsoft senden wollen oder ob detaillierte Informationen über auffällige Software versendet werden können, wie Speicherort des Programms, Dateinamen, Prozessinformationen usw.

12.2.4.6 Dateibeispiele senden, wenn eine weitere Analyse erforderlich ist

Computerkonfiguration – Administrative Vorlagen – Windows-Komponenten – Microsoft Defender Antivirus – MAPS

Über das MAPS-Programm können bei Erkennung einer auffälligen Software von Microsoft weitere Daten vom Computer angefordert werden. Hier legen Sie fest, ob und wann Beispieldaten übermittelt werden dürfen. Sie können das Senden von Daten komplett unterbinden, eine Benutzererlaubnis vor dem Senden anfordern oder das Senden automatisieren.

12.2.4.7 Programm zur Verbesserung der Benutzerfreundlichkeit deaktivieren

Computerkonfiguration – Administrative Vorlagen – System – Internetkommunikationsverwaltung – Internetkommunikationseinstellungen - Programm zur Verbesserung der Benutzerfreundlichkeit deaktivieren

Neben der Windows-Telemetrie ein weiteres Programm, um Verwendungsdaten zu sammeln. Das Programm zur Verbesserung der Benutzerfreundlichkeit wird dazu verwendet, um „Trends und Verwendungsmuster zu erkennen" – was immer das heißen mag. Sie können die Features dieses Programms einzeln deaktivieren oder mit der Richtlinie *Programm zur Verbesserung der Benutzerfreundlichkeit deaktivieren* die Datenübertragung komplett verhindern. Achten Sie darauf, dass die Richtlinie zweimal existiert – einmal bis Windows XP/Server 2003 und einmal ab Windows Vista.

12.2.4.8 Anwendungstelemetrie deaktivieren

Computerkonfiguration – Administrative Vorlagen – Windows-Komponenten – Anwendungskompatibilität - Anwendungstelemetrie deaktivieren

Mit dieser Einstellung verhindern Sie, dass die Verwendung von Systemkomponenten durch Anwendungen anonym an Microsoft gesendet wird. Wenn Sie das Programm zur Verbesserung der Benutzerfreundlichkeit deaktiviert haben, werden keine Anwendungstelemetrie-Daten übertragen.

12.2.4.9 Inventory Collector

Computerkonfiguration – Administrative Vorlagen – Windows-Komponenten – Anwendungskompatibilität – Inventory Collector

Der Inventory Collector sammelt Informationen über Geräte und Treiber und sendet sie anonym an Microsoft. Auch hier gilt, haben Sie das Programm zur Verbesserung der Benutzerfreundlichkeit deaktiviert, werden auch keine Inventardaten mehr übermittelt.

12.2.4.10 Features von Windows-Blickpunkt deaktivieren

Benutzerkonfiguration – Administrative Vorlagen – Windows-Komponenten – Cloudinhalt – Features von Windows-Blickpunkt deaktivieren

Wenn Sie diese Einstellung aktivieren, wird Windows-Blickpunkt vollständig deaktiviert. Windows-Blickpunkt ersetzt das klassische Hintergrundbild durch wunderschöne Fotos, die mit Werbeeinblendungen garniert sein können. Es handelt sich dabei um kleine Texteinblendungen, die dem Benutzer Windows-Features vorschlagen. Es können aber auch Fremdhersteller-Apps vorgeschlagen werden.

Neben der Möglichkeit, Windows-Blickpunkt vollständig zu deaktivieren, was leider auch die wechselnden Hintergrundbilder abschaltet, können Sie mit weiteren Gruppenrichtlinien unter „Cloudinhalt“ Windows-Blickpunkt auch gezielt konfigurieren.

Windows 10 Professional ignoriert diese Einstellung – Windows-Blickpunkt lässt sich hier nicht durch Gruppenrichtlinien deaktivieren.

12.2.4.11 Sammlung von Browserdaten für die Microsoft 365-Analyse konfigurieren

Benutzerkonfiguration – Administrative Vorlagen – Windows-Komponenten – Datensammlung und Vorabversion – Sammlung von Browserdaten für die Desktop Analytics konfigurieren

Diese Einstellung ist neu in Feature Release 1803 hinzugekommen. Deaktivieren Sie die Einstellung, um Edge daran zu hindern, Browserverlaufsdaten an Desktop Analytics zu senden. Analytics ist ein Zusatzdienst in Microsoft 365 (ehemals Office 365), der die Produktivität des Nutzers steigern soll und dazu seine Arbeitsweise auswertet. Standardmäßig ist das Übertragen deaktiviert, und Sie müssen zusätzlich eine Unternehmens-ID in den Gruppenrichtlinien konfigurieren, bevor überhaupt eine Zuordnung der Daten stattfinden kann.

12.2.4.12 Sensoren deaktivieren

Benutzerkonfiguration – Administrative Vorlagen – Windows-Komponenten – Position und Sensoren – Sensoren deaktivieren

Mit „Sensoren deaktivieren“ können Sie die Positionssensoren (vornehmlich GPS) abschalten. Alternativ können Sie auch den Zugriff auf die Positionssensoren abschalten, indem Sie **Speicherort deaktivieren** einschalten. Beide Einstellungen verhindern effektiv, dass Anwendungen den Standort des Gerätes auslesen können.

12.2.4.13 Windows Fehlerberichterstattung deaktivieren

Benutzerkonfiguration – Administrative Vorlagen – Windows-Komponenten – Windows-Fehlerberichterstattung – Windows Fehlerberichterstattung deaktivieren

Mit dieser Einstellung deaktivieren Sie das Senden von Fehlerinformationen an Microsoft. Dieses Feature wird dazu verwendet, Daten über Programmabstürze direkt an Microsoft zu senden. Nach einem Absturz kann man direkt in der Fehlermeldung das Senden von Daten anwenden oder über die Einstellung „Speicherabbild für vom Betriebssystem erstellte Fehlerberichte automatisch senden“ den Vorgang auch automatisieren. Diese Daten werden von Microsoft verwendet, um Windows-Fehler zu beheben. Wenn der Fehler behoben ist, kann Microsoft über das Benachrichtigungsfenster sogar eine Meldung an den Benutzer schicken. Wenn Sie die Fehlerberichterstattung deaktivieren, wird auch das Problemlösungsfeature in der Systemsteuerung und im Wartungsverlauf abgeschaltet, da es auf der Fehlerberichterstattung basiert.

12.2.4.14 gp-pack

Für diejenigen, die sich mit den Datenschutzeinstellungen in den Gruppenrichtlinien nicht herumschlagen möchten, gibt es noch eine (kostenpflichtige) Alternative. Mark Heitbrink, Betreiber von Gruppenrichtlinien.de und eine halbe Ewigkeit Microsoft MVP für Gruppenrichtlinien, hat eine ganze Reihe von fertigen Gruppenrichtlinien erstellt, die als Backup zur Verfügung gestellt werden und direkt in Ihre Umgebung importiert werden können. Die Pakete, gp-packs genannt, werden regelmäßig gepflegt und mit jeder neuen Windows-Version auf den aktuellen Stand gebracht. Da das jede Menge Arbeit macht, gibt es die Pakete allerdings nicht kostenlos, aber zu einem sehr überschaubaren Preis. Verschaffen Sie sich einfach selbst einen Überblick unter www.gp-pack.com

12.3 Der Microsoft Store

Der Microsoft Store ist der Ort, an dem Windows Apps beziehen kann. Apps (unter Windows 10 korrekterweise UWP-Apps oder Universal Windows Platform Apps) sind ein neues Anwendungsmodell, das Microsoft mit Windows 8 zum ersten Mal eingeführt hat und das eine Reihe von Vorteilen mit sich bringt. So sind Apps sicherer als normale Anwendungen, weil Apps grundsätzlich isoliert in einer Sandbox unter Windows laufen, also einem abgesicherten Container, aus dem die App nur auf die Daten zugreifen kann, die das System ihr erlaubt. Das System kann für Apps außerdem selektiv festlegen, auf welche Hardwareressourcen sie zugreifen darf. Sie kennen das vermutlich von Ihrem Mobiltelefon, denn dort ist dieses Konzept abgeschaut – wenn eine neue App zum ersten Mal gestartet wird, stellt das System die Frage, ob die App auf alle angefragten Ressourcen zugreifen darf. Sie können den Zugriff dann prüfen – braucht die App wirklich einen Zugang zu Ihrem Mikrofon, Ihrer Kamera oder Ihren Kontakten – und dann den Zugriff erlauben oder ablehnen. Apps werden außerdem nur dann installiert und ausgeführt, wenn der Anwendungscode digital signiert ist.

Apps können auf mehrere Arten installiert werden – über den Windows Store, über PowerShell oder in Form der neuen MSIX-Pakete. Der Windows Store ist selbst eine App und mit jeder Windows 10-Installation verfügbar. Über ihn kann der Benutzer beliebige Anwendungen selbst installieren – er benötigt hierfür keine administrativen Rechte! Da der Windows Store offenbar in erster Linie Filme und Spiele beinhaltet, ist das aber nicht unbedingt das, was sich ein Administrator wünscht – s. Bild 12.12.

Unter **Updates und Sicherheit – Für Entwickler** können Sie den Schieberegler **Installieren Sie Apps aus beliebigen Quellen einschließlich loser Dateien** aktivieren. Er erlaubt Benutzern das Installieren von Apps am App-Store vorbei. Diese Funktion hat Microsoft früher als Sideloading oder, hübsch ins Deutsche übersetzt, Querladen bezeichnet. Die Gruppenrichtlinie, um Sideloading zu aktivieren, heißt „Verhindern, dass Benutzer ohne Adminstratorrechte verpackte Apps installieren“ und findet sich in der Computerkonfiguration unter **Administrative Vorlagen – Windows-Komponenten – Bereitstellung von App-Paketen**. Microsoft hat das Feature angepasst, um höhere Akzeptanz bei den Benutzern zu erreichen – in früheren Feature-Releases war das Installieren von App-Paketen grundsätzlich für alle Benutzer gesperrt.

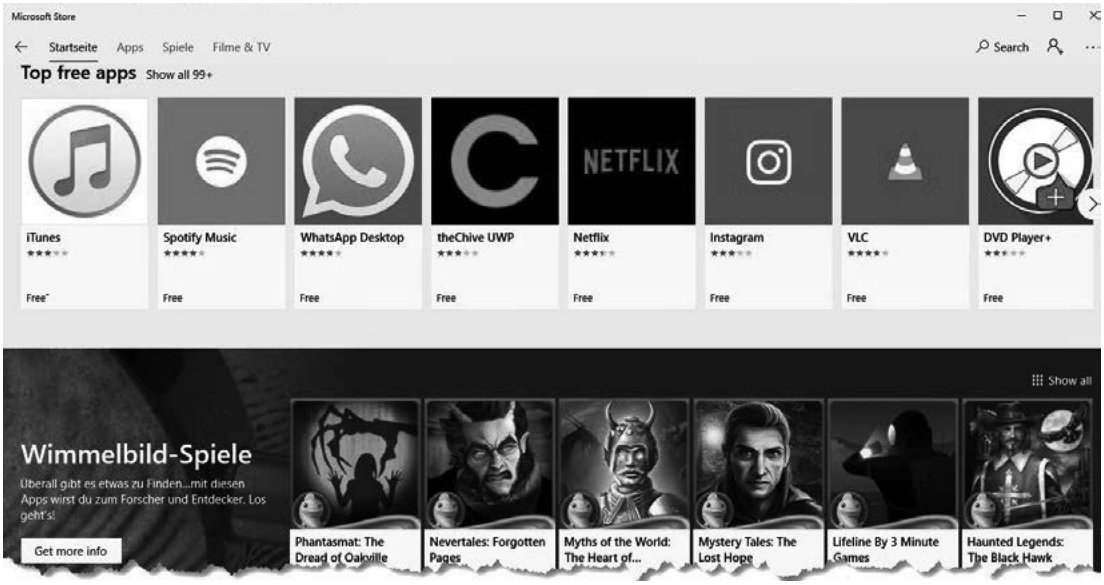


Bild 12.12 Der Albtraum jedes Administrators – der Windows Store

Es gibt mehrere Möglichkeiten, wie Sie mit dem Windows Store umgehen können. Zum einen können Sie ihn natürlich aktiviert lassen – Apps sind normalerweise sicher und werden auch nur pro Benutzer installiert, sodass der Anwender im Normalfall nichts kaputt machen kann. Malware sollte von vornherein nicht in den Windows Store gelangen, und im Zweifel schottet Windows eine App so gut ab, dass sie nicht viel Schaden anrichten kann.

Alternativ können Sie auch die Windows-Store-App entfernen. Dafür verwenden Sie PowerShell oder die dism.exe. Wichtig für das Verständnis – Sie müssen zwischen für den Benutzer installierten und von Windows für die Installation bereitgestellten (provisionierten Apps) unterscheiden. Eine provisionierte App ist quasi die lokale Installationsquelle für eine von Windows mitgelieferte App.

Installierte Apps entfernen Sie mithilfe des PowerShell-Cmdlets `Get-AppxPackage`, während Sie die Installationsquellen mithilfe des Cmdlets `Get-AppxProvisionedPackage` löschen.

Listing 12.1 Entfernen des Windows Store

```
Remove-AppxPackage -Package Microsoft.WindowsStore_11806.1001.21.0_x64__8wekyb3d8bbwe
Remove-AppxPackage -Package Microsoft.WindowsStore_11806.1001.21.0_
x64__8wekyb3d8bbwe`-AllUsers
$Store = Get-AppxProvisionedPackage -Online  | Where-Object displayname -eq
Microsoft.Store
Remove-AppxProvisionedPackage -PackageName $Store.PackageName -online
```

In Listing 12.1 sehen Sie drei Beispiele zum Entfernen des Stores, die alle etwas anderes machen. Der erste Aufruf entfernt die Windows-Store-App für den aktuell angemeldeten Benutzer. Für alle anderen lokalen Benutzerprofile bleibt der Store erhalten.

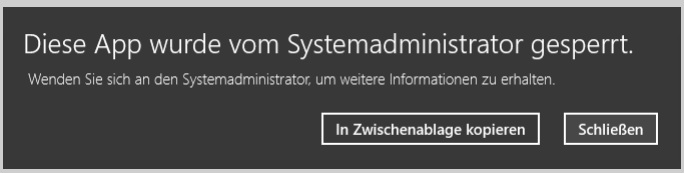
Der zweite Aufruf entfernt die Store-App für alle Benutzer, die auf dem Computer, auf dem das Skript ausgeführt wird, ein Benutzerprofil haben. In beiden Fällen bleiben allerdings

die Installationsquellen des Stores erhalten. Ein neuer Benutzer bekommt den Store also wieder installiert.

Mit dem Aufruf von `Remove-AppxProvisionedPackage` entfernen Sie die Installationsquellen des Stores. Alle neuen Benutzer bekommen keinen Store installiert. Bereits angemeldete Benutzer behalten ihren installierten Store aber, nur neue Benutzer sind von dieser Maßnahme betroffen.

Am besten ist es daher, den Store bereits vor der Installation aus dem WIM-Image zu entfernen. Dafür müssen Sie ein WIM-Image mithilfe von `Mount-WindowsImage` in einem leeren Ordner bereitstellen, mit `Remove-AppxProvisionedPackage -Path <Pfad zum Mount-Ordner>` das Paket entfernen und die Änderungen dann wieder im WIM-File speichern. Eine genaue Beschreibung finden Sie in meinem Blog unter *https://www.netz-weise-it.training/weisheiten/tipps/item/430-windows-apps-von-windows-entfernen-vor-und-nach-der-installation.html* oder kurz *https://bit.ly/2M3Bzlr*.

Sie können den App-Store auch über eine Gruppenrichtlinie blockieren und dem Benutzer so den Zugriff auf den App-Store verweigern. Die folgenden Richtlinien finden Sie in der Computerkonfiguration unter **Administrative Vorlagen – Windows-Komponenten – Store**, die beiden Einstellungen „Store-Anwendung deaktivieren“ und „Nur den privaten Store im Microsoft Store anzeigen“ auch in der Benutzerkonfiguration.

Einstellung	Auswirkungen
Store-Anwendung deaktivieren	Blockiert den Zugriff auf den Windows Store. Der Store ist also nach wie vor als App vorhanden, aber wenn der Benutzer den Store aufruft, bekommt er die Meldung „Microsoft Store ist blockiert“. Der Store wird beim ersten Starten nach Aktivieren der Richtlinie noch angezeigt, schaltet dann aber kurz darauf um. Die Richtlinie „Alle Apps aus dem Microsoft Store deaktivieren“ blockiert sofort. Der Store lässt sich mit dieser Einstellung unter Windows 10 nicht blockieren!
Alle Apps aus dem Microsoft Store deaktivieren	Wer die doppelte Verneinung in administrativen Vorlagen gut findet, wird diese Einstellung lieben. Wird sie DEAKTIVERT, wird der Microsoft Store deaktiviert und alle aus dem Store heruntergeladenen Apps ebenso. Dies ist also eine nochmals verschärfte Einstellung der Richtlinie „Store-Anwendung deaktivieren“. **Nochmal:** Sie müssen die Einstellung „Alle Apps aus dem Microsoft Store deaktivieren“ deaktivieren! Das ist auch keine Fehlübersetzung, die Richtlinie heißt im Original „Disable all apps from Microsoft Store“ und muss ebenfalls deaktiviert werden. Vermutlich war der Ersteller dieser Richtlinie von der doppelten Verneinung genauso irritiert wie der normale Admin … Der Benutzer bekommt dann eine Systemmeldung, dass die App gesperrt wurde.  **Bild 12.13** Diese Meldung wird dem Nutzer angezeigt, wenn er den Store öffnen will.

Einstellung	Auswirkungen
Nur den privaten Store im Microsoft Store-anzeigen	Wenn Sie diese Einstellung aktivieren, werden Benutzer in den Unternehmensstore umgeleitet. Mit dem Unternehmensstore ist es möglich, einzelne Apps aus dem öffentlichen Store auszuwählen und Benutzern zur Verfügung zu stellen. Für den Unternehmensstore ist ein Azure-AD-Account notwendig. Diesen erhalten Sie z. B., wenn Ihr Unternehmen Office 365 nutzt. Mehr Informationen dazu finden Sie im Kasten „Windows Store für Unternehmen“.
Deaktivieren des Angebotes zum Update auf die aktuelle Version von Windows	Diese veraltete Einstellung soll auf Windows 7 und Windows 8(.1) verhindern, dass der Client automatisch das kostenlose Upgrade auf Windows 10 herunterlädt und installiert. Das Angebot existiert nicht mehr, und Windows 10 ist von dieser Einstellung nicht betroffen.
Automatisches Herunterladen von Installieren von Updates deaktivieren	Die Store-App lädt standardmäßig App-Updates automatisch herunter, wenn sie verfügbar sind, und installiert sie. Mit dieser Einstellung können Sie das automatische Aktualisieren abschalten. Um die Einstellung lokal zu setzen, öffnen Sie die Einstellungen des Windows Store über die drei Punkte oben rechts. In den Einstellungen finden Sie eine Option **App updates – Update Apps Automatically**.

Windows Store for Business

Der öffentliche Windows Store ist für die meisten Unternehmen vor allem eins – eine Anwendung, die man so schnell wie möglich abschalten möchte, da man dort eigentlich kaum etwas findet, das ein Unternehmen gerne auf den Rechnern der Anwender sehen möchte. Das weiß auch Microsoft, und daher haben sie den Microsoft Store for Business eingeführt. Der Store for Business ist kein zweiter Store, sondern die Möglichkeit, als Unternehmen Anwendungen auszuwählen, die den Benutzern zur Verfügung stehen sollen, und dann nur diese Anwendungen für den Benutzer sichtbar zu machen. Damit das funktioniert, muss der Benutzer, wenn er sich mit dem Store verbindet, allerdings seinem Unternehmen zugeordnet werden können, und das funktioniert mithilfe seines Azure AD Accounts. Azure AD ist der Verzeichnisdienst, der von Office 365 für die Benutzerverwaltung verwendet wird. Sie müssen nicht zwingend Office 365 nutzen, um Azure AD benutzen zu können, aber dann müssen Sie für Ihre Benutzer Lizenzen für Azure AD erwerben. Mehr zum Thema Azure AD erfahren Sie in Kapitel 17, Intune einrichten.

Den Store for Business können Sie unter *https://businessstore.microsoft.com* einrichten, indem Sie sich mit einem administrativen Konto Ihres Unternehmens anmelden. Als Schule oder Universität steht Ihnen der Education Store zur Verfügung, den Sie unter *https://educationstore.microsoft.com* finden. Die Zukunft des Store for Business ist aktuell allerdings unklar. Anfang 2020 gingen Gerüchte um, dass Microsoft den Support für den Business-Store einstellen möchte. Offizielle Aussagen dazu gibt es allerdings keine. Das gleiche Schicksal könnte allerdings auch den Windows Store selbst treffen, da Microsoft das UWP-Konzept offensichtlich zugunsten von MSIX aufgeben will.

Mehr Informationen zum Store für Unternehmen finden Sie unter *https://docs.microsoft.com/de-de/previous-versions/mt622668(v=msdn.10)* oder kurz *https://bit.ly/2JzkSPx*.

■

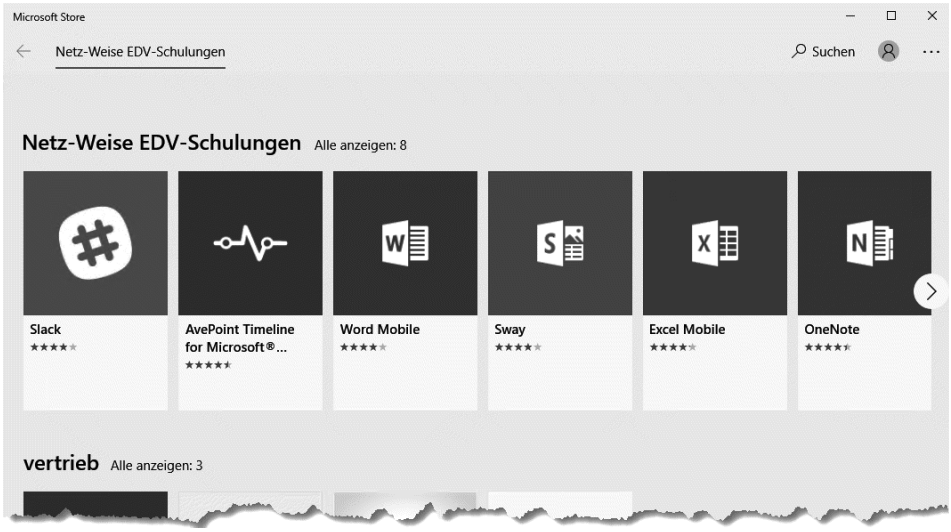


Bild 12.14 Der Microsoft Store for Business

Eine weitere Möglichkeit, den Store zu sperren, ist AppLocker. AppLocker wird aber ebenfalls nur von Windows 10 Enterprise unterstützt. Mehr über AppLocker und das Sperren von Apps erfahren Sie in Abschnitt 7.8.8.

12.4 Oberfläche anpassen

Microsoft hat nach dem Desaster mit Windows 8(.1) einige Anpassungen an der Benutzeroberfläche vorgenommen. Unter anderem wurde ein neues Startmenü programmiert. Es handelt sich hier um eine Neuentwicklung, die komplett anders funktioniert als das Startmenü von Windows 7. Außerdem hat Microsoft das Ändern von Programmverknüpfungen auf dem Client aus Sicherheitsgründen deutlich erschwert. Dadurch ist es nicht mehr möglich, mit den Gruppenrichtlinieneinstellungen die Standardverknüpfung anzupassen. Es gibt aber auch die Möglichkeit, sie mit Richtlinien zu konfigurieren.

12.4.1 Startmenü und Taskleiste

Bereits beim ersten Öffnen des Windows 10-Startmenüs merkt man, dass es mit dem Windows 7-Startmenü nur noch wenig gemein hat. Tatsächlich hat Windows 10 sogar zwei Startmenüs, nämlich ein administratives und ein Benutzer-Startmenü. Das administrative Startmenü (im Englischen Power User Menu) können Sie mit der Tastenkombination Windows-Taste+X öffnen oder alternativ über das Kontextmenü des Start-Buttons. Es enthält alle wichtigen Administrationswerkzeuge und lässt sich rudimentär über die Taskleisteneinstellungen (und damit über administrative Vorlagen) anpassen.

Das eigentliche Startmenü besteht aus zwei Komponenten – der Auflistung der installierten Programme (bei Windows 7 der Eintrag „Alle Programme") und dem Startbildschirm. Der Startbildschirm entspricht der Darstellung von Windows 8 und besteht aus Kacheln, die in Gruppen zusammengefasst sind. Im Prinzip ist er ein Schnellstartmenü, in dem der Benutzer beliebig eigene Verknüpfungen anlegen kann. Er wird automatisch im Vollbildmodus aktiv, wenn Sie ein Tablet benutzen oder ein Hybridgerät mit abgedockter Tastatur – dieses Feature bezeichnet Microsoft als Continuum. Eine Besonderheit hat der Startbildschirm – ist er in den Vollbildmodus geschaltet, haben Sie keinen Zugriff auf den Desktop. Die installierten Programme werden dann wie bei Windows 8.1 über den Eintrag „Alle Apps" im Startbildschirm aufgerufen.

Bild 12.15 Im Vollbildmodus sieht man nur noch Kacheln.

Was Sie in der Abbildung sehr schön sehen können, ist eine ganze Reihe von Anwendungen, die weder Bestandteil von Windows sind – es handelt sich um Fremdhersteller-Apps – noch von Windows mitgeliefert werden. Sie werden bei der ersten Anmeldung des Benutzers direkt aus dem Store heruntergeladen und installiert. Im Startmenü sind sie als Download-Links hinterlegt. Solange der Client keine Internetanbindung hat, werden hier nur blaue Kacheln mit weißen Pfeilen angezeigt.

Bild 12.16
Lernen Sie bald eine großartige App kennen …

Es geht sogar noch weiter. Windows blendet Werbung für andere Apps in das Startmenü ein, die mit einem einfachen Klick installiert werden. Das kann auch ein normaler Benutzer, denn zur Installation von Apps sind keine Admin-Rechte notwendig.

Bild 12.17
Falls man bei der Arbeit Langeweile bekommt, schlägt Microsoft Netflix als App vor.

Um sowohl vorgeschlagene Apps als auch das Herunterladen von Apps bei der ersten Anmeldung zu unterbinden, stellt Microsoft in der Computerkonfiguration unter **Administrative Vorlagen – Windows-Komponenten – Cloudinhalt** eine Gruppenrichtlinie mit dem Namen „Microsoft-Anwenderfeatures deaktivieren" zur Verfügung. Sie unterbindet außerdem das Einblenden von Werbung auf dem Sperrbildschirm von Windows. Leider gehört diese wichtige Richtlinie zu denen, die unter Windows 10 Professional nicht unterstützt werden. Stattdessen können Sie hier auf die Gruppenrichtlinie „Keine Verbindungen mit Windows Update-Internetadressen herstellen" zurückgreifen, die Sie in der Computerkonfiguration unter **Administrative Vorlagen – Windows-Komponenten – Windows Update** finden. Die Richtlinie verhindert den Download von Apps. Faktisch deaktivieren Sie über diese Einstellung den Windows Store. Leider werden im Startmenü auch weiterhin die Store-Apps angezeigt, sogar mit den korrekten Piktogrammen. Wenn der Benutzer versucht, die App zu starten, schlägt der Download aus dem Store allerdings fehl. Außerdem funktioniert diese Einstellung nur, wenn Sie auch einen internen WSUS-Server konfiguriert haben.

Mit der Enterprise- und Education-Edition von Windows 10 haben Sie die Möglichkeit, den Startbildschirm (also das Kachelmenü) und die Taskleiste per Gruppenrichtlinie anzupassen. Auch dieses Feature ist in der Pro Edition leider nicht enthalten.

Um ein benutzerspezifisches Startmenü zu verteilen, benötigen Sie zuerst einen sauberen Client, auf dem alle Programme und Apps installiert sind, die Sie verteilen wollen. Konfigurieren Sie auf diesem Client nun den Startbildschirm entsprechend den Standardeinstellungen, die Sie verteilen möchten. Eine wichtige Rolle hierbei spielen die Gruppen, mit denen Sie die Anwendungskacheln zusammenfassen können, da die Konfiguration die Gruppen einzeln exportiert und die Gruppen im Menü des Zielclients wieder erstellt. Enthält eine Gruppe auf dem Zielclient keine Links, wird die Gruppe nicht erstellt. Auf diese Art und Weise können Sie mit einem Startbildschirm unterschiedliche Clientkonfigurationen abbilden.

Um Kacheln zu entfernen, wählen Sie aus dem Kontextmenü der Kachel „Von Start lösen" aus. Wenn Sie eine neue Gruppe erstellen wollen, können Sie eine Kachel einfach in einen leeren Bereich des Startbildschirms verschieben. Gibt es keinen leeren Bereich, ziehen Sie den Startbildschirm am rechten Rand größer. Sie können auch die Größe der Kacheln anpassen, indem Sie aus dem Kontextmenü der Kachel **Grösse anpassen** auswählen. Anwendun-

gen und Apps, die Sie nicht im Startbildschirm finden, können Sie aus dem Startmenü über das Kontextmenü hinzufügen. Es ist möglich, Container von Kacheln zu erstellen, indem Sie eine Kachel über eine andere Kachel ziehen und dann fallen lassen.

Nachdem Sie Ihren Client konfiguriert haben, können Sie das Startmenü per PowerShell exportieren. Öffnen Sie hierfür eine PowerShell-Konsole und starten Sie das folgende Cmdlet.

Listing 12.2 Exportieren des Windows 10-Startbildschirms

```
Export-Startlayout -Path <Pfad zu Ihrer Layoutdatei>\Startlayout.xml
```

Windows generiert nun anhand Ihres konfigurierten Clients eine Konfigurationsdatei. Um sie zentral verteilen zu können, legen Sie sie in einer Freigabe ab, am besten in einem replizierten DFS-Laufwerk. Anschließend können Sie den Pfad zur Startlayout.xml in der Gruppenrichtlinie **Computerkonfiguration – Richtlinien – Administrative Vorlagen – Startmenü und Taskleiste – Startlayout** hinterlegen. Wenn Sie die Einstellung nicht pro Computer, sondern pro Benutzer anwenden möchten, verwenden Sie den gleichen Eintrag in der Benutzerkonfiguration.

Die Startlayout.xml wird bei jeder Anmeldung angewendet, zum Aktualisieren ist also immer eine neue Anmeldung notwendig.

Nach dem Anwenden der Startlayout.xml fallen zwei Dinge auf – das Startmenü ist für den Benutzer jetzt gesperrt und kann nicht mehr angepasst werden. Außerdem fehlen eventuell Programme, die auf dem Client installiert sind und vorher im Startmenü verfügbar waren. In meinem Beispiel ist das der Regedit, den ich dem Startmenü vor dem Export hinzugefügt hatte – s. Bild 12.18.

Bild 12.18 Das Startmenü ist für den Benutzer nicht mehr individualisierbar.

Wenn man sich die Startlayout.xml genauer ansieht, wird schnell klar, was beim Regedit schiefgelaufen ist.

Listing 12.3 Ein Ausschnitt aus der Startlayout.xml

```
DesktopApplicationLinkPath="%APPDATA%\Microsoft\Windows\Start
Menu\Programs\regedit.lnk"
```

In der Startlayout.xml sind die Einträge zu den Programmen genauso hinterlegt, wie sie im Startmenü hinterlegt worden sind. Der Link zum Regedit verwendet die Umgebungsvariable `%APPDATA%`, die in das Benutzerprofil in den Ordner `Appdata\Roaming` verweist. Da die Verknüpfung nur für den Benutzer existierte, der ihn erstellt hat, geht der Link ins Leere und das Programm wird nicht angezeigt. Achten Sie also darauf, dass Sie Links aus Benutzerprofilen in der Startlayout.xml anpassen.

Das Startmenü kann ab Windows 10 1607 trotz Startlayout.xml wieder angepasst werden, indem Sie dem Tag `<Defaultlayoutoverride>` das Attribut `LayoutCustomizationRestrictionType="OnlySpecifiedGroups"` hinzufügen, wie in Listing 12.4 zu sehen. Mit diesem Attribut werden die vorgegebenen Gruppen gesperrt, aber der Benutzer kann neue Gruppen erstellen und anpassen.

Listing 12.4 Mit diesem Attribut ist das Startlayout wieder anpassbar.

```
<DefaultLayoutOverride LayoutCustomizationRestrictionType="OnlySpecifiedGroups">
```

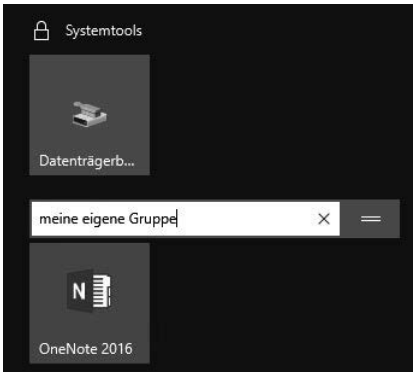


Bild 12.19
Das Schloss zeigt vom Administrator erstellte Gruppen, aber es können jetzt neue Gruppen angelegt werden.

Über die Startlayout.xml können Sie auch die Taskleiste anpassen. Eine vollständige Beschreibung aller Einstellungen finden Sie bei Microsoft unter *https://docs.microsoft.com/en-us/windows/configuration/windows-10-start-layout-options-and-policies* oder kurz *https://bit.ly/2viKILa*.

Neben der Möglichkeit, eine Layout-Datei für das Startmenü zu hinterlegen, gibt es vor allem in den administrativen Vorlagen der Benutzerkonfiguration unter **Startmenü und Taskleiste** noch eine Reihe von weiteren Anpassungsmöglichkeiten. Achten Sie darauf, dass Sie sehr genau zwischen den einzelnen Windows-Versionen unterscheiden müssen, da Microsoft hier faktisch Einstellungen für mindestens drei verschiedene Startmenüs bzw. Bildschirme hinterlegt hat, nämlich das Startmenü von Windows 7, den Startbildschirm von Windows 8(.1) und das Startmenü von Windows 10, die miteinander jeweils bestenfalls rudimentär kompatibel sind. Hier fasse ich die wichtigsten Einstellungen für Windows 10 zusammen. Wenn eine Einstellung auch in den Computereinstellungen zu konfigurieren ist, steht es in der Beschreibung explizit dabei.

Einstellung	Auswirkungen	FR
Anzeige von Sprechblasenbenachrichtigungen als Popups deaktivieren	Windows zeigt Benachrichtigungen normalerweise als viereckige Popups oberhalb der Benachrichtigungsleiste an. In früheren Windows-Versionen wurden Sprechblasen verwendet. Windows 10 rendert Sprechblasen normalerweise auch als Popups. Wenn ältere Anwendungen Kompatibilitätsprobleme mit der Konvertierung haben, kann Windows mit dieser Einstellung gezwungen werden, Sprechblasen wieder als Sprechblasen auszugeben.	1507
Benachrichtigungs- und Info-Center entfernen	Aktivieren Sie diesen Eintrag, um das Icon für das Benachrichtigungsfenster (die eckige Sprechblase) komplett auszublenden. Sie stellen damit die Taskleistenansicht von Windows 7/8 wieder her.	1507
Kontaktleiste von der Taskleiste entfernen	Deaktiviert die Kontaktleiste rechts neben der Taskleiste, die mit Windows 10 1703 eingeführt wurde. 	Ab 1703
Kontextmenüs im Startmenü deaktivieren	Deaktiviert das Kontextmenü des Startmenüs, ist in den Computer- und Benutzereinstellungen konfigurierbar.	Ab 1803
Liste „Alle Programme“ aus dem Startmenü entfernen	Mit diesem Eintrag können Sie das Startmenü ausblenden oder komplett entfernen. Der Startbildschirm mit den Kacheln bleibt aber weiterhin erhalten. Sie haben drei verschiedene Möglichkeiten: Reduzieren: Die Programme werden „eingeklappt“, können vom Benutzer aber durch Auswählen des Menüeintrags links wieder geöffnet werden. Reduzieren und Einstellungen deaktivieren: Die Programme werden „eingeklappt“, der Menüeintrag zum Öffnen ist aber deaktiviert. Das Menü lässt sich nicht wieder öffnen. Entfernen und Einstellung deaktivieren: Die Programme werden eingeklappt und der Menüeintrag zum Öffnen wird entfernt. Letztlich ist die Wirkung identisch wie „Reduzieren und Einstellungen deaktivieren“.	Ab 1507
Liste häufig verwendeter Programme aus dem Startmenü entfernen	Der Eintrag „Meistverwendet“ steht in Windows 10 oben im Startmenü direkt unter den zuletzt hinzugefügten Programmen.	Ab 1507
Menüeintrag „Ausführen“ aus dem Startmenü entfernen	Der Menüeintrag „Ausführen“ ist im administrativen Startmenü nach Aktivieren dieser Einstellung zwar weiterhin vorhanden, aber beim Aufrufen des Eintrags wird nur eine Meldung ausgegeben: „Der Vorgang wurde aufgrund von aktuellen Beschränkungen auf dem Computer abgebrochen. Bitte wenden Sie sich an Ihren Administrator“. Achtung, diese Einstellung hat eventuell eine unbeabsichtigte Nebenwirkung – der Zugriff auf UNC-Pfade aus der Explorer-Adressleiste wird mit der Fehlermeldung „Der Zugriff auf die Ressource <\\Freigabepfad> wurde gesperrt“ quittiert.	Ab 1507

(Fortsetzung nächste Seite)

Einstellung	Auswirkungen	FR
Volle Bildschirm- oder Menügröße für „Start“ erzwingen	Deaktiviert Continuum. Mit dieser Einstellung erzwingen Sie die Hybriddarstellung zwischen Startmenü und Startbildschirm oder die Vollbilddarstellung des Startbildschirms. Im Gegensatz zum Tabletmodus, den Sie im Benachrichtigungscenter aktivieren, können Sie durch Drücken des Startbuttons auf den Desktop wechseln, wenn Sie den Startbildschirm im Vollbildmodus erzwingen.	Ab 1507

12.4.2 Programmverknüpfungen anpassen

Programmverknüpfungen gehören in die Kategorie der Funktionen, von denen man eigentlich nicht erwartet, dass darüber ein eigener Abschnitt geschrieben werden muss. Leider ist das aber der Fall, denn mit Windows 10 hat Microsoft einige Änderungen vorgenommen, die aus sicherheitstechnischer Sicht sehr sinnvoll, aus Anwender- und Administratorensicht aber sehr nervig sind.

Ab Windows 10 werden Programmverknüpfungen pro Benutzer und nicht mehr pro Computer konfiguriert. Die Zuordnung von Dateiendung zu Programm kann auch nicht mehr von einer Anwendung direkt vorgenommen werden, sodass jede Verknüpfung einer Dateiendung mit einem neuen Programm vom Benutzer von Hand bestätigt werden muss. Windows fragt dann beim ersten Aufruf einer Datei, die mit dem neuen Programm geöffnet werden kann, mit welcher Anwendung diese Dateiendung in Zukunft geöffnet werden soll.

Bild 12.20
Nach der Installation einer neuen Software wird beim ersten Öffnen einer registrierten Dateiendung das Standardprogramm erfragt.

Versucht das Programm trotzdem, seine Dateiendungen auf herkömmliche Art und Weise zu registrieren, weist ein Popup darauf hin, dass die Verknüpfung wieder auf den Standardwert zurückgesetzt wurde.

Bild 12.21
IrfanView hat versucht, Dateiendungen automatisch zu registrieren.

Um Verknüpfungen nachträglich zu ändern, kann man die Dateiverknüpfungen in den Windows-Systemeinstellungen im Menü **Apps – Standardapps** anpassen, indem man einen der Einträge **Standard-Apps nach Dateityp auswählen** oder **Standard-Apps nach Protokoll auswählen** startet. Das ist allerdings sehr mühsam, da jede Verknüpfung einzeln ausgewählt werden muss und das Menü auch nicht besonders bedienerfreundlich ist. Für einen Endbenutzer ist das in den meisten Fällen außerdem schlicht zu kompliziert.

Man kann die Dateiverknüpfungen natürlich auch zentral per Gruppenrichtlinien vorgeben, wenn auch nicht mehr so einfach wie noch unter Windows 7 mithilfe von Gruppenrichtlinieneinstellungen. Stattdessen muss man alle zu konfigurierenden Dateiverknüpfungen zuerst auf einem Test-Client anpassen. Installieren Sie hierfür alle Anwendungen, die bei Ihnen zum Einsatz kommen und verknüpft werden sollen. Anschließend öffnen Sie alle Dateiendungen, die Sie neu verknüpfen möchten. Wenn Sie bereits bestehende Verknüpfungen ändern wollen, ist es am einfachsten, Sie öffnen das Kontextmenü einer zu verknüpfenden Datei und wählen „Öffnen mit“ aus. Ist der Eintrag im Kontextmenü nicht sichtbar, hilft das gleichzeitige Gedrückthalten einer der Shift-Tasten. Wählen Sie unter **Öffnen mit** den Eintrag **Andere App aussuchen** und wählen Sie den Eintrag „Immer diese App zum Öffnen von .<Endung>-Dateien verwenden“ aus.

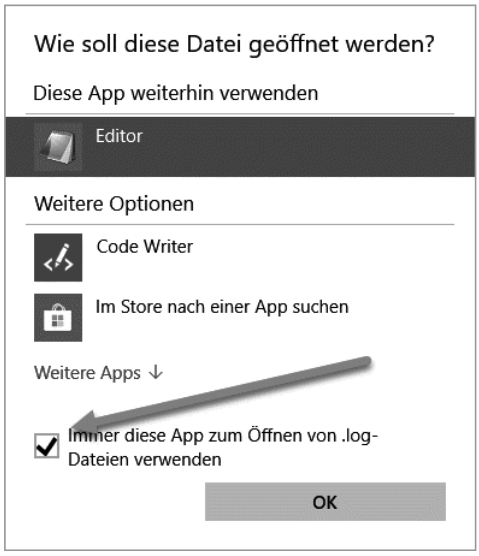


Bild 12.22
Dateiverknüpfungen können im Kontextmenü neu gesetzt werden.

Um Verknüpfungen von z. B. Mailprogrammen zu ändern, müssen Sie über die Standard-Apps in den Windows-Einstellungen gehen und dann „Standard-Apps nach Protokoll auswählen“ starten. Für das Mailprogramm suchen Sie hierzu in der linken Spalte „MAILTO“ aus, in der rechten Spalte dann das neue Programm.

Anschließend können Sie die Dateiverknüpfungen mit der `dism.exe` exportieren. Leider gibt es derzeit kein PowerShell-Cmdlet, das die gleiche Funktionalität bereitstellt. Wenn Sie die Dateiverknüpfungen auf einem zweiten Testclient noch einmal prüfen wollen, können Sie die Datei mit `dism` auch wieder importieren – s. Listing 12.5.

Listing 12.5 Exportieren und Importieren der Standard-Dateiverknüpfungen

```
# Exportieren der Dateiverknüpfungen
dism.exe /online /export-defaultappassociations:\\<Ihr FileShare>\fileassoc.xml

# Und auf einem zweiten Client wieder importieren
dism.exe /online /import-defaultappassociations:\\<Ihr FileShare>\fileassoc.xml
```

Die Datei mit den Verknüpfungsinformationen können Sie jetzt über eine Gruppenrichtlinie zentral bereitstellen. Sie finden die Richtlinie in der Computerkonfiguration unter **Administrative Vorlagen – Windows-Komponenten – Datei-Explorer**. Achten Sie darauf, dass diese Einstellung nur dann gültig wird, wenn der Computer Mitglied einer Domäne ist.

12.5 Der alte Edge-Browser

Der Edge-Browser ist seit dem ersten Release 1507 Bestandteil von Windows 10 und wird den Internet Explorer früher oder später beerben. Der IE wird nicht weiterentwickelt, obwohl er nach wie vor Bestandteil von Windows 10 ist. Der Edge ist aber schon jetzt der Windows-Standard-Browser.

Edge bekommt mit jedem neuen Feature Release neue Funktionen und nähert sich langsam, aber sicher Chrome und Firefox an. Das vielleicht wichtigste Feature von Edge ist, dass er standardkonform ist, also alle wichtigen Internet-Standards unterstützt und Microsoft auch nicht versucht, durch eigene Erweiterungen wie Active-X Scripting Mitbewerber auszubooten. Das dürfte bei der aktuellen Marktlage auch schwierig werden, denn Edge ist, wenn man sich die aktuellen Nutzungsstatistiken anschaut, sogar noch hinter dem Internet Explorer 11 mit ca. 5 % Marktanteil weit abgeschlagen.

Trotzdem kann Edge für Unternehmen durchaus interessant sein. Sein eckiges Design wirkt ein wenig altbacken, aber grundsätzlich ist der Edge ein solider Browser, der alle modernen Webseiten ohne Probleme anzeigen kann. Er unterstützt inzwischen Erweiterungen (Plug-ins), auch wenn aktuell nur knapp 100 Stück verfügbar sind, und die Synchronisierung mit Mobiltelefonen. Und ja, es gibt inzwischen sogar eine Edge-Version für Android und iOS. Microsoft meint es also wirklich ernst. Vor allem kann man ihn aber mit Gruppenrichtlinien konfigurieren, wenn auch nicht ansatzweise so umfangreich wie den Internet-Explorer, und mit Windows Defender Application Guard hat der Edge jetzt auch ein Allein-

stellungsmerkmal, das kein anderer Browser in dieser Form liefern kann. Man muss als Unternehmen also nicht unbedingt noch einen weiteren Browser unterstützen.

Eine ständig aktualisierte Liste der vorhandenen und geplanten Funktionen des Edge finden Sie unter *https://developer.microsoft.com/en-us/microsoft-edge/platform/status/* oder kurz *https://bit.ly/1V3ojLC*.

Die Gruppenrichtlinien zum Edge finden Sie sowohl in der Computer- als auch in der Benutzerkonfiguration unter **Administrative Vorlagen – Windows-Komponenten – Microsoft Edge**. Die Windows-Komponente Edge-UI, im deutschen Rand-UI, hat mit dem Edge-Browser nichts zu tun, sondern beschreibt die Funktion, mit der man unter Windows 8(.1) Menüs vom Rand des Bildschirms mit einer Wischbewegung öffnen kann.

Die Menge der Gruppenrichtlinien ist im Vergleich zum Internet Explorer überschaubar. In der Version 1809 werden aber wieder einige neue Richtlinien dazukommen. Die meiner Meinung nach wichtigsten Richtlinien beschreibe ich hier.

Einstellung	Auswirkungen	Ab FR
Adobe Flash zulassen	Adobe Flash ist in Edge integriert und wird von Microsoft regelmäßig aktualisiert. Flash wird hoffentlich sehr bald gar nicht mehr notwendig sein, da kaum noch eine moderne Website es verwendet. Nach aktuellen Statistiken sind es inzwischen weniger als 5%. Das ist auch kein Wunder, da Adobe angekündigt hat, ab Ende 2020 Flash endgültig nicht mehr zu supporten. Das Deaktivieren dieser Einstellung blockiert Flash im Edge. Das macht aus sicherheitstechnischer Sicht durchaus Sinn, da Flash nach wie vor sehr oft wegen Sicherheitsproblemen aktualisiert werden muss.	1507
Alle Intranetseiten an Internet Explorer 11 senden	Öffnet alle internen Websites im IE. Das kann sinnvoll 1sein, wenn Sie noch viele alte webbasierte Anwendungen haben, die auf Features wie Active Scripting setzen oder sonst Probleme mit Edge machen. Aktuelle Applikationen dürften mit dem Edge keine Probleme haben.	1703
Anpassung der Suchmaschine zulassen	Deaktivieren Sie diese Einstellung, um den Benutzern eine feste Suchmaschine vorzugeben. Die Einstellung funktioniert nur bei Computern, die Mitglied einer Domäne sind.	1709
Cookies konfigurieren	Mit dieser Einstellung legen Sie fest, wie der Edge mit Cookies umgehen soll. Aktivieren Sie diese Einstellung, und wählen Sie in der Drop-down-List aus zwischen „Alle Cookies blockieren“, „Nur Cookies von Drittanbietern blockieren“ und „Alle Cookies zulassen (Standard)“.	1703
DNT konfigurieren	DNT steht für Do Not Track und ist ein Feature, das Websites das Nachverfolgen von Benutzern mit Cookies erlaubt. Diese Einstellung ist im Edge standardmäßig deaktiviert, was bedeutet, dass Websites ihre Besucher über Websites hinweg z. B. für Werbezwecke tracken können. Dieses Feature sollte aus Gründen der Privatsphäre eingeschaltet sein, aber die Werbeindustrie hat erfolgreich Druck auf die Browserhersteller ausgeübt – soweit diese nicht eh schon von Werbung leben. Aktivieren Sie dieses Feature, um DNT zu aktivieren.	1507

(Fortsetzung nächste Seite)

Einstellung	Auswirkungen	Ab FR
Enterprise Mode Site List	Hier können Sie den Pfad zur einer Enterprise Mode Site List hinterlegen. Die Enterprise Site Mode List ist eigentlich ein IE-Feature, das den IE 11 anweist, bestimmte Websites im IE 8-Kompatibilitätsmodus zu starten. Wenn Windows die Liste kennt, werden Seiten mit dem IE anstatt mit Edge geöffnet. Zum Erstellen der Enterprise Site Mode List stellt Microsoft den Enterprise Site Mode List Manager zur Verfügung. Mehr Informationen zum Thema und den Link zum Download des Managers finden Sie unter *https://docs.microsoft.com/en-us/internet-explorer/ie11-deploy-guide/use-the-enterprise-mode-site-list-manager* oder kurz *https://bit.ly/2KpVKFk*.	1703
Erweiterungen zulassen	Deaktivieren Sie diese Einstellung, um Ihren Benutzern das Installieren von Edge-Plug-ins zu verbieten.	1607
Kennwort-Manager konfigurieren	Wenn Sie diese Einstellung deaktivieren, können Benutzer ihre Kennwörter nicht vom Browser speichern und automatisch ausfüllen lassen. Diese Einstellung ist insofern problematisch, als jeder, der sich Zugriff auf den Arbeitsplatz des Benutzers verschaffen kann, auch gleich noch Zugriff auf alle gespeicherten Kennwörter externer Websites bekommt.	1703
Klick-und-Los-Einstellung für Adobe Flash konfigurieren	Mal wieder eine interessante Namensverwirrung. Klick-und-Los hat in diesem Fall nichts mit der neuen Installationsvariante von Microsoft Office zu tun, sondern blockt das automatische Abspielen von Flash-Inhalten. Der Benutzer muss zuerst den Klick-und-Los-Button drücken, um Flash-Inhalte zu starten. Deaktivieren Sie diese Einstellung, um Flash-Inhalte automatisch starten zu lassen.	1703
Löschen von Browserdaten beim Beenden zulassen	Eine unglücklich ausgedrückte Einstellung, denn Sie lässt das Löschen von Browserdaten nicht zu, sondern aktiviert das automatische Löschen beim Beenden.	1703
Microsoft-Kompatibilitätsliste zulassen	Der Edge-Browser verwendet eine Kompatibilitätsliste, um ältere Websites, die nicht konform mit dem HTML-Standard arbeiten, korrekt darzustellen. Die Kompatibilitätsliste wird von Microsoft regelmäßig aktualisiert und vom Edge im Hintergrund heruntergeladen. Mit dieser Einstellung können Sie die Kompatibilitätsliste deaktivieren. Wenn Sie die Kompatibilitätsliste anzeigen lassen wollen, geben Sie in der Adressleiste des Edge `about:Compat` ein.	1507
Standardsuchmaschine festlegen	Zum Festlegen der Standardsuchmaschine reicht es nicht, einfach eine Suchmaschine einzutragen. Stattdessen benötigen Sie ein Search Description File, eine Konfigurationsdatei im XML-Format, die per HTTP geladen wird. Für Google verwenden Sie *https://www.google.com/searchdomaincheck?format=opensearch*, für DuckDuckGo *https://duckduckgo.com/opensearch.xml*. Sie können die Files auch herunterladen und auf einem internen Webserver zur Verfügung stellen oder ein eigenes File erstellen. Eine Beschreibung finden Sie unter *https://docs.microsoft.com/de-de/microsoft-edge/dev-guide/browser-features/search-provider-discovery* oder kurz *https://bit.ly/2O86FWk*.	1709

Einstellung	Auswirkungen	Ab FR
Startseiten konfigurieren	Legen Sie hier die Startseite fest, um zu verhindern, dass der Edge standardmäßig eine Reihe von Newsfeeds aus der Regenbogenpresse öffnet. Ab Feature Release 1803 versteht Edge auch `about:blank`, eine Konfiguration, die eine leere Website öffnet. Diese Einstellung konfiguriert nur den ersten Tab, wenn Sie auch für neue Tabs die Newsfeeds deaktivieren wollen, verwenden Sie die Richtlinie „Webinhalte auf der Seite „Neuer Tab“ zulassen“.	1703
Verhindern, dass Microsoft Edge beim Starten von Windows und bei jedem Schließen von Microsoft Edge die Seite „Neue Registerkarte“ startet und lädt.	Windows lädt Edge beim Anmelden des Benutzers automatisch in den Hintergrund. Außerdem werden die Startseite und zusätzliche Tabs, die beim Starten geöffnet werden sollen, vorgeladen. Wenn der Edge geschlossen wird, wird im Hintergrund automatisch wieder ein neuer Edge-Prozess gestartet. Wenn Sie dieses Verhalten verhindern wollen, aktivieren Sie die Richtlinie und wählen Sie im Drop-down Menü **Vorabladen von Registerkarten verhindern** aus. Wenn Sie den Edge nicht nutzen, sollten Sie dieses Verhalten auf jeden Fall deaktivieren. Kleine Nebenbemerkung – die Funktion des Deaktivieren-Knopfs scheint den Programmierern der Edge-Richtlinien irgendwie nicht aufgegangen zu sein.	1803
Vorschläge in der Drop-down-Liste der Adressleiste anzeigen	Wenn Sie Suchbegriffe in die Adressleiste eingeben, werden automatisch Daten zur Suchmaschine übermittelt, um Suchvorschläge als Drop-down-Listen anzuzeigen. Wenn Sie die Datenübermittlung im Hintergrund verhindern wollen, deaktivieren Sie diese Funktion.	1507
Webinhalte auf der Seite „Neuer Tab“ zulassen	Edge zeigt standardmäßig beim Öffnen ein Suchfenster und eine Reihe von ziemlich sinnlosen Newsfeeds aus der Regenbogenpresse an. Deaktivieren Sie diese Einstellung, wird beim Öffnen von neuen Tabs nur eine weiße Seite angezeigt.	1507
Zugriff auf die Seite „about:flags“ in Microsoft Edge verhindern	Geben Sie als URL about:flags ein, werden im Edge erweiterte Entwicklerfeatures zur Konfiguration angeboten. Deaktivieren Sie diese Einstellung für normale Benutzer am besten.	1703

Neu in Feature Release 1809, basierend auf der Insider Preview:

Einstellung	Auswirkungen	FR
Außerkraftsetzungen von Zertifikatsfehlern verhindern	Aktivieren Sie diese Richtlinie, um zu verhindern, dass Benutzer die Warnung vor fehlerhaften SSL-Zertifikaten deaktivieren können.	Ab 1809
Deaktivieren erforderlicher Erweiterungen verhindern	Definieren Sie Edge-Erweiterungen (Plug-ins), die der Benutzer nicht deaktivieren darf.	Ab 1809
Drucken zulassen	Deaktivieren Sie diese Einstellung, um das Drucken aus dem Edge zu verhindern.	Ab 1809

(Fortsetzung nächste Seite)

Einstellung	Auswirkungen	FR
Kioskmodus konfigurieren	Sie können Windows 10 in den sogenannten Kioskmodus schalten, der dem Benutzer nur das Starten einer einzelnen Applikation erlaubt. Der Kioskmodus ist von mir ausführlich in den Netz-Weise-Newslettern von Februar und April 2018 besprochen worden, die Sie unter *https://www.netz-weise-it.training/weisheiten/newsletter2.html* herunterladen können. Mit dieser Einstellung können Sie konfigurieren, wie Edge sich verhält, wenn er im Kioskmodus gestartet wird. Die Optionen sind in der Richtlinie ausführlich beschrieben.	Ab 1809
Konfigurieren des Kiosk-Reset nach LeerlaufTimeout	Der Leerlauftimeout-Zähler startet nach der letzten Benutzerinteraktion. Ist der Timeout erreicht, gibt Edge für 30 Sekunden eine Bestätigungsmeldung aus. Danach wird Edge auf die Standardwerte zurückgesetzt. Diese Einstellung wird nur aktiv, wenn der Computer sich im Kioskmodus mit zugewiesenem Zugriff (Assigned Access) befindet.	Ab 1809
Konfigurieren von „Microsoft Edge öffnen mit“	Hierüber können Sie vorgeben, mit welcher Startseite Edge gestartet wird. Mögliche Einstellungen sind: Bestimmte Seiten (Standard): Startet die Seite, die unter „Startseiten konfigurieren“ angegeben ist. Startseite: Verwendet die Edge-Startseite. Die Edge-Startseite öffnet standardmäßig eine Reihe ziemlich sinnloser Newsfeeds und eine Sucheingabe. Seite „Neue Registerkarte“: Öffnet den Edge mit den Einstellungen für neue Registerkarten. Was auf einer neuen Registerkarte angezeigt wird, können Sie über „Webinhalte auf der Seite ‚Neuer Tab‘ zulassen“ und „URL für Seite ‚Neue Registerkarte‘ festlegen“ konfigurieren. Bestimmte Seiten(n): Speichert beim Schließen des Browsers die URLs der aktuellen Tabs und öffnet sie beim nächsten Mal wieder. Das ist meine bevorzugte Einstellung.	Ab 1809
URL für Seite „Neue Registerkarte“ zulassen	Hier können Sie die URL angeben, mit der alle neuen Tabs geöffnet werden.	Ab 1809
Querladen der Erweiterung zulassen	Erlaubt das Sideloading von Edge-Erweiterungen. Diese Einstellung verhindert nur das Sideloading im Edge, per `Add-Appxpackage` können nach wie vor Apps installiert werden.	Ab 1809
Speichern des Verlaufs zulassen	Stellen Sie diese Richtlinie auf „Deaktiviert“, damit Edge den Browserverlauf nicht speichert.	Ab 1809

12.6 Der neue Edge-Browser

Microsoft hat die Entwicklung des alten Edge-Browsers aufgegeben, da die Akzeptanz bei den Benutzern eher niedrig war. Stattdessen gibt es seit FR 2004 offiziell den neuen Edge-Browser, der ab 20H2 Bestandteil des FR ist. Der neue Edge-Browser basiert auf Chromium, der Open-Source Browser-Engine, die auch Googles Chrome-Browser zugrunde liegt, was unter anderem den Vorteil hat, dass der neue Edge praktisch alle Plug-ins des Chrome Plug-in Store verwenden kann. Außerdem unterstützt Edge Application Guard (s. nächster Abschnitt 12.7 – Virtualisierungsbasierte Sicherheit), Sammlungen und Single Sign für Azure AD hinzugefügte Geräte sowie eine ganze Reihe von weiteren Funktionen. Tatsächlich hat der neue Edge in sechs Monaten bereits die Nutzerzahlen des alten Edge überholt, was auch daran liegen mag, dass Microsoft ihn auch für Android, Apple-Geräte und Linux zur Verfügung stellt.

Wenn Sie nicht Windows 10 FR 20H2 oder neuer im Einsatz haben, können Sie den Edge bei Microsoft unter *https://www.microsoft.com/de-de/edge/business/download* oder kurz *https://bit.ly/3mG2Nxt* herunterladen. Verwenden Sie Edge für Unternehmen, den Sie als komplettes MSI-Paket bekommen. Auf der Webseite können Sie auch die ADMX-Dateien sowie Konfigurations-Dateien für MacOS herunterladen, indem Sie **Richtlinien abrufen** auswählen. Der Download-Link ist erst aktiv, wenn Sie einen Kanal, einen Build und die Plattform ausgewählt haben.

Bild 12.23 Wählen Sie zuerst eine Version aus, auch wenn Sie nur die Richtlinien benötigen

Der Download besteht aus der Datei *MicrosoftEdgePolicyTemplates.cab*. Das Cabinett-Format ist ein Archiv und kann im Explorer direkt durch Doppelklick geöffnet werden. Hier finden Sie ein weiteres Archiv, diese Mal im Zip-Format. Das können Sie direkt durch Rechtsklick entpacken lassen. Ich war ein wenig überrascht, dass jetzt nicht noch eine msi-Datei zum Vorschein kam, sondern man im Unterordner **Windows** direkt die Administrativen Vorlagen als .adm- und .amdx-Dateien findet. Kopieren Sie den Inhalt jetzt einfach direkt in Ihren PolicyDefinitions-Ordner und erstellen Sie eine neue Gruppenrichtlinie, um den Edge zu konfigurieren.

Der neue Edge unterstützt zwei Typen von Einstellungen – obligatorische und empfohlene oder Standard-Richtlinien. Obligatorische Richtlinien entsprechen klassischen Richtlinien und können vom Benutzer nicht verändert werden. Empfohlene Richtlinien sind Einstellungen, die der Benutzer überschreiben kann. Außerdem bringt der Edge noch Richtlinien zum Steuern der Bereitstellung mit, da Edge genau wie Windows agil entwickelt wird und die Möglichkeit bietet, neben der stabilen Version noch Beta-, Dev- und Canary-Versionen zu verwenden. Canary ist wohl von Kanarienvogel abgeleitet, weil man hier tägliche Updates

bekommt und quasi dem Kanarienvogel der Bergarbeiter enstspricht, der tot umfällt, wenn der CO_2-Gehalt in der Luft zu hoch wird. Ich bin mir nicht sicher, ob das irgendjemand wirklich testen will …

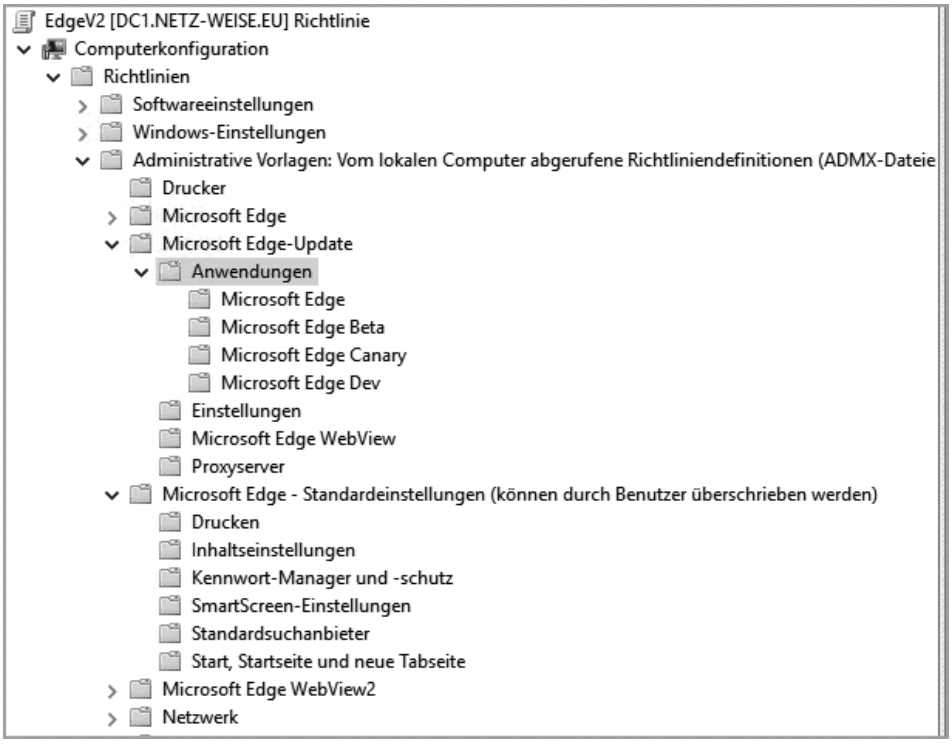


Bild 12.24 Edge WebView ist ein Entwicklerfeature und kann ignoriert werden

Die Einstellungen von Windows Edge Webview2 können Sie ignorieren, es handelt sich um ein Entwicklerfeature. Sie können die msedgewebview2.admx-Datei beim Kopieren in den PolicyDefinition-Ordner auch einfach auslassen.

Im Folgenden werde ich kurz beispielhaft auf einige der Policies eingehen, aber die Gesamtliste aller möglichen Einstellungen ist bei Weitem zu lang und ändert sich vermutlich auch zu häufig. Sie finden die vollständige Dokumentation in englischer Sprache unter *https://docs.microsoft.com/en-us/deployedge/microsoft-edge-policies* oder kurz *https://bit.ly/2JxDu2j*. Achten Sie darauf, dass in der tabellarischen Darstellung der Name der Gruppenrichtlinie in der zweiten Spalte *Caption* steht!

12.6.1 Edge-Updates verwalten

Der neue Edge wird unabhängig von Windows entwickelt und bereitgestellt. Der offizielle Plan von Microsoft sieht vor, alle sechs Wochen eine neue Produktiv-Version des Edge zu veröffentlichen. Der Browser aktualisiert sich dabei genau wie Chrome selbstständig, soweit Sie die Installation und Updates nicht durch Gruppenrichtlinien unterbinden. Sie können

für jeden der Veröffentlichungskanäle einzeln festlegen, ob Installation und automatisches Update stattfinden sollen. Edge kennt dabei vier Kanäle:

Kanal	Beschreibung	Aktualisierungs-Intervall	Mit Support
Stable	Als stabil freigegebene Version, fehlerbereinigt	Ca. 6 Wochen	Ja
Beta	Beta-Status für den Test-Ring	Ca. 6 Wochen	Ja
Dev(eloper)	Frühe Beta-Version, ähnlich dem Fast-Ring für Windows	Wöchentlich	Nein
Canary	Für Enthusiasten. Diese Version entspricht in etwa dem nicht bereinigten Code, der von den Entwicklern täglich fertiggestellt wird	Täglich	Nein

Relevant im Unternehmenseinsatz sind vor allem die Beta- und die Stable-Version. Die Beta erscheint alle sechs Wochen und wird dann jeweils in die stabile Version überführt. Während des Lebenszeitraums der Beta wird sie regelmäßig mit Sicherheits- und Qualitätsupdates aktualisiert.

Welche Versionen zum Einsatz kommen sollen, können Sie über die Gruppenrichtlinien der Kategorie **Computerkonfiguration – Administrative Vorlagen – Microsoft Edge-Update** steuern. Die deutsche Übersetzung der einzelnen Richtlinien ist dabei leider selbst für Gruppenrichtlinien manchmal sehr grenzwertig.

Einstellung	Auswirkung
Als Installationsstandard die Erstellung von Desktopverknüpfungen verhindern	Wenn Sie diese Richtlinie aktivieren, wird bei der Installation von Edge keine Desktopverknüpfung angelegt. Sie können die Einstellung für einzelne Kanäle überschreiben
Funktion „Nebeneinander“ für Microsoft Edge-Browser zulassen	Erlaubt, den alten Edge (Edge HTML) und den neuen, Chromium-basierten Edge parallel zu betreiben. Wenn diese Gruppenrichtlinie nicht aktiviert ist, wird der alte Edge bei der Installation des neuen Edge ersetzt.
Standardeinstellungen für die Überschreibung von Update-Richtlinien	Definiert für alle Kanäle, wie Updates ausgerollt werden. ▪ Nur manuelle Updates: Aktualisierung findet nur statt, wenn der Benutzer in den Einstellungen unter *Infos zu Microsoft Edge* eine manuelle Synchronisierung startet. ▪ Nur automatische Updates im Hintergrund: Wenn der automatische Updateprozess Aktualisierungen findet, werden diese ausgeführt. Manuelle Updates sind deaktiviert. ▪ Updates immer zulassen: Aktualisierungen können manuell und automatisch stattfinden. ▪ Updates deaktivieren: Aktualisierungen finden nicht statt. Wenn Sie Updates deaktivieren, sollten Sie einen alternativen Updateprozess verwenden. Die Updateeinstellungen können in jedem Kanal überschrieben werden.
Standardeinstellungen für Installation zulassen	Eine etwas missverständliche Bezeichnung. Wenn Sie diese Richtlinie deaktivieren, wird die Installation von Edge geblockt. Aktivieren Sie die Richtlinie, wird die Installation von allen Kanälen zugelassen. Sie können die Einstellung für alle Kanäle trotzdem in den jeweiligen Unterkategorien überschreiben.

Sie können die Einstellungen in jedem Kanal einzeln anpassen.

Einstellung	Auswirkung
Außerkraftsetzung der Zielversion	Hier können Sie eine feste Versionsnummer von Edge angeben, die installiert werden soll. Eine Liste aller Versionen des Stable Channel finden Sie unter *https://docs.microsoft.com/en-us/deployedge/microsoft-edge-relnote-stable-channel* oder kurz *https://bit.ly/2JEM8f8*. Die Funktion steht nur auf Domänencomputern zur Verfügung.
Bei Installation die Erstellung von Desktopverknüpfungen verhindern	Überschreibt die Einstellungen der allgemeinen Richtlinie.
Installation zulassen	Erlaubt die Installation, unabhängig von der Konfiguration unter *Standardeinstellungen für Installation zulassen*.
Überschreiben der Update-Richtlinie	Überschreibt die Einstellungen der allgemeinen Richtlinie.
Wiederherstellung der Zielversion	Mit dieser Option können Sie Edge dazu zwingen, auch auf ältere Versionen zurückzugehen. Definieren Sie die Zielversion unter „Außerkraftsetzung der Zielversion“ und aktivieren Sie diese Richtlinie. Diese Richtlinie funktioniert nur, wenn Updates zugelassen sind!

In der Kategorie **Einstellungen** können Sie den Prüfzyklus auf Updates überschreiben. Standardmäßig prüft Edge alle zehn Stunden, ob eine Aktualisierung vorliegt.

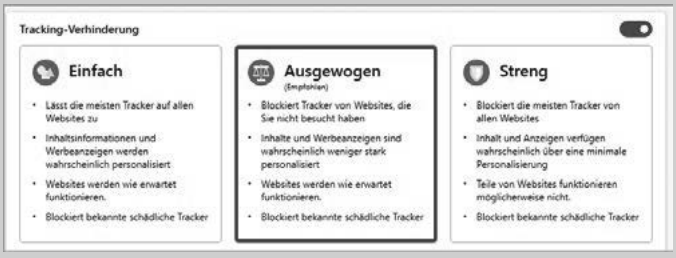
Einstellung	Auswirkung
Überschreiben des Zeitraums der automatischen Updateüberprüfung	Legen Sie das Intervall in Minuten fest, in dem Edge nach Updates suchen soll. Wenn Sie diesen Wert auf 0 setzen, wird die automatische Updateprüfung deaktiviert.
Zeitraum, für den die automatische Update-Überprüfung täglich unterdrückt wird	Hier können Sie eine tägliche Uhrzeit festlegen, ab der Edge für eine vorgegebene Dauer keine Prüfung ausführt. Faktisch legen Sie hier also einen Zeitplan für die Aktualisierung ähnlich der Nutzungszeit fest. Tragen Sie in die Felder „Stunde“ und „Minute“ die Startzeit ein, und in „Dauer“ die Frist, während der keine Prüfung stattfinden soll.

Unter Proxyserver können Sie mit Festlegen der Angabe von Proxyservereinstellungen einen festen Proxyserver angeben, der für die Installation verwendet werden soll. Die Einstellungen sind selbsterklärend, daher beschreibe ich sie hier nicht explizit.

12.6.2 Einstellungen vornehmen

In der Kategorie **Administrative Vorlagen – Microsoft Edge** können Sie Einstellungen erzwingen. In der Kategorie **Administrative Vorlagen – Microsoft Edge – Standardeinstellungen** finden Sie einige (aber deutlich weniger) der Einstellungen ein zweites Mal, allerdings hier als für vom Benutzer änderbare Vorgaben. Beide Kategorien sind sowohl in der Benutzer- als auch in der Computerkonfiguration verfügbar und verfügen über die glei-

chen Einstellungen. Sie können Edge also sowohl global für den Computer als auch für einzelne Benutzer konfigurieren.

Einstellung	Auswirkung
„Eindruck beim ersten Ausführen“ und Begrüßungsbildschirm ausblenden	Beim Erststart von Edge wird ein Mini-Assistent gestartet, der die neuen Funktionen von Edge erklärt. Da die Funktion zwar hübsch, aber ziemlich überflüssig ist, kann man Sie durch Aktivieren dieser Einstellung abschalten.
Adobe Flash-Inhaltseinstellungen auf alle Inhalte erweitern	Diese Einstellung ist verfügbar, wird aber ab Edge Version 87 nicht mehr unterstützt, da ab dieser Version die Flash-Unterstützung wegfällt.
Aktivieren der Sammlungsfunktion	Wenn Sie diese Einstellung deaktivieren, werden Webseiten-Sammlungen deaktiviert. Sammlungen sind über **Strg**+**Shift**+**Y** verfügbar. Es handelt sich um bessere Lesezeichen, die z. B. Notizen unterstützen.
AutoAusfüllen für Kreditkarten aktivieren	Deaktivieren Sie diese Einstellung um zu verhindern, dass Edge Kreditkartendaten sammelt.
Benutzerfeedback zulassen	Ist diese Richtlinie aktiviert oder nicht konfiguriert, öffnet sich ab und an ein Feedback-Fenster. Wenn Sie Ihre Nutzer nicht mit zusätzlichen Popups stören wollen, deaktivieren Sie diese Funktion.
Blockieren der Nachverfolgung der Webbrowsing-Aktivitäten von Benutzern	Mit dieser Einstellung können Sie festlegen, welche Websites Edge am Tracking hindert. Sie können Sie als Policy oder als optionale Einstellung konfigurieren.  Es werden vier Modi unterstützt: ▪ Aus (keine Tracking-Verhinderung) ▪ Grundlegend: Inhalte und Anzeigen werden personalisiert ▪ Ausgeglichen: Blockiert Tracker von Fremdwebsites (die auf einer besuchten Site nur verlinkt oder eingebettet sind). Inhalte und Anzeigen werden personalisiert. ▪ Streng: Blockiert alle Tracking-Aktivitäten, Inhalte und Anzeigen werden nicht personalisiert
Cookies von Drittanbietern blockieren	Aktiviert blockiert Edge Cookies von Domänen, die der Benutzer nicht besucht hat.
Den Modus von DNS-over-HTTPS steuern	Mit dieser Einstellung können Sie DNS-over-HTTPS aktivieren. Dieses Feature sendet DNS-Anfragen verschlüsselt, wird allerdings nicht von allen DNS-Servern unterstützt. Mögliche Optionen sind: ▪ Aktivieren von DNS-over-HTTPS mit unsicherem Fallback: Edge versucht die Namensauflösung über einen verschlüsselten DNS-Server. Schlägt die Namensauflösung fehl, verwendet Edge den normalen DNS-Dienst für die Auflösung.

(Fortsetzung nächste Seite)

Einstellung	Auswirkung
	▪ Aktivieren von DNS-over-HTTPS ohne unsicheres Fallback: Edge löst DNS nur verschlüsselt auf. Ist kein sicherer DNS-Server verfügbar, schlägt die Abfrage fehl. ▪ DNS-over-HTTPS abschalten. Wenn Sie DNS-over-HTTPS erzwingen, müssen Sie auch die Option *URI-Vorlage der gewünschten DNS-Über-HTTPS-Auflösung angeben* konfigurieren.
Einfrieren von Hintergrundtabs zulassen	Edge kann Tabs, die seit mindestens fünf Minuten im Hintergrund laufen, einfrieren. Dadurch sinken CPU- und Arbeitsspeicherverbrauch, weil Skripte und aktive Inhalte nicht mehr ausgeführt werden. Diese Einstellung ist standardmäßig aktiv, kann durch das Deaktivieren der Richtlinie aber abgeschaltet werden.
Enterprise Mode Site List konfigurieren	Mit Hilfe der Enterprise Mode Site List können Sie eine Liste von URLs angeben, die aus z. B. Kompatibilitätsgründen automatisch mit dem Internet Explorer geöffnet werden sollen. Die Einstellungen entsprechen denen des alten Edge-Browsers. Dort habe ich die Konfiguration auch beschrieben.
Erforderliche und optionale Diagnosedaten über die Browsernutzung senden	Diese Einstellung konfiguriert die Einstellung der Telemetrie für den Edge-Browser, aber nicht unter Windows! Hier greift der Edge-Browser auf die Windows-Telemetrie-Einstellungen zu.
Mindestversion von TLS aktiviert	Aktivieren Sie diese Option, um eine höhere Version als TLS 1.0 im Edge zu erzwingen. TLS (Transport Layer Security) ist der Sicherheitsmodus, unter dem https betrieben wird. Versionen vor TLS 1.2 gelten als unsicher, allerdings funktionieren Websites, die TLS 1.2 nicht unterstützen, dann nicht mehr verschlüsselt.
Nicht verfolgen (Do not track) konfigurieren	Aktivieren Sie diese Einstellungen, damit Websites angezeigt wird, dass ein Benutzertracking nicht erwünscht ist. Leider ist die Option komplett optional und wird von den meisten Websites ignoriert.
PDF-Dateien immer extern öffnen	Aktivieren Sie diese Option, wenn Sie Edge nicht als Standard-PDF-Viewer registrieren wollen.
Personalisierung von Anzeigen, Suche und News zulassen, indem Sie den Browserverlauf an Microsoft senden	Wenn Sie mit einem Microsoft-Konto im Edge angemeldet sind, speichert Edge persönliche Daten in Ihrem Account bei Microsoft. Deaktivieren Sie diese Richtlinie, um das Senden von Suchdaten an Microsoft zu unterbinden.
Shopping in Microsoft Edge aktiviert	Edge hat in der aktuellen Version (87) eine Funktion bekommen, die automatisch nach Rabatt-Gutscheinen sucht, wenn Sie sich auf einer Shopping-Website befinden. Deaktivieren Sie diese Richtlinie, um diese Option zu unterbinden. (Stand November 2020 hat Microsoft diese experimentelle Funktion zumindest temporär wieder deaktiviert)
Surf-Spiel zulassen	Der Edge hat auch ein Easteregg eingebaut, das Sie über die URL *edge://surf* aufrufen können. Deaktivieren Sie diese Richtlinie, um Ihre Benutzer am „Surfen“ zu hindern.

Einstellung	Auswirkung
URI-Vorlage der gewünschten DNS-über-HTTPS-Auflösung angeben	Wenn Sie DNS-over-HTTPS aktiviert haben, müssen Sie in dieser Richtlinie die URI eines DNS-Anbieters angeben. Eine Liste von Anbietern, die DNS-über-HTTPS anbieten, finden Sie, wenn Sie den Edge mit der URL *edge://settings/privacy* öffnen und dann unter Sicherheit „Einen Dienstanbieter auswählen“ aktivieren. Edge listet dann eine Reihe von öffentlich zugänglichen DNS-URIs auf. Google und Cloudflare sind nicht empfehlenswert, da Sie die DNS-Auflösung zum Benutzertracking und zur Datensammlung verwenden. Ein empfehlenswerter Anbieter ist Quad9. Die URI, die Sie in der Richtlinie eintragen müssen, lautet dann: *https://dns.quad9.net/dns-query*

Weitere Standard-Sucheinstellungen können Sie in den Unterkategorien wie Proxyserver oder Suchanbieter vornehmen. Da die Einstellungen selbsterklärend sind, gehe ich nicht im Detail drauf ein.

12.6.3 Auswertung der Richtlinien

Sie können sich im Edge die per Gruppenrichtlinien konfigurierten Werte anzeigen lassen, indem Sie die URI *edge://Policy* aufrufen.

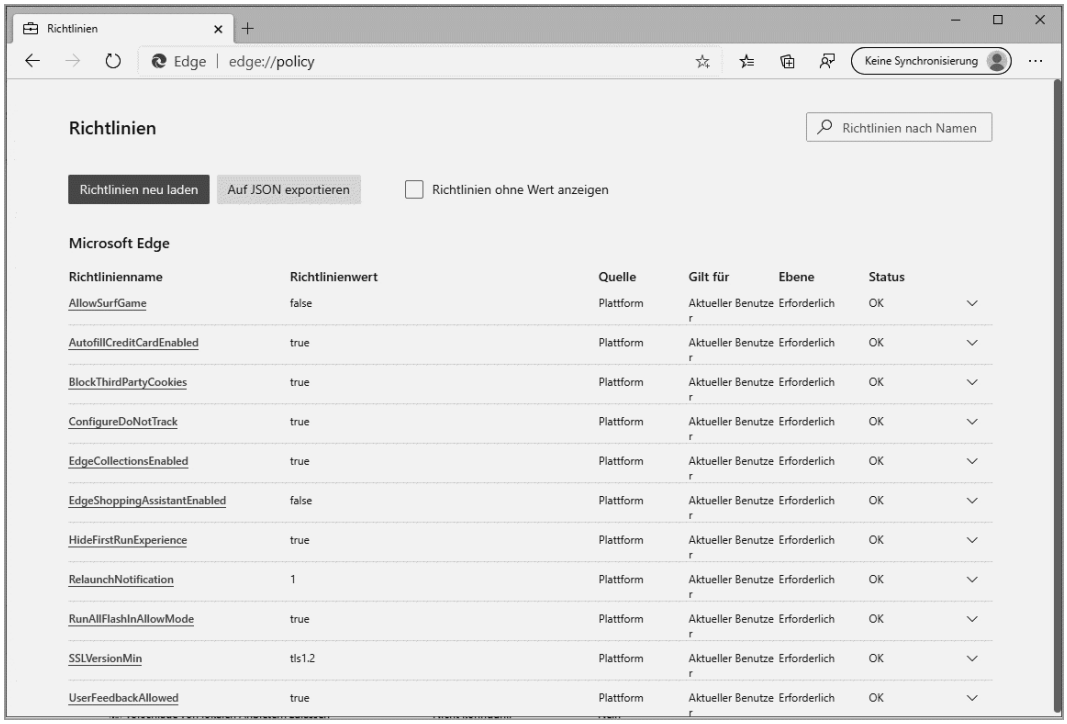


Bild 12.25 Der Edge zeigt Ihnen alle konfigurierten Richtlinien und auch Konfigurationskonflikte an

12.7 Virtualisierungsbasierte Sicherheit

Virtualisierungsbasierte Sicherheit bezeichnet eine Reihe von Sicherheitsfunktionen, die auf Microsofts Virtualisierungslösung Hyper-V basieren. Hyper-V ist mit Windows Server 2008 eingeführt worden. Es handelt sich wie bei VMWare ESX-Server um einen Type-1 oder Bare-Metal Hypervisor. Das bedeutet, dass Hyper-V als Betriebssystem fungiert. Wenn Sie Hyper-V aktivieren, wird das Betriebssystem des Rechners zu einer (speziellen) virtuellen Maschine „degradiert". Es läuft in der sogenannten Root-Partition – Partitionen bezeichnet in diesem Fall nicht Festplattenpartitionen, sondern die einzelnen „Hardware-Bereiche", die einer virtuellen Maschine zur Verfügung gestellt werden.

Um Hyper-V unter Windows 10 installieren zu können, werden zwei Prozessor-Funktionen benötigt – die CPU muss Virtualisierungserweiterungen mitbringen (bei Intel VT-x, bei AMD SVM), die im BIOS aktiviert sein müssen, und sie muss SLAT unterstützen, eine Funktion, die den virtuellen Arbeitsspeicher der VMs auf den physikalischen RAM abbildet. Das kann ohne SLAT auch direkt von der Virtualisierungssoftware durchgeführt werden, ist aber ressourcenintensiv und wird von Windows 10 auch nicht unterstützt. Die Abkürzung steht für Second Level Address Translation. Beide Features sollten von einer CPU, die nach 2010 herausgekommen ist, unterstützt werden. Die einzige Ausnahme bilden eventuell atombasierte Intel-CPUs. Ansonsten sind alle Core i-CPUs der zweiten Generation in der Lage, Hyper-V auf Windows 10 auszuführen.

Da Hyper-V zum eigentlichen Betriebssystem wird, steuert es letztendlich den Zugriff auf die Hardware und nicht das Root-OS. Dadurch wird es möglich, Programme auf dem Computer zu starten, die dem Betriebssystemzugriff komplett entzogen sind. Sicherheitskritische Prozesse, die vor Windows 10 immer als Teil des Betriebssystems ausgeführt wurden und damit von einer Malware mit administrativen Berechtigungen manipuliert oder beendet werden konnten, sind vor deren Zugriff geschützt. Diese Anwendungen werden als Trustlets bezeichnet.

Virtualisierungsbasierte Sicherheit setzt außerdem voraus, dass Ihre Computer über eine UEFI-Firmware verfügen und dass Secure Boot aktiviert ist.

UEFI und Secure Boot

UEFI steht für Unified Extensible Firmware Interface und ersetzt bei fast allen aktuellen Computern das in die Jahre gekommene BIOS, das von IBM Mitte der 1980er-Jahre eingeführt wurde. UEFI ist also kein BIOS, sondern es handelt sich bei beiden Systemen um eine Firmware, die dazu benötigt wird, einen Computer zu initialisieren und das eigentliche Betriebssystem dann von einem Startdatenträger zu booten.

UEFI ist deutlich moderner als die BIOS-Firmware und kann neben einer ganzen Reihe von Verbesserungen wie der Möglichkeit, von GPT-Datenträgern zu starten, auch Programme ausführen. UEFI-Programme haben normalerweise die Endung .efi. Auch der Windows Bootloader, also das Programm, das den Startvorgang von Windows einleitet, kommt in Form einer efi-Datei. Er liegt in einer FAT32-formatierten Systempartition, die Windows bei der Installation anlegt.

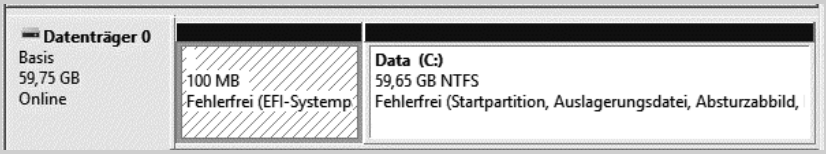


Bild 12.26 Die EFI-Systempartition

Diese Partition ist zwar vom Explorer aus nicht direkt zugreifbar, aber eigentlich direkt manipulier- und austauschbar. Auch in Windows geht das recht einfach mithilfe des Kommandozeilentools diskpart. Eine Malware oder ein Hacker ist damit in der Lage, den Bootloader direkt auszutauschen, und da es sich um eine Fat32-Partition handelt, benötigt er dafür noch nicht einmal besondere Rechte. Der manipulierte Bootloader kann damit bereits vor dem Start des Betriebssystems die Kontrolle über den Computer übernehmen. Um das zu verhindern, sollten Sie in den Firmwareeinstellungen auf jeden Fall Secure Boot aktivieren. Secure Boot ist der Schutzmechanismus, der verhindert, dass ein manipulierter Bootloader überhaupt erst gestartet wird. Dazu prüft die Firmware die digitale Signatur der Datei, die von Microsoft erstellt wurde und die sicherstellt, dass jede Manipulation an der Datei erkannt wird.

12.7.1 Windows Defender Credential Guard

Windows Defender Credential Guard löst ein Sicherheitsproblem, das in Deutschland vor allem durch den Bundestag-Hack bekannt geworden ist, die sogenannte Pass-the-Hash-Attacke.

Pass the Hash ist ein Netzwerkangriff, der es einem Hacker innerhalb kürzester Zeit ermöglicht, ein Netzwerk zu übernehmen. Er basiert darauf, dass Windows beim Anmelden eines Benutzers seine Anmeldeinformationen im Arbeitsspeicher zwischenspeichert. Das ist für das einmalige Anmelden (Single Sign-on) notwendig, also die Fähigkeit von Windows, einen Benutzer an beliebigen Ressourcen des Forest anmelden zu können, ohne dass er jedes Mal durch ein nerviges Anmelde-Pop-up von der Arbeit abgehalten wird. Eine Malware, die administrative Berechtigungen erlangt, kann diesen Zwischenspeicher aber direkt auslesen. Sie kann sich jetzt wie eine Spinne auf die Lauer legen und warten, bis ihr Benutzer mit umfassenderen Administratorrechten ins Netz geht. Sie kann das sogar recht einfach erzwingen, indem sie Fehler auf dem Benutzer-PC erzeugt, sodass der User ein Helpdesk Ticket öffnet. Sobald sich ein Helpdesk-Mitarbeiter zum Prüfen des Problems am Client anmeldet, hat die Schadsoftware seinen Kennwort-Hash und Zugriff auf seine Kerberos-Tickets. In den meisten Fällen ist das katastrophal, da der Helpdesk sich üblicherweise mit einem Benutzerkonto mit vollumfänglichen administrativen Rechten anmeldet, das die Schadsoftware jetzt nutzen kann, um sich im Netzwerk weiter zu verbreiten und zu warten, bis ein Benutzer mit noch vollumfänglicheren Rechten ihr ins Netz geht – also ein Domänenadministrator. Danach kann die Schadsoftware auf den Domänencontroller zugreifen und hat volle Kontrolle über alles.

Dieses Problem ließ sich bis Windows 10 nur auf einem Weg ausräumen, nämlich mit dem LAPS-Tool, das in Kapitel 7 vorgestellt worden ist. Windows 10 Enterprise Edition kann mit virtualisierungsbasierter Sicherheit aber einen deutlich besseren Schutz anbieten. Sobald Credential Guard aktiviert ist, werden die Kennwörter nämlich durch einen isolierten zweiten Anmeldeprozess geschützt, der durch die virtualisierungsbasierte Sicherheit abgeschirmt wird. Sobald der Benutzer sein Kennwort eingibt, überträgt der (unsichere) Anmeldeprozess das Kennwort per RPC (Remote Procedure Call, eigentlich ein Netzwerkzugriff) an den isolierten Anmeldeprozess, der die Daten in einem für das Betriebssystem unsichtbaren Arbeitsspeicherbereich ablegt.

Die Aktivierung beschreibe ich im nächsten Abschnitt, Windows Defender Application Control. Wenn Sie wissen möchten, wie virtualisierungsbasierte Sicherheit und Device Guard genau funktionieren, empfehle ich Ihnen eine Reihe von (leider) englischen Videos bei Channel 9 von Seth Juarez.

- *https://channel9.msdn.com/Blogs/Seth-Juarez/More-on-Processes-and-Features-in-Windows-10-Isolated-User-Mode-with-Dave-Probert* oder kurz *https://bit.ly/2NCbN4W*
- *https://channel9.msdn.com/Blogs/Seth-Juarez/Mitigating-Credential-Theft-using-the-Windows-10-Isolated-User-Mode* oder kurz *https://bit.ly/2LEWVSG*
- *https://channel9.msdn.com/Blogs/Seth-Juarez/Windows-10-Virtual-Secure-Mode-with-David-Hepkin* oder kurz *https://bit.ly/2NCbN4W* oder kurz *https://bit.ly/2LEVsMf*

12.7.2 Windows Defender Application Control/Device Guard

Windows Defender Application Control (WDAC) ist die Bezeichnung für ein Verfahren, das ähnlich funktioniert wie AppLocker oder Software Restriction Policies (SRS), die in Kapitel 7 beschrieben worden sind. Es handelt es sich also um eine Funktion, um nicht erlaubte Programme zu blockieren.

WADS basiert auf einem Feature, das sich Code Signature Integrity nennt. Kurz zusammengefasst geht es darum, nur vertrauenswürdige Programme auszuführen. Mit Treibern tut Windows das bereits seit Vista, was als Kernel Mode Code Integrity bezeichnet wird. Das heißt, dass Treiber immer eine digitale Signatur tragen müssen, die den Urheber des Treibers identifiziert und außerdem sicherstellt, dass der Treiber nicht verändert wurde. Kann die digitale Signatur nicht geprüft werden, wird der Treiber nicht geladen.

Seit Windows 10 gibt es einen zweiten Sicherheitsmechanismus, bezeichnet als User Mode Code Integrity. User Mode Code Integrity heißt nichts weiter, als dass der Prüfmechanismus für Treiber auch auf Programme ausgeweitet werden kann. Sobald User Mode Code Integrity aktiviert ist, werden Programme, die von Windows nicht geprüft werden können, blockiert. Dieses Feature wurde von Microsoft zur besseren Unterscheidbarkeit neu benannt und heißt jetzt Windows Defender Application Control (WDAC).

Windows Defender Application Control benötigt eine Konfigurationsdatei für die Aktivierung. Das Erstellen der Konfiguration ist recht komplex und hat mit Gruppenrichtlinien tatsächlich nichts zu tun, daher werde ich hier nicht im Detail auf den Prozess eingehen. Sie finden aber ein Video zur Konfiguration in meinem YouTube-Kanal „Gruppenrichtlinien in Windows Server“ unter *https://www.youtube.com/channel/UCmV-KA9FZaanVcIY72wIkbw* oder kurz *https://bit.ly/2uMpuY7*.

Windows Defender Application Control ist ein Feature, das in jeder Windows-Version aktiviert werden kann. Sie können Application Control aber durch virtualisierungsbasierte Sicherheit zusätzlich härten. Der Prozess, der Dateien prüft, bevor er sie ausführt, wird dabei wieder in einem vom Betriebssystem isolierten Prozess ausgeführt.

Zur Aktivierung sowohl von Credential Guard als auch von Device Guard müssen Sie in der Computerkonfiguration unter **Richtlinien – Administrative Vorlagen – System – Device Guard** die Gruppenrichtlinie **Virtualisierungsbasierte Sicherheit aktivieren** einschalten. In der Richtlinie finden Sie mehrere Einstellungen.

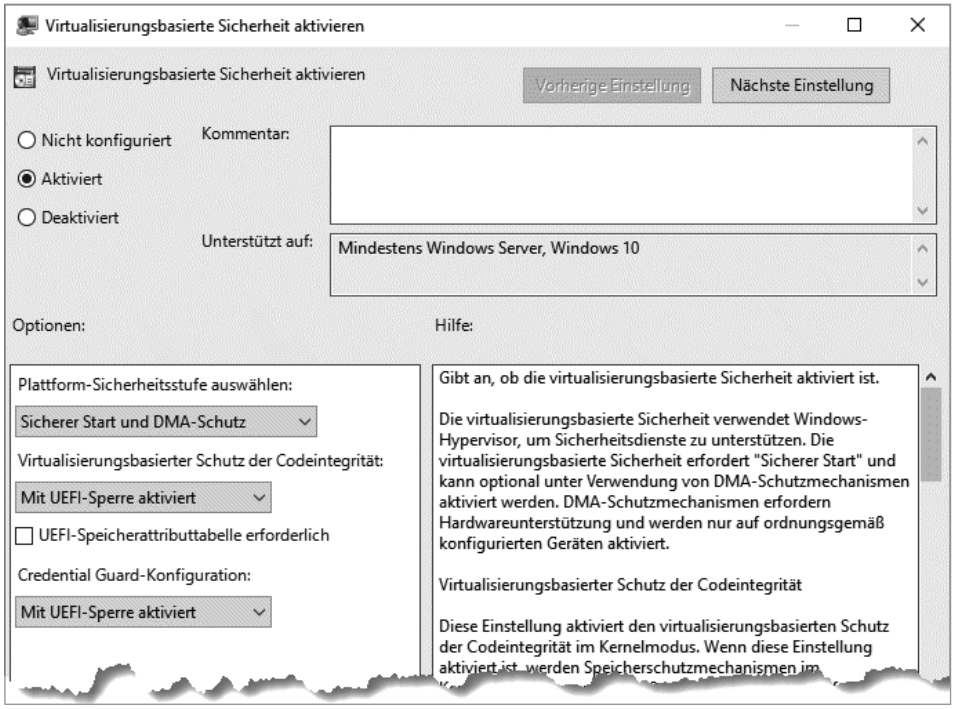


Bild 12.27 Secure Boot, Credential Guard und Device Guard werden auf einer Richtlinie konfiguriert.

Sie können weder Credential Guard noch Device Guard ohne Secure Boot betreiben. Unter „Plattform-Sicherheitsstufe“ können Sie auswählen, ob Sie nur Secure Boot (sicherer Start) unterstützen wollen oder ob Sie zusätzlich DMA-Schutz aktivieren möchten. DMA-Schutz (Direct Memory Access) setzt ein sogenanntes IOMMU-Modul voraus. IOMMU-Module schützen den Computer davor, dass externe Geräte direkt ungeschützt auf den Arbeitsspeicher zugreifen können. Das ist grundsätzlich eine gute Sache, und fast alle modernen CPUs sollten IOMMU unterstützen. Allerdings nur fast. IOMMU erkennen Sie bei Intel-CPUs an der Firmware-Funktion vt-d (Intel Virtualization Technology for Directed IO), die verfügbar und aktiviert sein muss. Bei einigen günstigen Celereon-CPUs ist vt-d aber nicht implementiert. Wenn Sie den DMA-Schutz in der Richtlinie aktivieren, erzwingen Sie dieses Feature. Wenn es nicht aktiviert werden kann, wird die Richtlinie und damit die virtualisierungsbasierte Sicherheit auch nicht aktiviert, Ihre Celerons bleiben also ungeschützt.

Eine gute Einführung in das Thema IOMMU und DMA finden Sie unter *https://www.synacktiv.com/posts/pentest/practical-dma-attack-on-windows-10.html* oder kurz *https://bit.ly/2LHJu4f*.

Für die Aktivierung des Credential Guard stehen auch mehrere Optionen zur Verfügung. Mit „Deaktiviert" können Sie Credential Guard direkt ausschalten. Er ist dann auch lokal nicht aktivierbar. Wenn Sie „Ohne Sperre aktiviert" auswählen, wird Credential Guard aktiviert. Wenn Sie „Mit UEFI-Sperre aktiviert" auswählen, können Credential Guard und Secure Boot nur noch lokal am Rechner wieder deaktiviert werden! UEFI-Sperre bedeutet also, dass Sie die Funktion in der Firmware sperren und nicht mehr über eine Gruppenrichtlinie verändern können! Das ist aus sicherheitstechnischer Sicht wünschenswert, aber man sollte sich der Konsequenzen bewusst sein.

Um Device Guard zu aktivieren, konfigurieren Sie die Einstellung „Virtualisierungsbasierter Schutz der Codeintegrität". Hier gelten die gleichen Einschränkungen wie für Credential Guard. Allerdings müssen Sie für Device Guard auch noch eine Policy-Datei zur Verfügung stellen. Hierfür verwenden Sie die Richtlinie Windows Defender-Anwendungssteuerung bereitstellen, die Sie ebenfalls unter **Richtlinien – Administrative Vorlagen – System – Device Guard** finden. Die Policy-Datei können Sie auf einer beliebigen Netzwerkfreigabe zur Verfügung stellen. Geben Sie unter „Dateipfad für Codeintegritätsrichtlinie" einfach den UNC-Pfad zur Datei an. Der Client kopiert die Datei dann automatisch in den richtigen Pfad: `%windir%\system32\Codeintegrity`. Achten Sie darauf, dass nach der Bereitstellung von der Policy erst ein Computerneustart notwendig ist, bevor die Einstellungen ziehen.

Um zu prüfen, ob die virtualisierungsbasierte Sicherheit aktiviert ist, starten Sie „Systeminformationen" aus dem Startmenü und suchen Sie in der Systemübersicht den Eintrag „Virtualisierungsbasierte Sicherheit".

HINWEIS: Sie müssen in den aktuellen Versionen von Windows 10 Hyper-V nicht mehr installieren, um die virtualisierungsbasierte Sicherheit einzuschalten, wie es bis Windows 10 1607 noch notwendig war. Auch Secure Boot wird automatisch aktiviert, wenn Sie es über eine Richtlinie erzwingen. Achten Sie aber darauf, dass die Virtualisierungserweiterungen der CPU nur von einem Virtualisierungsprogramm verwendet werden können. Sobald die virtualisierungsbasierte Sicherheit aktiviert ist, können Sie andere Virtualisierer wie Virtual Box oder VMWare Workstation nicht mehr nutzen!

12.7.3 Application Guard

Mirosoft Defender Application Guard ist ein neues Sicherheitsfeature, das Microsoft mit Feature Release 1709 eingeführt hat. Ist Application Guard aktiviert, können Anwendungen in einer sicheren virtuellen Maschine gestartet werden. Im Gegensatz zu Device Guard oder Credential Guard wird ein komplett eigenes Windows-Kernel in Hyper-V gestartet, das parallel zum eigentlichen Windows läuft und als Host für die Anwendung fungiert. Die virtuelle Sitzung hat weder Zugriff auf den Arbeitsspeicher der Benutzersitzung, noch kann sie persistent auf die Festplatte schreiben. Wird die Application-Guard-Sitzung beendet, werden alle Daten gelöscht, sodass alle Prozesse und Änderungen, die von einer Malware durchgeführt

wurden, einfach entfernt werden. Wenn der Benutzer also in einer Application-Guard-Sitzung eine Malware aus dem Internet herunterlädt, kann diese nur die virtuelle Sitzung kompromittieren, aber nicht das eigentliche Betriebssystem. Application Guard wird aktuell für den alten und neuen Edge unterstützt, Microsoft plant aber, ihn auch für andere Anwendungen verfügbar zu machen. Stand November 2020 ist Application Guard für Office 365 gerade in der Public Preview. Mehr dazu erfahren Sie unter *https://docs.microsoft.com/de-de/microsoft-365/security/office-365-security/install-app-guard* oder kurz *https://bit.ly/2NOMKkr*.

Application Guard gibt es in zwei verschiedenen Varianten, im Standalone Mode und im Unternehmensmodus (Enterprise Mode). Im Standalone-Mode legt der Benutzer selber fest, wann er eine durch Application Guard gesicherte Sitzung starten möchte, indem er im Edge-Browser im Menü „Neues Application Guard-Fenster“ auswählt.

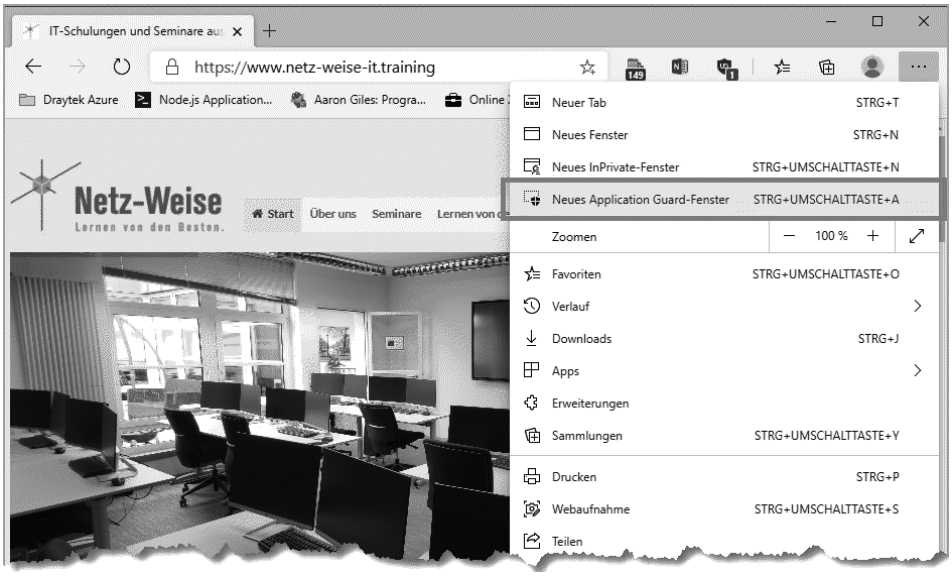


Bild 12.28 Im Stand-alone-Modus startet der Benutzer selbst eine sichere Sitzung.

Im Unternehmensmodus bestimmen Sie über Gruppenrichtlinien, welche Websites sicher sind und ungeschützt angesurft werden können und bei welchen Sites ungeschützter Verkehr nicht erlaubt sein soll.

12.7.3.1 Aktivieren von Application Guard

Um Application Guard aktivieren zu können, muss der Client eine Reihe von Voraussetzungen erfüllen. Zum einen muss er natürlich die gleichen Voraussetzungen mitbringen, die auch für Hyper-V notwendig sind, also Virtualisierungserweiterungen von Intel oder AMD und Second Level Address Translation (SLAT). Zum anderen gibt es aber auch Hard- und Softwarevoraussetzungen, die von Windows erzwungen werden. Sie benötigen mit dem Feature Release 1709 die Enterprise Edition. Ab der Version 1803 wird Application Guard auch in der Professional-Version unterstützt, allerdings nur im Stand-alone-Modus, also benutzerinitiiert. Außerdem muss Ihr Rechner mindestens vier Cores haben (oder zwei Cores mit Hyperthreading), 8 GB Arbeitsspeicher sowie 5 GB freien Festplattenspeicher. Wenn Sie

jetzt schlucken, gibt es eine gute Nachricht – die Limits lassen sich über die Systemregistrierung optimieren. Passen Sie hierfür folgende Werte an:

Limit für	Registrierungsschlüssel
Min. Kerne	HKLM\software\Microsoft\Hvsi\SpecRequiredProcessorCount
Min. RAM	HKLM\software\Microsoft\Hvsi\SpecRequiredMemoryInGB
Min. HDD	HKLM\software\Microsoft\Hvsi\SpecRequiredFreeDiskSpaceInGB

Alternativ verwenden Sie das Cmdlet `Set-ApplicationGuardLimits` aus dem PowerShell-Modul GPHelper.

Wenn Ihr Rechner alle Voraussetzungen erfüllt oder Sie die Grenzwerte angepasst haben, können Sie Application Guard über die Windows-Features oder alternativ mit PowerShell nachinstallieren.

Listing 12.6 Installieren von Application Guard mit PowerShell

```
Enable-WindowsOptionalFeature -Online -FeatureName Windows-Defender-ApplicationGuard
```

Application Guard benötigt einen Neustart.

12.7.3.2 Konfigurieren von Application Guard

Als Nächstes können Sie die Gruppenrichtlinien-Konfiguration für den Unternehmensmodus vornehmen. Die Einstellungen finden Sie an zwei verschiedenen Stellen. Die Features von Application Guard können Sie in der Computerkonfiguration unter **Administrative Vorlagen – Windows-Komponenten – Microsoft Defender Application Guard** festlegen.

Einstellung	Auswirkungen	FR
Dateien dürfen von Windows Defender Application Guard heruntergeladen und im Hostbetriebssystem gespeichert werden.	In der Standardeinstellung können heruntergeladene Dateien die Application-Guard-Sitzung nicht verlassen. Damit ist im Enterprise Mode faktisch kein Download aus dem Internet mehr möglich. Mit dieser Einstellung ist es möglich, den Download ins Dateisystem des Hosts zu aktivieren. Dateien werden dann im Download-Ordner des Benutzers im Unterordner „Nicht vertrauenswürdige Dateien“ abgespeichert. Der Benutzer kann beim Download den Pfad nicht angeben!	Ab 1803
Datenpersistenz für Windows Defender Application Guard zulassen	Mit dieser Einstellung wird festgelegt, ob alle Daten der Benutzersitzung komplett zurückgesetzt werden sollen oder ob die Daten über verschiedene Sitzungen hinweg erhalten bleiben. Das betrifft Downloads (was im Normalfall egal ist, da der Benutzer diese eh nicht starten kann), aber auch Cookies, gespeicherte Kennwörter usw. Wenn Sie die Sitzung jedes Mal zurücksetzen, ist das für den Benutzer, als würden die Browserdaten nach jeder Sitzung gelöscht. Wenn die Datenlöschung nach jeder Sitzung nachträglich aktiviert wird, müssen die gespeicherten Daten manuell mit dem Befehl `wdatgtool.exe /cleanup RESET_PERSISTENCE_LAYER` zurückgesetzt werden.	Ab 1709

Einstellung	Auswirkungen	FR
Druckeinstellungen für Windows Defender Application Guard konfigurieren	Legen Sie fest, ob der Benutzer aus der isolierten Sitzung heraus drucken darf. In dieser Einstellung können Sie anhand einer Ziffer von 0 bis 15 festlegen, welche Druckkombinationen erlaubt sein sollen, wobei 0 das Drucken komplett deaktiviert, 2 nur den PDF-Druck zulässt, 4 lokale Drucker erlaubt und 15 das Drucken global freischaltet. Die einzelnen Kombinationen entnehmen Sie einfach der Beschreibung der Richtlinie.	Ab 1709
Hardwarebeschleunigtes Rendering für Windows Defender Application Guard zulassen	Die virtuelle Maschine, in der Application Guard läuft, bekommt zum Rendern Zugriff auf die GPU (Grafikkarte), was die CPU entlastet und die Performance und Qualität der Grafikdarstellung erhöht. Dieses Feature ist noch experimentell und funktioniert auch nicht immer.	Ab 1803
Kamera- und Mikrofonzugriff in Windows Defender Application Guard zulassen	Erlaubt den Zugriff auf Kamera und Mikrofon des Host-Betriebssystems aus dem isolierten Container. Eine Schadsoftware kann damit direkt auf die Hardware des Hostsystems zugreifen.	1809
Microsoft Defender Application Guard im verwalteten Modus aktivieren	Aktivieren Sie die Gruppenrichtlinie und wählen Sie eine der folgenden Optionen: 0: Application Guard ist deaktiviert 1: Application Guard ist für Edge aktiviert 2: Application Guard ist im Anwendungsmodus (Office) aktiv 3: Application Guard kann für Edge und Office verwendet werden	Ab 1709
Überwachungsereignisse in Windows Defender Application Guard zulassen	Laut Beschreibung kann der virtuelle Edge-Browser mit dieser Einstellung in das Windows Eventlog schreiben. Ich konnte allerdings keine Dokumentation und kein Eventlog finden, das von Edge benutzt wird. Der Eintrag wird bei Microsoft in der Application-Guard-Dokumentation ebenfalls nicht erwähnt.	Ab 1709
Unternehmenswebsites am Laden von Nicht-Unternehmensinhalten in Internet Explorer und Microsoft Edge hindern	Edge und IE dürfen in einer Website im internen Netzwerk keine externe Website nachladen, beispielsweise in einem Frame. Dadurch kann sichergestellt werden, dass eine mit einem ungeschützten Edge aufgerufene Website keinen bösartigen externen Content nachladen kann.	Ab 1709

Verwendung von Host-Stammzertifizierungsstellen des Benutzergeräts durch Microsoft Defender Application Guard zulassen	Die isolierte Application-Guard Umgebung hat keinen Zugriff auf nachträglich installierte Root-Zertifikate. Um Zertifikate des Geräts in der isolierten Umgebung verfügbar zu machen, fügen Sie die Tumbprints hinzu. Wie üblich ermitteln Sie die Tumbprints am einfachsten mit PowerShell.
	`( dir Cert:\CurrentUser\Root\ |`
	`  Out-GridView -PassThru ).thumbprint -join „,"`
	`| set-Clipboard`
		2004

(Fortsetzung nächste Seite)

Einstellung	Auswirkungen	FR
	Das Skript öffnet ein Fenster, in dem Sie die Zertifikate auswählen können. Wenn Sie die Auswahl mit **OK** bestätigen, werden die Thumbprints der Zertifikate kommasepariert in die Zwischenablage kopiert. Wenn Ihre Zertifikate sich in einem anderen Container befinden, können Sie den Pfad hinter cert:\ anpassen. Der Tabulator hilft Ihnen beim Auflösen der möglichen Container.	
Zwischenablageeinstellungen für Windows Defender Application Guard konfigurieren	Legt fest, ob Daten zwischen dem Application-Guard-Modus und dem Host-Betriebssystem ausgetauscht werden können. Standardmäßig ist kein Datenaustausch möglich. Folgende Optionen sind möglich: Zwischenablage blockieren Zwischenablagevorgänge von einer isolierten Sitzung zum Host aktivieren: Daten können nur aus dem isolierten Edge zum Host kopiert werden. Zwischenablagevorgänge von einem Host zur isolierten Sitzung aktivieren: Daten können nur in die isolierte Sitzung kopiert werden. Bidirektionale Zwischenablagevorgänge aktivieren: Daten können in beide Richtungen ausgetauscht werden. Der Datenaustausch ist eingeschränkt auf bestimmte, ungefährliche Datentypen. Sie können festlegen, was erlaubt sein soll: 1: Text 2: Bilder 3: Text und Bilder Dateien und andere Daten können nicht über die Zwischenablage ausgetauscht werden.	Ab 1709

Im Unternehmensmodus erzwingen Sie die Benutzung des Application Guard für unsichere Websites, was per Definition Websites sind, die sich nicht unter Ihrer Kontrolle befinden. Welche Websites Sie kontrollieren, können Sie in der Computerkonfiguration unter **Administrative Vorlagen – Netzwerk – Netzwerkisolation** angeben. Diese Einstellungen kontrollieren auch, auf welche Websites eine App zugreifen darf. Von den Einstellungen sind nur drei für Application Guard relevant.

Einstellung	Auswirkung
Adressbereich des privaten Netzwerks für Apps	Hier tragen Sie die IP-Adressbereiche Ihres privaten Netzwerks ein. Alle Adressen, die hier angegeben sind, sind sicher und können normal im Edge-Browser geöffnet werden. Mehrere Netze werden durch Komma getrennt. Außerdem versucht Windows automatisch, das interne Netzwerk zu ermitteln. Wie Windows das tut, ist leider nicht dokumentiert. Z. B.: 10.1.0.0/16,10.2.1.0/24

Einstellung	Auswirkung
In der Cloud gehostete Unternehmensressourcendomänen	Websites, die nicht im Application-Guard-Modus angezeigt werden sollen. Tragen Sie hier mit dem | getrennt alle DNS-Domänen ein, die Sie erlauben wollen. * sind erlaubt: *.netz-weise.de|*.netz-weise-it.training|hanser.de
Sowohl als Arbeits- als auch als persönliche Ressourcen kategorisierte Domänen	Mit Komma separierte Liste von Domänennamen, die nicht im Application-Guard-Modus angezeigt werden sollen, sondern im normalen Edge-Browser.

Mit Application Guard können Sie sich auch effektiv vor bösartigen Links in E-Mails schützen, die auf kompromittierte Webserver verlinken, wenn Sie Edge zum Standardbrowser machen. Wenn der Benutzer einen Link anklickt, der sich außerhalb Ihres Unternehmens befindet, wird Edge automatisch im Application-Guard-Modus gestartet, auch wenn der Link für den Benutzer scheinbar auf einen internen Server zeigt.

Microsoft bewirbt, dass Sie auch Chrome und Firefox mit Application Guard betreiben können. Hierfür benötigen Sie allerdings zwei Erweiterungen – eine für den Browser und eine für das Betriebssystem. In Firefox geben Sie hierfür *about:addons* in der Adressleiste ein und geben dann unter **Weitere Add-ons finden** *application guard* ein. Wählen Sie dann aus den Suchergebnissen die *Application Guard Erweiterung* aus und installieren sie. Wenn Sie den Firefox erneut starten, weist er Sie in einer neuen Registerkarte darauf hin, dass Sie die Application-Guard-Begleit-App noch installieren müssen.

Bild 12.29 Firefox benötigt neben der Extension auch die Begleit-App aus dem Store

Der Link führt Sie direkt in den Microsoft-Store zur *Microsoft Defender Application Guard Companion-App*. Installieren Sie die App lokal und starten Sie den Rechner neu. Anschließend finden Sie im Firefox in der Adresszeile die Application-Guard-Erweiterung.

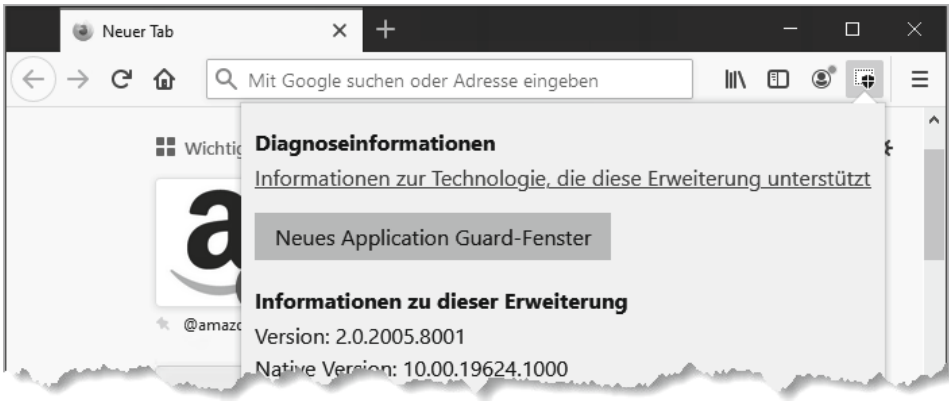


Bild 12.30 Starten Sie ein neues Application-Guard-Fenster mit Firefox

Lustigerweise machen die Erweiterungen aber nicht das, was man erwarten würde. Anstatt ein Firefox-Fenster geschützt zu starten, öffnet sich das neue Fenster wieder im Edge-Browser. Immerhin funktioniert mit der Erweiterung aber auch der Unternehmens-Modus. Mehr zur Integration von Firefox und Chrome finden Sie unter *https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-application-guard/md-app-guard-browser-extension* oder kurz *https://bit.ly/37JuBL2*.

Favoriten können aktuell nicht in eine Application-Guard-Sitzung übernommen werden. Das kann sich in Zukunft aber ändern.

Erweiterungen des Hosts laufen ebenfalls nicht im gesicherten Edge und können aktuell auch nicht installiert werden.

Proxyserver müssen als symbolische Namen (Computernamen) angegeben werden, nicht als IP-Adressen. Alternativ können Sie die IP-Adresse ohne Punkte angeben und ein P voranstellen, also z. B. P101255254 für die IP 10.1.255.254. Mehr dazu finden Sie in der Application-Guard-Dokumentation unter *https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-guard/faq-wd-app-guard* oder kurz *https://bit.ly/2Oz92Tk*. Die beste Dokumentation zur Funktionsweise von Application Guard finden Sie unter *https://cloudblogs.microsoft.com/microsoftsecure/2017/10/23/making-microsoft-edge-the-most-secure-browser-with-windows-defender-application-guard/* oder kurz *https://bit.ly/2LGWds6*.

12.8 Clientkonfiguration aus der Cloud

Microsoft ist seit einiger Zeit dabei, Windows 10 per MDM (Mobile Device Management) immer besser konfigurierbar zu machen. MDM ist ursprünglich für die Konfiguration mobiler Geräte entwickelt worden, und da Windows 10 ja quasi ein Hybrid ist, kennt es auch das MDM-Protokoll und lässt sich darüber konfigurieren.

Microsofts Lösung zur Konfiguration mobiler Geräte nennt sich Intune und ist ein komplett cloudbasierter Dienst, der inzwischen Teil von Office 365 ist. Mithilfe von Intune ist es möglich, Software und Updates auf Windows 10-Clients zu verwalten, ohne dass diese Clients sich im Unternehmensnetzwerk befinden müssen. Genau genommen müssen die Clients noch nicht einmal Teil einer Windows-Domäne sein. Neben der Softwareverteilung bietet Intune aber vor allem noch einen ganzen Stapel voll von Richtlinien an, die es ermöglichen, Windows 10 remote zu steuern. Es handelt sich hierbei nicht um Gruppenrichtlinien, aber die Einstellungen überschneiden sich an vielen Stellen, da Intune letztlich die gleichen Schnittstellen verwendet wie Gruppenrichtlinien.

Wie Sie Windows 10 per Intune verwalten können, erfahren Sie in den Kapiteln 17 und 18.