NV: Stand 07.11.2019
ergänzend zum Prüfschema

... das Ergebnis findet sich auf Seite 13.

Konferenz der unabhängigen
Datenschutzbehörden
des Bundes und der Länder

Anlage 1

Datenschutz bei Windows 10

– weitergehende technische Aspekte –

Impressum:

Titel:

Datenschutz bei Windows 10 – weitergehende technische Aspekte – Version 1.0 **– Arbeitsversion 6**

(Anlage 1 zum Prüfschema)

Herausgeber:

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

Edition und Redaktion:

AK Technik der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

Ansprechpartner/Autoren:

Rasmus Robrahn, Dr. Martin Krämer, Dr. Christoph Lahmann und Uwe Robra
(Die Landesbeauftragte für den Datenschutz Niedersachsen)

Inhalt

1. Einleitung

Das Prüfschema beleuchtet den Einsatz von Windows 10 im Wesentlichen aus rechtlicher Sicht.

Dabei wird darin sowohl auf allgemeine technische Aspekte als auch auf Windows-spezifische Sachverhalte eingegangen. Aus Gründen der besseren Lesbarkeit werden diese aber nicht ausführlich dargestellt und erläutert.

Aus diesem Grund widmet sich diese Anlage daher der vertieften Erläuterung der im Hauptteil verwendeten Begriffe und Sachverhalte und gliedert sich dabei in die folgenden Abschnitte:

- Editionen (Überblick über die existierenden Editionen von Windows 10 und der damit verbundenen verschiedenen Funktionalitäten und integrierten Anwendungen)

- Telemetriedaten (Definition des Begriffs, Erläuterung der verschiedenen Stufen der Datenübermittlung an Microsoft sowie Maßnahmen zur Reduktion des Datenaustauschs, der allerdings nicht vollständig unterbunden werden kann)

- Windows Update (Erläuterung der verschiedenen Updatekonzepte, die sich je nach Edition unterscheiden können sowie Darstellung der Problematik, dass Updates vom Nutzer nicht vollständig verhindert werden können)

Es ist zu beachten, dass die in dieser Anlage dargestellten Informationen sich auf den im August 2019 vorliegenden Kenntnisstand beziehen und aus verschiedenen Quellen zusammengeführt worden sind.

Die kontinuierliche Veränderung von Windows 10, sowie neue Erkenntnisse über die datenschutzrechtliche Nutzung von Windows 10 werden dazu führen, dass die Informationen in dieser Anlage schnell veralten.

2. Übersicht Windows 10 Editionen[1]

Windows 10 Home	Windows 10 Home ist für den Einsatz auf PCs, Tablets und 2-in-1-PCs konzipiert. Es beinhaltet vor allem verbraucherorientierten Funktionen.
Windows 10 Pro	Windows 10 Pro enthält alle Funktionen von Windows 10 Home, mit zusätzlichen Funktionen, die sich an Geschäftsumgebungen orientieren, wie Active Directory, Remote Desktop, BitLocker, Hyper-V und Windows Defender Device Guard.
Windows 10 Pro for Workstations	Windows 10 Pro für Workstations ist für High-End-Hardware für intensive Rechenaufgaben konzipiert und unterstützt Intel Xeon, AMD Opteron und die neuesten AMD Epyc-Prozessoren; bis zu vier CPUs; bis zu 6 TB RAM; das ReFS-Dateisystem; Non-Volatile Dual In-line Memory Module (NVDIMM); und Remote Direct Memory Access (RDMA).
Windows 10 Enterprise	Die Enterprise Editionen fügen basierend auf der Windows 10 Pro Edition Funktionen hinzu, um die zentrale Steuerung multiple Installationen des Betriebssystems innerhalb eines Unternehmens zu erleichtern. Im Regelfall wird sie als ein Volumenlizenzvertrag von Microsoft angeboten. Windows 10 Enterprise ist in drei Bereichen konfigurierbar, Semi-Annual Channel, Semi-Annual Channel (Targeted), und Windows Insider.
Windows 10 Enterprise LTSB/LTSC	Windows 10 Enterprise LTSC (Long-Term Servicing Channel) ist eine Langzeit-Support-Version von Windows 10 Enterprise, die alle 2 bis 3 Jahre erscheint. Jede Version wird 10 Jahre lang nach ihrer Veröffentlichung mit Sicherheitsupdates unterstützt und erhält bewusst keine Funktions-Updates. Einige Funktionen, darunter der Microsoft Store und gebündelte Anwendungen, sind in dieser Edition nicht enthalten. Microsoft Windows 10 LTSC ist speziell für Systeme gedacht, welche in kritischen Bereichen eingesetzt werden. Demzufolge eignet sich diese Version für Umgebungen, in denen es auf funktionale Stabilität und längere Wartungsoptionen ankommt.
Windows 10 Education	Spezielle Version der Enterprise Edition für Bildungseinrichtungen. Windows 10 Enterprise und Education bieten im Vergleich zu der Pro Version noch weitere Features und Einstellungsmöglichkeiten in den Bereichen Produktivität/Benutzerfreundlichkeit, Verwaltung/Bereitstellung, Sicherheit und Grundlagen.
Windows 10 Pro Education	Für Bildungseinrichtungen in den USA (K–12 academic license, nur über Hardware Partner von Microsoft), die auf PCs vorinstalliert ausgeliefert werden darf. Mit der Pro-Version vergleichbar. Seit dem Anniversary Up-

[1] Alle Editionen sind jeweils als 32-Bit- und 64-Bit-Version erhältlich sowie als Version ohne „medienrelevante Technologien“ (N- bzw. KN-Versionen).
Die N-Editionen von Windows 10, genau wie Windows 8 und Windows 7, haben laut Microsoft keine sogenannten „medienrelevanten Technologien“ installiert. Es fehlen also vorinstallierte Programme und Funktionen wie:

- Windows Media Player (Player für Audio- und Video-Dateien)
- Audiocodecs: MPEG, WMA, AAC, FLAC, ALAC, AMR, Dolby Digital
- Videocodecs: VC-1, MPEG-4, H.264, H.265 und H.263
- Windows-Media-Format (Support für ASF-Dateien, Audio- und Videocodecs, Streaming)
- Windows-Media-DRM (Verwaltung digitaler Rechte)
- Groove Music (App zur Musikwiedergabe)
- Video (App zur Videowiedergabe)
- Sprachrekorder (App zur Aufnahme von Sounds)
- Skype (App zum Chatten und für Videoanrufe)
- eine Kamera

Microsoft nennt die für Europa abgespeckte Version seines Betriebssystems Windows N. Für Korea heißt die Version ohne „medienrelevante Technologien“ Windows KN. Die Kürzel N und KN beziehen sich also nur auf das jeweilige Land, für das die Windows-Version gedacht ist.

	date verfügbar.
Windows 10 S[2]	Es handelt sich dabei um eine Windows Version, bei der nur Apps aus dem Windows Store (Ausnahme: Office) installiert werden können. Daher soll das Betriebssystem sicherer sein, mehr Akkulaufzeit bieten, schneller booten und arbeiten. Das Nutzen von Bing als Suchmaschine und Edge als Internetbrowser ist dabei Pflicht. Ein Upgrade auf andere Windows-Versionen ist gegen Aufpreis möglich. Windows 10 S ist als Konkurrenz für Google Chrome OS, vor allem im Bildungsbereich und für kostengünstige Hardware, konzipiert. Windows 10 S basiert auf Windows 10 Pro und nicht auf Windows 10 Home. Windows 10 S und Pro haben viele gemeinsame Features wie Azure Active Directory, Mobile Device Management, Business Versionen von Update und dem Store, Bitlocker und Enterprise Roaming. Diese Features sind wichtig, wenn Windows 10 S im Schuleinsatz von einem Administrator verwaltet werden soll.
Windows 10 IoT Core	Entwickelt speziell für den Einsatz auf Geräten mit niedriger TCO[3] und IoT-Szenarien. Kostenlose Internet der Dinge (IoT) Version für den Raspberry Pi 2/3, MinnowBoard Max und DragonBoard 410c
Windows 10 IoT Core Pro	Entwickelt speziell für den Einsatz auf Geräten mit niedriger TCO und IoT-Szenarien. Kommerzielle Internet der Dinge (IoT) Version („OEM-exklusive SKU“) für den Raspberry Pi 2/3, MinnowBoard Max und DragonBoard 410c
Windows 10 IoT Mobile Enterprise	Entwickelt speziell für den Einsatz auf Geräten mit niedriger TCO und IoT-Szenarien. Für mobile Geräte.
Windows 10 IoT Enterprise	Entwickelt speziell für den Einsatz auf Geräten mit niedriger TCO und IoT-Szenarien.
Windows 10 IoT Enterprise LTSB/LTSC	Entwickelt speziell für den Einsatz auf Geräten mit niedriger TCO und IoT-Szenarien. Langzeit-Support-Version.
Windows 10 Mobile[4]	Für Smartphones und kleine Tablets (z. B. Phablets)
Windows 10 Mobile Enterprise[5]	Für Smartphones und kleine Tablets (z. B. Phablets) , mit zusätzlichen Funktionen für Unternehmen
Team	Windows 10 Team ist eine gerätespezifische Version von Windows 10, die auf den Surface Hub geladen wird.

[2] Eingestellt zugunsten eines “S Mode” für Windows 10 Versionen.
https://www.theverge.com/2018/3/8/17095424/microsoft-windows-10-s-mode-free-upgrades
[3] TCO: Total Cost of Ownership (Gesamtkosten des Betriebs)
[4] Eingestellt
[5] Eingestellt

Die Windows 10 Editionen mit Unterscheidung der Features[6]:

Features	Home	Pro	Enterprise	Education
Existing Fundamentals				
Minimum telemetry level	Basic	Basic	Security	Security
Device Encryption	x	x	x	x
Domain Join		x	x	x
Group Policy Management		x	x	x
Bitlocker		x	x	x
Enterprise Mode Internet Explorer (EMIE)		x	x	x
Assigned Access 8.1		x	x	x
Remote Desktop		x	x	x
Client Hyper-V		x	x	x
Direct Access		x	x	x
Windows To Go Creator			x	x
AppLocker			x	x
BranchCache			x	x
Start Screen Control with Group Policy			x	x
Management and Deployment				
Side-loading of line of business apps	x	x	x	x
Mobile device management	x	x	x	x
Ability to join Azure Active Directory, with single sign-on to cloud-hosted apps		x	x	x
Business Store for Windows 10		x	x	x
Granular UX Control			x	x
Security				
Microsoft Passport	x	x	x	x
Enterprise Data Protection		x	x	x
Credential Guard			x	x
Device Guard			x	x

[6] Weitere Informationen finden sich unter: https://www.microsoft.com/de-de/windowsforbusiness/compare und https://www.microsoft.com/de-de/windows/compare-windows-10-home-vs-pro

Windows 10 Integrierte Apps

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

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

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

3. Telemetriedaten

Der Begriff Telemetrie ist mehrdeutig:

In komplexen IT-Landschaften werden Telemetriedaten benötigt, um Verbindung zwischen einem Server und mindestens einem Client herzustellen, zu halten und zu beenden. Hierzu stellt ein Server einen IT-Dienst bereit, der vom Client auf einem (End-) Gerät genutzt werden kann, falls ein entsprechendes Protokoll spezifikationsgemäß funktioniert. Anderenfalls wird eine Verbindung zu dem einem IT-Dienst nicht aufgenommen oder bei Störung terminiert[7].

In der Netzwerktechnik wie bei dem Einsatz von sensorbasierten Netzen bezeichnet die Telemetrie eine gegebenenfalls fortdauernde Reichweitenmessung mit der ermittelt wird ob ein Trägersignal besteht[8].

Microsoft Telemetrie wiederum ist eine Komponente in Windows 10, die für die automatische Erhebung und Übertragung von Daten an eine von Microsoft betriebene Backend-Infrastruktur verantwortlich ist. Bei den erhobenen Daten handelt es sich um unterschiedliche Daten wie z. B.: Daten über die Nutzung des Computers unter Windows 10 und der an ihn angeschlossenen Geräte, Daten über die Performance des Systems, Daten, die bei Fehlern, wie Programm- oder Systemabstürzen erhoben werden, sowie Daten des Windows Defenders und des Malicious Software Removal Tools (MSRT).

Microsoft weist in den Antworten auf den Fragenkatalog der DSK einerseits auf die Liste der „Windows-diagnostic-Data“ hin, die mit Stand vom 04.15.2019 veröffentlicht wurden und andererseits auf das von Microsoft bereitgestellte Tool „Diagnostic-Data-Viewer“. Microsoft behauptet, das der „Diagnostic Data Viewer“ alle vom Betriebssystem erhobenen Diagnosedaten in chronologischer Reihenfolge auflistet die dann intransparent verschlüsselt übertragen werden.

Die erhobenen Daten werden von Microsoft auch als Diagnose-Daten („diagnostic data“) bezeichnet. Sie dienen ausweislich Microsoft der Gewährleistung der Betriebssystemqualität und sollen die Benutzererfahrung und die Sicherheit von Windows 10 kontinuierlich verbessern.

Telemetrie in Windows 10 nutzt dazu die Funktionen von Event Tracing for Windows, um Daten zu erheben. Event Tracing for Windows (ETW) ist eine Protokollierungsfunktion von Windows 10, die Kernel-Buffer nutzt, um Daten aufzuzeichnen und diese in Form von Echtzeitdaten oder über Logdateien (wie z. B. das Ereignisprotokoll) zur weiteren Verarbeitung bereitzustellen.

ETW besteht aus verschiedenen Komponenten mit unterschiedlicher Funktion:

- (ETW-) Controller (ETW-Kontrollinstanzen) sind Entitäten (z. B. perfmon.exe oder logman.exe), die Größe und Ort der Protokolldatei definieren, Provider aktivieren und eine Session initialisieren und beenden können.
- (ETW-) Providers (ETW-Anbieter) sind Entitäten, die Events (Ereignisse) schreiben und diese über eine sogenannte (ETW-)Session einem (ETW-) Consumer zur weiteren Verarbeitung anbieten können, wenn sie von einem Controller vorher aktiviert wurden.
- (ETW-) Consumer (ETW-Konsumenten) sind Entitäten, die Events zur weiteren Verarbeitung über eine (ETW-) Session entweder in Echtzeit oder über Logdatei (z. B. Windows Ereignisprotokoll (eventvwr.exe)) erhalten können. Ein Consumer kann Events aus mehreren Sessions erhalten.

[7] F. Mattern: Total vernetzt - Szenarien einer informatisierten Welt. Heidelberg, Berlin 2003.
[8] H. Meinke, F. W. Gundlach: Taschenbuch der Hochfrequenztechnik. Berlin, Offenbach 2005.

- (ETW-) Sessions (ETW-Sitzungen) sind definiert durch Speicherbereiche (Kernel Buffer), in die aktivierte Provider ihre Events schreiben. (ETW-) Sessions zeichnen Ereignisse eines oder mehrere Provider auf, die vorher von dem Controller aktiviert wurden. ETW unterstützt in Windows 10 als Maximum die gleichzeitige Aufzeichnung von 64 Sessions.

Telemetrie-Level

Generell gibt es vier Telemetrie Stufen, die kumulativ zueinander aufgebaut sind:

Stufe	Gesammelte Daten	Wert
Sicherheit / Security	Nur Sicherheitsdaten.	**0**
Einfach / Basic	Sicherheitsdaten und grundlegende System- und Qualitätsdaten	**1**
Verbessert / Enhanced	Sicherheitsdaten, grundlegende System- und Qualitätsdaten sowie zusätzliche Einblicke und erweiterte Daten zur Zuverlässigkeit	**2**
Vollständig / Full	Sicherheitsdaten, grundlegende System- und Qualitätsdaten, verbesserte Einblicke und erweiterte Zuverlässigkeitsdaten sowie vollständige Diagnosedaten	**3**

wobei die Ebene „Security“ nur unter Windows 10 Enterprise, Windows 10 Education und Windows 10 IoT-Core –Editionen angezeigt, bzw. verwendet werden kann. Der Umfang der Datenerhebung nimmt aufsteigend von Security bis hin zu Full zu und hängt technisch von der Anzahl der ETW-Provider ab, die für jeden Level in den ETW-Sessions aktiviert sind[9].

Für die Stufe 1 (Basic) gibt Microsoft folgende Übersicht über die verarbeiteten und übertragenen Daten:

Stufe „Einfach“

*Auf der Stufe „Einfach“ wird ein begrenzter Umfang an Daten gesammelt, die wichtig sind, um das Gerät und dessen Konfiguration zu verstehen. Diese Stufe umfasst auch Daten der Stufe **Sicherheit**. Auf dieser Stufe können Sie Probleme identifizieren, die in einer bestimmten Hardware- oder Softwarekonfiguration auftreten können. Beispielsweise kann damit ermittelt werden, ob Abstürze häufiger auf Geräten mit einer bestimmten Speichergröße oder Treiberversion auftreten. Die Komponente „Benutzererfahrungen und Telemetrie im verbundenen Modus“ erfasst keine Diagnosedaten zu System Center, kann jedoch Diagnosedaten für andere Nicht-Windows-Anwendungen übertragen, wenn sie die Zustimmung des Benutzers besitzen.*

Der normale Uploadbereich für die Diagnosedatenstufe „Einfach“ liegt zwischen 109 und 159 KB pro Tag und Gerät.

Zu den auf dieser Stufe erfassten Daten gehören:

[9] Eine generische Übersicht, welche Arten von Daten auf welchem Telemetrie-Level erhoben werden, findet sich unter: https://docs.microsoft.com/de-de/windows/privacy/configure-windows-diagnostic-data-in-your-organization

- ***Grundlegende Gerätedaten**. Diese Daten gewähren einen Einblick in die verschiedenen Typen von Windows-Geräten und -Konfigurationen sowie von systemeigenen und virtualisierten Windows Server 2016-Instanzen im Ökosystem. Dazu gehören:*
    - *Geräteattribute, z. B. Kameraauflösung und Displaytyp*
    - *Internet Explorer-Version*
    - *Akkuattribute, z. B. Kapazität und Typ*
    - *Netzwerkattribute, z. B. Anzahl der Netzwerkadapter, Geschwindigkeit der Netzwerkadapter, Mobilfunkanbieternetzwerk und IMEI-Nummer*
    - *Prozessor- und Speicherattribute, z. B. Anzahl der Prozessorkerne, Architektur, Geschwindigkeit, Größe des Arbeitsspeichers und Firmware*
    - *Virtualisierungsattribute wie SLAT-Unterstützung (Second Level Address Translation) und Gastbetriebssystem*
    - *Betriebssystemattribute, z. B. Windows-Edition und Virtualisierungsstatus*
    - *Speicherattribute, z. B. die Anzahl der Laufwerke, Typ und Größe*
- ***Qualitätsmetriken der Komponente „Benutzererfahrungen und Telemetrie im verbundenen Modus“**. Geben Aufschluss über die Funktion der Komponente „Benutzererfahrungen und Telemetrie im verbundenen Modus“ – einschließlich Anteil in % der hochgeladenen und verworfenen Ereignisse und des Zeitpunkts des letzten Uploads.*
- ***Qualitätsbezogene Informationen**: Erlauben Microsoft einen grundlegenden Einblick hinsichtlich der Leistung eines Geräts und seines Betriebssystems. Zu diesen Daten zählen beispielsweise die Geräteeigenschaften eines verbundenen Standbygeräts, die Anzahl der Abstürze oder Blockierungen sowie die Änderungsdetails des Anwendungsstatus, etwa die genutzte Prozessorzeit und Speicherkapazität, oder die Gesamtbetriebszeit einer App.*
- ***Kompatibilitätsdaten**. Geben Auskunft darüber, welche Apps auf einem Gerät oder einem virtuellen Computer installiert sind, und identifizieren mögliche Kompatibilitätsprobleme.*
    - ***Allgemeine App-Daten und App-Daten für Internet Explorer-Add-Ons**. Enthält eine Liste der Apps, die in einer systemeigenen oder virtualisierten Instanz des Betriebssystems installiert sind, sowie Angaben dazu, ob diese Apps nach einem Upgrade ordnungsgemäß funktionieren. Diese App-Daten umfassen den App-Namen, den Herausgeber, die Version und grundlegende Angaben zu den für die Nutzung gesperrten Dateien.*
    - ***Internet Explorer-Add-Ons**. Enthält eine Liste der auf einem Gerät installierten Internet Explorer-Add-Ons sowie Angaben zur Funktionsfähigkeit nach einem Upgrade.*
    - ***Systemdaten**. Geben Auskunft darüber, ob ein Gerät die Mindestanforderungen für ein Upgrade auf die nächste Version des Betriebssystems erfüllt. Die Systeminformationen umfassen die Größe des Arbeitsspeichers sowie Informationen zum Prozessor und BIOS.*
    - ***Zubehörgerätedaten**. Enthält eine Liste mit Zubehörgeräten, z. B. Drucker oder externe Speichergeräte, die mit Windows-PCs verbunden sind. Zudem geben sie Auskunft darüber, ob diese Geräte nach einem Upgrade auf eine neue Version des Betriebssystems weiterhin funktionieren.*
    - ***Treiberdaten**. Enthalten spezielle Angaben zur Treiberauslastung, anhand derer ermittelt werden kann, ob Apps und Geräte nach einem Upgrade auf eine neue Version des Betriebssystems weiterhin funktionieren. Mithilfe dieser Daten lassen sich Blockierungen ermitteln, sodass Microsoft und unsere Partner Fehlerbehebungen und Verbesserungen anwenden können.*
- ***Microsoft Store**. Gibt Auskunft über die Leistung von Microsoft Store, einschließlich App-Downloads, Installationen und Updates. Enthält zudem Angaben zu Microsoft Store-Aufrufen, Seitenaufrufen zu unterbrochenen und fortgesetzten Einkäufen und zu bezogenen Lizenzen.*

Die auf einem Windows System tatsächlich konfigurierte Anzahl von ETW-Providern eines bestimmten Telemetrie-Levels ist dynamisch und hängt von dem Inhalt der folgenden Datei ab: %ProgramData%\Microsoft\Diagnosis\DownloadedSettings\utc.app.json. Diese Datei definiert den Inhalt der pro

Telemetrie-Level aktivierten ETW-Provider, sie wird **allein von Microsoft kontrolliert**, in Abständen über automatische Downloads erneuert und kann von Betriebssystemversion zu Betriebssystemversion sowie von Installation zu Installation (selbst bei gleicher Betriebssystemversion) variieren. Telemetrie bietet Microsoft darüber hinaus die Funktionalität, zusätzliche Programme oder auch einzelne Funktionen in Bibliotheken aufzurufen, um weitergehende Informationen wie bspw. **Speicherdumps**[10] zur Ergänzung einer Fehlermeldung zu erheben (was der Telemetrie-Dienst kann, da er mit System-Privilegien läuft). Darüber hinaus ist es technisch möglich, dass beliebige Prozesse (die über administrative Rechte oder höher verfügen) ETW-Provider registrieren und mit den DiagTrack ETW-Sessions assoziieren können.

Maßnahmen

Für die Übermittlung von personenbezogenen Daten an Microsoft benötigt der Verantwortliche gem. Art. 6 DSGVO eine Einwilligung oder eine sonstige zulässige Rechtsgrundlage. Soweit dies nicht vorliegt, müssen Maßnahmen zur Unterbindung dieser Datenübermittlungen getroffen werden. Es kommen sowohl systembasierte als auch netzwerkbasierte Maßnahmen in Frage.

Systembasierte Maßnahmen

Aus der Antwort des Bundesaamtes für Sicherheit in der Informationstechnik (BSI) vom 17.06.2019 auf die Anfrage des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) zum Verhalten der Telemetrie in Windows 10 vom 10.07.2019 wird wie folgt zitiert:

„Als Ergebnis der „SiSyPHuS Windows 10 Studie“ kann festgestellt werden, dass sich die Telemetriedatenverarbeitung in Windows 10 zwar deaktivieren lässt, dies jedoch erweiterte Systemkenntnisse voraussetzt, die von einem durchschnittlichen Benutzer nicht zu erwarten sind. Darüber hinaus stellen diese Einstellungen einen tiefen Eingriff in das Betriebssystem dar, der von Microsoft selbst nicht empfohlen und offiziell nicht unterstützt wird. Des Weiteren zeigt die Vergangenheit, dass derart vorgenommene Änderungen durch Systemaktualisierungen von Microsoft regelmäßig wieder rückgängig gemacht werden und dies somit einen hohen, nicht zumutbaren Pflegeaufwand für den Endbenutzer bedeutet.

Darüber hinaus besteht nur die Möglichkeit, über die Auswahl des Telemetrielevels die Häufigkeit der Telemetriedatenübertragung zum Hersteller zu ändern. Welche Daten und in welchem Umfang diese erhoben werden, ist nicht nur von der Auswahl des Telemetrielevels, sondern zusätzlich vom Nutzerverhalten abhängig. Die Zuordnung der Ereignisse zum Telemetrielevel ist zudem dynamisch und kann jederzeit durch Microsoft verändert werden.“

Netzwerkbasierte Maßnahmen

Konfigurationsmöglichkeiten für zentrale Netzwerkdienste, welche die Kommunikation der DiagTrack-Komponente Netzwerk-basiert für alle angeschlossenen Client-Systeme unterbinden oder einschränken können:

- Nutzung eines HTTP-Proxy
- Anpassung der Firewall
- Anpassung der DNS-Einträge auf zentralem Resolver

Eine Blockade über Proxy-Server funktioniert in der Regel nur für Systeme im eigenen LAN aber nicht für Heim- oder mobile Arbeitsplätze.

[10] Kopien oder Auszüge eines Speicherinhaltes.

Ergebnis

Die Datenschutzaufsichtsbehörden „Bayerisches Landesamt für Datenschutzaufsicht“ und das niederländische „Autoriteit Persoonsgegevens“ sowie das Bundesamt für Sicherheit in der Informationstechnik haben diese Problematik untersucht und sind zu dem Ergebnis gekommen, dass eine vollständige Übertragung mit systembasierten Abhilfemaßnahmen allein nicht verhindert werden kann[11].

Auch Netzwerkbasierte Abhilfemaßnahmen scheinen nur über den Umweg, eine direkte Internetanbindung von Windows 10 Systemen zu unterbinden und den Internetzugang (über Browser oder Fachanwendungen) über eine Virtualisierungs- oder Terminallösung erfolgen zu lassen, noch erfolgversprechend.

[11] Eine Deaktivierung ist mutmaßlich nur durch dezidierte Registry-Einträge möglich.

4. Windows Update

Die Strategie „Windows als eine Dienstleistung“ spiegelt sich auch beim Thema Updates wieder: Während der Updatemechanismus der Sicherheitspatches unverändert geblieben ist, welche nach wie vor einmal monatlich erscheinen, ist es ein Novum, dass neue Funktionalitäten und Dienste mit ihrer Fertigstellung veröffentlicht werden und sofort verfügbar sind. Wurden „große“ Updates früher in Form von Service Packs oder komplett neuen Windows-Versionen veröffentlicht, geschieht dies nun regelmäßig zweimal jährlich in Form von Funktions-Updates. Zudem werden nun alle Windows 10-Installationen regelmäßig automatisch upgedatet.

Ursprünglich hatte Microsoft ab 2015 die Modelle „Current Branch“ (CB) und „Current Branch for Business“ (CBB) zur Verwaltung von Updates im Enterprise -Bereich angeboten. Im Sommer 2017 wurde diese Modelle zugunsten von Semi-Annual Channel (SAC) und Semi Annual Channel-Targeted (SAC-T) abgeschafft. Mit der Bereitstellung von Windows 10 V1903 strich Microsoft nun die Auswahl zwischen SAC-T und SAC.

Aktuell[12] besteht Windows Update Channel (SAC) aus zwei halbjährliche Versionen, die sofort nach Freigabe bzw. nach eingestellter Verzögerungszeit zur Installation wirksam werden.[13]

Besonders kritische Bereiche sollten mit Windows 10 Enterprise LTSB (Long Term Servicing Branch) betrieben werden. Dort gibt es zwar ebenfalls regelmäßig Sicherheitsupdates und auch die Funktionsupdates sind verfügbar, letztere müssen jedoch erst spätestens nach 10 Jahren eingespielt werden. Microsoft wird aber regelmäßig nach großen Funktions-Updates ein neues LTSB-Build, d.h. einen jeweils aktuellen Snapshot für diese Version bereitstellen. Einige Dienste, wie Cortana, OneDrive oder der Windows Store sind für diese Version nicht verfügbar. Der garantierte Support für Windows 10 Enterprise LTSB beträgt zehn Jahre. Microsoft rät offiziell von der Verwendung von LTSB außerhalb von „Spezialgeräten“ ab, die eine feste Funktion erfüllen und somit keine neuen User Experience Features erfordern. Infolgedessen schließt es Windows Store, die meisten Cortana-Funktionen und die meisten gebündelten Anwendungen aus. Microsoft hat diesen Zweig 2018 in Long-Term Servicing Channel (LTSC) umbenannt[14].

Unterschiede von LTSC im Vergleich zum SAC:

- Verzicht auf neue Betriebssystem-Erweiterungen per Featureupdate
- Verzicht auf neue Sicherheitsfunktionen per Featureupdate.
- Keine Unterstützung für neuere Hardware
- Keine Windows Analytics Upgrade Readiness-Unterstützung bei LTSC
- Keine Unterstützung für den Edge-Browser
- Keine Unterstützung für Cortana
- Keine Unterstützung für Windows Store
- Keine Unterstützung für Surface Hardware
- LTSC unterstützt keine ConfigMgr Express Updates
- Ab Januar 2020 wird Microsoft Office 365 auf LTSC nicht mehr unterstützt.

[12] https://techcommunity.microsoft.com/t5/Windows-IT-Pro-Blog/Windows-Update-for-Business-and-the-retirement-of-SAC-T/ba-p/339523
[13] https://docs.microsoft.com/de-de/windows/release-information/
[14] https://techcommunity.microsoft.com/t5/Windows-10-servicing/Confused-about-Semi-Annual-Channel-Pilot-and-Semi-Annual-Channel/m-p/67179#M59

Microsoft hat bekanntgegeben, dass es keine LTSC-Version des Windows 10 Mai 2019 Update (Version 1903) geben werde. Die nächste LTSC-Version von Windows 10 sei frühestens für Ende 2021 geplant. [15]

Nachstehend sind die Verfügbarkeiten und End-of-Service Daten von Windows 10-Versionen aufgeführt.

Windows 10 Versionsgeschichte	**Verfügbar ab**	**End-of-Service für Home, Pro, und Pro für Workstation Editionen**	**End-of-Service für Enterprise und Education Editionen**
Windows 10, Version 1903	21. Mai 2019	8. Dezember 2020	8. Dezember 2020
Windows 10, Version 1809	13. November 2018	12. Mai 2020	11. May 2021
Windows 10, Version 1803	30. April 2018	12. November 2019	10. November 2020
Windows 10, Version 1709	17. Oktober 2017	9. April 2019	14. April 2020
Windows 10, Version 1703	5. April 2017	9. Oktober 2018	8. Oktober 2019
Windows 10, Version 1607	2. August 2016	10. April 2018	9. April 2019
Windows 10, Version 1511	10. November 2015	10. Oktober 2017	10. Oktober 2017
Windows 10, Release Juli 2015 (Version 1507)	29. Juli 2015	9. Mai 2017	9. Mai 2017

Die Windows 10 LTSC/LTSB-Editionen folgen der Fixed Lifecycle-Richtlinie. Weitere Informationen finden Sie unter Microsoft Business, Developer and Desktop Operating Systems Policy[16].

Windows 10 Enterprise Versionsgeschichte	**Verfügbar ab**	**Mainstream Support Enddatum**	**Erweiterter Support Enddatum**
• Windows 10 Enterprise LTSC 2019 • Windows 10 IoT Enterprise LTSC 2019	13. November 2018	9. Januar 2024	9. Januar 2029
• Windows 10 Enterprise 2016 LTSB • Windows 10 IoT Enterprise 2016 LTSB	2. August 2016	12. Oktober 2021	13. Oktober 2026
• Windows 10 Enterprise 2015 LTSB • Windows 10 IoT Enterprise 2015 LTSB	29. Juli 2015	13. Oktober 2020	14. Oktober 2025

[15] https://techcommunity.microsoft.com/t5/Windows-IT-Pro-Blog/What-s-new-for-IT-pros-in-Windows-10-version-1903/ba-p/622024
[16] https://support.microsoft.com/en-us/help/14085/microsoft-business-developer-and-desktop-operating-systems-policy

5. Referenzen

„Orientierungshilfe zur datenarmen Konfiguration von Windows 10“ der DFN AKIF-Arbeitsgruppe „Windows 10“ in der Version 2.0 vom 05.12.2016

https://www.it-sicherheit.mpg.de/Orientierungshilfe_Windows10.pdf

„Windows 10 Investigation Report“ des Bayerisches Landesamtes für Datenschutzaufsicht vom September 2017

https://www.lda.bayern.de/media/windows_10_report.pdf

„Rapport definitieve bevindingen Microsoft Windows 10 - De verwerking van persoonsgegevens via telemetrie -met correcties 6 oktober 2017“ von der Autoriteit Persoonsgegevens

https://autoriteitpersoonsgegevens.nl/sites/default/files/01_onderzoek_microsoft_windows_10_okt_2017.pdf

„SiSyPHuS Win10: Studie zu Systemaufbau, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10“ des Bundesamt für Sicherheit in der Informationstechnik vom 20.11.2018

https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/SiSyPHuS_Win10/SiSyPHuS_node.html