**Westfälische Wilhelms-Universität
Wirtschaftswissenschaftliche Fakultät
Betriebliche Datenverarbeitung**

**Windows 10 Datenschutz**

**Kann Cortana per Default deaktiviert werden?**

Microsoft benutzt das Opt-out-Prinzip, das bedeutet, dass alle Einstellungen von Anfang an aktiviert sind und diese von dem Anwender deaktiviert werden müssen. Bei dem ersten einrichten von Windows 10 können schon mehrere Datenschutzeinstellungen deaktiviert werden:

-Drei Einstellungen zur Personalisierung

-Eine Einstellung zur Position

-Zwei Einstellungen zum Browserschutz

-Drei Einstellungen zur Verbindungs- und Fehlerberichterstattung

**Kann Cortana so konfiguriert werden, dass ein Anwender Cortana selbständig aktiviert?**

Cortana kann während der Installation per Script deaktiviert werden. So kann jeder Anwender selbst entscheiden ob er Cortana wieder aktivieren möchte.

CMD-Befehl: „reg.exe delete "HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search" /v AllowCortana /f“

**Wie können die Datenschutzeinstellungen unter Windows 10 zunächst deaktiviert werden?**

Die Datenschutzeinstellungen können über die GPOs dauerhaft deaktiviert werden oder manuell über die Systemeinstellungen oder per Script. Die GPO soll unter „Computerkonfiguration/Richtlinien/Administrative Vorlagen/Windows-Komponenten/Suche zu finden sein.

**Wie können die Datenschutzeinstellungen durch den Anwender selbst aktiviert werden?**

Die Datenschutzeinstellungen können ohne Administratorrechte über die Systemeinstellungen deaktiviert / aktiviert werden.

**Soll der Anwender jede Datenschutzeinstellung selber aktivieren / deaktivieren können?**

**Einbindung des OneDrive-Laufwerks ermöglichen**

One-Drive kann ohne Probleme vom Anwender ohne Administratorrechte eingebunden werden. Für die Einbindung von One-Drive wird nur das Microsoft-Konto benötigt. Das Microsoft-Konto wird nur für One-Drive hinterlegt.

Einstellungen/Datenschutz:

Allgemein:

Unter Allgemein können 4 Datenschutzoptionen geändert werden.

1. Apps die Verwendung der Werbungs-ID für APP-übergreifende Erlebnisse erlauben (Bei Deaktivierung wird Ihre ID zurückgesetzt)

Die Windows-ID wird beim Erstellen des Benutzerkontos erstellt. Die Windows-ID wird dafür benötigt, um zugeschnittene Werbung über die Drittanbieter-Apps anzeigen zulassen.

1. SmartScreen-Filter einschalten, um von Windows Store-Apps verwendete Webinhalte (URLS) zu überprüfen.

 Die URL der Webseite wird von Microsoft überprüft. Sollte diese als Malware erkannt werden, wird diese vom Browser geblockt.

1. Informationen zu meinem Schreibverhalten an Microsoft senden, um die Eingabe- und Schreibfunktionen in Zukunft zu verbessern.

Hier kann festgelegt werden, dass Microsoft keine Informationen über Ihr Schreibverhalten zugesendet bekommt. Damit das Schreibverhalten an Microsoft geschickt wird muss unter „Feedback und Diagnose“ bei „Diagnose- und Nutzungsdaten“ mindestens „Verbessert“ ausgewählt sein.

1. Website den Zugriff auf die eigene Sprachliste gestatten, um die Anzeige lokal relevanter Inhalte zu ermöglichen

**Position:**

Hier kann ausgestellt werden, dass die autorisierten Apps und Dienste keine Position-Informationen erhalten. Dies gilt sehr wahrscheinlich nur für Gräte mit GPS. Auch wenn die Einstellung deaktiviert ist können laut Microsoft die Drittanbieter über andere Technologien den Standort ermitteln, wie z.B. Bluetooth oder WLAN: "Apps können auch andere Technologien verwenden, z.B. Bluetooth oder die WLAN-Suche, um den Standort Ihres Geräts zu ermitteln, selbst wenn der Windows-Positionsdienst bei Ihrem Gerät deaktiviert ist."

Solang das Internet verwendet wird, kann nicht ausgeschlossen werden das Apps oder Dienste Standortdaten erfassen.

**Kamera:**

Von Anfang an können Programme wie der Browser Edge aber auch Seiten wie Facebook und Twitter, aber auch Apps über die Kamera des Geräts zugreifen.

**Mikrofon:**

Sowie bei der Kamera können auch Programme auf das Mikrofon zugreifen. Hier empfiehlt sich einzelne Programme wie z.B. Microsoft Edge den Zugriff zu verbieten. Wenn das Mikrofon für Skype verwendet wird, sollte nicht eingestellt werden das keine App es verwenden darf.

**Spracherkennung, Freihand und Eingabe:**

Diese Einstellung wird für Cortana verwendet. Es werden verschiede persönliche Informationen gesammelt und an Microsoft gesendet, wie z.B. Kontakte, aktuelle Kalenderereignisse, Sprach- und Handschiftmuster sowie der Eingabe-Verlauf. Ob alles an Microsoft gesendet wird, was an Cortana gesagt wird, ist noch nicht sicher. Wenn diese Einstellung deaktiviert wird kann Cortana nicht mehr verwendet werden.

**Kontoinformationen:**

Dort kann der Zugriff auf die Kontoinformationen für Apps deaktiviert werden.

**Kontakte:**

Dort kann der Zugriff auf die Kontakte für einzelne Apps und Dienste deaktiviert werden.

**Kalender:**

Dort kann der Zugriff auf die Kalendereinträge für einzelne Apps und Dienste deaktiviert werden.

**Messaging:**

Sollte diese Einstellung aktiviert sein, können dritt Anbieter Nachrichten Lesen und versenden. Hier können auch einzelne Apps und Dienste deaktiviert werden.

**Funkempfang:**

Hier kann der Funkempfang für Apps deaktiviert werden

**Weitere Geräte:**

Dort können Geräte ausgewählt werden mit denen Informationen ausgetauscht werden. Welche Informationen ausgetauscht werden hängt von den Apps und Geräten ab.

**Feedback und Diagnose:**

Die Feedbackabfrage kann ganz einfach ausgestellt werden. Das Senden von Diagnose- und Nutzerdaten kann in diesen Einstellungen nur auf „Einfach“ gestellt werden. Um es ganz auszustellen muss im Registry Editor umgestellt werden.

Anleitung unter: „https://www.reddit.com/r/Windows10/comments/3f38ed/guide\_how\_to\_disable\_data\_logging\_in\_w10/“

Laut Microsoft sollen bei der Einstellung „ Vollständig“ keine persönlichen Informationen an Microsoft gesendet werden, mit denen man identifiziert, kontaktiert werden kann oder gezielte Werbung geschaltet wird. Hauptsächlich Informationen zu Feedback- und Diagnoseeinstellungen.

Bei den Versionen Enterprise- und Education-Editionen von Windows, sowie in den Server- und loT-Ausgaben kann über einer GPO noch eine letzte Stufe eingestellt werden. Diese Stufe nennt sich „nullte“ und dort werden noch weniger Informationen als bei „einfach“ an Microsoft übertragen. Sollte die Stufe auf „nullte“ stehen werden keine Updates von Microsoft angeboten, da nicht überprüft werden kann welche Updates schon installiert wurden. (GPO-Pfad: „Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Datensammlung und Vorabversionen/Telemetrie zulassen“)

Was bei den einzelnen Stufen übertragen wird:

Stufe „nullte“: Maschinenkennung, die installierte Windows-Version und die Geräteklasse.

Stufe „einfach“: mehr Informationen über das Gerät (Prozessortyp, Haupt- und Massenspeicher, Kamera- und Display-Auflösung, Akkukapazität, ob Windows in einer virtuellen Maschine läuft), System- und Anwendungsabstürze, Speicherverbrauch, CPU-Belastung durch Anwendungen, installierte Anwendungen, Internet-Explorer-Add-ons, Treiber mit der jeweiligen Version und angeschlossene Geräte.

Stufe „verbessert“: Ereignisse (fehlgeschlagene Updates, Installation von Treibern, Problemberichte aus der Systemsteuerung, System- und Anwendungsabstürze(dazu kann auch ein Hauptspeicherabbild übertragen werden, das auch sensible Daten beinhalten kann))

Stufe „vollständig (empfohlen)“: Mitarbeiter kann sich mit dem Rechner verbinden, um schwere Fehler zu untersuchen. Es wird ihm dadurch genehmigt Programme wie msinfo32 oder dxdiag laufen zulassen, Registry-einträge lesen und setzen. Auch auf die Daten die bei dem Absturz beigetragen haben können eingesehen werden.

**Konten:**

Diese Einstellung wird nur angezeigt, wenn ein Microsoft-Konto auf dem Rechner angemeldet ist. Die Einstellung ist unter „Systemeinstellungen/Konten/Einstellungen synchronisieren“ zu finden. In den Einstellungen kann die Synchronisation der Benutzerkontos-Einstellungen eingestellt werden. Bei der Synchronisation wird der Browserverlauf, WLAN-Passwörter sowie Passwörter für Webseiten gespeichert.

**WLAN-Einstellungen:**

Es ist Voreingestellt, dass sich das Gerät automatisch mit von Microsoft anerkannten öffentlichen Hotspots verbindet. Die WLAN-Einstellungen können für Freunde bei Skype, Outlook und Facebook freigeben werden, sodass sie sich damit automatisch verbinden. Diese Funktion war schon bei Windows 8.1 verfügbar.

**Edge:**

Bei dem neuen Browser von Microsoft kann unter „Erweiterte Einstellungen“ der Flash Player deaktiviert werden. Damit der Browser-Verlauf nicht an Microsoft gesendet wird, muss die Einstellung Seitenvorhersage deaktiviert werden.

**Windows 10 Updates (Peer to Peer):**

Windows Updates können über andere Rechner, die das Update schon installiert haben, aus dem LAN-Netzwerk oder auch übers Internet bekommen. Die Einstellung ist unter „Einstellungen/Update und Sicherheit/Windows Update/Erweiterte Optionen/Übermittlung von Updates auswählen“ zu finden. Dort kann die Einstellung deaktiviert werden oder „PCs in meinem lokalen Netzwerk“ oder „PCs in meinem lokalen Netzwerk und PCs im Internet“ ausgewählt werden. Standards gemäß ist „PCs in meinem lokalen Netzwerk“ eingestellt. Microsoft versichert, dass keine manipulierten Updates verteilt werden können, da sie durch spezielle Verschlüsslungs- und Signaturtechnik verschlüsselt sind.

**Cortana:**

Cortana kann nur im vollen Umfang verwendet werden, wenn die Datenschutz-Einstellung Kennenlernen erlaubt ist. Diese Einstellung ist unter „Spracherkennung, Freihand und Eingabe“ zu finden. Dazu muss noch die Standort Freigabe, Kalender und Messaging für Cortana aktiviert werden. Für Cortana wird ein Microsoft-Konto benötigt.

Cortana kann mithilfe einer .cmd Datei deinstalliert werden. Beim Deaktivieren von Cortana läuft der Prozess „SearchUI.exe“ im Hintergrund weiter und kann eine Menge Speicher belegen.

„<http://www.giga.de/downloads/windows-10/tipps/windows-10-cortana-deinstallieren-so-geht-s/>“

CMD-Befeh um Cortana zu deaktivierenl: „reg.exe delete "HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search" /v AllowCortana /f“

**Tools:**

**DoNotSpy10:**

-muss installiert werden

-sammelt Informationen über die Software-Ausstattung

-Anwendungen zum mitinstallieren werden angeboten

-42 Checkboxen mit Kurzbeschreibung

**Windows 10 Privacy-Settings:**

**-**muss nicht installiert werden

-nimmt Einstellungen in der Registry vor und beendet sich dann wieder

-Anwender sieht nicht welche Einstellungen vorgenommen werden.

**W10Privacy:**

-muss nicht installiert werden

-steht laut Entwickler noch in einem frühen Entwicklungsstadium

-Settings lassen sich speichern und wieder aufrufen

-hat die größte Sammlung bis jetzt

-nicht sehr übersichtlich dank den ganzen Einstellungen

-Beschreibungen zu den einzelnen Einstellungen fallen sehr knapp aus.

**O&O ShutUp10:**

-muss nicht installiert werden

-ca. 50 Einstellungsmöglichkeiten

-sortiert in sechs Kategorien

-Bewertung nach „Empfohlen“, „Eingeschränkt“ und „Besser nicht“

-Alle Schalter lassen sich auf einmal umlegen

-Erklärung zu den einzelnen Einstellungen sind vorhanden, doch nicht immer korrekt formuliert.

Laut dem Magazin c’t fällt die Bedienfreundlichkeit beim O&O ShutUp10 am besten aus.