

# IM „Redmond“

Sehr geehrte Leserinnen und Leser,

falls Sie LinuxUser schon länger lesen, dann wundern Sie sich vielleicht, dass der Titel der vorliegenden Ausgabe das brandneue Windows 10 mit keiner Silbe erwähnt. Viele Jahre boten wir beim Erscheinen neuer Microsoft-Releases zeitnah einen passenden Schwerpunkt zur Koexistenz mit Linux an. Das läge diesmal eigentlich noch näher als bisher, denn zum ersten Mal muss man ein neues Windows nicht kaufen, sondern erhält es als kostenloses Upgrade aus Redmond. Doch „kostenlos“ heißt: Hier sind der Benutzer und seine Daten die Ware.

Windows 10 treibt dieses wohlbekannte Paradigma in einer Art und Weise auf die Spitze, bei der sich die Nackenhaare sträuben [☞](#). Was Microsoft dem Benutzer hier unterschiebt, hat nichts mehr mit den üblichen Werbesperenzchen zu tun. Klar, die gibt es auch – wie etwa eine Werbe-ID, über die Microsoft Ihre Daten mit Drittanbietern teilt, und andere Späße dieser Art. Doch die Voreinstellungen erlauben Windows 10 viel mehr.

So kann es etwa „Informationen zum Schreibverhalten an Microsoft senden, um die Eingabe- und Schreibfunktionen in Zukunft zu verbessern“ – quasi ein eingebauter Keylogger. Parallel nimmt Windows 10 eine Standortbestimmung vor. Stellen Sie diesen Ortungsdienst ab, dann dürfen „Apps auch andere Technologien verwenden, z.B. Bluetooth oder die WLAN-Suche, um den Standort Ihres Geräts zu ermitteln“. Es lässt sich also praktisch nicht verhindern, dass Windows 10 Ihren Standort weitermeldet.

Damit nicht genug: Laut Voreinstellung dürfen Programme wie der Webbrowser Edge, aber auch Facebook, Twitter und weitere Apps auf die Kamera und das Mikrofon des Geräts zugreifen. Über den Assistenten Cortana sammelt Microsoft „Informationen wie Kontakte, aktuelle Kalenderereignisse, Sprach- und Handschriftmuster sowie den Eingabeverlauf“. Das Übertragen von „Diagnose- und Nutzungsdaten“ lässt sich nicht verhindern, nur beschränken. Für das Synchronisieren über mehrere Geräte speichert Microsoft nicht nur automatisch den Browserverlauf auf seinen Servern, sondern auch WLAN- und Website-Passwörter.

Eine genaue Erklärung, wer sich wozu an dieser Flut persönlicher Daten bedienen darf, bleibt Microsoft schuldig [☞](#). „Mitarbeiter, Auftragnehmer, Lieferanten und Partner“ erhalten „möglicherweise“ Zugriff auf „relevante Teile der gesammelten Informationen“, heißt es seitens des Unternehmens lapidar. Manche der Voreinstellungen lassen sich zwar deaktivieren, doch die Einstellungen verstreuen sich über zahlreiche Dialoge. Um überhaupt keine Daten an Microsoft zu senden, müssten Sie schon spezielle Tools wie den Registry-Editor Regedit und den Group-Policy-Editor Gpedit bemühen.

Um es noch einmal unmissverständlich zusammenzufassen: Mit der Benutzung von Windows 10 erteilen Sie Microsoft die Erlaubnis mitzuschneiden, wie Sie sich durchs Netz bewegen und wann Sie wo welche Daten an Ihrem Computer eingeben. Dabei kann der Rechner Sie gegebenenfalls auch noch filmen und abhören. Das wäre per se schon ungeheuerlich genug; hinzu kommt die wohlbekannte Tatsache, dass Microsoft innigst mit den US-Geheimdiensten kooperiert [☞](#).



Jörg Luther  
Chefredakteur

Die Free Software Foundation (FSF) zieht daraus folgendes Fazit [☞](#): „Die FSF empfiehlt dringend, von der Benutzung von Windows 10 Abstand zu nehmen. [...] Da [das Betriebssystem] grundlegend unsicher ist und die Privatsphäre nicht achtet, stellt Windows 10 ein offenes Fenster auf Sie dar. Es sperrt Sie ein und unabhängige Experten aus – damit verschließt es Ihnen die Tür zu Ihrem PC, und nur Microsoft hat den Schlüssel.“

Auch ich rate von der Verwendung eines solch abgefeimten Bespitzelungssystems dringend ab und kann dessen Einsatz nicht guten Gewissens unterstützen. Deswegen wird dieses Editorial die einzige Stelle bleiben, an der Sie in LinuxUser etwas über Windows 10 lesen.

Herzliche Grüße,



Weitere Infos und  
interessante Links

[www.linux-user.de/qr/35325](http://www.linux-user.de/qr/35325)