Team Datenschutz | K 3 – DS
TU Berlin |Straße des 17. Juni 135 | 10623 Berlin

An alle Einrichtungen der TUB

Team Datenschutz

Annette Hiller
+49 30 314-**21784**
Raum H 1038

Alexander Hoffmeier
+49 30 314-**29595**
Raum H 1042

Dr. Mattis Neiling
+49 30 314-**28973**
Raum H 1042

info@datenschutz.tu-berlin.de

Fax +49 30 314-28033

Unser Zeichen:
K3 - DS

Berlin, 19. Mai 2020

Empfehlungen zum Datenschutz-konformen Einsatz von Windows 10 auf privaten Geräten zur dienstlichen Nutzung beim mobilen Arbeiten

Version 1.0

Liebe Kolleg*innen,

im Sommersemester 2020 findet an der TU Berlin kein regulärer Präsenzbetrieb statt, so dass wir überwiegend von Zuhause im Home-Office (Mobilen Arbeiten) sind. Das ist nicht immer ganz einfach, einerseits da oft die Arbeitsumgebung nicht so gut eingerichtet werden kann wie am dienstlichen Arbeitsplatz und andererseits zumeist die ganze Familie mit den Computern und anderen mobilen Geräten arbeiten möchte.

Da nicht jede*r auf ein eigenes dienstliches Gerät zurückgreifen kann, möchten wir Ihnen eine Hilfestellung geben, wie Sie auch auf privaten Geräten datenschutzkonform und sicher arbeiten können.

Wir bitten Sie um Ihr Verständnis, dass Sie Zeit und Aufwand in die empfohlene Konfiguration von Windows 10 investieren sollen.

Diese Empfehlungen stellen den aktuellen Stand unserer Erkenntnisse dar und werden von uns regelmäßig aktualisiert. Schauen Sie bitte auf unserer Datenschutz-Webseite nach, dort publizieren wir ausführliche **Schritt-für-Schritt-Anleitungen**:

- https://www.tu-berlin.de/asv/menue/datenschutz/

Das Betriebssystem: Windows 10

Windows 10 ist das überwiegend genutzte Betriebssystem - für die dienstliche Nutzung sind die Home- und Pro-Editionen auf privaten Geräten nutzbar, auch wenn diese aus Datenschutz-Sicht weniger sicher sind als die für dienstliche Rechner lizensierten Education- und Enterprise-Editionen.

Sofern Sie noch Geräte mit Windows XP oder Windows 7 besitzen, empfehlen wir Ihnen zu prüfen, ob ein Update auf Windows 10 möglich ist. Die älteren Windows-Versionen werden nicht mehr von Microsoft unterstützt und dürfen deshalb nicht dienstlich genutzt werden, da Sicherheitsprobleme auftreten können.

Auch bei Windows 10 ist es wichtig, **Sicherheitspatches** und weitere von Microsoft bereitgestellte **Updates** zu installieren, da leider regelmäßig Sicherheitsprobleme auftreten. Zusätzlich sollten auch regelmäßig die vom Gerätehersteller bereitgestellten **Treiber- bzw. Firmware-Updates** eingespielt werden, da diese zunehmend Angriffen ausgesetzt sind.

Richten Sie regelmäßig **System-Wiederherstellungspunkte** ein, damit Sie nach Installation verschiedener Programme wieder zu einem vordefinierten Systemzustand zurückkehren können – oft wird das Betriebssystem langsamer oder ein durch ein neues Programm auftretendes ungewünschtes Verhalten ist nicht ohne Weiteres abstellbar. Da bei einer System-Wiederherstellung auch Daten zurückgesetzt werden, ist eine vorherige Datensicherung empfehlenswert.

- Schritt-für-Schritt-Anleitung: System-Wiederherstellungspunkt setzen

Insbesondere bei mobilen Geräten ist eine **Verschlüsselung der Systemfestplatte** angeraten, damit die Daten im Falle eines Geräteverlusts nicht in falsche Hände gelangen.

- Schritt-für-Schritt-Anleitung: Windows Systemfestplatte verschlüsseln

Sichern Sie Ihre Daten regelmäßig auf einem verschlüsselten externen Backup-Medium, damit Sie im Falle eines Datenverlusts darauf zurückgreifen können.

Achten Sie bitte darauf, dass die **Windows Firewall** und **Microsofts Virenschutzprogramm Defender** standardmäßig aktiviert sind.

*Bei Bedarf kann ein alternatives **Virenschutzprogramm** installiert werden, bspw. steht für Mitglieder der Universität **Sophos Antivirus** auch für private Geräte zur Verfügung. Wir empfehlen allerdings, es **ohne Sophos Firewall** zu installieren, da Probleme mit der Internetverbindung und beim Laden der Treiber-Updates vom Hersteller auftraten.*

Lokale Benutzerkonten einrichten und schützen

Generell empfehlen wir auch Zuhause den Computer mit einem Passwort zu schützen. Für die tägliche Nutzung sollten Benutzerkonten ohne administrative Rechte genutzt werden.

Eine Registrierung mit einem Microsoft-Konto ist weder erforderlich noch aus Datenschutzsicht empfehlenswert, da dann auch personenbezogene Daten in der Microsoft-Cloud gespeichert werden.

Bei neuen Geräten ist meist ein Benutzerkonto eingerichtet, das administrative Rechte hat. Richten Sie mit diesem zwei weitere Benutzerkonten ein, so dass insgesamt mindestens drei Benutzerkonten vorhanden sind:

- ein **lokales Administrations-Benutzerkonto**, mit dem die Basiskonfiguration und die Installation der gewünschten Software gepflegt wird,
- ein **lokales Standard-Benutzerkonto** für jede Person, die das Gerät für **dienstliche Zwecke** nutzt und
- ein oder mehrere (lokale) **Standard-Benutzerkonten** für die **private Nutzung**.

Das separate dienstliche Benutzerkonto ist erforderlich, damit personenbezogene und andere dienstliche Daten, Dokumente und Programme Dritten nicht zugänglich sind, auch nicht Familienmitgliedern.

- Schritt-für-Schritt-Anleitung: Benutzerkonten in Windows 10 verwalten

Bei Windows 10 kann ein Standardbenutzer Einstellungen anpassen und Apps aus dem Microsoft Store installieren. Lediglich bei sogenannten Desktop-Apps werden administrative Rechte benötigt.

Viele Angriffsszenarien nutzen administrative Zugriffsrechte aus, um tief in das Betriebssystem einzugreifen, z.B. um Backdoor-Programme zu installieren.

Software-Programme einrichten und überflüssige vorinstallierte Apps löschen

Für die tägliche Nutzung des Computers können Sie weitere Programme installieren. Sie benötigen dafür administrativen Rechte.

Wir empfehlen folgende Desktop-Apps - mit einem Asterix (*) sind die Programme markiert, die für eine **nichtkommerzielle Nutzung auf privaten Geräten** über die Webseiten der TU verfügbar sind:

- **Cisco Anyconnect*** als VPN Client
- **Sophos Antivirus*** als alternative Virenschutz-Software
- **Libre Office** als alternatives Office-Paket
- **Mozilla Thunderbird** als E-Mail-Client
- **Mozilla Firefox** als Internet-Browser
- **Chromium** oder **Google Chrome** als Ergänzung, da manche Websites nur damit vernünftig funktionieren
- **KeypassXC** zur Verwaltung von Passwörtern
- **PDF24** zur Erstellung und Kommentierung von PDF-Dokumenten
  (zum Anzeigen von PDF-Dokumenten genügt der Internet-Browser Microsoft Edge)

Installieren Sie die Software-Produkte nur aus vertrauenswürdigen Quellen, beispielsweise direkt vom Hersteller, sofern sie nicht über die TU verfügbar sind.

- Empfohlene Software-Produkte für Windows 10 mit Download-Links

Auf den meisten Geräten sind einige Apps aus dem Microsoft Store vorinstalliert, die nicht benötigt werden, zumindest nicht für den dienstlichen Gebrauch. Welche Apps bereits installiert sind, hängt vom Hersteller ab, oft sind auch spezifische Tools als App mit installiert, die nicht gelöscht werden sollten.

Die Apps werden für jedes Benutzerkonto getrennt verwaltet, d.h. im privaten Konto können andere Apps verfügbar sein als im dienstlichen Benutzerkonto. Unsere Empfehlungen beziehen sich auf das separate dienstliche Benutzerkonto. Auf dem von uns untersuchten Gerät waren einige Apps vorinstalliert, die mit den Rechten des dienstlichen Benutzerkontos als Standardbenutzer gelöscht werden konnten, u.a.:

- Amazon, Booking.com, Dropbox, LinkedIn, McAfee (als 1.-Jahr-kostenlos-Abo), Skype, Xing

Erfreulicherweise waren Facebook, Twitter und Instagram nicht vorinstalliert.

Bei Bedarf können in jedem Benutzerkonto weitere Apps aus dem Microsoft Store auch ohne Microsoft-Konto installiert werden.

- Schritt-für-Schritt-Anleitung: Apps in einem Windows-Benutzerkonto verwalten

Datenschutz-Einstellungen anpassen

In Windows 10 kann der Zugriff auf Daten, Standort, Mikrofon, Kamera und vieles mehr granular eingestellt werden. Einige Datenschutz-Einstellungen können für das Gerät durch einen Administrator als sogenannte Richtlinie festgelegt werden und damit alle Benutzerkonten steuern, wobei sich viele Einstellungen in den einzelnen Benutzerkonten ändern lassen. Deshalb sollten die Einstellungen für jedes Benutzerkonto geprüft und bei Bedarf angepasst werden.

Erfahrungsgemäß verändert Microsoft die Datenschutz-Einstellungen bei einem Systemupdate, so dass nach jedem Update eine kurze Überprüfung der Einstellungen angebracht ist.

Für den privaten Gebrauch können Sie die Einstellungen entsprechend Ihren Bedürfnissen anpassen. Im dienstlichen Benutzerkonto sind die Datenschutz-Einstellungen allerdings sehr streng vorzunehmen, z.B. sollten sowohl der **Sprachassistent Cortana deaktiviert** als auch der **Standort** und andere Daten nicht an Microsoft übertragen werden. Die Übertragung von **Telemetrie-Daten** lässt sich in Windows 10 Home und Pro leider nicht ganz abschalten, sondern nur minimieren.

Einige Einstellungen können für das Gerät mit administrativen Rechten als sogenannte Richtlinie festgelegt werden und damit alle Benutzerkonten steuern, diese Anpassungen beschreiben wir im ersten Teil der Anleitung:

- Schritt-für-Schritt-Anleitung: Windows 10 Datenschutz-Einstellungen anpassen (1)

Im zweiten Teil erläutern wir, wie Sie die Einstellungen für ein Benutzerkonto individuell anpassen können.

- Schritt-für-Schritt-Anleitung: Windows 10 Datenschutz-Einstellungen anpassen (2)

Bei einigen installierten Apps können individuelle Datenschutz-Einstellungen vorgenommen werden, z.B. bei Internet-Browsern und Microsoft Office (soweit Sie dieses nutzen).

Arbeiten mit Office, Cloud-Speicher und E-Mail-Programmen

Nutzen Sie die Open Source Software **Libre Office**, die wir aus Datenschutz-Sicht uneingeschränkt empfehlen. In der Zusammenarbeit im Team ist manchmal die Konvertierung/Umwandlung zwischen dem **Open Document Format** und den **Microsoft Office Dateiformaten** problematisch, so dass Sie sich dazu vorab auf ein Produkt für die gemeinsame Bearbeitung von Dateien abstimmen sollten.

Sofern Sie **Microsoft Office** lokal installiert haben, denken Sie bitte daran, dienstliche Dateien lokal zu speichern und nie in der Microsoft Cloud OneDrive.

Nutzen Sie als **Cloud-Speicher** ausschließlich die **tubcloud** (https://tubcloud.tu-berlin.de), speichern Sie dort aber weder vertrauliche noch personenbezogene Daten.

Der Zugang zu E-Mail, Kalender und Adressbuch soll mit einem geeigneten E-Mail-Client oder über den Outlook Web Access (https://exchange.tu-berlin.de) erfolgen. Nutzen Sie als E-Mail-Client Mozilla Thunderbird oder Microsoft Outlook.

- Informationen der ZECM zu E-Mail-Clients und Zugriff auf den Exchange Dienst

Achten Sie bitte darauf, dass Dokumente mit vertraulichen und/oder personenbezogenen Daten nicht in fremde Hände gelangen, schützen Sie beispielsweise Dokumente mit einem Passwort, bevor Sie diese per E-Mail versenden.

- Schritt-für-Schritt-Anleitung: Dateien mit Passwort schützen
- Personenbezogene Daten in E-Mails

Sicher unterwegs im Internet

Für viele dienstliche Aufgaben nutzen Sie das Internet, im Home-Office auch für Ressourcen, auf die Sie in der Universität direkt zugreifen können. Auch deshalb ist es wichtig aktuelle und sichere Software dafür zu nutzen, insbesondere bei den Webbrowsern darauf zu achten, dass sie nicht ungewollt Daten an Dritte übermitteln.

Auf den dienstlichen Computern ist zumeist auch der **Webbrowser Firefox** installiert, der als Open Source Software von der Mozilla Stiftung getragen wird. Wir empfehlen Ihnen, **Firefox als Standardbrowser** auf Ihren privaten Geräten zu nutzen, da er den bestmöglichen Schutz Ihrer Privatsphäre bietet.

Sofern Sie **Google Chrome** nutzen, empfehlen wir Ihnen auf **Chromium** zu wechseln, da dieser als Open Source Software weniger eng an Google gekoppelt ist.

Passen sie die Datenschutz-Einstellungen der von Ihnen genutzten Webbrowser an, wichtig sind unter anderem die Einstellungen zu Cookies und Websitedaten:

- Schritt-für-Schritt-Anleitung: Datenschutz-Einstellungen bei Firefox anpassen
- Schritt-für-Schritt-Anleitung: Datenschutz-Einstellungen bei Chromium und Google Chrome anpassen

Schützen Sie sich vor Aktivitätenverfolgung und ungefragt eingebunden externen Diensten in Webseiten

- Browser-Erweiterungen zum Schutz der Privatsphäre nutzen

Nutzen Sie einen Browser-übergreifenden sicheren **Passwort-Manager** für alle Webseiten, die eine Authentifizierung benötigen - wir empfehlen die Nutzung der Open Source Software **KeypassXC**.

- Download-Link in der Übersicht

Sofern Sie die browsereigenen Passwort-Manager zum Speichern von Zugangsdaten nutzen, sollten sie zumindest ein Masterpasswort verwenden, damit die Passwörter nicht gänzlich ungeschützt sind.

Weitere technische und organisatorische Maßnahmen

Nutzen Sie **VPN** für den Zugriff auf Ressourcen der TU, insbesondere in öffentlichen WLAN-Netzen. Als Software installieren Sie **Cisco AnyConnect**.

Lassen Sie Ihr Gerät nicht unbeaufsichtigt und bewahren Sie es bei Abwesenheit und Nichtnutzung ausschließlich in verschlossenen Räumen auf.

Schützen Sie die Benutzerkonten mit **Passwörtern**. Auf jeden Fall sollten alle Benutzerkonten mit administrativen Rechten sowie das separate dienstliche Konto mit nur Ihnen bekannten Passwörtern versehen sein. Das dienstlich genutzte Konto darf anderen nicht zugänglich sein.

Stellen Sie einen **Bildschirm-Timeout** ein, so dass bei Nichtbenutzung nach 5-10 Minuten eine Passwort-Eingabe erfolgen muss. Aktivieren Sie diese Sperre bei Bedarf mit **Windows-Taste + L** (L für „Lock“).

Vor **Außerbetriebnahme oder Weitergabe** eines Geräts soll eine Datensicherung (zumindest der dienstlichen Dateien) auf einem verschlüsselten externen Datenträger erfolgen sowie die Konfiguration zum Zugang zu dienstlichen Ressourcen zurückgesetzt werden. Denken Sie daran, alle lokal gespeicherten Daten zu löschen, einschließlich temporärer Dateien und Inhalte in Download-Ordnern. Am sichersten ist hierbei ein Neuformatieren der Festplatte mit anschließender Neuinstallation von Windows.

Bei **Verlust** eines Gerätes mit dienstlichen Daten benachrichtigen Sie bitte umgehend die Datenschutzbeauftragten, das Computer Emergency Response Team (CERT) sowie bei dienstlichen Geräten die zuständigen Administrator*innen.

Informationen der ZECM zu Windows 10 und Homeoffice

- Hinweise zur Nutzung von Windows 10
- Hinweise zur IT-Sicherheit und zum Datenschutz im Homeoffice
- Webseite des Computer Emergency Response Teams (CERT)

Schlussbemerkung

Dieses Dokument fasst unsere Empfehlungen zu Windows 10 zusammen, weitere Informationen finden Sie auf unserer Webseite und im Datenschutz-Blog, beispielsweise zur Nutzung von Videokonferenz-Tools:

- www.tu-berlin.de/asv/menue/datenschutz/
- blogs.tu-berlin.de/datenschutz_notizen/

Wir hoffen, Ihnen mit unseren Empfehlungen und umfangreichen Schritt-für-Schritt-Anleitungen eine Hilfestellung zum datenschutzsicheren Umgang beim mobilen Arbeiten geben zu können.

Wir freuen uns auf Ihr Feedback,

Ihr Team Datenschutz

Technische Universität Berlin

Anlage

Checkliste Datenschutz bei Windows 10

	Status	Ihre Anmerkungen / Datum
Systemfestplatte verschlüsselt	☐ Erledigt ☐ Später ☐ Nicht nötig	
Benutzerkonto mit administrativen Rechten eingerichtet	☐ Erledigt ☐ Später	
Separates dienstliches Benutzerkonto eingerichtet	☐ Erledigt ☐ Später	
Weitere Software-Produkte installiert	☐ Erledigt ☐ Später ☐ Nicht nötig	
System-Wiederherstellungs-punkt definiert	☐ Erledigt ☐ Später ☐ Nicht nötig	
Überflüssige Apps deinstalliert	☐ Erledigt ☐ Später ☐ Nicht nötig	
Office-Paket installiert und E-Mail-Client konfiguriert	☐ Erledigt ☐ Später ☐ Nicht nötig	
Windows Datenschutz-Einstellungen angepasst	☐ Erledigt ☐ Später	
Datenschutzeinstellungen für Firefox angepasst	☐ Erledigt ☐ Später	
Datenschutzeinstellungen für weiteren Browser angepasst	☐ Erledigt ☐ Später	
Browser-Erweiterung zum Schutz der Privatsphäre installiert	☐ Erledigt ☐ Später ☐ Nicht nötig	
Browser-übergreifenden Passwort-Manager eingerichtet	☐ Erledigt ☐ Später ☐ Nicht nötig	