Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: PRIVATE IT

Sichere Nutzung von Geräten unter Microsoft Windows 10

Empfehlungen für Privatanwender

1 Ausgangslage / Einleitung

Viele nützliche Dienstleistungen, wie Online-Banking, E-Commerce oder E-Government, werden heute über das Internet angeboten und genutzt. In Zukunft wird sich die Anzahl der Online-Services noch weiter erhöhen. Hinzu kommt der verstärkte Einsatz mobiler Endgeräte, wie Smartphones und Tablets, mit denen diese Dienste auch unterwegs genutzt werden können. Dennoch spielen derzeit auch Personal Computer (PCs) mit verschiedenen Betriebssystemen noch eine wichtige Rolle.

2 Ziel

Die vorliegende BSI-Veröffentlichung zur Cyber-Sicherheit bietet Hilfestellungen für eine sichere Basiskonfiguration eines Windows-PCs. Diese Empfehlung behandelt das Betriebssystem Microsoft Windows 10 in kleinen Umgebungen ohne Einsatz der Active Directory Dienste. Wenngleich Windows 10 auch auf Tablets und Smartphones eingesetzt werden kann, steht im vorliegende Dokument der Einsatz von Windows 10 auf Personal Computern im Mittelpunkt. Viele der genannten Punkte sind aber auf andere Geräte übertragbar. Das Dokument ist grundsätzlich für alle Editionen anwendbar, etwaige Einschränkungen bei den Editionen werden an den betreffenden Stellen ausdrücklich hervorgehoben.

Zur Festlegung der geeigneten Maßnahmen bietet sich zunächst die Betrachtung des Lebenszyklus eines Rechners an:

- Entscheidungen vor der Installation
- Installation und Inbetriebnahme
- Geregelter Betrieb
- Entsorgung des Systems

3 Vorbereitung vor der Inbetriebnahme

Bereits bei der Anschaffung des Systems gibt es wichtige Aspekte, die Sie für den sicheren Betrieb eines PCs beachten sollten.

3.1 Auswahl von Hardware und Betriebssystem

Achten Sie auf die Verwendung möglichst aktueller Hardware. Um die von Windows bereitgestellten Sicherheitsmechanismen vollständig nutzen zu können, müssen bestimmte Anforderungen erfüllt werden. Eine Aufstellung, welche Hardware-Voraussetzungen für welche Funktionalität in Windows 10 gegeben sein müssen, finden Sie unter https://www.microsoft.com/de-de/windows/windows-10-specifications.

Das Betriebssystem Windows 10 ist in mehreren Editionen mit unterschiedlichen Funktionen erhältlich. Eine Übersicht über die Funktionen der unterschiedlichen Editionen finden Sie unter https://www.microsoft.com/de-de/windows/compare. Darüber hinaus sind kompatible IT-Systeme im Handel in der Regel auch mit einem Windows 10 Logo gekennzeichnet.

3.2 Virenschutzprogramm (Auswahl und Beschaffung)

Virenschutzprogramme stellen einen Basisschutz gegen bereits bekannte Schadsoftware und häufig auch gegen möglicherweise unerwünschte Anwendungen (Potenziell unerwünschte Anwendung - PUA) dar..

Im Funktionsumfang von Windows 10 ist mit dem Windows Defender bereits ein Virenschutzprogramm enthalten. Windows Defender ist automatisch aktiviert, wenn kein anderes Virenschutzprodukt installiert ist, und bietet durch seinen Echtzeitschutz und Integration in die Microsoft Browser Internet Explorer und Edge einen Basisschutz. Da diese tiefe Integration in Drittprodukten, wie Browsern und E-Mail-Client-Programmen, nicht zur Verfügung gestellt wird, kann der Einsatz eines alternativen Virenschutzprogramms, das ähnliche Schutzmechanismen für diese Programme bietet, Vorteile bringen.

Entscheiden Sie sich für ein Virenschutzprogramm, das in seinem Funktionsumfang Ihren Anforderungen entspricht und, basierend auf Ergebnissen unabhängiger Testinstitute, eine möglichst gute Erkennungsleistung aufweist. Betreiben Sie Ihr System nicht ohne aktuelles Virenschutzprogramm und beachten Sie unbedingt die regelmäßig notwendige Verlängerung der Lizenz (in der Regel nach 12 Monaten).

Kostenfreie Virenschutzprogramme verfügen unter Umständen über einen geringeren Funktionsumfang als kostenpflichtige Produkte und sind häufig werbefinanziert. Zudem beinhalten meist nur die kostenpflichtigen Produkte bei Problemen technische Unterstützungsleistungen durch den Hersteller. Informieren Sie sich über aktuelle Testberichte zum Leistungsumfang von Virenschutzprogrammen, beispielsweise auf www.av-test.org, www.av-comparatives.org oder www.test.de.

3.3 Backups

Um Sicherungskopien von Ihrem System und Ihren Daten zu erstellen, können Sie die in Windows 10 eingebaute Funktionalität verwenden. Der Kauf einer gesonderten Backup-Software ist für Windows 10 im Allgemeinen nicht erforderlich. Sie sollten zudem darauf achten, dass ein regelmäßiges Backup durchgeführt wird, um den Datenbestand aktuell zu halten, und dass Sie hierbei gegebenenfalls verschiedene Speichermedien nutzen. Zudem sollte berücksichtigt werden, dass Speichermedien unter Umständen nach einiger Zeit nicht mehr lesbar sind.

Weitere Hinweise zur Datensicherung finden Sie im Abschnitt 5.2, Erstellen regelmäßiger Datensicherungen.

3.4 Verwendung zusätzlicher Software

Mit dem Funktionsumfang eines Systems steigt auch dessen Angriffsfläche. Sie sollten Ihr System daher nur um Anwendungen bzw. Programme und Apps erweitern, die Sie tatsächlich benötigen.

Anwendungsprogramme:
Bei allen zusätzlichen Anwendungsprogrammen, die Sie etwa zur Bearbeitung von Fotos oder die Erstellung von Dokumenten nutzen, sollten Sie darauf achten, dass die Software-Produkte mit einer Funktion zur automatischen Aktualisierung ausgestattet sind.

In der Regel lässt sich dies unter dem Menüpunkt *Einstellungen* in der jeweiligen Software überprüfen und konfigurieren. Updates sollten idealerweise ohne Ihr Zutun automatisch im Hintergrund installiert werden. Verbreiteter sind Aktualisierungsfunktionen, die Sie bei verfügbaren Updates benachrichtigen. Die Installation sollten Sie stets zeitnah durchführen.

Windows Apps:
In Windows 10 besteht über den Windows Store die Möglichkeit, ähnlich den bekannten App-Stores von mobilen Endgeräten, Zusatzprogramme und -spiele zu installieren. Die Apps können Sie teilweise kostenlos oder gegen eine Gebühr beziehen. Anstehende Aktualisierungen von Apps werden durch den Windows Store automatisiert ohne explizites Zutun durchgeführt. Genauso können diese Apps aber durch Microsoft auch wieder entfernt werden (sowohl aus dem Windows Store als auch von Ihrem PC).

3.5 Entscheidung zur Nutzung von Cloud-Diensten

Mit Windows 10 vollzieht Microsoft den Wandel von einem autarken zu einem online- bzw. Cloud-integrierten Betriebssystem. Im Gegensatz zu den vorherigen Windows-Versionen, die für den autarken Betrieb mit lokaler Datenhaltung und optionaler Nutzung von online angebotenen Dienstleistungen wie Online-Banking, E-Commerce oder E-Government optimiert waren, sind Cloud-Funktionen tief im Betriebssystem integriert. Online-basierende Dienste ermöglichen Sprachsteuerung und vereinfachte Bedienung des Personal Computers (Cortana), automatisierte online-Sicherungen (OneDrive) sowie geräteübergreifend einheitliche Benutzerprofile und Datenbestände bzw. -zugriffe bei der Nutzung von mehreren PCs oder auch mobilen Geräten, wie Tablets und Smartphones.

Viele der funktionalen Neuerungen von Windows 10, wie etwa die mittels Spracheingabe steuerbare Assistenzfunktion Cortana, erfordern den umfangreichen Zugriff auf persönliche Daten, wie Kontakte und Kalendereinträge, und ihre Übermittlung an Microsoft. Eine Beschränkung der Datenzugriffe ist teilweise nur eingeschränkt möglich und oftmals mit funktionalen Beschränkungen verbunden.

Weiterhin werden von verschiedenen Anbietern zusätzliche Cloud-Dienste angeboten, die die klassischen Office-Suiten ersetzen oder ergänzen. Darunter fallen unter anderem Textverarbeitung, Tabellenkalkulation, E-Mail, Internet-Telefonie und Speicherdienste. Bei der Nutzung solcher Cloud-Dienste teilen Sie persönliche oder geschäftliche Daten mit dem Anbieter bzw. Verarbeiten Ihre Daten auf dessen IT-Systemen und gewähren entsprechend die mit der Nutzung akzeptierten Allgemeinen Geschäftsbedingungen der Dienstleister. Hierin kann auch die Weitergabe Ihrer Daten an andere Unternehmen enthalten sein.

Bereits vor der Installation von Windows 10 bzw. der Nutzung ergänzender Cloud-Dienste sollten Sie daher für sich bewerten, ob und in welchem Umfang Sie dazu bereit sind, persönliche oder geschäftliche Daten mit dem jeweiligen Dienstanbieter zu teilen, um diese Dienste für sich nutzen zu können.

Bei der Entscheidungsfindung sollten auch die jeweiligen Regelungen der Datenschutzbestimmungen der Anbieter mit einbezogen werden. Die entsprechenden Regelungen von Microsoft finden Sie unter diesem Link: https://privacy.microsoft.com/de-de/privacystatement

Bei der Wahl der zu nutzenden Online-Dienste sollten Sie zudem die jeweiligen Allgemeinen

Geschäftsbedingungen gewissenhaft prüfen. Einzelne Anbieter lassen sich durch die Nutzung der Dienste Rechte an den dort verarbeiteten Inhalten einräumen. Dies kann unter Umständen Ihren Interessen oder rechtlichen Verpflichtungen entgegenstehen.

4 Installation und Inbetriebnahme

Einen wichtigen Grundstein für die Systemsicherheit Ihres PCs können Sie bereits bei der Installation und ersten Inbetriebnahme des Rechners legen.

4.1 Installation und Initialisierung

Sollte Microsoft Windows 10 nicht bereits vorinstalliert sein, so führen Sie zunächst eine vollständige Neuinstallation von Windows 10 durch. Bei einem vorinstallierten Windows-Betriebssystem sind meist weitere Software-Produkte vorinstalliert. Diese sollten auf ihre Lizenzdauer, die unter Umständen zeitlich beschränkt ist, geprüft werden. Nicht benötigte Software-Produkte sollten Sie deinstallieren.

Falls Sie einen bestehenden Rechner mit einem älteren Betriebssystem besitzen, können Sie diesen auf Windows 10 aktualisieren, wenn die Hardware-Voraussetzungen gegeben sind. Bei der Installation werden Sie gefragt, ob Sie Ihre bestehenden Daten übernehmen möchten. Vor der Aktualisierung sollten Sie dennoch eine vollständige Sicherung Ihrer Daten vornehmen, um Datenverlusten im Störungsfall vorzubeugen.

Bitte stellen Sie für den Installationsvorgang sicher, dass Ihr PC über eine funktionierende Internetverbindung verfügt, sodass anstehende Sicherheitsaktualisierungen durch die Installationsroutine direkt installiert werden können.

Die während des Installationsvorgangs vorgeschlagenen Expresseinstellungen sollten Sie nicht übernehmen. Stattdessen können Sie über die Option „Einstellungen anpassen“ selbst festlegen, welche Daten Sie mit Microsoft teilen möchten. Dabei sollten Sie jedoch berücksichtigen, dass Einschränkungen in der Datenfreigabe funktionale Einschränkungen zur Folge haben können.

Im Bereich der Verbindungs- und Fehlerberichterstattung sollten Sie die Optionen zur automatischen Verbindung mit öffentlichen Hotspots und ggf. das Teilen der WLAN-Verbindungen deaktivieren und sich bei der Systemnutzung selbst entscheiden, ob Sie sich mit einem WLAN-Hotspot verbinden bzw. Dritten den Zugang zu Ihren Netzen ermöglichen möchten.

4.2 Anlegen von Benutzerkonten

Bei der Installation von Windows 10 stehen Sie vor der Wahl, ein lokales Benutzerkonto oder ein Microsoft Benutzerkonto für die Anmeldung an dem PC zu nutzen. Bei einem Microsoft-Konto handelt es sich um ein Online-Konto von Microsoft, das sie auch zur Anmeldung an Ihrem PC nutzen können.

Die Verwendung eines Microsoft-Kontos ermöglicht die geräteübergreifende Synchronisation von Benutzereinstellungen und Daten sowie die automatisierte Anmeldung an Microsoft-Cloud-Diensten, wie etwa OneDrive, Hotmail oder Skype. Ein Microsoft-Konto ist Voraussetzung für die Nutzung des Windows Stores (zum Kaufen und Nutzen von Apps) und des vollständigen Funktionsumfangs von Cortana.

Wenn Sie auf diese Funktionen verzichten bzw. möglichst wenige Ihrer personenbezogenen Daten mit Microsoft teilen möchten, sollten Sie die Anmeldung bzw. Registrierung bei Microsoft überspringen und ein lokales Benutzerkonto anlegen. Sie können Ihr lokales Konto auch zu einem späteren Zeitpunkt mit einem Microsoft-Konto verbinden. Beispielsweise erfolgt eine Sicherung der Nutzerlizenz für Windows 10 über das Microsoft-Konto. Dieses kann zu diesem Zweck angelegt werden, zur weiteren Konfiguration und alltäglichen Nutzung kann

dann weiterhin ein lokales Benutzerkonto verwendet werden.

Das bei der Installation von Windows 10 angelegte Benutzerkonto ist ein Administrator-Konto mit umfassenden Berechtigungen zur Systemkonfiguration. Legen Sie für Ihre tägliche Verwendung des Windows-PCs auf jeden Fall zusätzlich ein Standard-Benutzerkonto an. Sollten Sie sich für ein Microsoft-Konto entscheiden, sollten Sie dieses nicht mit administrativen Rechten ausstatten, um auszuschließen, dass ggf. kritische Informationen mit Cloud-Diensten synchronisiert werden. Sollte der Windows-PC von mehreren Anwendern genutzt werden, sollten Sie für jeden Anwender ein eigenes Benutzerkonto ohne Administrationsrechte anlegen. Aktivieren Sie hier zudem unter „Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte“ die Option „Anforderungen für erhöhte Rechte automatisch ablehnen.“

Bei der Einrichtung der Benutzerkonten sollten Sie angemessen sichere Passwörter vergeben. Hilfestellung zur Wahl und Verwendung von Passwörtern finden Sie in Abschnitt 5.3, Gebrauch von Passwörtern.

4.3 Überprüfen der Datenschutzeinstellungen

Die Assistenz- und Unterstützungsfunktionen von Windows 10 erfordern einen umfangreichen Zugriff auf Ihre Daten. Die eingerichteten Zugriffsberechtigungen können Sie unter „Einstellungen\Datenschutz“ überprüfen und nach Ihren Wünschen anpassen.

Ein besonderes Augenmerk sollten Sie im Bereich „Netzwerk und Internet\WLAN“ auf die Funktion „bekannten WLAN-Netzwerke mit direkten Facebook-, Skype- und Outlook.com-Kontakten teilen“ legen.

Hilfestellung bei der Bewertung der einzelnen Einstellungen finden Sie bei den Verbraucherzentralen (z. B. http://www.verbraucherzentrale.de/windows10) oder auch bei den Datenschutzbeauftragten der Länder (z. B. http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2016/04/2016-04_leitfaden_win10.pdf).

Informationen von Microsoft zum Umgang mit Telemetrie können Sie nachlesen unter https://technet.microsoft.com/de-de/itpro/windows/manage/configure-windows-telemetry-in-your-organization .

4.4 Verschlüsselung der Festplatte

Zum Schutz Ihrer Daten vor unbefugtem Zugriff durch Dritte, etwa durch Diebstahl oder Verlust, sollten Sie die Festplatte des Computers verschlüsseln. Der Leistungsverlust ist bei aktuellen Systemen meist zu vernachlässigen, sodass diese Maßnahme sowohl für Notebooks als auch für einen Desktop-Rechner zu empfehlen ist.

Unter Windows 10 Home steht Ihnen dafür z. B. die Windows Geräteverschlüsselung zur Verfügung.

Ab Windows 10 Professional können Sie hierzu *BitLocker Drive Encryption* nutzen, was eine Schlüsselverwaltung mithilfe eines TPM (Trusted Platform Module) durchführen kann. Das TPM ist dazu nicht zwingend notwendig, die Sicherung kann auch mittels eines Passwortes oder der Speicherung des Schlüssels auf einem externen USB-Speicherstick erfolgen. Bei der Konfiguration sollten Sie den Boot-Vorgang durch ein Passwort absichern. Den bei der Verschlüsselung des Rechners erstellten Wiederherstellungsschlüssel sollten Sie abspeichern, ausdrucken und getrennt vom Gerät sicher verwahren. Das Speichern der Schlüssel in der Cloud sollten Sie vermeiden. Ein Verlust des Wiederherstellungsschlüssels kann Sie unter Umständen dauerhaft aus dem System aussperren!

4.5 Aktivieren von Sicherheitsfunktionen

Zum Schutz Ihres Systems vor unbefugtem Zugriff können Sie nach der Installation folgende zusätzliche Sicherheitsfunktionen aktivieren:

- Passwortgeschützter Bildschirmschoner

  Durch das Konfigurieren eines passwortgeschützten Bildschirmschoners können Sie vermeiden, dass Ihr Desktop längere Zeit geöffnet bleibt, wenn Sie nicht mit dem Rechner arbeiten (z. B. bei Abwesenheit).

  Diesen Schutz können Sie in den Einstellungen, Bereich „Personalisierung“ in der Kategorie „Sperrbildschirm“ unter „Einstellungen Bildschirmschoner“ konfigurieren. Wählen Sie hierzu einen Bildschirmschoner Ihrer Wahl und setzen Sie den gewünschten Wert für die Wartezeit (z. B. 15 Minuten). Zur Aktivierung des Passwortschutzes müssen Sie noch einen Haken bei „Anmeldeseite bei Reaktivierung“ setzen.

- Deaktivieren der automatischen Wiedergabe

  Die automatische Wiedergabe bzw. der Autostart von Programmen auf Wechseldatenträgern gefährdet die Sicherheit Ihres Systems durch Schadprogramme und sollte deaktiviert werden. Sie können diese Funktion in den Einstellungen in der Kategorie „Geräte“ unter „Automatische Wiedergabe“ deaktivieren.

- Passwort-Rateschutz (Brute-Force-Schutz) aktivieren

  Falls Sie Ihr Bitlocker-verschlüsseltes System zusätzlich gegen sehr viele Passwort-Rateversuche schützen möchten, können Sie ein Limit für Anmeldeversuche konfigurieren. Wird dieses Limit überschritten, kann der Zugriff auf Ihren PC nur mittels des Wiederherstellungsschlüssels von 48 Zeichen reaktiviert werden, den Sie bei der Verschlüsselung des Systems erstellt und dessen Ausdruck Sie sicher hinterlegt haben (Ziffer 4.4, Verschlüsselung der Festplatte). Diesen Schutz erreichen Sie durch Zuweisen eines Schwellwerts in der Einstellung: „Interaktive Anmeldung: Schwellenwert für Computerkontosperrung“

  Diese Einstellung können Sie über die lokale Sicherheitsrichtlinie unter „Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen“ konfigurieren.

4.6 Personal Firewall

Windows 10 besitzt eine integrierte Personal Firewall, die im Auslieferungszustand oder nach einer Neuinstallation bereits aktiviert ist und einen Basisschutz bietet. Achten Sie darauf, dass Sie diese Firewall in den Systemeinstellungen nicht versehentlich deaktivieren. Die Installation einer zusätzlichen Firewall ist nicht erforderlich.

4.7 Internet-Browser

Ihr Internet-Browser ist die zentrale Komponente für die Nutzung von Online-Angeboten im Internet. Mit der Einführung von Windows 10 wird von Microsoft zusätzlich zum Internet Explorer ein neuer Browser, Microsoft Edge, ausgeliefert und seitens Microsoft zur Verwendung empfohlen. Sie können aber auch einen alternativen Browser installieren. Microsoft Edge enthält zum Schutz vor Schadprogrammen und gefährlichen Websites den sogenannten Smart-Screen-Filter. Dieser blockiert gefährliche Webseiten und warnt davor, diese zu nutzen. Außerdem werden Downloads auf Schadsoftware geprüft. Der Filter ist zunächst standardmäßig aktiviert und bei der Installation über die Einstellungen in der Kategorie „Browser und Schutz“ zu finden. Im Browser Microsoft Edge kann der Filter über Menü → „Einstellungen“ →

„Erweiterte Einstellungen anzeigen“ → „Mich mit SmartScreen Filter vor schädlichen Websites und Downloads schützen“ aktiviert werden, im Internet Explorer über die Einstellungen (Zahnradsymbol) → „Internetoptionen“ → „Erweitert“ → „Sicherheit“ → „SmartScreen Filter aktivieren“.

Die gängigen Browser unterstützen verschiedene Sicherheitsfunktionen zum Schutz ihres Systems vor Schadprogrammen und Ihrer Privatsphäre. Bei der Wahl Ihres Browsers sollten Sie darauf achten, dass dieser Mechanismen zur Isolation, z.B. das Sandboxing von aufgerufenen Webseiten und von dort ausgeführten Programmcode (insbesondere aktive Inhalte) unterstützt.

Dennoch ist kein Internet Browser absolut sicher. Vielmehr sind sie beliebtes Ziel für Angriffe. Es ist daher entscheidend, dass Sie stets einen möglichst aktuellen Browser verwenden.

Viele gängige Browser unterstützen mit sogenannten Plug-Ins einen Erweiterungsmechanismus, über den die Funktionalität des Browsers erweitert werden kann. Auch diese Plug-Ins können Schwachstellen aufweisen und die Sicherheit Ihres Systems gefährden. Sie sollten daher nur Erweiterungen installieren, die Sie tatsächlich benötigen und diese stets aus den offiziellen Plug-In-Stores des Herstellers beziehen. Des Weiteren sollten Sie darauf achten, auch die Erweiterungen auf einem aktuellen Stand zu halten und Aktualisierungen zeitnah einspielen.

Einige Browser enthalten bereits Erweiterungen zur Darstellung von PDF-Dokumenten und Flash-Inhalten. So müssen Sie hierzu keine zusätzlichen Programme installieren und diese separat aktualisieren; dies geschieht dann gleichzeitig mit den Sicherheitsupdates für den Browser. Außerdem sollten Sie die Versorgung mit Sicherheitsupdates bedenken: Diese werden je nach Browser entweder über die jeweils Browser-eigene Aktualisierungsfunktion entsprechend Ihrer Konfiguration automatisch, manuell oder automatisiert im Hintergrund aktualisiert.

Für den sicheren Internetzugriff sollten Sie in Ihrem Browser „click to play“ aktivieren. Dadurch wird das Darstellen unerwünschter oder verborgener Inhalte verhindert, eingebettete Flash-Animationen werden daraufhin beispielsweise nur mit Ihrer Freigabe ausgeführt. Diese Einstellung verbessert die Sicherheit, da nur erwünschte Inhalte dargestellt werden, kann zugleich die Ladezeiten einer Website verkürzen und damit auch Datenvolumen und Batteriekapazität einsparen.

Zum Schutz vor schadhaften Inhalten, sogenannten Drive-by-Downloads, oder bösartigen Websites besitzen einige Browser Schutzfilterfunktionen, deren Einsatz zu empfehlen ist. In den Einstellungen sollten Sie daher entsprechende Optionen bzw. Filter aktivieren. Diese Filter können jedoch aufgrund der hohen Dynamik neuer Webseiten mit schädlichen Inhalten allein keine Garantie gegen eine ungewollte Infektion mit Schadsoftware bieten. Eine zusätzliche Möglichkeit zum Schutz vor schadhaften Inhalten ist die Nutzung von Plug-Ins zum Blockieren von Werbeeinblendungen durch sogenannte Adblocker. Der Einsatz von Adblocker-Programmen kann allerdings zu Einschränkungen beim Zugriff auf einzelne Webseiten führen und es vereinzelt erforderlich machen, diesen temporär für den Zugriff auf diese Webseite zu deaktivieren.

Ein zusätzlicher Schutz durch einen Virenscanner bleibt dennoch erforderlich.

4.8 E-Mail

Für die weitgehend sichere Nutzung von E-Mails ist es nicht erforderlich, zusätzliche Software zu installieren. E-Mail-Provider bieten Webmail-Zugänge an, die Sie über den Internet-Zugang mit Ihrem Browser nutzen können. Wichtig ist, auf eine verschlüsselte Verbindung (https) zum Webmail-Zugang zu achten, um von den Schutzmechanismen Ihres Browsers zu profitieren.

Achten Sie darauf, dass die verschlüsselte Verbindung nicht nur für den Login-Vorgang, sondern während der gesamten Webmail-Nutzung aktiviert ist.

Falls Sie erweiterte Anforderungen an Komfort und Funktionalität bei der Arbeit mit E-Mails haben (z. B. Senden und Empfangen von verschlüsselten Emails), sollten Sie einen modernen E-Mail-Client installieren und sicher konfigurieren. Insbesondere ist dabei auf die Verwendung verschlüsselter Übertragungsprotokolle (POP3S, IMAPS, SMTPS) zu achten. Den E-Mail-Client können Sie wahlweise als App aus dem Windows Store oder auch als klassische Windows Anwendung installieren. Falls Sie ein Microsoft-Konto verwenden, steht Ihnen eine in Windows integrierte E-Mail-App zur Verfügung. Diese kann allerdings nur den Microsoft Email-Dienst nutzen. Bei der Wahl Ihres E-Mail-Clients sollten Sie ggf. beachten, dass das Programm mit etwaig bestehenden E-Mail-Archiven oder anderweitig gespeicherten E-Mail-Formaten kompatibel ist. Dies gilt auch für das Datenaustauschformat und gemeinsame Schnittstellen.

Bei der Auswahl eines E-Mail-Clients sollten Sie darauf achten, dass sich das Programm selbst aktualisiert. Apps werden über den Windows Store automatisch aktualisiert. Die Notwendigkeit der Aktualisierung werden im Abschnitt 5.1, Zeitnahes Einspielen von Sicherheitsaktualisierungen, dargestellt.

Weiterführende Informationen zur sicheren E-Mail-Kommunikation finden Sie auf der BSI-Webseite „BSI für Bürger“ unter der Kategorie „Verschlüsselt kommunizieren“:

https://www.bsi-fuer-buerger.de/BSIFB/verschluesselt_kommunizieren

4.9 Erzeugen eines Datenträgers zur Systemreparatur

Die meisten neuen Systeme werden heute ohne Installationsmedien ausgeliefert. Wenn dies bei Ihrem neuen PC der Fall ist, sollten Sie nach der ersten Inbetriebnahme einen Systemreparaturdatenträger erzeugen. Hierzu wird ein USB-Speicherstick mit zumindest 8, besser 16 GB Speicherkapazität benötigt. Im Falle eines Defekts oder Absturzes können Sie mit diesem Datenträger Ihre Windows 10-Installation wiederherstellen.

Zur Erstellung eines Systemreparaturdatenträgers rufen Sie die Funktion „Wiederherstellungslaufwerk erstellen“ z. B. über das Eingabefeld für Suchanfragen auf. Achten Sie dabei darauf, dass auch die Systemdateien gesichert werden. Nur in diesem Fall können Sie den Datenträger später auch zur Neuinstallation nutzen.

5 Regelmäßiger Betrieb

Im Umgang mit Ihrem PC sollten Sie die folgenden Empfehlungen für einen sicheren Betrieb berücksichtigen.

5.1 Zeitnahes Einspielen von Sicherheitsaktualisierungen

Microsoft erweitert mit Windows 10 das Verfahren der Systemaktualisierung durch sogenannte Wartungsoptionen, bei denen zwischen Wartungsaktualisierung (Update) und Featureupgrade (Upgrade) unterschieden wird. Mittels Wartungsaktualisierung stellt Microsoft die klassischen Sicherheitsaktualisierungen und Fehlerbehebungen bereit, während Featureupgrades das Aktualisieren Ihres Windows 10 mit neuen Features und Funktionen ermöglichen und das System damit auf eine neue Version des Wartungszweiges hebt. Eine Übersicht finden Sie unter: https://technet.microsoft.com/de-de/windows/release-info.aspx

Der Current Branch (CB) ist für Privat- und Geschäftskunden gedacht. Wartungsaktualisierungen und Featureupgrades werden automatisiert nach Freigabe und einer vorangegangenen Testphase durch Windows Insider installiert.

Sofern Sie die Einstellungen zur automatisierten Systemaktualisierung in Windows 10 nicht angepasst haben, lädt das System Sicherheitsaktualisierungen und -Upgrades im Hintergrund

und spielt diese außerhalb der Nutzungszeiten automatisiert bzw. beim Neustart ein. Dies kann dazu führen, dass der PC während der Arbeit unerwartet neu startet. Nach einem Update sollten Sie prüfen, ob sich gegebenenfalls Ihre Einstellungen im Betriebssystem (unter anderem Sicherheits- und Datenschutzeinstellungen) geändert haben, und diese eventuell noch einmal anpassen.

Sie können die Aktualisierungseinstellungen nach eigenen Bedürfnissen unter den Einstellungen im Bereich „Update und Sicherheit“ optimieren, z. B. durch das Festlegen der Nutzungszeiten, um Unterbrechungen durch Neustarts bei anstehenden Aktualisierungen zu vermeiden. Abgesehen hiervon sollten Sie die Standardeinstellungen zur automatisierten Aktualisierung beibehalten und insbesondere darauf achten, dass die Funktion „Updates für andere Microsoft-Produkte bereitstellen“ aktiviert bleibt.

Neben der Aktualisierung der installierten Microsoft-Programme sollten Sie dafür Sorge tragen, dass auch Programme von Drittanbietern regelmäßig (z. B. monatlich) aktualisiert werden. Viele Zusatzprogramme verfügen über integrierte, automatisierte Aktualisierungsfunktionen. Über den Windows Store bezogene Apps werden automatisch aktualisiert, sobald neuere Versionen bereitstehen. Bei anderen Windows-Programmen werden bereitstehende Aktualisierungen lediglich angezeigt, sodass Sie den Aktualisierungsvorgang manuell anstoßen müssen. Patch-Management-Werkzeuge unterstützen dabei, installierte Software auf dem aktuellen Stand zu halten.

Unabhängig hiervon sollten Sie sporadisch prüfen, ob sich alle installierten Programme auf einem aktuellen Stand befinden. Oftmals unterstützen die Programme hierzu eine Prüfung, ob neuere Versionen bereitstehen. Fehlt es an einer solchen Funktion, kann es hilfreich sein, die Versionsangabe der installierten Anwendung mit der Webseite des Herausgebers abzugleichen. Sie sollten in diesem Zusammenhang zudem sporadisch prüfen, ob die von Ihnen eingesetzten Programme noch mit Sicherheitsaktualisierungen durch den Hersteller versorgt werden. Falls die eingesetzte Software abgekündigt ist, sollten Sie auf eine aktuelle Version wechseln.

5.2 Erstellen regelmäßiger Datensicherungen

Im Abschnitt 3.3 wurden bereits einige Punkte zu Backups kurz angerissen.

Unwiederbringliche Datenverluste sind eine der größten Bedrohungen bei der Nutzung Ihres PCs. Solche Datenverluste können aus technischen Defekten Ihres Systems, durch Diebstahl, Verlust aber auch durch versehentliches Löschen oder Überschreiben von Daten entstehen. In den vergangenen Jahren haben zudem Erpressungsversuche mit Verschlüsselungstrojanern stark zugenommen. Wurden Daten auf diesem Weg verschlüsselt, ist das erneute Aufsetzen des Systems und das Aufspielen einer Datensicherung ein wichtiger Weg, um Datenverlust zu vermeiden.

Datensicherungen können Sie auf Netzwerklaufwerken (z. B. ein NAS-System), Wechseldatenträgern, wie etwa USB-Sticks oder externen Festplatten, oder grundsätzlich auch auf Cloud-Speicherdiensten ablegen. Bei der Nutzung von Cloud-Diensten sollten Sie allerdings berücksichtigen, dass Sie Ihre Daten damit dem Anbieter zugänglich machen. Damit Sie möglichst wirksam vor Verschlüsselungstrojanern geschützt sind, sollten Sie zumindest auf einem getrennt verwahrten Speichermedium sichern. Wechseldatenträger, die zur Datensicherung dienen, sollten auch nur für diesen Zeitraum an den PC angeschlossen werden. Zur Datensicherung sollte möglichst ein anderes Benutzerkonto (z. B. Administrationskonto) auf dem Rechner verwendet werden. Um den Zugriff von Verschlüsselungstrojanern auf erstellte Sicherungen zu verhindern, darf der normale Benutzer möglichst keinen Zugriff auf die erstellten Datensicherungen erhalten.

Die Häufigkeit, mit der Sie sichern sollten, ist von Ihrem Nutzungsverhalten und Ihrer Risikobereitschaft abhängig. Je häufiger Sie Sicherungen durchführen, desto geringer der potenziell

mögliche Verlust an Daten. Gleiches gilt für die Verwendung mehrerer Sicherungsmedien: So kann gewährleistet werden, dass beim Überschreiben eines Sicherungsmediums mit einer aktuellen Sicherung noch ein weiteres Sicherungsmedium mit einer Sicherung zur Verfügung steht. Viele Anwender sind mit einer wöchentlichen Datensicherung gut gegen Datenverluste abgesichert.

Die Sicherungen können Sie mit den in Windows 10 integrierten Sicherungsfunktionen erstellen, die Sie in den Einstellungen im Bereich „Update und Sicherung“ finden. Eine Anleitung zur Einrichtung einer automatisierten Sicherung und zur Wiederherstellung finden Sie unter dem nachfolgenden Link: https://support.microsoft.com/de-de/help/17143/windows-10-back-up-your-files

Falls Sie einen Schutz Ihrer Sicherungen vor Elementarschäden benötigen, sollten Sie eine Kopie Ihrer Daten außer Haus aufbewahren. Weiterhin sollten Sie ggf. erwägen, auch Ihre Sicherungen vor unbefugtem Zugriff zu schützen (z. B. Verschlüsselung einer externen Festplatte mit Bitlocker oder einem anderen Verschlüsselungsprogramm, Aufbewahrung in einem Safe).

5.3 Gebrauch von Passwörtern

Der Zugang zu Online-Services im Internet erfolgt häufig mittels der Abfrage eines Benutzernamens und eines Passworts. Wenn Sie verschiedene Online-Dienste nutzen, sollten Sie dafür jeweils unterschiedliche und angemessen sichere Passwörter verwenden.

Um sich diese besser behalten zu können, sollten Sie Merkhilfen verwenden, etwa die Anfangsbuchstaben eines längeren Satzes. Notieren Sie Ihre Passwörter zudem auf Zetteln und bewahren Sie diese räumlich von Ihrem Rechner getrennt in einem Safe oder an einem sicheren Ort auf. Ergänzende Hilfestellungen zum Passwortgebrauch finden Sie auf der Webseite „BSI für Bürger“, erreichbar unter: https://www.bsi-fuer-buerger.de

Viele gängige Internet-Browser besitzen integrierte Funktionen, mit denen Sie Zugangsdaten für besuchte Webseiten in einem integrierten Passwort-Manager hinterlegen können. Falls Sie diese Funktionen nutzen möchten, sollten Sie den Zugriff auf die gespeicherten Passwörter durch ein Passwort (Master-Password) vor unbefugtem Auslesen und Nutzen schützen.

Eine Alternative hierzu können kostenlos erhältliche Zusatzprogramme zum Erzeugen und Verwalten komplexer Passwörter sein. Die Nutzung von Online-Passwort-Managern, bei denen Sie Ihre Passwörter in einem Cloud-Dienst speichern, wird nicht empfohlen.

Beim Einsatz eines Microsoft-Kontos haben Sie zudem die Möglichkeit, den Zugriff auf Ihren Rechner mittels Windows Hello zu schützen. Windows Hello ermöglicht es Ihnen, den Zugriff auf Ihr Konto mittels alternativer Authentifizierungsmerkmale abzusichern, etwa durch biometrische Merkmale, wie Fingerabdruck oder Gesichtserkennung. Sie haben außerdem die Möglichkeit, den Zugriff auf einen Rechner mittels einer gerätespezifischen PIN freizuschalten. Mit diesen Funktionen können Sie sich die Anmeldung am Rechner erleichtern und häufige Passworteingaben vermeiden. Windows Hello können Sie im Bereich der Einstellungen\Benutzerkonten unter den Anmeldeoptionen konfigurieren.

Sofern die von Ihnen genutzten Online-Services dies unterstützen, können Sie auch in Erwägung ziehen, Single-Sign-On-Anmeldungen mit den verfügbaren zusätzlichen Sicherheitsfunktionen, wie Mehrfaktorenauthentifizierung (Token, SMS, Gerätebindung, usw.) zu nutzen. Dabei sollten Sie jedoch berücksichtigen, dass Sie gegenüber dem Anbieter transparenter werden.

5.4 Notfallvorsorge

Damit Sie in Notfallsituationen vorbereitet sind, sollten Sie sich nachfolgende Situationen vorstellen und Ihre Reaktionsmöglichkeiten einschätzen.

- Der Rechner startet nicht mehr.
- Sie können keine Verbindung mehr mit dem Internet herstellen.
- Sie können nicht mehr auf Ihre Cloud-Dienste und -Daten zugreifen.
- Sie können sich nicht mehr in Ihrem Benutzerkonto an Ihrem PC oder einer Webanwendung anmelden.
- Auf Ihrem Bankkonto finden Sie eine nicht von Ihnen vorgenommene Überweisung.
- Ihre Daten sind plötzlich verschlüsselt oder fehlen.

Microsoft stellt verschiedene Hilfestellungen für solche und ähnliche Situationen unter der Seite zur Verfügung: https://support.microsoft.com/de-de/products/windows?os=windows-10

Wenn Sie das Gefühl haben, dass Sie in diesen Situationen unsicher reagieren würden oder keine angemessenen Antworten finden, dann suchen Sie sich schon jetzt einen vertrauenswürdigen Ansprechpartner, der Sie bei der Bewältigung im Bedarfsfall unterstützen kann.

6 PC-Entsorgung

Wenn Sie Ihren PC eines Tages entsorgen möchten, dann sollten Sie sicherstellen, dass alle Daten auf der Festplatte sicher gelöscht sind. Ein einfaches Löschen in den „Papierkorb“ oder im Windows Explorer ist hierfür nicht ausreichend.

Auf der BSI-Webseite „BSI für Bürger“ finden Sie Hilfestellungen und kostenfreie Werkzeuge zum sicheren Löschen Ihrer Daten: https://www.bsi-fuer-buerger.de/BSIFB/richtig_loeschen

Neben dem Löschen der Daten ist auch die physikalische Vernichtung der Festplatte eine Möglichkeit, den Zugriff auf die dort vorhandenen Daten zu verhindern. Hierbei sollten Sie jedoch vorsichtig sein und entsprechende Schutzkleidung tragen.

Bitte berücksichtigen Sie hierbei, dass diese Löschverfahren lediglich zum Löschen von Datenbeständen auf Ihrem Rechner geeignet sind. Daten, die Sie in Cloud-Diensten und -Speichern halten, müssen im Bedarfsfall von Ihnen dort ergänzend gelöscht werden.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an mail@bsi-fuer-buerger.de gesendet werden.