So geht's leichter...

Sicher im Netz

- Sicherheit im Internet
- Sicherheit auf dem Router
- Office sicher machen
- Daten und Dateien verschlüsseln
- Smartphone absichern

Autoren:
Jörg Schieb
Andreas Erle

Impressum:
Redaktion Schieb
Humboldtstr. 10
40667 Meerbusch
Kontakt: fragen@schieb.de
www.schieb.de

So geht's leichter | Sicher im Netz

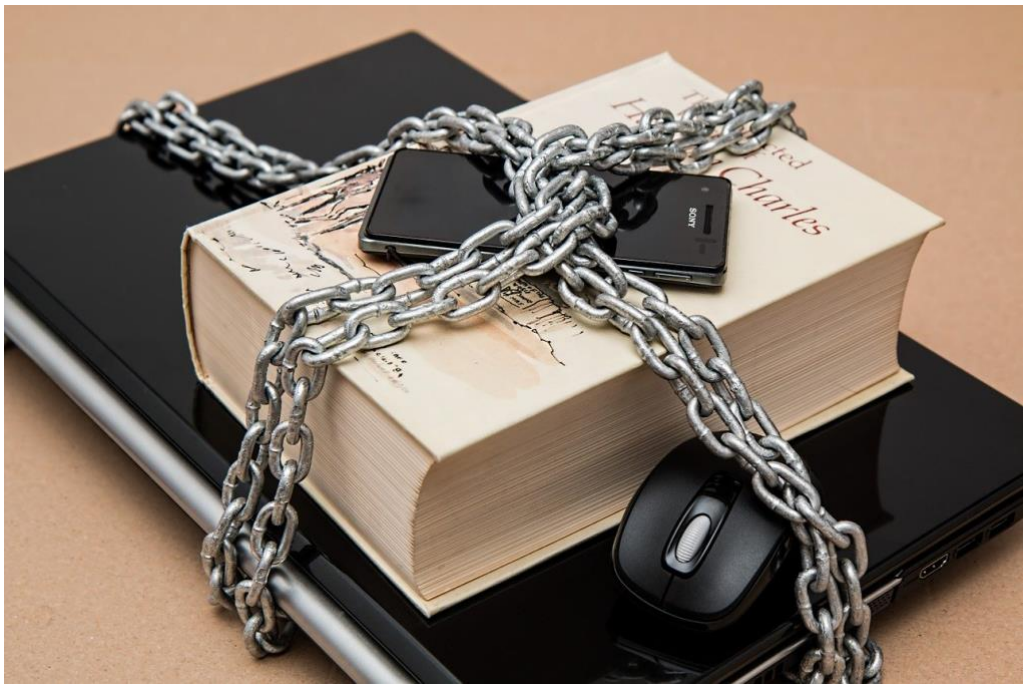
Inhaltsverzeichnis

So geht’s leichter | Sicher im Netz

So geht’s leichter | Sicher im Netz

Wenn Sie mit irgendeinem Ihrer Geräte arbeiten, dann vertrauen Sie ihm Informationen an, die ganz sicher nicht jeder sehen soll. Kurz: Sie wollen sicherstellen, dass das Gerät sicher ist und Ihre Daten darauf bleiben und nur von Ihnen eingesehen werden können.

Sicherheit ist in den vergangenen Monaten und Jahren zum Modewort geworden: Von allen Anwendern gewünscht, aber so kompliziert, dass sie kaum zu erreichen ist. Das ist aber überhaupt nicht wahr! Wenn Sie nicht in einem Hochsicherheitsbereich arbeiten, dann können Sie Ihre Geräte schon mit wenigen Schritten sicher machen.



Das schützt nicht nur Ihre Daten, sondern gibt Ihnen auch gleichzeitig noch ein besseres Gefühl.

Wir zeigen Ihnen, wie Sie Ihre Rechner mit Windows absichern, wie Sie in Office mit wenigen Schritten sicherstellen können, dass Ihre Dateien keinen Schaden anrichten und wie Sie auch auf Ihrem Smartphone möglichst wenig Spuren hinterlassen!

So geht's leichter | Sicher im Netz

Sicherheit im Internet

Das Internet ist – zumindest, wenn man der Presse glauben darf – die moderne Entsprechung des Wilden Westens. Hinter jeder Ecke lauern Bösewichter und versuchen, Sie um Ihr Erspartes zu bringen. Nur ist das nicht ganz so einfach: Microsoft hat mit Microsoft Edge schon eine Vielzahl von Mechanismen implementiert, die das verhindern sollen. Sie müssen Sie nur nutzen!

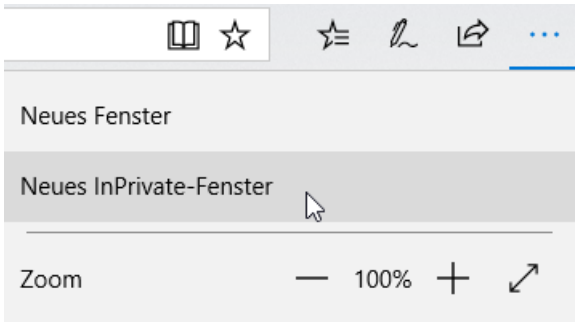
Sicherheit und Datenschutz in Edge

Ein immer wiederkehrendes Thema im Internet ist der Datenschutz. Durch die Kenntnis Ihres Surfverhaltens, der aufgerufenen Webseiten und verwendeten Daten kann ein Unbefugter eine Menge über Sie lernen. Dieses Wissen kann für alle möglichen Zwecke missbraucht werden. Oft haben Sie ein dringendes Bedürfnis, etwas online zu kaufen, und nutzen dann den Rechner eines Kollegen oder gehen in ein Internetcafé. Da gilt es, möglichst wenig Daten zu hinterlassen!

Der private Surfmodus

Im Regelfall speichert Edge automatisch eine Vielzahl von Informationen: Vor allem der Verlauf, also die Liste der aufgerufenen Webseiten, ist hier oft kritisch. Greifen mehrere Benutzer auf Ihren Rechner mit Ihrem Konto zu, dann können diese sehen, welche Seiten Sie aufgerufen haben.

Wenn Sie das nicht möchten, dann starten Sie einfach eine private Surf-Sitzung. Dazu klicken Sie in Edge auf die drei Punkte oben rechts, dann auf Neues In Private-Fenster.



So geht's leichter | Sicher im Netz

Edge öffnet jetzt ein neues Fenster. Alle während des Surfens in diesem Fenster angesurften Webseiten werden nicht im Verlauf gespeichert. Auch die Cookies und Temporären Dateien werden nach Schließen des Fensters automatisch gelöscht.

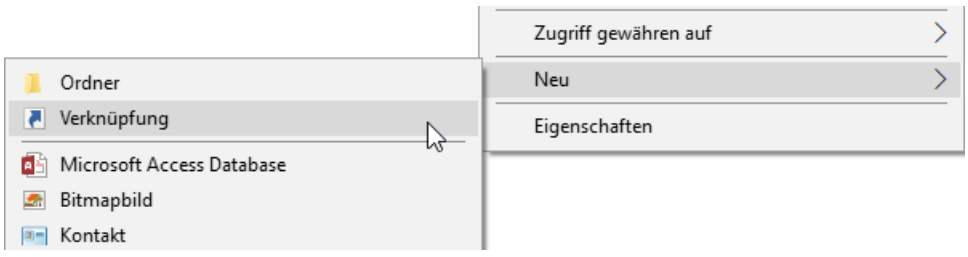
Wichtig

Wundern Sie sich nicht, wenn Sie sich auf bekannten Webseiten im privaten Surfmodus immer wieder anmelden müssen (statt wie bisher die Anmeldedaten zu bestätigen). Der Zugriff auf bereits gespeicherte Daten wird unterbunden, um die Privatheit sicherzustellen.

Edge immer im privaten Surfmodus starten

Wenn Ihr Rechner häufiger von anderen Personen benutzt wird, dann macht es vielleicht Sinn, Edge immer im privaten Surfmodus zu starten. Das erlaubt Windows 10 zwar nicht direkt. Sie können es aber über einen kleinen Trick schnell erreichen:

Legen Sie eine neue Verknüpfung auf dem Desktop an, indem Sie mit der rechten Maustaste auf das Desktop klicken und dann **Neu** > **Verknüpfung** anwählen.



Als Speicherort geben Sie den Text

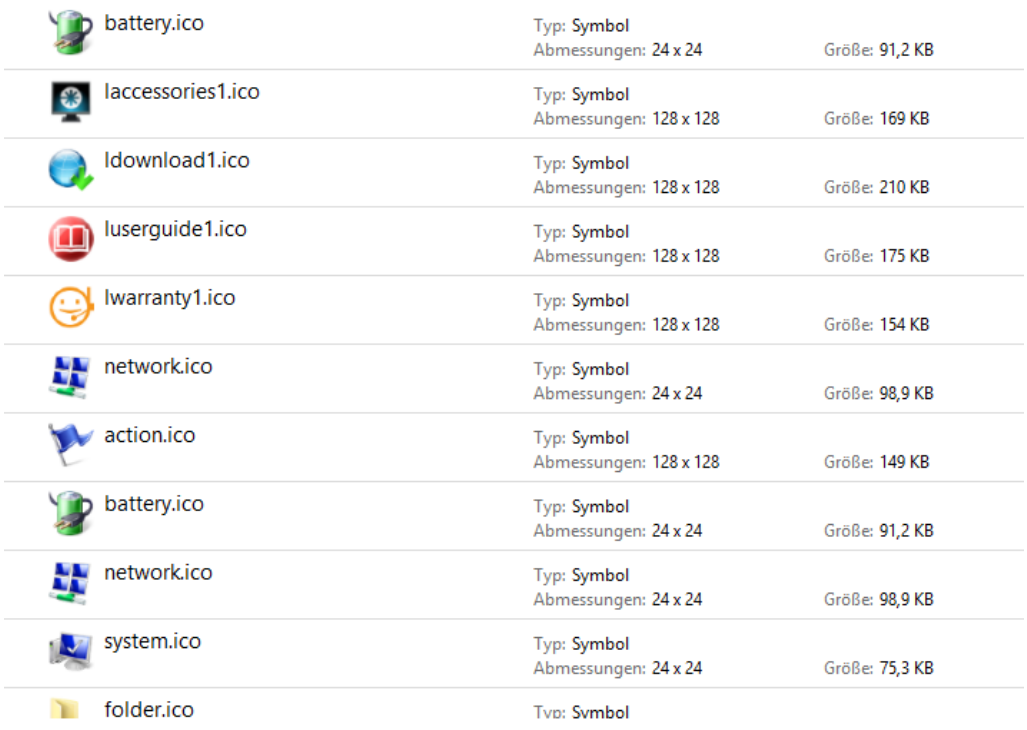
%windir%\System32\cmd.exe /c start shell:AppsFolder\Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge -private

So geht's leichter | Sicher im Netz

ein. Als Namen der Verknüpfung im nächsten Schritt geben Sie dann **Edge (privat)** ein.

Ein Doppelklick auf diese neue Verknüpfung startet dann immer ein neues Edge-Fenster, das direkt im privaten Surfmodus geöffnet wird.

Nun ist das Symbol der Verknüpfung nicht sonderlich schön. Das können Sie ändern: Klicken Sie mit der rechten Taste auf das Symbol und wählen Sie **Eigenschaften** > **Verknüpfung** > **anderes Symbol.** Normalerweise zieht Windows 10 passende Symbole aus der .EXE-Datei. Nun ist es so, dass Edge kein Programm im eigentlichen Sinne, sondern eine fest in Windows 10 integrierte Funktion ist. Sie bekommen also keine Auswahlmöglichkeit für ein neues Symbol angezeigt.

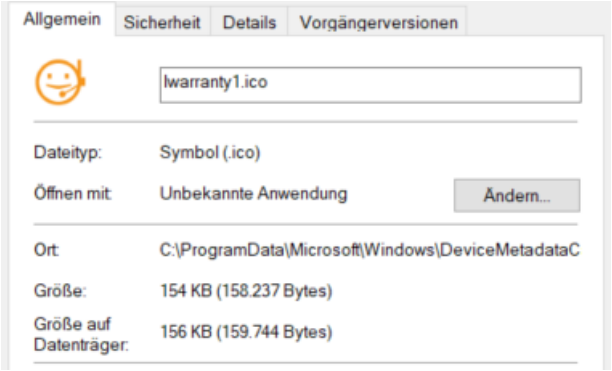


Windows verwendet Symboldateien, die die Erweiterung ICO (für Icon) haben. Sie können eine beliebige dieser Dateien für die Verknüpfung verwenden.

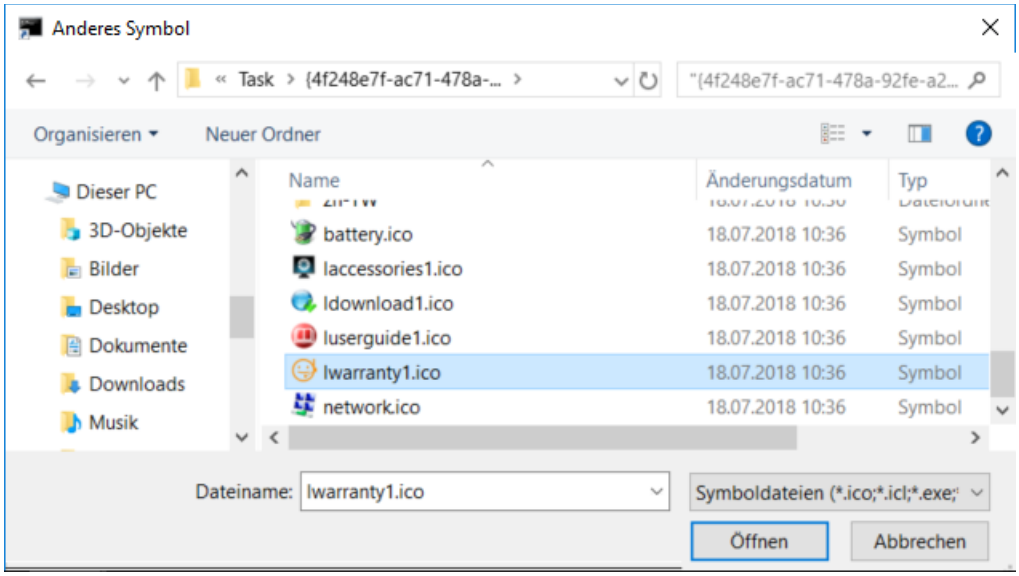
So geht's leichter | Sicher im Netz

Starten Sie stattdessen durch Drücken von der **Windows** und **E**-Taste ein neues Explorer-Fenster. Klicken Sie auf die Festplatte C:, dann geben Sie oben rechts in der Suchleiste ***.ico** ein. Windows 10 zeigt Ihnen jetzt alle Symboldateien an.

Wenn Sie darin ein Symbol gefunden haben, dann klicken Sie es einmal an, um es zu markieren. Ein Rechtsklick auf das Symbol zeigt Ihnen unter Ort den Pfad, an dem diese Symboldatei sich befindet. Markieren und kopieren sie ihn.



Diesen Pfad fügen Sie nun in den Eigenschaften des Symbols unter **Nach Symbolen in dieser Datei** suchen ein.



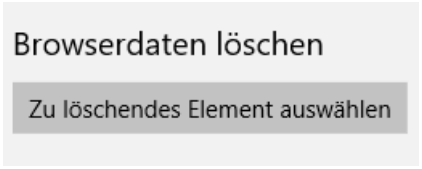
So geht's leichter | Sicher im Netz

Nach einem Klick auf Öffnen und auf OK hat Ihre Edge-Verknüpfung dann das gewünschte neue Symbol.

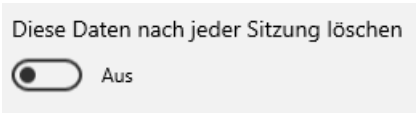
Löschen der Internetspuren

In den meisten Fällen haben Sie sich an Ihrem PC nicht im privaten Surfmodus im Internet bewegt. Wenn Sie nun den PC weitergeben wollen oder nicht an Ihrem eigenen PC gesurft haben, dann sollten Sie die gespeicherten Dateien löschen.

Unter **Einstellungen** > **zu löschendes Element auswählen** können Sie ganz fein festlegen, welche Dateien gelöscht werden sollen: der Verlauf, Cookies, temporäre Dateien, gespeicherte Tabs, Formulardaten, Kennwörter und vieles mehr. Wählen Sie alle möglichen Optionen, wenn Sie den Rechner komplett von ihren Spuren befreien wollen. Mit einem Klick auf **Löschen** entfernen Sie diese von der Festplatte.



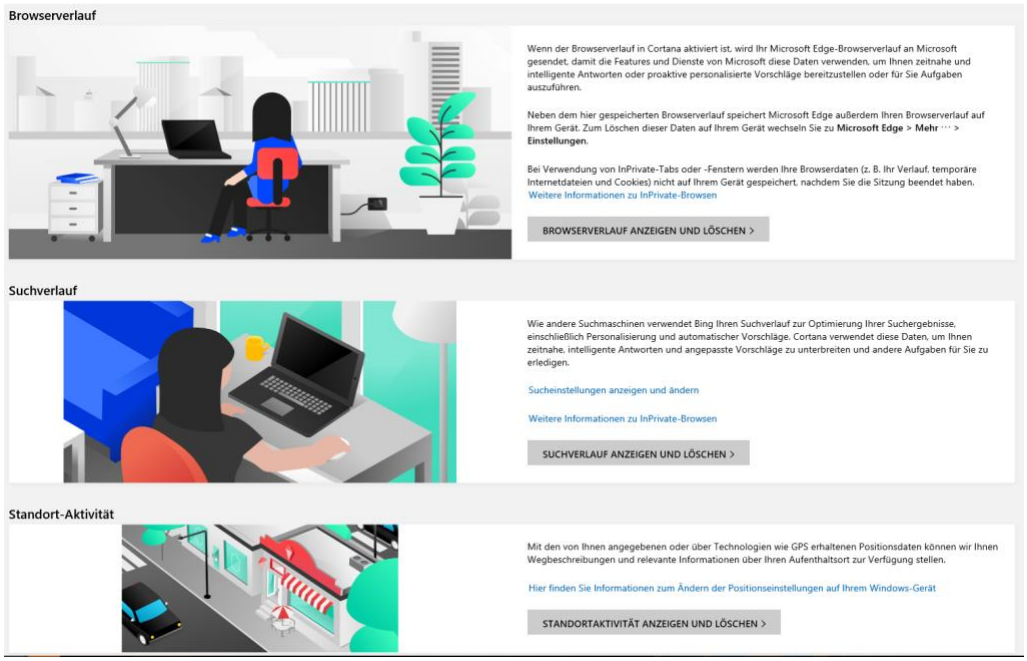
Wenn Sie häufiger an einem fremden PC arbeiten, dann macht es Sinn, den manuellen Löschvorgang zu automatisieren. Dazu aktivieren sie die Option **Diese Daten nach jeder Sitzung löschen**. Alle Optionen, die Sie im vorigen Schritt aktiviert haben, werden dann gelöscht, wenn Sie das Browserfenster schließen.



Damit haben Sie schon einmal die lokalen Spuren auf der Festplatte gelöscht. Allerdings synchronisiert Windows 10 im Standard einige dieser Daten mit der Cloud. Um diese zu löschen, klicken Sie in Windows 10 in den **Einstellungen** auf **Datenschutz** > **Meine Daten verwalten, die in der Cloud gespeichert sind**.

So geht's leichter | Sicher im Netz

Ironischerweise öffnet sich dann die Kontoverwaltungsseite in Edge. Nach der Anmeldung können Sie dann den Browserverlauf, den Suchverlauf und viele andere Elemente anzeigen lassen und auch löschen.



Schutz vor Schädlingen durch Smartscreen

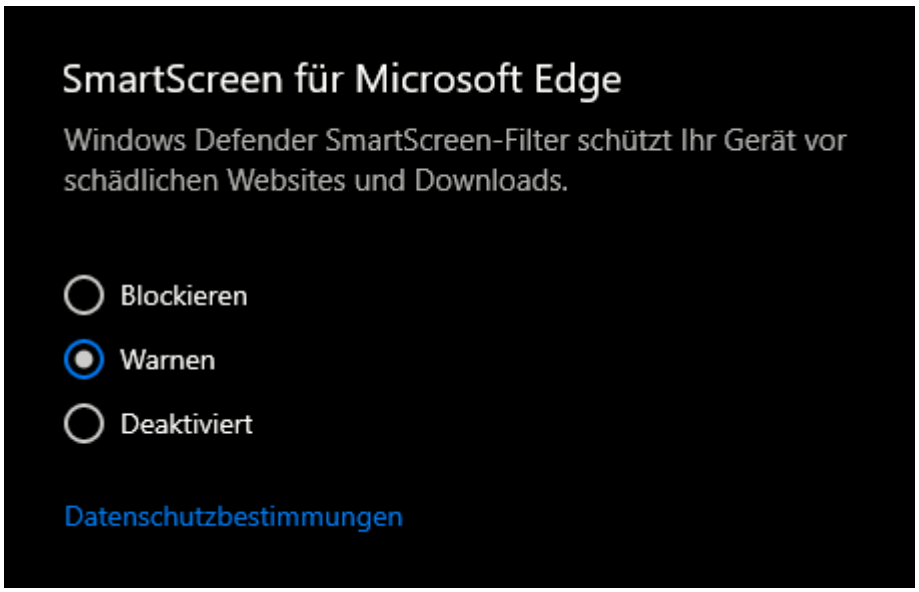
Das Internet bietet mehrere unterschiedliche Arten von Bedrohungen. Neben Viren und Phishing-Attacken handelt es sich hier vor allem um Webseiten, die Schadcode enthalten und beim Aufruf weiterverbreiten. Viele Antiviren-Programme haben eine separate Schutzfunktion dafür. Auch Windows 10 bietet mit SmartScreen eine integrierte Funktion, die Sie auf jeden Fall aktivieren sollten.

Unter **Einstellungen** > **Updates und Sicherheit** > **Windows Sicherheit** > **Windows Sicherheit öffnen** > **App- & Browsersteuerung** können Sie unter Smartscreen für Microsoft Edge aktivieren, dass Webseiten vor

So geht's leichter | Sicher im Netz

der Darstellung in Edge überprüft werden. Hier sollten Sie mindestens **Warnen** aktiviert haben.

SmartScreen überprüft jede Seite aktuell gegen die Microsoft Server, so werden auch neue erkannte Bedrohungen umgehend mit in die Prüfung einbezogen.



Tipp

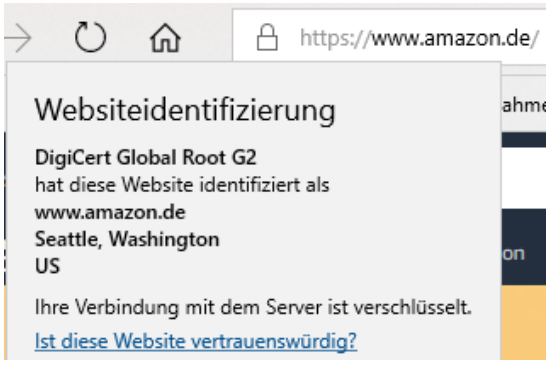
Wenn Sie Ihre Vorlagen sichern wollen: Diese finden sich in Ihrem Dokumente-Verzeichnis unter Benutzerdefinierte Office-Vorlagen. Wenn Sie die Vorlagen auf einen neuen Rechner kopieren wollen: speichern Sie wie oben beschrieben erst einmal eine neue, leere Vorlage ab. Erst dann legt Word dieses Verzeichnis an.

So geht's leichter | Sicher im Netz

Sichere Webseiten

Ideal ist es natürlich, wenn Sie gar nicht erst in Gefahr kommen, wenn Sie auf einer Webseite Surfen. Da macht es Sinn, wenn Sie sich die Seiten, die Sie besuchen, vorher genau anschauen.

Eine Webseite schafft Ihnen eine leicht andere Einkaufsumgebung als ein echter Laden. Beim Shopping in der Stadt können Sie sich vor dem Kauf anhand des Angebots, der Lage des Ladens, der Mitarbeiter zumindest einen visuellen Eindruck verschaffen. Und vor allem können Sie die Produkte anfassen und deren Qualität vorher beurteilen. Im Internet ist vieles Vertrauenssache. Wenn Sie kaufen, dann können Sie nur hoffen, auch die bestellte und meist vorbezahlte Ware zu bekommen.



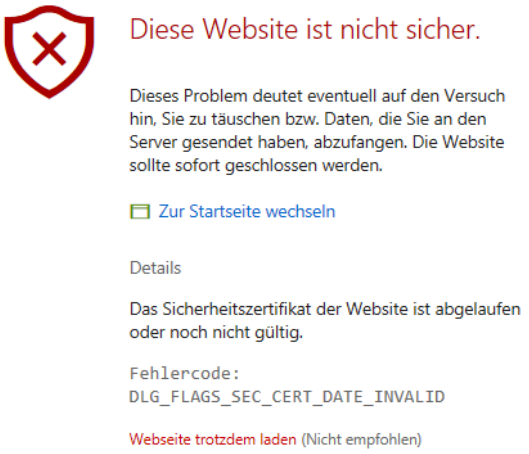
Einen Hinweis wenig bietet hier das Zertifikat der Webseite. Ein SSL-Zertifikat ist quasi ein Siegel, das die Organisation, der die Webseite gehört, und die Webseitenadresse miteinander in Verbindung bringen. Das Zertifikat ermöglicht es dann, die Kommunikation zwischen Ihrem Rechner und dem Shop zu verschlüsseln.

Das ist wichtig, damit beispielsweise Kreditkarten- oder Kontoinformationen für die Bezahlung nicht auf dem Weg abgefangen und missbraucht werden können. Erkennen können Sie den Einsatz eines SSL-Zertifikats daran, dass links (oder rechts, je nach Browser) der Internetadresse ein Schloss angezeigt wird. Klicken Sie darauf, dann sehen Sie die so genannte Webseitenidentifizierung. Die zeigt an, auf welchen Händler die Seite registriert ist. Keine Fake-Seite könnte sich

So geht's leichter | Sicher im Netz

also hier als Apple oder Amazon ausgeben, weil sei gar nicht erst durch den Prüfprozess zur Erteilung des SSL-Zertifikats kommen würde.

Vorsicht ist geboten, wenn eine Webseite nicht verschlüsselt ist oder gar das Zertifikat nicht zu Seite passt oder abgelaufen ist. Letzteres kann immer mal passieren, ist aber bei einem Online-Händler kein gutes Zeichen. Sie können die Webseite dann trotzdem besuchen, empfehlenswert (gerade bei Shopping- oder Online-Banking-Seiten) ist das nicht!



Nutzen von VPNs

Besonders im Firmenumfeld ist der Einsatz von Virtual Private Networks, kurz VPN, lange Standard. Diese Verbindung erzeugt einen Tunnel zwischen Ihrem Rechner und dem Ziel (beispielsweise einem Firmenserver), der auf dem kompletten Weg verschlüsselt ist.

Voraussetzung ist ein VPN-Server, der Sie mit dem Netzwerk, mit dem Sie sich verbinden wollen, verbinden lässt. Unter Windows 10 können Sie eine neue VPN-Verbindung einrichten, indem Sie auf **Einstellungen**, **Netzwerk und**

So geht's leichter | Sicher im Netz

Internet, **VPN** und dann auf **VPN-Verbindung hinzufügen** klicken.

Geben Sie dort dann die nötigen Zugangsdaten ein, um die Verbindung erfolgreich aufbauen zu können. Bei einigen VPN-Typen ist es nötig, dass Sie noch zusätzliche Software bzw. Treiber installieren, das kann Ihnen der Betreiber des Servers sagen.

Tipp

Setzen Sie eine Netzwerkfestplatte, ein so genanntes NAS, ein? Dann sollten Sie dessen Handbuch konsultieren: Die meisten NAS-Systeme bieten integriert einen VPN-Server. Aktivieren Sie den, dann können Sie von unterwegs eine Verbindung zu Ihrem NAS aufbauen, die verschlüsselt und sicher ist.

Zum Verbinden mit dem VPN klicken Sie auf das Verbindungssymbol unten rechts im Tray, dann auf den Namen des VPNs und auf **Verbinden**.

Haben Sie keinen eigenen VPN-Server im Router oder der Netzwerkfestplatte? Dann nutzen Sie doch einfach einen Fremdanbieter wie HideMyAss oder CyberGhost. Die bieten Ihnen den selben Service, nehmen Ihnen aber den Aufwand der Einrichtung ab. Installieren Sie

So geht's leichter | Sicher im Netz

deren Software, lassen Sie die Verbindung aufbauen, und schon sind Ihre Daten verschlüsselt unterwegs.

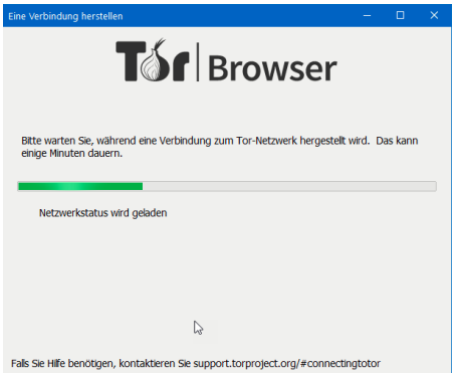
Die großen VPN-Anbieter haben auch Apps für Android und iOS im Programm. Schließlich sind Sie unterwegs ebenfalls viel online. Auch wenn es weniger Schadsoftware für mobile Geräte gibt als für den PC, ist das Risiko nicht von der Hand zu weisen!

Anonym und sicher Surfen: Der Tor-Browser

Im Internet finden Sie nahezu alle Informationen, die Sie benötigen. Manchmal auch mehr, als Sie tatsächlich wissen wollen. Sicher ist aber: Eine Suche im Internet hinterlässt Spuren. Und bei bestimmten Themen ist es Ihnen vielleicht nicht so recht, wenn man nachvollziehen kann, dass Sie eine Webseite besucht haben. Eine schnelle Lösung ist hier der kostenlose Tor-Browser (https://www.torproject.org/de/download/)

So geht’s leichter | Sicher im Netz

Die Idee dahinter ist einfach: Das Internet kann Suchen und Webseitenbesuche ja nur deshalb zu Ihnen zurückverfolgen, weil es über die IP-Adresse potenziell Zugriff zu Ihrem Anschluss hat. Der Tor-Browser löst das elegant: Er verwendet das Zwiebelschalenprinzip. Im Englischen heißt das Onion Routing, daher kommt auch der Name des Browsers: **T**he **O**nion **R**outer.



Die Idee: Im Internet laufen sie Daten immer über verschiedene Knotenpunkte, damit ist Ihre Adresse auch all diesen Knoten bekannt. Beim Tor-Browser werden Ihre Daten an jedem Knoten neu ver- bzw. entschlüsselt. Damit sieht am Ende nur der letzte Knoten Ihre Daten im Klartext und kann überhaupt etwas damit anfangen.

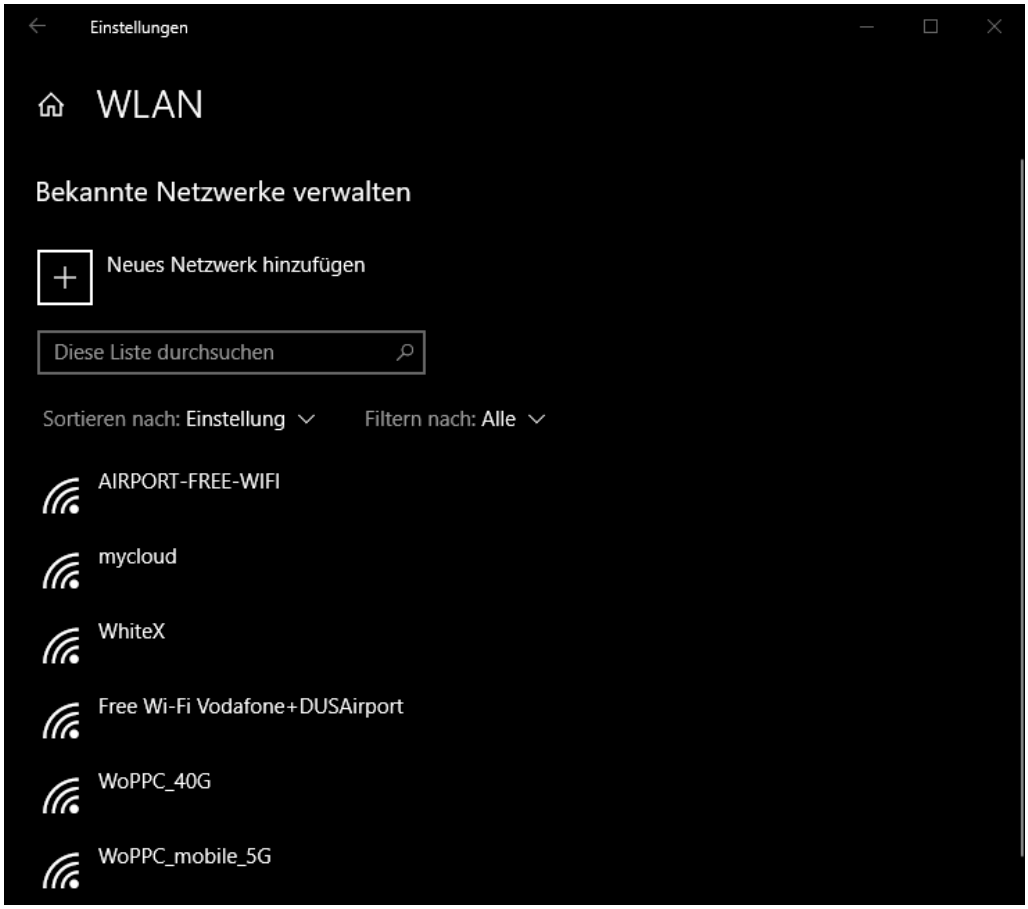
So geht's leichter | Sicher im Netz

Dazu kommt, dass die Daten durch die immer wieder durchgeführte Verschlüsselung immer anders aussehen, ein Tracking also nicht möglich ist. Und da jeder Knoten nur seinen Nachbarn kennt, kann die Seite, von der Sie Daten herunterladen bzw. an die Sie Daten senden auch nicht identifizieren, dass Sie es sind. Anonymer können Sie kaum Surfen!

Verwalten der gespeicherten WLANs

Sind Sie häufig mit Ihrem Windows 10-Rechner unterwegs? Dann ist die Wahrscheinlichkeit hoch, dass Sie eine nahezu nicht enden wollende Liste bekannter WLANs mit sich herumschleppen. Diese nehmen natürlich nicht viel Speicher weg, bergen aber doch ein Risiko: Windows 10 verbindet sich im Standard automatisch mit bekannten WLANs.

So geht’s leichter | Sicher im Netz



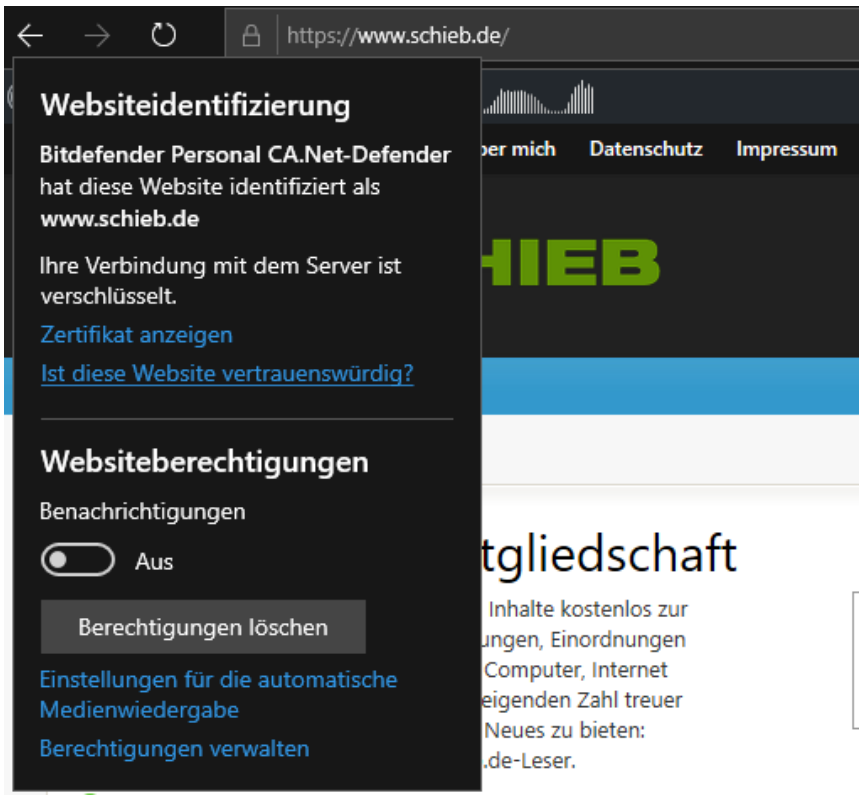
Wenn Sie also zufällig nach einiger Zeit wieder an den Ort kommen, wo sich ein gespeichertes WLAN befindet, wie die Verbindung wiederaufgebaut, ohne, dass Sie das mitbekommen.

Räumen Sie die Liste der WLANs einfach auf, indem Sie auf **Einstellungen**, **Netzwerk und Internet**, **WLAN** gehen, dann über **Bekannte Netzwerke verwalten** die Liste öffnen und das zu löschende WLAN anklicken. Durch **Nicht Speichern** vergisst Windows 10 das WLAN. Das heißt nicht, dass Sie sich damit nicht mehr verbinden können! Es wird Ihnen in der Liste der verfügbaren WLANs immer noch angezeigt, zum Verbinden müssen Sie dann allerdings das Kennwort des WLANs erneut eingeben.

So geht's leichter | Sicher im Netz

Obacht bei freien WLANs

Wie in so vielen anderen Situationen im Zusammenhang mit Internet und Dienstleistungen ist es nicht immer so, dass jemand Ihnen etwas Gutes will, wenn er Ihnen etwas kostenlos anbietet. Es gibt das eine oder andere „Free WLAN", das mehr Interesse daran hat, die von Ihnen übertragenen Daten zu erschnüffeln, statt Ihnen einen echten Service zu bieten.



Seien Sie also vorsichtig, welche Daten Sie übertragen, wenn Sie in einem solchen WLAN online sind. Beispielsweise sollten Sie nur auf solchen Seiten Benutzernamen und Kennwörter eingeben, die SSL-Verschlüsselt sind. Das erkennen Sie daran, dass die Adresse der Webseite mit **https://** (statt mit http://) beginnt. Bei solchen Webseiten können Sie dann auf das Schloss-Symbol neben der Adresse klicken und

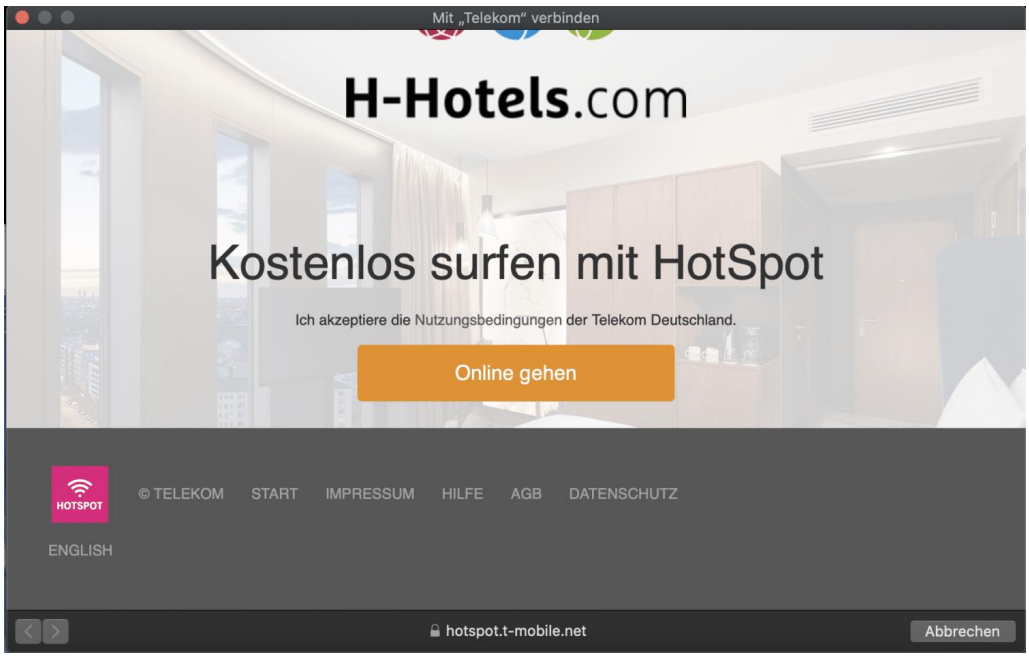
So geht’s leichter | Sicher im Netz

bekommen dann weitere Informationen über die Vertrauenswürdigkeit der Seite.

Unterwegs sicher in WLANs gehen

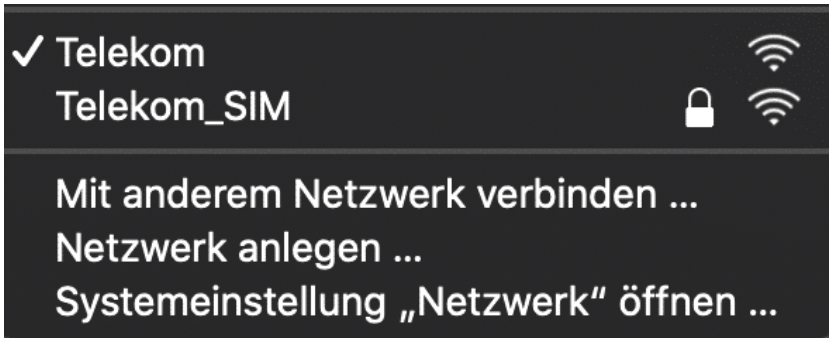
Mittlerweile ist es Standard, in einem Hotel ein freies WLAN angeboten zu bekommen. Entweder bekommen Sie die Zugangsdaten direkt beim Einchecken an der Rezeption, oder sie finden im Zimmer einen Handzettel. Nun ist "frei" nicht selten mit Vorsicht zu genießen. Was tun, wenn die Verbindung nicht klappt? Welche Risiken und Lösungen bestehen? Die Antworten lesen Sie in unserem Tipp.

Im Normalfall sollten Sie eigentlich keine weiteren Schritte manuell vornehmen müssen: Verbinden Sie sich mit dem Hotel-WLAN, das Sie angegeben bekommen haben, und Ihr Browser öffnet sich automatisch auf einer Übergabeseite. Auf dieser müssen Sie dann entweder die Zugangsdaten (oft Name und Zimmernummer) eingeben oder einfach nur die AGBs bestätigen.



So geht’s leichter | Sicher im Netz

Wenn das nicht der Fall ist, dann trennen Sie die Verbindung nochmal und stellen Sie erneut her. In den Ausnahmefällen funktioniert das aber immer noch nicht: Ihr PC oder Mac waren im Ruhezustand und davor schon in einem anderen WLAN, sind also über die Phase der Authentifizierung raus. Bevor Sie nun lange basteln: Starten Sie das Gerät neu. Direkt nach dem Neustart sehen Sie die Übergabeseite und können sich mit dem Internet verbinden.



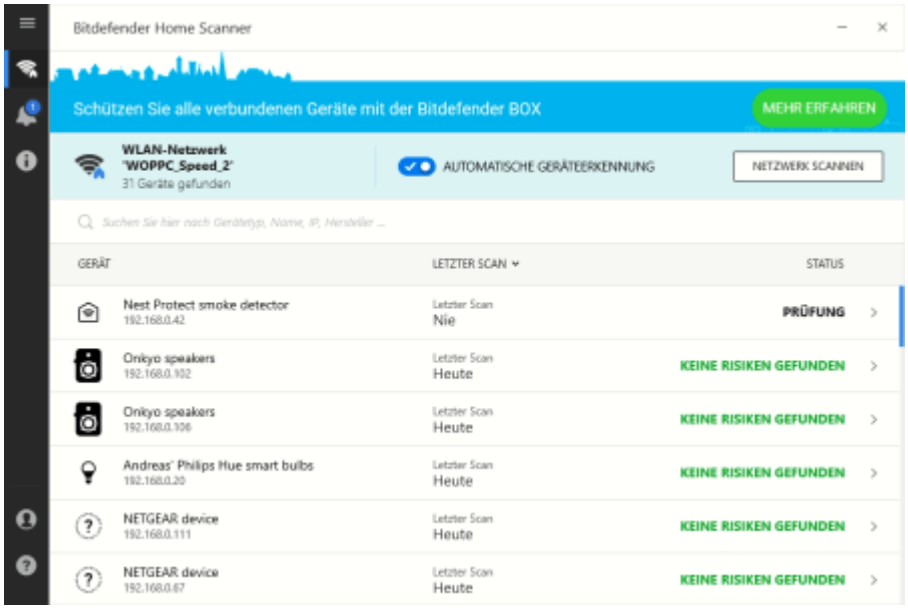
Nun haben die freien WLANs (nicht nur in Hotels) eine Einschränkung: Sie sind offen, also unverschlüsselt. Das erkennen Sie an dem Vermerk "Offen" (Windows 10) oder dem fehlenden Schloss neben dem WLAN-Namen (Mac OS). Daten werden also im Klartext übertragen. Keine gute Idee, wenn Sie beispielsweise Passwörter eingeben. Hier sollten Sie wie oben beschrieben einen VPN-Anbieter nutzen und die Verschlüsselung selber sicherstellen.

Schutz vor Schädlingen im WLAN: Bitdefender Home Scanner

Ein WLAN zu schützen, ist auf den ersten Blick eine einfache Aufgabe. Den Router schotten Sie soweit es geht ab, das WLAN mit einem langen, kaum merkbaren Kennwort verschlüsselt und die SSID am besten noch verborgen. So kann niemand, der dort nichts zu suchen hat, in Ihr WLAN gelangen und Daten stehlen. Wie so oft ist das eigentliche Problem oft ein Innentäter. Nicht ein Mitglied Ihres

So geht's leichter | Sicher im Netz

Haushalts, sondern ein Gerät, das infiziert ist und irgendetwas Böses versucht.



Auf Ihren normalen Geräten haben Sie meist Virenscanner. Regelmäßig aktualisiert schützen die vor bekannter Malware. In letzter Zeit erfolgen aber immer mehr gezielte Angriffe auf Geräte im Netzwerk. Kameras, Rauchmelder, Sprachassistenten: Auch vor Netzwerkfestplatten machen die Angreifer nicht Halt, wie die QSnatch-Malware eindrucksvoll zeigt. Für iOT-Geräte und andere „Nicht-PCs" gibt es leider keine Virenscanner, und so bleibt nur die Analyse des Netzwerkverkehrs auf Auffälligkeiten.

Der Antiviren-Software-Hersteller Bitdefender bietet mit dem kostenlosen Home Scanner (https://www.bitdefender.de/solutions/home-scanner.html) ein Programm an, das Ihr Netzwerk überwacht. Der zusätzliche Vorteil des ersten Scans: Jeder IP wird ein Produkt zugewiesen. In der Übersicht können Sie also erkennen, welches Gerät sich hinter einer IP-Adresse verbirgt. Danach bekommen Sie das Ergebnis für jedes Gerät angezeigt,

So geht's leichter | Sicher im Netz

idealerweise **Keine Risiken gefunden**. Sollte noch ein unnatürliches Verhalten erkannt worden sein, dann liefert Ihnen der Home Scanner dafür mögliche Lösungsansätze.

Das Programm bietet zwar keine absolute Sicherheit, aber zumindest einen guten Überblick über Gefahren in Ihrem WLAN.

Konfigurieren einer Firewall

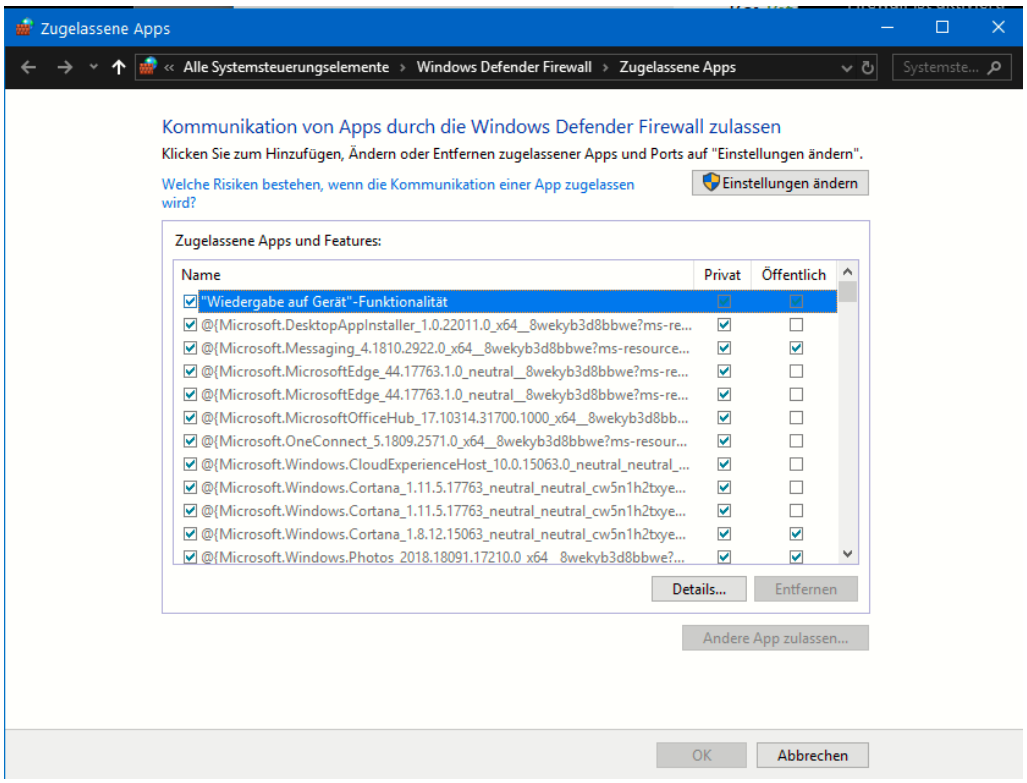
Eine Software-Firewall ist sinnvoll: Sie schützt sie vor ungewollten Datenübertragungen von oder auf Ihren Rechner. Die Funktionsweise ist ein wenig vergleichbar mit der eines Antivirenprogramms. Die Firewall erkennt Angriffsmuster, die verdächtig erscheinen. Den entsprechenden Datentransfer blockiert sie dann. Manchmal aber meint sie es zu gut. Wenn bestimmte Programme nicht mehr laufen, dann kontrollieren Sie die Firewalleinstellungen.

Windows 10 hat schon eine recht gute Firewall mit an Bord. Die Öffnen Sie, indem Sie in der Suchleiste **Firewall** ein geben und auf **Firewall- und Netzwerkschutz** klicken.

Windows unterscheidet drei Arten von Netzwerken: **Domänennetzwerke** (die meist in Firmenumgebungen vorkommen), **Private Netzwerke** (das sind Netzwerke, bei denen Sie den Standort kennen und unter Kontrolle haben) und **Öffentliche Netzwerke**.

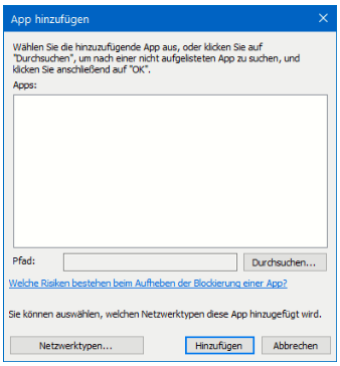
So geht’s leichter | Sicher im Netz

Für alle drei Netzwerktypen sollten Sie die Firewall aktivieren. Windows überprüft dann selbständig, ob eine App versucht, irgendwelche Verbindungen aufzubauen, die verdächtig sind. Das können Würmer sein, Viren, Hardwarekomponenten, die Daten irgendwo hinschicken. Nicht immer ist das ein Schädling, manchmal meldet die Firewall einen Einbruchsversuch, wenn ein echtes Programm seine Arbeit verrichten will. Solche „False Positives“ genannten Fehler können Sie selber korrigieren: Die Firewall meldet Ihnen jede blockierte Verbindung durch eine PopUp-Meldung auf dem Bildschirm Das führt dazu, dass die Verbindung erst einmal nicht zugelassen wird. Wenn Sie dann aber in die Firewalleinstellungen oben gehen und auf **Zugriff von App auf durch Firewall zulassen** anklicken, dann zeigt Ihnen Windows 10 eine Liste der Apps an, die über die Firewall gehe. Hier können Sie für private wie öffentliche Netzwerke einzeln festlegen, ob die App die Verbindung aufbauen darf oder nicht.

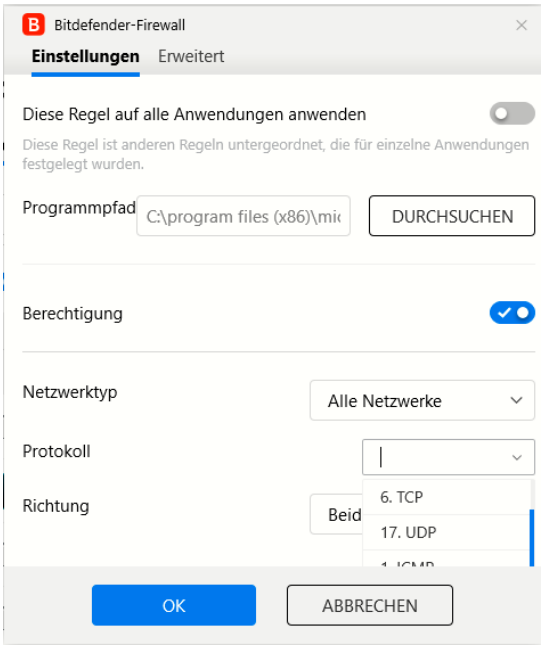


So geht's leichter | Sicher im Netz

Aktivieren Sie die gerade noch blockierte App einfach, dann bauen Sie die Verbindung erneut auf. Schon sollte sie funktionieren.



Findet sich die App, die Sie für die Firewall zulassen wollen, nicht in der Liste, dann können Sie sie manuell hinzufügen. Klicken Sie dazu auf die Schaltfläche **Andere App zulassen** und geben Sie deren Pfad auf der Festplatte an. Schon wird auch diese App nicht mehr blockiert!



Noch ein wenig komfortabler wird es, wenn Sie eine Firewall-Software von einem Fremdhersteller benutzen, zum Beispiel die in der Internet Security enthaltene Firewall von Bitdefender (http://www.bitdefender.com). Windows 10 lässt beliebige Fremdsoftware zu und integriert deren Funktionen in die eigenen Programme.

Hier können Sie nicht nur einfach den Zugriff eines Programmes auf das Netzwerk zulassen, sondern ganz fein Regeln definieren: in welchem Netzwerk soll der Zugriff zulässig sein? Welches Protokoll darf die App verwenden? Darf sie nur Daten senden oder empfangen oder gar beides? Der Einsatz einer solchen Software macht aber nur Sinn, wenn Sie ganz besondere Anwendungen und ein hohes Sicherheitsbedürfnis haben. Für den Normalanwender reicht die Windows Firewall aus.

So geht's leichter | Sicher im Netz

Kompromittierte Passwörter erkennen

Kompromittierte Passwörter sind die Wurzel alles Übels: In den diversen Datenbanken im Internet, die Benutzernamen und Passwörter enthalten, können sich übelmeinende Genossen bedienen und sich an fremden Konten anmelden. Sind Sie davon betroffen, dann kann das schlimme Auswirkungen haben. Wenn Sie Google Chrome als Browser benutzen, dann können Sie sich die manuelle Prüfung sparen, ob Ihr Account betroffen ist! Laden Sie sich die Erweiterung für Chrome kostenlos hier herunter.

Wenn diese installiert ist, dann zeigt Ihnen Chrome ein grünes Symbol an. sobald Sie einen Benutzernamen und ein Kennwort eingeben, prüft die Erweiterung, ob der Account von einem der Google bekannten Datenlecks betroffen war und warnt automatisch durch ein deutlich sichtbares, rotes Hinweisfeld.

Dabei setzt Google nach eigenen Angaben Techniken ein, die die sensitiven Daten wie Benutzername und Kennwort schützen und gar nicht in die Hände von Google geben. Auf jeden Fall ein Schritt weiter in Richtung der automatischen Information der Benutzer, wenn sie potenziell von einem Sicherheitsleck betroffen sind!

So geht's leichter | Sicher im Netz

Sicherheit auf dem Router

Ihr Internetzugang findet nicht auf Ihrem Rechner statt, sondern klassischerweise auf dem Router. Den bekommen Sie auf von Ihrem Internet-Anbieter meist gestellt, manchmal kaufen Sie ihn auch selbst. Hier gibt es einige Stellschrauben, die Sie in jedem Fall verwenden sollten, um nicht schon ganz vorne in der Kette ein Risiko einzugehen.

Ändern des Kennwortes

Man glaubt es kaum, wie viele Geräte sich im Internet tummeln, die immer noch das Standard-Passwort des Herstellers verwenden. Keine gute Idee, denn diese Kennwörter kann man frei im Internet finden. Und wer Böses will, der probiert als allererstes diese Kennwörter aus, um in Ihren Router zu gelangen.

Wenn Sie sich an Ihrem Router angemeldet haben, dann finden Sie bei den allermeisten Produkten einen Link, unter dem Sie mit Klick auf ein eigenes Passwort vergeben können. Machen Sie sich – wie bei allen Passwörtern – ein wenig Gedanken darüber. Es sollte nicht zu leicht zu erraten sein, aber auch nicht so schwer, dass Sie es sich nicht merken können.

Aktualisierung des Routers

Ebenfalls ein wichtiger Schritt: halten Sie die Firmware, also die interne Software aller Ihrer Geräte immer aktuell. Es kommen immer wieder Sicherheitslücken ans Licht, die die Hersteller dann sehr schnell durch

So geht’s leichter | Sicher im Netz

ein Update beseitigen. So ein Update hilft aber nichts, wenn Sie es nicht installieren.

Sie sollten also regelmäßig bei all Ihren mit dem Internet verbundenen Geräten in den **Einstellungen** unter System nach einem Update suchen. Wird eine neue Version der Software gefunden, dann installieren Sie sie.

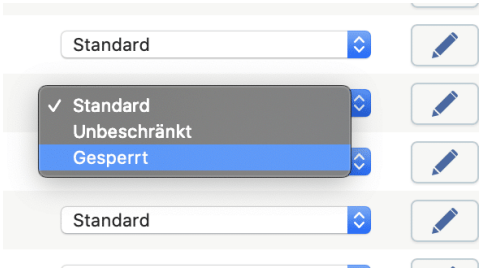
Es kann hier durchaus sinnvoll sein, vor der Installation erst einmal nach der Softwareversion zu Googeln. Es kommt sehr selten vor, aber ein Update kann manchmal auch Dinge „verschlimmbessern“. Ist das der Fall, dann finden Sie im Internet meist sehr zeitnah Fundstellen dazu und können die Installation verschieben, bis der Fehler beseitigt ist. Aus diesem Grund ist das Einschalten der automatischen Installation auch nur bedingt empfehlenswert.

So geht’s leichter | Sicher im Netz

Abkoppeln von Geräten im Router

Normalerweise ist Ihr Router Garant dafür, dass Sie alle Geräte sicher und schnell ins Internet bekommen. Er baut die Internetverbindung auf, und er dient auch als Verteiler für die Anfragen der Geräte. Nun kann es aber sein, dass Sie ein Gerät eben nicht frei ins Internet lassen wollen, sondern den Zugriff verhindert wollen. Statt nun die Verbindung an sich zu trennen, können Sie bei vielen Routern den Zugang für einzelne Geräte regeln.

Diese Funktion versteckt sich meist hinter dem Begriff "Kindersicherung". Nicht nur kritische Geräte, auch Kinder sollen oft nur zu bestimmten Zeiten, mit bestimmten Datenmengen oder eben auch gar nicht ins Internet kommen. Auf der FritzBox beispielsweise gehen Sie zur Einrichtung auf **Internet** > **Zugangskontrolle/Filter** und suchen sich das Gerät aus der Liste heraus. Die FritzBox vergibt Geräten entweder die Namen, unter denen sie im Netzwerk freigegeben sind, oder aber deren IP-Adresse. Die Suche nach dem richtigen Gerät kann also schon einmal einen Moment dauern.



Um nun den Internetzugang zu sperren, wechseln Sie neben dem Gerät in der Auswahlliste von **Standard** zu . Bei der nächsten Verbindung zum Router unterbindet dieser, dass das Gerät ins Internet kommt.

Wenn Sie stattdessen feiner einschränken wollen und beispielsweise nur für bestimmte Zeiträume den Zugriff erlauben oder unterbinden wollen, dann klicken Sie auf den Stift neben dem Gerät und geben Sie die genauen Zeiträume und das Verhalten ein.

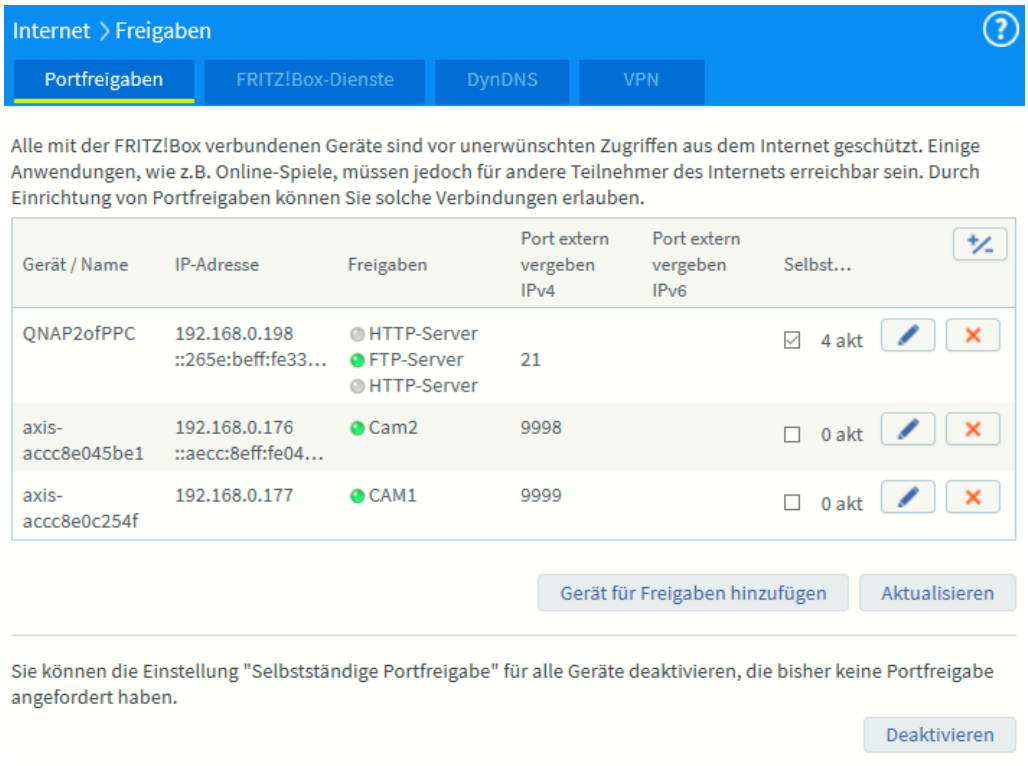
So geht's leichter | Sicher im Netz

Portfreigaben im Router

Für manche Anwendungen kann es sinnvoll sein, Zugriff aus dem Internet auf ein Gerät in Ihrem Netzwerk zu erlauben. Die Netzwerkfestplatte, auf die Sie per FTP zugreifen wollen, die Webcam, die Ihnen auch unterwegs Ihren Garten zeigen soll und vieles mehr ist denkbar. Auch hier ist der Router der Ansatzpunkt.

Unter **Internet** -> **Freigaben** finden Sie die bereits bestehenden Freigaben. Diese funktionieren wie ein Verteiler: Kommt eine Verbindung von außen an Ihren Router, dann geht diese über einen so genannten Port, einen virtuellen Anschluss des Routers. (https://de.wikipedia.org/wiki/Liste_der_standardisierten_Ports)

Im Router legen Sie dann fest, an welches Gerät die Verbindung geleitet werden soll. Beispielsweise einer Anfrage über Port 25, der für FTP-Verbindungen genutzt wird, an die IP-Adresse Ihrer Netzwerkfestplatte.

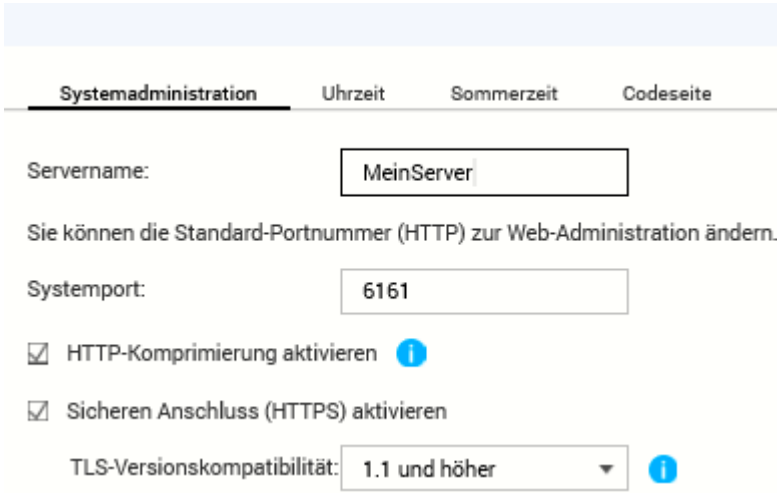


So geht's leichter | Sicher im Netz

Kontrollieren Sie sehr genau, ob die aktuell eingerichteten Freigaben nötig und aktuell sind. Löschen Sie umgehend jede Freigabe, die nicht mehr benötigt wird!

Weg von den Standardports

Wenn Sie Geräte ins Internet stellen, dann sind Portfreigaben, wie wir sie oben beschrieben haben, unabdingbar. Nun ist es aber natürlich so, dass die Standardports bekannt sind, und Angreifer von außen genau auf diese Ports ihre Angriffe starten. Aus diesem Grund sollten Sie überlegen, einfach die Ports Ihrer Geräte von dem Standard weg zuzuweisen. Das NAS läuft beispielsweise statt auf dem Standardport 80 oder 8080 auch wunderbar auf dem Port 6161.



Wenn Sie dann auf das Gerät zugreifen wollen, dann hängen Sie an die Internet- oder IP-Adresse einfach einen Doppelpunkt und den Port an. Beispielsweise MeinServer.dyndny.org:6161. Darauf kommt ein Angreifer nicht so einfach!

So geht's leichter | Sicher im Netz

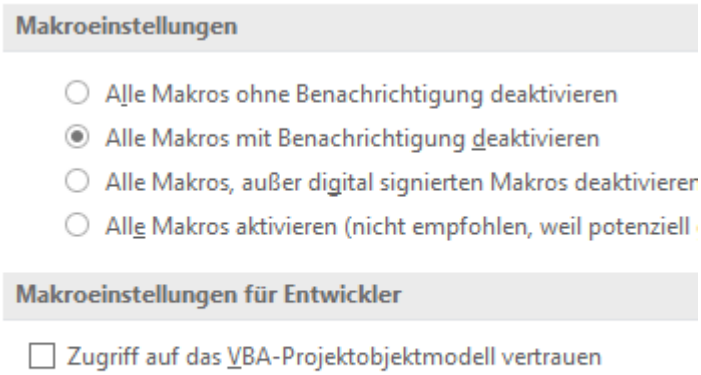
Office sicherer machen

Microsoft Office fällt Ihnen sicherlich als letztes ein, wenn es im das Thema Sicherheit geht. Nichts desto Trotz gibt es auch in den Office-Programmen einige Optionen, die für mehr Sicherheit sorgen. Wir zeigen Ihnen die wichtigsten!

Makros deaktivieren

Nicht nur Programme können Viren enthalten, auch Dokumente, die Sie beispielsweise in Microsoft Word öffnen. Der Hintergrund: Makros, im Hintergrund laufende Prozesse, die beispielsweise Daten aus anderen Dokumenten ziehen und im Dokument aktualisieren und vieles mehr. Auch wenn Makros in Word als Funktionen geliefert werden, sind sie in einer Programmiersprache geschrieben. Eine Kontrolle der Makroausführung ist also wichtig und gar nicht schwer.

Auch wenn eine Textverarbeitung als Programm eher unkritisch erscheint: sie hat eine Menge an Zugriffen auf das System, kann Dateien öffnen, auf Peripheriegeräte zugreifen und vieles mehr. In der praktischen Arbeit als Anwender werden Dokumente mit Makros aber eher die Ausnahme sein, insofern bremst die Einschränkung der Ausführung von Makros Ihre Arbeit normalerweise nicht wirklich aus.



So geht's leichter | Sicher im Netz

Unter Word klicken Sie auf **Datei** -> **Optionen** -> **Trust Center** und dann auf **Makro-Einstellungen**.

Hier können Sie einstellen, ob Makros komplett blockiert werden sollen (**Alle Makros ohne Benachrichtigung deaktivieren**) oder immer automatisch aktiviert werden sollen (**Alle Makros aktivieren**). Beide Einstellungen sind nicht empfehlenswert: Die erste gibt Ihnen keine Information, wenn ein Dokument ein Makro hat (der ja gegebenenfalls sinnvoll und wichtig sein kann). Die zweite nimmt Ohne die Möglichkeit, aufmerksam zu werden, wenn ein Dokument plötzlich ein Makro enthält, der gegebenenfalls bösartig ist.

Wählen Sie am besten **Alle Makros mit Benachrichtigung deaktivieren**: damit müssen Sie die Ausführung von Makros in einem Dokument explizit freigeben und können sich so gegebenenfalls noch beim Ersteller erkundigen, ob das seine Richtigkeit hat. Nach manueller Freigabe in einem Infotext am oberen Rand des Dokumentes werden Makros dann aber ganz normal und ohne Einschränkung ausgeführt.

Richtiges Löschen von Emails

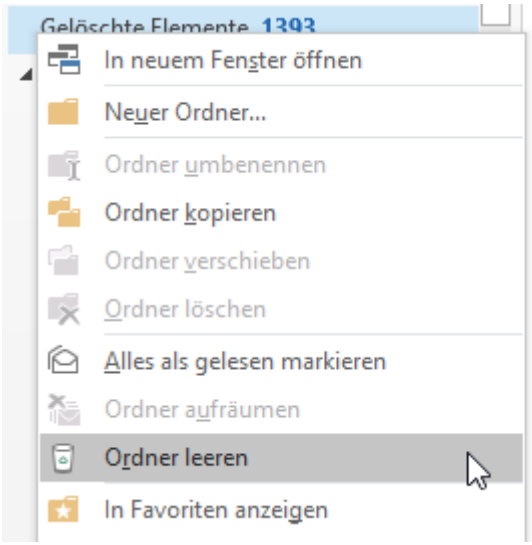
Sie bekommen am Tag viele E-Mails. Nur ein Teil davon ist tatsächlich wichtig, der Rest geht oft ungesehen in den Papierkorb. Dann aber gibt es noch die E-Mails, die wirklich wichtige, teilweise sensible Informationen enthalten. Die benutzen Sie, solange sie sie benötigen. Dann aber sollten Sie sie löschen. Was einfach klingt, bedarf einiger Überlegungen, die wir Ihnen abnehmen wollen.

Zu aller erst ist es beim Löschen von E-Mails wie beim Löschen einer Datei: Die E-Mail ist nicht sofort wirklich gelöscht, sondern landet erst einmal im Papierkorb. Der heißt von Programm zu Programm und von E-Mail-Anbieter zu E-Mail-Anbieter unterschiedlich: Gelöscht, Deleted, Papierkorb, suchen Sie einfach nach einem Ordner eines solchen

So geht's leichter | Sicher im Netz

Namens. Idealerweise löschen Sie die E-Mails darin immer wieder. Klicken sie dazu mit der rechten Maustaste auf den Ordner und dann auf **Ordner leeren**. Erst dann ist eine E-Mail tatsächlich gelöscht.

Wenn Sie eine E-Mail direkt endgültig löschen wollen, dann klicken Sie sie an und drücken gleichzeitig die Tasten **Umschalten** und **Entf**. Nach einer Sicherheitsabfrage ist de E-Mail dann direkt gelöscht und nimmt nicht erst den Umweg über den Papierkorb.



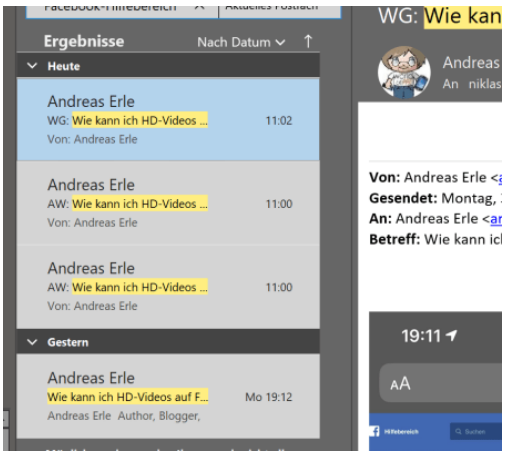
Wenn Sie einen kompletten Mailverlauf löschen wollen, also alle empfangenen und gesendeten E-Mails zu einem Thema:

Besonders in der professionellen Anwendung, aber auch bei komplexeren Diskussionen im Privatbereich kann es schnell vorkommen, dass Sie ein und dieselbe E-Mail mehrfach beantworten und weiterleiten. Wenn es dann darum geht, einen Nachrichtenverlauf zu rekonstruieren, dann wird das schnell unübersichtlich. Outlook bietet aber versteckt eine tolle Möglichkeit, alle mit einer bestimmten Nachricht zusammenhängende neue Nachrichten aufzulisten.

So geht's leichter | Sicher im Netz

Outlook zeigt im Standard an einer Nachricht unter den Betreff- und Adress-Angaben einen Vermerk an, was Sie zuletzt mit der Nachricht gemacht haben. Dort finden Sie beispielsweise „Sie haben diese Nachricht am … weitergeleitet". Nehmen Sie aber die Quellnachricht und beantworten Sie diese dann noch einmal, dann werden der Text und der Zeitstempel ersetzt. Es wird als immer nur eine Aktion dargestellt.

Um nun alle zugehörigen Nachrichten zu sehen, klicken Sie mit der rechten Maustaste auf den Infotext. Wählen Sie dann **Nachrichten zum gleichen Thema suchen**. Outlook startet nun eine Suche nach allen E-Mails in allen Verzeichnissen Ihres Postfaches, die sich auf die Quell-E-Mail beziehen.



Die gefundenen Ergebnisse werden chronologisch sortiert in einer Liste dargestellt. Wenn Sie die Sortierung ändern wollen, dann klicken Sie auf das Dreieck neben **Nach Datum** und wählen Sie dann das gewünschte Sortierkriterium.

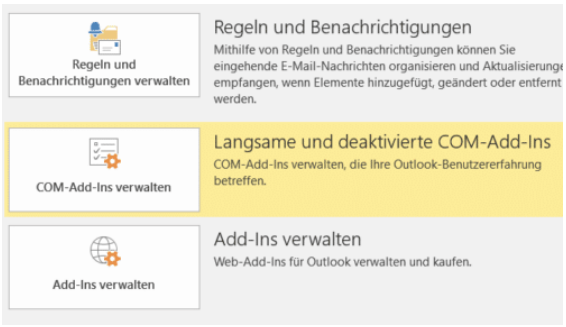
Die gefundenen E-Mails können Sie dann alle markieren und wie oben beschrieben endgültig löschen.

So geht's leichter | Sicher im Netz

Outlook Addins deaktivieren

Wenn Sie Programme oder Hardware installieren, dann installieren diese manchmal Erweiterungen von Outlook, so genannte Add-ins. So schön diese auch sind, wenn Sie sie nutzen wollen, so risikoreich können sie sein. Add-ins haben Zugriff auf Ihre Outlook-Daten und können damit allerhand anstellen.

Unter **Datei** > **Add-Ins verwalten** können Sie alle installierten Add-Ins aufrufen.



Klicken Sie jedes Add-In an, das sie nicht mehr benötigen. Über die Schaltfläche **Dieses Add-in deaktivieren** können sie es dauerhaft deaktivieren. Damit wird es beim Start von Outlook nicht mehr geladen. Die Funktionalität steht Ihnen dann aber selbstredend auch nicht zur Verfügung.

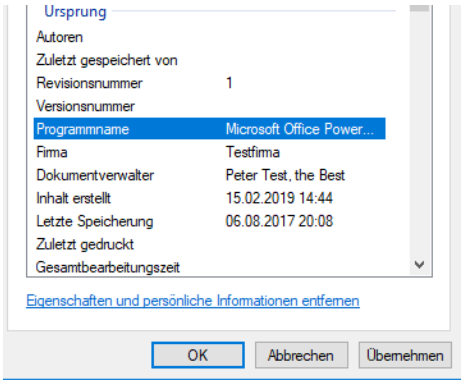
Es empfiehlt sich, Outlook nach einem Neustart des Rechners erneut zu starten. Erst, wenn das Add-in weiterhin zu einem Absturz führt, sollten Sie es dauerhaft deaktivieren.

Löschen von Dokumenteneigenschaften

Man glaubt es kaum: Bei geleakten Dokumenten sind oft nicht einmal die Inhalte kritisch, denn die haben Sie im Blick. Was viele Anwender aber nicht wissen: Microsoft Office pflegt eine Vielzahl von (Meta-) Informationen, die Sie so nicht sehen. Sind diese ausgefüllt und die Datei wird weitergegeben, dann kann das schnell zu Verwerfungen führen. Die Pflege und das Löschen dieser Eigenschaften sind aber schnell gemacht.

So geht's leichter | Sicher im Netz

Öffnen Sie den Speicherort der Datei, deren Eigenschaften Sie löschen oder verändern wollen. Dann klicken Sie mit der rechten Maustaste darauf und dann im sich öffnenden Menü auf **Eigenschaften**.



Unter der Liste der Eigenschaften können Sie durch einen Klick auf Eigenschaften und persönliche Informationen entfernen deren Änderung einleiten.

Sie können entweder eine Kopie der Datei anlegen, in der alle Eigenschaften entfernt worden sind (deren Inhalt aber natürlich unverändert ist) oder durch einen Klick auf **Folgende Eigenschaften aus der Datei entfernen** einzeln anwählen, welche Eigenschaften geleert werden sollen. So wird schnell aus einer irgendwo kopierten Datei das eigene Werk.

Daten und Dateien verschlüsseln

Ihre Dateien sind das A und O Ihrer Arbeit am Rechner. Sie wollen meist nicht, dass ein Unbefugter auf diese zugreifen kann und sehen kann, womit Sie sich beschäftigt haben. Darum verschlüsseln Sie Festplatte und Dateien!

Die gute Nachricht: Windows 10 hat mit Bitlocker eine Verschlüsselungssoftware mit an Bord, die Datenträger außerhalb Ihres Rechners unlesbar macht. Dies basiert auf dem so genannten Trusted Platform Module (TPM), einem Hardware-Modul, das in vielen Rechnern verbaut ist und quasi den Schlüssel zu Ihrer Festplatte darstellt.

So geht's leichter | Sicher im Netz

Tipp Wenn Sie nur die Home-Version von Windows 10 installiert haben und auch nicht das kostenpflichtige Update auf die Pro- oder Enterprise-Version machen möchten, oder kein TPM in Ihrem Rechner haben, dann empfiehlt sich VeraCrypt (https://www.veracrypt.fr/en/Downloads.html) als kostenlose Open-Source-Software.

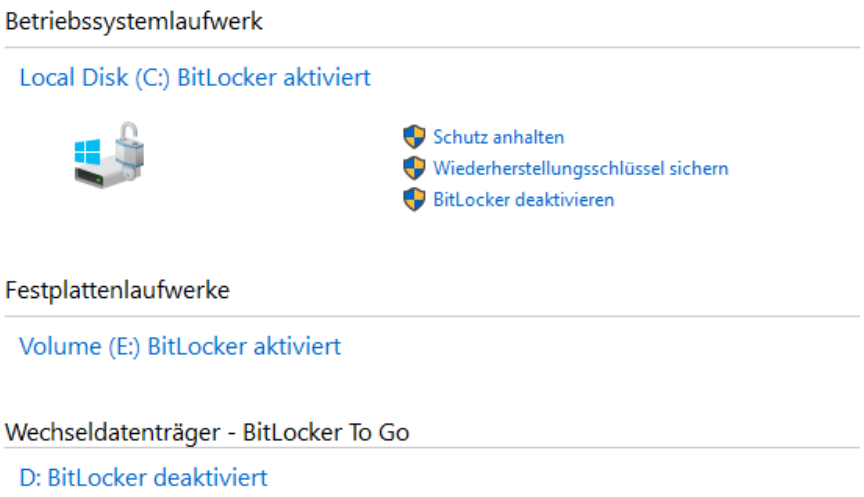
Wird die Festplatte entnommen und in einen anderen Rechner eingebaut, dann hat dieser einen anderen Schlüssel und kann die Daten nicht lesen: Ihre Daten sind dann nur unleserlicher Bitbrei, der dem Dieb nichts nützt.

Aktivierung von Bitlocker

Die Aktivierung und Deaktivierung von Bitlocker für Festplatten findet sich im Windows Explorer. Klicken Sie mit der rechten Maustaste auf die Festplatte, die verschlüsselt werden soll (meistens also C:) und dann auf **Bitlocker Aktivieren** (bzw. **Bitlocker Verwalten**).

Folgen Sie nun den Anweisungen auf dem Bildschirm, um Bitlocker zu aktivieren. Im normalen Betrieb werden Sie hier keine Unterschiede erkennen, Die Festplatte ist nicht spürbar langsamer und Sie müssen auch beim Systemstart kein zusätzliches Kennwort eingeben. Letzteres

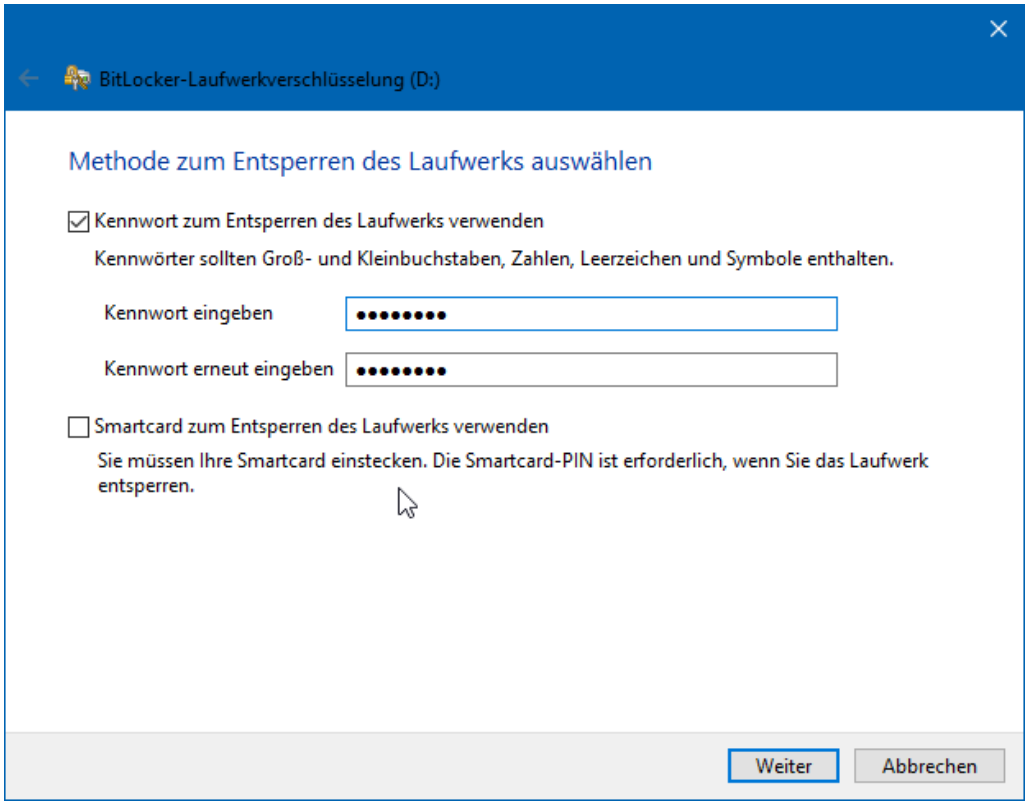
übernimmt hier das TPM-Modul im Hintergrund für Sie!



Bitlocker ist in der Standardversion nur für Festplatten gedacht. Wenn Sie häufiger mit einem USB-Stick unterwegs sind, dann haben Sie natürlich eine weitere Gefahrenquelle zu beachten: Verlieren Sie einen USB-Stick, dann verlieren Sie natürlich auch ungeschützte Daten darauf. Bitlocker kann ohne ein – auf einem USB-Stick nicht vorhandenes – TPM-Modul natürlich nicht funktionieren. Das mach aber nichts: Windows 10 bietet dafür **Bitlocker To Go**, eine Verschlüsselung für mobile Datenträger.

Die Aktivierung verläuft ähnlich: Im Explorer machen Sie einen Rechtsklick auf das USB-Laufwerk, dann auf **Bitlocker Aktivieren**.

So geht's leichter | Sicher im Netz



Hier können Sie nun auswählen, ob Sie vor der Verwendung des Sticks ein Passwort eingeben wollen (das wird der Standardfall sein) oder eine Smartcard verwenden wollen.

Geben Sie das gewünschte Passwort (unter Beachtung der diskutierten Passwortregeln) zweimal ein und voila: Ohne Passwort keine Daten! Die Entsperrung des Sticks muss jeweils nur dann gemacht werden, wenn Sie es in den PC einlegen. Während des Betriebs bleibt das Laufwerk entsperrt. Entwendet Ihnen jemand den Stick aus dem gesperrten PC, dann kann er damit einmal mehr nichts anfangen.

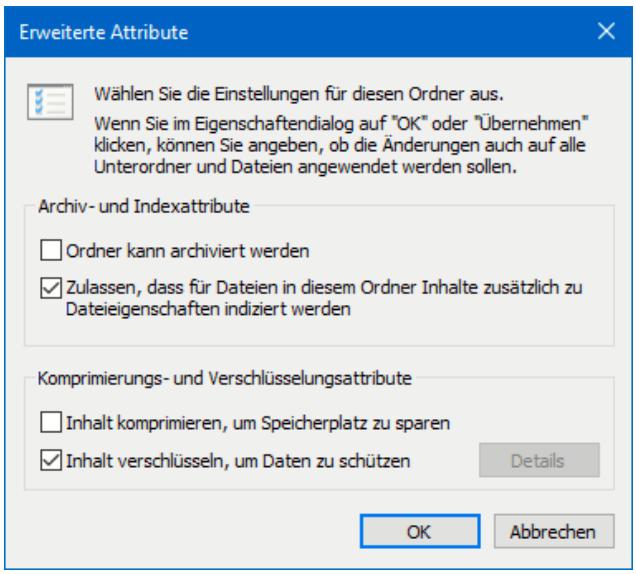
Verschlüsseln einzelner Dateien

Doppelt gemoppelt hält besser. Bitlocker ist eine schöne und vor allem leicht einzusetzende Möglichkeit, eine Festplatte zu verschlüsseln. Wenn

So geht's leichter | Sicher im Netz

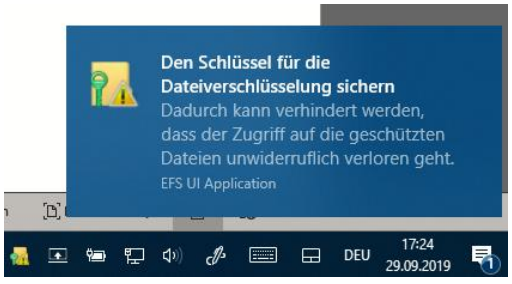
sie zusätzlich einzelne Dateien nochmal verschlüsseln wollen, dann geht das bei einem Windows 10 Pro- oder Enterprise-System ebenfalls mit Bordmitteln. EFS (Encrypted File System) heißt hier das Zauberwort.

Um eine Datei zu verschlüsseln, klicken Sie im Windows Explorer einfach mit der rechten Maustaste auf eine Datei. Dann können Sie in der Registerkarte **Allgemein** auf **Erweitert** klicken. Ganz unten sehen Sie dann **Inhalt verschlüsseln, um Daten zu schützen**.



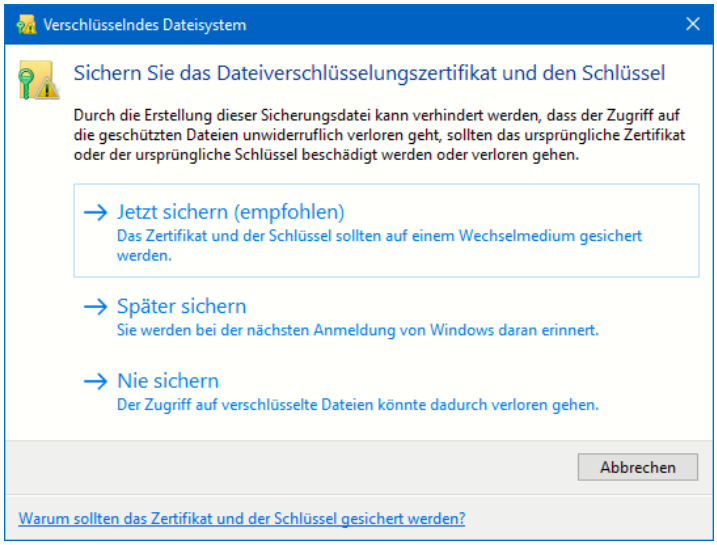
Nachdem Sie das angewählt haben, haben die betroffenen (und jetzt verschlüsselten) Dateien und Ordner ein kleines Schloss als Symbol. Auf dem selben Weg können Sie die Verschlüsselung wieder rückgängig machen.

Wichtig zu wissen: Die Verschlüsselung hängt am Benutzerkonto. Sobald sich jemand erfolgreich anmeldet, kann er die Dateien entschlüsseln. Geben Sie per EFS verschlüsselte Dateien per E-Mail oder einem Datenträger weiter, dann wird automatisch die Verschlüsselung aufgehoben.



Was aber, wenn Sie selbst nicht mehr an Ihr Benutzerkonto kommen, weil Sie die Zugangsdaten vergessen haben? Windows 10 versucht dies zu

verhindern, indem es Sie beim ersten Verschlüsseln einer Datei daran erinnert, ein Backup der Schlüssel durchzuführen.



Dazu zeigt Ihnen Windows nicht nur kurz einen Dialog an, sondern auch gleich ein Symbol im Tray. Klicken Sie auf das Symbol, dann auf **Jetzt sichern**. Folgen Sie den Dialogen, und geben Sie neben dem Zielort für die Sicherung (am besten ein USB-Stick, den Sie sicher weglegen können) auch ein Kennwort an. Ohne dieses kann der Schlüssel nicht mehr wiederhergestellt werden.

Verschlüsseln von Dateien in einem ZIP-Archiv

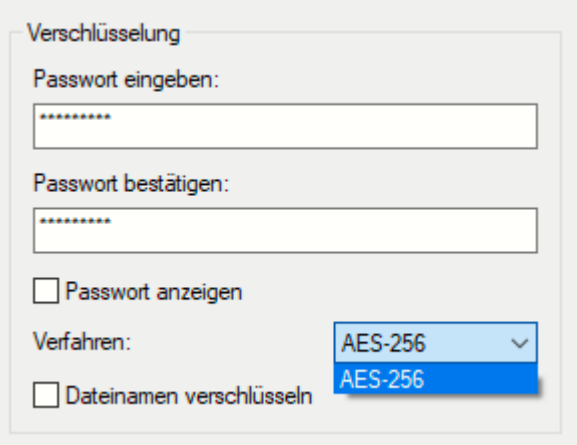
Wenn Sie sich nicht auf die Verschlüsselung auf der Festplatte verlassen wollen oder Dateien per E-Mal oder USB-Stick weitergeben müssen, dann verschlüsseln Sie sie einfach in einem Archiv. 7-Zip (https://www.7-zip.de/) ist ein gebräuchliches Archivierungsprogramm, das zudem auch noch kostenlos ist.

Nachdem Sie es installiert haben, starten Sie den Explorer und suchen Sie sich die Datei(en) heraus, die Sie verschlüsseln wollen. Markieren Sie sie, dann klicken Sie mit der rechten Maustaste hinein. Im Kontextmenü klicken Sie dann auf **7-Zip** > **Zu einem Archiv hinzufügen**.

Stellen Sie nun den Archivtyp auf **.ZIP** ein, damit können so gut wie alle gebräuchlichen Archiv- und Kompressionsprogramme die Datei öffnen.

So geht's leichter | Sicher im Netz

Unter Verschlüsselung können Sie jetzt ein Passwort eingeben. Das wird dazu verwendet, um das Archiv, das dann die Dateien enthält, zu verschlüsseln. Ohne das Passwort – oder signifikante Rechenleistung, um es zu knacken – kommt niemand mehr an die Dateien heran. Das so verschlüsselte Archiv können Sie dann bequem per E-Mail oder USB-Stick weitergeben. Der Empfänger wird beim Versuch, es zu öffnen, nach dem Passwort gefragt. Kennt er es nicht, wird das Archiv nicht geöffnet und die Dateien bleiben sicher verschlossen darin.



Sicheres Löschen von Dateien

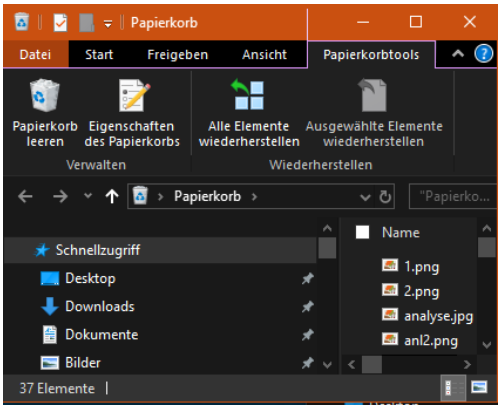
Das Löschen von Dateien ist nicht nur eine Sache des vernünftigen Umgangs mit Speicherplatz, sondern manchmal auch eine der Geheimhaltung. Bestimmte Daten müssen und sollen einfach nicht mehr auf Ihrem Rechner vorhanden sein, wenn Sie sie nicht mehr benötigen. Insofern ist es wichtig, Dateien richtig zu löschen.

Das Löschen von Dateien hat mehrere Ebenen. Eine Datei wird im Dateisystem abgelegt, ist aber nicht notwendigerweise ein zusammenhängender Daten-Container. Die Bits und Bytes, aus denen sie besteht, sind irgendwo auf der Festplatte abgelegt. Windows 10 verwaltet dann die Zuordnung von Dateien und zugehörigen Daten. Wenn Sie nun eine Datei über den Explorer löschen, dann landet die Datei im Papierkorb.

So geht's leichter | Sicher im Netz

Die Idee ist genial: Wie im Büro können Sie die Datei dort wiederherstellen. Das heißt aber auch: Die Datei ist immer noch für jeden vorhanden, der auf ihren Rechner zugreifen kann. Erst wenn Sie im Papierkorb auf **Papierkorb leeren** klicken, dann ist die Datei gelöscht. Die ist zwar dann immer noch als Bytewolke auf der Festplatte vorhanden, kann aber so einfach nicht mehr wiederhergestellt werden.

Sie können den Papierkorb aber auch direkt umgehen und so das manuelle Entfernen aus dem Papierkorb vermeiden: Ziehen Sie die Datei mit gedrückter **Shift-Taste** in den Papierkorb, dann löschen Sie sie sofort vollständig.



Tipp

Auch beim Löschen aus dem Papierkorb sind die Bits und Bytes der Datei noch auf der Festplatte vorhanden und können mit entsprechenden Tools wiederhergestellt werden. Um das zu vermeiden, müssen Sie die Teile der Festplatte, die freigegeben sind, tatsächlich überschreiben. „Irgendwann" passiert das automatisch, wenn neue Dateien dort gespeichert werden. Wenn Sie den Prozess beschleunigen wollen, dann nutzen Sie ein Tool wie den CCleaner (https://www.ccleaner.com/de-de/ccleaner).
Smartphones sicher machen

Smartphones sicherer machen

Wenn Sie an Sicherheit Ihres Smartphones denken, dann ist der erste Gedanke sicherlich der an den Zugangsschutz mittels PIN, Passwort,

So geht's leichter | Sicher im Netz

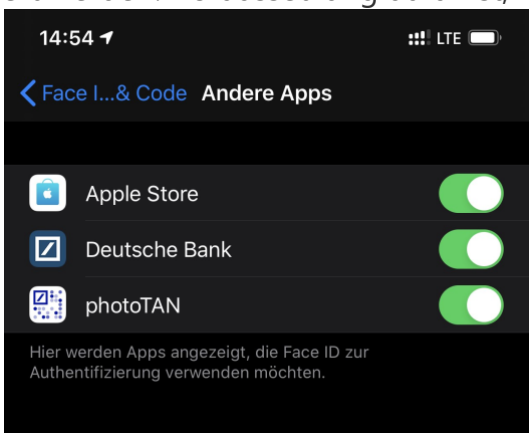
Fingerabdruck- oder IRIS-Scanner. Das ist aber nur ein Teil dessen, was Sie machen können!

Apps auf dem iPhone per Face ID schützen

Mehr und mehr Anwendungen wandern vom stationären PC auf das Smartphone. Zum einen, weil die Technik entsprechend weit ist, zum anderen, weil wir als Anwender immer mobiler und mehr unterwegs sind. Je mehr Sie unterwegs erledigen können, desto bequemer ist es schließlich!

iOS kennt einige Standardanwendungen, die per Face ID (übrigens auch dem Fingerabdrucksensor Touch ID) geschützt werden können. Diese finden Sie unter **Einstellungen** > **Face ID & Code** > **Face** ID verwenden für. Aktivieren Sie alle, wenn das nicht schon der Fall ist.

Auch Store-Apps können über die Gesichts- oder Fingerabdruckerkennung abgesichert werden. Voraussetzung dafür ist, dass die App selber eine Authentifizierung unterstützt. Das ist beispielsweise bei Outlook, vielen Banking- und Passwort-Apps der Fall. Diese finden Sie unter **Einstellungen** > **Face ID & Code** > **Andere Apps**.



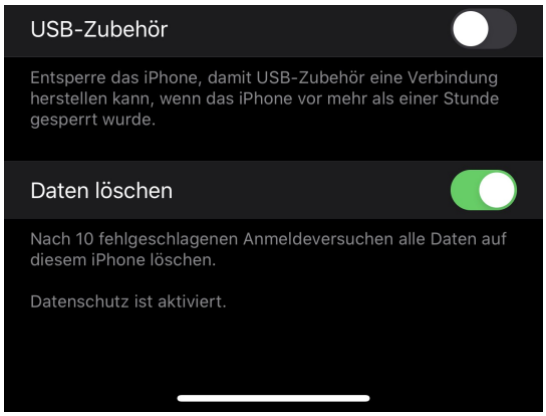
Hier finden Sie alle Apps aufgeführt, die die Authentifizierung unterstützen. Aktivieren Sie alle, bei denen Sie den zusätzlichen Schutz einer Anmeldung vor dem Start in Anspruch nehmen wollen. Der zusätzliche Aufwand ist gut investierte Zeit!

So geht’s leichter | Sicher im Netz

iPhones vor Verlust und Diebstahl absichern

Früher waren die Handys noch recht uninteressant für Bösewichte, die Informationen über Sie erhalten wollten. Das hat sich mit der Einführung der Smartphones deutlich geändert: Nicht nur Anrufe, Kontakte, E-Mails und Nachrichten sind potenziell vertraulich, auch die Daten, die Sie in den unzähligen Apps eingeben. Grund genug, Ihr Smartphone gut zu sichern!

Die neueren iPhones haben mit Face ID eine zusätzliche Kamera integriert, die Ihr Gesicht einmal scannt und dann mit demjenigen, der Ihr Telefon entsperren will, vergleicht. Das lässt sich nicht mit einem Foto täuschen. Auch verschiedene Android-Geräte haben solche Kameras an Bord. Alternativ Fingerabdrucksensoren, im einfachsten Fall zumindest eine PIN. Ohne eine dieser Anmeldemethoden kann niemand an die Daten und Apps Ihres Gerätes. Es sei denn, er hat genug Zeit und versucht alle möglichen PINs nacheinander.



Nahezu alle Smartphones bieten hier eine automatische Löschung an, wenn eine gewisse Zahl an Fehlversuchen überschritten ist. Beim iPhone aktivieren sie diese beispielsweise unter Einstellungen -> Face ID & Code -> Daten löschen. Nach zehn fehlgeschlagenen Versuchen wird das Gerät dann gelöscht. Damit sind Ihre Daten nicht mehr in Gefahr. Die Kehrseite: Wenn Sie aus Versehen den Code mehrfach falsch eingeben (zum Beispiel, weil das Gerät eingeschaltet in der Hosentasche steckt), dann sind die Daten natürlich ebenfalls weg!

So geht's leichter | Sicher im Netz

Passwörter sicher offline speichern mit Smartphone-App

Passwörter sind die Grundlage für jede Sicherheit. Egal, ob Sie online einkaufen, sich am Banking oder bei Ihrer Versicherung anmelden, Ihr Passwort ist die erste Sicherheitsschicht. Und die sollte sich von Zugang zu Zugang, von Internetseite zu Internetseite unterscheiden. Nehmen Sie jetzt noch die PINs Ihrer Kunden- und EC-Karten, und Sie haben eine unübersichtliche Vielzahl von Zugangsdaten. Wenn Sie die nicht auf Ihrem Smartphone speichern wollen, ist PIN-Safe vielleicht eine Alternative.

Einer der großen Unsicherheitsfaktoren bei der Speicherung Ihrer Kennwörter auf dem Smartphone ist das Vertrauen zu den Herstellern: Nicht erst die Diskussion um Huawei befeuert die Befürchtung, dass die Hersteller Daten auf den Geräten für eigene Zwecke nutzen könnten. Auf der anderen Seite ist das Aufschreiben auf einen Zettel auch keine Alternative. Der deutsche Hersteller PIN-SAFE versucht die beiden Welten zu kombinieren.

Der PIN-SAFE ist eine kreditkartengroße Karte, die in die Kartenfächer der Geldbörse passt. Auf einem verschlüsselten Chip werden Ihre Zugangsdaten dann gespeichert. Allerdings ist der Platz relativ beschränkt: "bis zu 50" passen darauf.

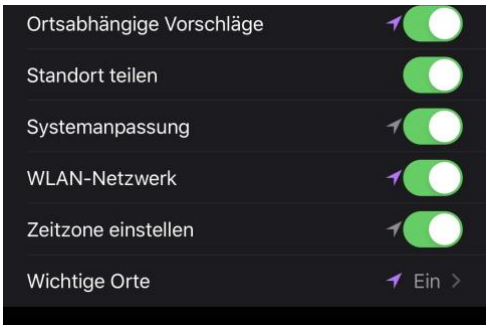
Der Clou: Die Daten bleiben auf der Karte und werden nur kontaktlos bei Verwendung der App flüchtig gespeichert. Nur bei der Abfrage oder Speicherung eines Kennworts. Dadurch sind die Kennwörter vom Smartphone getrennt, trotzdem aber darüber verfügbar. Den PIN-Safe gibt es für EUR 19,90 hier.

Datenschutz auf dem iPhone: Geheime wichtige Orte

Unser Smartphone ist steter Begleiter und damit auch unbestechlicher Zeuge unserer Aktivitäten. Das ist auf der einen Seite vorteilhaft. Auf der

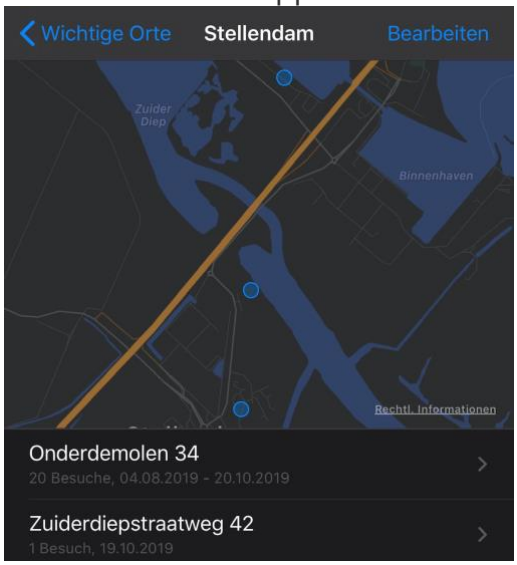
So geht's leichter | Sicher im Netz

anderen Seite befinden sich damit auf unseren Geräten Informationen, die dem Unberechtigten viel verraten können. Einer dieser Speicher auf dem iPhone ist relativ unbekannt: Die Wichtigen Orte. iOS speichert im Standard, wo Sie wann waren und fasst es übersichtlich zusammen. Wir zeigen Ihnen, wo Sie diese Einstellung finden und deaktivieren können.



Viele der positionsbezogenen Datenschutzeinstellungen finden Sie unter **Einstellungen** > **Datenschutz**. Tippen Sie dann auf **Ortungsdienste**. Im Standard sind diese eingeschaltet, sonst lassen sich viele Apps gar nicht nutzen. Sie sollten diese also nicht generell ausschalten, sondern App für App und Dienst für Dienst entscheiden.

Unter der Liste der Apps finden Sie den Eintrag **Systemdienste**. Dort finden Sie eine Vielzahl von Diensten, die zusätzlich die Position verwenden. Den ein oder anderen können Sie hier problemlos ausschalten. Am besten nach und nach, damit Sie bei einer nicht mehr funktionierenden App sehen können, die Einstellung noch kennen. Ganz unten finden Sie **Wichtige Orte**. Hier finden Sie eine chronologische Liste der Orte, die Sie besucht haben. Dabei ist nicht nur die Stadt aufgeführt, sondern nach einem Tipp en auf den Eintrag auch die genaue Adresse in dieser Stadt. Anhand der angezeigten Karte können Sie bis



So geht's leichter | Sicher im Netz

auf das Haus erkennen, wo das Gerät wann war.

Einzelne Einträge können Sie löschen, indem Sie auf **Bearbeiten** tippen und dann auf das **Stoppschild** neben der Adresse. Alle Einträge löschen Sie, indem Sie auf **Verlauf löschen** tippen.

Android-Geräte per Bluetooth entsperren

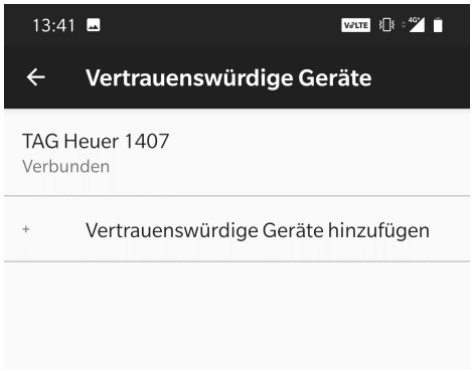
Ein mobiles Gerät wie ein Smartphone ist immer angreifbar. Alleine deshalb, weil es unterwegs immer mal wieder Fremden zugänglich ist. Das gleichen Sie durch Fingerabdrucksensoren, TOF-Kameras und Kennwortschutz aus. Es gibt aber Situationen, wenn das Entsperren zusätzlicher, unnötiger Aufwand ist. Beispielsweise, wenn Sie das Gerät bei sich haben oder es sich an Orten befindet, die Sie als sicher klassifizieren. Die Lösung dafür heißt Smart Lock, eine Funktion, die Android direkt mitbringt.

Aktivieren Sie sie unter **Einstellungen** > **Sicherheit und Sperrbildschirm** > **Smart Lock**. Android bietet Ihnen verschiedene Bedingungen, an denen Ihr Smartphone entsperrt bleiben kann.

Die **Trageerkennung** ist sicherlich die unsicherste Variante: Solange das Gerät bewegt wird, bleibt es entsperrt. Niemand sagt Android allerdings, dass es Sie sind, der es bewegt. Insofern können Sie diese Option eher vernachlässigen.

Wenn Sie an bestimmten Orten alleine an Ihr Gerät kommen, dann definieren Sies diese Orte einfach als **Vertrauenswürdige Orte**. Befindet sich Ihr Smartphone in einem engen Radius um einen solchen Ort, wird es nicht gesperrt.

So geht's leichter | Sicher im Netz



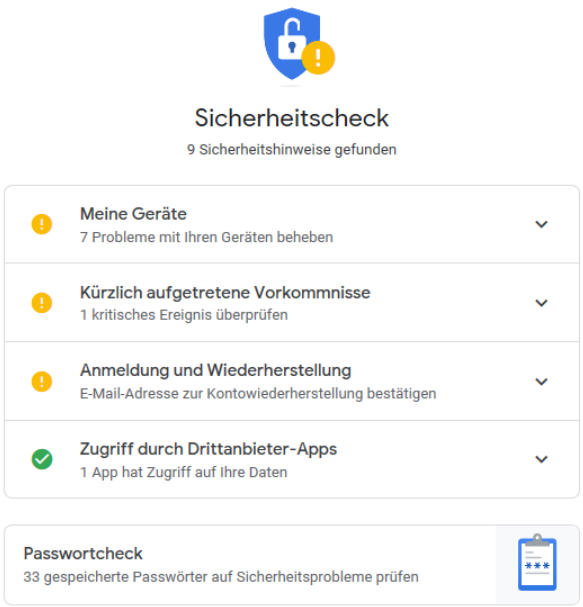
Noch sicher ist es, wenn Sie eine Smartwatch besitzen: Sobald diese in der Nähe des Telefons ist, sind auch sie da. Die Festlegung eines anderen Bluetooth-Gerätes als **Vertrauenswürdiges Gerät** schafft ein hohes Maß an Sicherheit. Ein anderes Beispiel ist die Freisprecheinrichtung des Autos. Diese hat weniger mit Sicherheit zu tun, vereinfacht es aber, das Gerät unterwegs zu bedienen.

Wie sicher ist mein Google-Konto? Der Sicherheitscheck

An den Diensten von Google kommen Sie kaum noch vorbei. Wenn Sie ein Smartphone mit Android als Betriebssystem haben, dann nutzen Sie den Play Store, GMail, das Google Drive und andere Services. Aber auch bei einer normalen Websuche läuft Ihr Google-Konto im Hintergrund mit, um Daten zu sammeln und Sie damit zu unterstützen. Kurz: Google kennt eine Menge Daten von Ihnen. Führen Sie regelmäßig den Google-Sicherheitscheck durch, um Risiken zu minimieren! Wenn Sie dann eine Gefahr für Ihr Konto angezeigt bekommen, dann können Sie die schnell schließen und es damit wieder sicher machen.

So geht’s leichter | Sicher im Netz

Nach Aufruf der Seite und Anmeldung mit Ihren Google-Kontodaten zeigt Ihnen der Sicherheitscheck die gefundenen Sicherheitsrisiken an. Keine Sorge: Nicht alle sind wirklich gefährlich, sollten aber einzeln betrachtet werden.



Unter **Meine Geräte** zeigt Google alle Geräte an, die schon länger nicht mehr mit den Google-Diensten verbunden waren. Das passiert vor allem dann, wenn Sie ein Gerät verkauft haben. Da Sie das sicherlich gelöscht haben, kann damit nichts mehr passieren. Trotzdem: Löschen Sie nicht mehr vorhandene Geräte aus Ihrem Google-Konto!

Kürzlich aufgetretene Vorkommnisse sind Anmeldungen, die von fremden Geräten oder unüblichen Orten durchgeführt wurden. Kontrollieren Sie hier, ob das wirklich von Ihnen ausgelöst wurde. Wenn nicht, klicken Sie auf **Nein, das war ich nicht**. In einem solchen Fall sollten Sie dringend Ihr Kennwort ändern!

Google speichert auf Wunsch Ihre Passwörter. Das hilft, wenn Sie sie sich nicht merken wollen. In diesem Zusammenhang bietet Ihnen Google dann auch eine Überprüfung an, ob diese zu einfach sind oder dem aktuellen Stand der Sicherheitsanforderungen genügen. Identifiziert Google ein Kennwort, das nicht sicher ist, dann ändern Sie es zeitnah auf der Internetseite, zu der es gehört!

So geht’s leichter | Sicher im Netz

Updates, Updates, Updates

Ob Sie am PC, am Smartphone, mit einem Smarthome-Gerät oder einer Konsole online sind: Eines ist im Hinblick auf die Sicherheit all diesen Geräten gleich: Sie haben eine Betriebssoftware. Ob die nun iOS, Android, Windows 10, macOS oder FRITZ!OS heißt, ist vollkommen egal. Keine Software ist perfekt. Auch beim ausführlichsten Test gehen Fehler unter, werden erst später erkannt oder entstehen durch äußere Bedingungen.

Der Vorteil hierbei: Sie müssen sich nicht darum kümmern, dass diese behoben werden, sondern der Hersteller übernimmt das für Sie. Ohne Ihre Mitwirkung aber geht es nicht: Sie müssen die Updates installieren. Ob Sie nun automatische Updates einschalten und zulassen oder regelmäßig manuell danach suchen, viele Angriffe uns Sicherheitslücken werden damit schnell behoben.

So geht's leichter | Sicher im Netz

Autoren:
Jörg Schieb
Andreas Erle

Impressum:
Redaktion Schieb
Humboldtstr. 10
40667 Meerbusch
Kontakt: fragen@schieb.de
www.schieb.de