So geht's leichter...

So klappt's mit dem Datenschutz

- Daten schützen in Office
- Es muss nicht immer Cloud sein
- Wichtige Daten verschlüsseln
- Sicher kommunizieren
- Sicher im Netz surfen

Autoren:
Jörg Schieb
Andreas Erle

So geht’s leichter | Datenschutz fängt bei mir an

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

So geht's leichter | Datenschutz fängt bei mir an

So geht's leichter | Datenschutz fängt bei mir an

So geht’s leichter | Datenschutz fängt bei mir an

Datenschutz – kaum ein Begriff hat in den letzten Jahre für so viele Diskussionen geführt. Sicherlich befeuert durch die Datenschutz-Grundverordnung (DSGVO), die 2018 endlich einen einheitlichen gesetzlichen Rahmen für den Datenschutz in Europa geschaffen hat.

Die Zahl der Datenschutzvorfälle, beiden denen personenbezogene Daten von Benutzern entweder aus Absicht oder durch einen Einbruch abhandengekommen und verwendet worden sind.

Datenschutz hat viele technische Komponenten. Die nützen aber alle nichts, wenn Sie als Anwender nicht genauso darauf achten, dass Ihre Daten geschützt sind. Durch vorsichtigen Umgang damit, indem Sie darauf achten, wer welche Daten bekommt und was Sie selbst über sich preisgeben.

Wir zeigen Ihnen, wie Sie beide Aspekte gleichermaßen im Auge behalten und trotzdem noch effektiv arbeiten können. Im Netz, in der Cloud und in sozialen Netzwerken genauso wie im analogen Leben!

So geht’s leichter | Datenschutz fängt bei mir an

Office und Dateien: Sicherer Austausch

Keine Frage: Sie müssen Daten mit anderen Anwendern austauschen, daran geht heutzutage kein Weg mehr vorbei. Dokumente, Tabellen und andere Dateien enthalten Informationen, die je nach Natur des Dokumentes durchaus kritisch sein können. Durch die rechtliche Brille betrachtet bezieht sich Datenschutz immer auf Daten, die auf eine natürliche Person Rückschluss erlauben. Unabhängig davon aber sind natürlich auch andere Informationen in dem falschen Händen unangenehm und potenziell schädlich.

Bevor Sie also Dateien online stellen oder schnell mal eben verschicken, machen Sie sich ein paar Gedanken dazu.

Datensparsamkeit und Zugriff absichern

Im Datenschutz ist der Begriff der „Datensparsamkeit“ immer wieder zu lesen. Dabei geht es darum, dass so wenig Daten wie möglich verarbeitet werden sollen oder andersherum: nur so viel wie nötig.

In der Praxis ist das oft anders: Sie sammeln alle Informationen, derer Sie habhaft werden können und speichern diese ab. Wenn Sie dann Dateien mit andren Anwendern teilen, dann befinden sich darin oft Informationen, die diese gar nichts angehen und die Sie vielleicht auch gar nicht weitergeben wollen.

Schauen Sie also auf jeden Fall einmal kritisch über die Inhalte, bevor Sie sie verschicken!

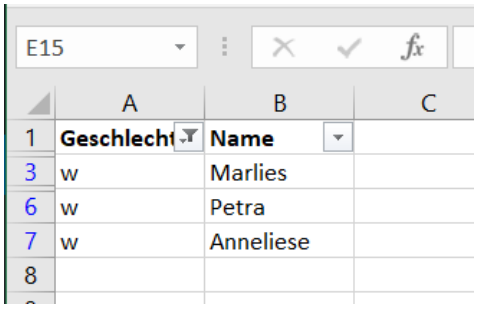
So geht's leichter | Datenschutz fängt bei mir an

Vorsicht bei gefilterten Excel-Listen

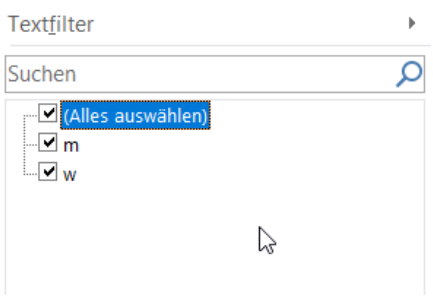
Wenn Sie eine Excel-Datei versenden wollen, dann ist eine vermeintlich gute Möglichkeit, nur die den Empfänger interessierenden Daten zu versenden die Filterung von Daten. Diese ist aber nicht ganz unkritisch!

Das Filtern von Daten ist dazu gedacht, aus einer großen Datenmenge nur Daten bestimmter Ausprägung herauszufiltern. Beispielsweise aus einer Liste von Personen nur die, die als Geschlecht "weiblich" haben. Zum Aktivieren der Filterung markieren Sie die Zellen, die gefiltert werden sollen, dann klicken Sie auf **Daten** > **Filter**.

In der obersten Zeile der Tabelle wird nun eine Dreieck nach unten angezeigt. Klicken Sie darauf, dann sehen Sie alle Ausprägungen der entsprechenden Spalte.



Um alle Ausprägungen der Zellen angezeigt zu bekommen, klicken Sie auf **Alles auswählen**. Um zu filtern, klicken Sie die Werte an, die Sie angezeigt bekommen möchten. Excel blendet nun alle Zeilen aus, in denen der ausgewählte Wert nicht enthalten ist.



Warum nun Vorsicht? Die durch den Filter ausgeblendeten Zellen sind immer noch da. So mancher Benutzer hat sich einigen Ärger eingefangen, weil er das nicht beachtet hat. Wenn sie also beispielsweise die Umsätze eines bestimmten Kunden filtern, dann senden sie ihm nicht die gefilterte Tabelle. Er kann den Filter

entfernen und damit alle anderen Daten sehen! Stattdessen kopieren Sie die ihn betreffenden Datensätze in eine neue Tabelle.

Es muss nicht immer die (große) Cloud sein

OneDrive, Dropbox und andere Cloud-Dienste sind ohne Frage eine große Hilfe in der täglichen Arbeit. Die Daten liegen nur als synchronisierter Bestand auf Ihren Geräten, zusätzlich aber auch auf einem fremden, abgesicherten Server. Über diesen können Sie die Daten dann freigeben und anderen Anwendern Zugriff darauf geben.

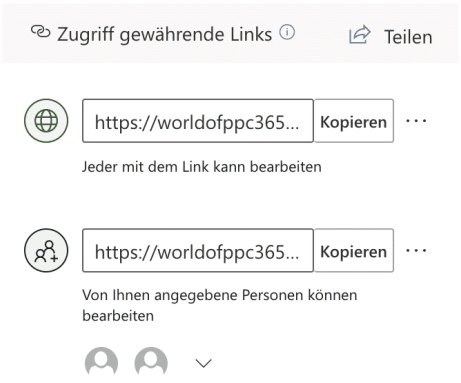
Auch wenn Sie einen etablierten Anbieter auswählen, ein gewisses Restrisiko bleibt, dass jemand an Ihre Daten kommen kann. Auch wenn Sies dies anders einschätzen, das Teilen von Dateien mit anderen Anwendern bedarf genauer Kontrolle der Rechte: Wer darf auf welche Datei zugreifen?

Freigaben kontrollieren in OneDrive

Nicht jede Freigabe soll für die Ewigkeit sein, ein Projekt ist zu Ende, ein Mitarbeitender scheidet aus. Dann soll auch dessen Zugriff auf die Dateien möglichst schnell widerrufen werden. Sonst laufen Sie Gefahr, dass ein ehemals Berechtigter weiterhin Zugriff auf Ihre Daten hat, obwohl er es gar nicht mehr sollte. Diese Funktion versteckt sich leider ein wenig in den Dialogen.

Melden Sie sich über Ihren Webbrowser an Ihrem Microsoft- (oder Office 365-) Konto an. Klicken Sie auf den Punktwürfel oben links, dann auf OneDrive. Suchen Sie den freigegebenen Ordner heraus und klicken Sie dann auf die drei Punkte rechts von dessen Namen. Wählen Sie Details.

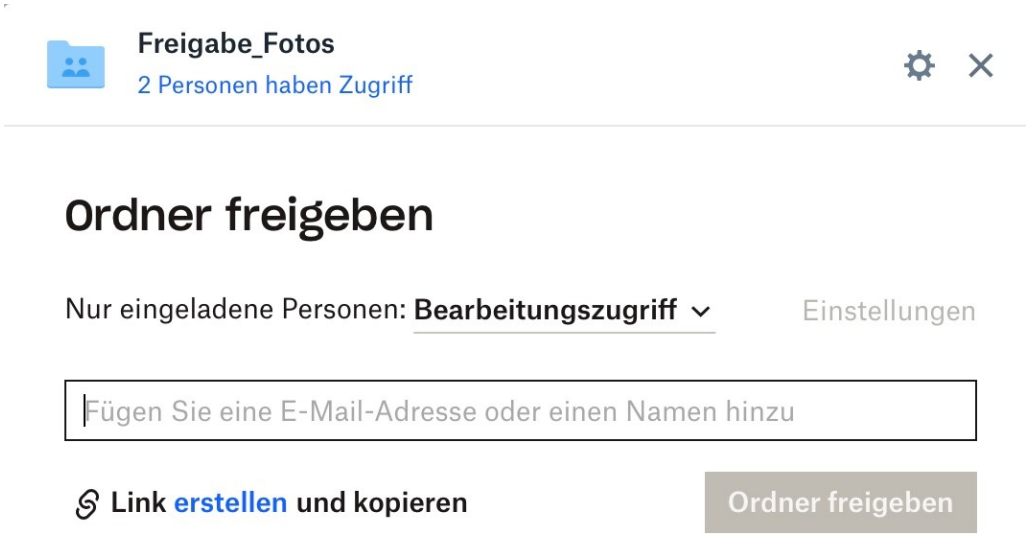
So geht's leichter | Datenschutz fängt bei mir an



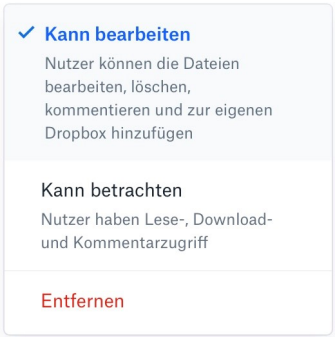
Rechts im OneDrive-Fenster sehen Sie nun die Freigaben. Klicken Sie auf **Zugriff verwalten**. OneDrive zeigt Ihnen alle Freigaben an. Klicken Sie auf die **drei Punkte** neben einer Freigabe, dann sehen Sie alle Benutzer, die diese nutzen können. Ein Klick auf das **Kreuz** neben einem Benutzer löscht dessen Zugriffsrechte. Sie können an dieser Stelle auch neue Benutzer hinzufügen oder die Berechtigungen zum Ändern von Inhalten anpassen.

Freigaben kontrollieren in DropBox

Auch bei DropBox können – und sollten - Sie Ihre Freigaben jederzeit kontrollieren. Dazu melden Sie sich mit Ihrem Konto an der DropBox-Webseite an. In der Übersicht der Verzeichnisse können Sie unter **Mitglieder** sehen, ob das jeweilige Verzeichnis freigegeben ist. In einem solchen Fall klicken Sie auf die drei Punkte neben dem Verzeichnis und dann auf **Teilen**.



So geht's leichter | Datenschutz fängt bei mir an



Oben klicken Sie dann auf die Information **x Personen haben Zugriff**.

Sie erhalten jetzt eine Übersicht aller Berechtigten. Klicken Sie auf das kleine Dreieck neben deren Berechtigungen. Hier können Sie zwischen Rechten zur Bearbeitung und um reinen Lesen wechseln und durch einen Klick auf **Entfernen** auch die Berechtigungen komplett zu löschen.

Schnelles Freigeben von Elementen unter Windows

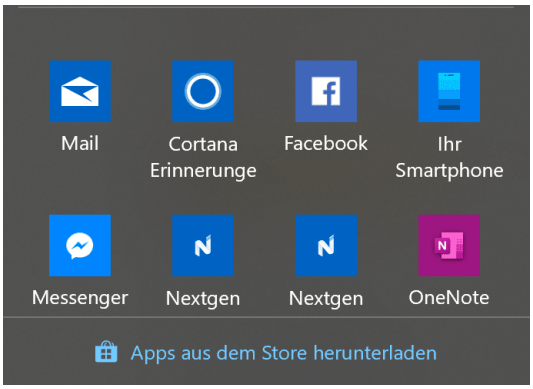
Große Dateien können Sie nicht per E-Mail senden, da liegt die Nutzung Ihres OneDrive oder der Dropbox nahe. Das muss aber nicht sein: Wenn Sie nebeneinander sitzen, dann können Sie mit Windows-Bordmitteln Dateien teilen.

Die Umgebungsfreigabe ist fester Bestandteil von Windows. Sie funktioniert so ähnlich wie das von macOS bekannte Airdrop: Die Umgegend wird nach Geräten durchsucht, die empfangsbereit wären. Grundvoraussetzung: Sie aktivieren auf jedem Gerät im InfoCenter die Umgebungsfreigabe durch Aktivieren der Schaltfläche. Nur dann ist ein Gerät auch sichtbar für andere Geräte.

Um ein Element (das kann eine Webseite, ein Word-Dokument, ein Bild sein) zu teilen, klicken Sie auf das Teilen-Symbol im jeweiligen Programmfenster. Windows 10 durchsucht jetzt die Umgebung nach empfangsbereiten Geräten.

So geht's leichter | Datenschutz fängt bei mir an

Wählen Sie aus der Liste dann einfach dasjenige aus, an das das Element geschickt werden soll. Ohne weiteres Zutun bauen die beiden Geräte nun eine Verbindung miteinander auf und das Element wird versendet.



Wenn Sie kein Gerät finden, dann stellt Ihnen Windows 10 gleich die Standardmethoden zur Verfügung. Wählen Sie aus der Liste aus, ob Sie per E-Mail, Facebook, dem Smartphone etc. den Versand vornehmen wollen. Das ist zwar vom Arbeitsablauf her ein wenig aufwändiger, funktioniert aber auch.

Temporärer Cloud-Service: WeTransfer

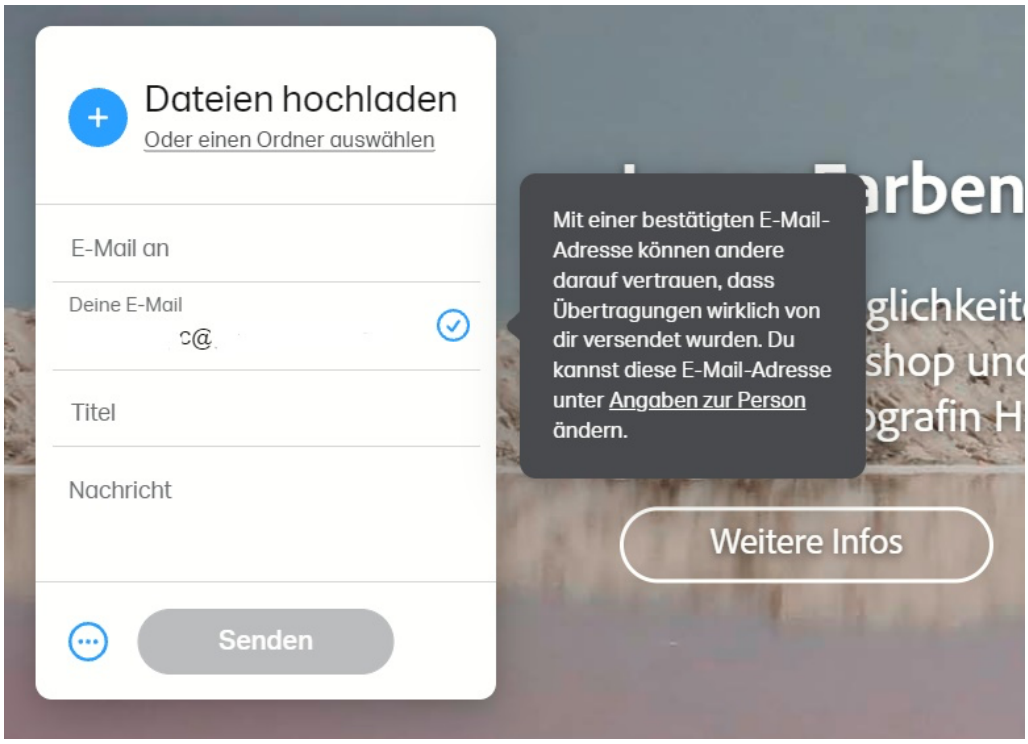
OneDrive und DropBox leben davon, dass Sie möglichst alle Daten in der Cloud liegen haben. Das muss aber nicht sein: Oft wollen Sie nur eine größere Datei oder ein Verzeichnis teilen und das nach dem Abruf durch den Empfänger wieder loswerden. Dazu bietet sich WeTransfer an. Diesen Dienst können Sie kostenlos nutzen bis zu einer Transfergröße von 2GB, für die meisten Anwender vollkommen ausreichend. Mit der kostenpflichtigen Version (ab EUR 10,- pro Monat) kommen dann noch einige Funktionen und mehr Speicher hinzu.

Nach der Anmeldung können Sie Dateien oder einen Ordner zum Transfer anwählen, geben dann die Empfänger und den Text der Nachricht ein. Mit dem Link können die Empfänger dann auf die Datei(en) zugreifen, solange sie da sind.

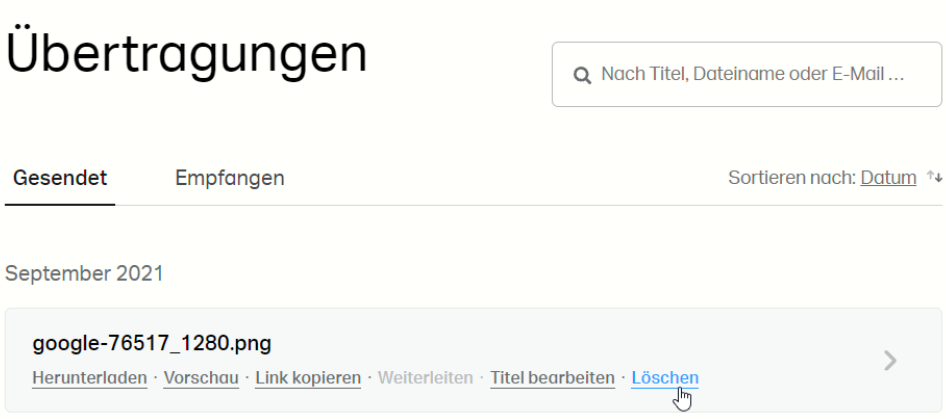
Mit der Pro-Version können Sie zusätzlich noch eine Gültigkeit festlegen. Damit können Sie die Freigabe automatisch beispielsweise

So geht's leichter | Datenschutz fängt bei mir an

nach einer Woche löschen lassen und müssen sich nicht selbst darum kümmern.



All Ihre Freigaben können Sie in der Übersicht Ihres WeTransfer-Kontos unter **Übertragungen** sehen.



So geht's leichter | Datenschutz fängt bei mir an

Bewegen Sie die Maus auf einen Eintrag, dann klicken Sie auf **Löschen**, um die Freigabe – und damit auch die Dateien – zu entfernen und nicht mehr zugänglich zu machen.

Kann das weg? Informationen löschen

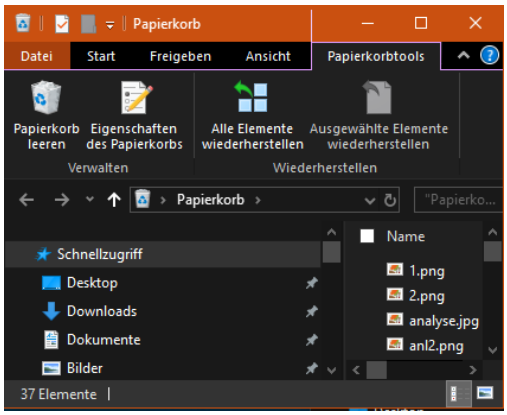
Die sichersten Informationen sind die, die gar nicht mehr da sind. Auf die kann nämlich auch kein Unberechtigter mehr zugreifen. Natürlich nur dann, wenn Sie das Löschen so ausführen, dass die Dateien nicht trotzdem noch irgendwo verfügbar sind, beispielsweise im Papierkorb!

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. Wir zeigen Ihnen, wie!

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 | Datenschutz fängt bei mir an



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.

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.

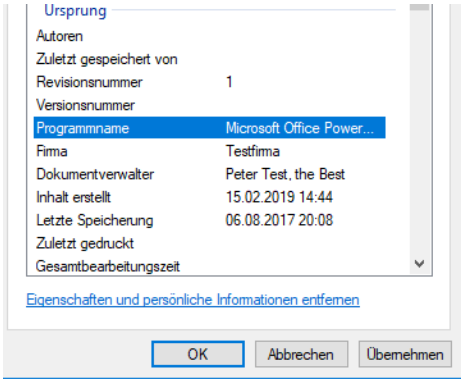
Löschen von Dokumenteneigenschaften

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

So geht's leichter | Datenschutz fängt bei mir an

führen. Die Pflege und das Löschen dieser Eigenschaften sind aber schnell gemacht.

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.

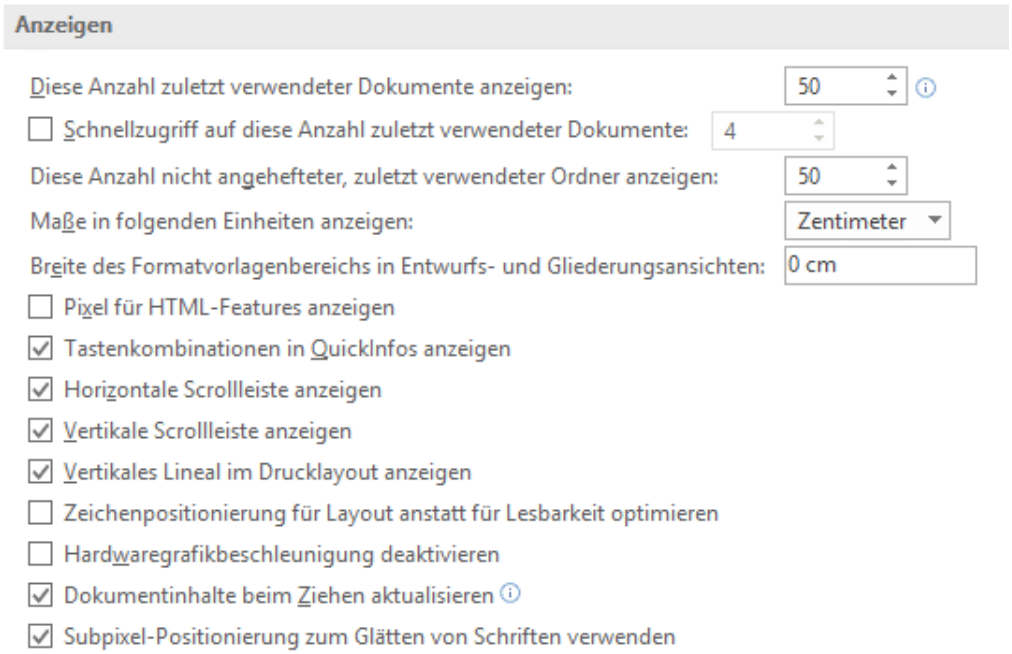
Sie können entweder eine Kopie der Datei anlegen, in der alle Eigenschaften entfernt worden sind (deren Inhalt aber natürlich unverändert ist) oder durch einen Klick auf **Folgende Eigenschaften aus der Datei entfernen** einzeln anwählen, welche Eigenschaften geleert werden sollen. So wird schnell aus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

Löschen der Liste der letzten Dateien in Office

Manche Funktionen von Microsoft Office sind gut gemeint und in den meisten Fällen hilfreich. Und dann kommen Sie in eine Situation, wo sie die so gar nicht brauchen können. Ein schönes Beispiel ist die Liste der zuletzt verwendeten Dateien in Word, Excel und PowerPoint. Die erlaubt Ihnen den schnellen Zugriff auf die letzten Dateien. Allerdings sieht diese dann auch jeder, der Ihren Rechner verwendet. Dumm, wenn Sie beispielsweise gerade eine Bewerbung geschrieben haben. Sie haben aber durchaus Möglichkeiten, hier einzugreifen!

So geht’s leichter | Datenschutz fängt bei mir an

Die erste Möglichkeit ist das komplette Ausblenden der Liste. Klicken Sie dazu in einem Office-Dokument auf **Datei** > **Optionen** > **Erweitert** > **Anzeige**. Setzen Sie die **Anzahl zuletzt verwendeter Dokumente** auf 0. Damit wird die Liste beim Öffnen einer Datei immer leer angezeigt. Allerdings ist die Historie nicht gelöscht: Setzen Sie die Zahl wieder hoch, dann werden die Dateien wieder dargestellt.



Nachhaltiger ist folgendes Vorgehen: Klicken Sie in der Liste eine Datei mit der rechten Maustaste an. Dann klicken Sie auf **Aus Liste entfernen**. Damit wird der Eintrag für die angeklickte Datei dauerhaft entfernt.

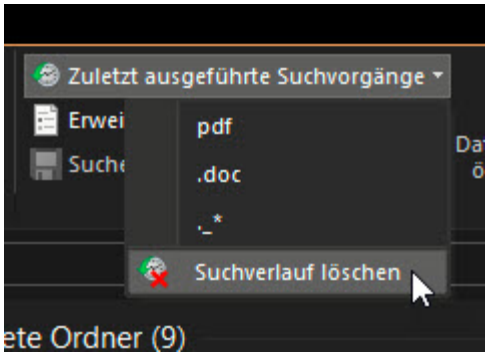
Wenn Sie stattdessen auf **Gelöste Dokumente entfernen** klicken, dann entfernt Office alle angezeigten Dateien aus der Liste. Allerdings rutschen dann die nächsten Dateien aus der Vergangenheit nach. Die Einstellung ist ja, die letzten n Dokumente anzuzeigen. Gegebenenfalls müssen Sie also eine Kombination von beiden Vorgehen wählen.

So geht's leichter | Datenschutz fängt bei mir an

Löschen der Suchhistorie im Explorer

Der Windows Explorer ist Ihr Tor zu den Dateien auf Ihrem PC. Das führt dazu, dass Sie ihn zum einen oft benutzen, zum anderen aber auch oft Suchen nach Dateien darin durchführen. Windows 10 speichert diese Suchen automatisch. Das ist hilfreich, gibt anderen Benutzern des PCs aber auch viele Informationen über Ihre Arbeit. Das können Sie aber unterbinden!

Eine Suche im Explorer starten Sie, wenn Sie den Suchbegriff in dem Eingabefeld rechts unter **Schnellsuche** eingeben. Sobald Sie das getan haben, wechselt der Explorer auf die Registerkarte **Suchtools**. Darin finden Sie unter anderem die **zuletzt ausgeführten Suchvorgänge**. Diese sind eine Historie der Suchen, die Sie bisher durchgeführt haben.



Um diese zu löschen, klicken Sie auf das nach unten zeigende Dreieck neben **Zuletzt ausgeführte Suchvorgänge** und dann auf **Suchverlauf löschen**. Die Liste der Suchbegriffe wird damit gelöscht und steht nicht mehr zur Verfügung. Damit werden aber natürlich keine Dateien auf einem der Datenträger gelöscht. Sie verlieren nur die Möglichkeit, bereits eingegebene Suchanfragen direkt wiederverwenden zu können.

Schützen/Verschlüsseln von Dateien

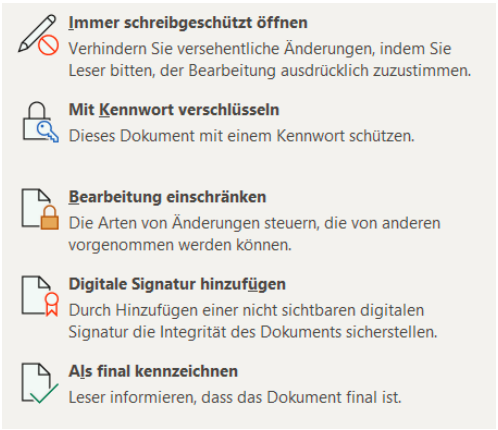
Ihre Dateien sind das A und O Ihrer Arbeit am Rechner. Sie wollen meist nicht, dass ein Unbefugter auf diese zugreifen kann und sehen kann, womit Sie sich beschäftigt haben. Darum schützen Sie Festplatte und Dateien durch Verschlüsselung oder Passwörter. Je höher die Hürde ist,

So geht's leichter | Datenschutz fängt bei mir an

die ein Angreifer überwinden muss, desto sicherer und geschützter sind Ihre Informationen!

Passwortschutz bei Office-Dokumenten

Wie schnell eine Datei in falsche Hände gelangen kann: Dazu bedarf es nicht unbedingt eines Datenlecks, oft ist die eigene Unachtsamkeit der Grund: Ein verlorener USB-Stick, eine versehentliche an eine E-Mail angehängte Datei, und schon ist eine Datei in den falschen Händen. Das macht aber noch nichts, wenn der Empfänger die Datei nicht verwenden kann, weil Sie durch ein Passwort geschützt ist. Das kennt der Unberechtigte ja nicht.



Office bietet die Möglichkeit des Passwortschutzes ein wenig versteckt in den Office-Apps. Klicken Sie auf **Datei** > **Informationen** > **Dokument schützen**. Klicken Sie dann auf **Mit Kennwort verschlüsseln**. Office fragt Sie nun nach dem Kennwort für das Dokument und fordert nach der Eingabe eine zweite Eingabe zur Absicherung an. Nachdem Sie das Kennwort festgelegt und die Datei gespeichert haben, kann die Datei nur noch durch Eingabe dieses Kennwortes geöffnet werden. Vergessen Sie dies, dann haben Sie sich selbst aus Ihrem eigenen Dokument ausgeschlossen.

Wichtig: Wenn Sie die Datei per E-Mail versenden, dann sollten Sie das Kennwort auf einem anderen Weg, beispielsweise per Anruf, SMS oder WhatsApp/Signal weitergeben. Damit vermeiden Sie, dass der Passwortschutz wirkungslos ist, weil jemand die E-Mail (und damit Datei und Kennwort) abfängt!

So geht’s leichter | Datenschutz fängt bei mir an

PDFs mit Passwort schützen

Manchmal hat auch eine PDF-Datei eine gewisse Vertraulichkeit, und Sie möchten sicherstellen, dass sie nur von einer berechtigten Person geöffnet werden kann. Die einfachste Möglichkeit ist auch hier die Vergabe eines Kennwortes, das Sie den Berechtigten zukommen lassen.

Die kostenlose Version des Acrobat Readers unterstützt die Vergabe von Kennwörtern nicht, hier müssen Sie einmal mehr ein Abonnement der kostenpflichtigen Version erwerben. Wenn es sich aber nur um einzelne Dateien handelt, dann ist der Webdienst SmallPDF eine gute Alternative. Auf den können Sie am Tag zwei PDF-Dateien hochladen, ein Passwort hinterlegen und dann die passwortgeschützte PDF-Datei wieder herunterladen. Der Empfänger kann diese ohne Eingabe des Kennworts nicht öffnen.

Das Kennwort, das Sie vergeben, müssen Sie dem Empfänger natürlich noch zukommen lassen. Am besten auf einem anderen Weg als das Dokument, beispielsweise per SMS. WhatsApp oder Telefon. So stellen Sie sicher, dass ein Unberechtigter, der auf die E-Mail mit der PDF-Datei zugreifen kann, das Kennwort nicht direkt mit findet.

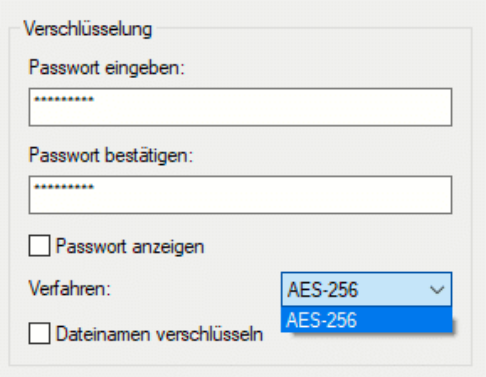
So geht's leichter | Datenschutz fängt bei mir an

Bei den beschriebenen Webdiensten müssen Sie natürlich immer das Vertrauen haben, dass diese die hochgeladenen (und damit zumindest kurzfristig auf deren Servern gespeicherten) Dateien nicht in irgendeiner Weise weiterverwenden!

Verschlüsseln von Dateien in einem ZIP-Archiv

Wenn Sie sich nicht auf die Verschlüsselung auf der Festplatte verlassen wollen oder Dateien per E-Mail 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. Also auch das Windows 10-interne, WinZIP und WinRAR.

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

So geht's leichter | Datenschutz fängt bei mir an

es nicht, wird das Archiv nicht geöffnet und die Dateien bleiben sicher verschlossen darin.

Verschlüsselung mit Bitlocker

Verschlüsselung geht noch einen Schritt weiter als die Vergabe und der Schutz durch ein Kennwort: Ein Kennwort schützt nur den Zugang zu den Daten, die Verschlüsselung macht die kompletten Daten unlesbar, ohne den Schlüssel kann niemand aus dem Bit-Brei eine lesbare Datei machen.

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.

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.

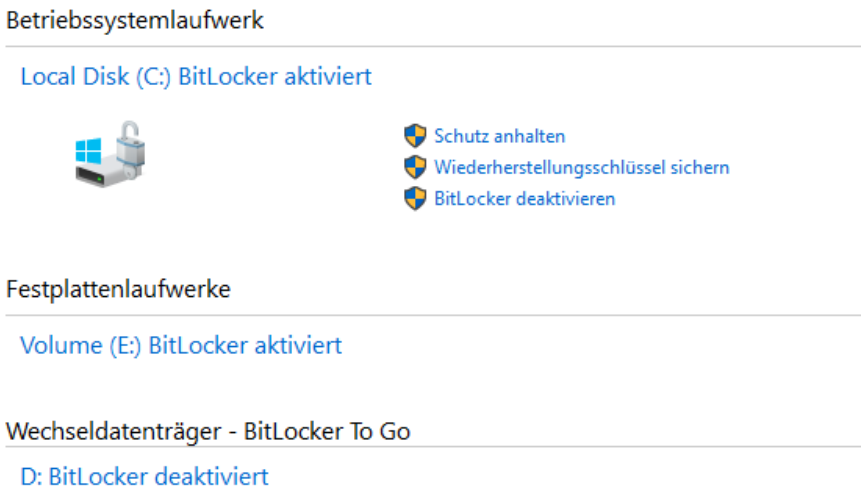
Aktivierung von Bitlocker

Die Aktivierung und Deaktivierung von Bitlocker für Festplatten findet nahezu automatisch statt. Um dies zu kontrollieren, suchen Sie in der

So geht’s leichter | Datenschutz fängt bei mir an

Windows-Suche nach Bitlocker und klicken Sie auf das Suchergebnis **Bitlocker verwalten**.

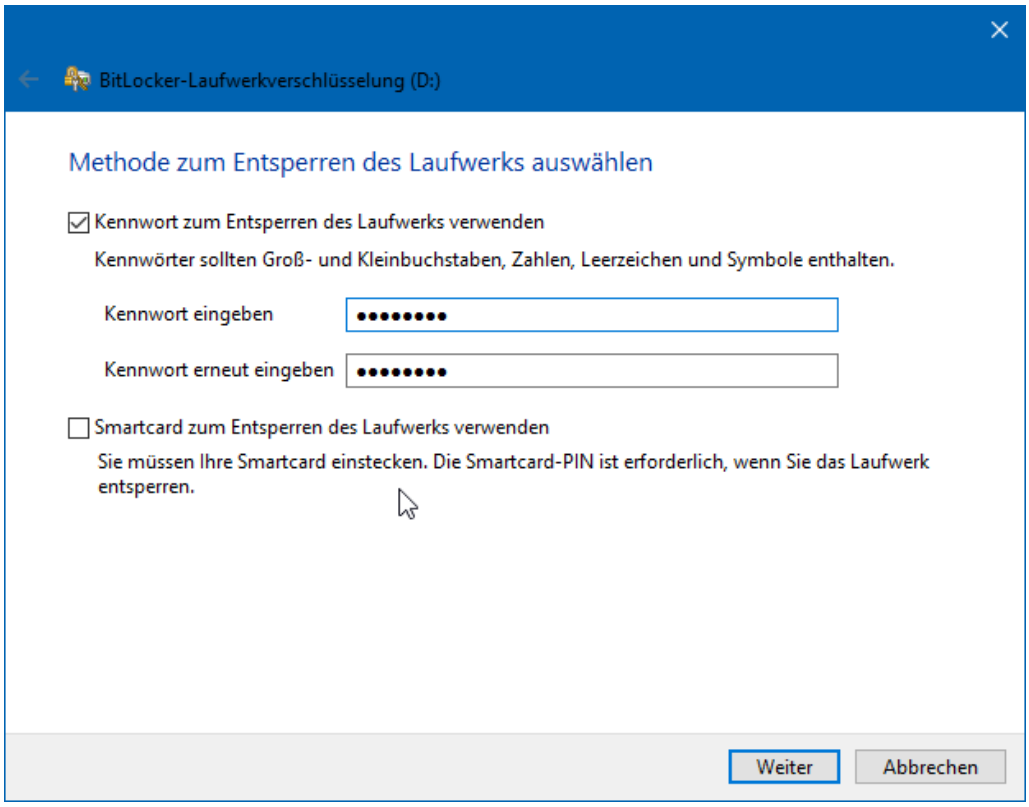
Im normalen Betrieb werden Sie hier keine Unterschiede erkennen, Die Festplatte ist nicht spürbar langsamer und Sie müssen auch beim Systemstart kein zusätzliches Kennwort eingeben. Letzteres übernimmt hier das TPM-Modul im Hintergrund für Sie!



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 | Datenschutz fängt bei mir an



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 per EFS

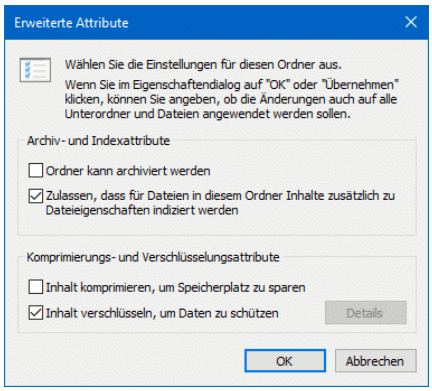
Doppelt gemoppelt hält besser. Bitlocker ist zwar eine schöne und vor allem leicht einzusetzende Möglichkeit, eine Festplatte zu verschlüsseln.

So geht’s leichter | Datenschutz fängt bei mir an

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

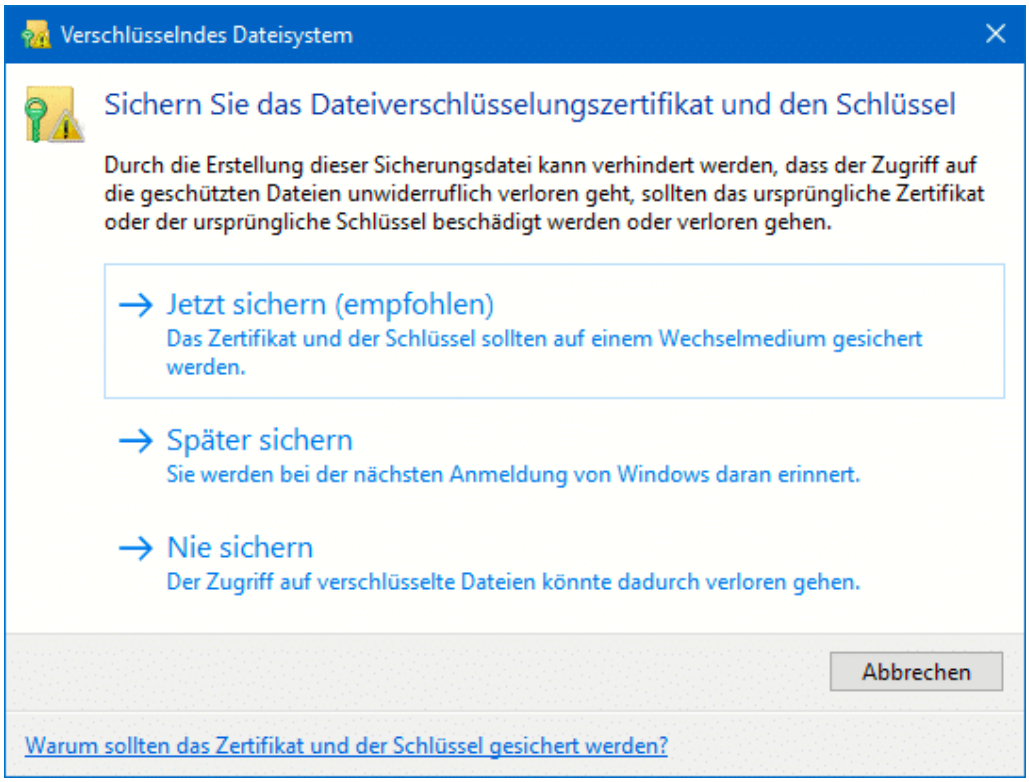
Um eine Datei zu verschlüsseln, klicken Sie im Windows Explorer einfach mit der rechten Maustaste auf eine Datei. Dann können Sie in der Registerkarte Allgemein auf Erweitert klicken. Ganz unten sehen Sie dann Inhalt verschlüsseln, um Daten zu schützen.

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.

So geht’s leichter | Datenschutz fängt bei mir an



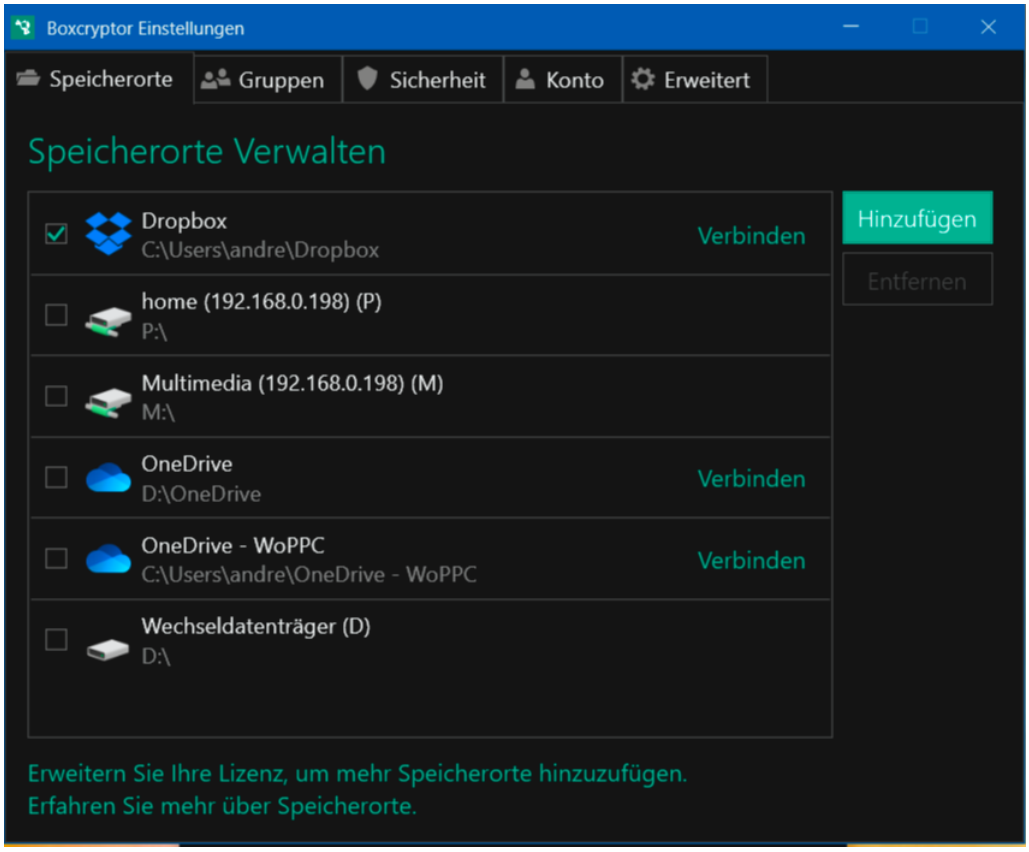
Was aber, wenn Sie selber nicht mehr an Ihr Benutzerkonto kommen, weil Sie die Zugangsdaten vergessen haben? Windows 10 versucht dies zu verhindern, indem es Sie beim ersten Verschlüsseln einer Datei daran erinnert, ein Backup der Schlüssel durchzuführen.

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.

So geht's leichter | Datenschutz fängt bei mir an

Verschlüsselung in der Cloud

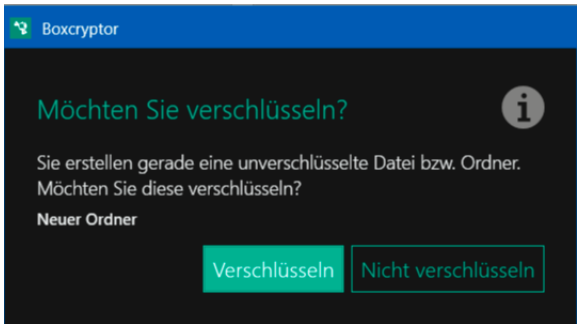
Die Cloud? Die ist doch sicher, vor allem liegen die Daten verschlüsselt auf den Server? Warum müssen wir darüber reden? Müssen wir nicht, sollten wir aber! Natürlich sind die meisten Cloud-Anbieter alleine schon aus Eigeninteresse so weit, dass die Daten der Kunden verschlüsselt abgelegt sind. Damit haben Sie als Kunde und Nutzer nichts zu tun, und das ist genau der Punkt: Eine Eingangstür, zu der nicht nur Sie, sondern auch der Vermieter einen Schlüssel haben, ist eben doch nicht ganz sicher. So ungefähr können Sie die Verschlüsselung bei einem Cloud-Anbieter beschreiben: Der hat den Schlüssel und kann so theoretisch Ihre Daten lesen.



Ein weiteres Schloss anzubringen, ist im Standard nicht möglich, aber dafür gibt es Dienste wie BoxCryptor. Dieser ist im Standard kostenlos

So geht's leichter | Datenschutz fängt bei mir an

für einen Cloud-Anbiete rund zwei Endgeräte, kostenpflichtige und leistungsfähigere Abos gibt es dann ab EUR 36,- im Jahr.



BoxCryptor hängt sich in den Windows Explorer und lässt sich mit den gängigen Cloud-Diensten, unter anderem OneDrive und Dropbox, aber auch mit lokalen Dateisystemen verbinden. Sobald Sie einen neuen Ordner anlegen, fragt die App Sie, ob Sie diesen verschlüsseln wollen. Stimmen Sie dem zu, dann werden alle Dateien und Verzeichnisse, die Sie in diesem Ordner ablegen, ebenfalls verschlüsselt. Die so für Unberechtigte unleserlichen Dateien werden dann auf den Cloud-Server hochgeladen. Ihr Anbieter kann damit überhaupt nichts anfangen, auch ein Hacker findet nur eine zufällige Ansammlung von Bits und Bytes, nicht aber Ihre Daten und Informationen.

Wenn Sie eine Datei öffnen, dann wird diese automatisch entschlüsselt, einen Unterschied zur einer unverschlüsselten Datei spüren Sie im Normalfall nicht.

Kommunikation und Social Networks

Datenschutz wird oft reduziert auf die rein technischen Aspekte: Passwörter, Firewalls, Antiviren-Programme und vieles mehr sind ohne Frage wichtig und dürfen nicht vernachlässigt werden, aber mindestens genau so wichtig sind die weichen Faktoren. Beispielsweise das Mitteilungsbedürfnis der Anwender. Dazu müssen Sie nur einmal mit offenen Augen und Ohren mit dem Zug fahren: Da stehen Notebooks

So geht's leichter | Datenschutz fängt bei mir an

mit Umsatzstatistiken auf dem Bildschirm offen herum, Berater telefonieren lauthals mit Kollegen und reden über ihre Kunden und vieles mehr.

Elektronische Kommunikation ist uns so in Fleisch und Blut übergegangen, dass wir wenig darüber nachdenken. Wie schnell ist eine E-Mail verschickt und versehentlich der falsche Adressat oder das falsche Dokument angehängt?

Oder nehmen Sie die sozialen Netzwerke: Was Sie darin veröffentlichen, können viel mehr Menschen lesen, als wenn Sie eine E-Mail schreiben. Informationen, die auf diesem Weg einmal in der Welt sind, sind kaum ungeschehen zu machen.

Technisch lassen sich die weichen Faktoren kaum kontrollieren. Sie können aber Vorkehrungen treffen, die es unwahrscheinlicher machen, dass Ihre Informationen an die Falschen Empfänger kommen!

Pannen bei E-Mails vermeiden

E-Mails trotz des Vormarsches der Messenger-Dienste immer noch ein wichtiges Kommunikationsmedium. Besonders kritisch, weil Sie oft nicht nur kurze Texte austauschen, sondern auch Dokumenten mit teils vertraulichem Inhalt anhängen. Treffen Sie Vorkehrungen, damit dabei möglichst wenig schiefgehen kann!

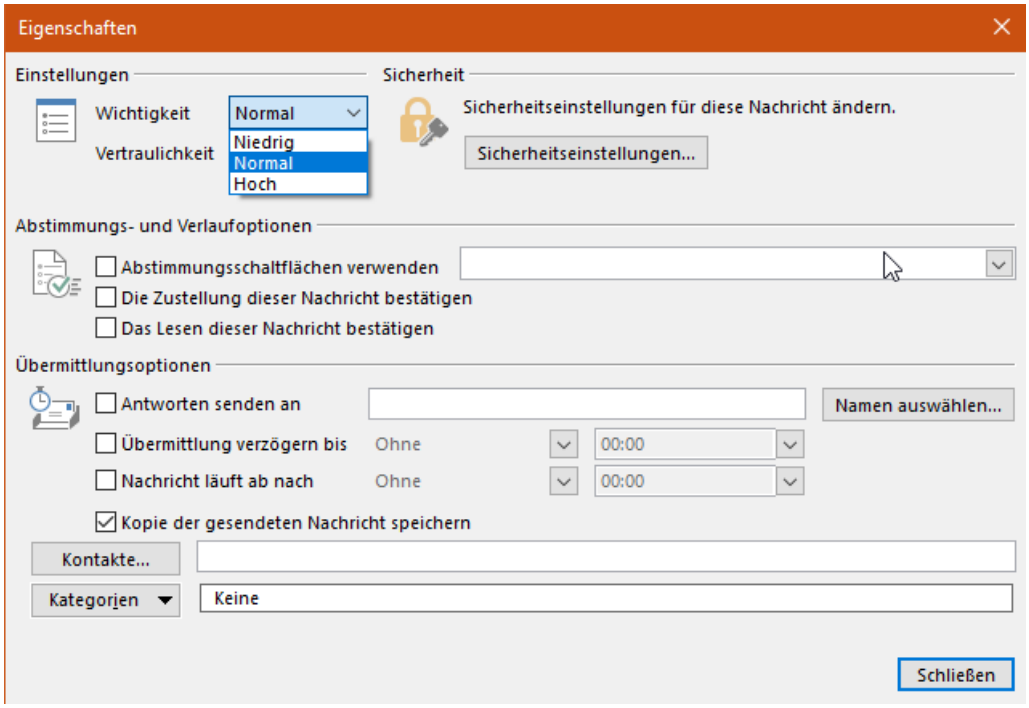
Wichtigkeit, Vertraulichkeit Verschlüsselung von E-Mails

Eine E-Mail besteht nicht nur aus den Verwaltungsinformationen. Natürlich sind Empfänger, Betreff und der Mailkörper wichtig, weil sie die0 Informationen transportieren. Zusätzlich können Sie aber noch einige Einstellungen vornehmen, die nahezu unsichtbar mit versendet

So geht's leichter | Datenschutz fängt bei mir an

werden und dem Empfänger weitere Informationen liefern. Wir zeigen Ihnen, wo Sie in Outlook die entsprechenden Einstellungen finden!

Zum Inhalt der Mail gibt es noch drei große Bereiche, die Sie beeinflussen können. Nicht jede E-Mail ist gleich wichtig, und so können Sie eine zusätzliche Kennzeichnung mitgeben, die dem Empfänger Aufschluss darüber gibt. Unter Markierungen in der Symbolleiste einer neuen E-Mail können Sie unter **Wichtigkeit** zwischen **Normal**, **Niedrig** und **Hoch** auswählen. Normal ist die Standardeinstellung. Wenn Sie dem Empfänger sagen wollen, dass die Bearbeitung nicht eilig ist, ist niedrig die richtige Wahl. Auf der anderen Seite hoch, wenn es pressiert!



Parallel dazu können Sie unter **Vertraulich** festlegen, dass die E-Mail vertraulich behandelt werden soll. Damit untersagen Sie beispielsweise eine Weiterleitung an Andere.

Die dritte Möglichkeit ist die Verschlüsselung von E-Mails. Im Standard versendet Outlook E-Mails im Klartext. Das klingt schlimmer, als es ist,

So geht's leichter | Datenschutz fängt bei mir an

denn der Transfer zwischen den E-Mail-Servern ist im Normalfall schon verschlüsselt. Unter **Sicherheitseinstellungen** können Sie die E-Mail an sich aber noch einmal verschlüsseln. Dazu muss aber ein Zertifikat installiert sein. Das macht am besten der Administrator, der das E-Mail-System aufgesetzt hat.

Vorsicht bei Massenmailings

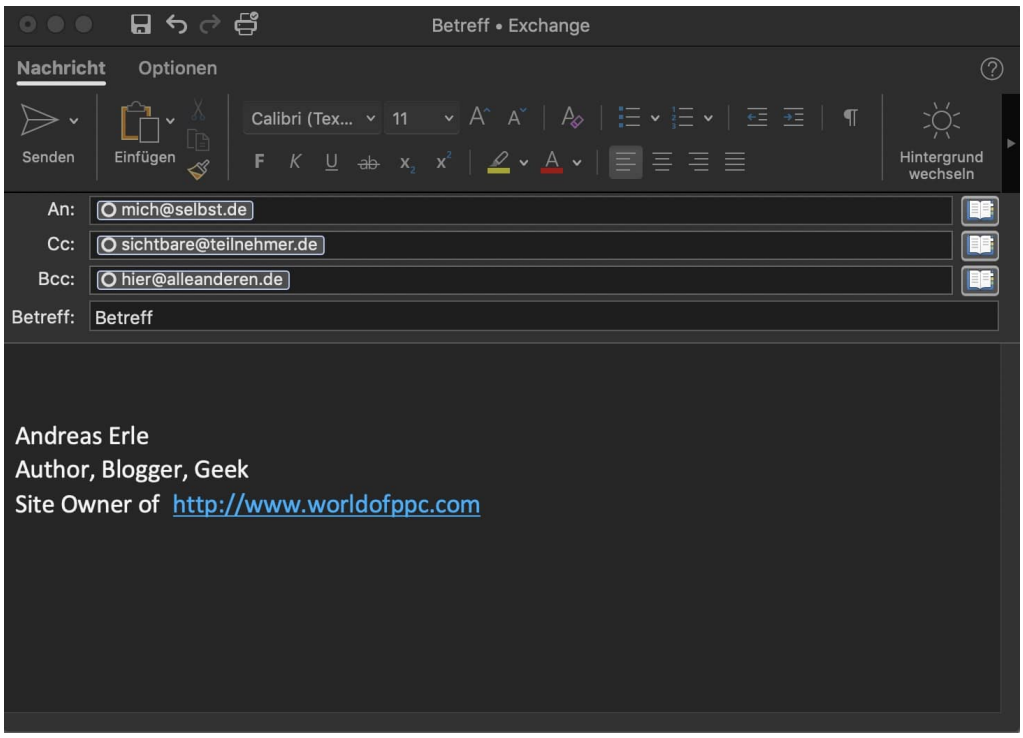
Mailingliste, Newsletter, Exceltabellen mit Mitgliederdaten: Tolle Möglichkeiten, vielen Menschen auf einen Streich Informationen zukommen zu lassen. Was technisch so einfach scheint ist nicht ganz so unproblematisch, wie der erste Blick vermuten lässt. Wir zeigen Ihnen, wie Sie die größten Fehler vermeiden können!

Die Zeiten von ungetrübter Massenmailfreude sind spätestens seit der Datenschutz-Grundverordnung (DSGVO) vorbei. Zumindest im nicht-privaten Bereich benötigen Sie eine rechtliche Grundlage, denn die E-Mail-Adressen sind ja auch personenbezogene Daten. Im Zweifel konsultieren Sie einen Experten!

Gehen wir davon aus, dass Sie eine Grundlage für die Versendung von E-Mails an viele Adressaten gleichzeitig haben, dann sollten Sie vor allem auf zwei Dinge achten:

E-Mail-Empfänger bei Massen-E-Mails gehören ins BCC:
Normalerweise schreiben Sie die Empfänger einer E-Mail in die **AN**-Zeile. Bei einer Massen-E-Mail sollten Sie das nicht tun, denn dann sieht jeder Empfänger jeden anderen. Das ist nicht angenehm, wenn die Empfänger sich nicht alle kennen. Datenschutzrechtlich ist es ebenfalls kritisch. Stattdessen schicken Sie die Mail an sich selbst und nehmen die eigentlichen Empfänger in die **BCC**-Zeile. Dann sieht jeder Empfänger nur seine Adresse und die Ihre.

So geht’s leichter | Datenschutz fängt bei mir an



Zu viele E-Mails parallel können als SPAM angesehen werden: Je mehr Empfänger Ihre E-Mail hat, desto mehr einzelne E-Mails werden verschickt. Der ein oder andere E-Mail-Server vermutet einen SPAM-Angriff und verzögert oder sperrt die Zustellung Ihrer E-Mail. Dann bekommen Sie in Ihren Posteingang eine Nachricht. Wenn das passiert, versuchen Sie beim nächsten Mal die E-Mails in kleineren Tranchen zu schicken.

Verzögern des Mail-Versandes bei Outlook

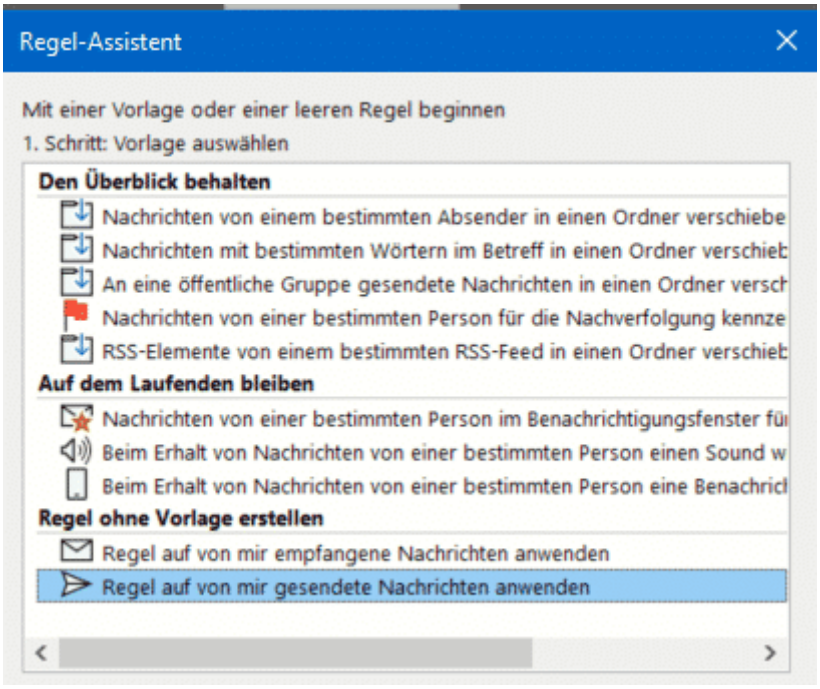
Kennen Sie die Situation? Eine Mail geht an einen riesigen Verteiler, Sie wollen dem Absender antworten und stattdessen klicken Sie auf "Allen Antworten" und Ihre Antwort erreicht nicht einen, sondern viel zu viele Adressaten. Oder Sie stellen direkt nach Versand fest, dass der Anhang viel zu viele Daten enthält oder der falsche für die Adressaten ist. Das

So geht’s leichter | Datenschutz fängt bei mir an

Zurückziehen der Nachricht hilft da leider nur sehr eingeschränkt. Oft merken Sie Ihren Fehler sehr schnell, da kann es helfen, wenn Ihre Mails nicht direkt, sondern mit einer leichten Verzögerung rausgehen. Wir zeigen Ihnen, wie Sie das einstellen können!

Die Idee dabei ist simpel: Sie sagen Outlook einfach, dass alle E-Mails, die Sie senden, nicht direkt rausgehen sollen, sondern mit einer Verzögerung von beispielsweise 5 Minuten. Dazu bietet Outlook die Funktion der Regeln an.

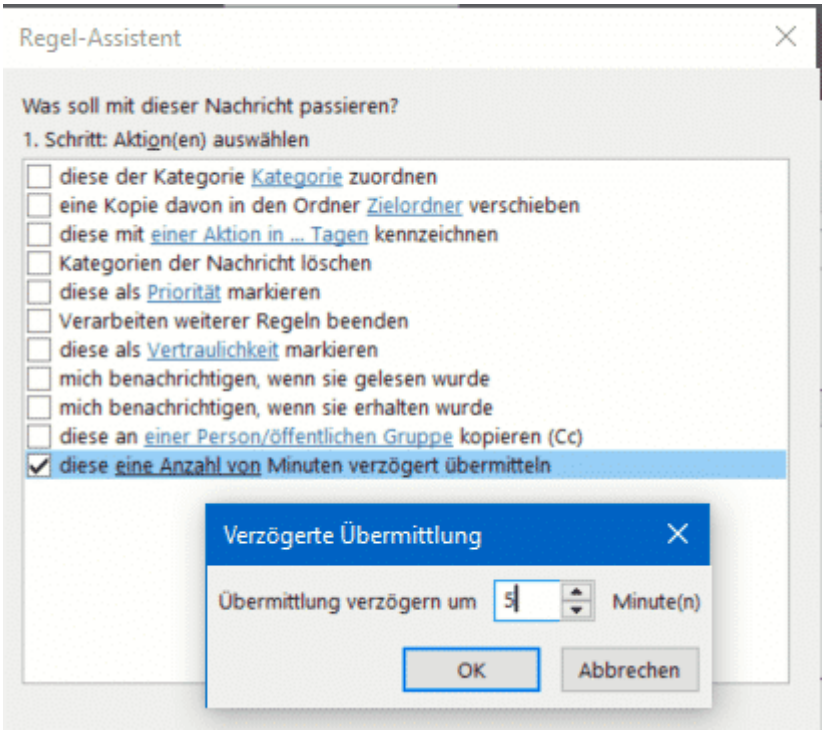
Klicken Sie auf **Datei** > **Regeln und Benachrichtigungen verwalten** > **Neue Regel**. Klicken Sie ganz unten in der Liste auf **Regel auf von mir gesendete Nachrichten anwenden**.



Im nächsten Bildschirm setzen sei keinen Haken bei den angezeigten Bedingungen. Outlook hinterfragt dann, ob Sie diese Regel tatsächlich auf alle Nachrichten anwenden wollen, das bestätigen Sie dann.

So geht's leichter | Datenschutz fängt bei mir an

Outlook fragt Sie jetzt nach Ausnahmen, auch hier wählen Sie keine der Optionen an. Klicken Sie sich nun bis zum Ende durch den Einrichtungsvorgang, dann bestätigen Sie die Aktivierung der Regel. Aktivieren Sie nun ganz unten **diese eine Anzahl von Minuten verzögert übermitteln**. Klicken Sie auf **eine Anzahl von** im Text der Aktion und geben Sie dann die Zahl der Minuten an, die die Übermittlung verzögert werden soll.



Ab diesem Zeitpunkt warten alle Nachrichten für 5 Minuten, nachdem Sie auf Senden geklickt haben, im Postausgang und werden erst dann versendet. Dies gilt nur den Rechner/das Outlook, in dem Sie die Regel definiert haben. Innerhalb dieses Zeitraums können Sie die E-Mail noch problemlos löschen und damit den Versand verhindern.

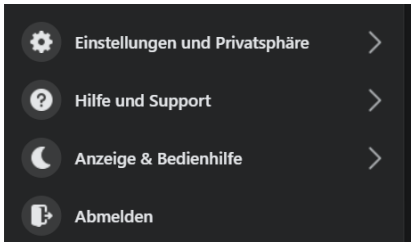
So geht's leichter | Datenschutz fängt bei mir an

Privatsphäre und Anmeldungen

Soziale Netzwerke lassen sich aus unserem Leben kaum noch wegdenken. Facebook, Instagram, Twitter und viele mehr üben einen eigenartigen Einfluss auf uns aus: Wer hätte ohne sie den Drang verspürt, mit der Welt zu teilen, was er wann isst oder wo er gerade in welcher Stimmung was macht? Diese Gedanken werden uns nahezu abgenommen, weil diese Mitteilsamkeit heute zum guten Ton gehört.

Dass damit ein Risiko verbunden ist, liegt auf der Hand: Das Internet vergisst nichts, zumindest nicht übergreifend und schnell. Aus diesem Grund sollten Sie ein wenig Zeit in die Privatsphäreeinstellungen investieren. Die schützt nicht nur Ihre Privatsphäre, sondern auch die der Menschen, die Sie in Ihren Beiträgen markieren!

Privatsphäreeinstellungen bei Facebook



Facebook hat eine eigene Rubrik in den Einstellungen für die Privatsphäreeinstellungen. Klicken Sie auf der Facebook-Webseite auf das Dreieck nach unten neben Ihrem Profilbild, dann auf **Einstellungen und Privatsphäre**. Sollte der Pfad ein wenig anders aussehen: Facebook entwickelt sich kontinuierlich weiter, dabei werden auch die Menüs immer mal wieder angepasst!

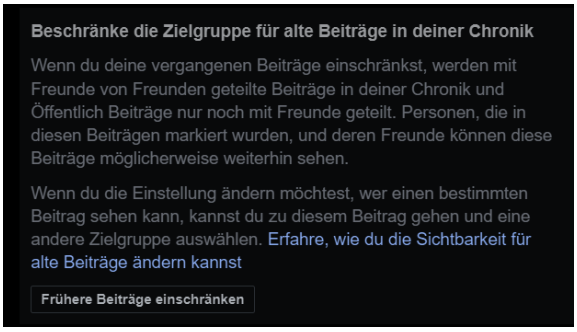
Klicken Sie dann auf **Einstellungen** > **Privatsphäre**. Facebook zeigt Ihnen nur eine umfangreiche Übersicht Ihrer Möglichkeiten, die Privatsphäre zu beeinflussen.

So geht's leichter | Datenschutz fängt bei mir an

Kontrollieren Sie hier, dass Sie Ihre privaten Beiträge nicht öffentlich teilen. Da mag bei einem öffentlichen Anliegen Sinn machen, auf Ihre privaten Beiträge aber sollten nur bestimmte Personen Zugriff haben. Das können Sie unter **Wer kann Deine zukünftigen Beiträge sehen?** festlegen.

Hier können Sie ihre gesamte Freundesliste, Ihre Freundesliste außer bestimmten Personen oder gar nur bestimmte Freunde freischalten.

Natürlich können Sie diese Einstellung für jeden Post auch verändern. Achten Sie dann nur darauf, dass Facebook nicht „zufällig" beim nächsten Post die falsche Einstellung verwendet!



Oft ist man am Anfang noch entspannter, was die Privatsphäre angeht, der Reiz des Neuen überwiegt noch. Das macht aber nichts, denn Sie können die Zielgruppe für Beiträge, die für die Öffentlichkeit oder Freunde von Freunden sichtbar waren, mit einem Klick auf Ihre Freunde einschränken. Klicken Sie dazu auf **Frühere Beiträge einschränken** und folgen Sie den Anweisungen. Vorsicht: Rückgängig machen können Sie dies nur, wenn Sie jeden einzelnen Beitrag wieder anpassen und freigeben!

So geht's leichter | Datenschutz fängt bei mir an

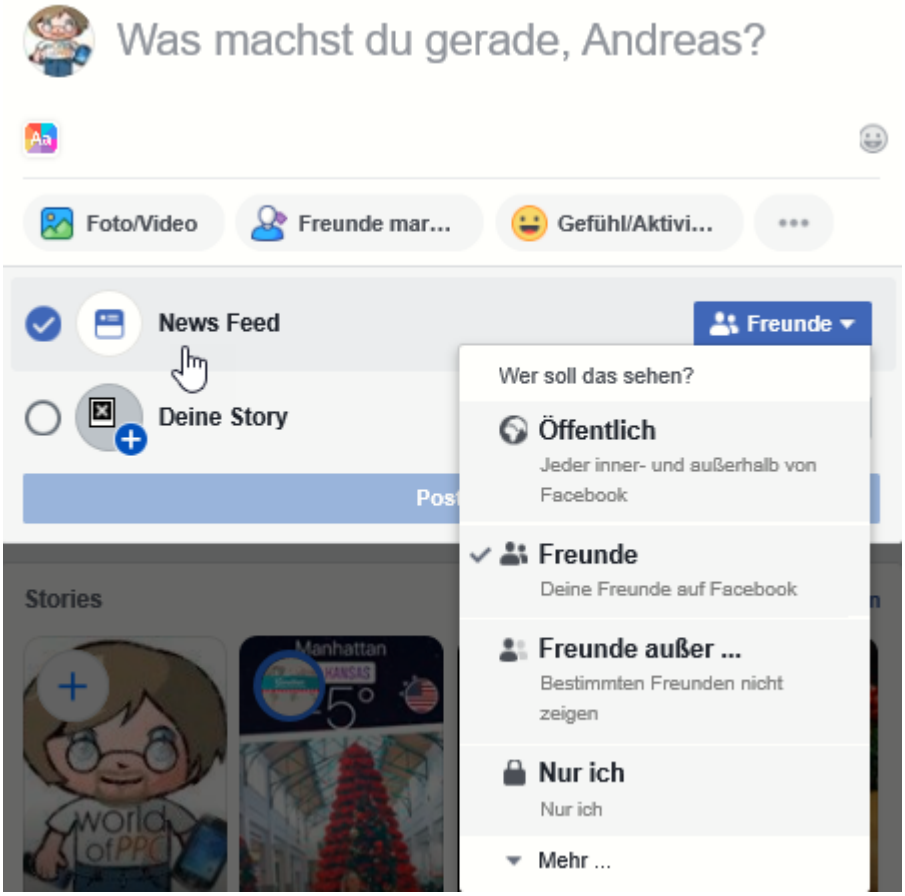
Wenn Sie in Beiträgen markiert sind, das aber nicht sollen, dann können Sie dies über das **Aktivitätenprotokoll** beeinflussen. Löschen Sie einfach die Markierungen, die Sie nicht wollen, oder geben Sie sie frei.

Bestimmte Personen von einem Facebook-Post ausschließen

Facebook ist vor allem deshalb toll, weil es den eigenen Aussagen eine ungeahnte Reichweite gibt. So können Sie mit einer Nachfrage mehr Leute erreichen, als Sie im direkten Zugriff haben. Dumm nur, wenn einer Ihrer virtuellen Freunde gerade eben nicht den Post nach einem Geschenk für ihn lesen soll. Kein Problem: Über Facebook können Sie einzelne Freunde aus Posts ausschließen. Oder Ihre Mutter! Wir zeigen Ihnen, wie.

Facebook erlaubt sehr feine Einstellungen der Privatsphäre, Und dazu gehört auch das Einschränken von Beitragen für bestimmte Freunde. Klicken Sie dazu in das Eingabefeld Was machst Du gerade. Fangen Sie jetzt noch nicht an, den Beitrag zu tippen. Stattdessen wählen Sie aus, dass der Beitrag in Ihren **News Feed** soll. Daneben finden Sie das Feld Freunde. Klicken Sie es an, dann wählen Sie **Freunde auße**r...

So geht’s leichter | Datenschutz fängt bei mir an



Sie sehen nun eine Liste Ihrer Freunde. Für jeden Freund in der Liste können Sie durch ein Anklicken des Stoppschild-Symbols auswählen, dass der Beitrag ihm oder ihr nicht angezeigt werden soll. Sie können jederzeit diese Blockade wieder aufheben und den Post durch deaktivieren der Einstellung wieder anzeigen lassen.

Klicken Sie auf Änderungen speichern, um dem Beitrag seine Sichtbarkeit zuzuweisen. Viel Erfolg bei Ihrer geheimen Geschenkabfrage!

So geht's leichter | Datenschutz fängt bei mir an

Einmal-Anmeldungen in Facebook löschen

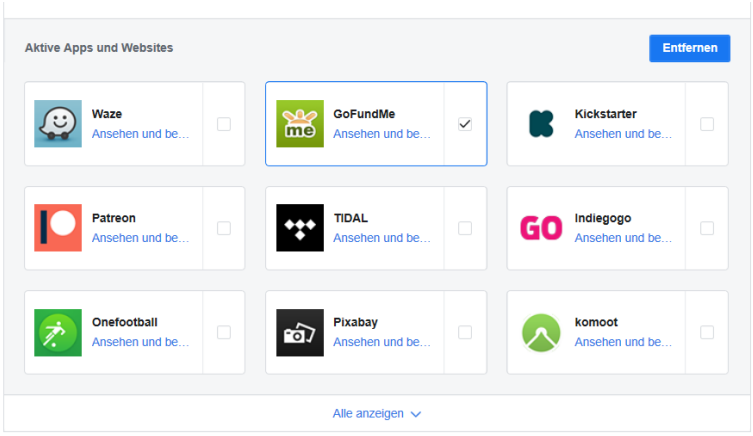
Das Anmelden bei einer Webseite oder einem Service über das normale Facebook-Login ist bequem: Sie melden sich mit Ihren bekannten Kontodaten an, müssen kein weiteres Konto anlegen und Passwort ausdenken, und Ihre persönlichen Daten werden schon voreingetragen. Im Standard ist aber jede App oder Webseite, die die Authentifizierung via Facebook nutzt, erst einmal als aktiv gespeichert. Es macht also Sinn, die Zugänge wieder zu löschen.

Wenn Sie das erste Mal die Anmeldung per Facebook bei einer neuen App oder Webseite vorgenommen haben, informiert Sie Facebook darüber. Per Push-Nachricht, E-Mail und Benachrichtigung auf der Webseite. Ein Klick auf diese Benachrichtigung führt Sie dann direkt zur Übersicht der aktiven Apps und Webseiten.

Alternativ klicken Sie auf **Einstellungen** > **Apps und Websites,** um in die Übersicht derjenigen zu kommen, die mit Ihrem Facebook-Konto gekoppelt sind. Wenn Sie auf eines der Symbole klicken, dann zeigt Ihnen Facebook alle Berechtigungen, die die App/die Webseite hat.

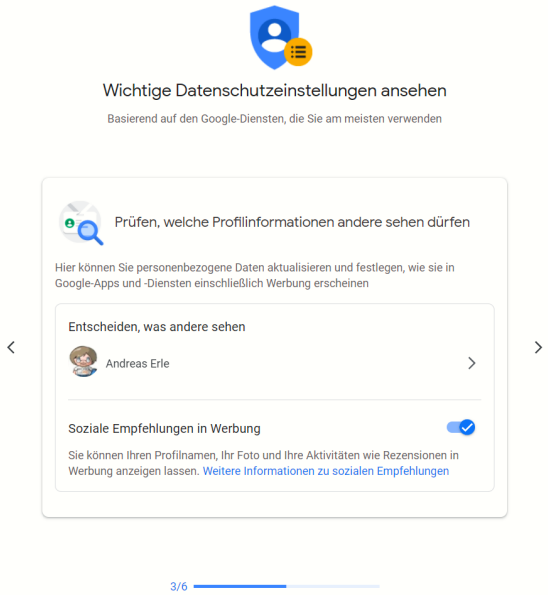
Hier können Sie für jedes Element, auf die Zugriff besteht, ein- oder ausschalten. Das Ausschalten kann natürlich dazu führen, dass bestimmte Funktionen nicht mehr funktionieren.

So geht's leichter | Datenschutz fängt bei mir an



Markieren Sie in der Übersicht einen Eintrag und klicken Sie dann auf **Entfernen**, um den Zugriff der App/Webseite zu löschen. Besonders bei nur einmal verwendeten Anmeldungen sollten Sie dies direkt machen, dann vergessen Sie es später nicht mehr.

Google und die Privatsphäre



Lachen Sie nicht: Auch wenn Google ohne Frage gefühlt der größte Konsument und Verwerter Ihrer Daten ist, Privatsphäre ist alleine schon auf Grund der Datenschutzgesetzgebung ein Muss. In der Folge bietet auch Google eine Vielzahl an Hilfestellungen rund um Ihre Privatsphäre an. Diese sind gebündelt im Privatsphäre Check, einer Unterseite Ihrer Kontoeinstellungen. Es empfiehlt sich, diese Seite regelmäßig aufzurufen und die Einstellungen zu kontrollieren und gegebenenfalls zu korrigieren. Google ändert

So geht's leichter | Datenschutz fängt bei mir an

regelmäßig den Leistungsumfang seiner Dienste. Damit werden auch Ihre Daten schnell anders verwendet oder neue Daten erhoben.

Wenn sie sich nicht auf die Empfehlungen von Google verlassen wollen, dann können Sie alle Einstellungen auch manuell vornehmen. Dazu melden Sie sich an Ihrem Google-Konto an und klicken dann auf **Übersicht** > **Datenschutz und Personalisierung**. Hier können Sie beispielsweise festlegen, wer Ihre persönlichen Daten sehen darf, welche Daten zu Ihrem Verhalten gespeichert werden und vieles mehr. Wie immer: Datenschutz kostet Zeit und Aufwand, rechnet sich am Ende aber!

Wenn Sie übrigens ein Android-Telefon nutzen, dann können Sie all diese Einstellungen auch direkt in den Datenschutz-Einstellungen des Gerätes vornehmen. Am Ende machen die nichts anderes, als Sie auf eine mobilfreundliche Version der Google-Webseite zu leiten. Die Einstellungen, die Sie dort vornehmen, sind übergreifend gültig.

Twitter und andere Netzwerke

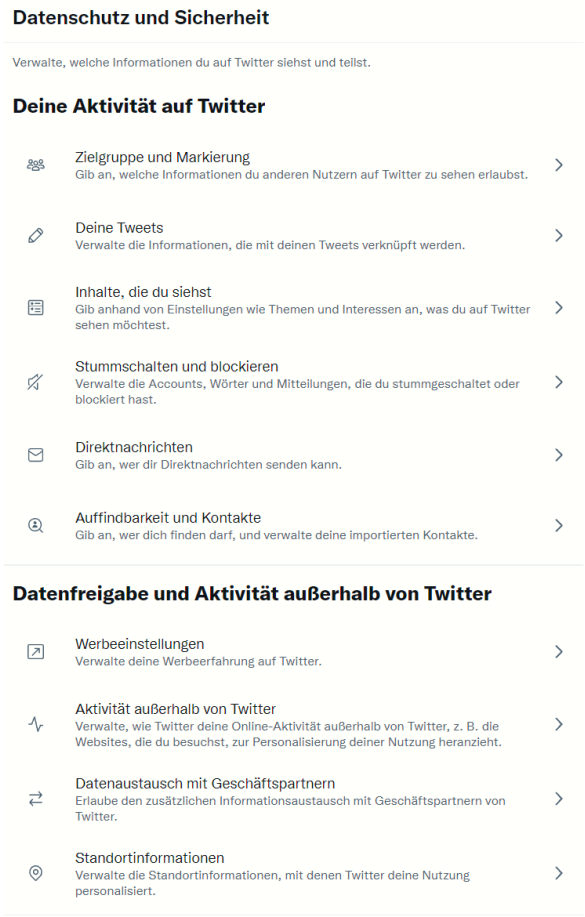
Soziale Netzwerke gibt es mittlerweile wie Sand am Meer, die Privatsphäreeinstellungen aber unterscheiden sich nicht sonderlich. Am Beispiel von Twitter lässt sich dies gut beschreiben:

Melden Sie sich an Ihrem Konto an, dann klicken Sie auf die **drei Punkte** und auf **Einstellungen und Datenschutz**. Schon öffnet sich eine lange Übersicht von Optionen, die Sie beeinflussen können.

Diese Optionen beziehen sich immer auf zwei Bereiche: Wer kann Ihre Beiträge sehen, und was können andere Anwender von Ihnen als Person sehen.

Für jeden Dienst sind die Detaileinstellungen ein wenig anders, aber die grundsätzliche Empfehlung bleibt gleich: Setzen Sie die

So geht’s leichter | Datenschutz fängt bei mir an



Privatsphäreeinstellungen so, dass Sie die meiste Kontrolle über Ihre Daten haben. Schänken Sie die Sichtbarkeit Ihrer Beiträge auf Personen ein, die Ihnen bekannt sind und die sie vorher einmal bestätigen müssen.

Die Entscheidung, Ihr Informationen mit der ganzen Welt zu teilen, sollten Sie bewusst treffen. Wenn Sie eine Firma oder eine Interessengruppe vertreten und tatsächlich öffentlich posten wollen, weil eine Freigabe von Lesern nicht möglich ist, dann gibt es immer noch die Möglichkeit, ein zweites Konto anzulegen und Ihr privates Konto davon klar abzugrenzen. Am Ende können Sie frei bestimmen, wer was von Ihnen erfährt, es gibt kein „Richtig“ oder „Falsch“.

Signal als Messenger-Alternative

Viele Anwender sind mittlerweile vorsichtig geworden: WhatsApp mag der verbreitetste Messenger-Dienst sein, spätestens seit der Übernahme durch Facebook haben aber viele Anwender ein schlechtes Gefühl bei der Nutzung. Vor allem dann, wenn es um vertrauliche Informationen

So geht's leichter | Datenschutz fängt bei mir an

geht. Diese landen immer noch auf den Facebook-Servern und für den Benutzer besteht folglich wenig Transparenz, was damit geschieht.

Bisher scheiterten andere Anbieter daran, dass sie zum einen eine sichere Infrastruktur schaffen mussten und auf der anderen Seite genug Anwender von ihrem Produkt überzeigen mussten. Der beste Messenger bringt nichts, wenn er von zu wenig Menschen genutzt wird!

Signal hat diesen Spagat geschafft. Vor allem dadurch, dass die Sicherheitsmechanismen deutlich transparenter sind: Alle Kommunikation wird auf dem Gerät des Senders bereits verschlüsselt und auf dem Gerät des Empfängers erst wieder entschlüsselt. Die Daten laufen damit zwar über die Signal-Server, sind dort aber nicht lesbar.

In Verbindung mit dem sicheren Datenaustausch zwischen zwei Parteien ergibt sich hier ein weiterer Vorteil: Signal hat einen Desktop-Client für

So geht's leichter | Datenschutz fängt bei mir an

Windows und macOS, mit dem Sie Dateien bis zu einer Größe von 100MB versenden können. Diese unterliegen natürlich derselben Verschlüsselung und damit einen Schutz vor Mitlesern wie Ihr Chats und andere Kommunikation.

Um eine Datei an eine Nachricht anzuhängen, klicken Sie im Chatfenster in der Desktop-Version auf das **Plus-Zeichen** und wählen Sie dann die Datei im sich öffnenden Explorer-Fenster aus.

Datenschutz in Internet

Das Surfen im Internet erinnert manchmal an einen undichten Duschkopf: Vorne kommt das Wasser raus, was Sie zum Duschen brauchen, aber hinten sprüht es aus einem kleinen Loch im Schlauch unbemerkt an die Wand. Während Sie im Internet surfen, hinterlassen Sie über Ihre IP-Adresse, Cookies und Browserkennungen eine Menge Daten, die Aufschluss über Ihre Vorlieben und Gewohnheiten geben.

Neben den Cookie-Einstellungen und dem Privaten Modus der verschiedenen Webbrowser können Sie auf Wunsch noch ein wenig mehr machen!

Surfen in einer Sandbox

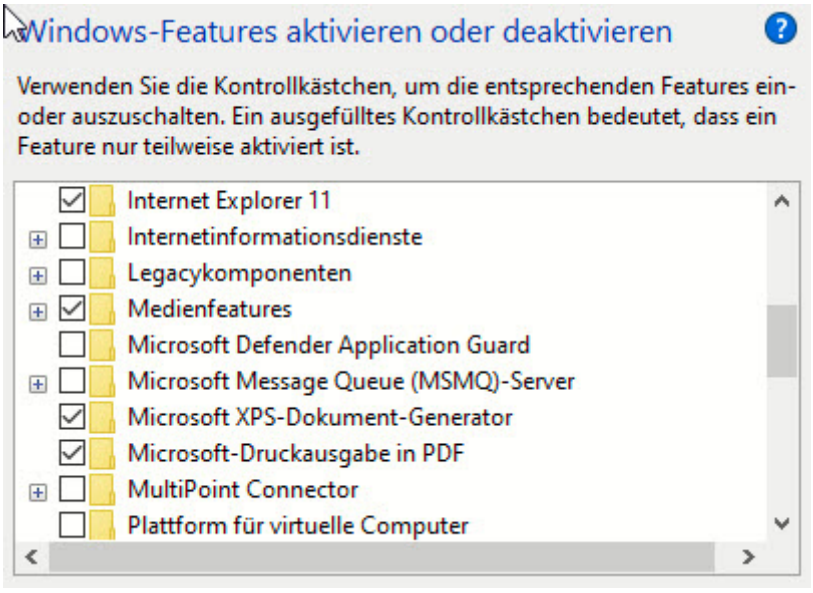
Das Internet ist eine Sammelstelle für Informationen, ein Schmelztiegel des Wissens. Allerdings gleichzeitig auch ein Ort, an dem sich auch viele üble Gesellen herumtreiben, die Ihnen möglichst viele Informationen

So geht's leichter | Datenschutz fängt bei mir an

und Ressourcen abnehmen wollen. Schadsoftware, Phishing-Angriffe, kurz: Gefahr für Ihren PC. Microsoft versucht hier entgegenzuwirken, unter anderem durch den Microsoft Defender Application Guard (MDAG). Wir zeigen Ihnen, wie Sie den nutzen können.

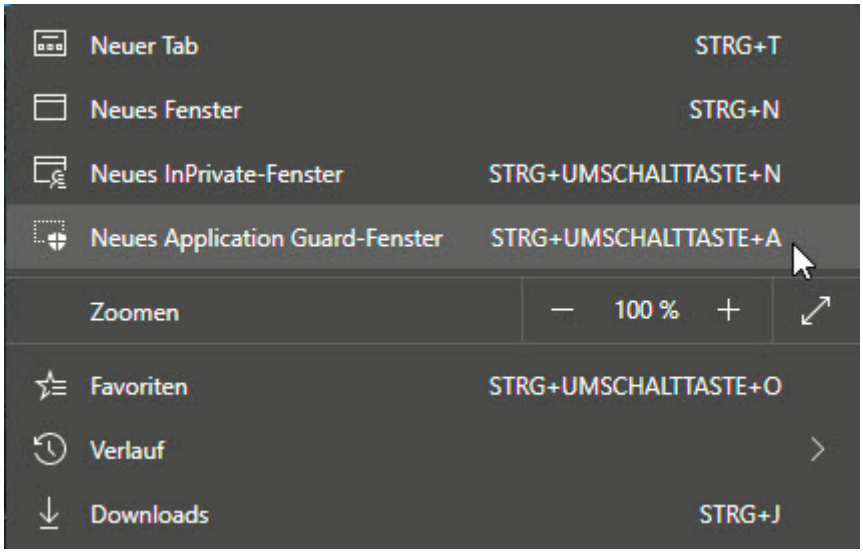
Einfach gesagt ist der MDAG eine kleine virtuelle Maschine, die zu Ihrem Rechner keinerlei Verbindung hat. Der Vorteil: Was immer Sie sich an Schadsoftware einfangen, kann nur in dieser virtuellen Maschine Schaden anrichten. Die wird aber beim Beenden der Internetsitzung gleich komplett weggeworfen. Die Schadsoftware ist damit dann auch entfernt. Was kompliziert klingt, ist in der Anwendung mit wenig Aufwand umgesetzt.

Suchen Sie in Windows nach **Windows Features aktivieren oder deaktivieren**. Dort haken Sie **Microsoft Defender Application Guard** an und dann auf OK. Das Feature wird nun installiert, der Vorgang dauert einige Minuten.



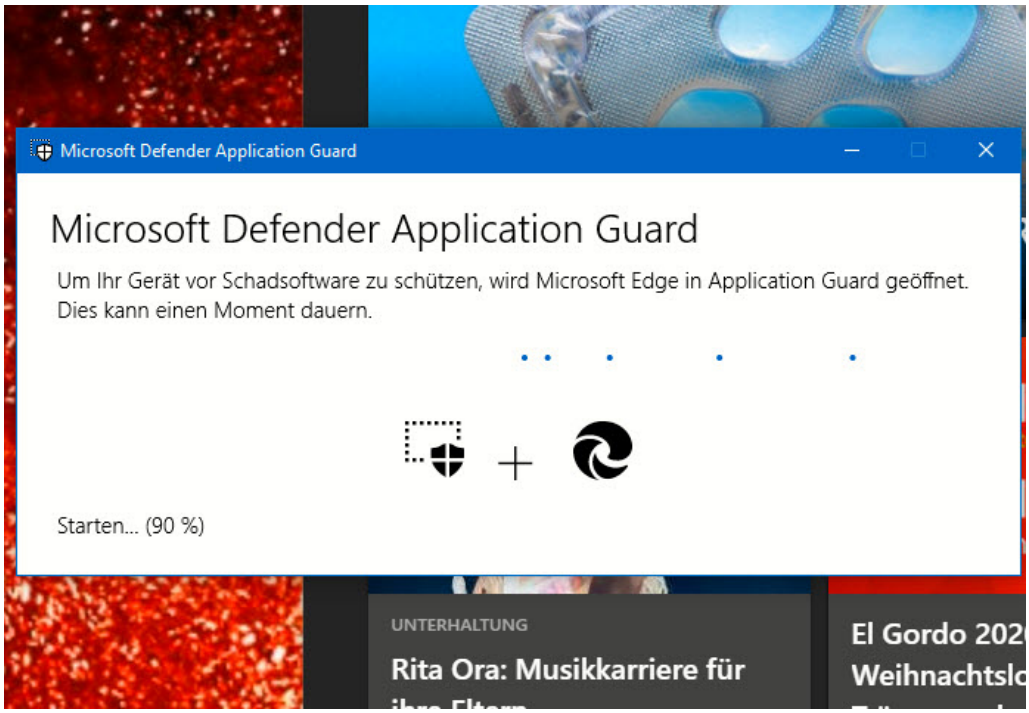
So geht's leichter | Datenschutz fängt bei mir an

Nach einem Neustart Ihres Rechners haben Sie in Edge im Menu einen neuen Punkt **Neues Application Guard-Fenster**. Klicken Sie darauf, damit die virtuelle Umgebung installiert wird.



Das kann einige Sekunden dauern, Edge zeigt Ihnen den Fortschritt auf dem Bildschirm an. Sobald der Browser offen ist, können Sie wie gewohnt surfen. Sie sollten sich bei aller Sicherheit aber bewusst sein, dass alles, was Sie in diesem Browser eingeben, natürlich immer noch ins Internet geht und abgefangen werden kann!

So geht’s leichter | Datenschutz fängt bei mir an



Anonym 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.

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.

So geht's leichter | Datenschutz fängt bei mir an

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.

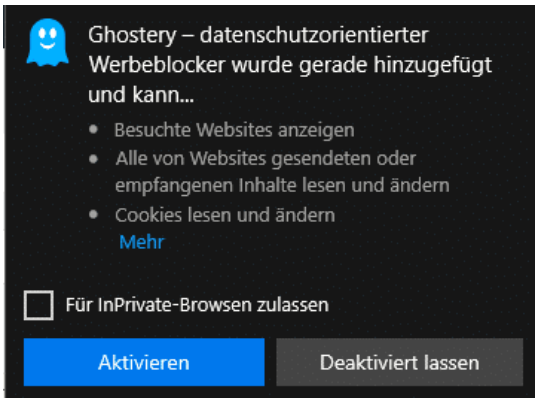
Dazu kommt, dass die Daten durch die immer wieder durchgeführte Verschlüsselung immer anders aussehen, ein Tracking also nicht möglich ist. Und da jeder Knoten nur seinen Nachbarn kennt, kann die Seite, von der Sie Daten herunterladen bzw. an die Sie Daten senden auch nicht identifizieren, dass Sie es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

So geht's leichter | Datenschutz fängt bei mir an

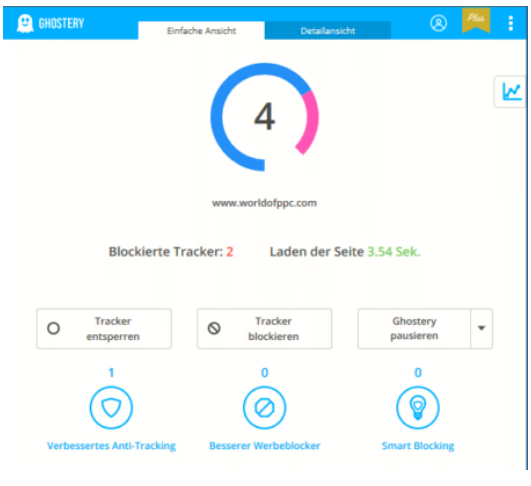
Tracking auf Webseiten mit Ghostery verfolgen

Das Tracking auf Webseiten ist mehr und mehr ein Problem: Für den Betreiber nahezu unverzichtbares Hilfsmittel, um die Webseite betreiben, finanzieren und kontrollieren zu können. Für Sie als Betroffenen nervige Datenkrake und damit nicht gerne gesehen. Irgendwo dazwischen liegt die Wahrheit, und mit dem Tool Ghostery können Sie die Kontrolle selber in die Hand nehmen.

Nach der Installation meldet sich Ghostery durch eine kleine Meldung oben rechts neben der Adresszeile Ihres Browsers. Einmalig müssen Sie zustimmen, dass das Tool aktiviert werden darf.



Jede Seite, die Sie aufrufen, wird jetzt automatisch vorher untersucht und die Elemente die Ghostery für unnötig hält, werden automatisch ausgeblendet. Am kleinen Geist-Symbol rechts neben der Adresszeile des Browsers können Sie immer die Zahl der ausgeblendeten Tracker und Werbemedien sehen.



Ein Klick darauf öffnet die Details:

Sie sehen die Zahl der blockierten Tracker und können mit einem Klick entscheiden, diese dann doch zuzulassen. Das ist immer eine Gewissensentscheidung: "Normale" Tracker (Wenn es denn sowas überhaupt gibt), die

So geht's leichter | Datenschutz fängt bei mir an

die Webseitenanalyse im Hinblick auf Besucher, Geografie etc. regeln, sind sicherlich unkritisch. Diese finden Sie unter **Website Analytics**. Unbekannte Tracker, vor allem die unter **Werbung** zu findenden, sollten Sie deaktiviert lassen.

Durch einen Klick auf **Detailansicht** können Sie weitere Informationen anzeigen lassen. Das rote Kreuz neben einem Tracker zeigt an, dass dieser Webseitenübergreifend gebockt wird. Wenn Sie das wider Erwartung nicht wollen, dann klicken Sie in das rote Kreuz und lassen Sie ihn zu.

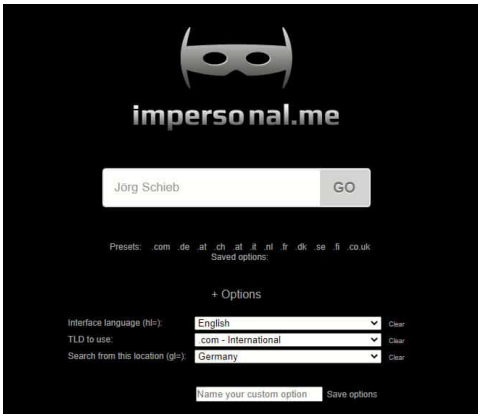
Löschanträge bei Suchmaschinen stellen

Das Internet ist ein Elefant: Es vergisst freiwillig erst einmal nichts. Das ist im Sinne einer Historie vielleicht nicht einmal schlecht, nicht alle Informationen werden über die Zeit falsch oder ungültig. Wenn es aber über individuelle Suchergebnisse geht, dann kann das durchaus anders aussehen: Nur, weil Sie in der Vergangenheit einmal in eine Zwangsversteigerung gerutscht sind, ist das Jahr später nicht mehr relevant, sondern eher schädlich. In solchen Fällen können Sie einen Löschantrag an den Suchmaschinenbetreiber stellen.

Hintergrund der Betrachtung ist der Prozess eines Spaniers gegen einen solchen Fall: Google fand immer noch den Artikel einer Zeitung, in der das Haus als in der Versteigerung befindlich dargestellt wurde. Die Schuld war lange getilgt, und dieses Suchergebnis erweckte den Eindruck, dass er immer noch Schulden habe. Nach langen Prozessen hat der EUGH klar gemacht: Diese Einträge sind zu löschen.
http://www.msn.de

Was können Sie aber jetzt aktiv tun? Kontrollieren Sie regelmäßig, welche Suchergebnisse eine Suche nach Ihrem eigenen Namen ergibt.

So geht's leichter | Datenschutz fängt bei mir an



Idealerweise mit einer Suchmaschine wie impersonal.me, die die Suche über Google durchführt, Ihre Identität aber verschleiert. Damit bekommen Sie ein nicht an Sie ausgerichtetes Suchergebnis.

Finden Sie in diesem Suchergebnis Links, die falsch oder veraltet sind und Ihnen Schaden zufügen können, dann können Sie diese in diesem Formular bei Google melden und die Löschung anfordern. Wichtig dabei: Eine Löschung der Webseite - so diese noch existiert - erreichen Sie damit nicht und müssen diese manuell anfordern!

Schützen Sie Ihre Konten

Manche Dinge sind schon von der

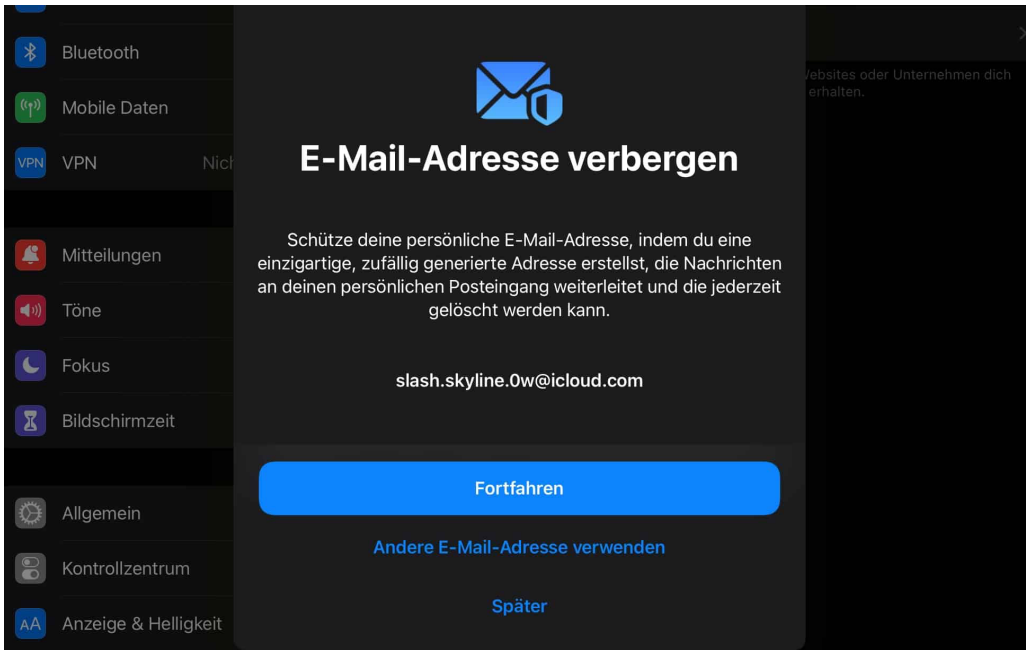
Verwenden von Einweg-E-Mail-Adressen in iOS 15

Immer mehr Bestellungen laufen über das Internet. Je mehr unterschiedliche Shops sie nutzen, desto häufiger hinterlegen Sie Ihre E-Mail-Adresse. Die Wahrscheinlichkeit steigt, dass die in einem Datenleck kompromittiert wird. Verwenden Sie stattdessen die neue integrierte Funktion von iOS 15!

Die Alternative zum Schutz der eigenen E-Mail-Adresse sind Einmal-Adressen, die Sie bei einer Vielzahl von Anbietern im Internet anlegen können und die oft nur eine ganz geringe Lebenszeit haben, schließlich reicht ja für das Abfragen der Bestell- und dann der Versandbestätigung meist ein Zeitraum von wenigen Tagen. Trotzdem: Das Anlegen und Verwalten ist ein Zusatzaufwand, der einfach Zeit kostet. Aus diesem

So geht’s leichter | Datenschutz fängt bei mir an

Grund hat Apple diese Funktion in den neuen iCloud+-Funktionen integriert.



Tippen Sie auf **Einstellungen** > **Funktions-Updates für iCloud+** > **E-Mail-Adresse verbergen**. Wenn Sie auf **+ Neue Adresse Erstellen** tippen, dann schlägt Ihnen iCloud eine neue Einmal-Adresse vor, die nicht zu Ihnen zuzuordnen ist. Sie können dazu eine Notiz eingeben, um sich selbst zu merken, für welchen Zweck Sie die Adresse verwenden wollen.

Wählen Sie als Weiterleitungsadresse eine der mit Ihrem iCloud-Konto verbundenen Adressen aus der Liste aus. Alle E-Mails an die Einmal-Adresse gehen dann erst einmal intern an iCloud und werden dann automatisch an Ihre echte E-Mail-Adresse weitergeleitet. Wenn Sie die Adresse nicht mehr brauchen, dann löschen Sie sie hier einfach.

Wenn Sie stattdessen am Desktop ein Konto anlegen wollen: Es gibt im Internet verschiedene Anbieter von Einmal-E-Mail-Konten wie beispielsweise EmailOnDeck oder TrashMail.

So geht’s leichter | Datenschutz fängt bei mir an

Schnell reagieren: Anmeldungen von fremden Geräten

Das Internet: Zentrum Ihres Lebens und Sammeltopf von Informationen. Je mehr Sie sich darin bewegen, desto mehr potenzielles Risiko auf Datenverlust haben Sie. Wenn einer der Dienste, die Sie nutzen, Sie über einen fremden Anmeldeversuch informiert, dann sollten Sie schnell reagieren!

Viele Anbieter wie Google, Netatmo, Microsoft und viele mehr überwachen die Anmeldungen an die von ihnen angebotenen Diensten sehr genau. Ihr Nutzungsverhalten gibt klare Hinweise, wann und vor allem von wo eine Anmeldung "normal" ist, und eben auch, wann nicht. Wenn Sie in Deutschland sitzen und eine Anmeldung aus Russland erfolgt, dann ist das klar zumindest fragwürdig. Wenn Sie eine E-Mail mit einer Warnung vor einem solchen Anmeldeversuch erhalten, dann reagieren Sie umgehend.

Zuerst: Auch solche E-Mails können gefälscht sein. Klicken Sie keinesfalls auf einen Link, der sich in der E-Mail befindet. Der kann Sie bei einer Fälschung schnell auf eine Fake-Seite leiten, die Ihre Anmeldedaten klaut. Stattdessen rufen Sie manuell die Seite des Anbieters auf und melden Sie sich an Ihrem Konto an. Kontrollieren Sie, ob irgendwelche Änderungen vorgenommen wurden, Bestellungen ausgelöst wurden, die Sie nicht gemacht haben etc. Und: Ändern Sie umgehend das Passwort!

Wir haben eine Anmeldung bei deinem Konto an einem neuen Standort oder über ein neues Gerät erkannt.

Ort: Russland

Gerät: okhttp 4.4.1 Other

Datum: Freitag, 24. September 2021 um 07:38:22 Moskauer Normalzeit

So geht's leichter | Datenschutz fängt bei mir an

Wenn der Google-Sicherheitscheck sich meldet

Wenn Sie sich im Internet bewegen, dann haben Sie potenziell immer ein Risiko. Sie legen Kundenkonten an, hinterlegen dort Zahlungs- und Adressinformationen und vieles mehr. Auch die Kaufhistorie ist dort jeweils hinterlegt. Sie wollen sicherlich nicht, dass jemand ohne Berechtigung darauf zugreift. Da ist es schon ein Schreckmoment, wenn Google meldet, es habe kompromittierte Passwörter gefunden.

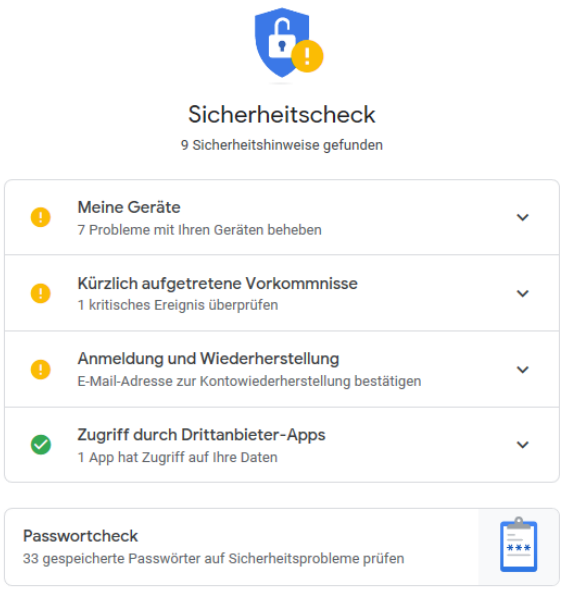
Lesen Sie die Meldung, die als E-Mail zugestellt wird, genau: In den meisten Fällen handelt es sich um einen Regelcheck, den Google über die im Konto gespeicherten Passwörter durchführt. Wird in diesem automatischen Abgleich zwischen Datenbanken über Datenlecks und Ihren gespeicherten Passwörtern eine Übereinstimmung gefunden, dann bekommen Sie diese Warn-E-Mail:

Diese Meldung bezieht sich nicht auf Ihr Google-Konto, sondern "nur" auf die darin gespeicherten Passwörter. Diese sind nicht bei Google abhandengekommen, meist sind es Datenlecks, die auf irgendwelchen Webseiten entstanden sind.

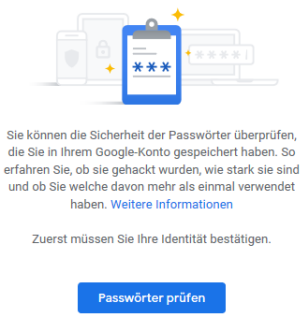
Um dies zu kontrollieren und die betroffenen Passwörter zu ändern, klicken Sie auf **Sicherheitscheck durchführen** oder rufen Sie diesen direkt auf.

So geht’s leichter | Datenschutz fängt bei mir an

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

So geht's leichter | Datenschutz fängt bei mir an

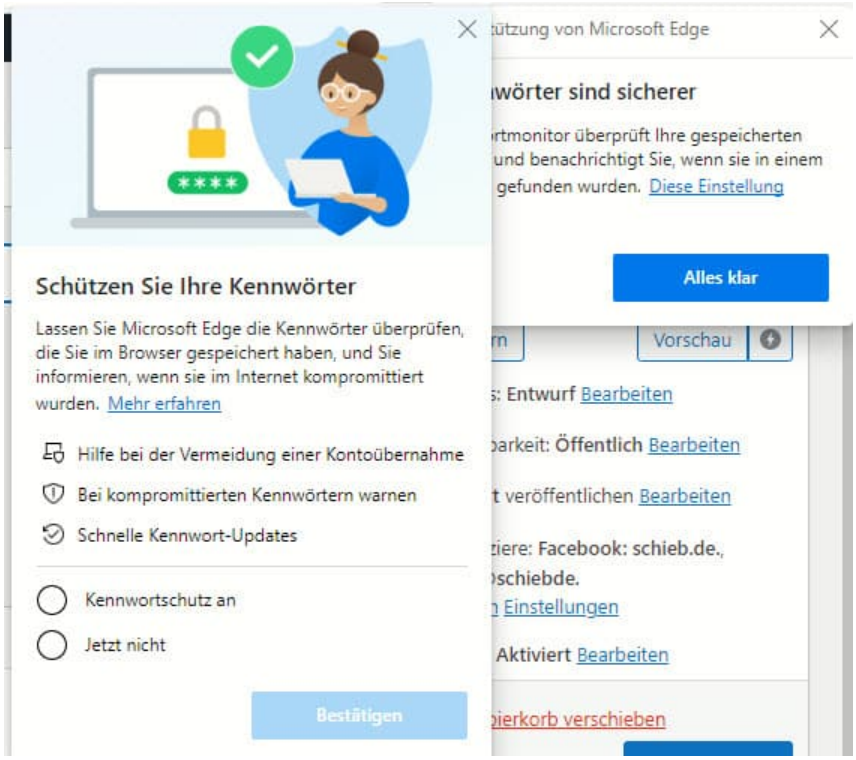
Sicherheitsanforderungen genügen. Identifiziert Google ein Kennwort, das nicht sicher ist, dann ändern Sie es zeitnah auf der Internetseite, zu der es gehört!

Kennwortschutz bei Microsoft Edge aktivieren

Kennwörter sind immer noch der Kern der Sicherung Ihrer Zugänge zu Webseiten, Online-Konten und anderen Diensten. Das bringt mit sich, dass Ihre Zugangsdaten auf allen möglichen Servern gespeichert sind. Werden durch Sicherheitslücken diese Daten Angreifern verfügbar gemacht, dann sind Ihre Login-Daten schnell in Datenbanken wie Collection #1 frei verfügbar. Gerade bei nicht häufig genutzten Konten denken Sie oft nicht an dieses Risiko. Lassen Sie sich durch Microsoft Edge unterstützen!

In den aktuellen Versionen von Edge bekommen Sie beim ersten Start die Nachfrage angezeigt, ob Sie Ihre Kennwörter schützen wollen. Wenn Sie dies aktivieren wollen, dann führt der Browser bei jeder Anmeldung an eine Webseite eine Überprüfung durch, ob Ihr Benutzername/Ihr Kennwort in einem Datenleck gefunden wurde. Klicken Sie auf **Kennwortschutz an**, um die Funktion zu aktivieren.

So geht’s leichter | Datenschutz fängt bei mir an



Wenn Sie das nachträglich machen wollen, dann klicken Sie in Edge auf die **drei Punkte** oben rechts, dann auf **Einstellungen** > **Profile** > **Kennwörter** und aktivieren Sie **Warnungen anzeigen, wenn Kennwörter in einem Onlinedatenleck gefunden werden**.

Ein solcher Hinweis sagt nicht zwingend aus, dass das Konto, an dem Sie sich gerade anmelden, kompromittiert ist. Allerdings wurde die Kombination Benutzername/Kennwort in einem Leck gefunden. Sie sollten die Zugangsdaten also umgehend ändern.