schieb.de

Jörg Schieb

Windows 10 Report

Ausgabe 19/01

- Windows 10 sicher machen
- Anforderungen an Passwörter
- Zwei-Faktor-Authentifizierung
- Sicherheit auf dem Datenträger (Bitlocker)

Inhaltsverzeichnis

Sicherheit – Bring- oder Holschuld?

Der gleich zu Anfang des Jahres 2019 durch alle Medien gegangene Fall (Stichwort: „Daten-Leak“) hat die Menschen aufgeschreckt: Wenn ein 20-jähriger Schüler mehr oder weniger mühelos auf die Daten von Prominenten und Politikern zugreifen kann, dann wohl auch auf weniger gut geschützte Daten und Informationen.

Der Daten-Leak hat die Themen Datensicherheit und Datenschutz in den Vordergrund gezerrt. Es wird wird darüber diskutiert: Wie lassen sich Daten wirkungsvoll schützen – auch die eigenen?

Eine zweifellos sehr wichtige Diskussion. Denn auch wenn die Person hinter dem Pseudonym mittlerweile identifiziert und verhaftet wurde, so ist das eigentliche Problem längst nicht gelöst.

Viele fordern eine strengere Kontrolle von Dienstleistern, die Daten speichern und verwalten. Denn Mail-Dienste und Cloud-Dienste sind bevorzugte Ziele von Hackangriffen jeder Art.

Die Politik sollte unbedingt die Rahmenbedingungen anpassen. Dass es immer noch Mail-Dienste gibt, die simpelste Passwörter wie „passwort“ oder „123456“ zulassen, ist keine zu vernachlässigende Unaufmerksamkeit, sondern ein ernsthaftes Sicherheitsrisiko. Wir finden: Die Zwei-Faktor-Authentifizierung sollte als Mindeststandard zumindest angeboten werden.

Technische Maßnahmen der Anbieter

Technische Maßnahmen sind ein wichtiger Bestandteil der Sicherheit von Daten, nicht umsonst ist die Informationssicherheit untrennbar mit dem Datenschutz verbunden.

Verarbeiter von personenbezogenen Daten sind verpflichtet, durch „geeignete technisch-organisatorische Maßnahmen“ sicherzustellen, dass nur berechtigte Personen Zugriff darauf haben. Sei es das Shop-System im Internet, die Krankenkasse oder das soziale Netzwerk Ihrer Wahl: Ohne entsprechende technische Schutzmaßnahmen ist ein Betrieb dieser Systeme zumindest fahrlässig.

Leider ist es aber immer noch so, dass viele Anbieter keinen allzu großen Wert auf Datensicherheit und Schutz der Daten legen. So lange der Gesetzgeber die Messlatte nicht höher hängt, sollten wir Konsumenten wählerisch sein – und den Anbietern den Vorzug geben, die uns die Möglichkeit geben, unsere Daten gut abzusichern.

Die EU Datenschutz-Grundverordnung (DSGVO), die seit 25. Mai 2018 in ganz Europa gilt, hat den Unternehmen zwei Jahre Zeit gegeben, die gestiegenen Anforderungen an die Verarbeitung personenbezogener Daten umzusetzen. Um dies zu stützen, erlaubt sie die Verhängung drastischer Geldstrafen in Form von Bußgeldern, wenn beispielsweise Daten unberechtigterweise an die Öffentlichkeit gelangen.

Auch wenn man sich bewusst sein muss, dass absolute Sicherheit wohl nur in der Theorie denkbar ist: Es gibt eine Vielzahl von Diensten und Produkten, die es Hackern deutlich erschweren, sich den Daten der Menschen zu nähern. Diese müssen eben nur angeschafft und eingesetzt werden, und scheinbar ist das Drohszenario, dass durch die bestehenden Bußgeldvorschriften aufgebaut wird, noch nicht groß genug, dass Firmen dies auch tatsächlich tun. Hier ist sicherlich der Gesetzgeber gefragt, sich Gedanken über Alternativen zu machen.

Die Facebook-Skandale des vergangenen Jahres beispielsweise zeigen, dass der laxe Umgang mit Daten offensichtlich immer noch zum guten Ton gehört und Unternehmen die öffentliche Kritik abschütteln können, ohne dass daraus ernsthafte Konsequenzen entstehen.

Sicherheit hat (mindestens) zwei Seiten

Ein System kann noch so sicher ausgestaltet, mit Hardware und Software geschützt sein: Es bleibt ein Risikofaktor, der immer schwer in den Griff zu bekommen – der Anwender.

Die Pferdekoppel, die mit verschiedenen Zäunen und elektronisch hochkomplexen Schlössern gesichert ist, kann die Pferde dann nicht vor Ausbruch bewahren, wenn der Pferdepfleger das Gatter offenstehen lässt. Anders ausgedrückt: Ein sicheres System ist ein System, das den User abgeschafft hat.

Dabei ist es doch so einfach: Windows 10 bietet schon im Standard so viele Hilfestellungen, mit denen Sie Ihren PC, Ihre Daten und E-Mails schützen können. Sie müssen Sie am Ende nur nutzen und konsequent umsetzen. Auf den folgenden Seiten finden Sie viele Hinweise, Tipps und Tricks, um den Windows 10-PC deutlich besser abzusichern.

Die „weichen" Sicherheitsfaktoren

Auch wenn Sicherheitsmaßnahmen noch so ausgeklügelt sind: Das mächtigste Mittel gegen das Ausspähen Ihrer Daten ist kein technisches, sondern ein biologisches: Ihr eigenes Misstrauen. Hinterfragen Sie alles kritisch, was Sie tun. Einige Beispiele:

Das unglaubliche Schnäppchen

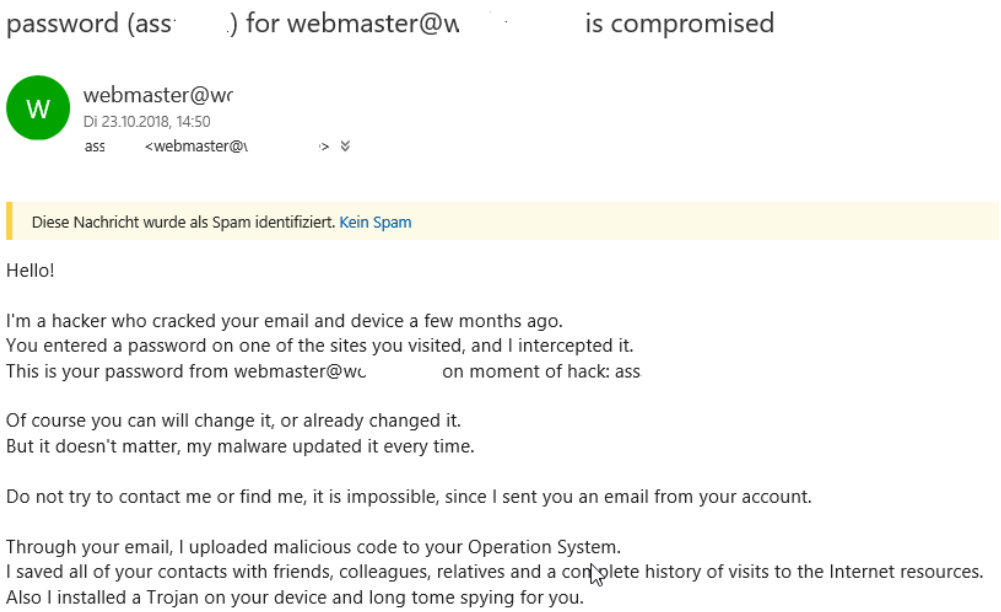
Im Internet tummeln sich bei weitem nicht nur freundlich gesinnte Zeitgenossen. Wer Ihnen angeblich Ware oder Dienstleistungen für den Bruchteil des normalen Preises feilbietet, der hat mit großer Sicherheit eine ganz andere Absicht.

Oft finden sich beispielsweise bei Facebook Anzeigen, die ein Produkt bewerben, dass eigentlich von einem anderen Händler kommt. Die Seite ist komplett identisch, nur der Zahlungsempfänger ist ein anderer. Wer dann meint, ein iPhone im Wert von EUR 1000,- für EUR 300,- als „super limitiertes Angebot" zu bekommen, der bekommt schnell die Quittung für seine Unvernunft.

Kennen Sie den Händler nicht tatsächlich aus Geschäften, dann lassen Sie lieber die Finger davon. Schnell ist das Geld weg, und die bestellte Ware wird gar nicht oder in deutlich schlechterer Qualität geliefert.

Die Erpressung

Haben Sie auch schon einmal die Mail bekommen, dass Ihr E-Mail-Account gehackt wurde und das mit einer richtigen E-Mail-Adresse und einem korrekten Passwort?



Diese vermeintlich authentische E-Mail fordert Sie auf, ganz schnell einen bestimmten Betrag in Bitcoins zu beschaffen und an den Absender zu überweisen. Ein Ändern des Passwortes nütze nichts, weil der Rechner schon lange mit einem Virus infiziert sei… und so weiter.

In den allermeisten Fällen sind diese E-Mails heiße Luft. Sie beziehen ihre Informationen aus Datenbanken, die gestohlene Passwörter enthalten, und versuchen einfach mal, Panik zu erzeugen.

Überweisen Sie nichts! Aber prüfen Sie natürlich, ob das Kennwort tatsächlich noch aktuell ist – und ändern Sie es.

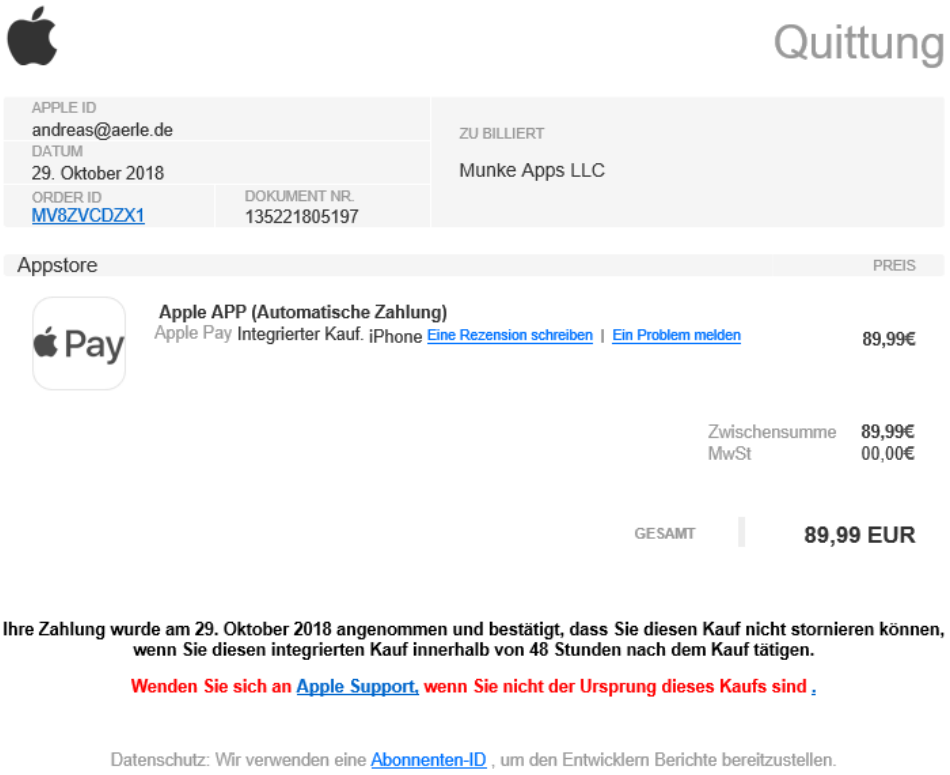
Phishing: Die gefälschte Händler-E-Mail

Ein anderer beliebter und leider auch weit verbreiteter Trick das die Phishing-Mail. Die Rezeptur ist einfach: Die Betrüger verschicken eine E-Mail, die so aussieht, als käme sie von einem bekannten Online-Shop, einem Telekommunikationsanbieter oder einer Bank oder einem Zahlungssystem wie Paypal.

Die Betrüger schicken an ihnen bekannte E-Mail-Adressen (die ihrerseits auch wieder ergaunert sein können) eine vermeintliche Rechnung über ein gar nicht gekauftes Produkt oder warnen vor Unzulänglichkeiten im Konto. Die Wahrscheinlichkeit ist hoch, dass der Empfänger sich angesprochen fühlt und eine Reaktion erfolgt.

Auch eine Aufforderung, aufgrund eines Sicherheitsvorfalles unbedingt die Zugangsdaten zu ändern, ist Garant dafür, dass der betroffene Anwender umgehend aktiv wird, auf den Link in der E-Mail klickt und sich schnell anmeldet. Mit seinem echten Benutzernamen und seinem echten Passwort.

Dummerweise ist in vielen Fällen die Webseite, auf die Sie geleitet werden, nicht echt. Sie sieht nur echt aus. Genau das ist der Trick der Phishing-Betrüger. Wem das nicht auffällt, der trägt die korrekten(!) Zugangsdaten auf einer gefälschten Webseite ein – und übermittelt die sensiblen Daten so einem Betrüger. Der hat dann Ihre Zugangsdaten und kann fröhlich Bestellungen auslösen, Ihr Konto übernehmen und Schaden anrichten: Eine klassische Phishing-Attacke.



Quittung

APPLE ID
andreas@aerle.de
DATUM
29. Oktober 2018
ORDER ID
MV8ZVCDZX1
DOKUMENT NR.
135221805197
ZU BILLIERT
Munke Apps LLC

Appstore PREIS

Pay
Apple APP (Automatische Zahlung)
Apple Pay Integrierter Kauf. iPhone Eine Rezension schreiben | Ein Problem melden 89,99€

Zwischensumme 89,99€
MwSt 00,00€

GESAMT 89,99 EUR

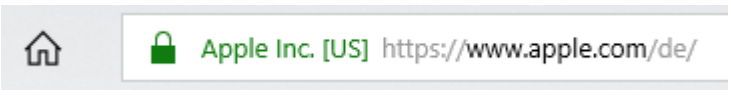
Ihre Zahlung wurde am 29. Oktober 2018 angenommen und bestätigt, dass Sie diesen Kauf nicht stornieren können, wenn Sie diesen integrierten Kauf innerhalb von 48 Stunden nach dem Kauf tätigen.

Wenden Sie sich an Apple Support, wenn Sie nicht der Ursprung dieses Kaufs sind .

Datenschutz: Wir verwenden eine Abonnenten-ID , um den Entwicklern Berichte bereitzustellen.

Die wichtigste Empfehlung in diesem Fall: Klicken Sie auf keine Links in solchen E-Mails. Rufen Sie manuell die Webseite des Händlers auf und melden Sie sich an. Damit können Sie vermeiden, dass Sie auf eine falsche Seite geleitet werden.

Wenn Sie bereits versehentlich auf den Link geklickt haben, dann kontrollieren Sie unbedingt die Adresse, die Ihnen angezeigt wird. Steht dort die „echte“ Internet-Adresse, dann ist alles gut.



Meist versuchen die Phishing-Seiten, durch möglichst ähnliche Adressen den Anschein der Echtheit zu erwecken, im Beispiel vielleicht *apple.xxlservices.com* oder ähnlich. Abgewandelte Adressen sind ein nahezu sicheres Zeichen für einen Betrugsversuch.

Der freundliche Anrufer

Eine ebenfalls gerne gewählte Masche, Zugriff auf einen fremden Rechner oder die Daten darauf zu bekommen, ist der Anruf eines freundlichen Servicemitarbeiters. In oft gebrochenem Deutsch ist angeblich Microsoft aufgefallen, dass es einen Defekt oder Virenbefall auf Ihrem Rechner gibt und man bietet Ihnen ganz selbstlos Hilfe an.

Dazu müssen Sie nichts mehr machen als dem Anrufer durch Aufruf einer Webseite oder Fernwartungssoftware Zugang zu Ihrem Rechner geben, am besten noch unter Preisgabe Ihrer Zugangsdaten.

Ist das geschehen, behebt der Bösewicht natürlich nicht etwaige Probleme auf Ihrem Rechner, ganz im Gegenteil: Er schließt Sie aus Ihrem Rechner durch Änderung des Passwortes aus, und verlangt dann Geld dafür, Sie wieder hineinzulassen. Oder er schleust

Schad-Software ein, die ihm dann die Fernsteuerung des Rechners und den Zugriff auf Ihre Daten erlaubt.

Zusammengefasst: Neben all den auf den folgenden Seiten beschriebenen technischen Maßnahmen bewahren Sie sich unbedingt Ihren gesunden Menschenverstand! Und treffen Sie die folgenden technischen Maßnahmen…

Sicherheit bei der Anmeldung

Je mehr an für Sie wichtigen Informationen Sie auf einem Gerät speichern, desto höher werden Ihre Ansprüche an deren Sicherheit: Kein Fremder soll an Gerät und Daten kommen, wenn Sie das nicht explizit so wünschen.

Dabei ist es egal, ob es sich um Ihren PC zuhause, das Notebook, Tablet oder Smartphone handelt. Im Falle eines Verlustes oder Diebstahls ist der Verlust der Hardware meist das kleinere Problem, denn die ist ersetzbar. Vertrauliche Dokumente, Kontoinformationen oder gar den Zugriff auf das Online-Banking in den Händen Fremder wiegt da viel schwerer.

Windows 10 bietet Ihnen serienmäßig eine Vielzahl an Möglichkeiten, aktiv an der Sicherheit Ihrer Daten und Geräte mitzuarbeiten und sich auf Ihre tatsächliche Arbeit konzentrieren zu können.

Die Herausforderung

Bei einem Windows 10-Gerät gibt es verschiedene Bereiche, die Einfluss auf die Sicherheit Ihrer Daten haben. Es reicht nicht, wenn Sie hier nur in einem Bereich aktiv werden. Schon das kleinste Schlupfloch kann einem Eindringling reichen. Das ist wie bei einem Dach: Auch wenn nur eine kleine Stelle undicht ist, dann kann Wasser eindringen. Je länger das der Fall ist, desto größer wird das Loch – und desto nasser werden die Decken und Wände. Besser also, Sie lassen erst gar kein Wasser hinein!

Wie sie es gewohnt sind, stellen wir Ihnen hier hauptsächlich den Dachdecker, der das Dach auf Dichtigkeit prüft, und nur für den Notfall den Eimer, der das Wasser sammelt!

Das Zwiebelprinzip

Das Dach Ihres Hauses ist in mehreren Schichten abgedichtet: Die Dachziegel, darunter Folie, Isolierung und eine Deckenverkleidung sollen sicherstellen, dass bei einem Loch in einer der Schichten das Wasser nicht gleich ungehindert in die Wohnung fließen kann.

Dieses Prinzip, seiner verschiedenen Schichten wegen auch „Zwiebelprinzip" genannt, lässt sich genauso auf einen PC mit Windows 10 anwenden. Verschiedene Sicherheitsschichten schützen einander und wirken zusammen, um einen optimalen Schutz zu bieten.

Die Hardware

Normalerweise wird Ihr Windows 10-PC in Ihrem Arbeitszimmer in einem Haus oder einer Wohnung stehen. Damit sind schon mal zwei Sicherheitsschichten vorhanden.

Sind diese aber einmal durchdrungen, weil ein Dieb sich widerrechtlich Zugang verschafft, dann hat er Zugriff auf die Festplatte und kann die darauf befindlichen Daten auslesen.

Es sei denn, Sie nutzen die Windows-eigene Verschlüsselung, die für jeden Außenstehenden aus den Daten einen unleserlichen Datenbrei macht, den nur Sie in Ihrem Rechner entschlüsseln können. Nur dann sind die Daten lesbar und zu verwenden.

Noch wichtiger ist dies, wenn sie ein mobiles Gerät wie ein Tablet oder ein Notebook verwenden: Hier fällt unterwegs der Schutz der eigenen vier Wände weg!

Der Zugang

Statt physischen Schlössern, wie sie in Ihrem Haus und Arbeitszimmer vorhanden sind, gibt es die Zugangsberechtigungen: Sie müssen sich an Ihrem PC anmelden, in dem Sie entweder das Microsoft-Konto mit seinem Benutzernamen und Passwort nutzen oder ein lokales, nur auf Ihrem PC vorhandenes Konto einrichten. Nur mit den entsprechenden Zugangsdaten ist dann ein Zugriff auf Ihren PC möglich.

Windows 10 bietet mit „Windows Hello“ zusätzlich noch die Möglichkeit der Anmeldung mittels Fingerabdruck oder Gesichts-Scan, was die Anwendung deutlich vereinfachen kann. Klar, nicht jeder Rechner/Notebook ist serienmäßig mit Spezialkameras oder Sensoren ausgestattet. Doch entsprechende Zusatz-Hardware lässt sich günstig kaufen.

Neben dem Zugang zu Windows 10 selbst haben Sie auf dem PC eine Vielzahl von Zugängen zu Webseiten, Konten und Programmen, für die Sie jeweils einen Benutzernamen und ein Passwort benötigen. Da ist es wichtig, all diese Zugangsdaten sicher zu verwalten. Denn einen Fehler

sollten sie nicht machen: Ein Benutzername und ein Standard-Passwort zu verwenden. Erhält ein Unberechtigter Kenntnis davon, dann bekommt er damit Zugang zu all Ihren Konten!

Der Schutz vor Viren und anderen Schädlingen

Eindringlinge in ein Windows 10-System müssen nicht aus Fleisch und Blut sein: Viren, Tojaner und andere virtuelle Schädlinge können dafür sorgen, dass Ihre Daten nicht sicher auf Ihrem PC bleiben, sondern heimlich nach draußen gegeben werden.

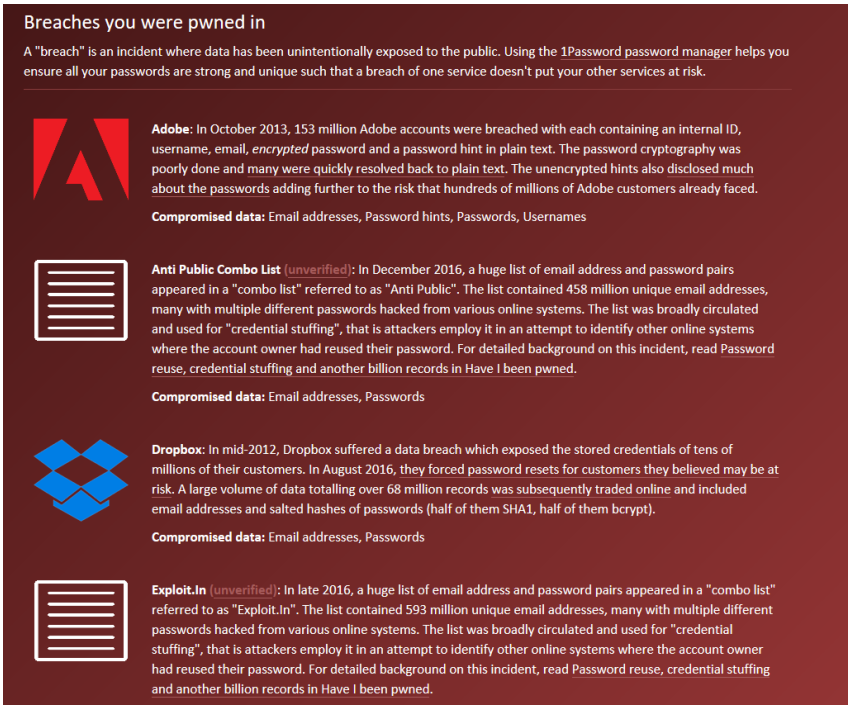
Virenschutz und Firewall sind also eine weiter Schicht der Sicherheit Ihres Windows 10-Systems. Windows 10 hat einiges serienmäßig an Bord. Ich habe im Windows 10 Report die Funktionen auch bereits ausführlich vorgestellt, etwa in Ausgabe 16/06.

Zugangsschutz: Anforderungen an Passwörter

Jedes Konto – ob für den Zugang zu Windows 10, einem Online-Shop oder Ihre Banking-Software – benötigt einen Anmeldenamen und ein Passwort. Als Benutzername kommt häufig die eigene E-Mail-Adresse zum Einsatz, die Sie zur Kommunikation verwenden, sodass „nur" das Passwort der wirklich geheime und geheim zu haltende Teil ist. Grund genug, bei der Vergabe ein wenig Zeit zu investieren und ein möglichst sicheres Passwort zu vergeben.

Ist es schon zu spät?

Immer wieder wird in den Nachrichten über Datenlecks berichtet: Durch Sicherheitsvorfälle werden E-Mail-Adressen, Nutzernamen und Passwörter gestohlen – und dann im Internet verkauft. Käufer dieser erbeuteten Zugangsdaten hat dann Zugriff auf all Ihre Benutzerkonten, zumindest Sie das Passwort nicht geändert haben.



Die bekanntesten Sicherheitsvorfälle (zumindest die, die öffentlich bekannt geworden und dadurch dokumentiert sind), haben Experten auf der Webseite https://haveibeenpwned.com/ zusammengefasst. Dort können Sie erfahren, ob und bei welchem Hack Ihre Zugangsdaten schon mal erbeutet wurden. Dazu muss lediglich die Mail-Adresse eingegeben werden,

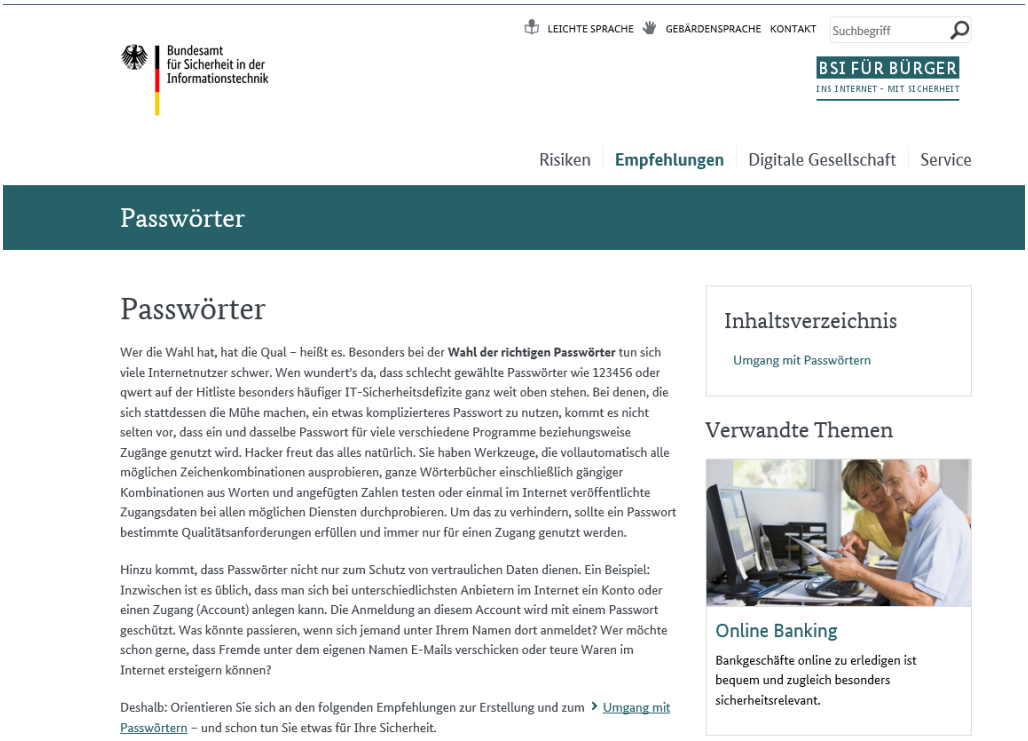
Wenn Sie betroffen sind, dann ändern Sie so schnell wie möglich das Passwort. Am besten regelmäßig. Auch wenn Sie das nach dem Vorfall wissentlich oder unwissentlich schon gemacht haben: Besitzer der erbeuteten Daten wissen zumindest, dass die Benutzernamen und E-Mail-Adressen existieren und müssen sich so nur noch darauf konzentrieren, das Passwort herauszufinden.

Das sichere Passwort

Eigentlich ist der Begriff irreführend. Ein „sicheres" Passwort ist ebenso theoretisch wie ein Perpetuum Mobile. Denn mit genügend Rechenpower und Zeit lässt sich jedes Passwort irgendwann herausfinden. Sie können den Aufwand aber zumindest so hochtreiben, dass die Wahrscheinlichkeit, dass das passiert, gegen Null geht.

Was ist nun ein sicheres Passwort? Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt unter https://www.bsi-fuer-buerger.de im Bereich **PASSWORT** einige Hinweise:

1. **ES SOLLTE EINFACH ZU MERKEN SEIN:** Je schwerer ein Passwort zu merken ist, desto höher ist die Wahrscheinlichkeit, dass sie es sich aufschreiben. Das widerspricht dem Anspruch, dass es nur Ihnen selbst bekannt sein soll. Das so beliebte kleine, gelbe PostIt als Zwischenspeicher ist eben nicht sicher!



2. **Es sollte mindestens 8 Zeichen haben:** Mehr (an Buchstaben) ist hier tatsächlich mehr (an Sicherheit). Bei den Passwörtern für Ihr WLAN werden gar 20 Zeichen empfohlen.

3. **Nutzen Sie Sonderzeichen, Groß- und Kleinschrift und Ziffern:** Je komplexer das Passwort ist, desto schwerer ist er herauszubekommen. Wichtig dabei auch:

4. **Verwenden Sie keine über sie bekannten oder herauszufindenden Daten als Passwort:** Namen von Familienmitgliedern, Haustieren, Freunden, Geburtstage, Hochzeitstage etc. eignen sich nicht als Passwort. Auch keine Wörter, die in einem Wörterbuch vorkommen, oder Zeichen- oder Ziffernfolgen, die auf- oder absteigend sind wie 123456 oder abcdef.

Verlieren Sie nicht den Mut: Diese Anforderungen lassen sich tatsächlich umsetzen.

Wichtig

Passwörter aus dem Wörterbuch auszuwählen, ist keine gute Idee: So genannte Wörterbuch-Angriffe (Dictionary Attacks) sind nicht selten: Automatisiert wird der Benutzername immer wieder angemeldet, das Passwort wird eines nach dem anderen aus einem Wörterbuch genommen. Bei den heutigen Rechenkapazitäten ist es nur eine Frage der (kurzen) Zeit, bis das richtige Passwort erraten wäre!

Passwörter müssen nicht lesbar sein oder aus tatsächlich vorhandenen Begriffen bestehen, damit Sie sich daran erinnern können. Der Ausgangspunkt zu einem guten Passwort kann beispielsweise ein für Sie ganz persönlich leicht zu merkender Satz oder eine Zeile aus einem Lied sein.

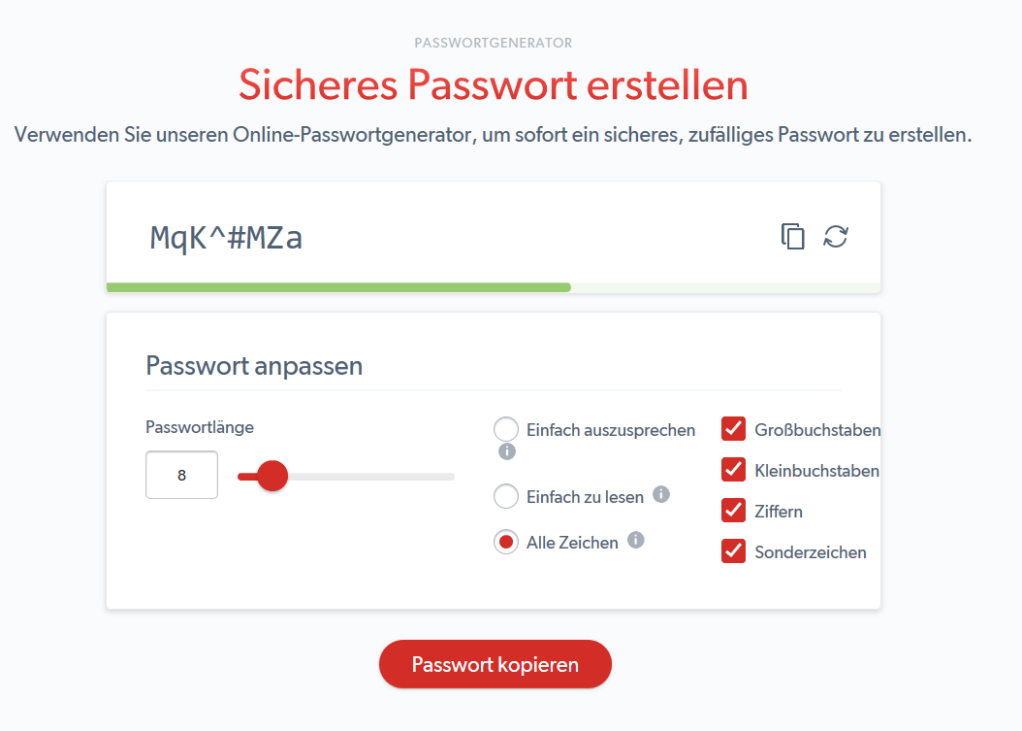
„Ich habe im Sommer 2018 den Motorradführerschein gemacht!" beschreibt ein Ereignis, an das Sie sich sicherlich noch lange erinnern werden. Nehmen Sie davon nur die Anfangsbuchstaben (unter Beachtung der Groß- und Kleinschrift) und lassen Sie Ziffern und Satzzeichen an ihrem Platz, und schon haben Sie *IhiS2018dMg!* als Passwort. Dieses Passwort errät niemand, der nicht Ihren speziellen Satz kennt.

Verwendung eines Passwortgenerators

Eine weitere Alternative ist die Verwendung eines Passwortgenerators, also eines Programms bzw. einer Webseite, die Ihnen nach bestimmten Vorgaben sicher Passwörter generiert. Kostenlos finden Sie dies beispielsweise unter https://www.lastpass.com/de/password-generator

Wählen Sie gewünschte **PASSWORTLÄNGE** ein, wählen Sie ob **GROßBUCHSTABEN**, **KLEINBUCHSTABEN**, **ZIFFERN** und/oder **SONDERZEICHEN** verwendet werden sollen. Auf Wunsch können Sie dann das Passwort

noch für das Lesen oder Sprechen optimieren, diese Einstellungen beeinflussen die Verwendung von Sonderzeichen bzw. leicht verwechselbaren Zeichen im Passwort.



Aus LastPass können Sie das Kennwort dann über das Symbol mit den beiden Seiten oben rechts in die **Zwischenablage** kopieren und vor dort aus weiterverwenden.

Speichern von Passwörtern in einem Safe

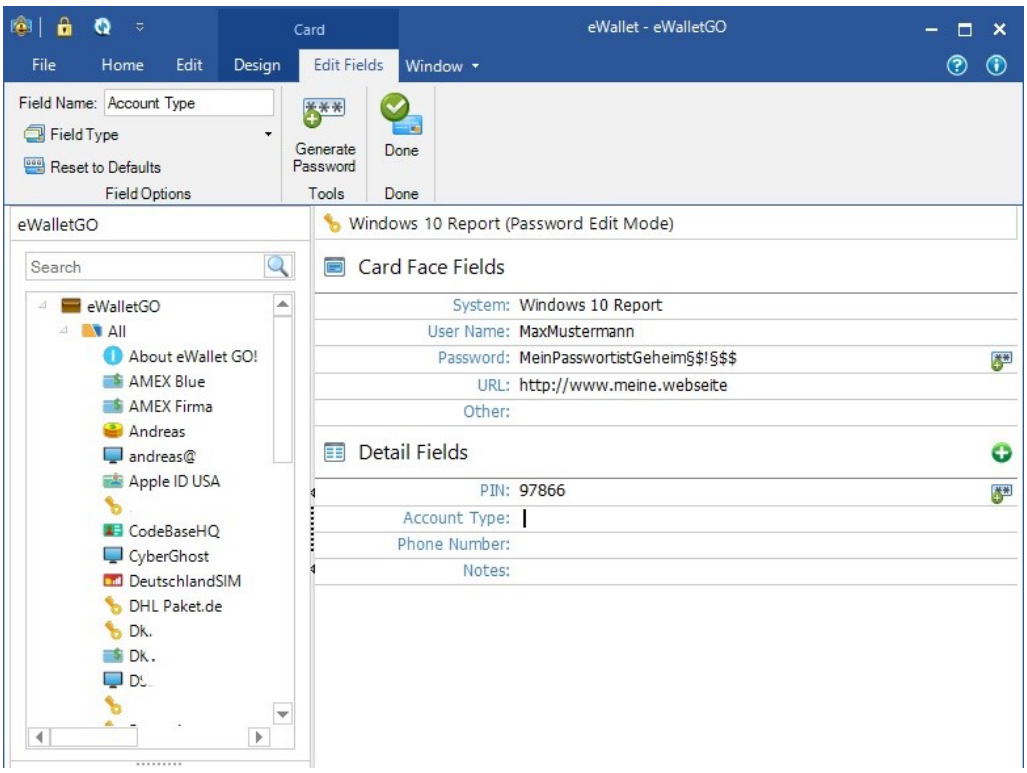
Es bedarf keiner langen Erklärung, dass das Aufschreiben von Passwörtern keine wirklich gute Idee ist. Auch wenn es kaum zu glauben ist: Viele erfolgreiche Angriffe auf Systeme kommen nicht über einen technischen Einbruch über das Internet oder interne Netzwerk, sondern über kleine, gelbe Klebezettelchen, auf denen Anwender ihre Passwörter aufschreiben und „ganz geheim“ am Monitor oder unter der

Schreibtischauflage verstecken. Auch eine Excel-Tabelle ist nur eine bedingt gute Idee!

Natürlich fordert der Anspruch, komplexe und unterschiedliche Passwörter zu verwenden und sich diese auch noch zu merken, aber auch dafür gibt es sichere Lösungen: Die so genannten Passwortsafes.

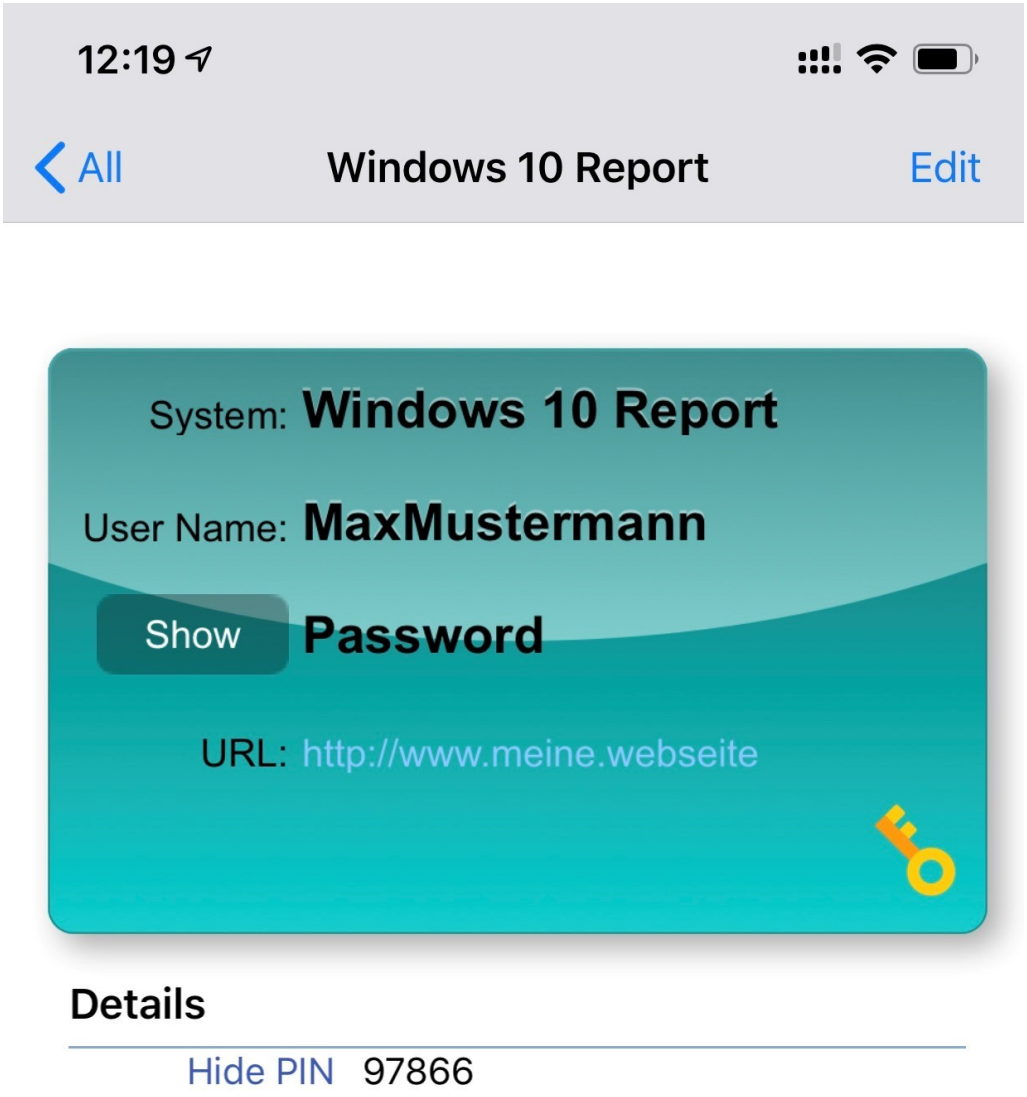
Dies sind Programme, in denen Sie Ihre Passwörter speichern können und die die Datei, in denen diese abgelegt werden, verschlüsselt und so vor unberechtigtem Zugriff schützt.

Bekannte Passwort-Safes sind zum Beispiel 1Password (https://1password.com) und KeePass (https://keepass.info). Wenn Sie mit verschiedenen Plattformen auf Desktop, Tablet und Smartphone arbeiten, dann ist Ilium´s eWallet (https://www.iliumsoft.com/) eine gute Wahl. Auch Dashlane ist ein hervorragender Passwort-Manager.



eWallet bietet die Synchronisation der (256bit-verschlüsselten) Passwortdatei mit verschiedenen Online-Speichern an und hat für alle großen Plattformen (Windows, MacOS, iOS, Android) einen entsprechenden Client.

Diese kosten zwar jeweils knapp EUR 10,-, lösen Ihnen aber die Herausforderung, dass Sie die Passwörter synchron halten und von überall her darauf zugreifen können. Eine einmal eingegebene Passwort-Karte ist nach Beendigung des Speichervorgangs sofort auf den anderen Geräten verfügbar, bei Änderungen verhält es sich ebenso.



Wichtig

Wenn Sie die Windows-Version von eWallet verwenden möchten, dann müssen Sie von der Ilium-Webseite die **Desktop-Version** herunterladen, nur diese ist mit den anderen Plattformen kompatibel. Die im Windows 10-Store verfügbare „eWalletGo"-App leider nicht: Sie verwendet ein eigenes Format und ist nicht für alle Systeme verfügbar!

Sichere Anmeldung unter Windows 10

Anders als bei älteren Windows-Versionen hat Windows 10 im Standard eine Bindung an das Microsoft-Konto (auch Microsoft Account). Dieser verbindet alle Geräte mit Windows miteinander, sei es ein Desktop, Notebook, Tablet, die XBOX oder ein Windows Phone.

Der Vorteil: Die automatische Synchronisierung von Einstellungen und Informationen zwischen all diesen Geräten. Dazu gehören unter anderem auch die Kennwörter, die Sie auf Internetseiten verwenden und bei denen Sie in Microsoft Edge zustimmen, dass diese gespeichert werden sollen.

Tipp

Wenn Sie sich mit Ihrem Microsoft-Konto an Windows 10 anmelden, können Sie festlegen, ob und welche Inhalte synchronisiert werden sollen. Die Einstellungen finden Sie unter **Konten**, **Einstellungen synchronisieren**.

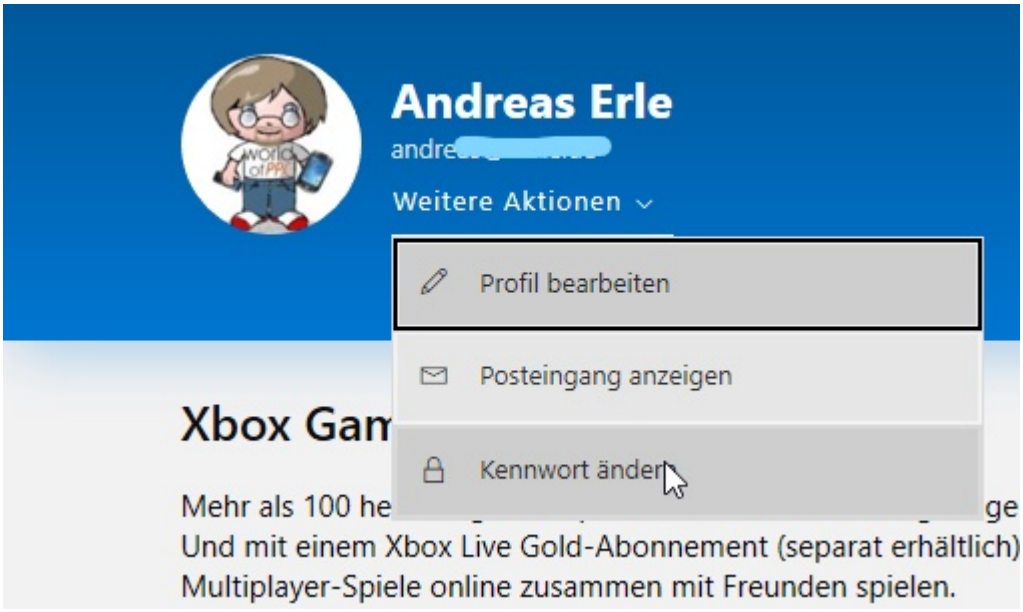
In der Liste der möglichen Synchronisierungsobjekte findet sich auch ein separater Eintrag für die **Passwörter**. Eine große Hilfe, wenn Sie zwischen eigenen Geräten wechseln. Wenn Sie aber an einem PC mit mehreren Leuten arbeiten und dieser mit Ihrem Microsoft-Konto angemeldet ist, dann sollten Sie diese Option ausschalten.

Ändern des Windows-Kennwortes

Im Normalfall sind Sie nicht mit einem auf Ihrem Windows 10-PC lokal gespeicherten Kennwort angemeldet, sondern mit dem Microsoft-Konto, und dessen Kennwort muss dann auch im Internet geändert

werden. Nichts desto trotz können Sie sich das lästige Eingeben der Webadresse der Verwaltungsseite sparen:

Klicken Sie in den **Einstellungen** von Windows 10 auf Konten, dann unter Ihrem Namen auf **Mein Microsoft-Konto verwalten**. Die Microsoft Konto-Seite wird automatisch aufgerufen und Sie können unter **Weitere Optionen**, **Kennwort ändern** unter Eingabe des alten Kennwortes das neue eingeben und bestätigen.



Die Änderung wird sofort aktiv. Es kann aber einen Moment dauern, bis diese auch bei jedem Gerät ankommt, auf dem Sie das Microsoft-Konto verwenden. Nach und nach werden Sie alle Geräte dann nach der Eingabe des Kennwortes fragen, denn das alte Kennwort wird als falsch zurückgewiesen.

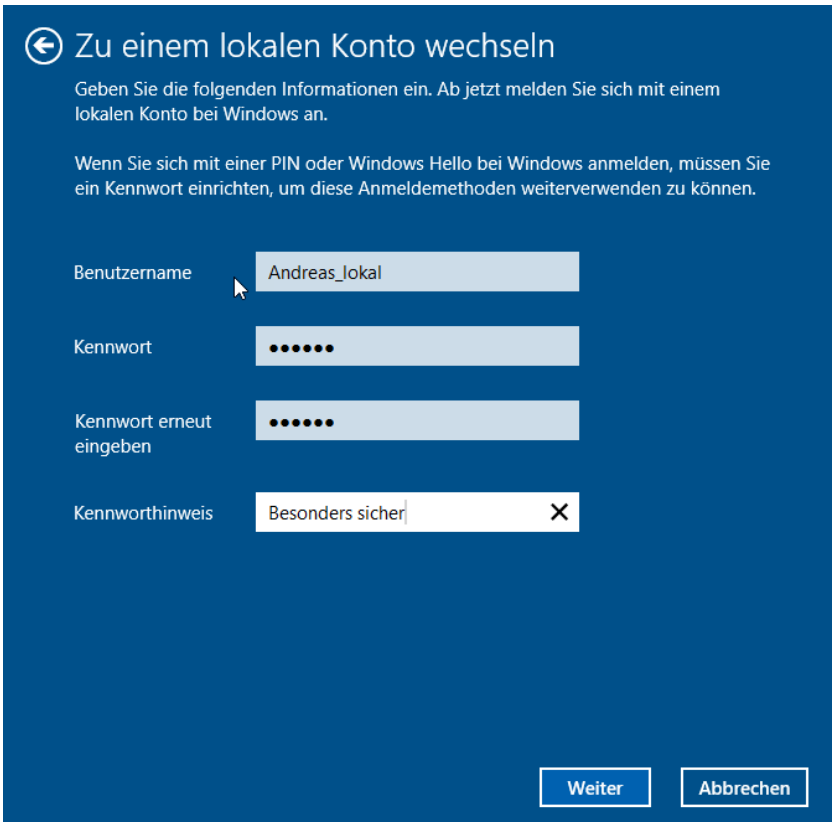
Geben Sie einfach das neue Kennwort ein, wenn Sie danach gefragt werden. Die Geräte laufen dann ganz normal weiter, wie Sie es gewöhnt sind.

Tipp Sie haben Ihr altes Passwort vergessen? Dann ist erst einmal auch die Anmeldung zur Konto-Änderung natürlich nicht mehr so einfach möglich. Auch hier müssen Sie nicht verzweifeln: Sie können statt der Eingabe des alten Passworts auf den Link **Kennwort vergessen** klicken. Microsoft schickt Ihnen dann an die hinterlegte E-Mail-Adresse eine E-Mail, mit der Sie auch ohne Eingabe des alten ein neues Kennwort vergeben können.

Wechseln zwischen lokalem und Microsoft-Konto

Nicht jeder Anwender möchte seine Daten in der Cloud haben. Und so ist die Verwendung eines lokalen Kontos, bei dem alle Daten auf der Festplatte Ihres Windows 10-PCs bleiben, durchaus eine gängige Alternative.

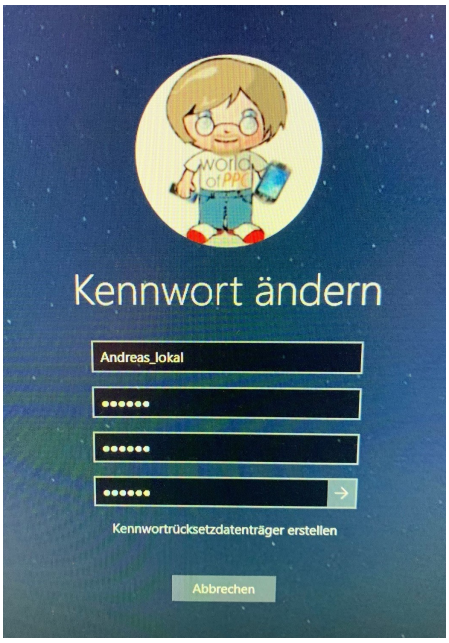
Wenn Sie den Wechsel zwischen den beiden Kontotypen vornehmen wollen, dann klicken Sie in den EINSTELLUNGEN von Windows 10 auf Konten, dann unter Ihrem Namen auf STATTDESSEN MIT EINEM LOKALEN KONTO ANMELDEN.



Geben Sie nun einen lokalen Benutzernamen ein (diese muss keine E-Mail-Adresse sein wie es beim Microsoft-Konto der Fall ist), dann ein Passwort für das neue Konto, das Sie dann noch einmal bestätigen müssen.

Zu guter Letzt können Sie noch einen Kennworthinweis eingeben, um sich besser an das Passwort erinnern zu können. Dieser sollte natürlich so kryptisch sein, dass er einem Fremden keinen Hinweis auf das tatsächliche Kennwort gibt.

Wenn Sie nun bei einem lokalen Konto das Passwort ändern wollen, dann drücken Sie gleichzeitig die Tasten **Strg, Alt** und **Entf**, und dann auf **Kennwort ändern**.



Der Prozess ist wieder derselbe: Geben Sie das alte und dann zweimal das neue Passwort ein, und schon haben Sie die Passwortänderung durchgeführt.

Wichtig

Während Sie bei der Anmeldung mit dem Microsoft-Konto ein vergessenes Passwort wiederherstellen können, ist der Prozess bei einem lokalen Konto leider nicht so einfach. Hier sind einige Eingriffe ins System nötig, die zeitaufwändig sind. Für den Notfall finden Sie durch eine Suche nach „Kennwort lokales Konto vergessen" diverse Anleitungen im Internet.

Es ist empfehlenswert, bei der Passwortänderung auf „Kennwortrücksetzdatenträger erstellen" zu klicken. Damit können Sie auf einem USB-Stick verschlüsselt Ihr Kennwort hinterlegen, um im Notfall damit die Passwortänderung ohne Eingabe des alten Passworts durchführen zu können. Diesen Datenträger sollten Sie allerdings wie Ihren Augapfel hüten: Was Sie können, kann auch derjenige, der den USB-Stick in seine Hände bekommen hat!

Windows Hello als komfortable Alternative

Den mangelnden Komfort einer Passworteingabe über die Tastatur hat Microsoft schon lange erkannt, nur gab es für den privaten Benutzer lange Zeit keine echte Alternative: Smartcards und andere Authentifizierungs-Hardware waren teuer und schwer zu bekommen.

Mit Windows 10 und dem Start der neueren Microsoft Surface Tablets- und Notebooks hat Microsoft mit **Windows Hello** eine neue Möglichkeit geschaffen, sich an einem Windows 10-PC anzumelden.

Allerdings setzt diese voraus, dass eine zusätzliche Hardware auf dem PC verfügbar ist.

1. **Eine 3D-Kamera:** Die Verwendung eines Kamerabildes des Benutzers zur Anmeldung ist theoretisch eine nette Idee. Sie ließe sich aber leicht überlisten, wenn ein Fremder einfach ein Bild aufnehmen, ausdrucken und dann vor die Kamera halten würde.

   Für Windows Hello ist deshalb eine spezielle Kamera nötig, die ein dreidimensionales Bild der Person aufnimmt, die sich gerade anmelden möchte, und dies mit der gespeicherten Version abgleicht. Hier ist eine Fälschung zwar nicht unmöglich, aber mit erheblichem Aufwand verbunden. Geeignete Kameras sind entweder direkt in den Geräten verbaut oder im Handel zu bekommen. Achten Sie darauf, dass eine Kompatibilität mit Windows Hello bei der Kamera explizit angegeben ist!

2. **Fingerabdruckscanner:** Es mutet schon ein wenig futuristisch an, ist aber mittlerweile Realität: Es gibt Sensoren, die den Fingerabdruck eines Menschen lesen und gegen einen gespeicherten Fingerabdruck abgleichen können. Auf dem Smartphone ist das nichts Neues mehr, auf dem PC wird es auch immer gebräuchlicher.

Um Windows Hello zu aktivieren, klicken Sie in den **Einstellungen** von Windows 10 auf **Konten**, dann auf **Anmeldeoptionen**. Windows 10 zeigt Ihnen nun alle zur Verfügung stehenden Möglichkeiten an. Die Liste variiert, abhängig davon, welche Sensoren in Ihr Gerät eingebaut sind.

Bei der ersten Einrichtung werden Sie aufgefordert, neben Ihrem Passwort eine PIN, also einen meist vierstelligen Zahlencode zu vergeben, wenn Sie dies vorher noch nicht getan haben. Dieser vereinfacht die Anmeldung, weil er schneller und fehlerfreier einzugeben ist als ein Passwort. Bei jeder Änderung der Einstellungen von Windows Hello muss diese PIN vorab eingegeben werden.

Wenn Sie bereits einmal die **GESICHTSERKENNUNG** durchgeführt haben, dann können Sie diese nur noch verbessern. Wobei „nur noch“ relativ

ist: Je häufiger Sie diesen Prozess wiederholen, desto genauer wird die Erkennung. Besonders für Brillenträger ist dies quasi schon ein Muss.

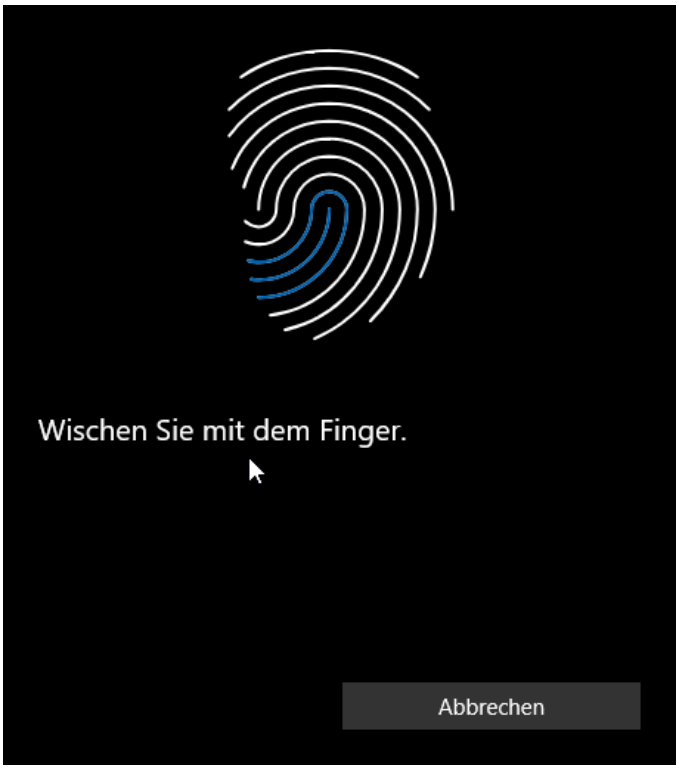
Tipp

Wenn Ihnen bei dem Gedanken unwohl ist, ein 3D-Modell Ihres Gesichts auf Ihrem Windows 10-PC gespeichert zu haben: Es wird kein echtes 3D-Modell erfasst und gespeichert. Eine Nachbildung des Gesichts ist anhand der – verschlüsselt! – gespeicherten Daten nicht möglich. Die gespeicherten Daten erlauben den Abgleich: Ist das aktuell vorhandene Gesicht identisch mit dem gespeicherten. Beim Fingerabdruck wird genauso vorgegangen.

Sie können es aber jederzeit in den Windows Hello-Einstellungen unter **Gesichtserkennung**, **Entfernen** aus dem Speicher des PCs löschen. Dies gilt natürlich auch für gespeicherte Fingerabdrücke!

Wenn Sie sich auf die Anmeldung per **FINGERABDRUCK** verlassen, dann sollten Sie die Erfassung gleich für mehrere Finger durchführen, indem Sie auf **WEITERE HINZUFÜGEN** klicken.

Es kann durchaus passieren, dass Sie sich einen Finger verletzen und dieser dann unter einem Pflaster oder Verband verborgen ist, sodass eine Erkennung des Fingerabdruckes nicht mehr möglich ist. Empfehlenswert ist daher das Erfassen und Speichern von jeweils zwei Fingern beider Hände. Wenn all diese Finger nicht mehr genutzt werden können, dann ist es fraglich, ob Sie Ihren PC zu diesem Zeitpunkt überhaupt noch nutzen können.

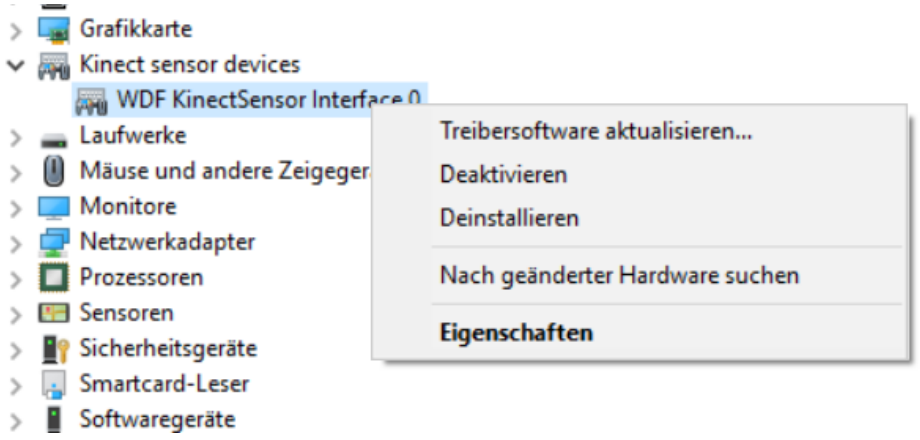


Microsoft Kinect als Windows Hello-Kamera

Die für Windows Hello nötige Hardware ist nicht günstig, wenn Sie sie separat anschaffen müssen. Wir haben aber eine Möglichkeit gefunden, wie Sie Ihren vielleicht bereits vorhandenen und nicht oder nur wenig genutzten Kinect-Sensor der XBOX One verwenden können. Interessant also nur für jene Windows-10-Benutzer, die auch eine Spielekonsole Xbox One betreiben.

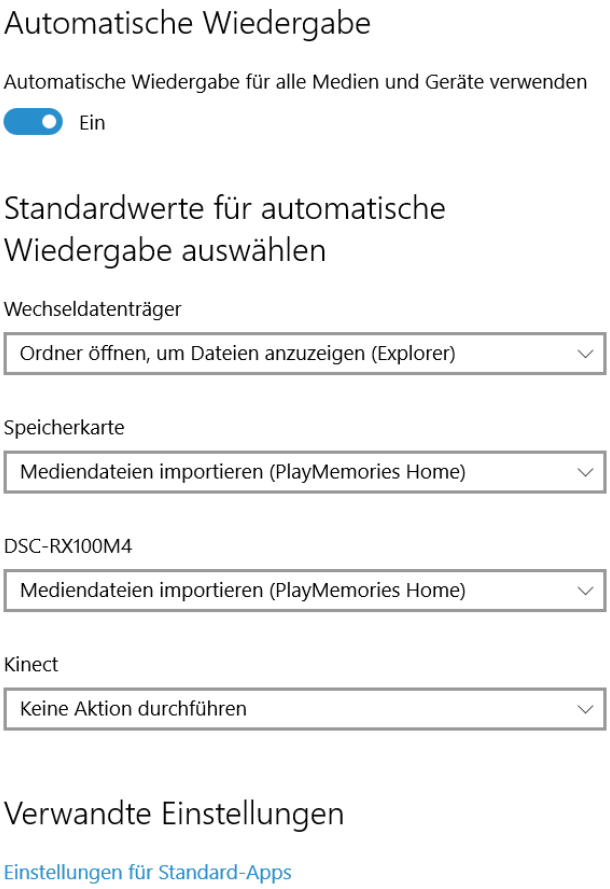
Um das Ganze ans Laufen zu bekommen, bedarf es einiger kleinerer Vorbereitungen. Zu allererst sollte das Kinect SDK v2.0 heruntergeladen und installiert werden, das kostenlos unter https://www.microsoft.com/en-us/download/details.aspx?id=44561 ier heruntergeladen werden kann.

Wenn Sie Kinect bereits an Ihrem PC genutzt haben und auf das Herbst Update (1809) aktualisiert haben, dann müssen sie den Treiber aktualisieren. Dazu klicken Sie **Kinect Sensor Devices**, dann auf das **WDF KinectSensor Interface**, rechte Maustaste und **Treibersoftware aktualisieren**. Im folgenden Menü müssen Sie dann anwählen, dass im Internet nach neuen Treibern gesucht werden soll.



Ein wenig nervig ist, dass Windows 10 bei jedem Anschließen des Kinect-Adapters meint, Sie wollten die App 3D Scan öffnen, weil diese als Standard für 3D-Kameras hinterlegt ist (und ganz nebenbei auch wunderbar den Kinect-Sensor verwenden kann, Gegenstände in 3D-Objekte umzuwandeln).

Dies können Sie vermeiden, wenn Sie über die Windows-Suche nach **Einstellungen für die automatische Wiedergabe** suchen und dann neben Kinect einfach **Keine Aktion Durchführen** auswählen.



Kinect wird nun wie eine interne Kamera für Windows Hello erkannt und kann wie eine solche verwendet werden.

Großartig dabei: Wenn bereits eine Erkennung eingerichtet wurde (weil das Gerät intern eine Hello-fähige Kamera hat, wie es beim Surface Book der Fall ist), dann werden die aufgenommenen Daten weiterverwendet und müssen nicht neu angelegt werden. Natürlich lässt sich die Erkennung weiter verbessern und somit die beiden Kameraquellen mischen!

Anmelden mit einem Hardware-Token

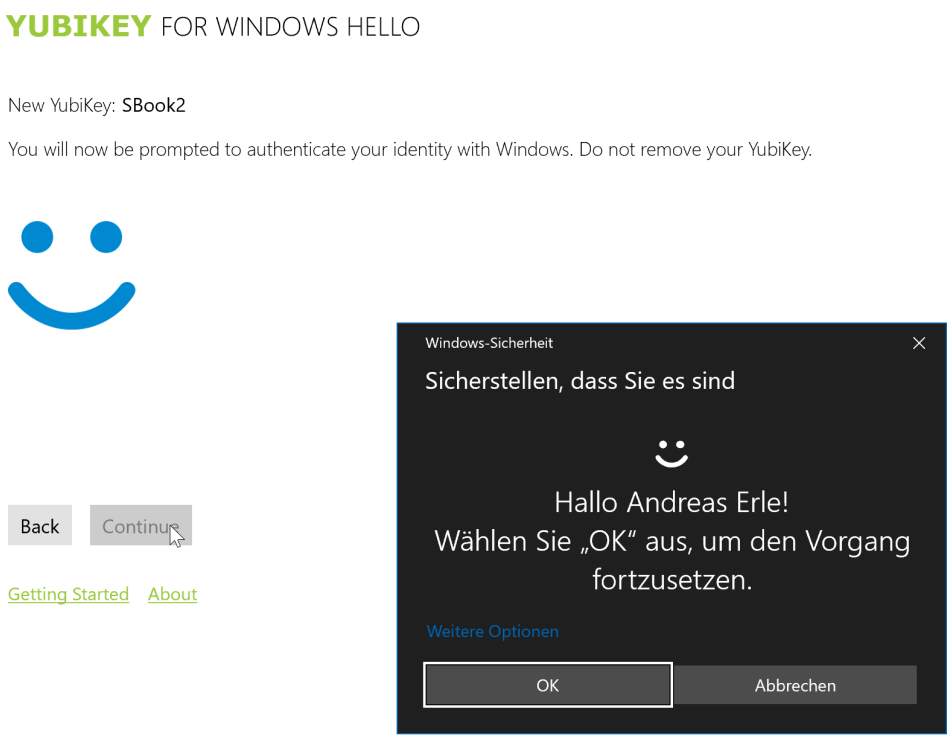
Eher unbekannt, aber durchaus charmant ist die Verwendung eines Hardware-Tokens. Eine Art Schlüssel, um den Rechner aufzuschließen. Solche Tokens sind schon für deutlich unter EUR 100,- zu bekommen.

Wo früher noch eine Smartcard oder ein großer USB-Stick nötig waren, hat die Miniaturisierung ebenfalls Einzug gehalten: Security Keys haben heute oft nur die Größe eines Fingernagels und können an einem normalen USB- oder sogar USB-C-Anschluss verwendet werden. Wichtig dabei: Windows 10 muss diese auch unterstützen!

Nicht viele Sicherheit-Tokens unterstützen auch die Anmeldung bei Windows 10 direkt. Yubicos Yubikeys (https://www.yubico.com/de/yubikeys/) erreichen dies durch eine

separate Windows Store-App, die dem Anmeldebildschirm von Windows 10 eine weitere Authentifizierungsmethode hinzufügt.

Einmal konfiguriert, wird der Anmeldebildschirm automatisch geschlossen, wenn das Token bei der Anmeldung eingelegt ist. Dannb ist keine Passworteingabe mehr erforderlich, denn die Berechtigung für die Anmeldung an Ihren PC ist mit der initialen Einrichtung auf dem Token abgelegt worden.



Die Zwei-Faktor-Authentifizierung

Die oben beschriebenen Tokens können unter anderem auch dazu verwendet werden, eine zweite Sicherheitsschicht zu bilden. So gut und sicher sie ein Passwort auch entwerfen und speichern, es besteht immer

noch die latente Gefahr, dass es jemand in Erfahrung bringt und verwenden kann.

Die Idee der Zwei-Faktor-Authentifizierung (abgekürzt 2FA) ist die folgende: Wenn Sie sich mit dem Passwort angemeldet haben, wird noch ein weiteres Authentifizierungsmerkmal angefordert. Das kann ein Hardware-Token (wie oben beschrieben) sein. Häufig ist es aber ein separater zweiter Code. Eine meist 6-stellige Nummer, die durch einen Generator erzeugt wird – und sich alle paar Sekunden ändert.

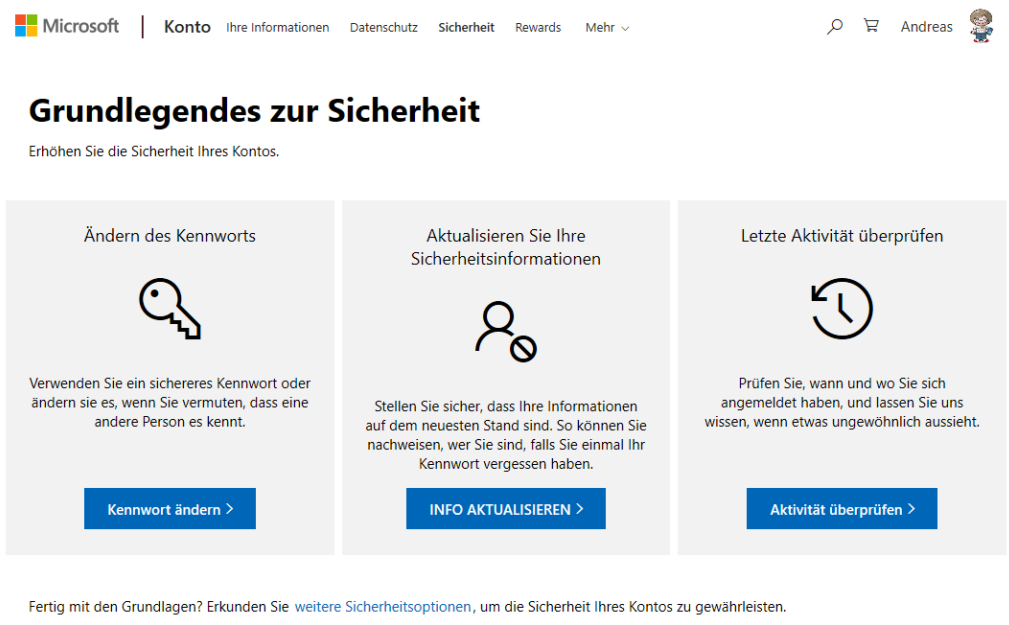
Nur wer das Kennwort des Kontos uns gleichzeitig die aktuelle Nummer hat, der kann sich anmelden. Dem Unberechtigten wird – wenn der das Passwort entwendet hat – die zweite Nummer fehlen, und eine Anmeldung ist nicht nötig.

Microsoft stellt die Zwei-Faktor-Authentifizierung für die eigenen Online-Konten zur Verfügung. Statt eines Hardware-Schlüssels verwendet man einfach das, was Sie (fast) immer im Zugriff haben: Ihr Smartphone.

Aktivieren der Zwei-Faktor-Authentifizierung

Keine Frage: Ein zusätzlicher Schritt bei der Anmeldung bedeutet gleichzeitig, dass Sie länger für selbige brauchen, aus diesem Grund ist die Zwei-Faktor-Authentifizierung auch im Standard deaktiviert.

Um sie für Ihr Microsoft-Konto zu aktivieren, wechseln Sie zur Microsoft Konto-Sicherheitsseite https://account.microsoft.com/security und melden sich mit Ihrer E-Mail-Adresse und Ihrem Passwort an.

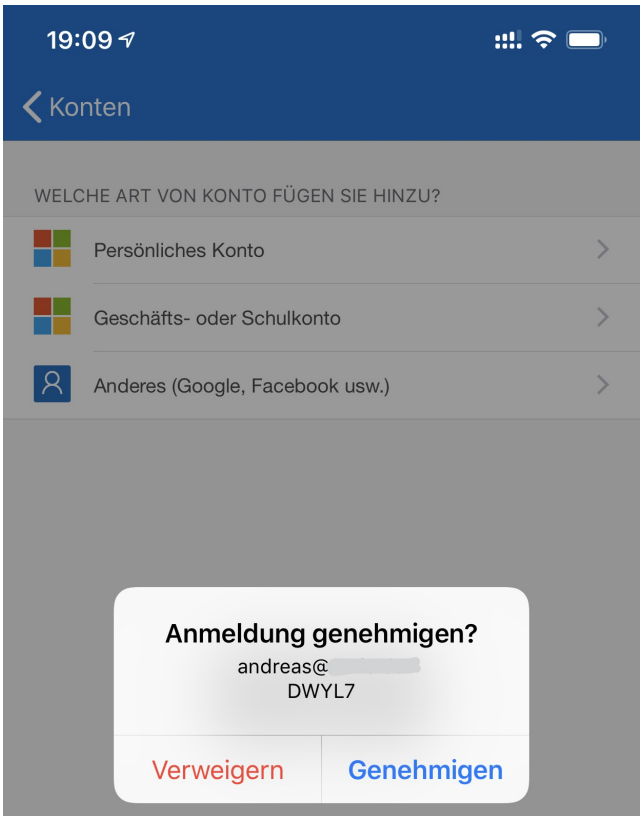


Klicken Sie dann auf **WEITERE SICHERHEITSOPTIONEN** am unteren Rand der Seite und auf **ZWEISTUFIGE ÜBERPRÜFUNG EINRICHTEN**. Sie werden nun durch die Einrichtung geführt.

An deren Ende empfiehlt Ihnen Microsoft den Download der eigenen „Authenticator"-App. Diese finden Sie kostenlos im App Store (für iOS-Geräte) oder im Google Play Store (für Android-Geräte).

Fügen Sie Ihr Microsoft-Konto durch Tippen auf das Plus-Zeichen hinzu und melden Sie sich mit Ihrer E-Mail-Adresse und dem Passwort an.

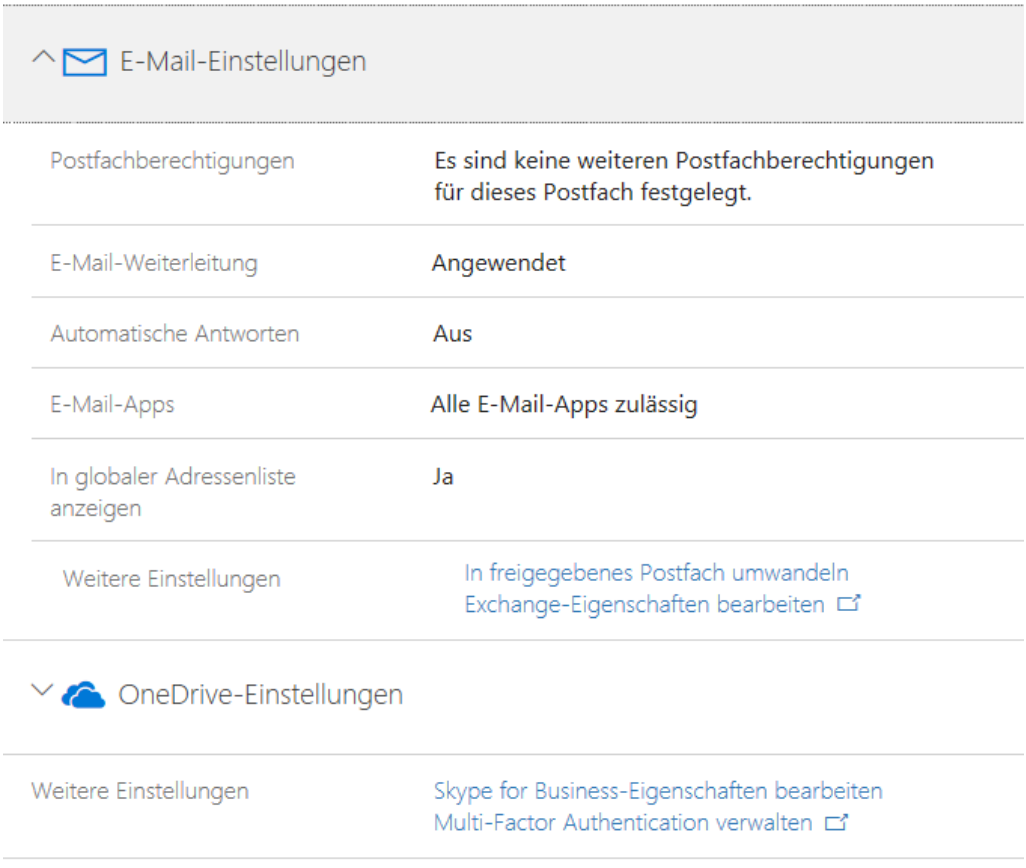
Nachdem der Vorgang erfolgreich abgeschlossen wurde, bekommen Sie – soweit Sie in der App einmal auf Nachfrage die Berechtigung erteilen, Push-Nachrichten zu versenden – bei jeder Anmeldung am Konto die Anforderung auf dem Smartphone, diese zu genehmigen.



Bei Smartphones mit biometrischem Zugangsschutz wie einem Fingerabdrucksensor oder einer 3D-Kamera muss die Genehmigung

selbst dann sogar noch darüber freigegeben werden. Mehr Schutz geht (für den Privatanwender) kaum!

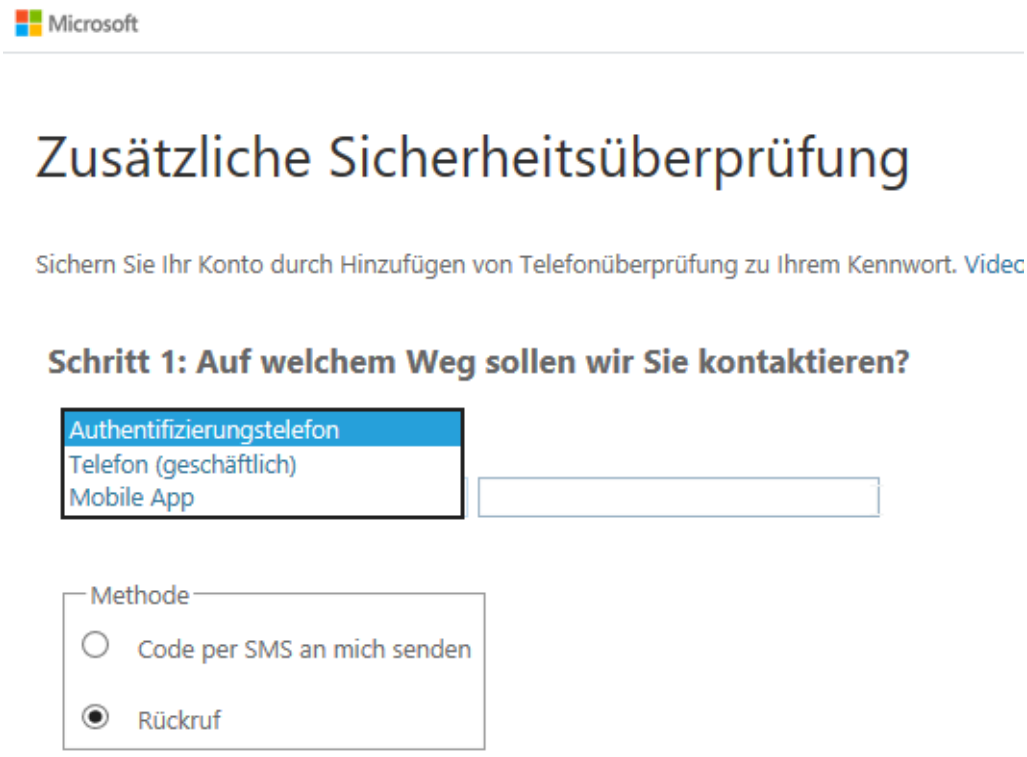
Bei Office 365 ist die Aktivierung ein wenig anders: Melden Sie sich als Administrator an Office 365 an und gehen Sie dann auf **Benutzer**, klicken Sie den Benutzer an, der die Zwei-Faktor-Authentifizierung bekommen soll. Ganz unten auf der Seite finden sie unter **Weitere Einstellungen** den Link zu **Multi-Factor Authentication verwenden**.



Rechts auf dem Bildschirm finden Sie dann den Link zum **Aktivieren** der Einstellung. Damit ist die Zwei-Faktor-Authentifizierung eingerichtet, aber nicht aktiviert. Im Gegensatz zum „normalen" Microsoft-Konto kann bei Office 365 neben der Authenticator-App auch ein Anruf oder

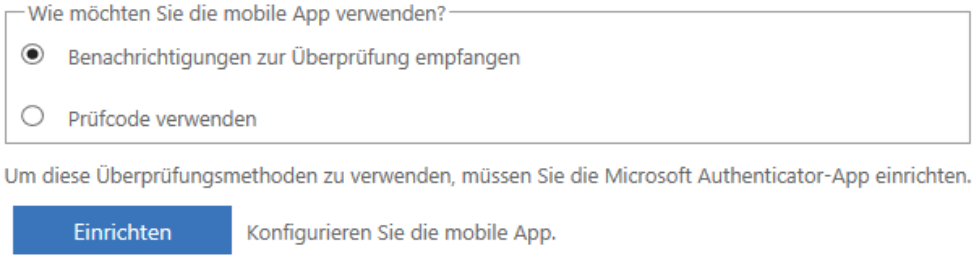
eine SMS als zweiter Faktor verwendet werden, sie Auswahl liegt dann beim Benutzer selbst.

Bei der ersten Anmeldung des Benutzers meldet Office 365 dann auch, dass noch weitere Informationen nötig sind. Klicken Sie dann einfach auf **Weiter**.

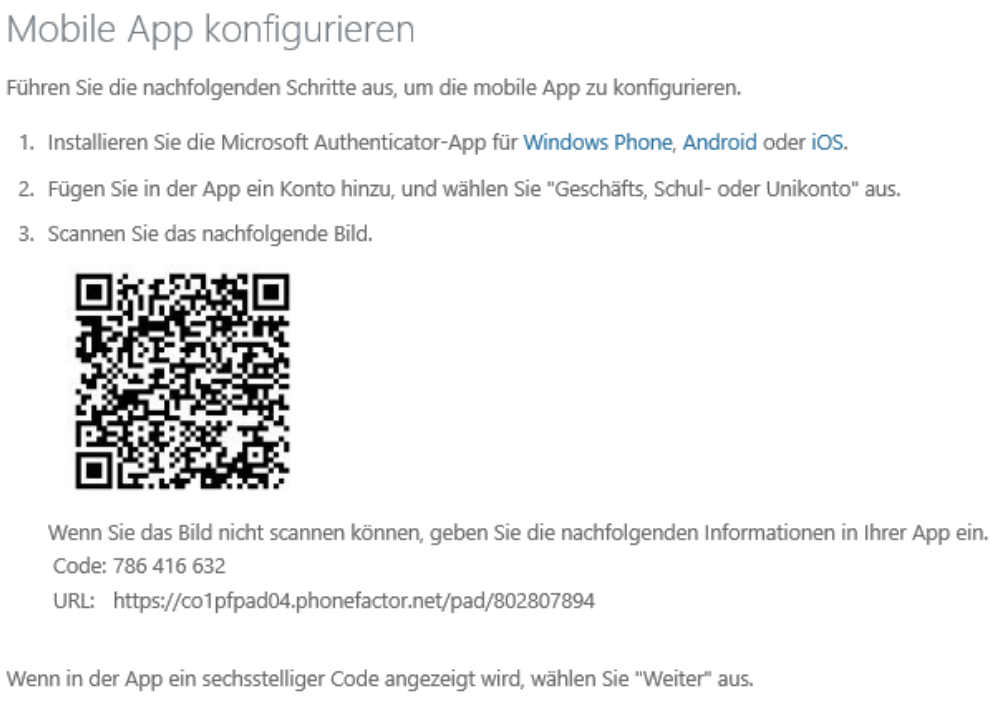


Im folgenden Dialog können Sie auswählen, ob Sie telefonisch kontaktiert werden möchten (dazu müssen Sie dann Ländervorwahl und Rufnummer eingeben) oder die oben schon beschriebene **Mobile App**.

Wählen Sie diese Option aus. Sie müssen sich nun entscheiden, ob sie immer einen **Prüfcode** (den die App Ihnen dann anzeigt) eingeben möchten oder über eine **Push-Benachrichtigung** die Anmeldung bestätigen möchten.



Die zweite Variante ist hier die deutlich komfortablere, weil sie nur einen Klick erfordert statt der Eingabe einer Ziffernkette. Klicken Sie dann auf **Einrichten**. Im Gegensatz zur Authentifizierung eines Microsoft-Kontos müssen Sie sie beim Hinzufügen in der Authenticator-App nicht mit Ihren Zugangsdaten anmelden, sondern benötigen einen Code und eine Web-Adresse, die die Webseite Ihnen nun unter dem QR-Code anzeigt.



In der Authenticator-App tippen Sie auf das **+**, um ein neues Konto anzulegen, und dann auf **Geschäfts- oder Schulkonto**. Geben Sie nun

Code und URL aus der Admin-Oberfläche von Office 365 ein und klicken Sie auf **Weiter**. Die App und Ihr Office 365-Konto synchronisieren sich nun miteinander. Bei jeder Anmeldung an Ihr Konto müssen Sie nun neben dem Passwort auch noch (je nach Konfiguration) einen Code eingeben oder die Anmeldung über Ihr Handy bestätigen.

Sicherheit der Datenträger: Bitlocker

Nun haben Sie eine Menge an Zeit und Hirnschmalz in die Absicherung Ihres Windows 10-Systems investiert. Die schlechte Nachricht: Das hilft Ihnen wenig, wenn Ihr PC (oder die Festplatte darin) gestohlen werden. In ein geeignetes Festplattengehäuse eingebaut kann der Dieb dann potentiell Ihre Festplatte an seinen PC anschließen und auf die Daten darauf zugreifen.

Die gute Nachricht: Mit Bitlocker ist 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.

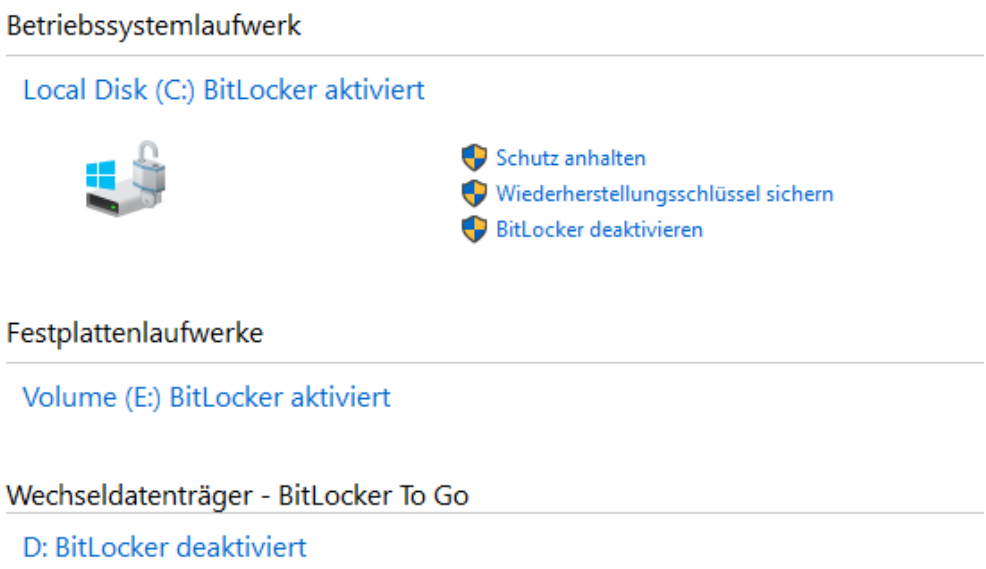
Wird die Festplatte entnommen und in einen anderen Rechner eingebaut, dann hat dieser einen anderen Schlüssel und kann die Daten

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 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**).

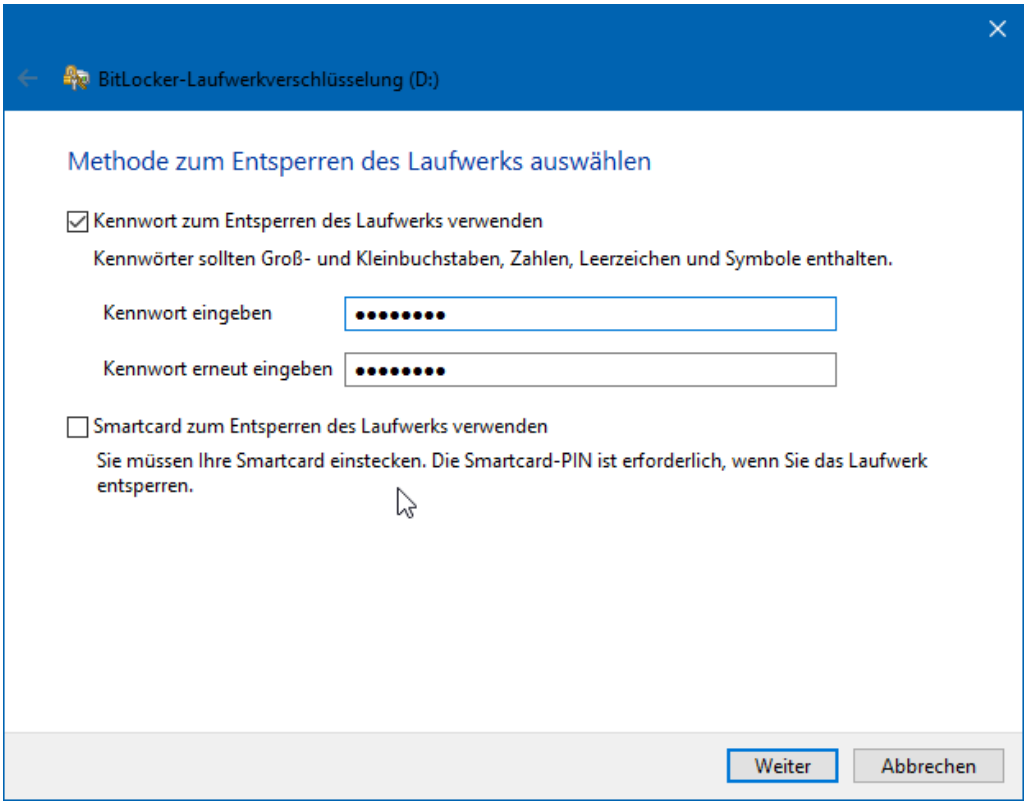
Folgen Sie nun den Anweisungen auf dem Bildschirm, um Bitlocker zu aktivieren. Im normalen Betrieb werden Sie hier keine Unterschiede erkennen. Die Festplatte ist nicht spürbar langsamer und Sie müssen auch beim Systemstart kein zusätzliches Kennwort eingeben. Letzteres übernimmt hier das TPM-Modul im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



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.

Wiederherstellung verschlüsselter Festplatten

„Eigentlich" sollte der Ottonormalanwender gar nicht damit konfrontiert werden, aber „eigentlich" ist bekanntermaßen der beste Freund von „fast", und so kommt es unter anderem manchmal bei der Installation eines BIOS-Updates zu folgender Situation: Windows 10 erkennt eine Veränderung der Hardware eines Notebooks oder Tablets und fordert den Anwender auf, den Recovery Key für die Festplattenverschlüsselung Bitlocker einzugeben.

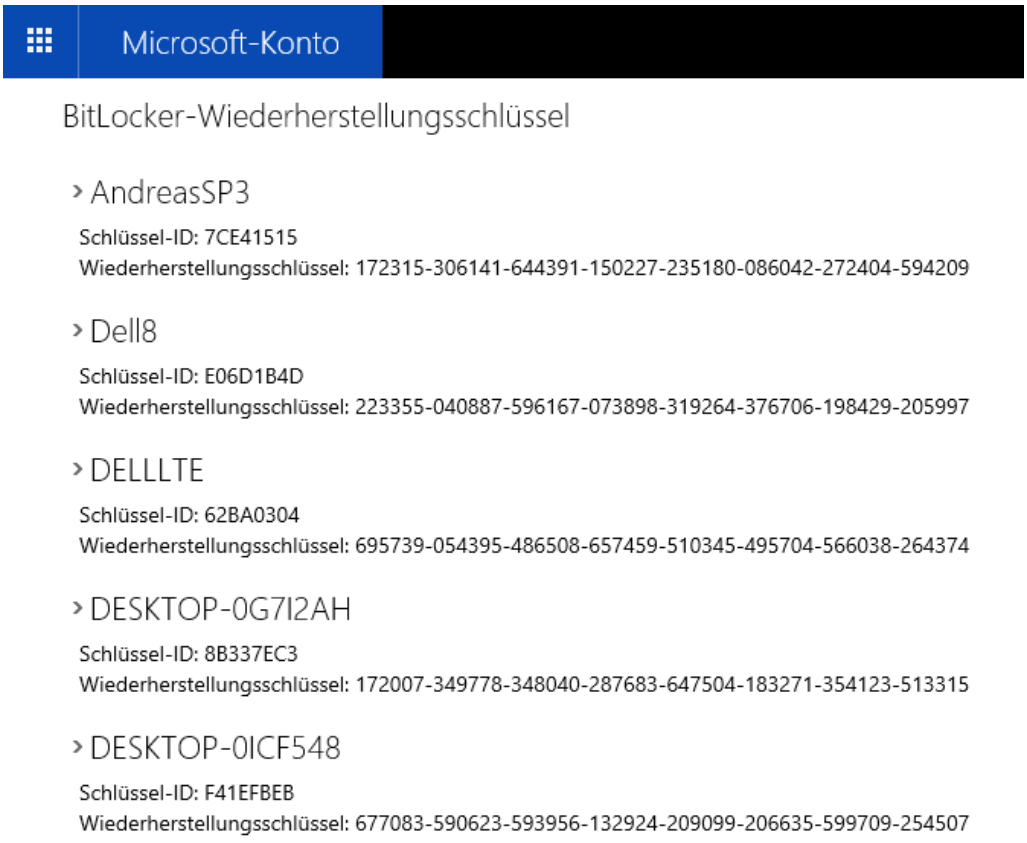
Erst nach erfolgreicher Eingabe wird die Festplatte freigegeben und Windows kann starten. Nun macht sich der Normalanwender meist wenig Gedanken über seine Festplattenverschlüsselung, im schlimmsten Fall ist er sich derer nicht einmal bewusst. In der Folge existieren auch keine Sicherheitskopien der Schlüssel auf einem USB-Stick, die hier zu verwenden wären.

Microsoft hat dieses Problem in der Vergangenheit bereits erkannt und speichert die Schlüssel automatisch auf dem OneDrive, dass zum Microsoft-Konto auf dem Gerät gehört. Es bleibt dem geschockten Anwender nicht viel mehr übrig, als sich einen anderen PC oder Tablet zu suchen und dort **https://onedrive.live.com/recoverykey** aufzurufen.

Wichtig Die URL, die Windows selber anzeigt, ist manchmal nicht mehr gültig und führt auf das Hauptverzeichnis des OneDrives, zeigt aber nicht die Wiederherstellungsschlüssel an. Verwenden sie also

die oben angegebene Adresse durch manuelle Eingabe in die Adresszeile des Browsers!

Der Bitlocker-Dialog zeigt auf dem betroffenen Gerät dessen Kennung an, die sich in der Liste auf dem OneDrive findet. Diese muss eingegeben werden und damit die Festplatte wieder freigeschaltet.



Noch mehr Sicherheit für Windows 10

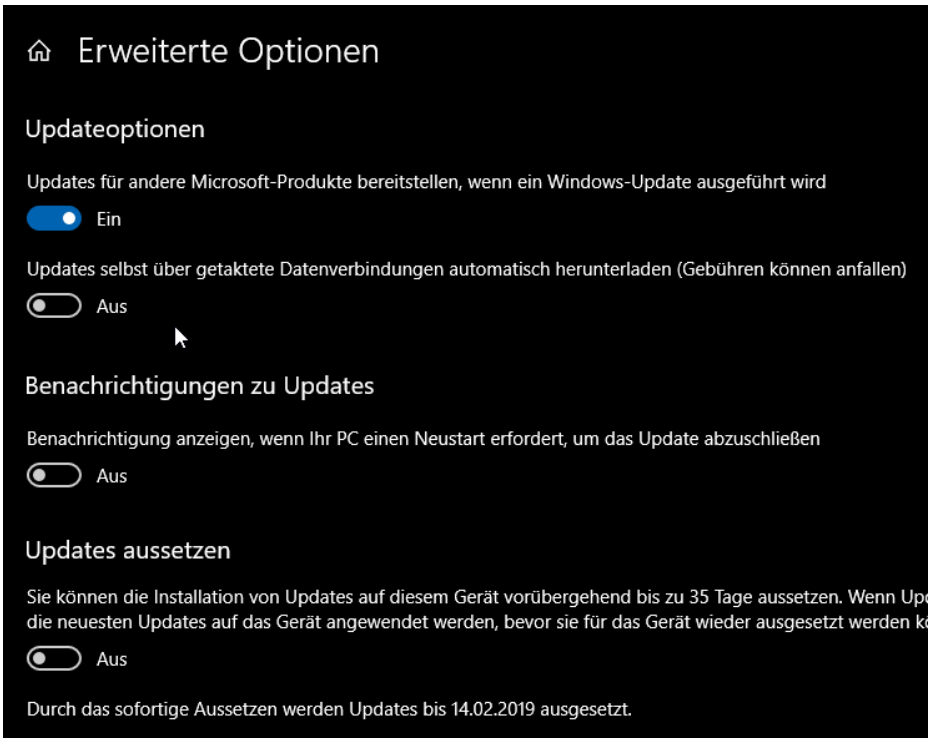
Windows 10 bietet schon bei der Installation die Möglichkeit, eine Menge an automatischer Kommunikation auszuschalten, bei der Daten Ihres Rechners an Microsoft übertragen werden. Wenn Sie also noch die Chance haben, dann wählen Sie immer die **EXPRESS-EINSTELLUNGEN**, bei denen die Voreinstellungen so gemacht werden, wie es aus Sicht von Microsoft Sinn macht, sondern **EINSTELLUNGEN ANPASSEN**.

Damit wird Ihnen vor der physischen Windows 10-Installation eine Vielzahl von Auswahlmöglichkeiten gegeben, bei denen Sie detailliert bestimmen können, welche Einstellungen Sie möchten.

Aber auch bei einer bestehenden Windows-Installation haben Sie noch eine Menge Möglichkeiten einzugreifen!

Automatische Updates aktivieren – aber richtig

Updates sind bei einem komplexen Produkt wie Windows 10 das Salz in der Suppe. Nicht wegen der neuen Features, die Windows produktiver machen, sondern vor allem wegen der kontinuierlich ausgerollten Fehlerbehebungen. Viele Sicherheitsvorfälle hätten sich vermeiden lassen, wenn die betroffenen Systeme „auf dem aktuellen Patchlevel“ (sprich: mit den aktuellsten Updates versehen) gewesen wären.



Die hat Microsoft erkannt und sich mit Windows 10 aktiv gegen die Update-Muffel positioniert. Die automatischen Updates lassen sich nur kurzfristig pausieren, nicht aber mehr komplett deaktivieren.

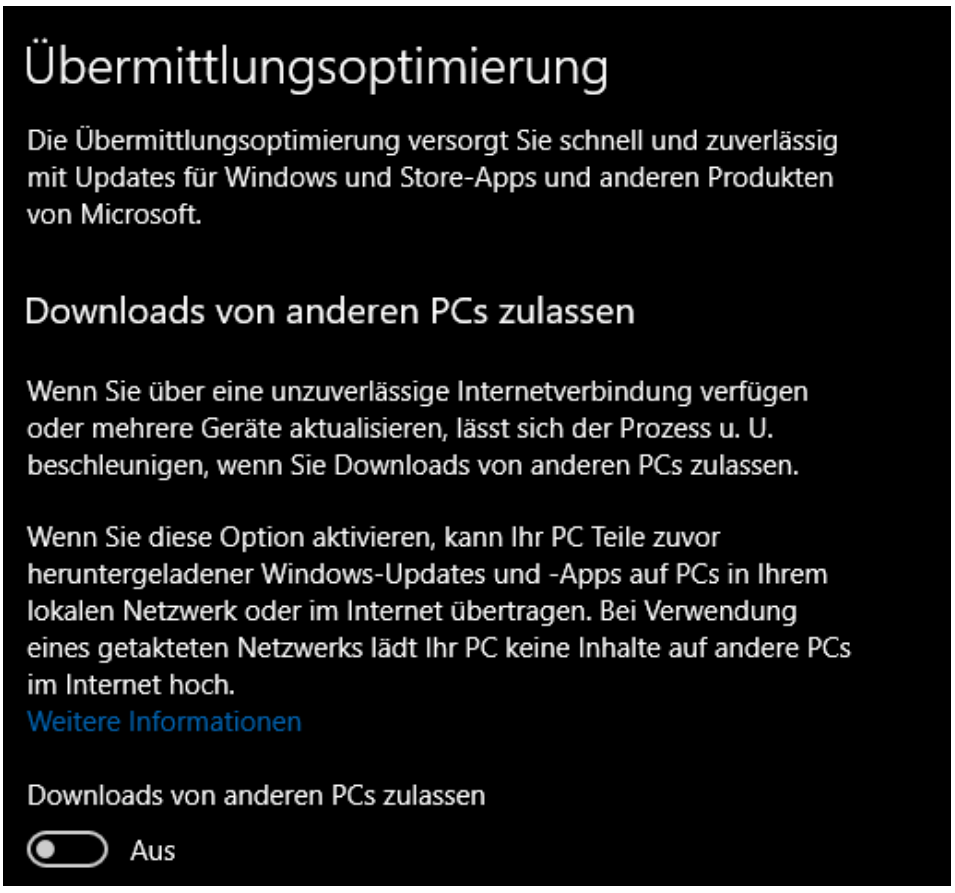
Unter Einstellungen, Updates und Sicherheit können Sie manuell nach Updates suchen. Stellen Sie hier sicher, dass die Option **Updates für andere Microsoft-Produkte bereitstellen** aktiviert ist. Damit stellen Sie sicher, dass die automatische Aktualisierung nicht nur für Windows 10, sondern auch für die Office Apps und andere Microsoft-Programme automatisch heruntergeladen und installiert werden. Auch diese können Sicherheitslücken haben, die durch ein Update behoben werden und damit die Sicherheit des Systems erhöhen.

Kontrollieren Sie ebenfalls, dass Updates aussetzen nur dann eingeschaltet ist, wenn Sie einen echten Grund dazu haben,

beispielsweise, weil eine Inkompatibilität zwischen einem Update und der von Ihnen verwendeten Hardware bekannt ist!

Eine weniger bekannte Einstellung der Windows 10-Updates ist die Möglichkeit, über das eigene Netzwerk bereits auf einem Gerät heruntergeladene Updates oder Teile davon für andere Geräte zur Verfügung zu stellen.

Das ist grundsätzlich eine nette Idee, macht allerdings Ihren PC dann automatisch zum Update-Server im Netzwerk. Im Falle einer Infektion kann dies theoretisch dazu führen, dass Schadsoftware über das Netzwerk verteilt werden kann. Es empfiehlt sich also, die Option **Downloads von anderen PCs zulassen** auszuschalten.



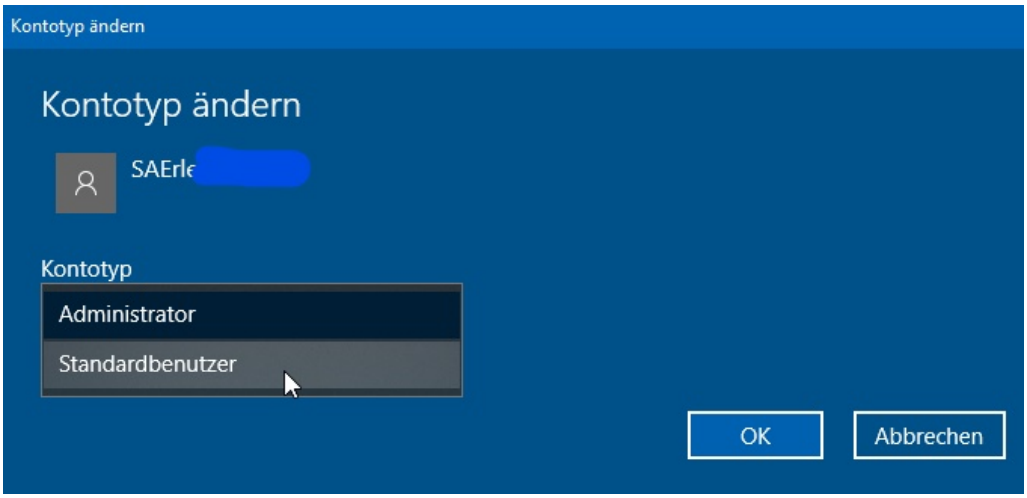
Weniger Rechte sind mehr

Keine Frage: Je mehr Rechte man als Benutzer hat, desto besser kann man arbeiten. Zumindest glauben das viele Anwender. Allerdings hat das auch Risiken: Wer als Administrator, der für normale Installationen standardmäßig verwendeten Rolle unterwegs ist, der gibt Schadsoftware natürlich auch alle Möglichkeiten der Systemänderungen, die ein Administrator hat.

Das ist vor allem auch beim Surfen im Internet ein Risiko, auch beim versehentlichen Öffnen einer virenbefallenen E-Mail, die der Virenscanner nicht erkennt, was sich leicht vermeiden lässt:

Wechseln Sie wie vorhin beschrieben auf ein lokales Konto und geben Sie diesem nur Benutzer- aber keine Administrationsberechtigungen. Das können Sie unter den Windows 10-Einstellungen durch Klick auf **Konten**, **Familie und andere Benutzer**, dann einen Klick auf den Benutzer erreichen.

Wählen Sie unter **Kontotyp** einfach **Standardbenutzer**, um dem Benutzer die Administrationsrechte zu nehmen. Melden Sie sich dann mit dem Standardbenutzer an. Bei jeder Änderung, die Administrationsrechte erfordert, muss diese dann durch Anmeldung eines Administrators freigegeben werden.



Im laufenden System wird dies eher selten vorkommen, insofern beeinträchtigt das Ihre Arbeit nicht. Die explizite Freigabe aber sensibilisiert Sie zu überlegen, ob die Änderung tatsächlich gewollt ist oder vielleicht tatsächlich durch Schadsoftware ausgelöst wird.