So geht's leichter...

10 häufige Gefahren abwehren

- Schutz vor Spam, Viren&Würmer
- Phishing vermeiden
- Abhören vermeiden: VPNs helfen
- Schutz vor Datenverlust

Autoren:
Jörg Schieb
Andreas Erle

So geht's leichter | Zehn Gefahren vermeiden/abwehren

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

So geht's leichter | Zehn Gefahren vermeiden/abwehren

Inhalt

So geht's leichter | Zehn Gefahren vermeiden/abwehren

So geht's leichter | Zehn Gefahren vermeiden/abwehren

So geht's leichter | Zehn Gefahren vermeiden/abwehren

Die Arbeit an PC, Tablet und Smartphone ist Ihr tägliches Brot. Normalerweise läuft alles wie geschmiert und Sie haben keine Probleme. Trotzdem bleibt ein mulmiges Gefühl: Was, wenn etwas schiefgeht und Sie dringend arbeiten müssen? Plötzlich Ihr Rechner nur noch schleicht statt rennt, Sie nicht mehr an Ihre Daten kommen oder gar der ganze Rechner nicht mehr verfügbar ist?

Sie können nicht alle Eventualitäten berücksichtigen. Die größten Probleme aber können Sie schon im Vorfeld verhindern oder direkt nach Auftreten lösen.

In diesem Report zeigen wir Ihnen, wie Sie sich vor Schadsoftware und Ausspähungsversuchen schützen, wie Sie den Verlust von Passwörtern, Daten und ganzen Geräten schützen können und so ein deutlich sichereres Gefühl bekommen!

Schutz vor SPAM und Mailverlust

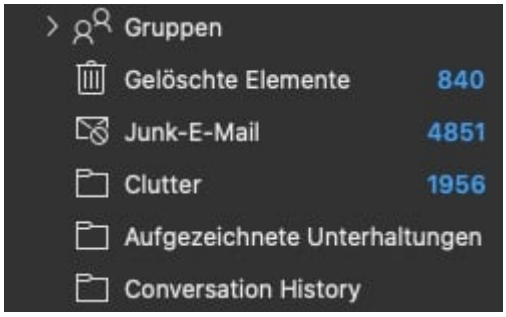
SPAM ist ein riesiges Ärgernis. Neben den wirklich an Sie gerichteten und von Ihnen erwarteten E-Mails erhalten Sie am Tag oft deutlich mehr

So geht's leichter | Zehn Gefahren vermeiden/abwehren

E-Mails, deren Herkunft und Bedeutung Ihnen nicht klar wird. Oft sind es Werbe-Emails, die blind an Tausende von Adressen geschickt werden. Manchmal auch Newsletter, die Sie irgendwann einmal abonniert haben, aber gar nicht lesen. Gemein haben SPAM-Mails eines: Sie stören und nehmen Platz weg. Ihr E-Mail-Anbieter und auch Ihre bevorzugte E-Mail-Software reagieren darauf, indem sie versuchen, Mails schon vorab als SPAM zu identifizieren und weg zu sortieren. Das funktioniert oft, aber zumindest am Anfang nicht ohne Fehler. Greifen Sie ein und Verbessern Sie die Erkennung!

Junk und Clutter optimieren

Alle E-Mail-Programme und -Anbieter haben eigene Die Namen der SPAM-Ordner unterscheiden sich zwischen unterschiedlichen Mail-Anbietern und E-Mail-Programmen. Outlook bietet eine zweischichtige Klassifizierung: Die **Junk-Emails** sind die wirklichen SPAM-E-Mails, **Clutter** sind die E-Mails, die Outlook anhand Ihres Nutzungsverhaltens als "für Sie nicht wichtig" klassifiziert. In Ihrem Outlook-Fenster finden Sie für beide **Kategorien** einen eigenen Ordner.



Bei Clutter können Sie eine E-Mail einfach wieder aus dem Ordner in den Posteingang schieben. Outlook lernt dazu und wird ähnliche Mails in der Zukunft nicht mehr in Clutter ablegen. Geben Sie Outlook ein wenig Zeit, manchmal braucht es mehrere Anläufe!

Bei Junk-E-Mails ist es einfacher: Ist eine E-Mail SPAM und landet im Posteingang, dann klicken Sie mit der rechten Maustaste darauf und Wählen Sie **Junk-E-Mail** > **Als Junk-E-Mail markieren**. Andersherum

So geht's leichter | Zehn Gefahren vermeiden/abwehren

funktioniert es ebenso: Klicken Sie eine fälschlich als SPAM einsortierte E-Mail mit der rechten Maustaste an und **Junk-E-Mail** > **Junk-E-Mail-Markierung aufheben**. Auch hier lernt Outlook (wie auch diverse andere Mail-Programme) hinzu. Die Erkennung verbessert sich kontinuierlich.

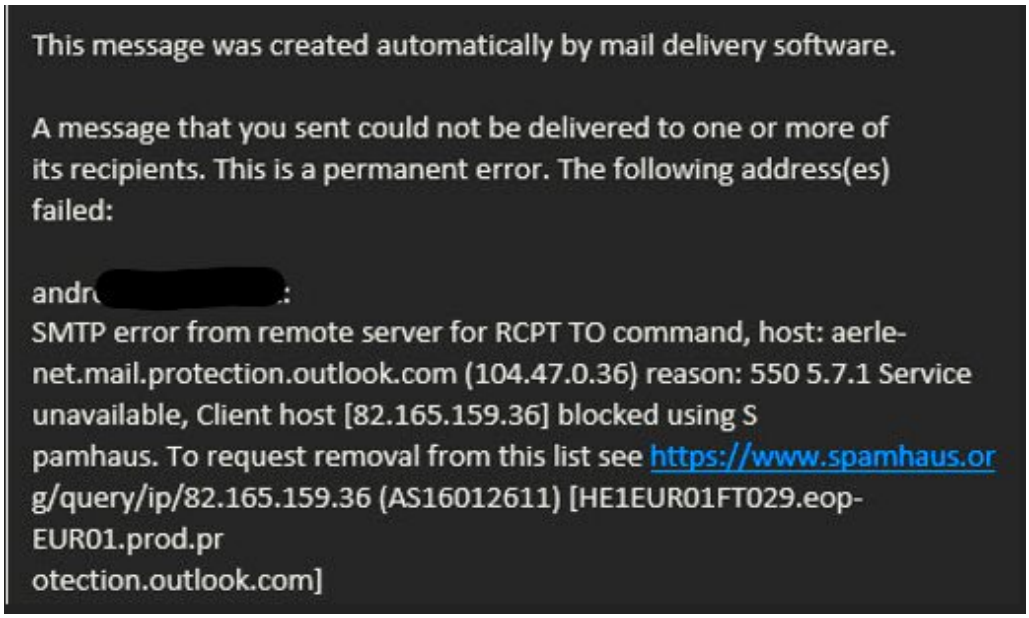
Wenn Ihre Mails als SPAM eingeordnet werden

Die SPAM-Behandlung auf dem eigenen PC ist hilfreich, weil Sie Ihnen eine Menge an Kontrolle gibt. Die Mail-Anbieter selbst plagt aber eine ganz anderes Problem: SPAM kommt ja irgendwo her. Meist von verseuchten Rechnern, die Zehntausende E-Mails in einem Rutsch verschicken. Ist das der Fall, dann wird ein Mailserver schnell gesperrt. Auch wenn nicht nur der Spammer, sondern auch normale Anwender ihn nutzt.

Die Folge: Mails dieses Servers werden einfach blockiert, bevor sie überhaupt in Ihr Postfach gelangen. Der Briefträger bekommt die Werbung gar nicht zur Zustellung. Stattdessen wird sie bereits im Verteilzentrum weggeworfen.

Das hat Auswirkungen in zwei Richtungen: Sie erhalten bestimmte E-Mails nicht mehr. Vermeintlich im Recht beschweren Sie sich dann beim Absender. Der aber kann das nicht nachvollziehen. Im besten Fall bekommt er eine Fehlermeldung, oft aber gar keine Information. Ein schon länger existierendes Problem beispielsweise besteht zwischen Microsofts Outlook und T-Online. Outlook erkennt Mailserver von T-Online als SPAM-Schleudern und blockiert diese. Die betroffenen Anwender wundern sich über ausbleibende E-Mails. Beide Unternehmen allerdings lassen wenig Motivation erkennen, das Problem zu lösen. Der Leidtragende ist einmal mehr der Anwender.

So geht's leichter | Zehn Gefahren vermeiden/abwehren


This message was created automatically by mail delivery software.

A message that you sent could not be delivered to one or more of its recipients. This is a permanent error. The following address(es) failed:

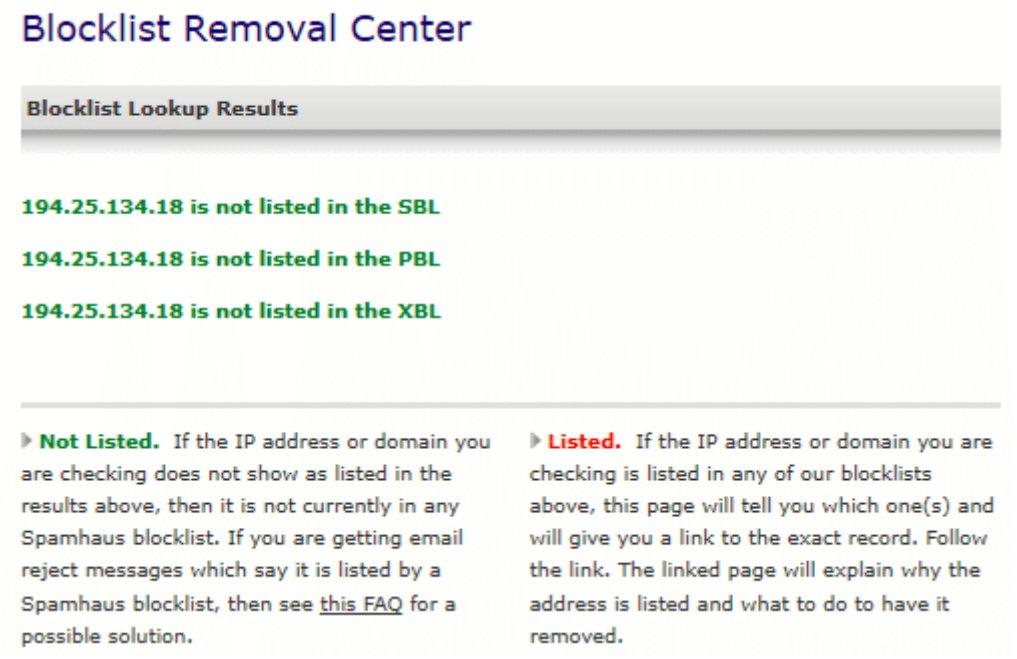
andr[redacted]:
SMTP error from remote server for RCPT TO command, host: aerle-net.mail.protection.outlook.com (104.47.0.36) reason: 550 5.7.1 Service unavailable, Client host [82.165.159.36] blocked using S
pamhaus. To request removal from this list see https://www.spamhaus.org/query/ip/82.165.159.36 (AS16012611) [HE1EUR01FT029.eop-EUR01.prod.pr
otection.outlook.com]

Gerade beim automatisierten E-Mail-Versand erkennen die versendenden Systeme, dass wiederholte Fehler auftreten. Nach einer gewissen Zeit entfernen sie die betroffenen E-Mail-Adressen automatisch. Wenn die Blockade des Mailservers dann irgendwann aufgehoben ist, sind Sie automatisch aus dem Verteiler rausgefallen.

Wir versuchen Ihnen immer gleich die Lösungen mitzuliefern. In diesem Fall aber haben Sie als Empfänger leider keine Einflussmöglichkeit.

Immerhin eine Möglichkeit zur Identifikation des Problems können wir Ihnen bieten: Es gibt verschiedene Anbieter von SPAM-Blockierungs-Listen, einer davon ist SPAMHaus.org. Dort können Sie den Namen oder die IP Ihres Mailservers eingeben. Sie bekommen dann die Information, ob dieser gesperrt ist. Ist das der Fall, dann können Sie über das Meldeformular einen Antrag auf Entsperren stellen. Ob und wann eine Reaktion darauf erfolgt, ist vollkommen ungewiss.

So geht's leichter | Zehn Gefahren vermeiden/abwehren



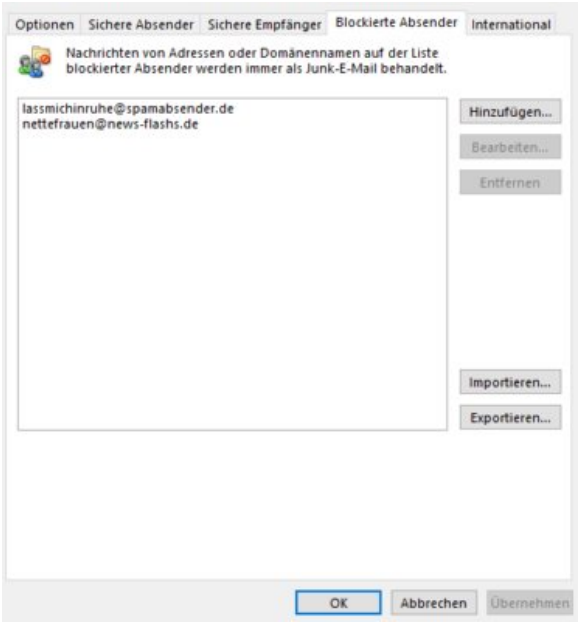
Verwenden von SPAM-Listen

Der Aufbau einer eigenen Liste unerwünschter (oder erwünschter) Absender ist eine mühsame Angelegenheit, zumal es keine wirklichen Anbieter dieser Listen gibt: Dienste, die Mails gegen eigene Absenderlisten abgleichen, lassen sich gut bezahlen. Zumindest im Freundes- und Bekanntenkreis können Sie aber mit einem kleinen Trick Ihre SPAM-Adresslisten austauschen!

Klicken Sie der rechten Maustaste auf eine beliebige E-Mail und dann auf **Junk-E-Mail** > **Junk-E-Mail-Optionen**. Je nach der Liste, die Sie bekommen haben oder weitergeben möchten, klicken Sie auf **Sichere Absender** oder **Blockierte Absender** (letzteres ist hier die sinnvollere Wahl, denn Spammer treffen die meisten Anwender gleichermaßen, während jeder Anwender unterschiedliche "sichere" Absender haben wird).

So geht's leichter | Zehn Gefahren vermeiden/abwehren

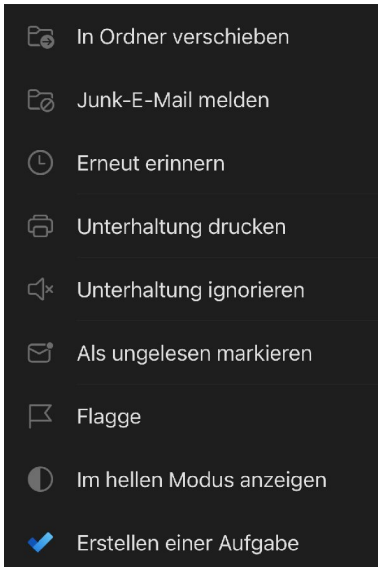
Klicken Sie nun auf **Exportieren**, um Ihre Liste der Absender in eine Textdatei exportieren zu können. diese Datei können Sie per E-Mail oder auf einem USB-Stick an Bekannte weitergeben, wenn Sie das möchten. Wenn Sie eine Liste bekommen haben, die Sie importieren wollen, dann klicken Sie auf **Importieren**.



Dieses Vorgehen kann Ihnen auch helfen, wenn Sie Ihr E-Mail-Postfach wechseln und das neue schon von Anfang an schützen wollen.

SPAM auf dem Smartphone?

Ihr Postfach lernt, und die Erkenntnisse, welche E-Mails Sie als SPAM ansehen, werden auf den Server übertragen. Damit werden E-Mails schon vorab in die entsprechenden Ordner geschoben. Auf dem Smartphone kommt also genau so viel oder so wenig SPAM an wie auf dem PC.



Trotzdem bieten die meisten mobilen E-Mails Apps die Möglichkeit, SPAM zu melden. Dazu halten Sie den Finger auf die entsprechende E-Mail, dann tippen Sie auf die drei Punkte (iOS wie auch Android) und wählen Sie **Junk-E-Mail melden** (je nach App kann die Option leicht anders heißen).

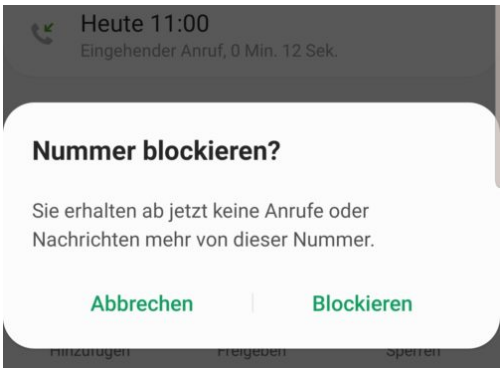
So geht's leichter | Zehn Gefahren vermeiden/abwehren

Auf dem Smartphone kommen dann noch die SPAM-Anrufe hinzu: Ihr Handy klingelt immer um ungünstigsten Zeitpunkt. Gerade bei einer unbekannten Nummer sind Sie eher bereit, trotzdem dran zu gehen, es könnte ja etwas Wichtiges sein. Und dann ist es der fünfte Versuch, Ihnen telefonisch etwas zu verkaufen, das Sie gar nicht wollen. Leider sind die Anrufer oft so unverschämt, und rufen immer und immer wieder an. Android und iOS bieten beide die Möglichkeit, Rufnummern zu sperren.

Die Sperre einer Rufnummer ist immer eine Sache des Smartphones. Sie kann nur dort aktiviert werden und gilt natürlich nur für das jeweilige Telefon, auf der sie eingerichtet wurde.

Rufen Sie auf Ihrem Smartphone die Anrufliste auf und lassen Sie sich die eingehenden Anrufe anzeigen. Klicken Sie dann neben das **i** neben der Rufnummer. Sowohl iOS als auch Android zeigen Ihnen jetzt den letzten Anruf der Rufnummer, die Länge des Anrufes und vieles mehr.

Um die Rufnummer nun zu blockieren, klicken Sie bei einem Android-Gerät auf das Symbol unten rechts (das durchgestrichene Schild), bei iOS tippen Sie auf **Anrufer blockieren**.



Bestätigen Sie die Blockierung, wenn Ihr Smartphone Sie fragt, ob sie das wirklich wollen.

Sollten Sie versehentlich eine Nummer blockiert haben, dann können Sie dies natürlich richtigstellen. Gehen Sie über denselben Weg in die Anrufliste, rufen Sie die Nummer auf und wählen Sie dann **Entsperren** bzw. **Blockierung aufheben**.

So geht's leichter | Zehn Gefahren vermeiden/abwehren

Viren und Würmer: Schädlinge bekämpfen

Virenschutz ist ein Thema, das kontinuierlich diskutiert wird. Immer mehr Viren sind im Umlauf, und täglich kommen mehr hinzu. Mittlerweile sind es weniger die allgemein verteilten Viren, die in der Breite auftreten, sondern kleine, rasend schnell neu auftretende Bedrohungen, die teilweise sogar nur auf bestimmte Anwendergruppen zielen. Die zeitnahe Aktualisierung der Virendefinitionen ist für Hersteller so immer mehr eine Herausforderung. Schützen Sie sich, so gut es eben geht!

Virenschutz mit Windows Defender

Gerade bei einem neuen PC haben Sie vielleicht die gewünschte Antivirus-Software noch nicht zur Hand, sie wollen sich noch informieren oder abwarten. Das bedeutet aber nicht, dass Sie auf Virenschutzverzichten sollten: Windows 10 bietet mit dem Windows Defender schon im Standard eine cloudbasierte Lösung.

Unter **Einstellungen** > **Update & Sicherheit** > **Windows Defender** können Sie den Windows Defender aufrufen und konfigurieren.

So geht’s leichter | Zehn Gefahren vermeiden/abwehren

Unter **Viren- & Bedrohungsschutz** können Sie schnell eine Überprüfung Ihres PCs vornehmen lassen oder **eine Erweiterte Überprüfung**, die dann tatsächliche alle Dateien scannt.

Wichtig ist hier vor allem, dass Sie unter den Einstellungen für Viren- & Bedrohungsschutz den **Cloudbasierten Schutz** aktiviert haben. Dessen Funktionsweise ist einfach: Über die Masse der Windows 10-PCs, die kontinuierlich auf Bedrohungen überwacht werden, sind unterschiedlichste Bedrohungen schnell erkennbar, auch wenn sie einem klassischen Virenscanner noch nicht bekannt sind. Die Cloud-Systeme von Microsoft erkennen die Bedrohung und können durch KI-Analysen innerhalb von Sekunden entscheiden, dass die Quelle blockiert werden muss.

So geht's leichter | Zehn Gefahren vermeiden/abwehren

Dabei ist es egal, ob es sich um eine Webseite handelt, einen Dienst, der kompromittiert wurde oder einen Treiber/ein Programm, dass befallen ist.

Aktivieren Sie den Windows Defender ruhig zusätzlich zu Ihrer präferierten klassischen AV-Lösung!

Verwenden einer Antivirus-Software

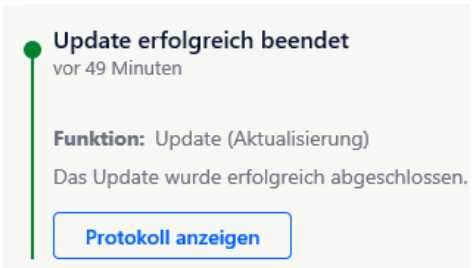
Antivirenprogramme sind wie alle andern Programme stetigen Veränderungen unterworfen. Wenn Sie noch keine präferierte Antivirenlösung im Einsatz haben, dann hilft es, wenn Sie im Internet nach **Test Antivirus** suchen, dort finden Sie eine Vielzahl von Testberichten. Wählen Sie sich die Tests renommierter Magazine und Tester aus! Beispielsweise testet die Stiftung Warentest regelmäßig die aktuellen Antivirus-Lösungen nach unterschiedlichen Kriterien.

So geht's leichter | Zehn Gefahren vermeiden/abwehren

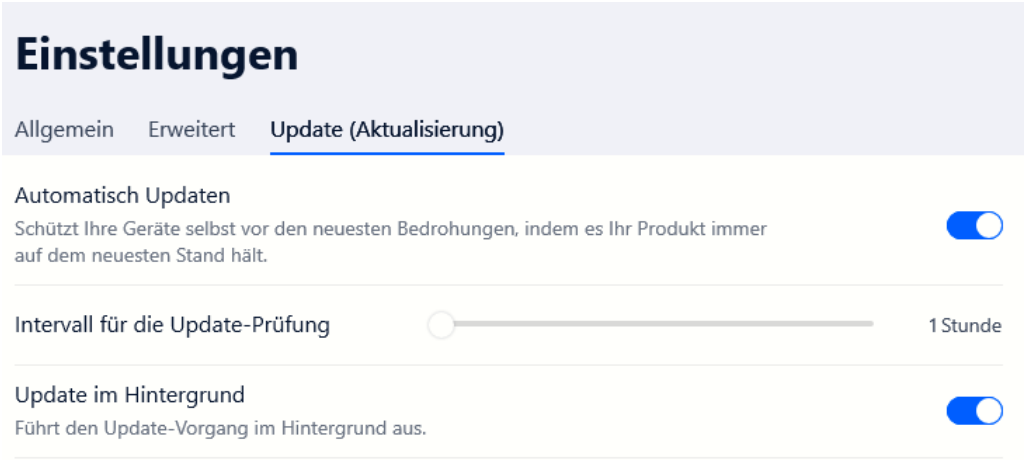
Dabei kommen auch immer wieder kostenlose Lösungen wie Avira gut weg, bei den kostenpflichtigen Programmpaketen die von Kaspersky und von Bitdefender. Diese sind auch parallel mit der Windows Defender-Lösung verwendbar und ergänzen sich.

Virenscanner müssen genutzt werden!

Einen Virenscanner zu haben reicht natürlich nicht aus. Laufen muss er, und stetig aktualisiert werden muss er auch. Kontrollieren Sie regelmäßig, ob Ihr Virenscanner seine Virendefinitionen aktualisiert. In den Einstellungen sollte in jedem Fall das automatische Aktualisieren aktiviert sein, und auch wenn es übertrieben scheint: Ein Aktualisierungsintervall von einer Stunde ist nicht zu kurz! Es werden minütlich neue Viren entdeckt. Die Hersteller der Antivirensoftware reagieren sehr schnell, je kürzer das Intervall ist, desto schneller sind sie auch vor neu erkannten Viren geschützt.



So geht's leichter | Zehn Gefahren vermeiden/abwehren



Erkennen ist besser als Entfernen

Das klingt so toll: Sie haben eine Antivirussoftware installiert, dann kann Ihnen ja nichts mehr passieren. Oder? Diese Aussage ist ähnlich wahr wie „Ich schnalle mich an, dann kann ich ja einen Auffahrunfall riskieren!". Besser ist es, wenn Sie sich schon im Vorhinein schützen, damit Viren gar nicht erst auf Ihren PC kommen.

Ist die Quelle sicher?

Die Verlockungen sind groß: Da gibt es den neuesten Kinofilm oder die angesagte Serie kostenlos zum Download, per Mail bekommen Sie ein Dokument mit vermeintlich anstößigem Inhalt, das Sie unbedingt öffnen sollen und vieles mehr. Viele dieser Angebote bringen das Risiko von Malware mit.

So geht's leichter | Zehn Gefahren vermeiden/abwehren

Achten Sie darauf, ob die Quelle vertrauenswürdig ist. Bei Downloads im Internet ist es wie im Versandhandel: Ist etwas viel günstiger als überall sonst oder gar kostenlos, dann verbirgt sich hinter dem Angebot oft eine böse Absicht.

Schickt Ihnen ein Absender, den Sie nicht kennen plötzlich irgendwelche Dateien, dann widerstehen Sie der Neugier und öffnen diese einfach nicht!

Der Download aus App Stores

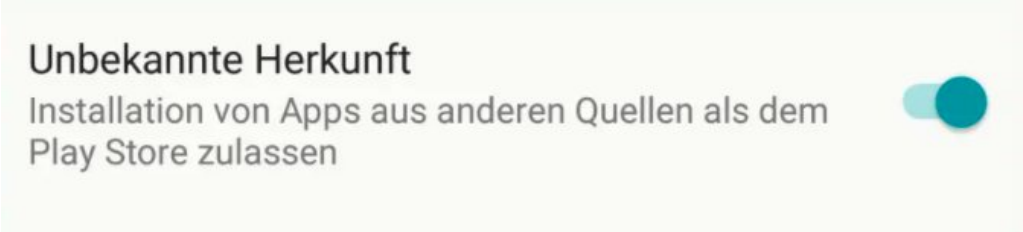
Windows, Mac, iOS, Android: Für die meisten Betriebssysteme gibt es eigene Software-Stores. Diese sind für den Download deutlich sicherer als irgendwelche Webseiten im Internet. Auch hier gilt wieder: Bietet man Ihnen sonst kostenpflichtige Software kostenfrei an, dann ist mit diesem Angebot oft etwas faul.

Besonders bei Android-Geräten sollten Sie vorsichtig sein: Es gibt den einen oder anderen vermeintlichen Softwareanbieter, der Ihnen die Android-Apps als APKs, zum Download anbietet. Normalerweise läuft der Download zwischen dem Android Play Store und Ihrem Gerät, ohne, dass Sie die Dateien in die Hand bekommen.

Diese APKs sind oft nicht signiert und unterliegen keiner Prüfung durch Google oder eine andere Instanz. Solche Dateien sollten Sie nur in absoluten Ausnahmefällen verwenden. Dann, wenn Sie den Entwickler kenne und der Ihnen beispielsweise zur Fehlereingrenzung eine solche Datei zur Verfügung stellt.

Prüfen Sie, ob auf Ihrem Android-Smartphone **Einstellungen** > **Sicherheit** > **Unbekannte Herkunft** aktiviert ist. Diesen Schalter sollten Sie grundsätzlich deaktiviert lassen und nur dann aktivieren, wenn es wie oben beschrieben im Ausnahmefall nötig sein sollte.

So geht's leichter | Zehn Gefahren vermeiden/abwehren



Jailbreaks und Custom ROMs

Unter iOS und iPadOS haben Sie schon per se mehr Sicherheit, denn Apple hat das System sehr stark gekapselt. Damit kommen (Schad-) Apps gar nicht an die Systemdaten und können kaum Schaden anrichten. Hinzu kommt, dass jede App, die im Apple AppStore verfügbar ist, einem umfangreichen Test unterzogen wird, bevor sie zum Download verfügbar gemacht wird.

Auch hier gilt allerdings: Keine Regel ohne Ausnahme. Der so genannte Jailbreak (die Befreiung des Telefons aus dem von Apple verordneten Gefängnis) wird von Händlern angeboten. Im Internet finden sich dazu sogar einige Anleitungen, wie Sie diesen selber durchführen können.

Auch wenn Sie plötzlich auf alle Dateien zugreifen können, andere Programme nutzen können und vieles mehr: Lassen Sie es. Das Risiko, dass die Aufhebung des Schutzes vor Schädlingen zu einer Infektion führt, ist höher als dieser Nutzen.

Dasselbe gilt übrigens auch die die so genannten Custom ROMs bei Android!

Phishing und Scamming vermeiden

Virenschutz folgt einer gewissen Systematik: Sie haben eine App installiert, die die Dateien auf Ihrem Rechner scannt. Die prüft

So geht's leichter | Zehn Gefahren vermeiden/abwehren

Codemuster in den Dateien gegen eine Liste bekannter Viren und warnt, wenn sie eine (vermeintlich) infizierte Datei findet.

Wofür es keine App gibt, ist Ihr natürliches Vertrauen darin, dass eine Mail von Apple oder Amazon oder ein Anruf von Microsoft schon echt sein werden. Das ist leider aber nicht immer der Fall!

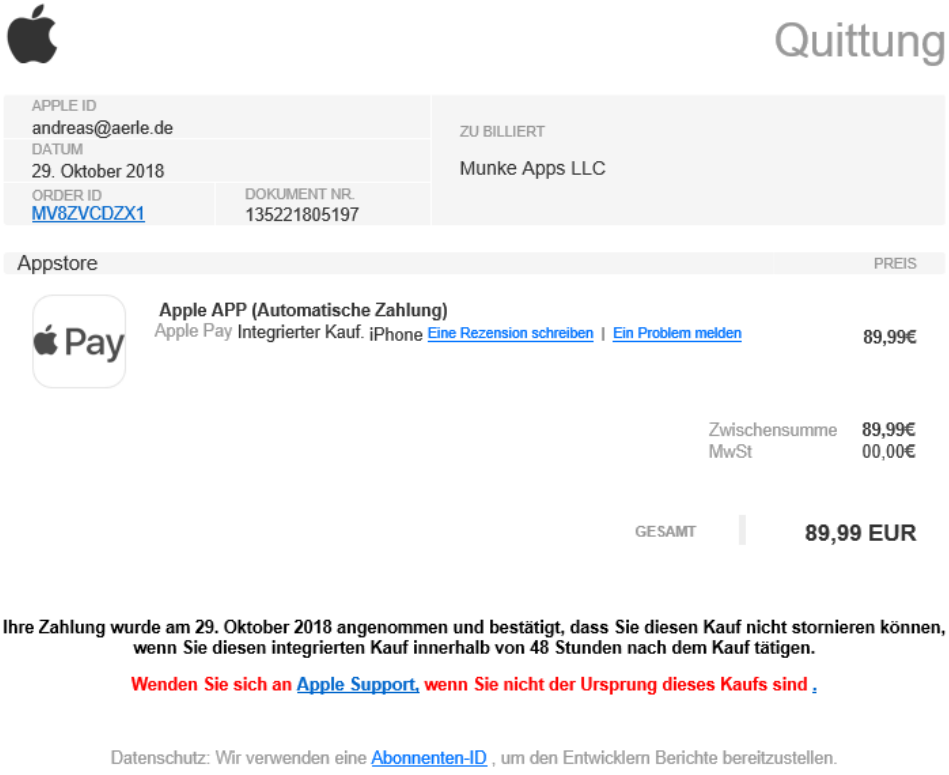
Phishing: Die gefälschte Händler-E-Mail

Es gibt eine bestimmte Menge von Händlern im Internet, bei denen die Wahrscheinlichkeit hoch ist, dass ein Benutzer ein Konto bei ihnen hat. Amazon, Media Markt, die Telekom, Apple gehören beispielsweise dazu. Wenn man also nun eine Liste von E-Mail-Adressen nimmt und an diese Adresse dann eine vermeintliche Rechnung über ein gar nicht gekauftes Produkt schickt, dann ist die Wahrscheinlichkeit hoch, dass eine Reaktion erfolgt. Auch eine Aufforderung, auf Grund eines Sicherheitsvorfalles unbedingt die Zugangsdaten zu ändern, ist Garant

So geht's leichter | Zehn Gefahren vermeiden/abwehren

dafür, dass der betroffene Anwender sich umgehend in Bewegung setzt. Er klickt auf den Link in der E-Mail und meldet sich schnell an.

Mit seinem echten Benutzernamen und seinem echten Passwort. Dummerweise ist in vielen Fällen die Webseite, auf die Sie geleitet werden, nicht echt. Und so hat unversehens ein Fremder 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.

So geht's leichter | Zehn Gefahren vermeiden/abwehren

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.

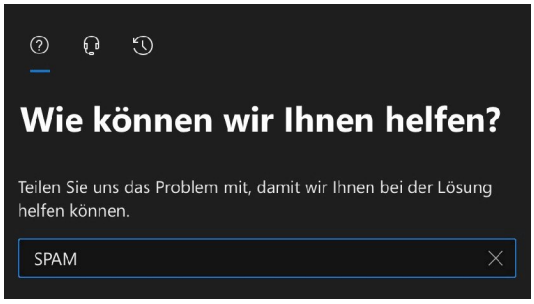
Der freundliche Anrufer

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. Das nennt man „Tech Support SCAM".

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, dann 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

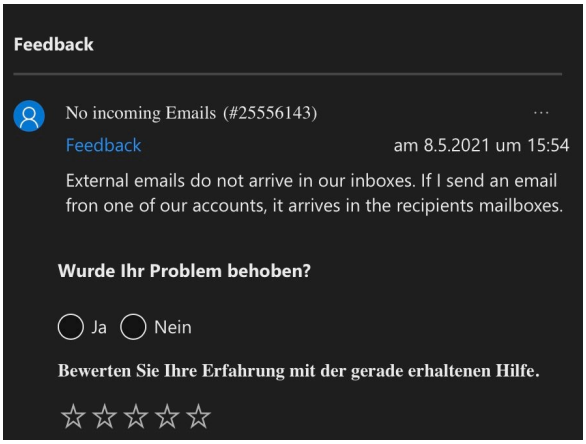
So geht's leichter | Zehn Gefahren vermeiden/abwehren

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



Gerade im Beispiel von Microsoft ist ein Anruf immer ausgelöst von einem Ticket, das Sie selber aufmachen. Wenn Sie Microsoft 365-Kunde sind, dann melden Sie sich dazu an Ihrem Admin-Center an. Dort klicken Sie auf das Fragezeichen oben rechts und geben eine Beschreibung Ihres Problems an. Das System stellt Ihnen jetzt automatisch verschiedene Lösungsmöglichkeiten zur Verfügung. Wenn diese Ihnen nicht helfen, dann können Sie auf das vorher noch gesperrte Symbol mit dem Kopf mit Headset klicken und alle relevanten Daten inklusive der Rückrufnummer eingeben.

Erst dann erfolgt ein Anruf von Microsoft, und wenn Sie das Ticket zu den deutschen Geschäftszeiten aufmachen, dann findet der Kontaktversuch auch auf Deutsch statt. In Ihrem Ticket können Sie sogar live verfolgen, dass Microsoft sie gerade anruft!



So geht's leichter | Zehn Gefahren vermeiden/abwehren

Ransomware und mehr: Die Erpressung

Ein weiteres Übel in der Arbeit mit Ihrem PC ist die versuchte Erpressung: Die bekommen eine E-Mail, in der man Sie mit einem vermeintlich schlüpfrigen Video erpressen will, oder Ihr PC meldet plötzlich, er könne nicht mehr auf die Dateien zugreifen, weil diese verschlüsselt sind. Je nach Art der Erpressung müssen Sie unterschiedlich reagieren!

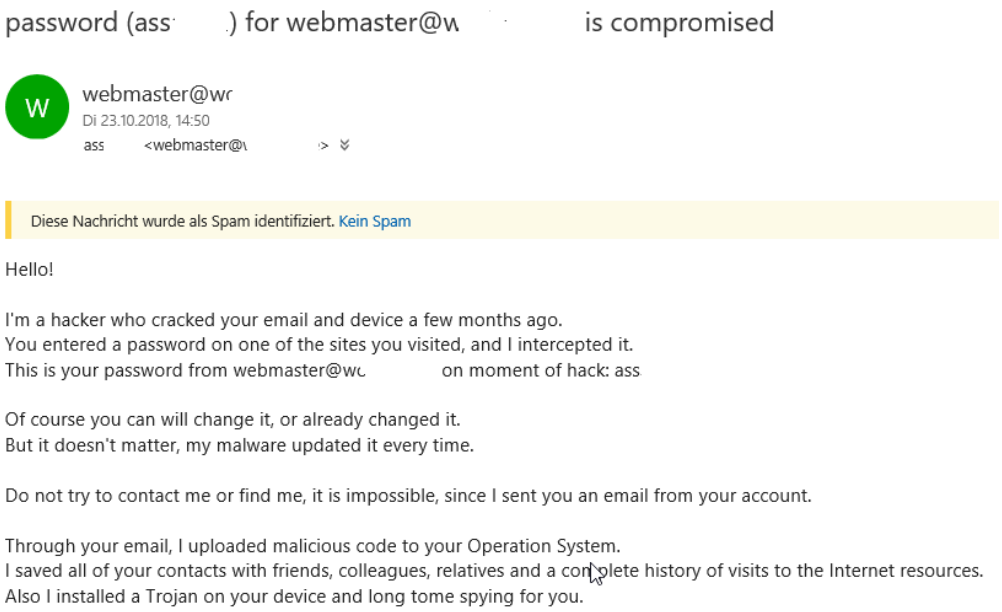
Der Erpressungs-E-Mail

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 dann 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.

So geht's leichter | Zehn Gefahren vermeiden/abwehren


password (ass .) for webmaster@w is compromised

W webmaster@wr
Di 23.10.2018, 14:50
ass <webmaster@

Diese Nachricht wurde als Spam identifiziert. Kein Spam

Hello!

I'm a hacker who cracked your email and device a few months ago.
You entered a password on one of the sites you visited, and I intercepted it.
This is your password from webmaster@wc on moment of hack: ass

Of course you can will change it, or already changed it.
But it doesn't matter, my malware updated it every time.

Do not try to contact me or find me, it is impossible, since I sent you an email from your account.

Through your email, I uploaded malicious code to your Operation System.
I saved all of your contacts with friends, colleagues, relatives and a complete history of visits to the Internet resources.
Also I installed a Trojan on your device and long tome spying for you.

Klicken Sie in diesen E-Mails auf keinen Link und öffnen Sie keine Anhänge: Die Wahrscheinlichkeit ist hoch, dass sich darin Schadsoftware befindet.

Ransomware: Verschlüsselter Rechner

Deutlich schlimmer ist es, wenn Sie sich eine Ransomware (einen Verschlüsselungstrojaner) eingefangen haben. Das ist eine Schadsoftware, die Dateien auf Ihrem PC verschlüsselt und diese nur gegen Zahlung einer teils heftigen Gebühr wieder entschlüsselt. Zumindest ist das das Versprechen, was die Ransomware Ihnen in der Meldung auf Ihrem Bildschirm anzeigt.

Eine Garantie dafür haben sie nicht, und ein allgemeingültiges Verfahren gibt es auch nicht.

Zuerst aber die gute Nachricht: Die meisten Antivirenprogramme haben auch einen Schutz gegen Ransomware integriert. Die Wahrscheinlichkeit einer Infektion ist also begrenzt.

So geht's leichter | Zehn Gefahren vermeiden/abwehren

Identifikation der Ransomware

Programmierer eines Virus oder einer Ransomware sind meist mitteilsam: Sie wollen Ihnen zeigen, wie gut sie sind. Natürlich nicht so, dass Sie die Person dahinter identifizieren können, aber eines können Sie immer machen: Die Infotexte mit der Suchmaschine Ihrer Wahl finden.

Das geht in den allermeisten Fällen, weil der Natur der Erpressung nach der Browser benötigt wird, damit Sie die Überweisung in Bitcoins ausführen können. Wenn Sie die Ransomware identifizieren konnten, dann finden Sie darin meist eine wichtige Entscheidung: Fahren Sie den Rechner herunter oder lassen sie ihn laufen.

Bei einem Teil der Ransomwares findet die Verschlüsselung erst nach einem Neustart des Rechners statt. Bei anderen sollten Sie den Rechner schnellstmöglich herunterfahren.

Beheben der Schäden

Um weitere Hilfe zu bekommen, können Sie auch einen Screenshot der Lösegeldforderung oder eine bereits verschlüsselte Datei bei dem kostenlosen Dienst ID Ransomware hochladen und bekommen Informationen über die Malware inklusive der ersten Tipps, was Sie als nächstes machen sollten.

Auch die Seite NoMoreRansom.com ist eine gute Anlaufstelle. Sie bietet Ihnen für immer mehr Ransomwares Entschlüsselungssoftware an, die Ihre Dateien entschlüsselt und wieder zugänglich macht.

Das alleine ist allerdings nur ein Teil der Gegenmaßnahmen. Dieser nützt Ihnen nur kurzfristig, wenn Sie die Ransomware selber nicht loswerden. Das kann durch Ihre Antivirensoftware geschehen, die Ransomware als Virus erkennen sollte. Wenn Sie sich jetzt die Frage

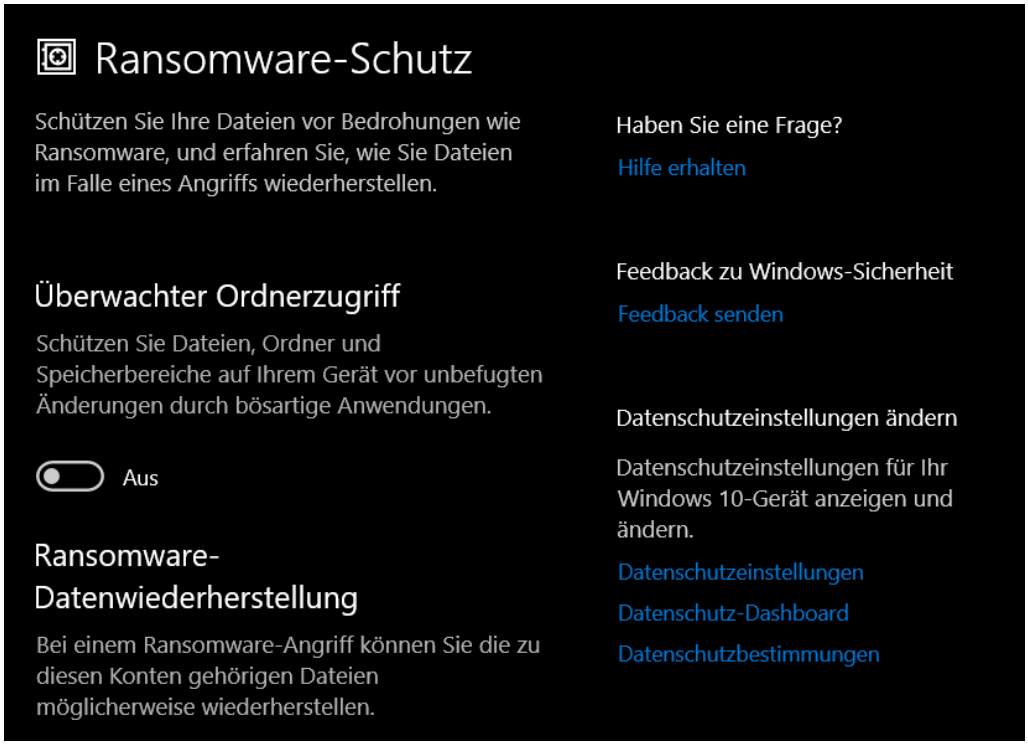
So geht's leichter | Zehn Gefahren vermeiden/abwehren

stellen, warum diese nicht schon die Infektion verhindert hat: Das kann viele Gründe haben, beispielsweise die Tatsache, dass auch Computerviren schnell mutieren und es immer eine Zeit dauert, bis die Virendefinitionen angepasst sind.

Um sicher zu gehen, installieren Sie Windows/macOS komplett neu! Das Einspielen eines Backups über eine Systemwiederherstellung (Windows) oder Time Machine (macOS) macht nur Sinn, wenn Sie sicher sind, dass zu dem Zeitpunkt die Infektion noch nicht erfolgt war.

Schutz vor Ransomware in Windows 10

Windows 10 hat einen eigenen Ransomware-Schutz integriert. Dieser ist nur dann verfügbar, wenn keine Sicherheitssoftware erkannt wird, die diese Funktion übernimmt.



So geht's leichter | Zehn Gefahren vermeiden/abwehren

Unter **Einstellungen** > **Update und Sicherheit** > **Windows-Sicherheit** > **Viren- & Bedrohungsschutz** können Sie in den Einstellungen den **Überwachten Ordnerzugriff** aktivieren. Sie können darin festlegen, welche Ordner überwacht werden sollen und welche Programme in diesen Ordnern Veränderungen an Dateien vornehmen können sollen. Das ist kein absoluter Schutz, verringert das Risiko der Verschlüsselung der Daten aber signifikant.

Abhören vermeiden: VPNs und Browser

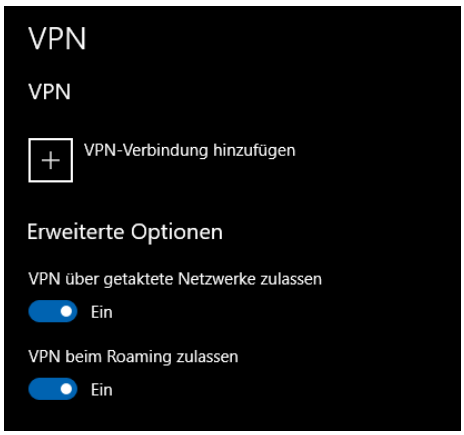
Eine Menge Informationen gehen durch die Leitungen, wenn Sie arbeiten. Der Natur des Internets nach können Sie nie sicher sein, dass nicht an irgendeiner Stelle jemand mitlesen kann. Dazu kommt noch die Besonderheit, dass die meisten Anwender immer mobiler werden. Der Internetzugang erfolgt oft dann nicht mehr lokal, sondern über eine Datenverbindung oder fremde WLANs, für die Sie die Sicherheit schlecht beurteilen können. Vermeiden Sie Risiken und sichern Sie sich ab.

Nutzen von VPNs

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

So geht's leichter | Zehn Gefahren vermeiden/abwehren

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



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

Tipp

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

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

Haben Sie keinen eigenen VPN-Server im Router oder der Netzwerkfestplatte? Dann nutzen Sie doch einfach einen Fremdanbieter wie HideMyAss oder CyberGhost. Auch der vor allem durch den Firefox-Browser bekannte Anbieter Mozilla bietet mittlerweile einen eigenen VPN-Dienst an.

Die VPN-Dienste bieten Ihnen den selben Service wie ein eigener VPN-Server, nehmen Ihnen aber den Aufwand der Einrichtung ab. Installieren

So geht’s leichter | Zehn Gefahren vermeiden/abwehren

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

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

Ganz nebenbei kann ein VPN die Lösung sein, wenn Sie bestimmte Seiten aus dem Ausland nicht erreichen können. Natürlich sind Sie in einem ausländischen Mobilfunknetz oder WLAN, und damit erkennt der Dienst, dass Sie eben nicht in Deutschland sind. Die Konsequenz: Er verweigert die Wiedergabe mit einer Meldung wie "Diese Sendung ist nur aus Deutschland zugreifbar". Guter Rat ist teuer? Nicht unbedingt! Die Nutzung eines VPN-Dienstleisters schafft nicht nur Sicherheit, sondern auch eine Lösung für das beschriebene so genannte **Geofencing**.

Bei den meisten VPN-Diensten können Sie als zusätzliche Option beim Verbindungsaufbau das Land wählen, in dem der VPN-Server stehen soll. Wählen Sie hier **Deutschland** an (die Standardeinstellung ist meist "automatisch").

So geht's leichter | Zehn Gefahren vermeiden/abwehren

Da die aufgerufenen Webseiten dann nicht Ihre IP-Adresse (die ja im Ausland liegt), sondern die des VPN-Servers sehen, ist die oben beschriebene Geoeinschränkung nicht aktiv. Die Anfrage kommt aus Deutschland, und ist damit zulässig, damit bekommen Sie die gewünschte Seite angezeigt.

Anonym und sicher Surfen: Der Tor-Browser

Eine Suche im Internet hinterlässt Spuren. Und bei bestimmten Themen ist es Ihnen vielleicht nicht so recht, wenn man nachvollziehen kann, dass Sie eine Webseite besucht haben. Eine schnelle Lösung ist hier der kostenlose Tor-Browser (https://www.torproject.org/de/download/)

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

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

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

So geht's leichter | Zehn Gefahren vermeiden/abwehren

Seite, von der Sie Daten herunterladen bzw. an die Sie Daten senden auch nicht identifizieren, dass Sie es sind. Nutzen Sie die Kombination aus VPN und Tor-Browser für die minimalen Internetspuren und Abhörmöglichkeiten!

Freunde betrügen nicht? Social Media

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, was Sie tun, kritisch.

Gerade die sozialen Netzwerke haben sich in der vergangenen Zeit immer mehr zu einem Sammelbecken von Ausspähversuchen und dubiosen Angeboten entwickelt. Gehen sie darauf ein, dann kann es schnell passieren, dass Sie Geld verlieren oder Ihr Konto gekapert wird.

So geht's leichter | Zehn Gefahren vermeiden/abwehren

Das unglaubliche Schnäppchen

Im Internet allgemein und in den sozialen Netzwerken im Speziellen 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.

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

Hilfreich ist es auch, das Produkt an sich noch einmal zu Googlen. In den meisten Fällen finden Sie die Originalseite unter einer ganz anderen Internetadresse und die „Schnäppchenseite" ist eine identische Kopie.

Sonderbare Freundschaftsanfragen

„Paul McCartney, der Beatle, will mit mir auf Facebook befreundet sein? Cool! Das Angebot nehme ich doch gerne an!". Seien wir ehrlich: Die Wahrscheinlichkeit, dass das passiert, ist verschwindend gering.

Eine solche oder ähnliche Situationen kommen aber immer wieder vor. Die Seiten der Fake-Accounts sehen täuschend echt aus, weil sie meist einfach Inhalte der echten Konten kopieren.

So geht's leichter | Zehn Gefahren vermeiden/abwehren

Akzeptieren Sie eine solche Freundschaftsanfrage, dann werden Sie schnell auf irgendwelche Preisausschreiben oder dubiose Webseiten geleitet.

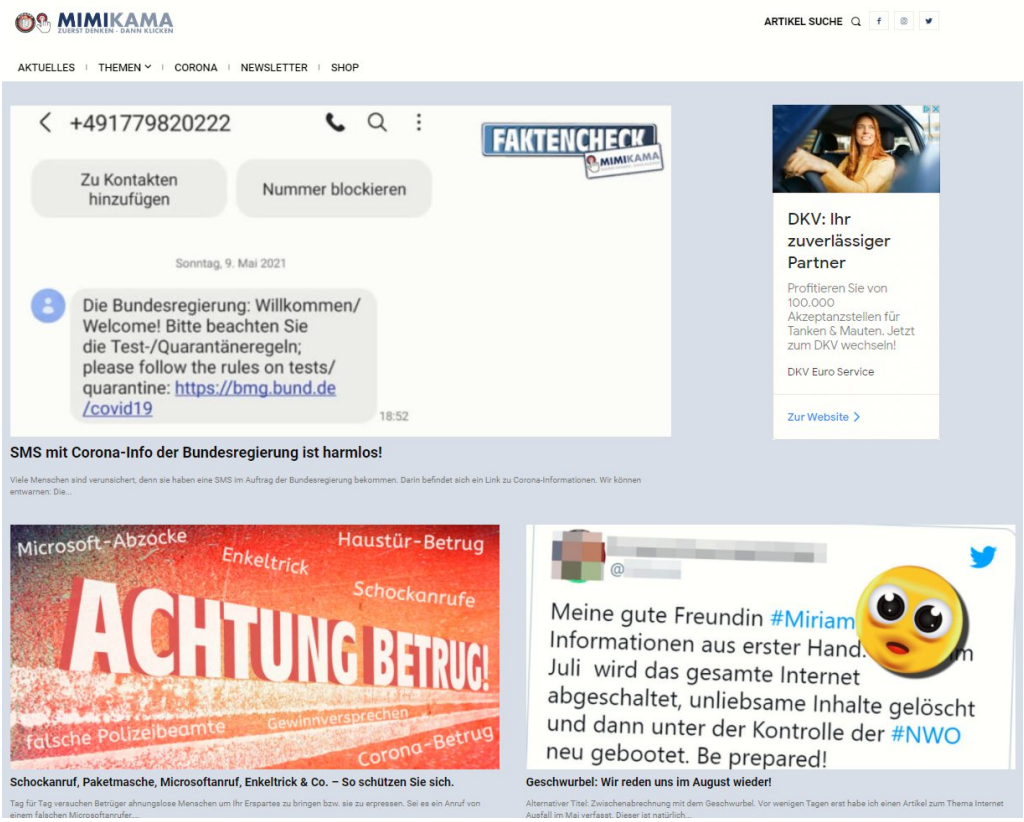
Bevor Sie eine solche Freundschaftsanfrage annehmen: Alle größeren sozialen Netzwerke haben ein Kennzeichen für Benutzerkonten, die verifiziert sind und damit garantiert. Schauen Sie neben dem Nutzernamen, ob sich dort ein blauer Haken befindet und klicken Sie darauf. Der Infotext sollte Ihnen anzeigen, dass es sich bei dem Konto um ein „echtes" Konto der Person handelt.

Fakes erkennen und vermeiden

Eine weitere Falle sind die diversen Fake-Meldungen, Kettenbriefe und Preisausschreiben, die Sie allüberall in den sozialen Netzwerken finden. Das angebliche Video, in dem Sie in einer schlüpfrigen Situation zeigen soll, das eBike, dass Sie einfach durch Kommentieren einer Nachricht

So geht's leichter | Zehn Gefahren vermeiden/abwehren

kostenlos bekommen, diese haben eines gemeinsam: Sie wollen Sie dazu animieren, zu klicken.



Im einfachen Fall, damit Ihre Daten gesammelt werden können. Im schlimmeren Fall, um Sie zur Preisgabe Ihrer Kontoinformationen zu animieren und Ihr Konto zu übernehmen. Eine tolle Anlaufstelle ist die Webseite Mimikama. Deren Motto „Zuerst denken – dann klicken" fasst gut zusammen, wie Sie sich vor solchen Fakes schützen können: Viele der verbreiteten Aktionen werden auf Mimikama erklärt und bewertet. Das gibt Ihnen eine größere Sicherheit, nicht auf einen Hoax reinzufallen. Neben den wirtschaftlichen Schäden, die entstehen können, ist es auch für Ihre Follower ein schlechtes Zeichen, wenn Sie eine Nachricht posten, die schon lange als Fälschung bekannt ist!

So geht's leichter | Zehn Gefahren vermeiden/abwehren

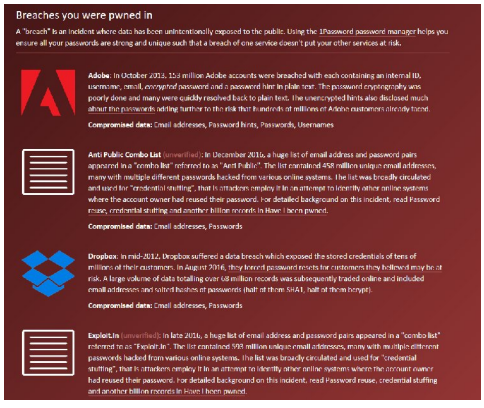
Richtig mit Passwörtern umgehen

Passwörter sind und bleiben erst einmal das Identifikationsmittel für Ihren PC, Applikationen und Online-Konten. Grund genug, hier ein wenig Zeit zu investieren und diese sinnvoll und sicher zu wählen und dann vor allem regelmäßig zu kontrollieren. Keine Sorge: Wenn Sie ein Passwort so gewählt haben, dass Sie sich nicht mehr daran erinnern können, dann sperrt Sie das nicht aus Ihrem Konto aus!

Wie Sie Passwörter richtig und sicher wählen, haben wir Ihnen hier zusammengeschrieben.

Passwörter regelmäßig checken

Immer wieder kommen Datenlecks und -pannen in die Nachrichten: Durch Sicherheitsvorfälle werden E-Mail-Adressen, Nutzernamen und Passwörter gestohlen und im Internet verkauft. Der Käufer hat dann so lange theoretisch Zugriff auf all Ihre Benutzerkonten, wie Sie das Passwort nicht geändert haben.



Die bekanntesten Sicherheitsvorfälle (zumindest die, die bekannt geworden sind), sind auf der Seite https://haveibeenpwned.com/ zusammengefasst. Dort können Sie nach Eingabe Ihres Passwortes sehen, ob und bei welchem Hack Ihre Zugangsdaten erbeutet wurden.

Wenn Sie betroffen sind, dann ändern Sie so schnell wie möglich das Passwort, und wiederholen Sie dies häufiger. Auch wenn Sie das nach dem Vorfall wissentlich oder unwissentlich schon gemacht haben:

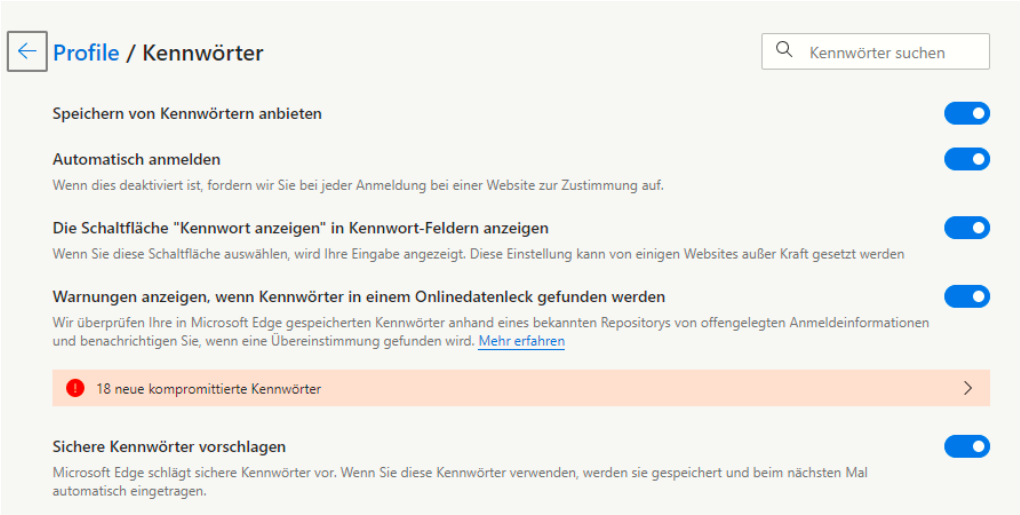
So geht's leichter | Zehn Gefahren vermeiden/abwehren

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.

Passwörter in Edge überprüfen lassen

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 | Zehn Gefahren vermeiden/abwehren

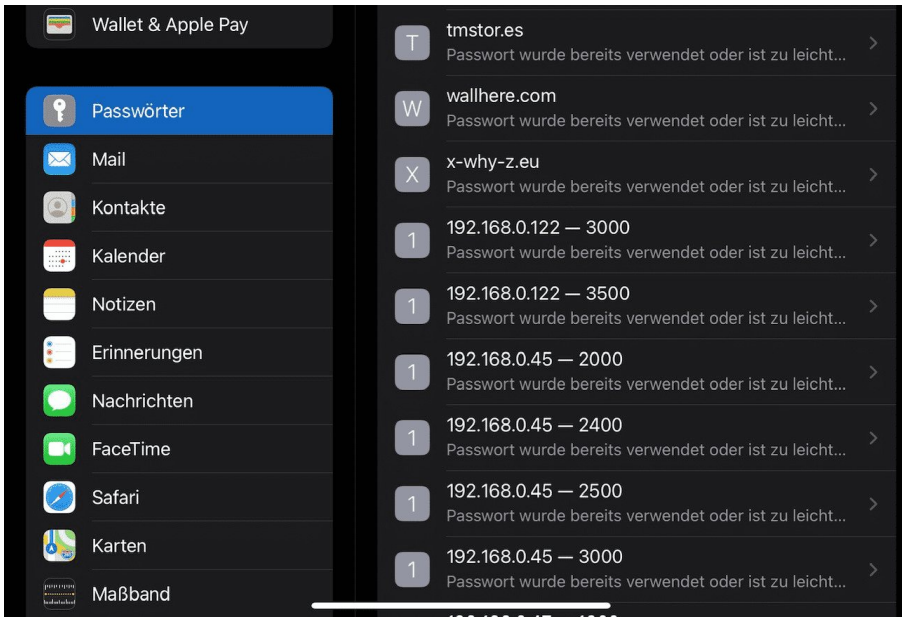
Wenn Sie das nachträglich machen wollen, dann klicken Sie in Edge auf die **drei Punkte** oben rechts, dann auf **Einstellungen** > **Profile** > **Kennwörter** und aktivieren Sie **Warnungen anzeigen, wenn Kennwörter in einem Onlinedatenleck gefunden werden**.

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.

Passwortcheck in iOS

So schön es ist, dass sie immer mehr Dinge online auch mit dem Smartphone durchführen können, einen Nebeneffekt hat das Ganze: Sie müssen immer mehr Benutzerkonten anlegen und dafür natürlich auch Passwörter vergeben. iOS 14 bietet hier eine zentrale Stelle, an der Sie die entstehenden Risiken kontrollieren und verringern können.

iOS speichert die Passwörter im Schlüsselbund. Das ist die interne, sichere Passwort-Datenbank von iOS.



So geht's leichter | Zehn Gefahren vermeiden/abwehren

Unter **Einstellungen** > **Passwörter** finden Sie direkt die Informationen zu den Konten/Webseiten, den verwendeten Passwörtern und der Bewertung, warum das Passwort nicht geeignet scheint oder ein Risiko beinhaltet. Tippen Sie auf einen Eintrag, dann können Sie direkt auf die Webseite wechseln, um das Kennwort zu ändern. Alternativ können Sie das Passwort aus dem Schlüsselbund löschen. Das macht Sinn, wenn Sie das Konto bereits gelöscht haben oder nicht mehr nutzen.

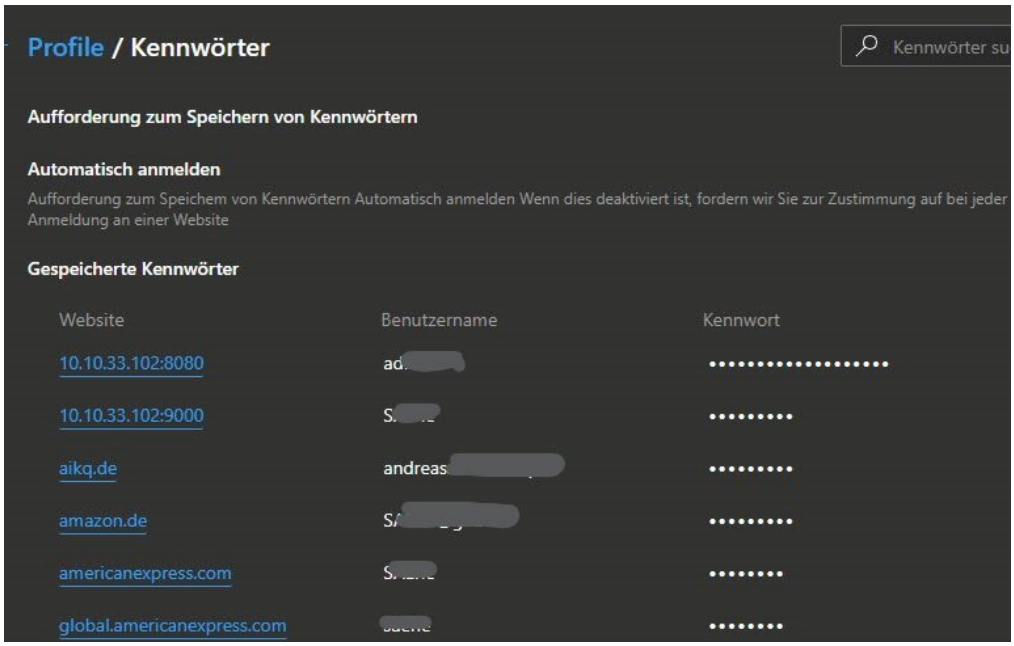
Passwort vergessen? Kein Problem!

Wenn Sie keinen Passwortmanager verwenden, dann kann es schon einmal vorkommen, dass Sie ein Passwort vergessen. Das schließt Sie auf den ersten Blick aus Ihrem Konto aus und kann Sie ausbremsen. Meist passiert das nämlich, wenn Sie überhaupt keine Zeit haben. Oft können Sie das mit wenig Aufwand korrigieren!

Herausfinden vergessener Kennwörter in Microsoft Edge

Sie kennen die Situation bestimmt: Da Gehirn ist noch wach, das Gedächtnis gut und so können Sie sich alle Kombinationen von Benutzernamen und Kennwort merken. Bis Sie dann eine Seite länger nicht mehr besucht haben und in der Folge genau deren Zugangsdaten vergessen haben. Wenn Sie keinen Passwort-Manager verwendet haben, dann ist guter Rat teuer. Es sei denn, Sie verwenden den neuen Edge-Browser. Der erlaubt nämlich den Export der darin gespeicherten Passwörter.

So geht's leichter | Zehn Gefahren vermeiden/abwehren



Klicken Sie auf die drei Punkte oben rechts am Bildschirm, dann auf **Einstellungen** > **Profile** > **Kennwörter** zeigt Edge Ihnen alle Webseiten an, auf denen Sie ein Passwort gespeichert haben. Ein Klick auf das Augen-Symbol rechts von einem Eintrag ändert die angezeigten Sternchen dann in das gespeicherte Passwort.

Um alle Passwörter in einer Excel-Tabelle zu erhalten, klicken Sie auf die drei Punkte neben **Gespeicherte Kennwörter** und wählen Sie dann **Kennwörter exportieren**. Vorsicht: Diese Excel-Tabelle in den Händen eines Unbefugten verursacht größtmöglichen Schaden: Darin stehen die Webseiten-URLs und die Kennwörter in Klarschrift!

So geht's leichter | Zehn Gefahren vermeiden/abwehren

Zurücksetzen von Kennwörtern

Wenn Sie das Kennwort partout nicht mehr finden, dann bieten die meisten Webseiten eine schnelle Hilfestellung. Voraussetzung ist, dass Sie noch Zugriff auf die E-Mail-Adresse haben, mit der Sie sich angemeldet haben.

In einem solchen Fall klicken Sie auf **Passwort vergessen**, dann bekommen Sie vom Anbieter automatisiert eine E-Mail mit einem Link. Auf diesen Link klicken Sie, dann können Sie ein neues Passwort eingeben und sich danach direkt damit anmelden.

Ohne die ursprüngliche E-Mailadresse wird eine Wiederherstellung des Kontos meistens leider schwer. Versuchen Sie in einem solchen Fall, den Anbieter direkt zu kontaktieren.

Schutz vor Datenverlust: Backups

Programme können Sie jederzeit neu installieren, das Betriebssystem notfalls auch. Ganz bitter wird es, wenn Sie Dateien verlieren. Die sind Ihre eigene, individuelle Kreation und ohne Datensicherung nur wiederherstellbar, wenn Sie sie mit hohem manuellen Aufwand rekonstruieren beziehungsweise neu erstellen. Wenn Sie Ihre Dateien in der Cloud speichern, dann übernimmt das der Anbieter. Wenn nicht: Vermeiden Sie den Stress, indem Sie Daten regelmäßig sichern!

Grundlagen der Datensicherung

Bei einer Datensicherung sollten Sie einige Dinge beachten:

So geht's leichter | Zehn Gefahren vermeiden/abwehren

Quell- und Ziellaufwerk sollten immer unterschiedlich sein. Eine Sicherung von Dateien auf das selbe Laufwerk kann Sinn machen, wenn Sie ein Dokument verändern/weiterentwickeln und verschiedene Versionen aufbewahren wollen. Gegen Verlust oder Defekt hilft Ihnen das aber nicht!

Das Sicherungslaufwerk sollte idealerweise nicht oder zumindest nicht dauerhaft in dem Windows 10-PC sein, von dem die Daten gesichert werden sollen. Hier bieten sich USB-Sticks oder externe Festplatten an, die nach der Datensicherung entfernt werden können. Eine weitere Alternative sind Netzwerkfestplatten, die an einem anderen Ort stehen. So können Sie die Wahrscheinlichkeit erhöhen, dass Sie nach einem Verlust des gesamten PCs zumindest Ihre Daten noch zur Verfügung haben.

Genügend freier Speicher: Natürlich muss das Sicherungslaufwerk mindestens so viel freien Speicherplatz haben wie die zu sichernden Dateien beanspruchen. Es macht durchaus Sinn, für die Datensicherung einen entsprechend großen USB-Stick anzuschaffen und diesen exklusiv dafür zu benutzen!

Sicherungen in Windows 10

Um Ihre Daten zu sichern, haben Sie verschiedene Möglichkeiten: der einfachste Weg ist eine manuelle Kopie der Daten über den Windows Explorer. Diese ist der schnellste und einfachste Weg, ist auf Grund der manuellen Tätigkeit aber natürlich fehleranfällig. Schnell geht der Wunsch des Backups im Alltagsstress unter, und wenn Sie verschiedene Speicherorte zu sichern haben, dann ist der Aufwand unverhältnismäßig hoch.

Eine manuelle Sicherung empfiehlt sich, wenn es schnell gehen muss oder die Sicherung ein einmaliger oder seltener Vorgang ist.

So geht's leichter | Zehn Gefahren vermeiden/abwehren

Durchführen eines manuellen Backups

Die Ausgangssituation: Sie kennen den Ort, an dem die zu sichernden Dateien stehen (beispielsweise die Dokumente) und wollen diese auf einen externen Datenträger sichern.

Starten Sie auf Ihrem Windows 10-PC den Windows Explorer, indem Sie gleichzeitig die **Windows-Taste und E** drücken.

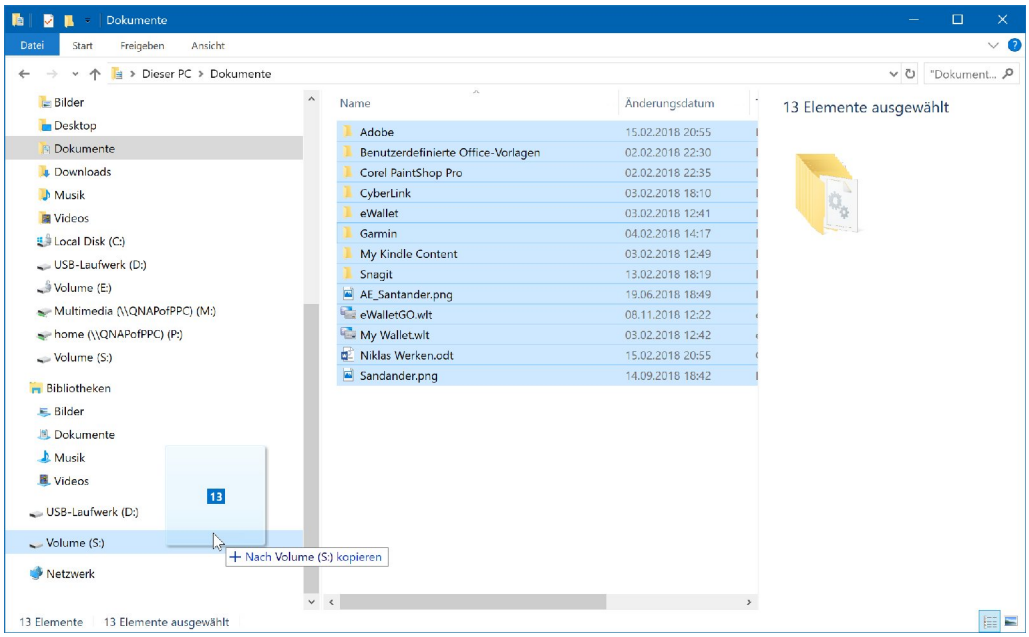
Wählen Sie das Verzeichnis aus, in dem sich die zu sichernden Dateien befinden, indem Sie links im Navigationsbereich des Explorers den entsprechenden Ordner öffnen, am Beispiel in den Bibliotheken den Ordner Dokumente.

Wenn Sie alle Dateien und Ordner eines Speicherortes rechts im Detailfenster des Explorers sehen, dann markieren Sie diese entweder, indem Sie mit der Maus einen Rahmen um sie herumziehen, oder drücken Sie auf der Tastatur gleichzeitig die Tasten **STRG und A**. Damit sind alle Dateien markiert, auch Dateien, die sich in Unterordnern befinden, werden mitgesichert.

Wählen Sie nun im linken Teil des Explorers das Sicherungslaufwerk aus. Wichtig dabei: Klicken Sie es nicht an, sondern machen Sie es nur sichtbar, indem Sie es mit den kleinen Pfeilen neben **Dieser PC** und dem Scrollbalken aus seinem virtuellen Versteck holen.

Alternativ können Sie auch zwei Explorer-Fenster öffnen und diese nebeneinander ziehen und dann in dem einen die Quelldateien und -verzeichnisse auswählen, in dem anderen das Ziellaufwerk für das Backup öffnen.

So geht's leichter | Zehn Gefahren vermeiden/abwehren



Bewegen Sie nun den Mauszeiger auf die markierten Dateien, drücken und halten Sie die **linke Maustaste** und ziehen Sie die Dateien auf das Ziellaufwerk. Wenn dieses markiert ist, dann lassen Sie die Maustaste los. Die markierten Dateien werden nun kopiert.

Wenn Sie immer dasselbe Laufwerk zur Datensicherung benutzen, dann ist die Wahrscheinlichkeit hoch. Dass Sie vom Explorer eine Nachfrage erhalten, ob die Dateien überschrieben werden sollen. Diese bestätigen Sie einfach, indem Sie **Dateien im Ziel ersetzen** anwählen.

Datensicherung über die Freeware Personal Backup

Wenn Sie nicht nur sporadisch an Ihrem PC arbeiten, werden Sie immer und immer wieder Datensicherungen durchführen wollen und müssen. Allgemein gilt: Eine Datensicherung ist schon veraltet, nachdem die letzte Datei kopiert wurde.

So geht's leichter | Zehn Gefahren vermeiden/abwehren

Statt den manuellen Aufwand zu treiben, sollten Sie bei Arbeit mit vielen Dateien eine Software wie Personal Backup zur Automatisierung einsetzen.

Diese können Sie kostenlos unter http://personal-backup.rathlev-home.de/ herunterladen.

Nach der Installation können Sie sich bequem zurücklehnen und sich vom Assistenten des Programms durch die Einrichtung Ihres ersten Backup-Auftrags führen lassen.

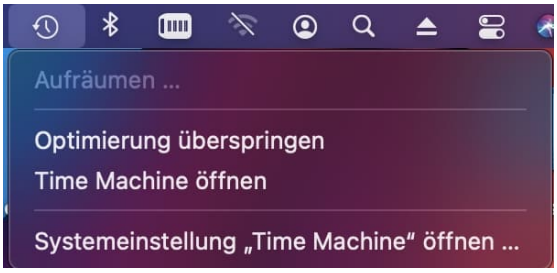
Unter **Diesen Auftrag automatisch starten** können Sie bis zu 16 Auftrage anlegen, die dann bei bestimmten Systemereignissen automatisch ausgeführt werden. Das sollten Sie für Ihre Standardaufträge auf jeden Fall aktivieren, dann vergessen Sie die Sicherung nicht.

Die sinnvollste Einstellung für den automatischen Start ist **Immer beim Abmelden**. Damit sichert Personal Backup die ausgewählten Dateien jedes Mal, wenn Sie sich von Ihrem PC abmelden oder Ihn herunterfahren.

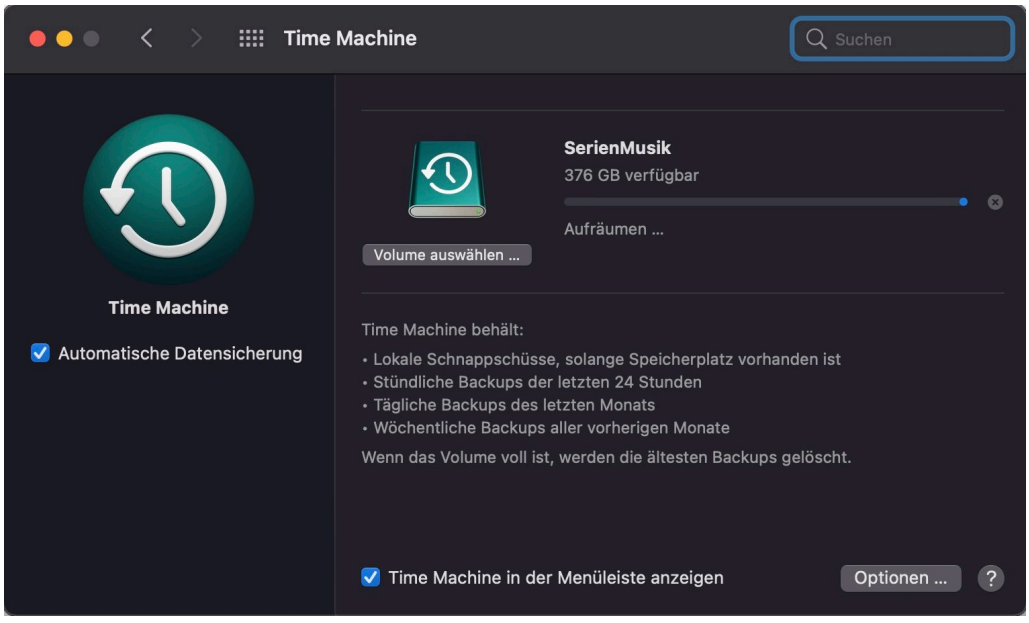
So geht's leichter | Zehn Gefahren vermeiden/abwehren

Sicherungen bei macOS: Time Machine

Time Machine ist direkt in macOS integriert und damit auf jedem Mac verfügbar. Der direkte Zugang versteckt sich in der Titelleiste von macOS unter dem Symbol mit der Uhr in einem kreisförmigen Pfeil. Klicken Sie darauf und dann auf Systemeinstellung **Time Machine öffnen**. Alternativ können Sie auch unter **Einstellungen** > **Time Machine** zu den Einstellungen gelangen.



Time Machine können Sie entweder auf eine externe Festplatte oder auf ein geeignetes Netzlaufwerk ausführen. Viele NAS-Anbieter (wie QNAP und Synology) unterstützen Time Machine. Zur Einrichtung konsultieren Sie das Handbuch Ihres NAS.



So geht's leichter | Zehn Gefahren vermeiden/abwehren

Klicken Sie auf **Volume auswählen**, um das Sicherungslaufwerk auszuwählen. Das sollte leer sein oder Sie nicht böse darum sein, wenn die Daten gelöscht werden: MacOS formatiert das Laufwerk und nutzt es nur für die Sicherung. Mehr müssen Sie nicht machen: Die Sicherung läuft automatisch, wenn der Mac eingeschaltet und das Laufwerk verbunden ist. Ist es voll, dann werden automatisch die ältesten Sicherungen gelöscht.

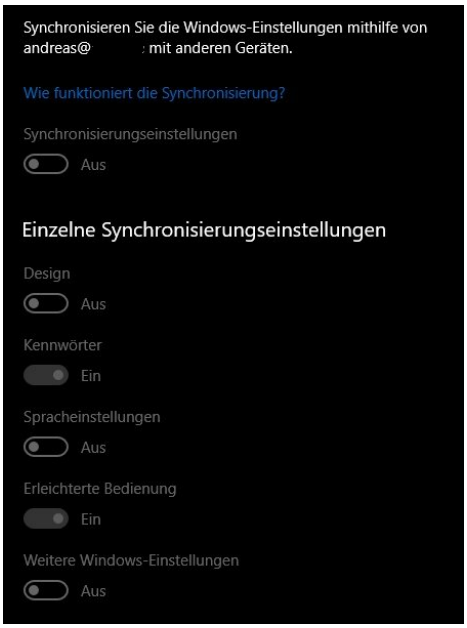
Verlust der Hardware abmildern

Wenn Sie noch nicht in der Situation waren, dann ist die erste Reaktion sicherlich „Wie kann man Hardware verlieren?! Das passiert doch nicht, wenn man aufpasst". Freuen Sie sich, wenn Sie eine solche Situation noch nicht erleben mussten! Die Ursachen sind vielfältig: Das Notebook wird aus dem Haus, Büro oder der Bahn gestohlen, das Handy fällt Ihnen im Taxi aus der Tasche. Manchmal quittiert auch einfach die Technik den Dienst. Wie auch immer: Wenn Sie eine Datensicherung haben, dann haben Sie zwar eine Sorge weniger, aber trotzdem eine Menge Arbeit. Alle Apps und Einstellungen nachzuziehen, wenn Sie ein neues Gerät angeschafft haben und dieses einrichten müssen

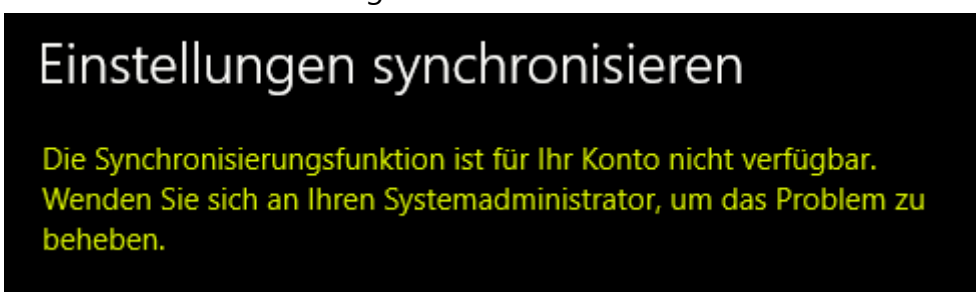
So geht's leichter | Zehn Gefahren vermeiden/abwehren

Einschalten der Synchronisation

Wenn Sie auf Ihrem PC mit einem Microsoft-Konto angemeldet sind, dann hat Windows 10 Zugriff auf Ihr OneDrive und kann bestimmte Elemente von Windows automatisch mit der Cloud synchronisieren. Das müssen Sie allerdings einschalten: Klicken Sie auf **Einstellungen** > **Konten** > **Synchronisieren**. Unter **Einstellungen synchronisieren** können Sie dann die verschiedenen Elemente auswählen, die Sie synchronisieren möchten. Schalten Sie **Synchronisierungseinstellungen** ein, dann können Sie unter **Einzelne Synchronisierungseinstellungen** fein abstimmen, welche Elemente synchronisiert werden sollen und welche nicht. Schalten Sie auf dem neuen Rechner später die Synchronisation ebenfalls ein. Dann lädt sich dieser automatisch alle synchronisierten Elemente herunter.



Sollten alle Schalter ausgegraut sein und Windows 10 Ihnen melden, dass Sie die Synchronisation nicht einschalten können, dann kontrollieren Sie die konfigurierten Konten.



So geht's leichter | Zehn Gefahren vermeiden/abwehren

Unter **E-Mail und Konten** finden Sie alle in Windows verwendeten Konten. Haben Sie zusätzlich ein Geschäfts- oder Schulkonto angelegt, dann kann das Windows durcheinanderbringen. Bei diesem Kontotyp müssen die Synchronisierungseinstellungen zentral verwaltet werden.

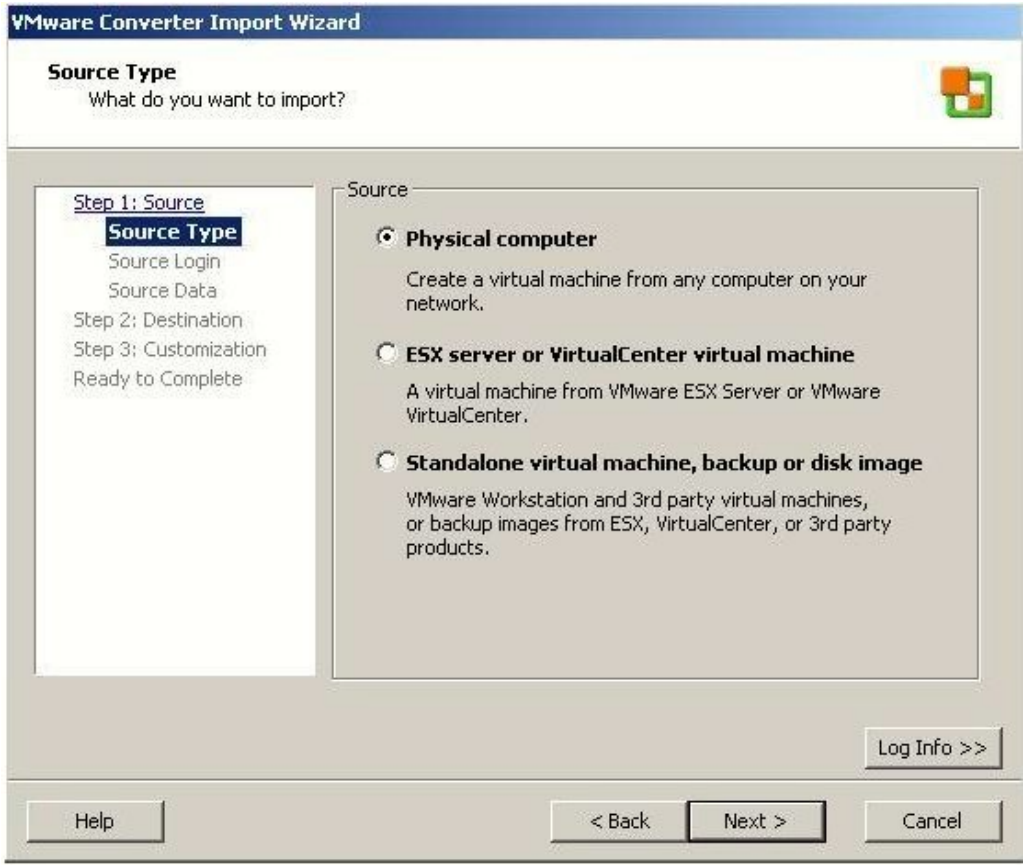
Entfernen Sie zum Aktivieren der Synchronisation das Geschäftskonto. Nachher können Sie es wieder einbinden!

Nach der Installation eines neuen Gerätes und dem erneuten Einschalten der Synchronisation stellt Windows die damit gesicherten Elemente automatisch wieder her.

Windows in eine virtuelle Maschine umwandeln

Das Sichern der Programme ist leider nicht ganz so einfach wie das von Dateien und Einstellungen. Das heißt aber nicht, dass Sie sich nicht eine Sicherheitskopie Ihres gesamten Rechners anlegen können:: Überführen Sie Ihr altes Windows in eine virtuelle Maschine. Damit können Sie den alten Rechner wie ein Programm auf einem anderen PC starten und Programme und Daten weiterverwenden. Einen Unterschied merken Sie – einen entsprechend leistungsfähigen PC vorausgesetzt – eher nicht.

So geht's leichter | Zehn Gefahren vermeiden/abwehren



Ein kostenloses Tool dafür ist der VCenter Converter von VMWare (https://www.vmware.com/de/products/converter.html). Folgen Sie nach Installation einfach den Anweisungen des Programms und wandeln Sie Ihren alten Rechner in eine virtuelle Maschine um. Diese können Sie dann mit dem ebenfalls kostenlosen VMPlayer (https://www.vmware.com/products/workstation-player.html) auf Ihrem Windows 10 PC ausführen und damit auf alle Programme und Daten weiterhin zugreifen.

Die virtuelle Maschine können Sie auf Ihrem Ersatzrechner starten und verwenden. Vorausgesetzt natürlich, Sie haben sie wie Ihre Dateien auf einem externen Laufwerk gesichert.

So geht's leichter | Zehn Gefahren vermeiden/abwehren

Time Machine beim Mac

Wenn Sie wie im vergangenen Kapitel Time Machine auf Ihrem Mac oder MacBook eingerichtet haben, dann sind Sie gut auf einen Hardwareverlust vorbereitet. Time Machine sichert nämlich nicht nur Dateien, sondern auch Systemzustände mit den Apps, Einstellungen etc.

Bei der Einrichtung des neuen Macs fragt macOS Sie automatisch, ob Sie die Daten wiederherstellen wollen. Eine der Optionen ist dann Time Machine. Bis auf Registrierungen mancher Anwendungen und einiger Passwörter können Sie das neue Gerät nach dem Wiederherstellen genauso nutzen wie das Alte.

Sicherungen des Smartphones

Alleine seiner Größe wegen ist Ihr Smartphone das Gerät, das sich am ehesten in Gefahr befindet, dass Sie es verlieren. Da Sie mehr und mehr

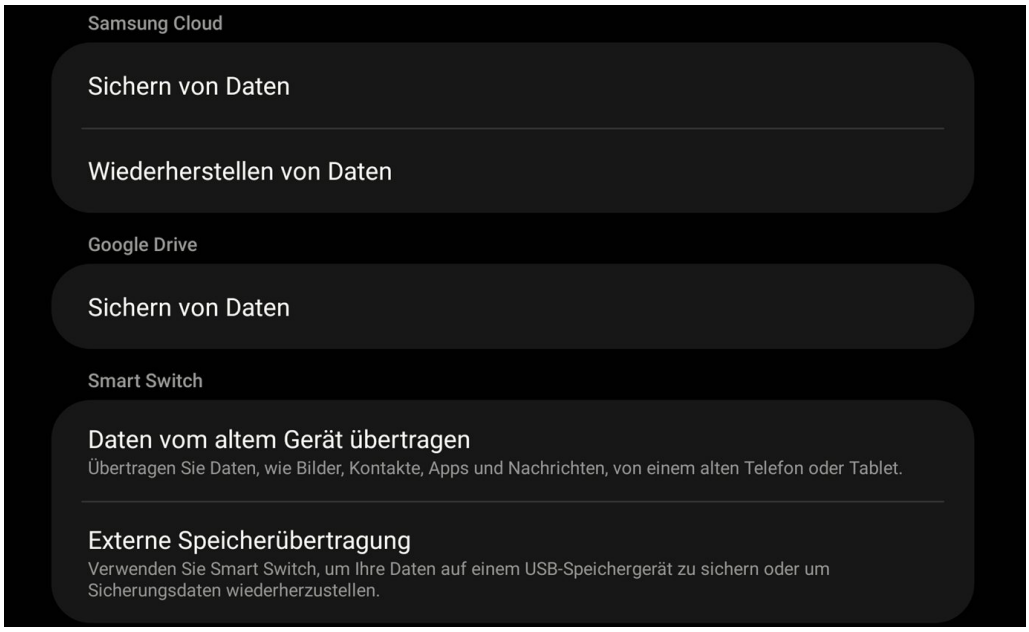
So geht's leichter | Zehn Gefahren vermeiden/abwehren

Daten auf dem mobilen Gerät verarbeiten, auf der anderen Seite aber eine manuelle Sicherung von Daten nicht ganz trivial ist, sollten Sie sich vorbereiten.

Sicherungen bei Android

Android ist im Gegensatz zu iOS nicht so standardisiert, wie sich viele Anwender das wünschen. Zwischen Android-Versionen und sogar zwischen Herstellern kann das leicht anders aussehen. Nichtsdestotrotz: Unter **Einstellungen** > **Konten und Sicherungen** finden Sie die Standardsicherung von Android unter **Google Drive**.

Tippen Sie auf **Jetzt sichern**, um eine Komplettsicherung zu starten.



Je nach Hersteller können Sie parallel beispielsweise noch weitere Daten in die Samsung-, Huawei- oder sonstige herstellerspezifische Cloud sichern.

So geht's leichter | Zehn Gefahren vermeiden/abwehren

Beim Einrichten eines neuen Gerätes fragt Android dann ab, ob eine Sicherung wiederhergestellt werden soll und führt Sie dann durch den Prozess.

Sicherungen bei iOS/iPadOS

Bei einem iPad oder iPhone ist die Sicherung immer an derselben Stelle: Wenn Sie sich mit iCloud anmelden, dann finden Sie unter den Einstellungen ganz oben Ihr Profilbild und den iCloud-Account. Tippen Sie darauf, dann auf **iCloud-Backup**. Stellen Sie sicher, dass das Backup eingeschaltet ist. iOS/iPadOS sichern automatisch, wenn Ihr Gerät mit der Stromversorgung verbunden und in einem WLAN eingebucht ist.

Kontrollieren Sie regelmäßig, wann das letzte Backup durchgeführt wurde und starten Sie es gegebenenfalls manuell mit einem Tippen auf **Backup jetzt erstellen**.

Beim Einrichten eines neuen Gerätes fragt iOS/iPadOS dann ab, ob eine Sicherung wiederhergestellt werden soll und führt Sie dann durch den Prozess.

Überfrachtung von Windows lösen

Windows ist als Betriebssystem im Standard so konfiguriert, dass es für die meisten Anwender alle Möglichkeiten bietet. Dann kommen noch die Hersteller und packen das eine oder andere Programm dazu, das sie testen und möglichst kaufen sollen. All das läuft im Hintergrund und nimmt Einfluss auf die Performance Ihres Rechners. Statt nun in die Falle

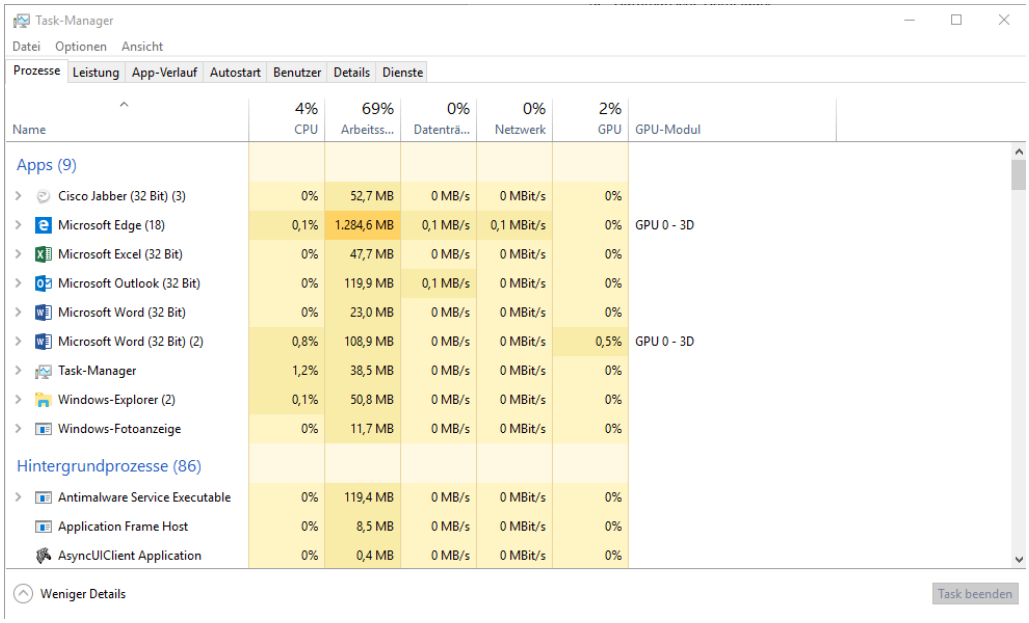
So geht's leichter | Zehn Gefahren vermeiden/abwehren

zu tappen und langsamer arbeiten zu müssen, davon aber keinen Vorteil zu haben, räumen Sie auf!

Beenden von Programmen und Diensten

Auch wenn Sie in der Taskleiste nur einige wenige Programme sehen: Unter der Motorhabe läuft eine Vielzahl von Prozessen. Und die nicht immer rund: Sie beenden Word als Programm, der zugehörige Prozess läuft aber weiter und verbraucht CPU-Kapazität. Damit wird das System langsam und hält Sie davon ab, schnell zum Ziel zu kommen. Die Abhilfe: Der Windows Task-Manager.

Drücken Sie gleichzeitig die Tasten **Alt**, **Strg** und **Entf**. Wählen Sie dann in der Liste den **Task-Manager**.



Sie sollten nun die laufenden **Apps** und die **Hintergrundprozesse** sehen. Sehen Sie letztere nicht, dann klicken Sie auf **Mehr anzeigen**.

So geht's leichter | Zehn Gefahren vermeiden/abwehren

Klicken Sie auf die Spalte **CPU**, um eine Sortierung nach der CPU-Last angezeigt zu bekommen. Je höher diese ist, desto ausgelasteter (und langsamer) ist Ihr Rechner.

Wenn Sie einen Prozess oder ein Programm sehen, das Sie kennen und eine zu hohe CPU-Last verursacht, dann klicken Sie es an und dann auf **Task beenden**. Dadurch wird Ihr PC schneller, weil er sich nicht mehr mit diesem Programm/Dienst beschäftigen muss.

Wichtig

Bevor sie ein Programm oder einen Prozess über den Task-Manager beenden, speichern Sie alle Daten – soweit das noch geht. Handelt es sich um ein Programm, das nicht mehr bedienbar ist, dann sollten sie eine Weile abwarten, ob es nicht doch wieder von allein reagiert. Im schlimmsten Fall verlieren Sie alle Daten, die Sie noch nicht gespeichert haben!

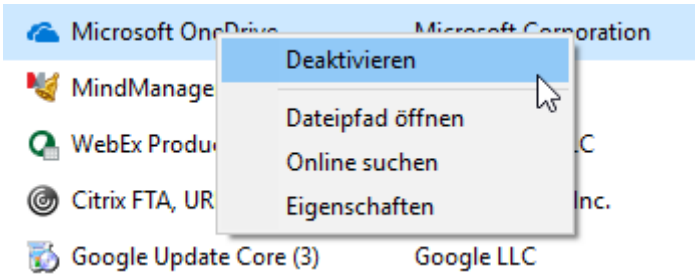
Unnötige Programme aus dem Autostart löschen

Windows versucht, Ihnen alle benötigten Dienste und Programme direkt beim Systemstart zur Verfügung zu stellen. Diese Auswahl wird allerdings auch davon beeinflusst, dass installierte Programme und Apps oft der Meinung sind, sie seien unverzichtbar, und sich auch zum direkten Start registrieren lassen.

Das führt schnell dazu, dass Programme im Hintergrund laufen, die Sie gar nicht brauchen und sowohl der Start des Systems verzögert wird als auch CPU-Zeit verschwendet wird.

So geht's leichter | Zehn Gefahren vermeiden/abwehren

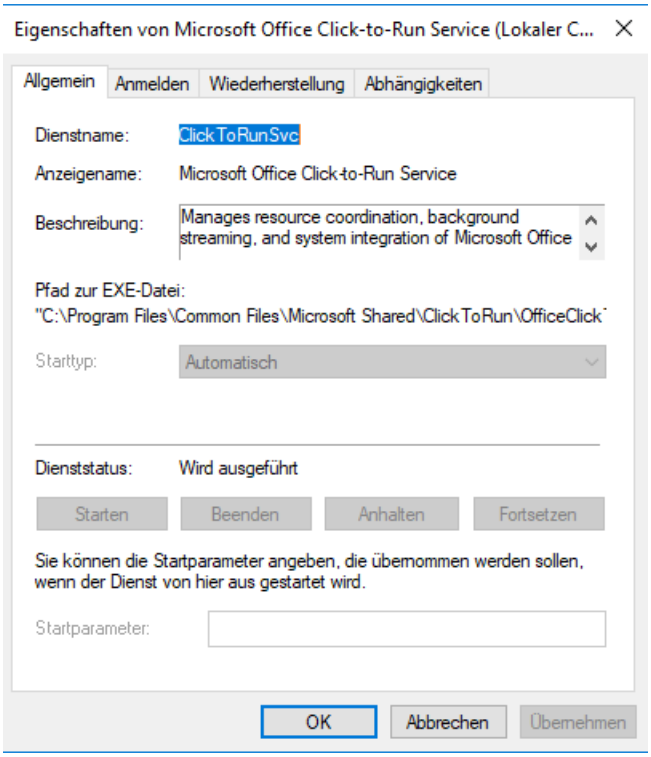
Statt diese immer wieder manuell zu beenden, verhindern Sie einfach ihren automatischen Start! Klicken Sie dazu im TaskManager auf den Reiter **Autostart**, dann mit der rechten Maustaste auf den Dienst/das Programm. Ein Klick auf Deaktivieren verhindert den automatischen Start. Sollte das zu Problemen führen, können Sie ihn jederzeit auf demselben Weg wieder aktivieren.



Unnötige Dienste beenden

Mit den Diensten verhält es sich wie mit den Programmen: Windows 10 startet viele automatisch mit, aktiv benötigen Sie aber nur einen Teil davon. Die anderen langweilen sich und verbrauchen nur Rechner-Kapazitäten. Auch Dienste können Sie davon abhalten, automatisch gestartet zu werden.

So geht's leichter | Zehn Gefahren vermeiden/abwehren



Drücken Sie **Windows** und **R**, dann geben Sie in das Eingabefeld als Befehl **services.msc** ein. Windows 10 zeigt Ihnen nun alle Dienste an, die auf Ihrem PC vorhanden sind.

In der Spalte Status können Sie sehen, ob der Dienst gerade läuft („wird ausgeführt"). Klicken Sie mit der rechten Maustaste darauf und dann auf **Eigenschaften**.

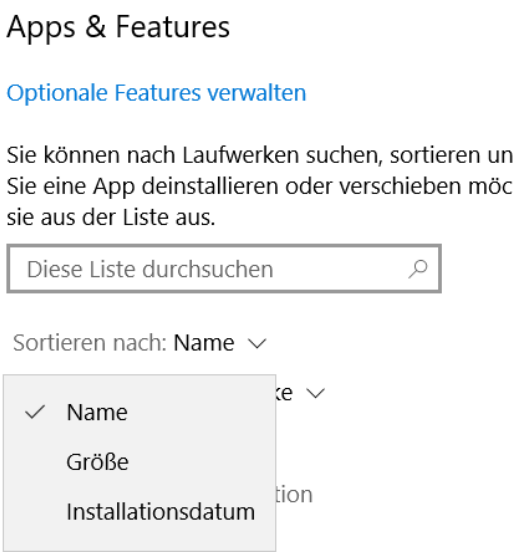
Ein Klick auf **Beenden** beendet einen laufenden Dienst. Unter **Starttyp** können Sie festlegen, dass der Dienst nur **manuell** gestartet wird, nicht automatisch. Gerade bei Diensten zu Programmen, die Sie eher selten brauchen, kann das Ihr System spürbar beschleunigen. Im Normalfall startet das Programm beim Start die Dienste sowieso, wenn sie noch nicht laufen.

Deinstallieren von Programmen

Im Leben Ihres PCs werden Sie eine Vielzahl von Programmen installieren. Viele davon sind nur ein Versuch auf der Suche nach der richtigen App für Ihre Anwendung. Diese nutzen Sie dann meist selten bis gar nicht mehr. Jedes installierte Programm nimmt aber wertvollen Speicherplatz weg. Hinzu kommt, dass Programme oft nicht nur während ihrer Verwendung Ressourcen belegen, sondern durch Hintergrunddienste eigentlich immer. Warum das System mehr

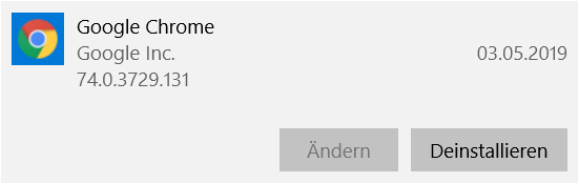
So geht's leichter | Zehn Gefahren vermeiden/abwehren

belasten, als es wirklich nötig ist? Installieren Sie einfach unnütze Programme!



Dazu klicken Sie auf **Einstellungen** > **Apps** > **Apps & Features**. Sie bekommen nun alle installierten Apps angezeigt. Wenn Sie bereits wissen. Welches Programm Sie deinstallieren wollen, dann suchen Sie es sich in der alphabetisch sortierten Liste heraus. Manchmal möchten Sie auf Grund von Platzproblemen vor allem große Programme deinstallieren. Dann klicken Sie auf **Sortieren nach** und wählen dann **Größe**. In der umsortierten Liste stehen die am meisten Platz belegenden Apps an oberster Stelle.

Wenn Sie die zu deinstallierende App gefunden haben, dann klicken Sie sie an. Es öffnet sich ein weiterer Anzeigebereich unter der App, in dem Sie auf **Deinstallieren** klicken können. Mit der App selbst werden dann auch alle Dienste und Systemprogramme mit deinstalliert. Vorsichtshalber führen Sie noch einen Neustart durch, dann sollte Ihr System spürbar schneller sein.



So geht’s leichter | Zehn Gefahren vermeiden/abwehren