So geht's leichter...

Effektiver Schutz vor Hack-Attacken

- **Windows und Cloud absichern**
- **Eure wirksamste Waffe: Updates!!**
- **Router & andere Hardware updaten**
- **Phishingangriffe abwehren**
- **Tipp: Zwei Faktor Authentifizierung**

Autoren:
Jörg Schieb
Andreas Erle

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

So geht's leichter | Effektiver Schutz vor Hack-Attacken

Inhalt

So geht's leichter | Effektiver Schutz vor Hack-Attacken

So geht's leichter | Effektiver Schutz vor Hack-Attacken

So geht’s leichter | Effektiver Schutz vor Hack-Attacken

Hacker? Bots? Das kennen wir aus Fernsehen und Kino. Firmen werden angegriffen, Staaten gar – aber doch nicht wir Privatleute – oder etwa doch?

Leider hat sich die Welt in den letzten Wochen und Monaten sehr verändert, und das nicht nur in dieser Hinsicht. Auch Privatleute können Ziel von Hackerangriffen sein – von allgegenwärtigen Cyber-Betrügern sowieso. Aktuell warnen BSI (Bundesamt für Sicherheit in der Informationstechnik) und andere Behörden vor einer höheren Gefahr als sonst schon.

Hacker attackieren schon längst nicht mehr einzelne Unternehmen, um diese zu erpressen. Diesen Geschäftsmodell existiert zwar immer noch, immer stärker aber wird der gezielte Angriff auf Infrastrukturen zur Regel. Vom sozialen Netzwerk über E-Mail-Dienste bis hin zu einzelner Hardware: Das Ziel ist Chaos, Spionage, Manipulation und Betrug. Dass sich damit auch finanzielle Interessen verbinden, keine Frage. Der Unterschied ist aber, dass mittlerweile jeder Anwender davon betroffen sein kann.

So geht’s leichter | Effektiver Schutz vor Hack-Attacken

Die Urheber sind immer öfter nicht nur „normale“ Cyberkriminelle, die auf eigene Rechnung handeln, sondern Kollektive, die im Auftrag von Organisationen und sogar Staaten agieren.

Keine Sorge: Die Situation ist zwar aktuell alles andere als angenehm, aber sie ist nicht hoffnungslos. Ihr müsst kein IT-Profi sein, um Euch zu schützen. Es gibt viele verschiedene Ansätze, die Eure Sicherheit erhöhen und mit wenig Aufwand umsetzbar sind.

So geht´s leichter: Kümmert Euch um Updates für alle Geräte und Programme. Achtet darauf, welche Informationen Ihr wem gebt, wie Ihr diese freigebt und wie Ihr Zugriffe kontrolliert und berechtigt.

Keine Frage: Diese Maßnahmen kosten Zeit. Viel weniger aber, als wenn Ihr irgendwann feststellt, dass Ihr gehackt worden seid oder Eure Daten in fremde Hände geraten sind.

Wir zeigen Euch, worauf Ihr achten müsst!

Warum sind (auch) Privatleute im Fokus?

Das Prinzip kommt aus der Natur: Bei der Jagd konzentrieren sich die Jäger erst einmal auf das schwächste Tier der Herde. Der Aufwand ist deutlich geringer und der Erfolg schneller, als würde man sich einen würdigen Gegner nehmen.

Übertragen auf die Herde der Internetbenutzer: Die meisten Firmen investieren eine Menge Geld und Aufwand in ihren Schutz. Ausgeklügelte Antiviren- und Firewall-Systeme, Intrusion Detection-

So geht's leichter | Effektiver Schutz vor Hack-Attacken

Programme, die sehr schnell Eindringlinge erkennen und nötige Maßnahmen empfehlen – und vieles andere mehr.

Dieses Maß an Schutz kann sich der normale Benutzer nicht leisten. Damit ich er ein leichteres Ziel. Und weil in den letzten zwei Jahren pandemiebedingt mehr Menschen als jemals zuvor im Home Office waren (und sind), eignen sich diese Menschen besonders gut als Ziel. Denn zu Hause sind die Systeme (PCs, Mobilgeräte) in der Regel deutlich schlechter geschützt als im Unternehmen.

Darauf folgt die unweigerlich die Frage: „Was kann bei mir schon für ein Schaden angerichtet werden?".

Ransomware

„Ransom" ist das englische Wort für Lösegeld, und genau das will der Angriff mit einer Ransomware erreichen: Die Daten auf der Festplatte werden verschlüsselt. Die Daten sind zwar noch vorhanden, aber nicht mehr zugreifbar. Und statt Eurer Dateien seht Ihr eine Aufforderung, per Bitcoin einen bestimmten Betrag zu zahlen (Lösegeld, daher der Name).

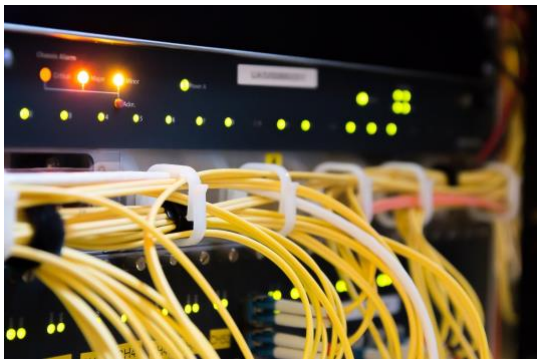
Auch wenn die Empfehlung immer wieder ist, solche Zahlungsaufforderungen zu ignorieren: Nicht wenige Anwender zahlen nicht geringe Summen für ihre Daten, die Masse der Benutzer spült einiges Geld in die Kassen der Verbrecher.

Abhilfe: Die meisten Antivirenprogramme (und auch der Windows Defender) schützen vor bekannter Ransomware. Installiert sie und haltet die Virendefinitionen immer aktuell!

So geht's leichter | Effektiver Schutz vor Hack-Attacken

Feindliche Übernahme von Hardware

Ihr selbst nutzt Eure Hardware zu bestimmten Zwecken. So leistungsfähig sie ist, so viel Schaden kann sie in den falschen Händen anrichten. Vor allem dann, wenn es sich nicht um einen, sondern um hunderte oder gar tausende von Geräten geht: DoS- (Denial of Service-) Attacken, bei denen durch gleichzeitige Zugriffe auf Webseiten oder Firmenserver Dienste blockiert und zum Absturz gebracht werden, der Betrieb von Botnetzen, in die Ihre Hardware eingebunden wird und die gemeinsame Angriffe starten oder Rechenkapazitäten für irgendwelche Zwecke einsetzen sorgen für immensen Schaden. Vielleicht nicht bei Euch selbst, aber unter Eurer unfreiwilligen Mitwirkung.



Dank Smart Home und Internet of Things hat jeder Haushalt eine riesige Menge an Geräten im Netzwerk, auch hier wieder gilt: Die Masse macht es.

Abhilfe: Kontrolliert, was Geräte in Eurem Netzwerk machen und haltet Sie immer auf dem aktuellen Softwarestand!

Datendiebstahl

Die Währung im Internet sind Eure Daten. Teile davon gebt Ihr in vielen Fällen mehr oder minder freiwillig heraus, um dafür Dienste nutzen zu können.

So geht's leichter | Effektiver Schutz vor Hack-Attacken

Haben Angreifer aber den freien Zugriff auf all Eure Daten, dann könnt Ihr damit auf Eure Kosten einkaufen, Meinungen äußern und vieles mehr in Eurem Namen machen. Je länger und detaillierter sie sich mit Euren Daten beschäftigen, desto größer wird der Schaden. Selbst der Diebstahl der kompletten Identität ist kein Einzelfall!

Abhilfe: Neben den schon genannten technischen Hilfsmitteln wie Virenschutz und Updates ist hier vor allem der Anwender gefordert: Aufmerksamkeit beim Austausch von Daten und Informationen und gesunder Menschenverstand sind die wichtigsten Helfer!

Updates, Updates, Updates

Ihr verwendet im Normalfall keine eigene, hausgemachte Lösung, sondern Standards: Windows oder macOS, Office, Cloud-Dienste, Produkte von großen Herstellern, die weit verbreitet sind.

Der große Vorteil daran: Die Hersteller haben ein Eigeninteresse daran, dass ihre Produkte sicher sind und nicht durch Datenverluste und Sicherheitslücken in der Presse auftauchen. Darum stecken diese erheblichen Aufwand in regelmäßige Updates, in denen neben neue Funktionen vor allem Sicherheitslücken und Fehler behoben werden. Gerade bei sicherheitsrelevanten Themen folgt das Update meist sehr kurz nach der Entdeckung der Lücke.

So geht's leichter | Effektiver Schutz vor Hack-Attacken

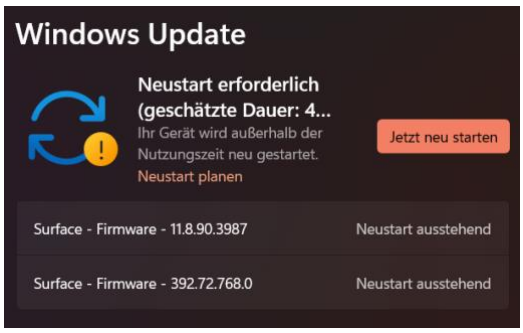
Automatische Updates des Betriebssystems

Gleich, ob Ihr Windows oder macOS nutzt: Das Betriebssystem ist der erste und wichtigste Punkt, über den Angreifer versuchen, ins System zu kommen. Gleichzeitig bietet das Betriebssystem viele übergreifende Funktionen, die das verhindern sollen. Ein immer aktuell gehaltenes Betriebssystem ist schon einmal ein guter Basisschutz.

Updates in Windows

Manuelle Prozesse sind meist nicht optimal. Sie verlassen sich auf die schwächste Komponente an unseren Rechnern: Den Menschen. Das hat auch Microsoft nach vielen Jahren erkannt und mit Windows 10 Updates quasi verpflichtend gemacht. Wo Ihr bei früheren Windows-Versionen noch dauerhaft manuell nach Updates suchen (lassen) konntet, machen Windows 10 und 11 das zwingend automatisch.

- Liegt ein Update vor, dann erscheint in der Taskleiste das Symbol 
- Ein Klick darauf öffnet das Update-Menü. Dieses kann auch durch **Einstellungen** > **Windows Update** manuell aufgerufen werden.



- Wenn ein Update einen Neustart erfordert, dann führt Windows die Installation außerhalb der festgelegten Nutzungszeit statt (dazu gleich mehr).

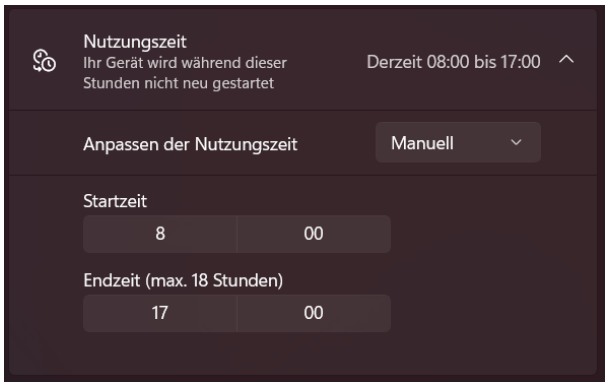
So geht's leichter | Effektiver Schutz vor Hack-Attacken

- Ein Klick auf **Jetzt neu starten** stößt die Installation des Updates direkt an. Vorsicht dabei: Vorher solltet Ihr alle Daten speichern und Programme beenden. Das stellt sicher, dass im unwahrscheinlichen Fall keine Daten verloren gehen.
- Die Installation kann mehrere Neustarts mit sich bringen, abhängig von der Komplexität des Updates.
- Nach Abschluss könnt Ihr Windows wieder normal nutzen.

Planen des Neustarts

Der optimale Zeitpunkt für ein Update ist für jeden Anwender anders. Meist aber gibt es regelmäßig Phasen, zu denen Ihr den Rechner nicht benutzt. Diese könnt Ihr individuell festlegen:

- Klickt auf **Einstellungen** > **Windows Update** > **Erweiterte Optionen** > **Nutzungszeit**.
- Im Standard legt Windows die Nutzungszeit anhand Eurer tatsächlichen Nutzung automatisch fest: Wenn Ihr zwischen 08:00 und 17:00 meist am Rechner sitzt, dann wird dieser Wert angenommen.
- Klickt auf die Schaltfläche **Automatisch** und wählt im sich öffnenden Menü **Manuell** aus.



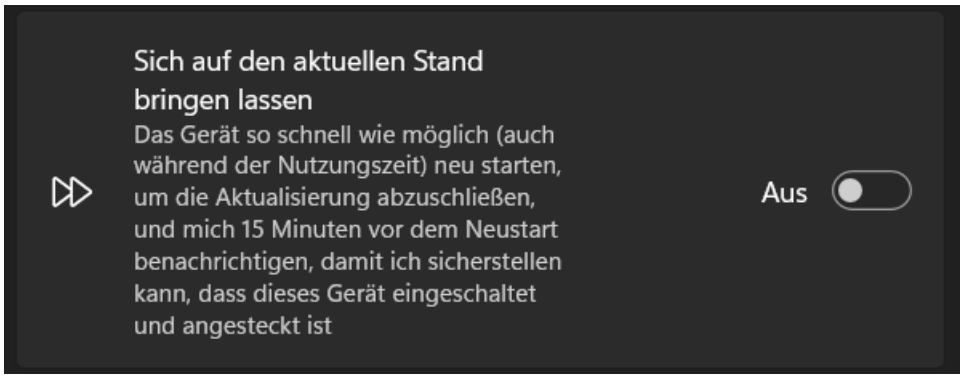
- Legt die **Startzeit** und die **Endzeit** manuell fest. Die außerhalb dieser Angaben liegenden Zeiten verwendet Windows als mögliche Update-Zeiten.

So geht's leichter | Effektiver Schutz vor Hack-Attacken

Updates noch mehr beschleunigen

Durch die verpflichtenden automatischen Updates hat Windows den Zeitraum zwischen Verfügbarkeit eines Updates und Installation deutlich verkürzt. Es geht aber noch mehr:

- Klickt auf **Einstellungen** > **Windows Update** > **Erweiterte Optionen**.
- Aktiviert den Schalter neben **Sich auf den aktuellen Stand bringen lassen**.



- Hierbei ignoriert Windows die vorgeschriebenen Nutzungszeiten und installiert Updates, sobald sie vorliegen. Einzig eine Warnung 15 Minuten vor der Aktualisierung sorgt für eine gewisse Vorwarnzeit.
- Diese Einstellung macht nur dann Sinn, wenn Ihr dringend auf ein spezifisches Update wartet!

Verschieben von Updates

Ungerne und zähneknirschend lässt Windows es dann doch zu, dass Updates verschoben werden. Der maximale Zeitraum hängt von der verwendeten Windows-Version ab. Windows 11 beispielsweise erlaubt das Verschieben von einer Woche. Das macht nur Sinn, wenn Ihr den Rechner wirklich dringend und durchgängig braucht und nicht riskieren

So geht's leichter | Effektiver Schutz vor Hack-Attacken

wollt, dass ein Update oder ein Neustart irgendetwas durcheinander bringt.

- Klickt auf **Einstellungen** > **Windows Update**.
- Unter **Weitere Optionen** findet Ihr die Option **Für 1 Woche anhalten**. Klickt diese an, dann setzt Windows die Update für eine Woche aus.
- Ihr könnte jederzeit manuell nach Updates suchen (und damit auch das Aussetzen der automatischen Updates beenden), wenn Ihr auf **Nach Updates suchen** klickt.

Automatische Updates beim Mac

Auch wenn das manchmal nicht so offensichtlich ist: Auch ein Gerät mit macOS benötigt Updates. Dabei geht es nicht nur um die neuen Versionen von macOS, die nahezu im Jahresrhythmus veröffentlicht werden, sondern viel mehr um die vielen kleineren Patches. Die beseitigen kleinere Fehler bis hin zu gefährlichen Sicherheitslücken. Es macht Sinn, diese zeitnah zu installieren. Warum nicht gleich automatisch?

- Das Vorliegen von Updates findet Ihr auf dem Mac am schnellsten, wenn Ihr auf den Apfel oben links ab Bildschirm klickt.

So geht's leichter | Effektiver Schutz vor Hack-Attacken

- Neben **Systemeinstellungen** findet Ihr die Zahl der macOS-Updates, unter **App Store** die Zahl der Apps, für die es ein Update gibt.
- Ein Klick auf einen der beiden Einträge führt direkt zu den Updates und deren manueller Installation.

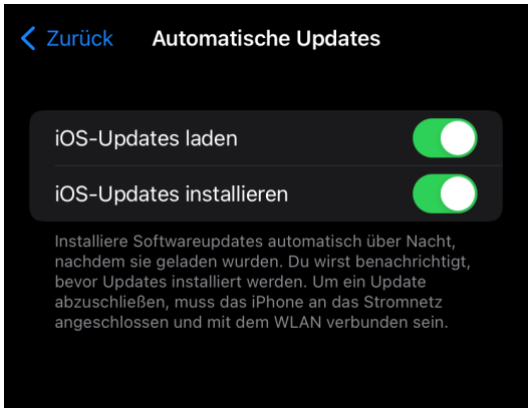
- Für macOS-Updates könnt Ihr direkt im Update-Bildschirm (oder unter **Einstellungen** > **Softwareupdate**) einen Haken neben **Meinen Mac automatisch aktualisieren setzen**. MacOS prüft dann regelmäßig auf Updates und installiert diese.
- Für App-Updates startet den App Store, klickt in der Menüleiste auf **App Store** > **Einstellungen**.

- Aktiviert dort **Automatische Updates**. Auch hier sucht der Mac automatisch nach Updates und installiert diese. Er informiert nur, wenn er die Zustimmung für Lizenzbedingungen oder ähnliches benötigt.

So geht's leichter | Effektiver Schutz vor Hack-Attacken

Updates auch für Smartphones

Auch Smartphones haben ein Betriebssystem. Ob Android oder iOS, Sicherheitslücken gibt es bei beiden Systemen. Wenn Ihr überlegt, wie viele persönliche und schützenswerte Daten Ihr auf Eurem Smartphone dabei habt, dann sind auch hier die potenziellen Schäden groß, wenn Daten verloren gehen. Also: Automatische Updates sind auch auf einem Smartphone Pflicht!



Unter iOS tippt auf **Einstellungen** > **Allgemein** > **Softwareupdate** > **Automatische Updates** > **Ein**, um die automatischen Updates zu installieren.

Bei Android tippt auf **Einstellungen** > **Geräteinformationen**" und aktiviert unter **Automatische Aktualisierung** die automatischen Updates.

Das Smartphone weist nach dem Herunterladen darauf hin, dass ein Update installiert werden soll und erlaubt es den Anwender, das zu verschieben. Durch den Neustart, der bei Smartphone-Updates Standard ist, würden Telefonate unterbrochen und Ihr wärt eine Zeit nicht erreichbar. Das könnt Ihr selbst durch verschieben der Installation beeinflussen.

Updates von Apps

Das Betriebssystem liefert die Basiskomponenten für den Schutz Eures Rechners und der Daten darauf. Ist es auf dem aktuellen Stand, dann werden schon viele Bedrohungen abgefangen.

So geht’s leichter | Effektiver Schutz vor Hack-Attacken

Den Großteil der Arbeit verbringt ein Anwender allerdings in einen Programmen und Apps. Die verwalten ihre eigenen Daten und haben weitreichende Rechte im Betriebssystem. Eine Sicherheitslücke in einer App ist nahezu so gefährlich wie eine im Betriebssystem.

Aktualisierungen von Microsoft Software

Microsoft nimmt eine Sonderstellung ein: Als Hersteller von Windows und auch des am meisten verwendeten Office-Pakets bietet es sich an, das automatische Update von Microsoft-Apps direkt in Windows zu integrieren. Leider ein wenig versteckt:

- Klickt auf **Einstellungen** > **Windows Update** > **Erweiterte Optionen**.
- Aktiviert den Schalter neben **Updates für andere Microsoft-Produkte erhalten**. Windows übernimmt jetzt parallel zu den eigenen Updates auch die Aktualisierung von Office.

Auf dem Mac wird bei der Installation von Office automatisch der Microsoft AutoUpdater installiert und prüft im Hintergrund auf Updates, die dann auch installiert werden.

Aktualisieren von Apps in Windows 11

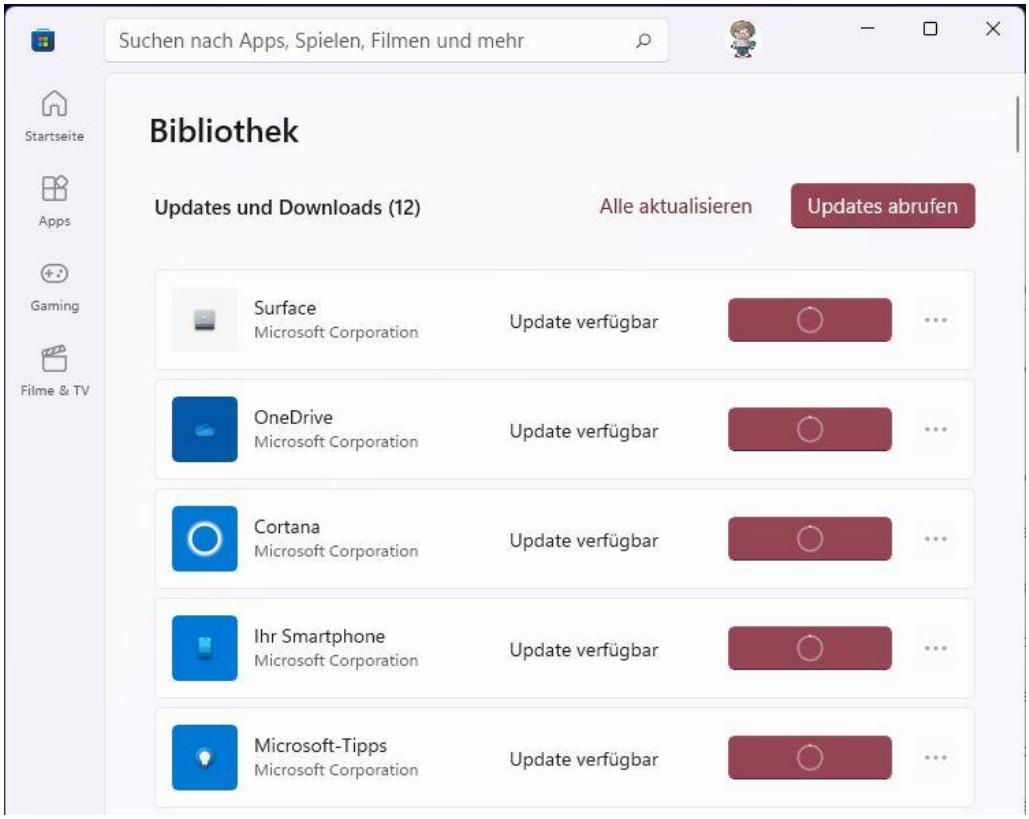
Auch Windows 11 hat einen Windows Store, aus dem Ihr Euch Apps und Spiele herunterladen oder Filme und Fernsehsendungen leihen oder kaufen können. Die Bedienung bei der Aktualisierung von Apps ist allerdings ein wenig anders als bei Windows 10.

Nicht nur Windows 11 selbst, auch die Apps aus dem Store bekommen regelmäßig Updates. Auch wenn "Never change a Running System" - ändere nie etwas, wenn alles gut läuft - manchmal als Motto durchaus seine Berechtigung hat, solltet Ihr hier davon abweichen: Die meisten

So geht's leichter | Effektiver Schutz vor Hack-Attacken

Updates mögen nicht viele neue Funktionen liefern, aber sie sorgen für mehr Stabilität und eben oft auch Sicherheit.

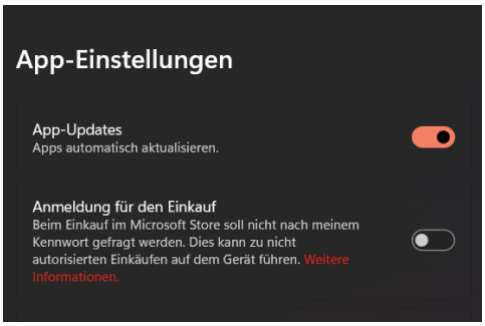
- Öffnet den Windows Store durch einen Klick auf das **Store-Symbol** im Startmenü.



- Im Gegensatz zu Windows 10 findet sich die Bibliothek - also die installierten Apps - nicht unter dem Kontobild, sondern in einem separaten Bereich.
- Unten links im Programmfenster befindet sich ein Symbol, das wie mehrere nebeneinander stehende Bücher aussieht. Ein Klick darauf öffnet die Benutzer-Bibliothek.
- Oben rechts klickt dann auf **Updates abrufen**. Der Store sucht nun nach Updates der Apps. Übrigens gehört dazu auch die Store-App, die sich selbst aktualisieren kann!

So geht’s leichter | Effektiver Schutz vor Hack-Attacken

- Nachdem die App-Updates heruntergeladen sind, könnt Ihr diese mit einem Klick aktualisieren. Es empfiehlt sich, alle laufenden Apps vorher zu beenden und damit sicherzustellen, dass alle Daten, die Ihr vielleicht darin noch bearbeitet habt, gespeichert sind!
- Um sicherzustellen, dass die Updates automatisch geladen werden, klickt in den Einstellungen der Store App auf App-Einstellungen und aktiviert den Schalter neben **App-Updates**!

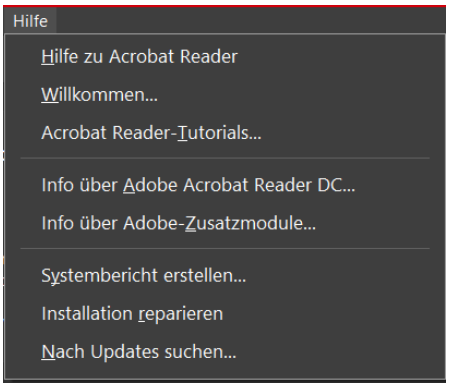


Aktualisieren anderer Apps

Ein wenig aufwändiger ist die Aktualisierung bei Apps und Programmen, die nicht direkt aus dem Microsoft- oder App Store stammen. Die offiziellen Stores haben einen Automatismus integriert, der App-Updates automatisch identifiziert und installiert. Bei anderen Programmen ist der Hersteller dafür verantwortlich. Idealerweise hat er ebenfalls einen Automatismus vorgesehen, über den das Programm aktualisiert werden kann.

So geht's leichter | Effektiver Schutz vor Hack-Attacken

- Der findet sich bei den meisten Apps unter **Hilfe** > **Nach Updates suchen**. Zum Beispiel auch beim Adobe Reader, der auf Grund seiner Funktionen immer mal wieder von Sicherheitslücken geplagt wird.



- Es empfiehlt sich dringend, die manuelle Suche regelmäßig durchzuführen. Abhängig davon, wie anfällig ein Programm sein kann und wie oft es benutzt wird.

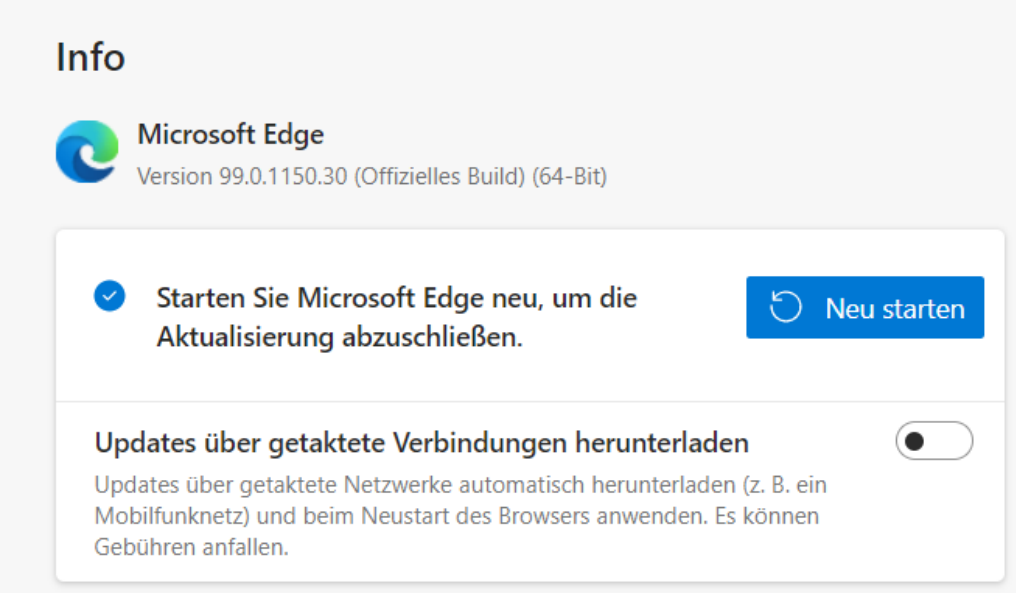
Aktualisierung des Browsers

Alle Programme aktualisiert? Sicher? Was ist mit dem Browser? Kaum zu glauben, aber wahr: Der Browser ist eines der „gefährlichsten" Programme, weil er die direkte Verbindung zur nicht immer wohlmeinenden Welt außerhalb unserer Büros herstellt. Dahin, wo sich Schadsoftware und Phishingversuche tummeln.

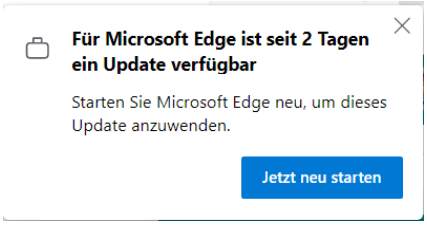
Microsoft Edge

Die Idee war gut: Windows Updates sind ein Automatismus, der auf jedem Windows-Rechner eingespielt ist: Windows sucht nach den Updates, informiert den Benutzer und installiert sie. Kaum ein manueller Eingriff, kaum Zeitverzögerung zwischen Verfügbarkeit und Installation. Die zunehmenden Angriffe aus dem Internet aber haben hier eine Anpassung des Prozesses bewirkt: Sicherheitslücken im Browser werden rasend schnell ausgenutzt, jeder Anwender ist potenziell betroffen. Auf der anderen Seite lässt sich der Browsers eigenständige App schneller aktualisieren. Die Konsequenz: Edge hat einen eigenen Update-Mechanismus. Den könnt - und solltet - Ihr beeinflussen!

So geht’s leichter | Effektiver Schutz vor Hack-Attacken



- Im drei-Punkte-Menü von Edge unter **Einstellungen** > **Infos zu Microsoft Edge** > **Info** findet Ihr den aktuellen Stand der Version von Edge.
- Edge sucht automatisch nach Updates, wenn Ihr den Bildschirm öffnet. Wird ein Update gefunden, dann zeigt Edge es an und es kann über einen Klick auf **Jetzt neu starten** installiert werden.



Das Programm sucht selber in regelmäßigen Abständen nach Updates. Wird eines gefunden, dann zeigt Edge eine Meldung und einen Infotext in den Einstellungen an. Reagiert darauf und wendet das Update durch einen Klick auf **Jetzt neu starten** an. Je schneller ein Update installiert wird, desto sicherer surft Ihr im Internet!

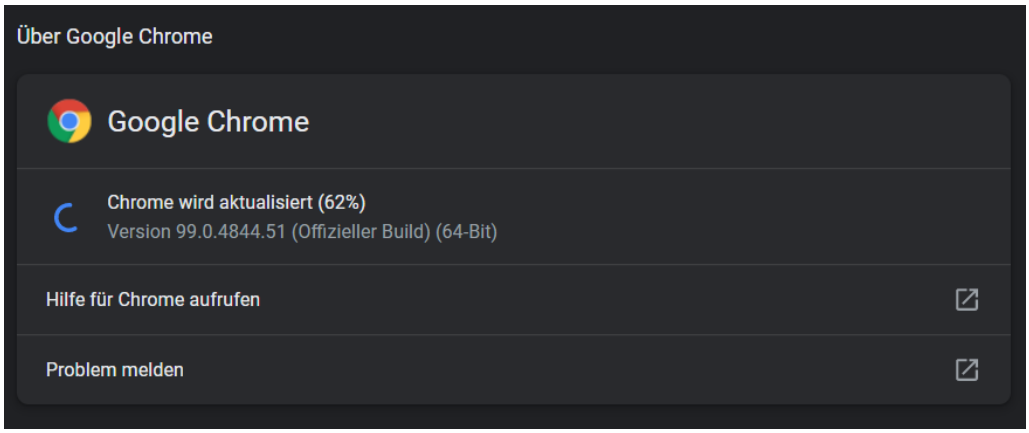
So geht’s leichter | Effektiver Schutz vor Hack-Attacken

Mozilla Firefox

Auch Firefox sucht automatisch nach Updates. Das könnt Ihr beschleunigen, indem Ihr auf das Hamburger-Menü, dann auf **Hilfe** > **Über Firefox** klickt. Firefox Installiert das Update und beim Neustart habt Ihr direkt die neue Version zur Verfügung.

Google Chrome

Auch Google Chrome lässt sich über denselben Weg durch die Menüs aktualisieren:



So geht's leichter | Effektiver Schutz vor Hack-Attacken

Aktualisieren der Hardware

Updates scheinen das Allheilmittel zu sein, wenn es um die Beseitigung von Sicherheitslücken geht. Windows, Apps, die Smartphones, das sind die Kandidaten, die sofort einfallen. Dabei gehen oft zwei Kategorien von Geräten komplett unter, die für eine Vielzahl von Sicherheitslücken verantwortlich sind: Der Router, der den Internetzugang herstellt, und die kleinen, mit dem Internet verbundenen Geräte wie Webcams, Netzwerkfestplatten etc.

Sicherheit auf dem Router

Der Internetzugang findet nicht auf dem Rechner statt, sondern klassischerweise auf dem Router. Den bekommt der Anwender meist vom Internet-Anbieter gestellt, manchmal kauft er ihn auch selbst. Hier gibt es einige Stellschrauben, die Ihr in jedem Fall verwenden solltet, um nicht schon ganz vorne in der Kette ein Risiko einzugehen.

Ändern des Kennwortes

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

- Wenn Ihr Euch an Euren Router angemeldet habt, dann findet Ihr bei den allermeisten

So geht's leichter | Effektiver Schutz vor Hack-Attacken

Produkten im Menü einen Link, unter dem Ihr mit Klick auf ein eigenes Passwort vergeben könnt.

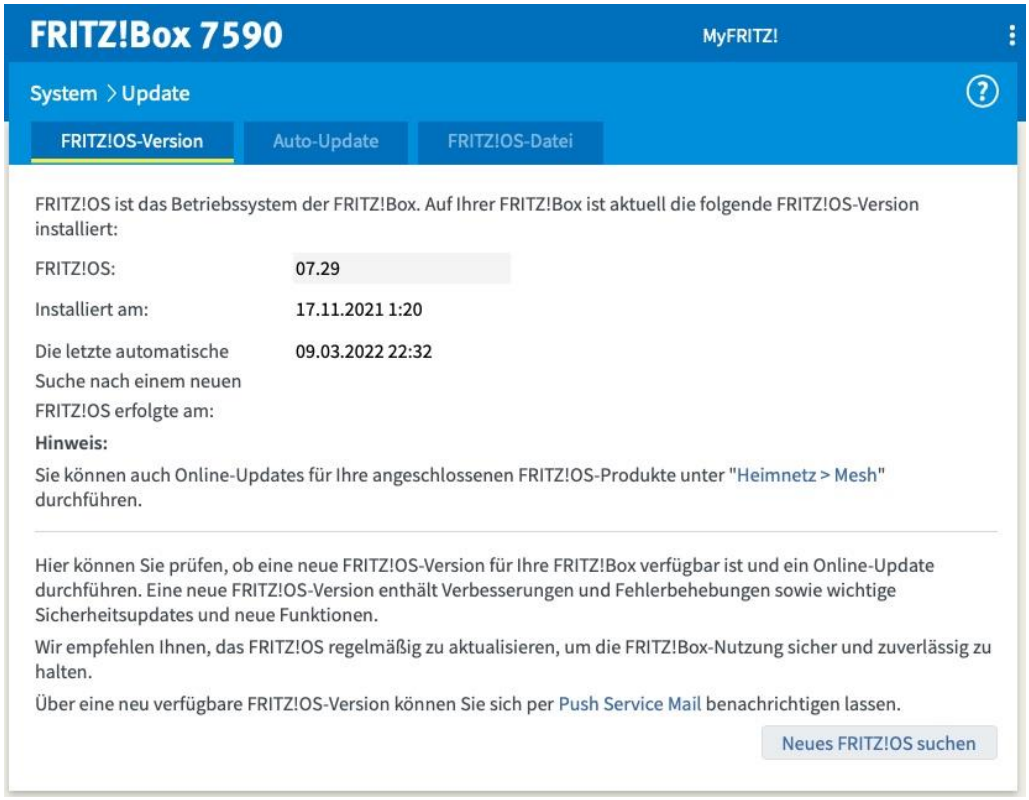
- Macht Euch – wie bei allen Passwörtern – ein wenig Gedanken darüber. Es sollte nicht zu leicht zu erraten sein, aber auch nicht so schwer, dass Ihr es Euch nicht merken könnt!
- Dieses Kennwort sollte einmalig sein, also nicht noch bei einem anderen Konto im Internet Verwendung finden. Angreifer versuchen oft, verschiedene Adressen im Internet aufzurufen und dann Benutzername/Kennwort aus gestohlenen Datenbanken durchzuprobieren.

Aktualisierung des Routers

Ebenfalls ein wichtiger Schritt: haltet die Firmware, also die interne Software aller Geräte immer aktuell. Es kommen immer wieder Sicherheitslücken ans Licht, die die Hersteller dann sehr schnell durch ein Update beseitigen. So ein Update hilft aber nichts, wenn es nicht installiert wird.

- Sucht also regelmäßig bei allen mit dem Internet verbundenen Geräten in den **Einstellungen** unter **System** nach einem Update.
- Wird eine neue Version der Software gefunden, dann installiert sie.

So geht’s leichter | Effektiver Schutz vor Hack-Attacken



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

Automatische/externe Installation

Wenn Ihr Updates ungesehen und so schnell wie möglich installieren wollt, dann ist die automatische Installation eine Alternative.

So geht's leichter | Effektiver Schutz vor Hack-Attacken

- Bei den meisten Routern lässt sich das in den Systemeinstellungen aktivieren.
- Dazu meldet Euch an der Adminoberfläche des Routers an und klickt im Menü auf **System**.
- Darunter findet sich meist ein Menüpunkt **Aktualisierung** oder **Update**. Hier lassen sich neben den Statusinformationen über die aktuelle Softwareversion des Routers und der neuesten verfügbaren auch festlegen, dass der Router Updates automatisch suchen und installieren soll.

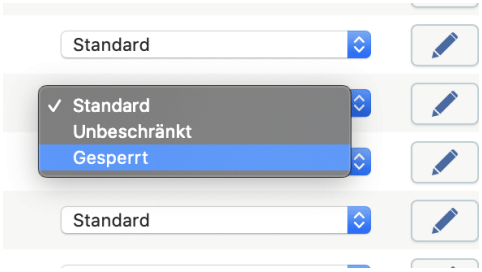
Manchmal funktioniert das nicht und der Router verweigert die Suche mit einer abstrusen Fehlermeldung wie "Update nicht möglich, überprüfen Sie die Internetverbindung!". In einem solchen Fall könnt Ihr die Firmwaredatei vom Hersteller herunterladen (bei der AVM Fritz!Box zum Beispiel hier) und manuell installieren.

Abkoppeln von Geräten im Router

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

So geht's leichter | Effektiver Schutz vor Hack-Attacken

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



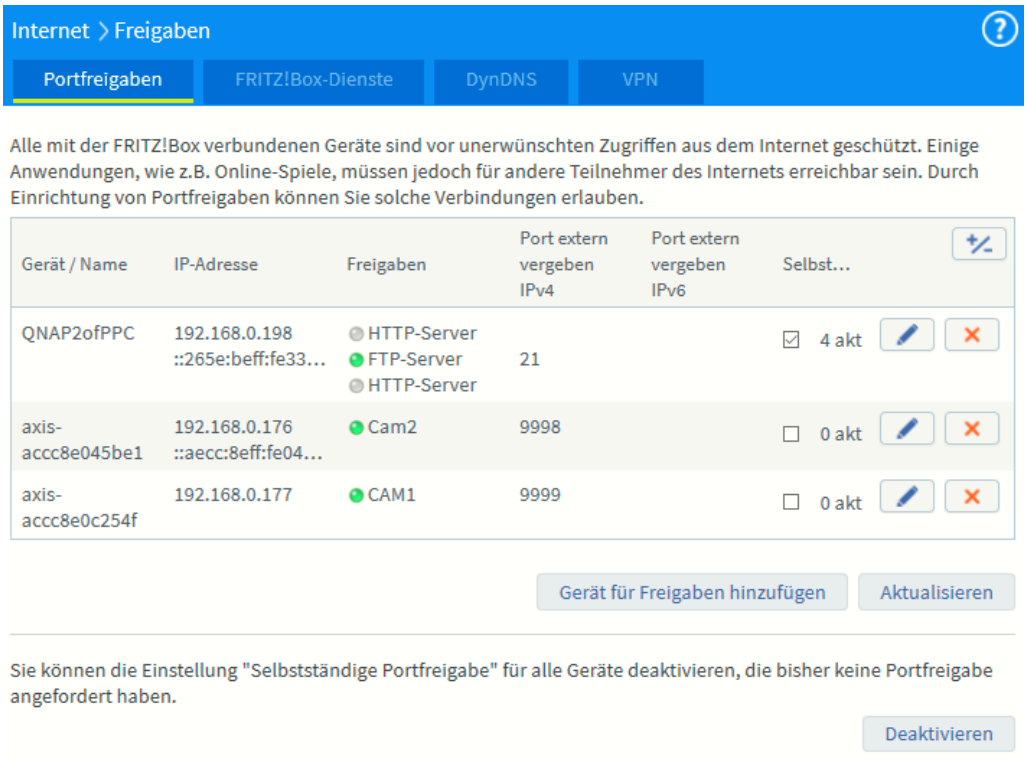
- Um nun den Internetzugang zu sperren, wechselt neben dem Gerät in der Auswahlliste von **Standard** zu **Geperrt**. Bei der nächsten Verbindung zum Router unterbindet dieser, dass das Gerät ins Internet kommt.
- Wenn Ihr stattdessen feiner einschränken wollt und beispielsweise nur für bestimmte Zeiträume den Zugriff erlauben oder unterbinden wollt, dann klickt auf den Stift neben dem Gerät und gebt die genauen Zeiträume und das Verhalten ein.

Portfreigaben im Router

Für manche Anwendungen kann es sinnvoll sein, Zugriff aus dem Internet auf ein Gerät im Netzwerk zu erlauben. Die Netzwerkfestplatte, auf die Ihr per FTP zugreifen wollt, die Webcam, die Euch auch unterwegs den Garten zeigen soll und vieles mehr ist denkbar. Auch hier ist der Router der Ansatzpunkt.

So geht's leichter | Effektiver Schutz vor Hack-Attacken

- Unter **Internet** -> **Freigaben** findet Ihr die bereits bestehenden Freigaben. Diese funktionieren wie ein Verteiler: Kommt eine Verbindung von außen an den Router, dann geht diese über einen so genannten Port, einen virtuellen Anschluss des Routers. (https://de.wikipedia.org/wiki/Liste_der_standardisierten_Ports)
- Im Router legt dann fest, an welches Gerät die Verbindung geleitet werden soll. Beispielsweise einer Anfrage über Port 25, der für FTP-Verbindungen genutzt wird, an die IP-Adresse der Netzwerkfestplatte.

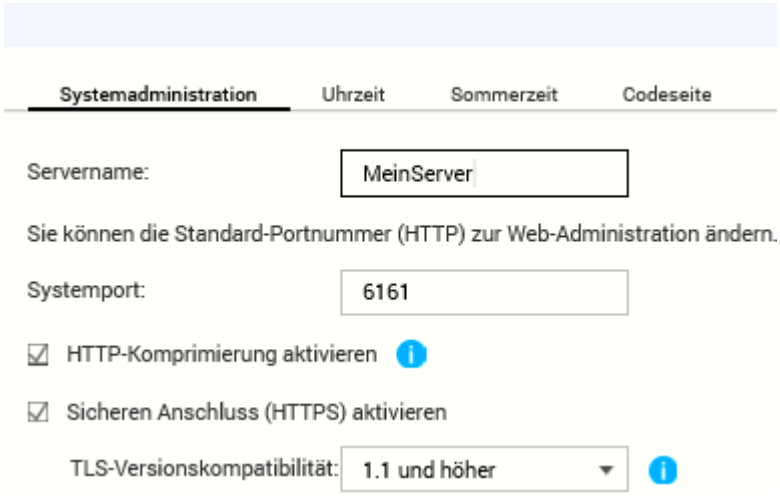


- Kontrolliert sehr genau, ob die aktuell eingerichteten Freigaben nötig und aktuell sind. Löscht umgehend jede Freigabe, die nicht mehr benötigt wird!

So geht's leichter | Effektiver Schutz vor Hack-Attacken

Weg von den Standardports

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



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

Geräte nach IP-Adresse finden

Irgendein Gerät treibt Unsinn im Netzwerk. Ihr habt die IP-Adresse, aber damit immer noch nicht das Gerät. Die AVM Fritz!Box und andere Router helfen hier!

Als Anwender ist man von den dauernden Hiobsbotschaften rund um Viren, Hacks und Datenlöcher sensibilisiert. Manchmal sogar

So geht's leichter | Effektiver Schutz vor Hack-Attacken

übersensibilisiert: Jede kleine Fehlermeldung über eine vermeintlich unnormale Aktivität am eigenen PC, Mac oder im Netzwerk sorgt für einen Schreck und ein unwohles Gefühl.

XBOX	LAN 4 mit 1 Gbit/s	192.168.0.158	
PC-192-168-0-156	WLAN verbunden mit Buero	192.168.0.156	5 GHz, 43 / 72 Mbit/s
iPhone-von-Andreas	WLAN verbunden mit Buero	192.168.0.155	5 GHz, 780 / 144 Mbit/s
Andreass-iPadPro129	WLAN verbunden mit Buero	192.168.0.154	5 GHz, 650 / 78 Mbit/s
MBP-M1Pro	WLAN	192.168.0.151	5 GHz, 650 / 526 Mbit/s
dda5852c-6a45-408d-8e8b-df70f5e15399	WLAN verbunden mit Buero	192.168.0.143	5 GHz, 520 / 234 Mbit/s
Lukas-iPad-Kindle	WLAN verbunden mit Buero	192.168.0.141	5 GHz, 780 / 468 Mbit/s
none-22	WLAN	192.168.0.140	2,4 GHz, 52 / 65 Mbit/s
iPad-Niklas-neu	WLAN verbunden mit Buero	192.168.0.136	5 GHz, 780 / 585 Mbit/s

Ein Netzwerk ist vollkommen einfach strukturiert. Das heißt wie so oft leider aber auch: Nicht wirklich sprechend und komfortabel! Geräte identifizieren sich nicht mit ihrem Namen, sondern mit der Netzwerkadresse, IP-Adresse genannt. Die ist eine Kombination aus mehreren Ziffernkolonnen, die quasi eine Wegbeschreibung der Datenpakete ermöglichen. Meist hat der Router im heimischen Netzwerk die IP-Adresse 192.168.0.1, ein Gerät die Adresse 192.168.0.151. Jede IP-Adresse ist zu einem Zeitpunkt nur einmal vergeben, gibt aber in ihrer ursprünglichen Form keine Auskunft darüber, welches Gerät sie gerade verwendet.

Viele Geräte identifizieren sich auch mit ihrem Namen im Netzwerk, die Zuordnung zwischen IP und Namen kann nur der Router herstellen. Bei

So geht's leichter | Effektiver Schutz vor Hack-Attacken

eine Meldung "192.168.0.151 betrachtet gerade Ihren Bildschirm" ist erst einmal keine Panik nötig.

- Ruft die Konfigurationsoberfläche des Router auf und wechselt dort in die Netzwerkeinstellungen/die Netzwerkübersicht.
- Da steht in der einen Spalte die IP-Adresse, in einer anderen aber auch gleich der Name des Gerätes.
- Der muss nicht immer sprechend sein. Im vorliegenden Fall zeigt sich aber schnell, dass es sich um ein Macbook Pro handelt.
- Mit der Information lässt sich schnell identifizieren, ob das Gerät ein Recht hat, den eigenen Bildschirm zu beobachten oder nicht.

Solltet Ihr immer noch unsicher sein, dann deaktiviert das Gerät wie im vorigen Abschnitt beschrieben. Achtet genau darauf, ob und was dann nicht mehr funktioniert, vielleicht ist es doch ein nützliches oder wichtiges Gerät!

Das Internet of Things (IoT)

Kaum ein Gerät ist heutzutage noch ohne Internetverbindung. Kühlschrank, WebCam, Kinderspielzeug, Alexa und Apple HomePod, alle verbinden sich mit dem WLAN und funken munter Informationen ins Netz.

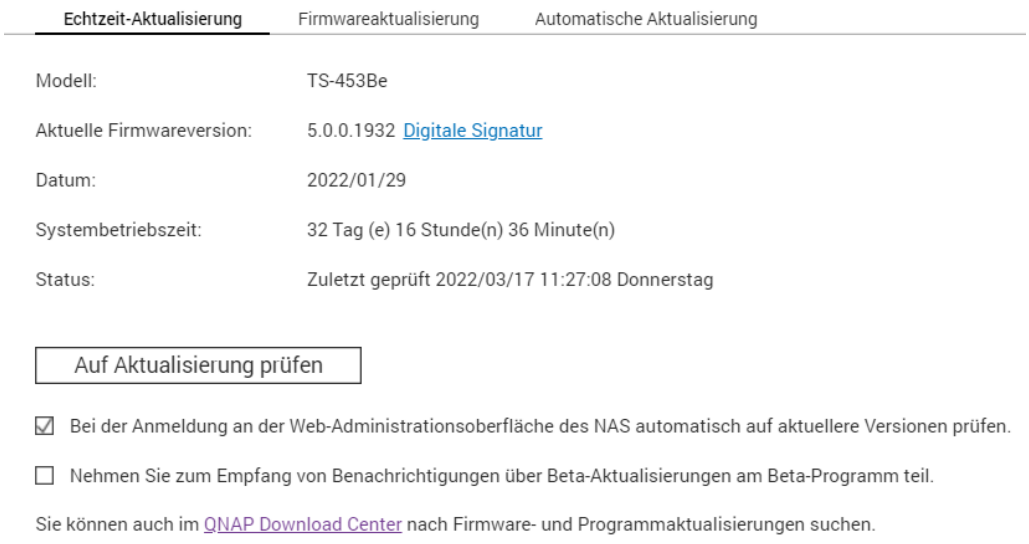
Auf der einen Seite solltet Ihr regelmäßig (wie im vorigen Abschnitt beschrieben) prüfen, ob alle Geräte in Eurem Netzwerk überhaupt da sein sollen/müssen und ins Internet dürfen.

Zum anderen gilt aber auch hier: Updates sind extrem wichtig: Jedes dieser Geräte hat ein eigenes Betriebssystem. Und jedes Betriebssystem hat Sicherheitslücken, die durch Updates behoben werden. Ein nicht

So geht's leichter | Effektiver Schutz vor Hack-Attacken

geringer Anteil der Geräte in Botnetzen sind Webcams, Babyphone und andere „normale" Geräte.

- Die Aktualisierung könnt Ihr auf der Weboberfläche des Gerätes durchführen.
- Wie Ihr diese aufruft, findet Ihr in der Anleitung.
- Nutzt dann auch gleich die Möglichkeit, das Standard-Passwort zu ändern. Das ist meist bei allen Geräten desselben Typs gleich und der erste Versuch, wenn ein Angreifer ein solchen Gerät im Netz findet.



Phishingangriffe vermeiden

Schutz vor Malware und Ausspähung folgt einer gewissen Systematik: Ihr habt eine App installiert, die die Dateien auf dem Rechner scannt. Die prüft Codemuster in den Dateien gegen eine Liste bekannter Viren und warnt, wenn sie eine (vermeintlich) infizierte Datei findet.

So geht’s leichter | Effektiver Schutz vor Hack-Attacken

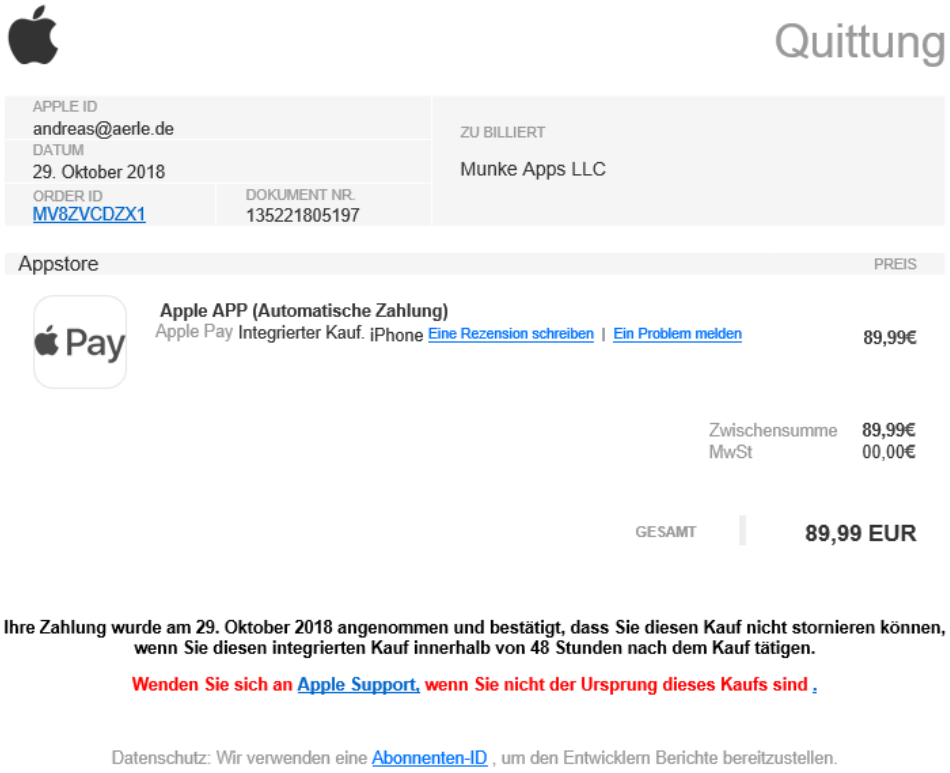
Wofür es keine App gibt, das ist das natürliche Vertrauen darauf, dass eine Mail von Apple oder Amazon oder ein Anruf von Microsoft schon echt sein werden. Das ist leider aber nicht immer der Fall!

Phishing: Vertrauen kann schaden

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 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 Ihr geleitet werden, nicht echt. Und so hat unversehens ein Fremder Eure Zugangsdaten und kann fröhlich Bestellungen auslösen, das Konto übernehmen und Schaden anrichten: Eine klassische Phishing-Attacke.

So geht’s leichter | Effektiver Schutz vor Hack-Attacken



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€

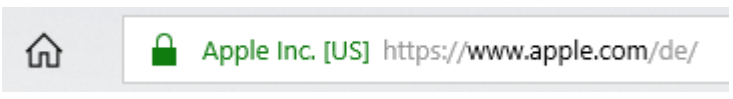
GESAMT 89,99 EUR

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: Klickt auf keine Links in solchen E-Mails. Ruft manuell die Webseite des Händlers auf und meldet Euch sich an. Damit könnt Ihr vermeiden, dass Ihr auf eine falsche Seite geleitet werdet.
- Wenn Ihr bereits versehentlich auf den Link geklickt habt, dann kontrolliert unbedingt die Adresse, die 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

So geht's leichter | Effektiver Schutz vor Hack-Attacken

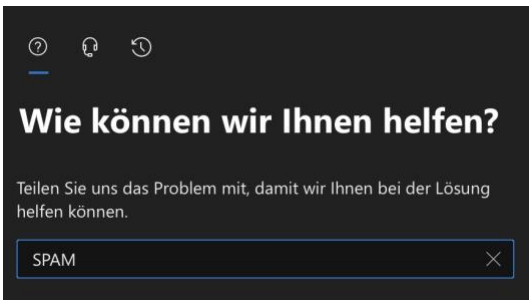
Adressen sind ein nahezu sicheres Zeichen für einen Betrugsversuch.

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 Eurem Rechner gibt und man bietet ganz selbstlos Hilfe an. Das nennt man „Tech Support SCAM".

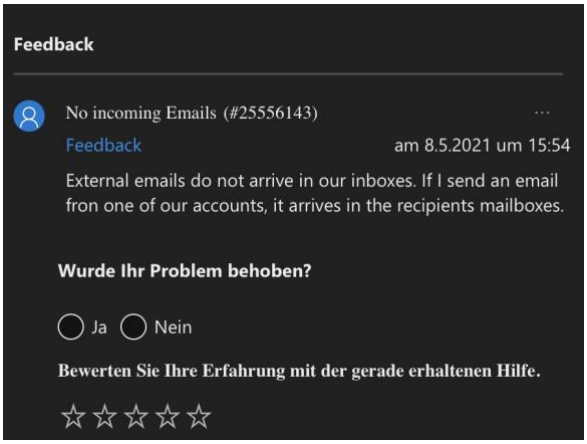
Dazu müsst Ihr nichts mehr machen als dem Anrufer durch Aufruf einer Webseite oder Fernwartungssoftware Zugang zum Rechner geben, am besten noch unter Preisgabe der eigenen Zugangsdaten. Ist das geschehen, dann behebt der Bösewicht natürlich nicht etwaige Probleme auf dem Rechner, ganz im Gegenteil: Er schließt den Benutzer aus dem Rechner durch Änderung des Passwortes aus, und verlangt dann Geld dafür, ihn wieder hineinzulassen. Oder er schleust Schadsoftware ein, die ihm dann die Fernsteuerung des Rechners und den Zugriff auf die Daten erlaubt.

- Gerade im Beispiel von Microsoft ist ein Anruf immer ausgelöst von einem Ticket, das Ihr selbst selber aufmachen müsst.



So geht's leichter | Effektiver Schutz vor Hack-Attacken

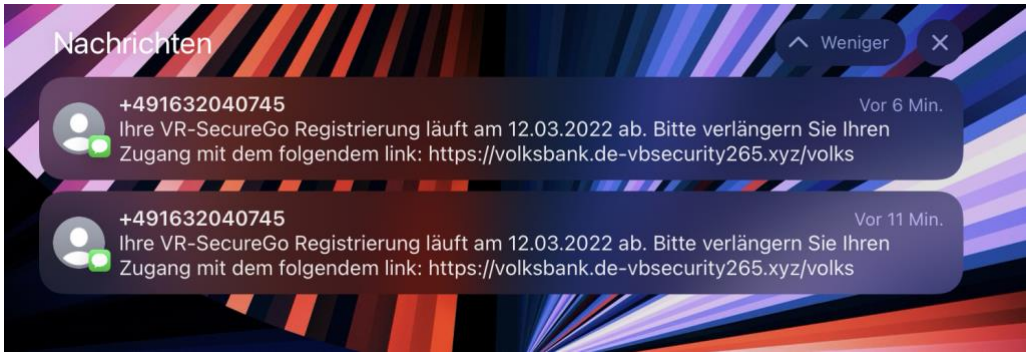
- Wenn Ihr Microsoft 365-Kunde seid, dann meldet Euch dazu am Admin-Center an. Dort klickt auf das Fragezeichen oben rechts und gebt eine Beschreibung des Problems an.
- Das System stellt jetzt automatisch verschiedene Lösungsmöglichkeiten zur Verfügung. Wenn diese nicht helfen, dann könnt Ihr auf das 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 Ihr das Ticket zu den deutschen Geschäftszeiten aufmacht, dann findet der Kontaktversuch auch auf Deutsch statt. Im Ticket könnt Ihr sogar live verfolgen, dass Microsoft gerade anruft!



Soziale Netzwerke, WhatsApp, SMS

Ihr nutzt keine E-Mails? Macht nichts. Facebook, WhatsApp, SMS und iMessage: Die Wege, auf denen Phishingversuche an Euch herangetragen werden, sind vielfältig.

So geht’s leichter | Effektiver Schutz vor Hack-Attacken

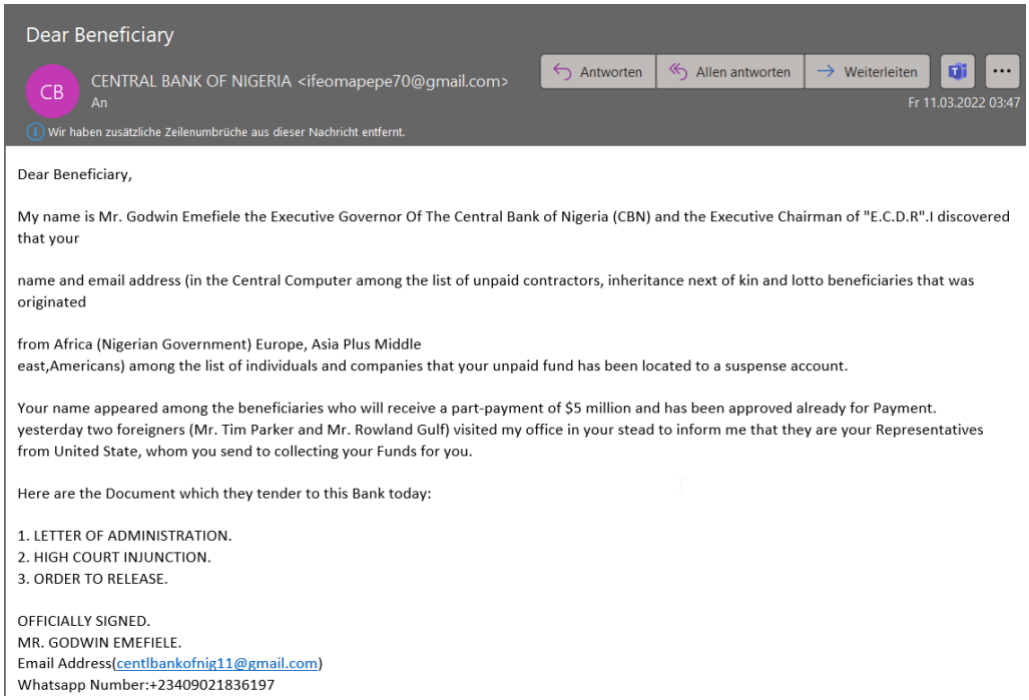


Eure Handynummer ist nicht ganz so geheim, wie sie es vielleicht sein sollte. Aus diversen Datenlecks ausgelesen wird sie verwendet, um Eure Daten zu kompromittieren.

Meist kommen die Anfragen von fremden Telefonnummern, die Ihr nicht in Euren Kontakten gespeichert habt. Auch hier gilt: Ignoriert die Nachrichten. Wenn Euch darin ein Sicherheitsvorfall wie ein geknacktes Konto oder ein kompromittiertes Passwort gemeldet werden, ruft wieder manuell – und nicht über den Link in der Nachricht – die betroffene Webseite auf. Meist stellt Ihr erleichtert fest, dass alles in Ordnung ist.

Und Ihr müsst tapfer sein: Die fünf Millionen Dollar, die die nigerianische Bank Euch aus dem Nachlass eines unbekannten Gönners verspricht, werdet Ihr auch nie bekommen!

So geht's leichter | Effektiver Schutz vor Hack-Attacken



Dear Beneficiary

CB CENTRAL BANK OF NIGERIA <ifeomapepe70@gmail.com>
An

Antworten | Allen antworten | Weiterleiten

Fr 11.03.2022 03:47

Wir haben zusätzliche Zeilenumbrüche aus dieser Nachricht entfernt.

Dear Beneficiary,

My name is Mr. Godwin Emefiele the Executive Governor Of The Central Bank of Nigeria (CBN) and the Executive Chairman of "E.C.D.R".I discovered that your

name and email address (in the Central Computer among the list of unpaid contractors, inheritance next of kin and lotto beneficiaries that was originated

from Africa (Nigerian Government) Europe, Asia Plus Middle
east,Americans) among the list of individuals and companies that your unpaid fund has been located to a suspense account.

Your name appeared among the beneficiaries who will receive a part-payment of $5 million and has been approved already for Payment.
yesterday two foreigners (Mr. Tim Parker and Mr. Rowland Gulf) visited my office in your stead to inform me that they are your Representatives from United State, whom you send to collecting your Funds for you.

Here are the Document which they tender to this Bank today:

1. LETTER OF ADMINISTRATION.
2. HIGH COURT INJUNCTION.
3. ORDER TO RELEASE.

OFFICIALLY SIGNED.
MR. GODWIN EMEFIELE.
Email Address(centlbankofnig11@gmail.com)
Whatsapp Number:+23409021836197

Ransomware und mehr: Die Erpressung

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

Der Erpressungs-E-Mail

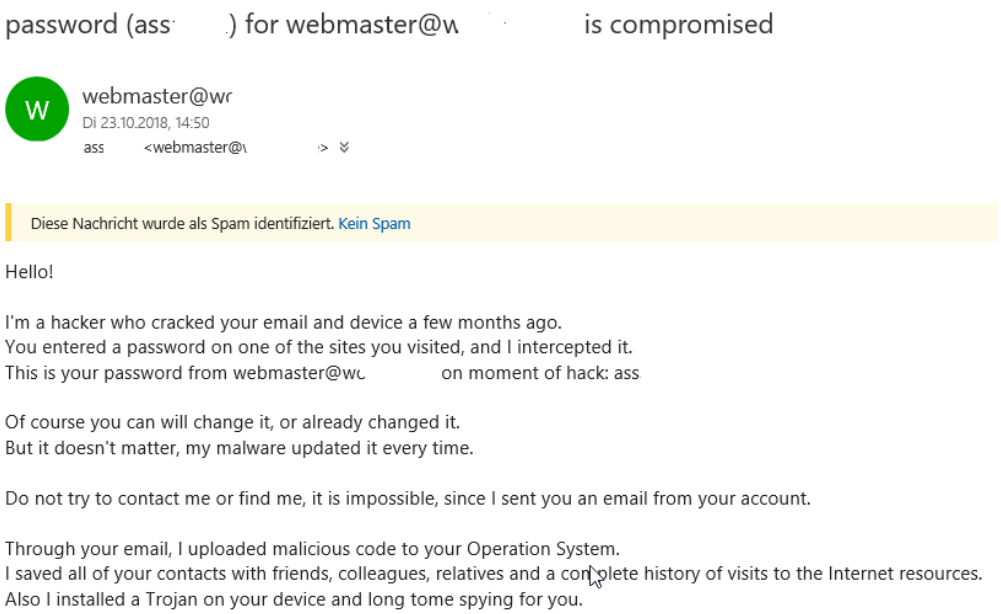
Habt Ihr auch schon einmal die Mail bekommen, dass der E-Mail-Account gehackt wurde und das mit einer richtigen E-Mail-Adresse und einem korrekten Passwort?

Diese vermeintlich authentische E-Mail fordert Euch dann auf, ganz schnell einen bestimmten Betrag in Bitcoins zu beschaffen und an den

So geht's leichter | Effektiver Schutz vor Hack-Attacken

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. Überweist nichts… aber prüft natürlich, ob das Kennwort tatsächlich noch aktuell ist und ändert es.



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

Ransomware: Verschlüsselter Rechner

Deutlich schlimmer ist es, wenn Ihr Euch eine Ransomware (einen Verschlüsselungstrojaner) eingefangen habt. Das ist eine Schadsoftware, die Dateien auf dem PC verschlüsselt und diese nur gegen Zahlung einer teils heftigen Gebühr wieder entschlüsselt. Zumindest ist das das

So geht's leichter | Effektiver Schutz vor Hack-Attacken

Versprechen, was die Ransomware in der Meldung auf Ihrem Bildschirm anzeigt.

Eine Garantie dafür habt Ihr 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.

Identifikation der Ransomware

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

Das geht in den allermeisten Fällen, weil der Natur der Erpressung nach der Browser benötigt wird, damit die Überweisung in Bitcoins ausgeführt werden kann. Wenn Ihr die Ransomware identifizieren konntet, dann findet Ihr darin meist eine wichtige Empfehlung: Ob Ihr den Rechner herunterfahren oder ihn laufen lassen sollt.

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

Beheben der Schäden

Um weitere Hilfe zu bekommen, könnt Ihr 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 Ihr als nächstes machen solltet.

So geht's leichter | Effektiver Schutz vor Hack-Attacken

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

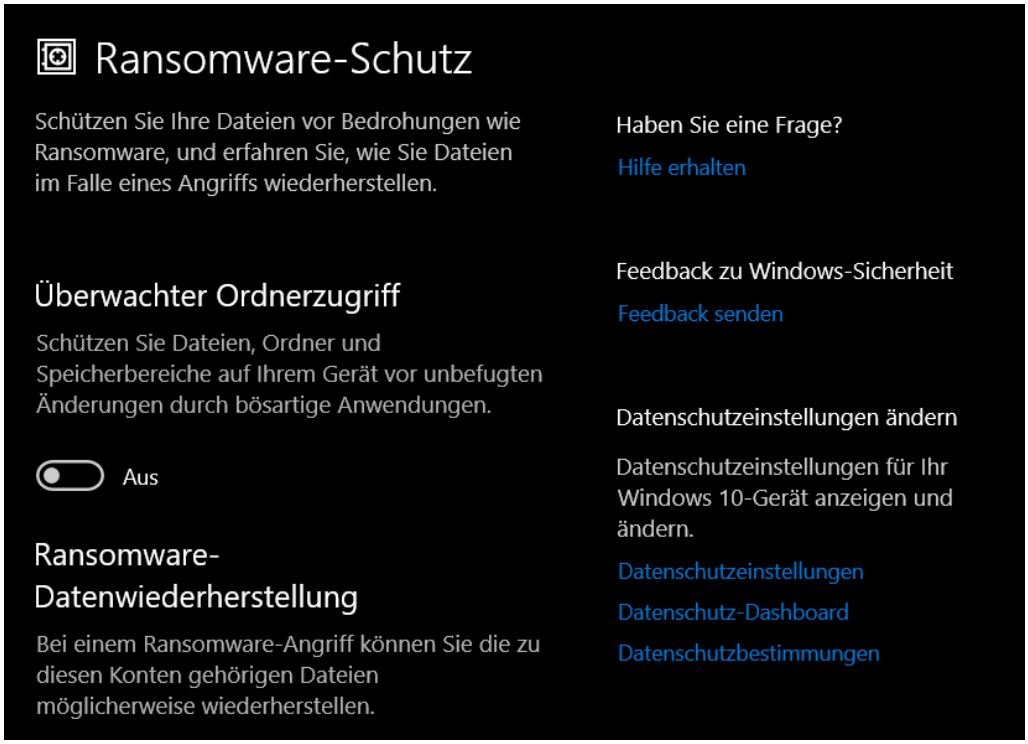
Das alleine ist allerdings nur ein Teil der Gegenmaßnahmen. Dieser nützt nur kurzfristig, wenn Ihr die Ransomware selber nicht loswerdet. Das kann durch eine Antivirensoftware geschehen, die Ransomware als Virus erkennen sollte.

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

Schutz vor Ransomware in Windows 11

Windows 11 hat einen eigenen Ransomware-Schutz integriert. Dieser ist nur dann verfügbar, wenn keine Sicherheitssoftware erkannt wird, die diese Funktion übernimmt.

So geht's leichter | Effektiver Schutz vor Hack-Attacken



- Klickt auf **Einstellungen** > **Datenschutz und Sicherheit** > **Windows-Sicherheit** > **Viren- & Bedrohungsschutz**
- Dort könnt Ihr in den Einstellungen den **Überwachten Ordnerzugriff** aktivieren. Ihr könnt 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.

Der Browser als Frühwarnsystem

Hinter allen Browsern stehen große Hersteller, für die das Thema Sicherheit extrem wichtig ist: Schwindet das Vertrauen der Anwender, dann verringert sich der Marktanteil und damit die eigene Bedeutung.

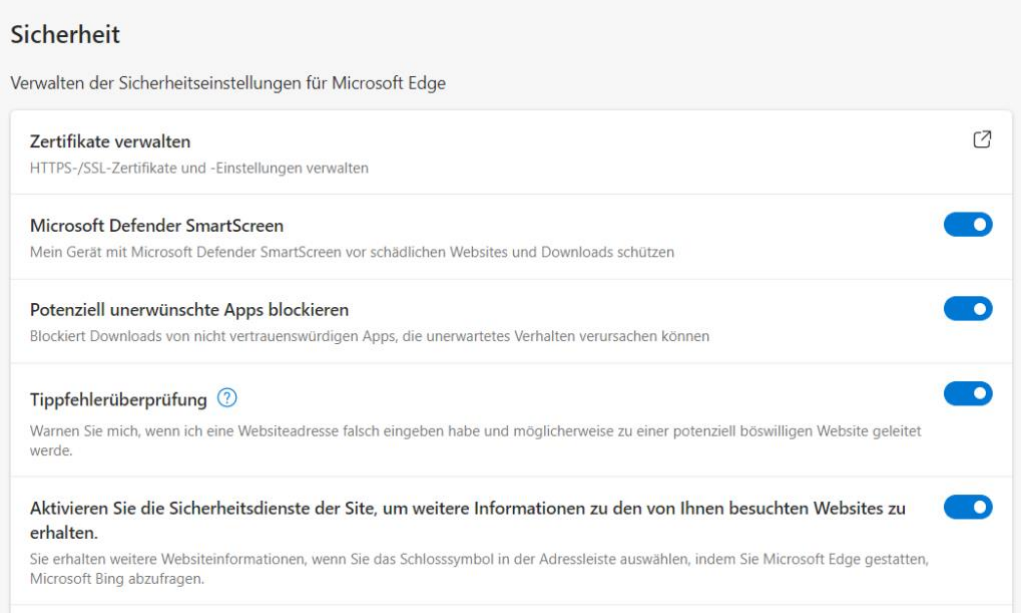
So geht’s leichter | Effektiver Schutz vor Hack-Attacken

In der Folge haben alle bekannten Browser eigene Mechanismen an Bord, die Euch vor betrügerischen Webseiten und Phishingversuchen schützen sollen. Ihr müsst sie nur aktivieren und nutzen!

Microsoft Edge

Einmal mehr hat Microsoft es einfacher als andere Hersteller: Man nutzt einfach die Mechanismen, die sich auch für Windows als Betriebssystem bewährt haben.

- In Edge klickt Ihr auf die **drei Punkte** oben rechts > **Einstellungen** > **Datenschutz, Suche und Dienste**.
- Rollt ganz nach unten in den Bereich Sicherheit, dort finden sich zwei wichtige Optionen.



- **Microsoft Defender Smartscreen** nutzt den Cloud-Service von Microsoft, in dem Informationen von Benutzern aus der ganzen Welt zusammen laufen und aktuelle Phishing-Attacken sammeln, analysieren und die Browser der Benutzer dagegen wappnen.

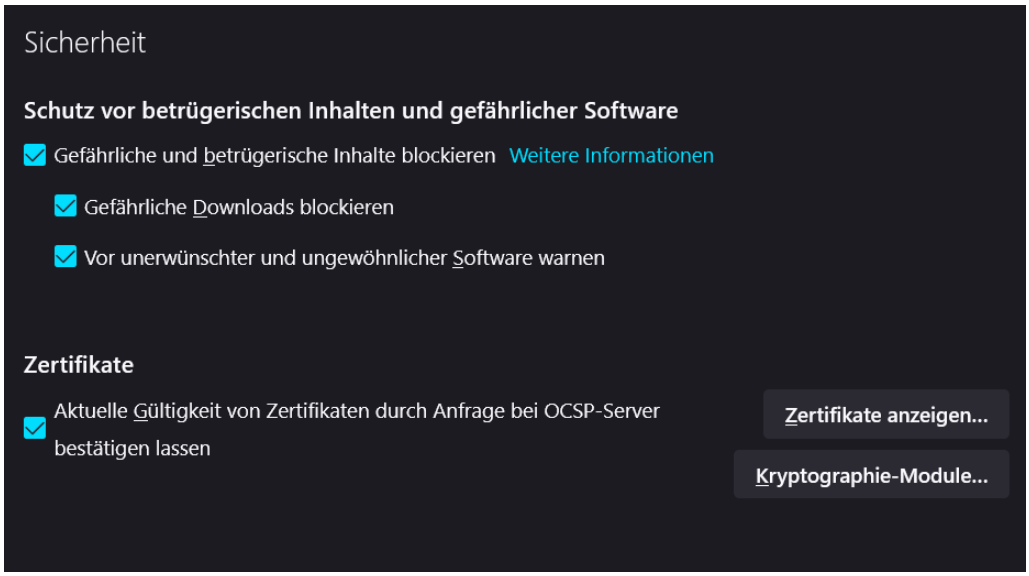
So geht's leichter | Effektiver Schutz vor Hack-Attacken

- **Potenziell unerwünschte Apps blockieren** verhindert den versehentlichen oder absichtlichen Download von Apps, die Schaden verursachen oder das System instabil machen können.
- Aktiviert beide Optionen, um Euch zu schützen!

Mozilla Firefox

Auch Firefox bietet entsprechende Schutzfunktionen:

- Klickt auf das **Hamburgermenü** oben rechts > **Einstellungen** > **Datenschutz & Sicherheit**.
- Rollt ganz nach unten in den Bereich Sicherheit, dort befindet sich die Option **Gefährliche und betrügerische Inhalte blockieren**. Aktiviert darunter beide Punkte.

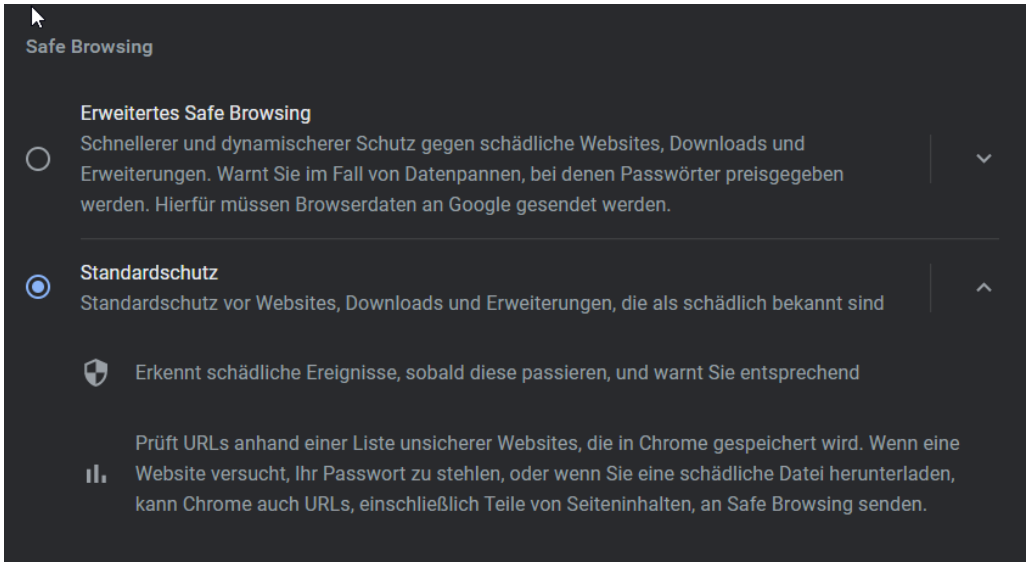


- Zusätzlich Aktiviert den **Zertifikatscheck**. Der sorgt dafür, dass die Zertifikate, die die Vertrauenswürdigkeit von Webseiten sicherstellen, noch einmal unabhängig bestätigt werden.

So geht's leichter | Effektiver Schutz vor Hack-Attacken

Google Chrome

Google Chrome nutzt wie Microsoft Edge die Chromium Engine als Basis, trotzdem sind die Anti-Phishing-Optionen ein wenig anders:



- Klickt auf die **drei Punkte** oben rechts > **Einstellungen** > **Datenschutz & Sicherheit**.
- Rollt nach unten zu **Safe Browsing**.
- Neben dem **Standardschutz** bietet Chrome auch noch das **Erweiterte Safe Browsing**, das ein Cloud-Lösung ähnlich dem SmartScreen von Microsoft, verwendet. Dazu müsst Ihr allerdings zustimmen, dass detailliertere Informationen an Google geschickt werden.

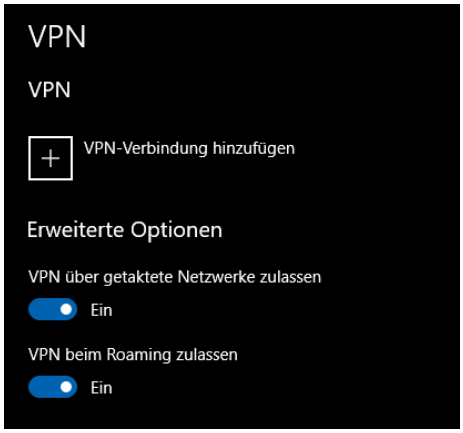
So geht's leichter | Effektiver Schutz vor Hack-Attacken

Abhören vermeiden: VPNs und Browser

Eine Menge Informationen gehen durch die Leitungen, wenn Ihr arbeitet. Der Natur des Internets nach könnt Ihr 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 Ihr die Sicherheit schlecht beurteilen könnt. Vermeidet Risiken und sichert Euch ab!

Nutzen eigener VPNs

Besonders im Firmenumfeld ist der Einsatz von Virtual Private Networks, kurz VPN, lange Standard. Diese Verbindung erzeugt einen Tunnel zwischen Eurem Rechner und dem Ziel (beispielsweise einem Firmenserver), der auf dem kompletten Weg verschlüsselt ist. Die Daten fließen also nicht mehr frei lesbar durchs Netz. Das verhindert, dass sie auf dem Weg abgefangen und missbraucht werden.



- Voraussetzung ist ein VPN-Server, der Euch mit dem gewünschten verbinden lässt.
- Unter Windows 10/11 könnt Ihr eine neue VPN-Verbindung einrichten, indem Ihr auf **Einstellungen**, **Netzwerk und Internet**, **VPN** und dann auf **VPN-Verbindung hinzufügen** klickt.
- Gebt dort dann die nötigen Zugangsdaten ein, um die Verbindung erfolgreich aufbauen zu können.

So geht's leichter | Effektiver Schutz vor Hack-Attacken

- Bei einigen VPN-Typen ist es nötig, dass Ihr noch zusätzliche Software bzw. Treiber installiert.

Tipp

Setzt Ihr eine Netzwerkfestplatte, ein so genanntes NAS, ein? Dann solltet Ihr dessen Handbuch konsultieren: Die meisten NAS-Systeme bieten integriert einen VPN-Server. Aktiviert den, dann könnt Ihr von unterwegs eine Verbindung zum 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**.

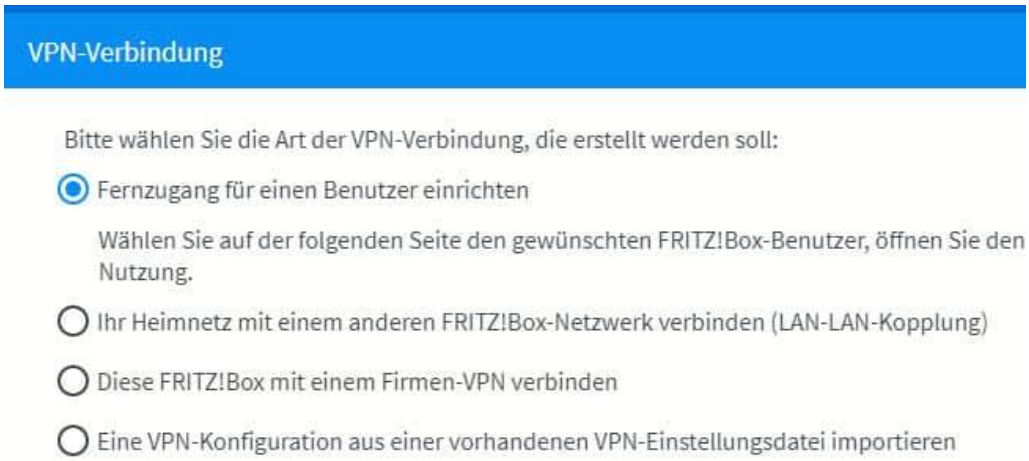
Einrichten der AVM Fritz!Box als VPN-Server

Der Router ist ja sowieso die Verbindung Ihres Netzwerks zum Internet. Damit bietet er sich an, auch von außen Berechtigten die Möglichkeit zu geben, auf Euer Netzwerk zuzugreifen. Folgerichtig haben viele Router einen eigenen VPN-Server integriert. So auch die AVM Fritz!Box. Den müsst Ihr nur noch konfigurieren.

- Im ersten Schritt richtet unter **Internet** > **MyFritz-Konto** ein Konto bei AVM ein. Dieses erlaubt den Fernzugriff auf die Fritz!Box über einen internen Dienst des Herstellers. Ihr könnt direkt über die Oberfläche der Fritz!Box alle nötigen Schritte abarbeiten und seid schon über dieses Konto in der Lage, den Router aus dem Internet zu steuern.
- Als nächstes müsst Ihre den VPN-Server der Fritz!Box aktivieren und einrichten. Klickt dazu im Hauptmenü der Konfigurationsoberfläche auf **Internet** > **Freigaben** > **VPN**.

So geht's leichter | Effektiver Schutz vor Hack-Attacken

- Durch einen Klick auf **VPN-Verbindung hinzufügen** könnt Ihr eine neue VPN-Verbindung einrichten. Hier kommt es nun darauf an: Wenn Ihr nur von außen auf die Fritz!Box und Ihr Netzwerk zugreifen können wollt, dann wählt **Fernzugang für einen Benutzer einrichten**.
- Alternativ könnt Ihr auch die Netzwerke zweier Fritz!Boxen miteinander verbinden. Beispielsweise dann, wenn Zuhause und Büro oder Ferienwohnung miteinander verbunden werden sollen und an beiden Orten eine Fritz!Box vorhanden ist.
- Im Normalfall werdet Ihr auf das Netzwerk und die Rechner als Einzelbenutzer zugreifen wollen. Hier solltet Ihr nicht den Standardbenutzer verwenden, sondern einen separaten Benutzer anlegen!



- Gebt nun die von der Fritz!Box abgefragten Daten ein, legt den VPN-Benutzer fest, dann seid Ihr schon so gut wie fertig. Der Router sucht sich nämlich selber die eher komplexeren Angaben (wie das „Shared Secret" der VPN-Verbindung etc.) aus. Das erspart den Aufwand, sich dieses ausdenken zu müssen.

So geht's leichter | Effektiver Schutz vor Hack-Attacken

- Keine Sorge: Wenn Ihr in der VPN-Übersicht auf **VPN-Einstellungen** klickt, dann bekommt Ihr alle relevanten Informationen angezeigt.
- Nun müsst Ihr nur noch auf dem Gerät, das Ihr dabei habt, die VPN-Verbindung anlegen. Wählt dazu als Verbindungstyp **IPSec** (bei macOS **CISCO IPSec**) und gebt die Daten aus der Übersicht der VPN-Einstellungen der Fritz!Box ein.

Externe VPN-Dienste

Habt Ihr keinen eigenen VPN-Server im Router oder der Netzwerkfestplatte? Dann nutzt 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 den selben Service wie ein eigener VPN-Server, nehmen aber den Aufwand der Einrichtung ab. Installiert deren Software, baut die Verbindung auf, und schon sind Ihre Daten verschlüsselt unterwegs.

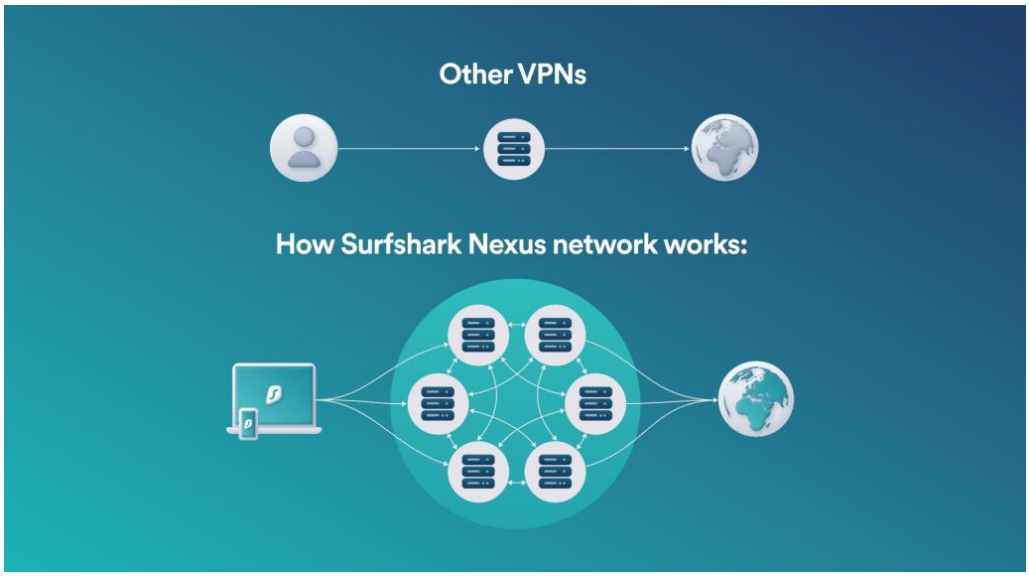
Die großen VPN-Anbieter haben auch Apps für Android und iOS im Programm. Schließlich seid Ihr unterwegs ebenfalls viel online. Auch

So geht's leichter | Effektiver Schutz vor Hack-Attacken

wenn es weniger Schadsoftware für mobile Geräte gibt als für den PC, ist das Risiko nicht von der Hand zu weisen!

Sonderfall Surfshark Nexus

Wenn Ihr einen externen VPN-Anbieter nutzt, dann ist das immer ein Stück eine Vertrauensfrage. Während Ihr Eure Daten vor dem Netz im Tunnel versteckt, laufen sie ohne den Schutz des VPNs beim Dienstleister auf. Dem müsst Ihr also vertrauen.



Surfshark Nexus geht hier einen angenehmeren Weg: Die Verbindung wird nicht nur mit einem Server, sondern gleich über mehrere geleitet. Dabei werden nicht Geschwindigkeitsvorteile erzielt, sondern auch die Nachverfolgbarkeit und damit das Risiko verringert: Die IP-Adressen werden immer wieder gewechselt. Damit kommen die abgerufenen Daten zwar sicher auf dem eigenen Rechner an, für die aufgerufenen Webseiten scheint es aber so, als würden unterschiedliche Rechner anfragen. Eine Zuordnung zu einem Benutzer wird damit deutlich erschwert.

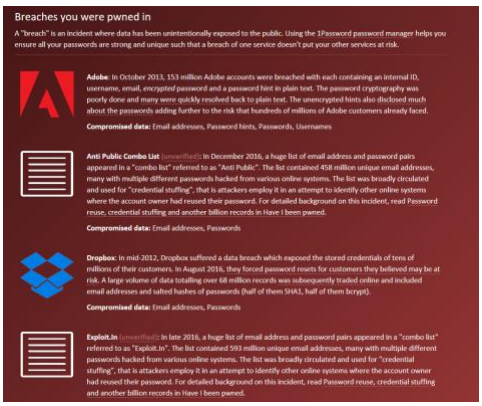
So geht's leichter | Effektiver Schutz vor Hack-Attacken

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.

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 Eure Benutzerkonten, wie Ihr das Passwort nicht geändert habt.



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

Wenn Ihr betroffen seid, dann ändert so schnell wie möglich das Passwort, und wiederholt dies häufiger.

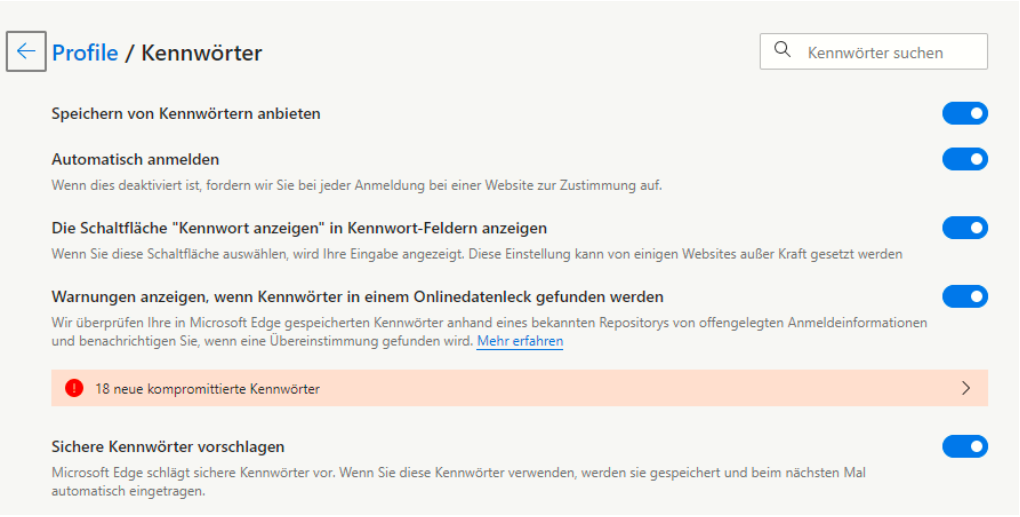
Passwörter in Edge überprüfen lassen

Kennwörter sind immer noch der Kern der Sicherung der Zugänge zu Webseiten, Online-Konten und anderen Diensten. Das bringt mit sich, dass die Zugangsdaten auf allen möglichen Servern gespeichert sind.

So geht’s leichter | Effektiver Schutz vor Hack-Attacken

Werden durch Sicherheitslücken diese Daten Angreifern verfügbar gemacht, dann sind die Login-Daten schnell in Datenbanken wie Collection #1 frei verfügbar. Gerade bei nicht häufig genutzten Konten denkt Ihr oft nicht an dieses Risiko. Lasst Euch durch Microsoft Edge unterstützen!

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



- Wenn Ihr das nachträglich machen wollt, dann klickt in Edge auf die **drei Punkte** oben rechts, dann auf **Einstellungen** > **Profile** > **Kennwörter** und aktiviert **Warnungen anzeigen, wenn Kennwörter in einem Onlinedatenleck gefunden werden**.

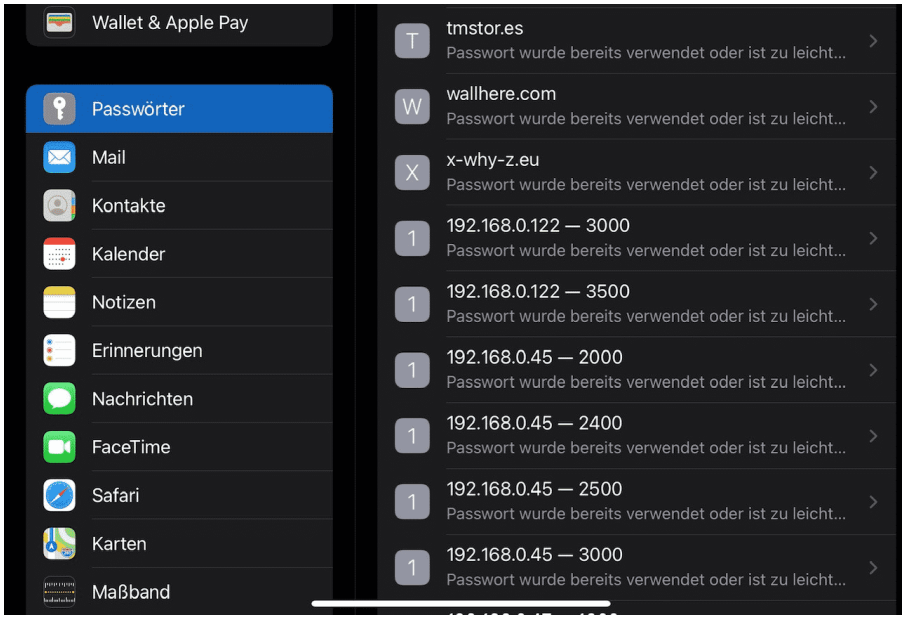
So geht's leichter | Effektiver Schutz vor Hack-Attacken

Ein solcher Hinweis sagt nicht zwingend aus, dass das Konto, an Ihr Euch gerade anmeldet, kompromittiert ist. Allerdings wurde die Kombination Benutzername/Kennwort in einem Leck gefunden. Ihr solltet die Zugangsdaten also umgehend ändern.

Passwortcheck in iOS

So schön es ist, dass immer mehr Dinge online auch mit dem Smartphone durchgeführt werden können, einen Nebeneffekt hat das Ganze: Ihr müsst immer mehr Benutzerkonten anlegen und dafür natürlich auch Passwörter vergeben. iOS 15 bietet hier eine zentrale Stelle, an der die entstehenden Risiken kontrolliert und verringert werden können.

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



- Unter **Einstellungen** > **Passwörter** findet Ihr direkt die Informationen zu den Konten/Webseiten, den verwendeten

So geht's leichter | Effektiver Schutz vor Hack-Attacken

Passwörtern und der Bewertung, warum das Passwort nicht geeignet scheint oder ein Risiko beinhaltet.

- Tippt auf einen Eintrag, dann könnt Ihr direkt auf die Webseite wechseln, um das Kennwort zu ändern.
- Alternativ könnt Ihr das Passwort aus dem Schlüsselbund löschen. Das macht Sinn, wenn das Konto bereits gelöscht oder nicht mehr in Benutzung ist.

Besser doppelt: Zwei-Faktor-Authentifizierung

Mit Netz und doppeltem Boden, das ist die klassische Absicherung in vielen Bereichen des täglichen Lebens. Eine alleineige Kombination aus Benutzername und Passwort ist anfällig: Kommt ein Fremder in deren Besitz, weil er sie aus einem Datenleck bekommen, von Euren Fingern abgelesen oder erraten hat, dann kommt er ohne weitere Schritte an das betroffene Konto.

Eine Lösung ist die Zwei-Faktor-Authentifizierung (2FA). Hier unterscheidet man bei den Schutzmaßnahmen in **Wissen** und **Besitz**. Eine Kombination von Benutzername und Passwort fällt in den Bereich Wissen: Wer sich anmelden will, muss diese wissen. Eine Anmeldung ist von jedem Ort der Welt möglich, unabhängig davon, ob Ihr es seid.

Der Zweite Faktor sollte also anders beschaffen sein. Man setzt gerne eine zweite Authentifizierungsschicht ein, die den Besitz von etwas voraussetzt. Beispielsweise die SMS eines Zahlencodes an eine vordefinierte

So geht's leichter | Effektiver Schutz vor Hack-Attacken

Telefonnummer oder ein so genanntes Token, das eine ständig wechselnde Zahlenkombination anzeigt. Nach der Anmeldung mit Benutzername und Passwort müsst Ihr dann noch diesen Zahlencode eingeben.

Für eine erfolgreiche Anmeldung müsst Ihr also nicht nur die Zugangsdaten **kennen**, sondern zusätzlich auch noch das Smartphone oder Token **besitzen**, in der Hand haben. Ist das eine kompromittiert, dann hilft das dem Dieb oder Finder nicht. Erst beide Informationen erlauben den Zugriff auf das so geschützte Konto.

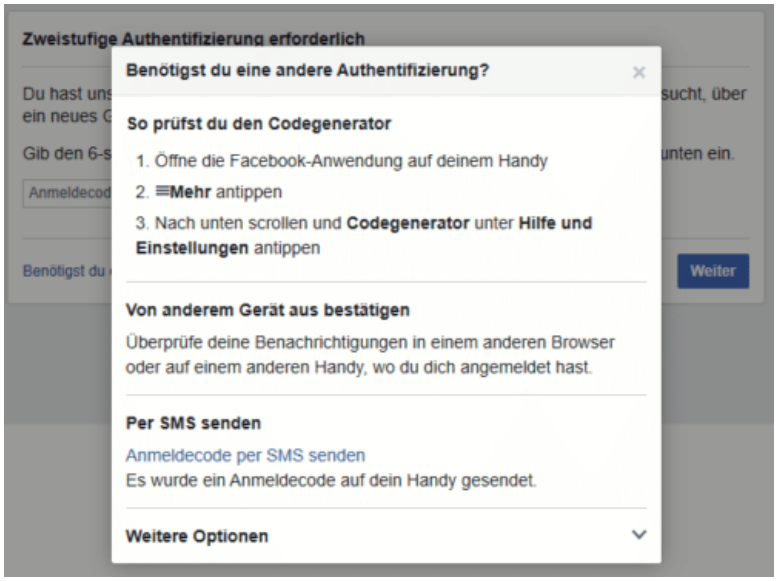
2FA bei Facebook

Facebook trifft es immer wieder hart. Oder besser: Die Benutzer trifft es hart. Datenlecks, offen zugängliche Passwörter, Sicherheit ist offensichtlich kein Unternehmensziel. Es macht also Sinn, das selber in die Hand zu nehmen. Facebook bietet die Möglichkeit der Zwei-Faktor-Authentifizierung (2FA). Kommt ein Unbefugter an das Passwort, dann kann er damit nichts anfangen, denn zur Anmeldung wird dann ein immer wieder wechselnder Code angefordert. Die Einrichtung geht schnell und einfach.

- Unter **Einstellungen** > **Sicherheit und Login** könnt Ihr die Zwei-Faktor-Authentifizierung **unter Zweistufige Authentifizierung** einschalten.
- Im Standard versucht Facebook, Euch von der Verwendung einer Authenticator-App zu überzeugen: Diese kann auf Ihrem Smartphone installiert werden und zeigt dann immer den richtigen Code an.
- Unabhängiger seid Ihr, wenn Ihr Euch den Code per SMS schicken lassen. Wenn die Facebook-Anmeldung (auf der

So geht's leichter | Effektiver Schutz vor Hack-Attacken

Webseite oder der App) den Code abfragt, dann klickt auf **Benötigst Du eine andere Authentifizierung**.



- Ein Klick auf **Anmeldecode per SMS** senden löst dann eine SMS mit dem Anmeldecode an die Eurem Konto hinterlegte Handynummer aus.

2FA bei Outlook

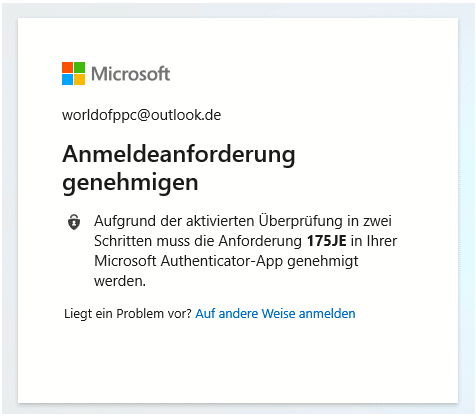
Die Zwei-Faktor-Authentifizierung funktioniert wunderbar, wenn der Zugriff über den Webbrowser stattfindet. Greift Ihr aber mit einem Programm auf das Outlook-Postfach zu, dann kann das Vorgehen von Programm zu Programm abweichen. In der Regel trefft Ihr dabei aber nur auf zwei Möglichkeiten. Einmal eingerichtet, ist auch die Mail-Abfrage auf dem PC abgesichert.

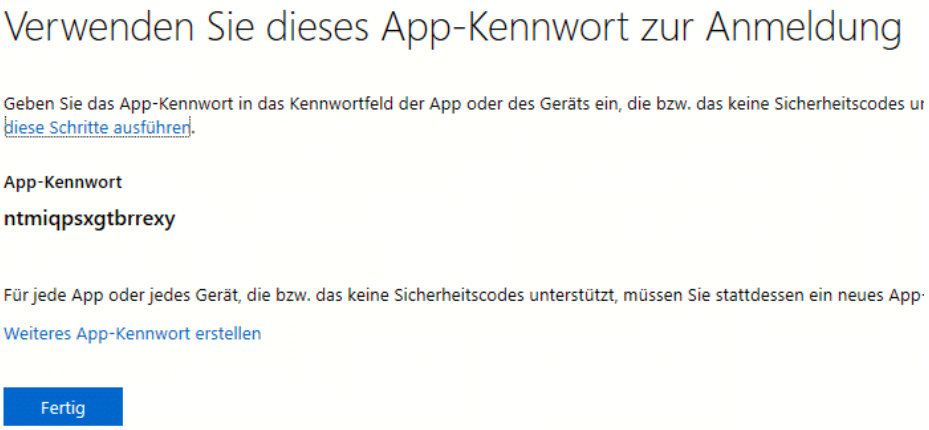
- Im idealen Fall ist Ihre E-Mail-Software in der Lage, mit der Anforderung eines zweiten Faktors direkt umzugehen und sie zu

So geht's leichter | Effektiver Schutz vor Hack-Attacken

verarbeiten. Outlook 2016 und 365 wie auch die interne E-Mail-App gehören dazu.

- Bei den aktuellen Versionen von Windows wird der Authentifizierungscode der App nur einmalig abgefragt. Direkt danach schaltet sich Windows Hello ein und fordert einmalig die Anmeldung über eine der in Windows hinterlegten Methoden (Wie Fingerabdruck, Gesicht oder Token) an. Wenn Ihr die ausgeführt habt, dann wird Windows Hello bei jeder Anmeldung am Postfach als zweiter Faktor verwendet. Deutlich bequemer, als wenn Ihr immer Codes eingeben müssen!





- Ältere Versionen von Outlook, Smartphones und andere Programme, die nicht nativ den zweiten Faktor bei der Anmeldung anfordern können, könnt Ihr austricksen.

So geht's leichter | Effektiver Schutz vor Hack-Attacken

- Wechselt wieder in die Sicherheitseinstellungen des Microsoft-Kontos und klickt auf **Zusätzliche Sicherheitsoptionen**.
- Unter App-Kennwörter könnt Ihre ein **zufälliges App-Kennwort** erzeugen. Das besteht aus einer Kombination aus dem Passwort und einem zufälligen Code. Es ist weder lesbar noch von einem Fremden zu erraten.
- Gebt dieses Kennwort statt des Kontokennwortes ein. Das E-Mail-Programm fragt nicht mehr nach dem zweiten Faktor, ein Fremder, der nur Euer eigentliches Passwort hat, kommt aber nicht an die E-Mails.

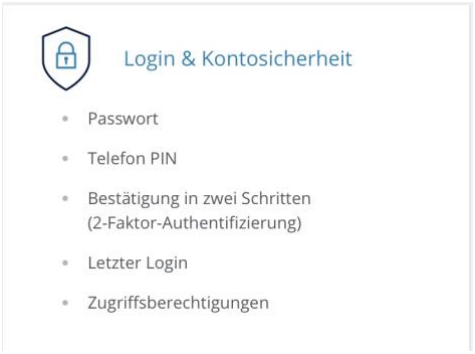
2FA bei Microsoft 365

- Ruft die Admin-Seite von Office 365 auf, dann klickt auf **Benutzer**.
- Setzt einen Haken beim dem Benutzer, den Ihr anpassen wollt und klickt ihn an.
- Unten rechts klickt dann auf **Mehrstufige Authentifizierung**. Office 365 öffnet den Benutzer und erlaubt unten rechts die Aktivierung der **Mehrstufigen Authentifizierung**.
- Bei jeder Anmeldung müsst Ihr nun neben dem Passwort einen Code eingeben. Diesen bekommt Ihr entweder per SMS, per E-Mail oder über die Microsoft Authenticator-App.

So geht’s leichter | Effektiver Schutz vor Hack-Attacken

2FA für Webseiten

Passwort-Leaks, Phishing-Attacken, Social Engineering, die Möglichkeiten, das Passwort an Übeltäter zu verlieren, sind unzählbar. Das ist bei E-Mail- und Dienstkonten schon eine Katastrophe, bei einer Webseite sind die Auswirkungen noch einmal andere. Das Defacing, das Ersetzen der Inhalte der Seite durch Nachrichten der "Eroberer", hat eine direkte Außenwirkung. Diese Fall kann eintreten, wenn ein Angreifer die Zugangsdaten erbeutet. Das Anmelden am Hosting-Konto und das Ändern der FTP- oder Wordpress-Zugangsdaten ist dann ein Klacks. IONOS/1&1 als einer der verbreitetsten Hoster bietet als Schutz dagegen die Zwei-Faktor-Authentifizierung bei der Anmeldung an die Administrationskonten an.



- Um die einzurichten, meldet Euch (noch nur mit dem Passwort) an der Admin-Oberfläche an und klickt dann auf **Euren Namen** > **Mein IONOS** > **Login & Kontosicherheit** > **Bestätigung in zwei Schritten**.

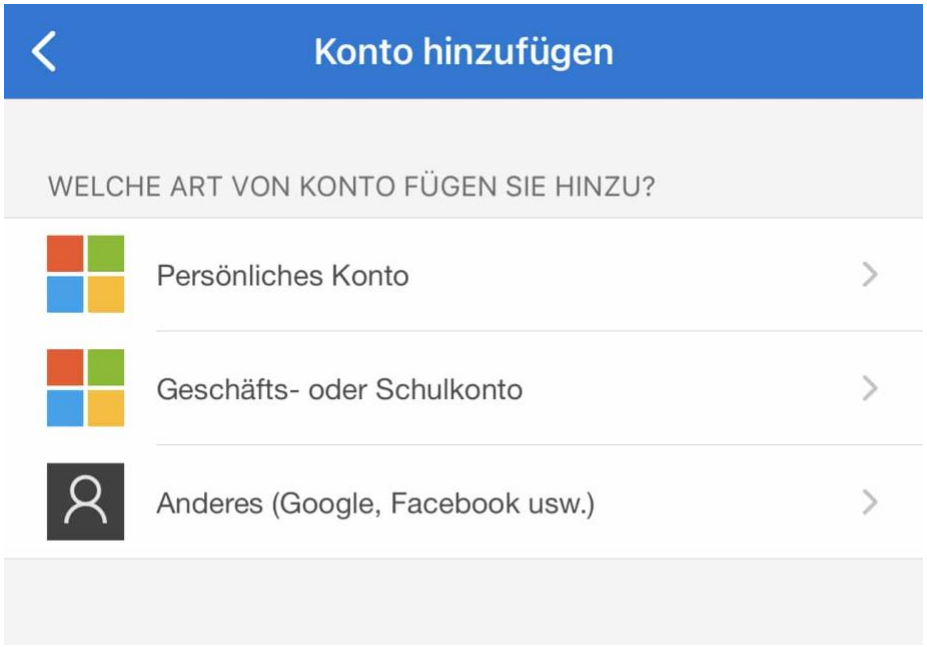
So geht's leichter | Effektiver Schutz vor Hack-Attacken

- IONOS bietet zwei verschiedene Möglichkeiten für den zweiten Faktor an: Zum einen die IONOS Mobile App, die unter anderem auch Einstellungen zum Hostingkonto erlaubt.
- Die zweite Möglichkeit ist die Verwendung einer normalen Authenticator-App, die dann auch für andere Konten verwendet werden kann.
- Egal welche der beiden Lösungen gewählt wird: Nach Eingabe des Passwortes fordert die Admin-Konsole von IONOS/1&1 dann die Ziffernfolge ab, die die installierte App gerade anzeigt. Wer Euer Smartphone nicht in seinem Besitz hat, der bleibt außen vor!

Authenticator-Apps

Weitere Alternativen zu SMS oder E-Mail als zweitem Faktor sind die kostenlose Authenticator-App von Microsoft und der ebenfalls kostenlose Google Authenticator, denn die benötigen im Vergleich zu SMS oder E-Mail keine Datenverbindung!

So geht’s leichter | Effektiver Schutz vor Hack-Attacken



- Nach Installation der App könnt Ihr Eure Microsoft-Konten, aber auch diverse Konten von anderen Anbietern (wie Facebook, Google, GMX etc.) einbinden.
- Dazu scannt den vom Anbieter für die Authenticator-App angegebenen Barcode in der Kontokonfiguration unter **Zwei-Faktor-Authentifizierung**.
- Das Konto erscheint dann in der App und zeigt bei Auswahl den jeweils aktuellen Code an, der nach Eingabe des Passwortes bei der Anmeldung in einem separaten Fenster eingegeben werden muss.

Beim Google Authenticator gibt es noch eine Besonderheit: Wenn Ihr das Telefon wechselt, dann müsst Ihr die eingerichteten Konten nicht manuell übertragen, sondern könnt das über einen automatisierten Prozess machen.

So geht's leichter | Effektiver Schutz vor Hack-Attacken

- Klickt in der App oben rechts auf die drei Punkte und dann auf **Konten übertragen**.
- Die App erzeugt einen QR-Code, den Ihr mit der App auf dem neuen Handy scannen müsst.
- Auf dem neuen Handy tippt nach der Installation auf **Konten importieren > QR Code scannen**.
- Die Konten werden nun automatisiert übertragen und sind direkt nutzbar. Einzige Voraussetzung: Die Mobilfunknummer in beiden Geräten muss die selbe sein!

Kontrolle geteilter Dateien

Das Arbeiten in der Cloud gehört heute zum Standard, egal auf welchem Gerät Ihr arbeitet. Und so teilt Ihr die eine Datei, dann noch eine, dann braucht jemand anderes noch eine Freigabe und am Ende habt Ihr komplett den Überblick verloren.

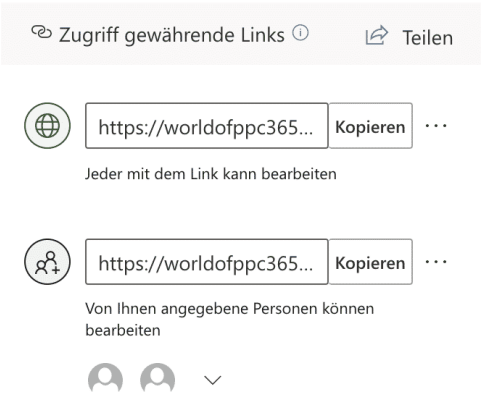
Nun sind Freigaben nicht für die Ewigkeit, und Ihr wollt (und solltet!) die Berechtigungen auch wieder entfernen. Das geht aber nur, wenn Ihr auch wisst, welche Dateien und Ordner freigegeben sind.

Ändern von Freigaben in OneDrive

Ein Projekt ist zu Ende, ein Mitarbeitender scheidet aus, ein Bearbeiter der Datei soll ausgetauscht werden. Dann soll auch der Zugriff auf die Dateien möglichst schnell widerrufen oder angepasst werden. Diese Funktion versteckt sich leider ein wenig in den Dialogen.

So geht's leichter | Effektiver Schutz vor Hack-Attacken

- Meldet Euch über den Webbrowser an Eurem Microsoft- (oder Office 365-) Konto an.
- Klickt auf den Punktwürfel oben links, dann auf **OneDrive**.
- Sucht den freigegebenen Ordner heraus und klickt dann auf die **drei Punkte** rechts von dessen Namen und auf **Details**.



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

Anzeigen aller Freigaben

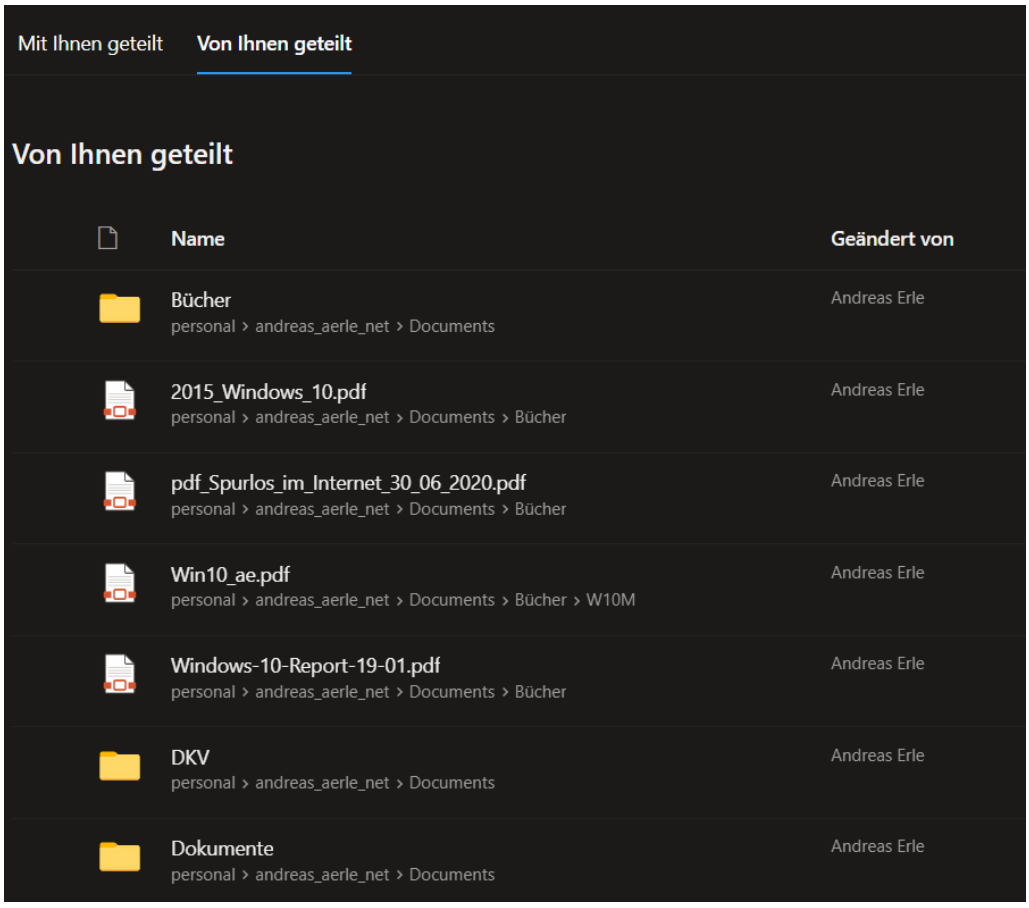
Egal, welchen Cloudservice Ihr nutzt, über die Zeit sammeln sich riesige Mengen an Dateien an. Auch wenn Ihr nur einen geringen Prozentsatz davon teilt: Die Übersicht ist schnell dahin. Mit unserem Hack könnt Ihr Euch für OneDrive und Dropbox alle Freigaben anzeigen lassen und dann schnell entscheiden, welche Freigaben Ihr schnell entfernen wollt!

So geht's leichter | Effektiver Schutz vor Hack-Attacken

Übersicht über OneDrive-Freigaben

Bei Dateifreigaben auf einem OneDrive – auf Grund der Integration in Windows die am häufigsten verwendete Freigabemethode – könnt Ihr Euch alle Freigaben auf einmal anzeigen lassen:

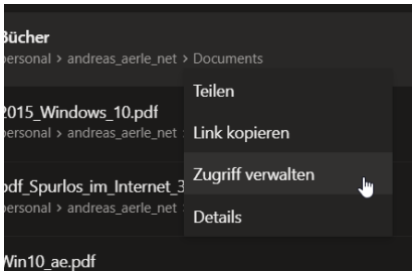
- Klickt im Webclient von OneDrive links im Menü auf **Geteilt**.
- Aktiviert dann die Registerkarte **Von Ihnen geteilt** im Detailfenster.



- OneDrive zeigt jetzt alle freigegebenen Dateien in einer Liste an. Wo die in der Verzeichnisstruktur des OneDrive stehen, erkennt Ihr in der Angabe unter dem Dateinamen.

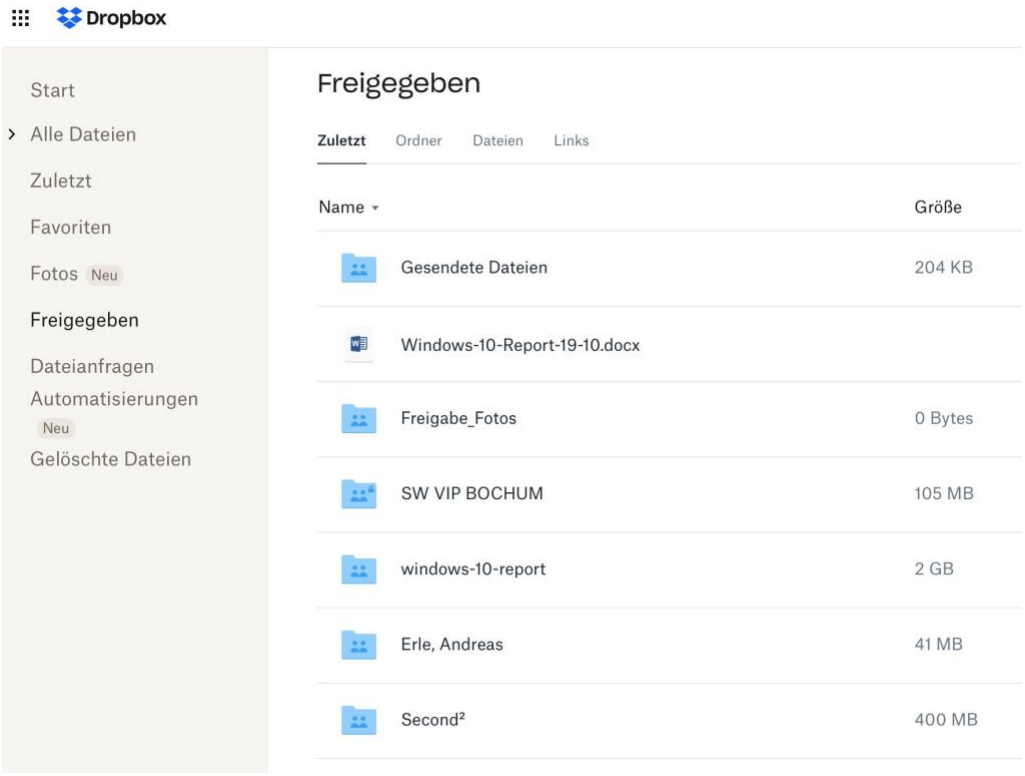
So geht's leichter | Effektiver Schutz vor Hack-Attacken

- Um die Freigabe zu ändern oder zu beenden, klickt mit der rechten Maustaste auf den Dateinamen und dann auf **Zugriff verwalten**. Hier könnt Ihr nun Zugriffen entfernen oder verändern.



Übersicht über DropBox-Freigaben

Auch auf einer Dropbox sammeln sich mit der Zeit unzählige freigegebene Dateien. Da hilft es, dass auch hier eine Möglichkeit des Überblicks über Freigaben gibt:



- Meldet Euch an Eurer DropBox im Webclient an.

So geht's leichter | Effektiver Schutz vor Hack-Attacken

- Klickt dann in der Übersicht auf der linken Seite auf **Freigegeben**.
- Im Detailfenster zeigt Dropbox jetzt verschiedene Möglichkeiten an: **Zuletzt** sortiert die vorhandenen Freigaben nach dem Zeitpunkt des Zeitpunkts der Freigabe, die jüngsten sind oben. **Ordner** zeigt nur freigegebene Ordner an, **Dateien** nur einzeln freigegebene Dateien.
- Klickt auf die drei Punkte rechts neben dem Namen des freigegebenen Objekts, dann auf **Teilen**.
- Oben rechts findet Ihr ein **Zahnrad**-Symbol. Klickt darauf und dann auf **Freigabe beenden**, um die Freigabe zu entfernen und die Datei wieder nur noch lokal verfügbar zu machen.