Schieb Report

Ausgabe 2020.04

Störende PopUps bei der PS4 ausschalten

Spielekonsolen wie die Playstation 4 oder die XBOX One sind eigentlich nur für Ihren privaten Spaß gedacht und sollen - im Gegensatz zu einem Gaming PC - ohne weiteren Konfigurationsaufwand funktionieren. Um so ärgerlicher, wenn dann etwas nicht funktioniert. Oder Dinge passieren, die Sie nicht wollen. Bei der Playstation ist ein immer wiederkehrendes Ärgernis, dass Sie bei Filmszenen in einem Spiel eine Meldung angezeigt bekommen. Diese sagt, dass die "Spielaufzeichnung gestoppt worden sei". Warum das so ist und was Sie dagegen tun können, zeigen wir Ihnen hier.

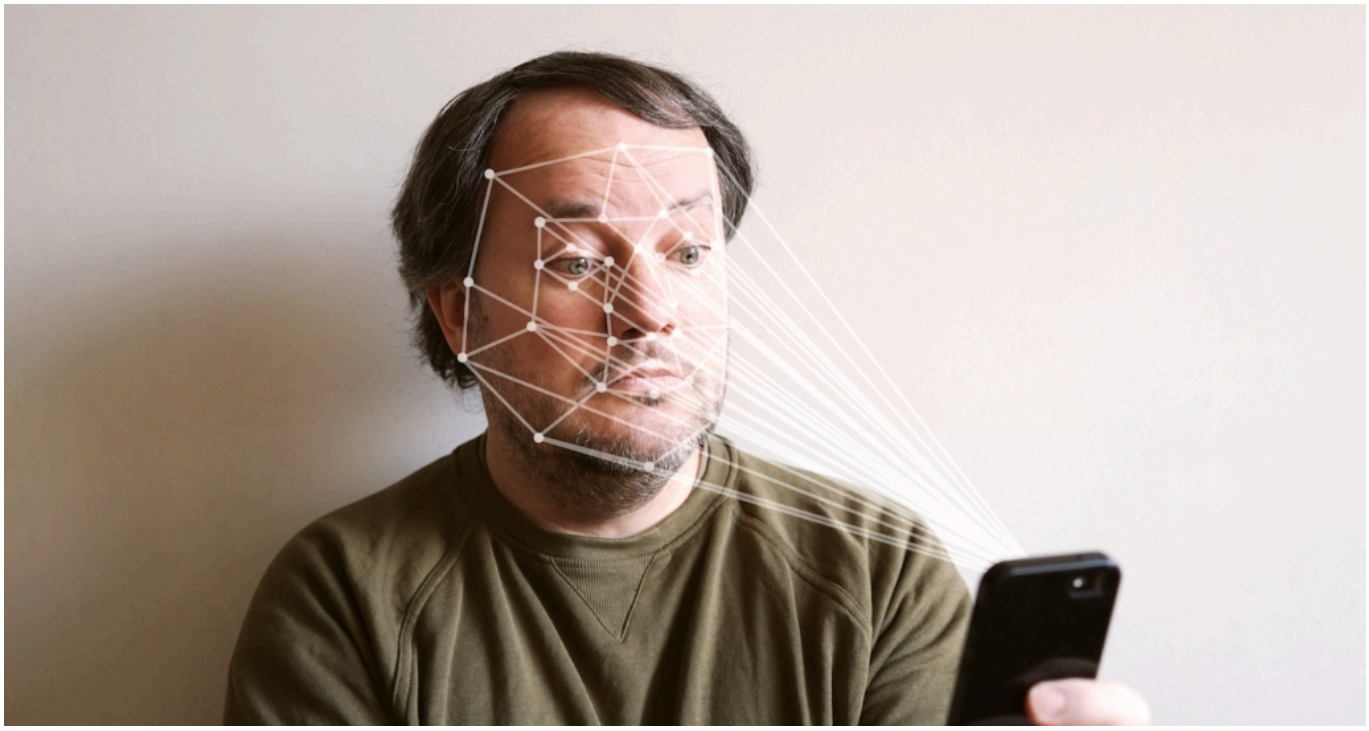
Der Hintergrund dieser Meldung ist die Tatsache, dass die PS4 im Standard Ihre Spielaktivitäten aufnimmt. Damit können später gegebenenfalls Spieleclips teilen. Das an sich ist kein Problem, nur sind einige Spieleanbieter davon nicht begeistert: Die so genannten Cut Scenes, also die Filmsequenzen im Spiel, sollen eine Überraschung bleiben. Sie sollen also nicht auf YouTube oder in Blogs geteilt werden. Und genau da kollidieren die Aufzeichnung und die Herstellervorgaben. Das sorgt für die genannte Fehlermeldung.

Die Lösung: Gehen Sie auf der Playstation auf **Einstellungen** -> **Mitteilungen** -> **PopUp-Mitteilungen** -> **Blockierte Szenen für Videoaufzeichnung** und entfernen Sie dort den Haken. Das verhindert nicht den Fehler, er wird Ihnen aber nicht mehr durch ein PopUp angezeigt.

Clearview AI kennt wahrscheinlich auch Dein Gesicht

Ein US-Unternehmen hat dreist Milliarden Fotos aus den Netzwerken gezogen - und in einer Datenbank gespeichert. Nun können angemeldete Nutzer diese Datenbank durchsuchen und in Sekunden fast jeden entdecken. Ein Dammbruch.

Spätestens seitdem wir Smartphones mit unserem Gesicht entsperren können, wissen wir: Unser Gesicht kann von Maschinen erkannt werden. Selbst ein kleines Smartphone kann das. Ein Albtraum, wenn ein System die Gesichter aller Menschen kennen würde - und so jeden Menschen auf der Straße sofort zuverlässig erkennen könnte. Doch genau das könnte schon bald der Fall sein - denn technisch ist das jetzt möglich.



Clearview AI hat ungefragt Milliarden Gesichter gescannt

Einem US-Unternehmen ist es gelungen, die Gesichter von Milliarden Menschen in einer Datenbank zu speichern. Clearview AI - so nennt sich das Unternehmen - hat dazu dreist Unmengen öffentlich zugänglicher Fotos und Videos gescannt. Auf Facebook, auf Youtube, auf Instagram. Dort zeigen wir unsere Bilder ja her - und verknüpfen diese mit unseren Daten. Auch die von Freunden.

Clearview AI hat laut Bericht in der New York Times Milliarden(!) solcher Fotos geladen, gespeichert und ausgewertet. Ohne die Betroffenen oder die Sozialen Netzwerke um Erlaubnis zu bitten oder sie in Kenntnis zu setzen.

Und diesen Daten-Pool zu Geld gemacht: Polizeistationen in den USA wurde Zugriff auf die Datenbank gewährt. Für 2.0000 Dollar im Jahr. Das System funktioniert besser als viele andere.

Schon allein deshalb stellen die Behörden in den USA wohl keine Fragen.

Abfrage in Echtzeit möglich

Der Service ist für Fahnder verlockend: Die Beamten laden ein Foto hoch und erfahren Sekunden später, um wen es sich handelt. Selbst eine App wäre denkbar, sagt der Anbieter, die das blitzschnell und in Echtzeit macht: Mit der Kamera eine Person auf der Straße einfangen - und die App durchsucht die Datenbank und verrät, wer es ist. Die Technologie ist heute so weit. Gesichtserkennung ist keine Hexerei mehr. Bei Amazon lassen sich Cloud-Dienste mieten, die das anbieten.

Erschreckend: Die Lösung funktioniert. Sie ist marktreif. Sie ist offenbar sogar im Einsatz. Auf der Webseite des Unternehmens heißt es, das alles sei "im Einklang mit geltendem Recht". Das darf wohl bezweifelt werden - selbst in den USA sitzt der Schock tief. Es gibt Empörung.

Die App macht deutlich, dass es allerhöchste Zeit ist, derartiges eindeutig zu regulieren und zu verbieten. Wir müssen vor Anwendungen dieser Art geschützt werden. Während Google sich zumindest ein vorübergehendes Verbot solcher Anwendungen vorstellen kann, um Zeit für Regulierung zu haben, bezeichnet Microsoft ein Verbot als "regulatorisches Hackebeil".

Das zeigt, dass dringend eine strenge Regulierung erforderlich ist.

Doppelt gemoppelt: NordVPN verschlüsselt zweifach

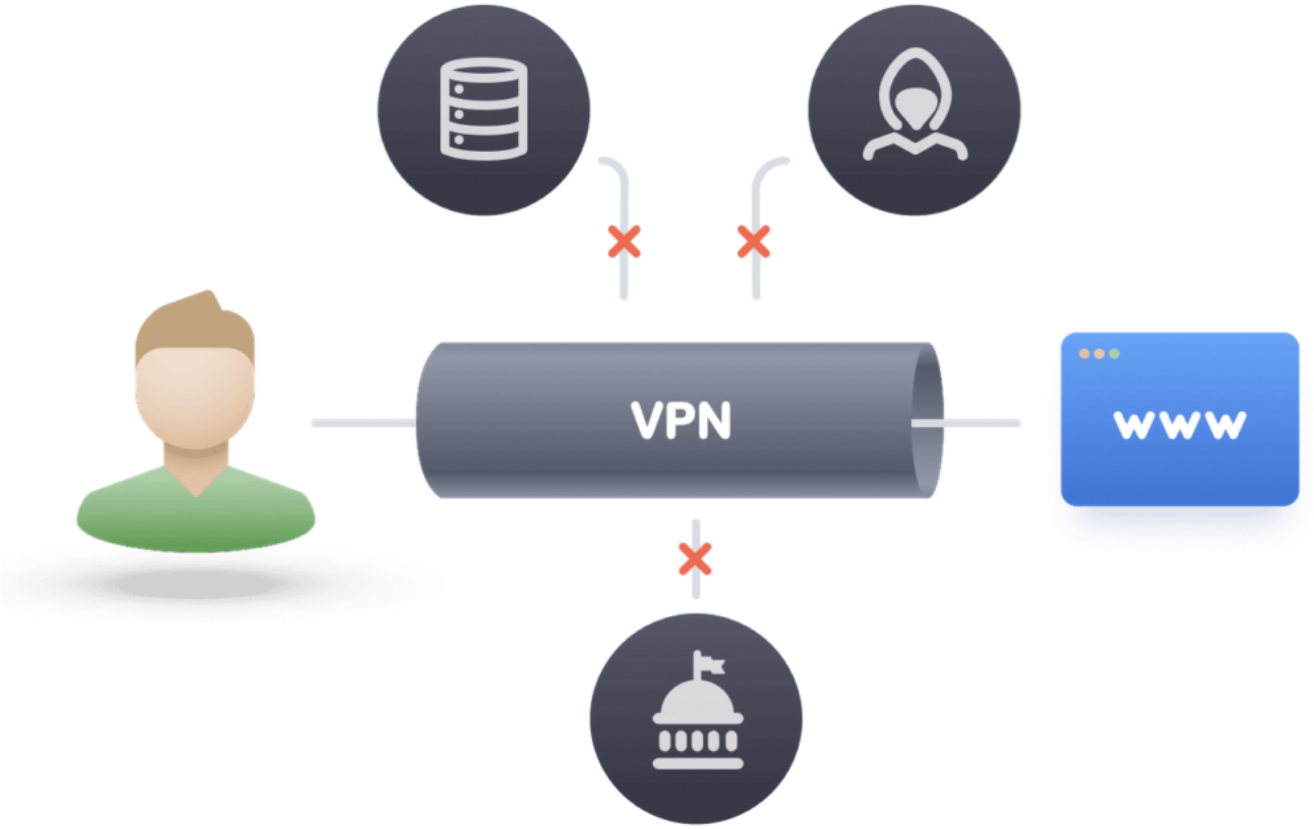
Mit einem Virtuellen Privaten Network (VPN) lassen sich bequem Daten verschlüsseln, Aufenthaltsort und Identität verschleiern, Werbenetzwerke austricksen und generell die Netznutzung absichern. Es gibt mittlerweile Dutzende VPN-Anbieter. Sie alle haben verschiedene Stärken und Schwächen - und manche Besonderheiten. NordVPN bzum Beispiel ietet sogar doppelte Verschlüsselung an - und damit ein höheres Maß an Datensicherheit.

Früher haben nur Menschen, die sich in ein Firmen-Netzwerk "einklinken" wollen, ein Virtual Privat Network (VPN) benutzt. Bereitgestellt vom Arbeitgeber. Heute nutzen viele Menschen ein VPN, ob am Desktop-PC oder auf dem Smartphone. Denn mit einem VPN wird das Onlinegehen deutlich sicherer: Fremde können den Datenverkehr nicht einfach "abhören" (zum Beispiel in einem offenen WLAN), Werbenetzwerke können einen weniger gut "erfassen" (durch Verschleierung) - und last not least können Internet-Nutzer anonym unterwegs sein.

Komplette Verschleierung von Identität und Daten

Wer ein VPN nutzen möchte, verwendet dazu in der Regel spezielle Software, die den technischen Teil erledigt. Vorteil: Die Nutzung des VPN wird dann sehr einfach, egal ob man Webseiten aufruft, Streamingdienste nutzt (und so Inhalte sehen kann, die einem sonst verborgen bleiben) oder andere Internet-Dienste einsetzt. Das VPN ist dann fast ohne jeden Aufwand vorhanden. Nutzer bemerken höchstens, dass es etwas langssamer geht als sonst. Bei guten VPN-Anbietern fällt das aber in der Regel kaum ins Gewicht, da sie über sehr schnell Verbindungen verfügen.

Sobald das VPN aktiviert ist, wird der komplette Datenverkehr durch einen Remote-VPN-Server geleitet. Dieser Server verändert (maskiert) zum Beispiel die IP-Adresse. Wichtig, um die eigene Identität zu verschleiern. Darüber hinaus werden aber auch alle Daten, die Du im Internet versendest oder empfängst, automatisch verschlüsselt. Auf diese Weise können Fremde (etwa Datenspione, Behördern oder Cyberkriminelle) nicht sehen, was online passiert. Selbst welche Webseiten angesteuert werden, wird auf diese Weise verschleiert.



Der VPN-Anbieter NordVPN bietet einen interessanten Extra-Service: Mit **Double VPN** werden Onlineaktivitäten nicht nur hinter einem, sondern sogar hinter zwei Servern versteckt. Eine doppelte Absicherung also. Das Prinzip dieser sogenannten VPN-Server-Verkettung ist recht einfach:

1. Der Datenverkehr wird an einen Remote-VPN-Server gesendet und verlässt diesen sicher verschlüsselt.
2. Der verschlüsselte Datenverkehr wird dann durch einen zweiten VPN-Server geleitet und ein weiteres Mal verschlüsselt.
3. Der Nutzer kommt sicher und vertraulich an sein Ziel.

Wichtig: Das Datentempo sinkt bei einem aktiven VPN zwangsweise. Schließlich werden Server zwischengeschaltet. Aber NordVPN gehört zu den Anbietern, die über eine schnelle Infrastruktur verfügen, so dass sich das aktive VPN kaum bemerken lässt. Nutzer können hier aus 5.500 Servern auswählen. Ist einer mal nicht so schnell wie gewohnt: Einfach wechseln. Auf Wunsch kann die VPN-Software auch automatisch mit dem aktuell schnellsten Server verbinden. Es gibt keine Bandbreitenbeschränkung, die durch das System vorgegeben wäre. Wichtig bei voluminösen Downloads.

Der Anbieter erlaubt, bis zu sechs Geräte gleichzeitig mit einem VPN zu schützen.

Kill-Switch verhindert Indiskretion

Ein häufiges Ärgernis bei manchen VPN-Anbietern sind plötzlich abbrechende Verbindungen - was aufgrund der Besonderheit einer VPN-Verbindung leicht passieren kann. Das Problem: Wenn die im Einsatz befindliche Software das nicht "bemerkt", ist beim nächsten Zugriff plötzlich die eigene IP-Adresse sichtbar. Die tatsächliche.

Doch das muss nicht sein: Ein VPN-Kill Switch überwacht ununterbrochen die Verbindung zum VPN-Server. Wenn die Verbindung versehentlich abbricht, verhindert der Kill Switch, dass ein Gerät (bzw. die Apps, die im Einsatz sind) auf das Internet zugreift. Die eigene IP-Adresse bleibt so unsichtbar - der Datenverkehr durchgängig verschlüsselt.

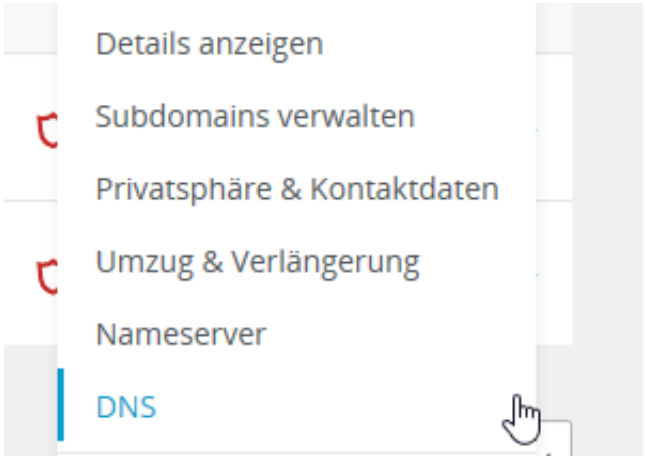
NordVPN verschlüsselt den Internet-Traffic und leitet ihn über einen VPN-Tunnel um, sodass die eigene IP-Adresse verschleiert wird und private Daten vor den neugierigen Augen Dritter geschützt sind. Der Kill Switch ist gewissermaßen der letzter Schutzwall. Er schützt private Daten konsequent vor versehentlicher Enthüllung.

Umleiten einer Internetadresse auf einen anderen Server

Eine eigene Internetseite ist einfach erstellt und kein Hexenwerk. Und wie bei so vielen Dingen etwas, das wächst: Erst starten Sie mit einem kleinen Vertrag, wachsen und ziehen irgendwann um. Nun sind die Internetadresse (URL) und der Server, auf dem sie liegt (der Webspace) zwei verschiedene Dinge. Wir zeigen Ihnen, wie Sie schnell auf einen anderen Webspace wechseln können und trotzdem die URL behalten können.

Der Zauber hinter den tollen Internetadresse heißt "DNS", der Dynamic Name Server. Dieser setzt die menschenlesbaren Namen in maschinenlesbare IP-Adressen um. Wenn Sie also "schieb.de" in die Adreßzeile Ihres Browsers eingeben, dann wandelt der DNS-Server diese in die IP-Adresse um und der Browser kann sie aufrufen. Beim Wechsel des Webspaces ändert sich die IP-Adresse, weil der neue Anbieter andere IP-Bereiche nutzt.

Um die URL nun auf einen neuen Webspace umzuleiten, melden Sie sich bei dem alten Anbieter an und gehen sie in die Einstellungen Ihrer URLs. Suchen Sie die heraus, die umgeleitet werden soll. In den Optionen der Adresse finden Sie einen Eintrag **DNS**. Wählen Sie diesen aus, dann geben Sie dort die neue IP-Adresse für alle Dienste ein.



Sie können durchaus mehrere Einträge ändern müssen, wenn Sie mehrere Dienste für die Webseite nutzen, zum Beispiel FTP, WWW und administrative Dinge. Speichern Sie die Änderungen, nach spätestens einer Stunde sollten diese aktiv sein.

Verschlüsselung nicht mehr sicher

Wir verschlüsseln bewusst oder unbewusst Daten, Passwörter, Zugangsinfos - und gehen davon aus, dass die wertvollen Daten mit sicher sind. Doch leider ist das nicht mehr uneingeschränkt der Fall: Quantencomputer können eine Verschlüssselung schon bald knacken. Was tun?

Dieses Jahr wurde auf der Tech-Konferenz DLD in München die praktisch überall eingesetzte RSA-Verschlüsselung als ab sofort nicht mehr sicher eingestuft. Was für eine Überraschung. Denn normalerweise empfehlen IT-Experten mantraartig alles zu verschlüsseln: Datenverbindungen, Passwörter, Daten auf der Festplatte, Chats und Kommunikation - einfach alles, was andere nichts angeht. Doch: vorbei!

Bislang ist man davon ausgegangen, dass es Jahrhunderte dauern würde, mit einem leistungsfähigen Computer eine verschlüsselte Nachricht oder einen Schlüssel zu knacken. Doch nun zeichnet sich eine neue Supercomputer-Generation am Horizont ab: Quantencomputer rechnen Tausend, Millionen Mal schneller als heutige Supercomputer und könnten einen gängigen 256-Bit-Schlüssel in wenigen Minuten knacken – irgendwann vielleicht sogar in Sekunden. Spätestens dann bringt es einem überhaupt nichts mehr, einen heute als modern geltenden Schlüssel zu verwenden.

Erst können Geheimdienste solche Nachrichten oder Daten knacken, irgendwann dann auch Unternehmen. Das wird nicht gleich morgen so weit sein, aber spätestens in 10 Jahren.

Quantencomputer knacken Verschlüsselung wie Kekse

Ein von Google entwickelter Quantencomputer hat kürzlich eine Aufgabe in 3 Minuten und 20 Sekunden geknackt, für die ein Supercomputer 10.000 Jahre bräuchte. Quantencomputer sind nicht einfach eine Weiterentwicklung heutiger Computer (kleiner, smarter, schneller), sondern etwas grundlegend Neues. Quantencomputer arbeiten auf der Basis der Quantenphysik. Sie verwenden quantenmechanischen Zuständen. In der Theorie braucht man weniger Platz, es geht schneller – aber es ist unheimlich kompliziert.

„Hören Sie noch heute auf, RSA-Verschlüsselung zu benutzen", rät Google-Forscher Jack Hidary deshalb auf der DLD. Der Grund: Die heute gängige RSA-Verschlüsselung ist ab sofort veraltet. In einer Zukunft mit Quantenkommunikation gebe es aber nur eine sichere Verschlüsselungstechnik: **PQC - Post-Quantum Kryptographie**. Also ein ganz neues Verfahren, komplex genug, um auch Quantencomputer auszuknocken.

Das Problem: Geheimdienste setzen auf eine neue Taktik: **SNDL – Store Now, Decrypt Later**.

SNDL: Store Now, Decrypt Later

Die Geheimdienste in den USA, Russland und vor allem China sammeln alles, was sie kriegen können – auch wenn sie es jetzt noch nicht entschlüsseln können. Store Now. Und

entschlüsseln es, sobald es geht, sobald Quantencomputer am Start sind. Encrypt Later. Das bedeutet: Im Grunde sind wir heute schon gefährdet, auch wenn die vertraulichen Daten erst später enttarnt werden. Kein beruhigender Gedanke.

Die Großen der Branche werden neue Methoden entwickeln (müssen), um Daten zu schützen. Wir werden uns in den nächsten Jahren damit alle beschäftigen. Denn die Chinesen haben bereits einen Satelliten im All, der Quanten-Kommunikation kann: Kommunikation, die quantentechnisch verschlüsselt wird – unknackbar für alle anderen. Es könnte zu einem Wettlauf der Technologie in diesem Bereich kommen.

Dorothee Bär will definitiv keine Klarnamenpflicht

Bundestagspräsident Wolfgang Schäuble hat jetzt - nicht zum ersten Mal - eine Klarnamenpflicht im Netz gefordert. Jeder soll sich mit seinem richtigen Namen im Netz aufhalten. Das Ziel: Weniger Drohungen, Hass und Hetze im Netz. Das Problem ist allerdings: Es würde nichts bringen. Die Staatsministerin für Digitalisierung Dorothee Bär ist deshalb entschieden dagegen.

Von einer angenehmen Gesprächskultur kann "im Netz" nur selten die Rede sein. Soziale Netzwerke fördern bekanntlich Erregung - und das funktioniert hervorragend. Viele User empören sich bis zum Äußersten.

Nicht wenige lassen jeden Anstand vermissen. Sie pöbeln, beleidigen, hetzen oder drohen - in machen Fälle mit dem Tode. Eine bedrückende Verrohung. Natürlich nicht nur im Netz, aber hier wird Hetze sichtbar.

Manche halten die vermeintliche Anonymität im Netz für die Ursache. Oder zumindest für einen Brandbeschleuniger. Bundestagspräsident Wolfgang Schäuble (CDU) hat deshalb vor einigen Tagen erneut eine Klarnamenpflicht gefordert.

Die Hoffnung: Wenn alle sich mit Klarnamen im Netz bewegen, steigt die Hemmung, sich unflätig oder strafrechtlich relevant im Netz zu äußern. CDU-Chefin Annegret Kramp-Karrenbauer ist ähnlicher Ansicht.

Studie belegt: Anonyme User diskutieren weniger aggressiv

Viele halten diese Forderung für "Irrsinn" oder "weltfremd". Das ist zwar eine Meinung, aber noch kein Argument. Ich gebe zu: Auch ich würde annehmen, dass mehr Anstand einzieht, wenn jeder Name bekannt und/oder für jeden sichtbar ist.

Eine Studie der Universität Zürich belegt genau das Gegenteil: Anonyme User kommentieren weniger aggressiv als User mit Klarnamen.

Das einzige Argument, das **für** eine Klarnamenpflicht spricht, scheint also - wissenschaftlich gesehen - ein Trugschluss zu sein. Ich habe deshalb mit Dorothee Bär (CSU) gesprochen, der Staatsministerin für Digitalisierung im Bundeskanzleramt. Ihre Haltung ist eindeutig:

> Ich halte 0,0 von der Klarnamenpflicht. Aus ganz verschiedenen Gründen. Ich kann verstehen, dass man die Hoffnung hat, so wie Sie es formuliert haben, dass es sich dadurch bessert. Ich persönlich sage aber: Allein mir fehlt der Glaube. Natürlich wäre es wünschenswert zu sagen: Lasst es uns doch einfach mal verbieten, diese Pseudonyme und dann wird alles gut. Dann wird eben nicht alles gut.
>
> *Dorothee Bär*.

Klarnamen: Keine echten Vorteile, aber viele Nachteile

Also: Glasklar eine andere Haltung als Wolfgang Schäuble – und übrigens auch als Annegret Kramp-Karrenbauer. Auch sie würde lieber eine Klarnamenpflicht oder etwas Vergleichbares einführen.

Dorothee Bär ist der Überzeugung, dass eine Klarnamenpflicht das Problem nicht löst. Denn heute schon begehen viele Straftaten im Netz unter Klarnamen. Und deutsche Täter zu ermitteln ist auch möglich, wenn keine Klarnamen verwendet werden.

Die Nachteile einer Klarnamenpflicht wären ungleich größer als die möglichen Vorteile. Abgesehen davon ist fraglich, wie sich das überhaupt durchsetzen ließe, wenn man kein komplettes Überwachungs-Internet will.

Daher gibt’s derzeit nur eins: Alles melden und anzeigen, was einem auffällt. Und die Politik muss Behörden und Justiz besser dafür ausstatten. Viel besser!

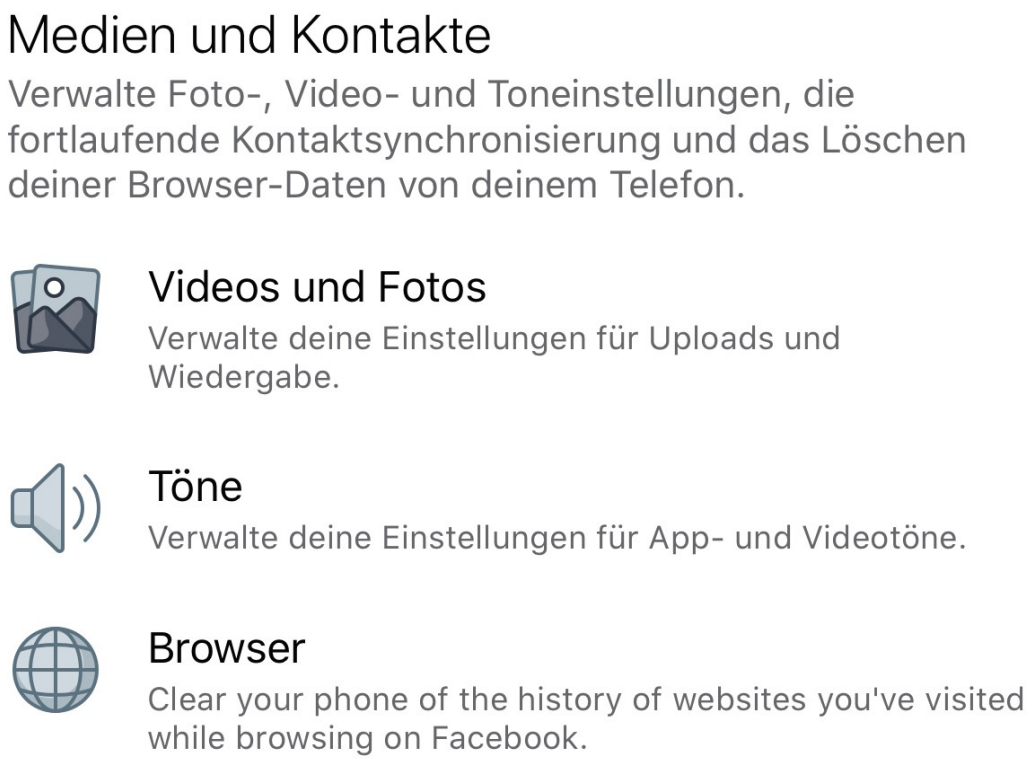
https://vimeo.com/385483373

Hochladen von Filmen und Bildern auf Facebook in HD

Moderne Smartphones haben sehr hochauflösende Kameras und riesigen Speicher. Die Konsequenz: Sie fotografieren und filmen in der best möglichen Qualität. Viele dieser Erzeugnisse wandern dann direkt zu Facebook: Die Welt soll teilnehmen an Ihren Erlebnissen! Die Enttäuschung ist groß, wenn Sie dann den Post anschauen: Aus dem 4K-Video ist plötzlich eine Folge verschwommener Bilder geworden. Das können Sie vermeiden!

Im Standard versucht Facebook, den Speicherbedarf Ihrer Posts so gering wie möglich zu halten. Das bedeutet auch, dass die Fotos und Videos komprimiert werden. Die Verringerung des Speicherbedarfs hat aber einen Nebeneffekt: Die Kompression verschlechtert die Qualität deutlich. Das mag bei Bildern noch tragbar sein, bei Videos aber nicht.

Öffnen Sie Ihre Facebook-App und tippen Sie auf die drei Striche unten rechts. Tippen Sie dann auf **Einstellungen und Privatsphäre** -> **Einstellungen** -> **Medien und Kontakte** -> **Videos und Fotos**.



Sie sehen nun die Einstellungen für die Upload-Qualität getrennt für Fotos und Videos. Aktivieren Sie hier die Option **HD hochladen**. Die App komprimiert dann die hochgeladenen Medien immer noch, allerdings deutlich weniger als bisher. Videos haben dann automatisch die Markierung **HD** in Ihrer Timeline. Allerdings muss der Betrachtende dann immer noch manuell anwählen, dass das Video auch in dieser Qualität abgespielt wird. Das soll Rücksicht darauf nehmen, dass viele Anwender mobil kein unlimitiertes Datenvolumen haben.

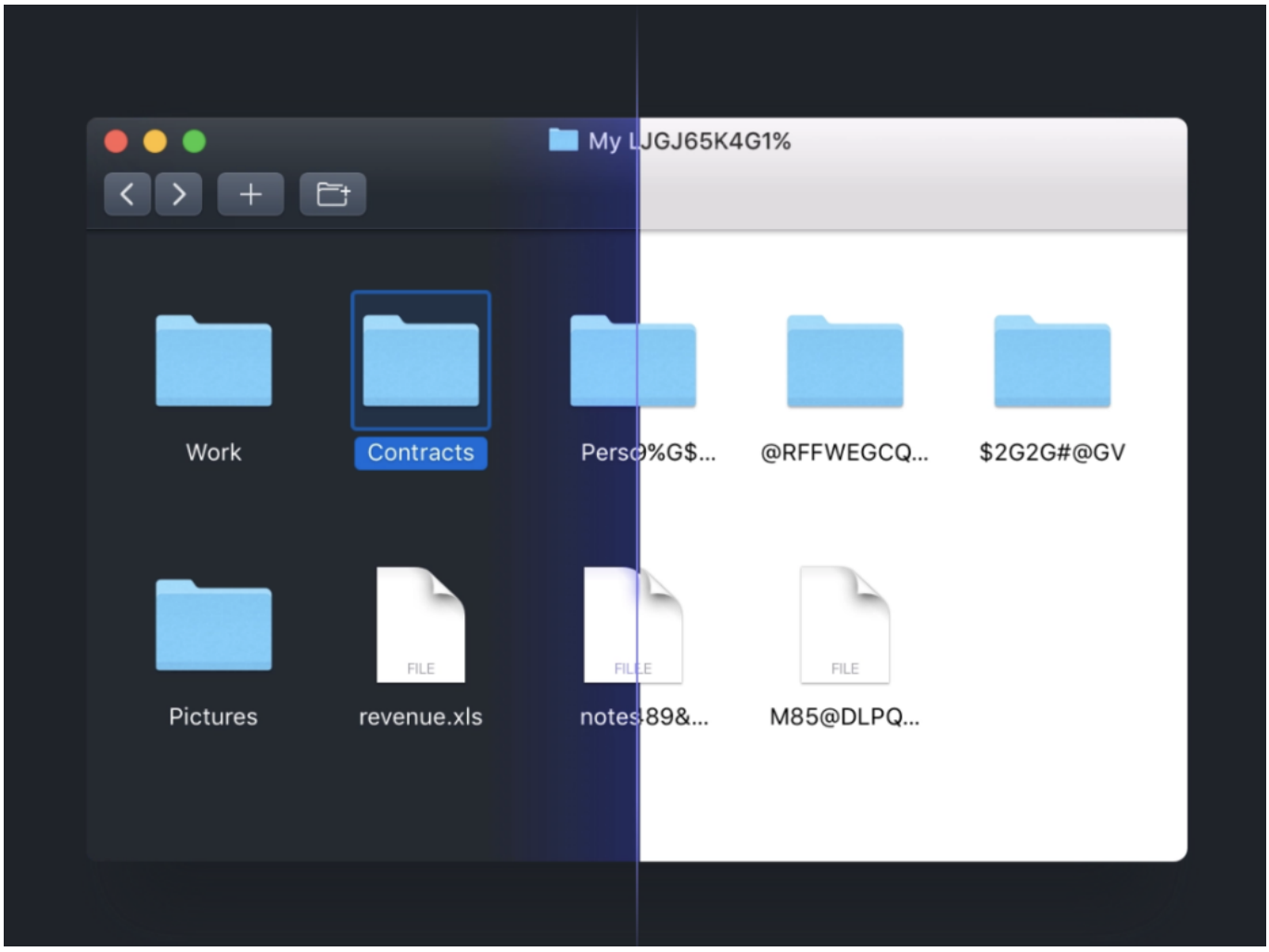

Videos und Fotos
TONEINSTELLUNGEN
Videos im News Feed starten mit Ton
EINSTELLUNGEN FÜR VIDEOS
HD hochladen
Autoplay
Mobile Daten + WLAN
EINSTELLUNGEN FÜR FOTOS
HD hochladen

5 GB gratis Daten absichern mit NordLocker

Die eigenen Daten absichern: Das wird immer wichtiger. Denn Notebooks könnten geklaut werden, Hacker können in PCs eindringen - und es greifen Unbefugte auf gesicherte Daten zu. Erst Recht in der Cloud. Wenn die Daten nicht verschlüsselt sind, haben die Angreifer leichtes Spiel. Doch es lässt sich etwas dagegen unternehmen.

Daten verschlüsseln - das ist wichtig. Damit Unbefugte keinen Zugriff auf sensible oder privte Daten haben. Wer seine komplette Festplatte verschlüsselt, wie es Windows oder MacOS anbieten, macht es schon mal richtig. Dann lassen sich die gespeicherten Daten zumindest nicht "einfach so" auslesen, etwa. wenn die Festplatte ausgebaut und ausgelesen werden soll. Nur mit den passenden Zugangsdaten gibt die Festplatte die Daten frei.

Doch manchmal wünscht man sich eine Art Datentresor. Nur bestimmte Daten sollen gut weggeschlossen werden - solide abgesichert mit einem Schlüssel. Es gibt verschiedene Lösungen, die genau so etwas anbieten. Verschlüsseln on the fly - indem die abzusichernden Dateien in einem speziellen Ordner landen. Schiebt man sie dort hinein, werden sie verschlüsselt und lasssen sich nur mit Schlüssel und Zugangsdaten öffnen.



NordLocker verschlüsselt auch Daten auf Cloud-Laufwerken

Das ist eine gute Sache. Einfach und pratkisch - und ziemlich sicher. Besonders nützlich ist so eine Lösung, wenn sich der Ordner mit den verschlüsselten Dokumenten in der Cloud befindet, etwa auf Dropbox, OneDrive, Google Driver oder wo auch immer. Dann dann landen die Dokumente in der Cloud - und sind trotzdem sicher, da sie von der Verschlüsselungs-Lösung vollkommen automatisch ver- und entschlüsselt werden. Ohne dass man es groß bemerkt.

Eine solche Lösung ist NordLocker. Es gibt Software für Windows und Mac. Einfach laden, installieren und ein Konto einrichten. Wichtig: Den generierten Schlüssel unbedingt an einem sicheren Ort verwahren. Denn wer den Schlüssel und sein Passwort verliert oder verlegt, hat keine Chance mehr, an die gespeicherten Daten zu kommen. Das ist der Preis, den man für mehr Datensicherheit bezahlt. Ich empfehle daher, den Schlüssel sofort auszudrucken und ohne weitere Notiz an einem geheimen, aber sicheren Ort zu verwahrten.

Die Handhabung der NordLocker-Software ist einfach. Bei der Installation legt man den Ordner fest, der für NordLocker die Basis ist. Diesen Ordner kann man auch auf einem Cloud-Drive anlegen, dann landet der Ordner samt Daten automatisch in der Cloud (und wird automatisch synchronisiert). Wer Dokumente oder sogar komplette Ordner in den NordLocker-Ordner zieht, sorgt dafür, das sie automatisch verschlüsselt werden. Zugriff darauf ist nur möglich, wenn NordLocker gestartet und die nötigen Credentials eingegeben wurden.

5 GB sind kostenlos

Natürlich lässt sich NordLocker auch auf mehreren Geräten installieren, um auf allen im Einsatz befindlichen Geräten auf seinen verschlüsselten Ordner zugreifen zu können.

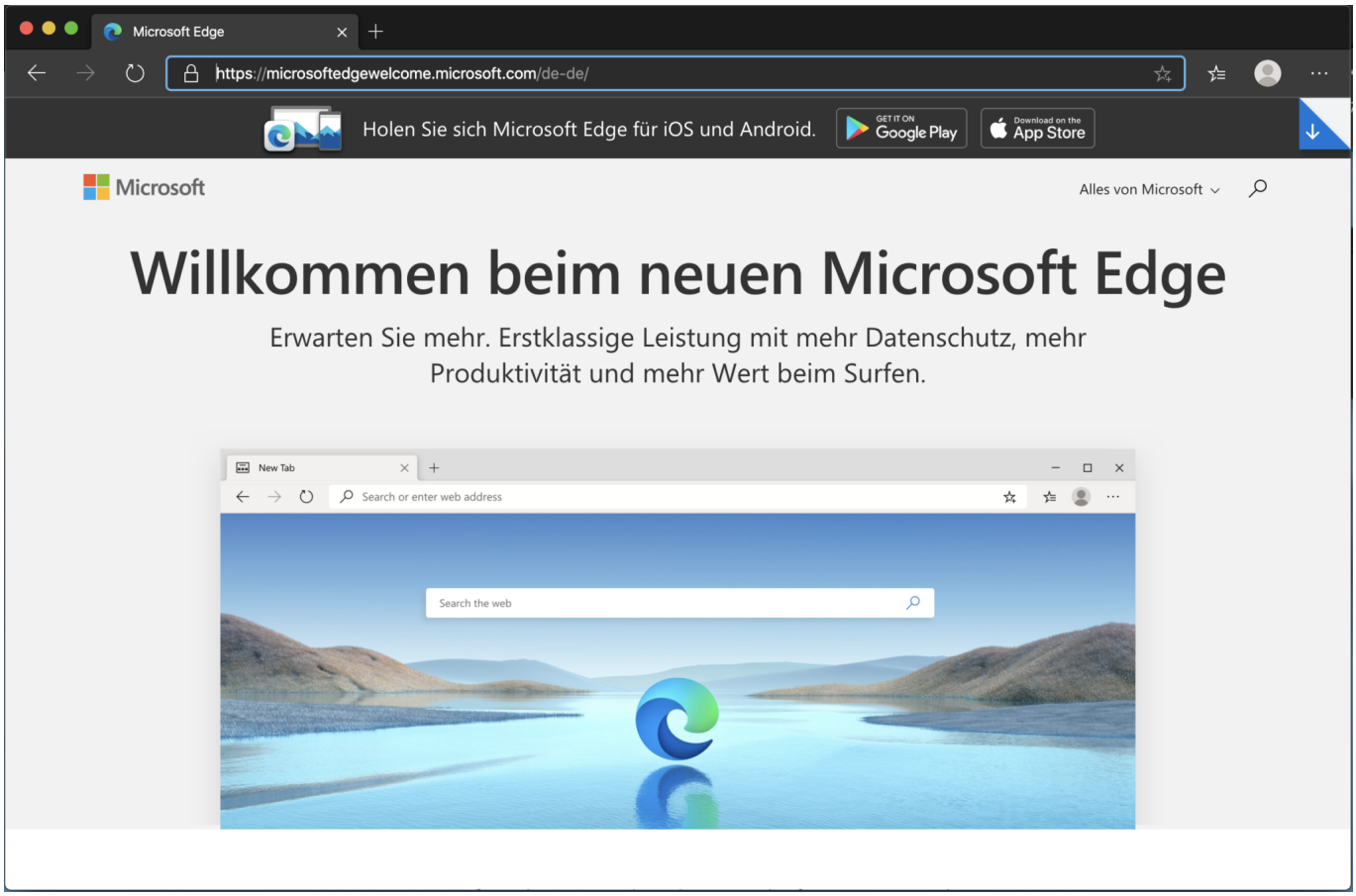
Die ersten 5 GB verschlüsselt die praktische Software kostenlos. Wer auf den Geschmack kommt und mehr verschlüsseln will, muss dann zur kostenpflichtigen Version greifen.

Praktisch: Bei Bedarf lassen sich Dokumente im NordLocker-Ordner auch teilen. Entweder mit Nutzern, die ebenfalls NordLocker verwenden -- dann alles verschlüsselt. Oder indem einzelne Dokumente so herausgegeben werden. Für den Empfänger dann entschlüsselt zu laden. Die Software bietet eine Menge Möglichkeiten, um gespeicherte Dokumente und Daten komfortabel zu verwalten.

Für Technik-Nerd: NordLocker basiert auf GoCryptFS. Ein eigenes Dateisystem, das auf komplette Verschlüsselung setzt - und bei Bedarf auf Ordner und Daten angewendet wird. Dabei kommen bewährte Verschlüsselungsmechanismen zum Einsatz, etwa Argon2, AES256, ECC (mit XChaCha20, EdDSA and Poly1305.

Microsoft Edge Chromium unter Windows ARM

Windows für ARM-Geräte (wie das Surface Pro X) ist ein eigenes Softwarepaket, das auch mit den entprechenden Apps für die Prozessorarchitektur versehen ist. Desktop-Apps werden dann - solange es sich um 32bit-Programme handelt - für den Benutzer unsichtbar durch eine Emulation betrieben. Der neue Edge-Browser läuft auf dem Pro X langsamer als auf echten Windows-Geräten, und das hat einen Grund. Microsoft hatte mit Edge unter Windows 10 den ersten Versuch gestartet, den schon lange in die Jahre gekommenen Internet-Explorer abzulösen. Moderner sollte er sein, schneller, schicker. So recht geklappt hat das aber nie: Erst im November 2019 sind die Marktanteile zugunsten von Edge ausgefallen. Allerdings, nur, weil der Marktanteil des IE deutlich zurückgegangen ist.



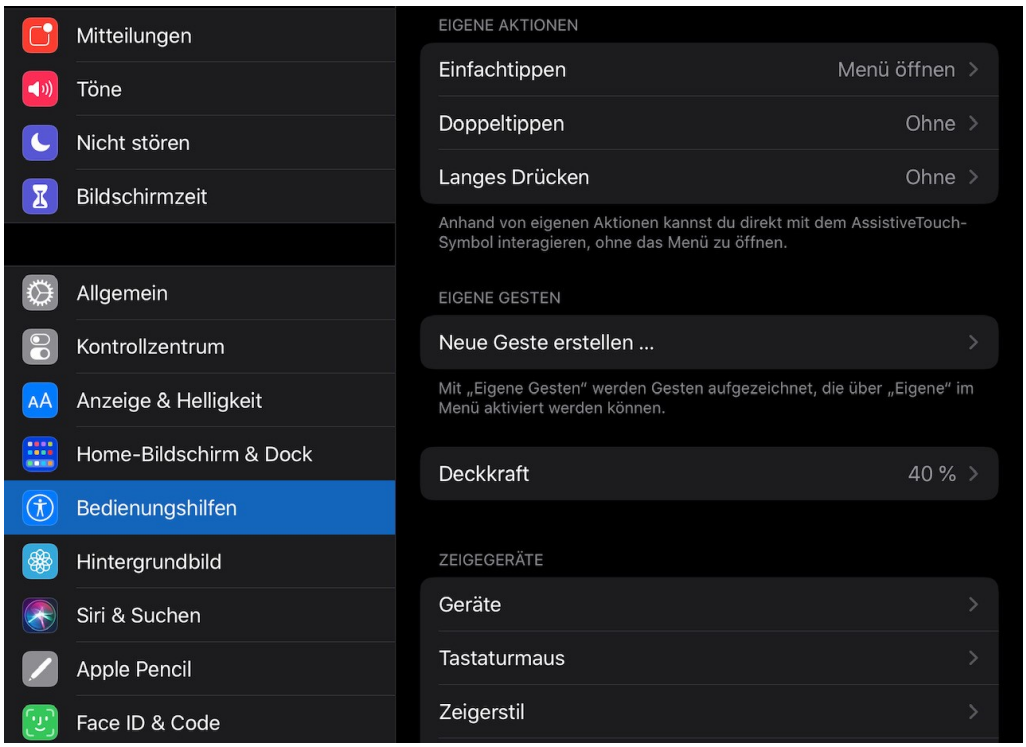
Zuerst sind die klassischen Plattformen bedient worden: "normales" Windows, macOS, iOS und Android. Windows for ARM ist nicht mit der höchsten Priorität versehen gewesen, schließlich läuft die Windows 10-App als 32Bit-App ja in der Emulation. Für einen Browser ist eine Emulation aber nicht ganz optimal, denn der ist auf Performance angewiesen.

Die dedizierte 64bit ARM-Version von Edge soll 5-6 Wochen nach dem Erscheinen der normalen Version verfügbar sein. Wenn Sie nicht warten wollen, dann können sie hier schon die Insider-Version herunterladen. Das ist eine offizielle Betaversion von Microsoft, die schon funktional, aber noch nicht komplett fertig ist.

Anpassen der Mauseinstellungen für das iPad Pro

Eine Maus? Am iPad Pro? Wenn Sie sich diese Frage stellen, dann sollten Sie vorher diesen Artikel lesen. Nachdem Sie die nötigen Einstellungen für die Verwendung einer Maus am iPad Pro vorgenommen haben, können Sie noch einige Einstellungen vornehmen, die Ihnen die Arbeit noch einfacher machen. Wir zeigen Ihnen, wo Sie diese finden.

So ist beispielsweise die Geschwindigkeit des Mauszeigers wie beim PC eine Einstellung, die sehr stark von den Vorlieben des Benutzer abhängt. Was dem einen zu schnell ist, ist für den anderen die optimale Geschwindigkeit. Für die Maus können Sie unter **Einstellungen** -> **Bedienungshilfen** -> **Tippen** -> **Assistive Touch** mit dem Einstellungsregler die für Sie beste Geschwindigkeit einstellen.



Auch die Funktion der Maustasten können Sie direkt in den iOS-Einstellungen konfigurieren. Klicken Sie dazu auf **Einstellungen**▷**Bedienungshilfen**▷**Tippen**▷**Assistive Touch** -> **Zeigegeräte**. Wählen Sie dann in der Liste der Geräte die verwendete Maus aus. Sie können nun einstellen, was bei **Linksklick** (idealerweise ein einfaches Tippen des (virtuellen) Fingers, **Rechtsklick** und bei Drücken der **mittleren Maustaste** passieren soll.

Keine Frage: Die Verwendung einer Maus am iPad ist gewöhnungsbedürftig, vor allem, wenn Sie nur den PC gewöhnt sind. Mit ein wenig Einstellungsarbeit aber gewöhnen Sie sich schnell daran!

Wohin mit den ganzen Geräten? Intelligente Lösungen für Smartphone und Tablet

Lange sind sie Zeiten vorbei, in denen Sie nur ein Smartphone und einen stationären PC hatten. Firmen- und Privattelefon, Tablet, Notebook und noch das eine oder andere weitere Gerät sind immer in Ihrer Nähe und wollen gelagert und geladen werden. Das führt schnell zu Kabel- und Ordnungschaos. Wir zeigen Ihnen intelligente Lösungen, mit denen Sie das vermeiden!

Das Thema Strom bringt bei unterschiedlichen Geräten oft das Problem der unterschiedlichen Ladekabel und Netzteile mit sich. Hier hilft es, dass viele der mobilen Geräte mittlerweile den kabellosen Qi-Standard unterstützen und kabellos zu laden sind. Verschiedene Anbieter (zum Beispiel der Möbelriese IKEA) bieten hier Möbel an, die direkt Qi-Ladepads integriert haben. Legen Sie Ihr Smartphone einfach auf die Ladefläche im Lampenfuß, um es zu laden. Kein Kabel, kein zusätzlicher Platzbedarf. Viele dieser Lampen haben dann sogar noch USB-Buchsen, an denen Sie Geräte, die nicht Qi-fähig sind, laden können. Dann allerdings mit einem Kabel.

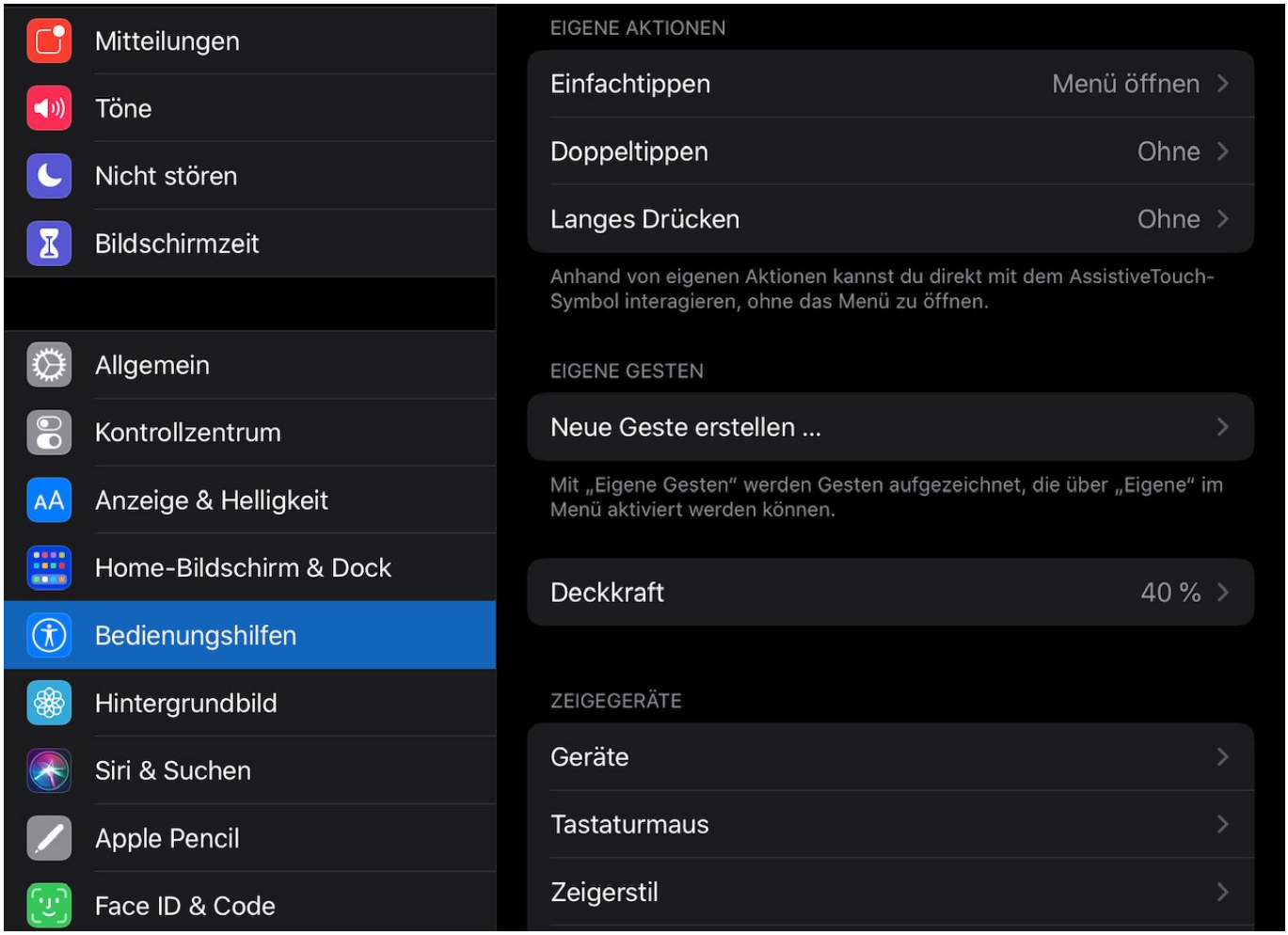
Eine tolle Idee für das Verstauen von Geräten bis hin zu Notebooks ist der Kangaroo Stand von manu.nl. Den stellen Sie neben Ihr Sofa und können darin in verschiedenen Taschen unterschiedliche Geräte laden. Der Clou: Ein Netzteil mit fünf USB-Ports ist schon integriert. So können Sie kleine Geräte direkt mit ihren USB-Kabeln laden, ohne Kabelgewirr zu verursachen.

Alternativ legen Sie den Kangaroo Couch Organizer über eine Seitenlehne der Couch. Neben den Lagerflächen können Sie dann auch noch Geräte per Qi laden!

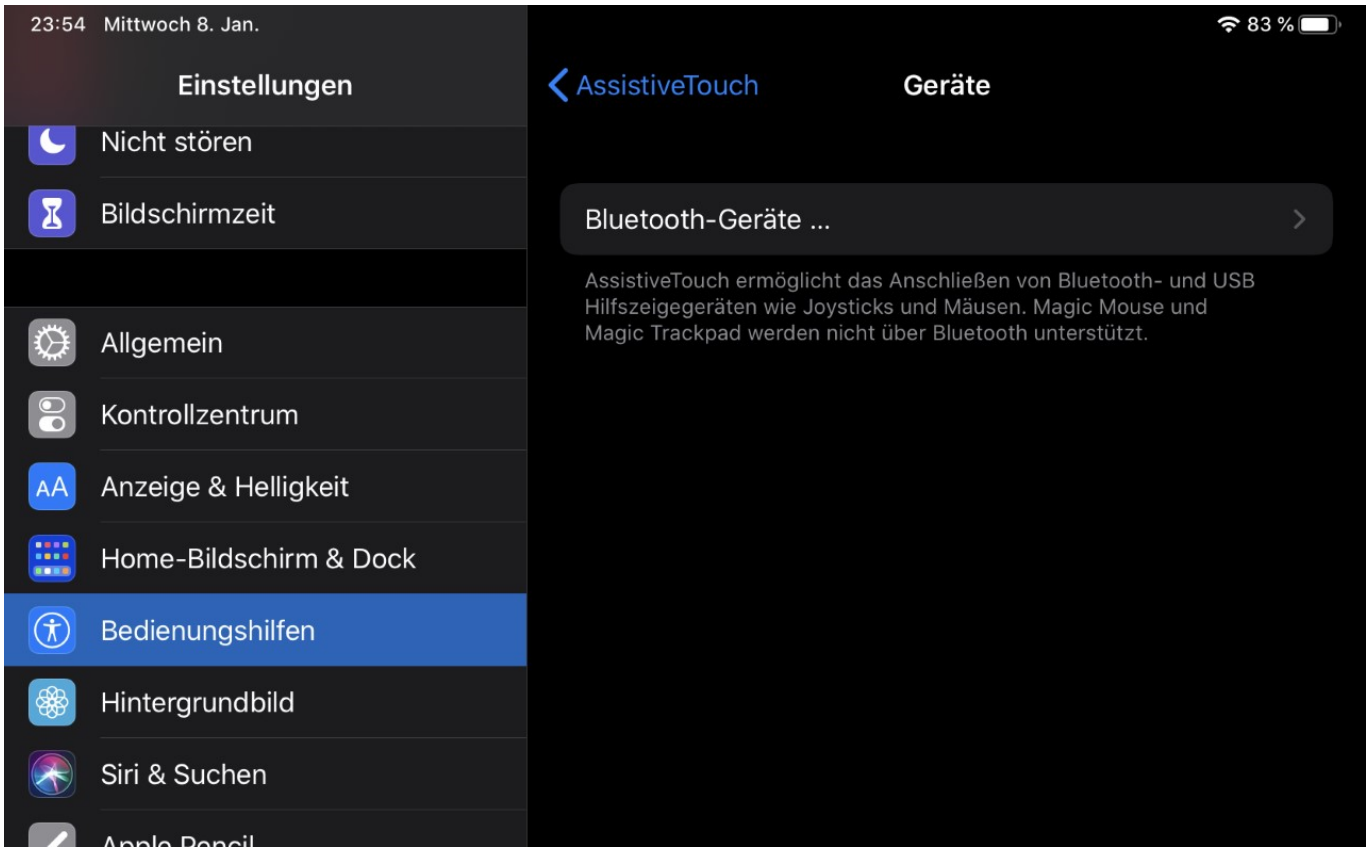
Nutzung einer Maus am iPad Pro

Apple positioniert das iPad mehr und mehr als Alternative zum Notebook oder Business Tablet. Mit dem Smart Keyboard erinnert das iPad schon an ein Notebook, und lässt sich auch fast so bedienen. Was aber fehlt und von iOS immer noch nicht unterstützt wird, ist die Nutzung einer Maus. Wobei die fehlende offizielle Unterstützung nicht bedeutet, dass die Nutzung nicht möglich ist. Wir zeigen Ihnen, wie Sie eine Maus verwenden können.

Apple sieht die Maus für iPad OS nicht primär als Eingabegerät, sondern als Ergänzung und Hilfe für Anwender, die Einschränkungen haben. Folgerichtig finden sich die benötigten Einstellungen unter **Einstellungen** -> **Bedienungshilfen**. Dort müssen Sie als erstes **Assistive Touch** einschalten. Dahinter verbirgt sich die Unterstützung für alternative Zeigegeräte.



Unter Zeigegeräte -> Geräte können Sie nun eine Bluetooth-Maus verbinden. Wichtig dabei: Die Maus muss im Kopplungsmodus sein (konsultieren Sie dafür das Handbuch der Maus) und darf nicht aktuell mit einem anderen Gerät verbunden sein.



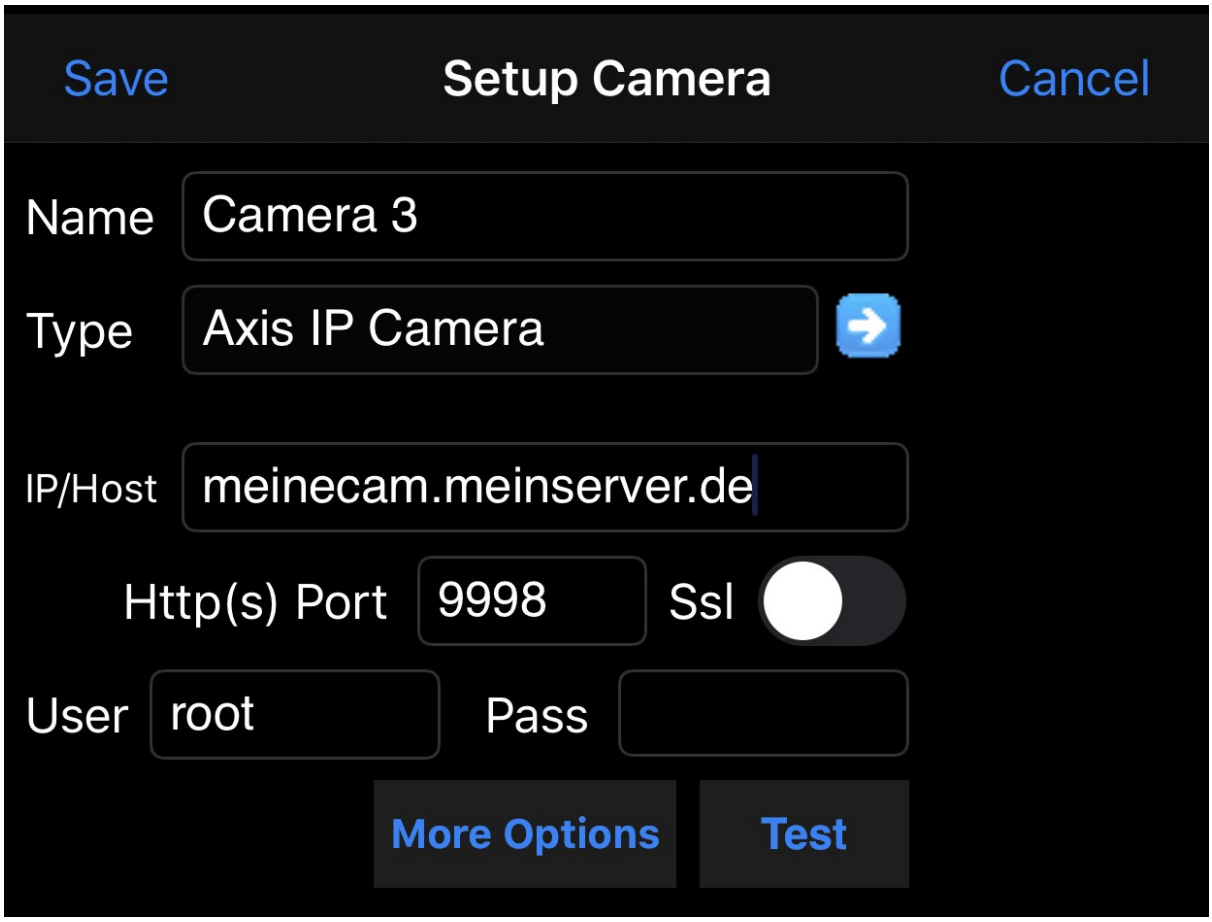
Sollte die Maus bei der Kopplung eine PIN verlangen, so geben Sie an der Stelle 0000 ein. Verwendet Ihre Maus eine eigene, abweichende PIN, dann finden Sie diese im Handbuch der Maus.

Erwarten Sie keinen klassischen Mauszeiger, iPad OS simuliert mit der Maus Ihren Finger. Damit ist der Mauszeiger ein runder Punkt, der Ihre Fingerspitze darstellen soll. Für die Bedienung von Programmen reicht dies allemal.

IP-Webcams mit dem Smartphone abrufen

Smarthome ist in aller Munde, und das Smartphone natürlich das optimale Zugangsmittel, weil Sie es immer dabei haben. Für die meisten Smarthome-Geräte gibt es eine separate App, um das Gerät zu steuern oder darauf zuzugreifen. Bei IP-Webcams, die Sie zuhause oder im Ferienhaus einsetzen, um aktuelle Bilder zu erhalten, ist das nicht der Fall. Es gibt viel zu viele Modelle. Das macht aber nichts: Wir stellen Ihnen den IpCamViewer vor.

Die App IPCamViewer können Sie kostenlos für Android und iOS herunterladen. Nach der Installation müssen Sie Ihre Kamera einrichten. Tippen Sie dazu auf **Add Camera**. Die App enthält unter **Type** eine Vielzahl von Herstellern und Modellen. Selbst wenn die spezielle Kamera nicht aufgeführt ist, funktionieren meist auch andere Modelle. Nach der Eingabe der URL, unter der die Kamera erreichbar ist, geben Sie Benutzername und Kennwort ein. Durch einen Klick auf Test baut die App die Verbindung zu Kamera auf.

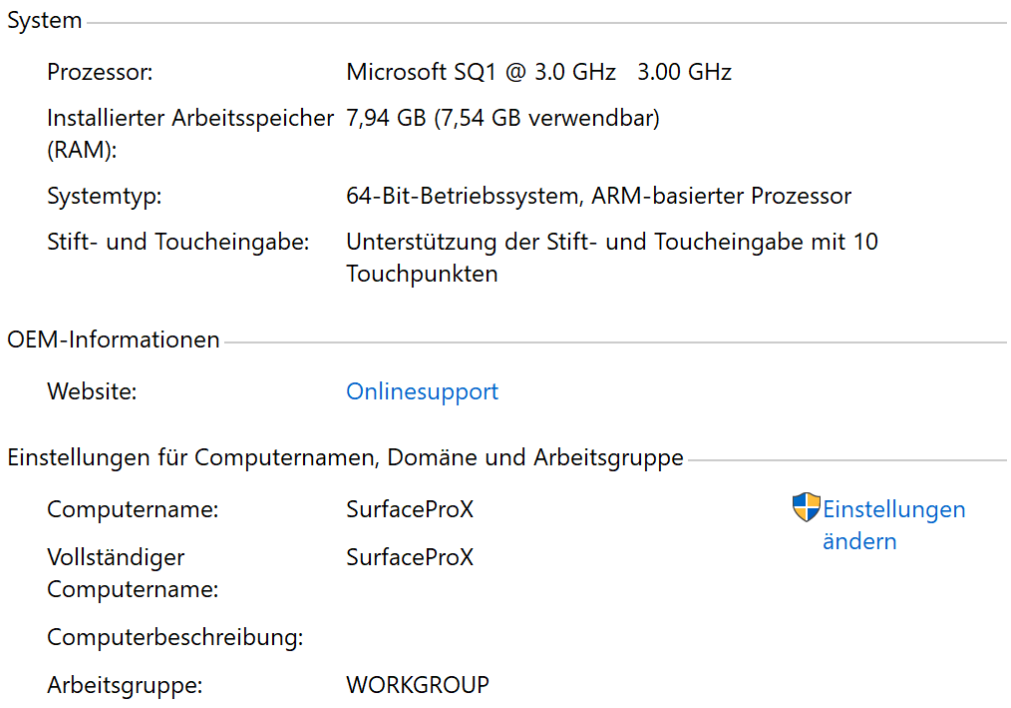


Im Idealfall bekommen Sie nun direkt das Live-Bild der Kamera angezeigt. Ist das nicht der Fall, dann kontrollieren Sie die Adresse der Kamera, den Port sowie Benutzername und Kennwort. Wichtig auch: Wenn Sie die Kamera im heimischen WLAN erreichen, dann genügt die IP-Adresse. Soll der Zugriff auch von Außen erfolgen, dann müssen Sie sie aus dem Internet erreichbar machen. Wie das geht, lesen Sie hier.

Surface Pro X: Windows auf ARM

Die Surface-Reihe von Microsoft hat schon die eine oder andere Überraschung gebracht: Allem voran das bis zur Präsentation nicht geleakte Surface Book mit seinem abnehmbaren Display, auch das Surface Duo und Neo, die Ende 2010 erscheinen sollen. Da war man von der Präsentation des Surface Pro 7 wenig überrascht: Viel interessanter schien das das SurfacePro X mit seinem deutlich moderneren Design, den kleineren Bildschirmrändern (neudeutsch „Bezel“) und dem doppelten USB-C-Anschluß. Mit einem ARM-Prozessor. Was heißt das für den Anwender?

Diesmal kommt der selbst entwickelte SQ-1-Prozessor zum Einsatz. Garant für Performance und Abstimmung, so der Ansatz. Allerdings: ARM-Prozessoren benörigen eigene Apps. Unproblematisch bei Store-Apps, aber eben nicht geeignet für Desktop (x86-) Apps. Dafür hat Microsoft dem System einen Emulationsmodus verpasst, der x86-Apps laufen lassen kann. Wie bei jeder Emulation aber natürlich mit Perdformance-Einbußen. Und noch schlimmer: 64bit-Apps schafft der Emulator nicht. Entweder ist eine App also direkt als ARM64-App verfügbar, oder der Anwender schaut in die Röhre.



Soweit zur Theorie. Wie aber schlägt sich das Surface Pro X in der Praxis? Die kurze Antwort: Besser als erwartet, wenn man die ein oder andere Einschränkung in Kauf nehmen mag.

Von der Hardware an sich ist das Surface Pro X ein wunderschönes Gerät: Mattschwarz, das Microsoft-Logo wie bei den Pros gewohnt glänzend auf dem Kickstand. Deutlich schmalere Bildschirmränder als die Geschwister, damit von der Wirkung her deutlich größer. Das 13 Zoll PixelSense-Display mit einer auflösung von 2880*1920 ist kontrastreich, superscharf und mit 450 nits auf höchster Stufe extrem hell. Mit 774 Gramm knapp 150 Gramm schwerer als das

12.9 Zoll iPad Pro, aber immer noch in der Hand haltbar. Zwei Dinge aber sorgen für Verwunderung: Der nicht mehr vorhandene Kopfhöreranschluß mag zu verschmerzen sein, das ist mittlerweile Standard bei mobilen Geräten und durch Adapter heilbar. Viel schlimmer (und mir tatsächlich komplett durchgegangen): Das Surface Pro X hat keine Speicherkartenslot. Das Standardvorgehen, eine kleine SSD mit einer 400GB microSD zu ergänzen, ist also hinfällig.

Apropos SSD: Die kommt auch von Microsoft und ist proprietär. Wer sich einen Wechsel der internen SSD überlegt hat, kann das getrost vergessen…

Die zwei USB-C-Ports lösen das Problem, dass beim Anschluss eines USB-C-Hubs ohne Ladestecker der Platz für den selbigen fehlt. Bei den Surfaces eh kein Problem, denn der Dock Connector ist ebenfalls mit dabei. Übrigens der selbe wie bei den Vorgängern, sodass die originale Dock und Netzteile weiterhin Verwendung finden können. Die kompletten Specs finden sich hier.

In der Theorie also ein tolles Gerät, haptisch wie optisch ansprechend. Technisch wünscht sich der eine oder andere Anwender Thunderbolt 3 statt USB-C, ich muss aber gestehen: Die Anwendung habe ich noch nicht gehabt. Die höheren Transferraten wie auch spezielle TB3-Hardware gehören nicht zum Standard.

Nur spezielle Programmme für ARM?

In der Praxis geht man erst einmal vorsichtig an das Gerät. Erst einmal die Software installieren,

die nicht aus dem Store kommt, und die man wirklich braucht. Und bei jeder Installation hält man die Luft an, ob das denn nun alles funktioniert. Dieser Vorgang wird deutlich entspannter, wenn man die Erwartungshaltung korrigiert: 64Bit Desktop-Apps, Antivirensoftware, CAD-Software und spezielle Gerätetreiber sind ein NoGo. So scheiterte die Installation von Bitdefender 2020 ganz am Ende, weil eine Komponente nicht installiert werden konnte. CyberGhost als VPN-Tool hatte ich eher abgehakt, trotz Fehlermeldung (die ich aber auch vom Surface Book in Erinnerung hatte) läuft es problemlos. Wie auch alle anderen Programme. Wie es immer so ist: Die Office-Aktivierung scheiterte, weil „Dieser Typ Gerät nicht aktiviert werden dürfe“. Genaueres Lesen . nach dem ersten Schock – zeigte dann aber die Zahl der aktivierten Lizenzen bei Office 365 (und nicht den ARM-Prozessor) als Ursache. Behoben, aktiviert, läuft.

Das Surface Pro X bzw. sein SQ-1-Prozessor soll oberhalb des i5-Prozessors liegen. Schwer zu testen, denn die gängigen Benchmark-Programme – tadaaa! – laufen auf ARM nicht. Gefühlt ist das Surface Pro X flott unterwegs. Emulierte X86-Programme haben dann und wann spürbare Einbrüche, die an der Kreiselsanduhr zu erkennen sind. Allerdings wenig reproduzierbar und nicht so, dass sie ein wirklicher Bremser wären.

Unverständlicherweise ist das LTE-Modul eines der besonderen Merkmale des Pro X. Microsoft hat nur wenigen Modellen bisher die integrierte Möglichkeit des mobilen Surfens spendiert. Beim Pro X ist der Nano-SIM-Slot keine Option, sondern Serienausstattung. Karte rein, WLAN aus und Mobilfunk an, PIN eingeben, und das wars. So einfach wie bei einem iPad. Der Slot befindet sich unter dem Kickstand und bedecktsowohl die SSD als auch eben den Slot. Gelöst wird die Abdeckung durch die beiliegende SIM-Nadel.

Mit an Bord ist einmal mehr die Infrarotkamera, die im Zusammenspiel mit Windows Hello die Anmeldung über einen 3D-Scan des Gesichts erlaubt. Gefühlt ein wenig schneller und unempfindlicher als beim Surface Book 2, auch wenn es keine unterlegenden Zahlen dazu gibt.

Wie alle Surface Pro bietet Microsoft optional (!) das Type Cover an, eine an den unteren Dock-Port magnetisch anzuklickende Tastatur. Und einen Stift. Hier ist eine weitere Weiterentwicklung der Reihe zu finden: Die höherwertige Version des Covers für das Pro hat eine Aussparung für den neuen Surface Slim Pen. Der ist deutlich flacher als die Standardversion des Surface Pens und wird induktiv aufgeladen. Entweder im Type Cover, wenn das am Surface hängt. Kauft man den Pen alleine, dann liegt eine USB-Ladestation bei. Fakt ist: Die Kombination aus Stifthalter und Ladeschale im Cover führt dazu, dass der Stift deutlich öfter mit an Bord ist als der nur magnetisch am Gehäuse zu befestigende Standard-Pen. Cooler Effekt: durch gepolte Magnete kann man den Stift nicht falsch einlegen: Er dreht sich automatisch richtig herum. Allerdings schlagen für die Kombination Cover/Stift noch einmal knapp EUR 300 zu Buche...

Die Akkulaufzeit war eines der Hauptargumente für ARM als Plattform. Das wirkt sich aber nicht wirklich auf die Laufzeit des Pro X aus: Die von Microsoft angegebenen 13 Stunden sind im Praxisbetrieb Surfen, Office und E-Mail nicht annähernd zu erreichen: Knappe 8 Stunden waren bisher das Maximum. Keine Frage, Firmwareupdates und Gewöhnung des Akkus können hier noch ein wenig rausholen, trotzdem: Das Gerät bewegt sich im Bereich seiner

Vorgänger und Geschwister.

Fazit

Es bleibt die Frage: Warum ein Pro X und nicht ein günstigeres und leistungsfähigeres Pro 7? Die Antwort ist schwer. Bei vielen Anwendern führen das Design und zum anderen das „endlich was Neues!“ zum Kauf. Bereuen tut man ihn nicht, wenn es sich um ein Zweitgerät handelt. Als Hauptgerät würde man vermutlich tatsächlich eher zum Pro 7 oder Surface Laptop greifen. Einzig integriertes LTE und die geringe Dicke/das geringe Gewicht sprechen noch für das Pro X.