iOS
Datenschutzfreundlich

untertauchen.info

WIDMUNG

Ich widme diesen Text all denen, die sich um Menschenrechte jedweder Art kümmern, die sich einsetzen, kämpfen und nicht locker lassen. Bitte gebt nicht auf.

INHALTSVERZEICHNIS

DANKSAGUNG

Es gibt viele Menschen, denen ich danken kann und will. Michael Bazzell, der mit seinem Podcast mein Leben verändert hat. Mike Kuketz's Blog, Security Now Podcast, den GrapheneOS Entwicklern uvm.

EINFÜHRUNG

Apple baut tolle und auch sehr sichere Geräte. Sie sind “hipp”. Die Software funktioniert gut, die Geräte sind sicher und wenn man noch ein Apple TV, ein iPad, ein MacBook etc. hat, harmonieren alle ganz wunderbar miteinander.

Der Preis für die störungsfreie, anwender-freundliche Integration ist, dass Apple Daten sammelt. Viele Daten. In macOS sind es über 90 Prozesse, die nach Hause telefonieren. Apple verkauft keine oder sehr wenige Daten an andere. Doch der Gewinn durch Werbung in ihrer Jahresbilanz steigt stetig.

Außerdem sind die Geräte relativ teuer. Sie bezahlen die Infrastruktur, die auch zum Sammeln Ihrer Daten genutzt wird, mit.

Trotz des Preises und der Sammelei fällt es mir sehr schwer, Menschen von GrapheneOS zu überzeugen. Die Bequemlichkeit und Einfachheit von iOS sind sehr überzeugend. Nicht jeder hat meinen Anspruch an Datenschutz. Daher höre ich immer wieder die Frage: Ich will mein iPhone behalten, aber ein bisschen mehr Datenschutz wäre schon gut. Was also tun?

Zuerst müssen wir Datenschutz aufspalten: Das, was Apple erhält und das, was alle anderen beim Surfen oder bei Verwendung von Apps einsammeln.

Auf iPhones und iPads kann man das Sammeln von Apple nur sehr eingeschränkt unterbinden. Zumindest nicht wie bei macOS. Aber ganz hilflos ist man nicht.

Ich versuche, das absolute Maximum an Daten-schutz und Privatsphäre zu erreichen. Das muss nicht Ihr Profil sein. Ich mag Dinge übersehen oder nicht besser wissen. Daher entscheiden Sie selber, welche Einstellungen Sie vornehmen möchten und welche für Sie nicht aktzeptabel sind.

Nicht alle Einstellungen beschreibe ich und erkläre warum, aber bei denen ich denke, es könnte hilfreich sein, gibt es einen kurzen Kommentar.

Ich glaube, dass der Datenschutz und die Sicherheit eines benutzerdefinierten, nicht mit Google-Software versehenen Android-Geräts (z. B. GrapheneOS), jedem im Handel erhältlichen Apple- oder Android-Handy weit überlegen ist. Verstehe aber auch die Beweggründe, doch ein iPhone zu kaufen.

Hinweis: Wenn Sie kein neues iPhone gekauft haben und Ihres auch nicht zurücksetzen wollen, dann steigen Sie ab Kapitel 5, Einstellungen ein. Es sei denn, Sie interessiert es sowieso.

IOS UND GRAPHENEOS

Ich möchte noch einmal betonen, dass ich iOS-Geräte nicht mehr täglich benutze und sie nur selten Leuten empfehle, die auf ein GrapheneOS-Gerät umsteigen könnten. Als ich dieses Kapitel geschrieben habe, habe ich ein iPhone SE mit iOS 16.6 verwendet, um alle Einstellungen zu testen.

Wenn man nicht täglich mit dem Gerät arbeitet, oder auch aus anderen Gründen, macht Apple manchmal Druck, Daten abzugeben. Folgendes ist bei mir schon vorgekommen: Ich wollte einfach eine kostenlose App herunterladen, da blockiert mich Apple. Sie wollten wieder mein Passwort. Danach verlangten sie, dass ich die gespeicherte Telefonnummer überprüfe. Sie verlangten dann, dass ein Code an diese Nummer gesendet wird, sendeten ihn aber manchmal einfach nicht. Sie senden den Code auch nicht an die hinterlegte E-Mail-Adresse. Alles, was Sie versuchten, damit ich Zugang zu meinem eigenen Konto erhalte, schlug fehl. Apple sperrte mir den Zugang zum App Store, nur weil ich eine kostenlose App herunterladen wollte. Dies beschreibt einen Fall für meine Abneigung gegen Apple. Das passt auch zu meinem Eindruck, dass mir nichts mehr gehört. Selbst wenn ich das iPhone gekauft habe, nichts falsch mache, können die Firmen, in diesem Fall Apple, mir die Nutzung entziehen oder stark einschränken. Oder, wie Apple das gerade voran treibt, mich überwachen.

Würden Sie ein iPhone kaufen, wenn Sie wüssten, dass Sie keine zusätzlichen Apps herunterladen können? Wären Sie betroffen, wenn Apple den Zugriff auf neue Apps oder die Inhalte von iCloud blockieren würde? Ich kenne unzählige Fälle, in denen ich oder andere unterwegs waren und das iOS-Gerät nur eingeschränkte Funktionen hatte. Deshalb ziehe ich es immer vor, Geräte zu verwenden, die kein aktives Online-Konto erfordern, um vollen Zugriff auf das Gerät zu erhalten. Apple hat die Macht, Sie jederzeit auszusperren oder zu überwachen. Apple entscheidet, welche Apps Sie installieren können. Es gibt keinen alternativen App Store, wie bei Android. Apps, die legal in Deutschland sind, lässt Apple im App Store nicht zu. Der Kundensupport wird Ihnen bei derartigen Problemen nur dann helfen, wenn Sie alle Abfragen zu deren Zufriedenheit beantworten können. Wenn Sie verschiedene Praktiken zum Schutz der Privatsphäre anwenden, wird Apple dies oftmals nicht akzeptieren und seine Hilfe verweigern.

Bei GrapheneOS habe ich diese Probleme nicht. Keine Daten werden über mich gesammelt, ich muss keine Telefonnummer hinterlegen, diese wird nicht alle paar Minuten mit der Geräte-ID und anderen, eindeutigen Identifizierern an eine Firma in den USA geschickt. Ich kann alternative App Stores und jede App, die ich nutzen will, herunterladen, installieren und nutzen. Mein Gerät gehört mir. Und kostet nur die Hälfte. Hinzu kommt, dass der GrapheneOS Support in deren Chats technisch/inhaltlich überragend und in Echtzeit

stattfindet. Ja, der Stil der Entwickler ist manchmal etwas rüde oder „nerdig“. Aber bisher haben sie mir immer in Echtzeit, direkt, geholfen.

Wenn ich Freunde oder Teilnehmer meiner Seminare nicht davon überzeugen kann, zu GrapheneOS zu wechseln, ist ein iPhone die zweitbeste Wahl. Ich halte iPhones für sicher und Apple macht sicherlich vieles richtig. Aber sie sammeln auch wie verrückt Daten und setzen mehr und mehr mit Werbung um. Hinzu kommt, dass die Apps aus dem App Store oft Daten sammeln, die Hinweise im App Store zur Datensammlung falsch sind und viele Apps Ihren Wunsch, nicht getrackt zu werden, einfach ignorieren.

Wir können niemals ein GrapheneOS Gerät in einem iPhone nachbilden, aber wir können viele der allgemeinen Strategien auf ein iOS Gerät für den täglichen Gebrauch anwenden.

VORBEREITUNG

Für diesen Artikel gehe ich davon aus, dass Sie ein brandneues (bevorzugt) oder werkseitig zurückgesetztes Gerät in den Händen halten (Einstellungen > Allgemein > iPhone Übertragen/Zurücksetzen > Alle Inhalte und Einstellungen löschen).

Verwenden Sie den folgenden Link, um alle Vorbereitungen zum Zurücksetzen auszuführen:

https://support.apple.com/de-de/HT201351

Wenn Sie nicht alles komplett löschen und zurücksetzen, ist der Datenschutzefffekt reduziert. Weil Apple Ihre Telefonnummer und Ihre IMEI (ist eine 15-stellige Seriennummer, anhand derer jedes GSM– oder UMTS–Endgerät weltweit eindeutig identifiziert werden können soll) sowie eine Apple Geräte-ID erhält. Sollten Sie wirkliche einen Datenschutz-Reboot anstreben, benötigen Sie ein neues iPhone mit einer anderen Telefonnummer und wie ich später noch erkläre, einer anderen Wohnung. Ok, das ist für 99% aller Menschen ein bisschen übertrieben.

Um Ihre Privatsphäre zu schützen, sollte dieses Gerät niemals von zu Hause aus konfiguriert werden. Das gilt auch für Betriebssystem-Updates. Die meisten iPhones haben Standortdienste, Wi-Fi, Bluetooth und Mobilfunkverbindungen standardmäßig aktiviert. Während ich das schreibe, habe ich eine neue Version

installiert. Ich hatte nur das Mobilfunknetz angeschaltet. Nach der Installation hat Apple alles erstmal aktiviert. Und sammelt damit schon viele Daten. Außerdem kennt Apple Ihre Wi-Fi Namen zu Hause. Daher wäre es ideal, das Handy nicht mehr im heimischen Netz zu nutzen. Es ist nicht bekannt, ob Apple tatsächlich die verbundenen WLANs auswertet und damit die Profile befüllt. Die meisten Sicherheitsforscher, die ich gesprochen habe, meinen: Sie können es, machen es aber wohl nicht.

Zur Erinnerung: Ich versuche das Maximum auszuloten. Apple macht einem das nicht leicht.

Durch die Erstinstallation im heimischen WLAN könnte Ihr Konto aufgedeckt und mit Ihrem Wohnort in Verbindung gebracht werden. Google, Apple und Microsoft verwenden sog. WLAN-Maps, um Sie besser lokalisieren zu können. Außerdem werden bei den meisten Apple-Updates alle Funkverbindungen wieder aktiviert, s.o.. Wenn man seinen Standort also privat halten möchte, kann man Updates nur an einem anderen Ort machen. Wobei man auch betrachten muss: Apple scannt bei aktiviertem WLAN die Umgebung und wertet die ersten drei Ziffernpaare der MAC-Adresse, die den Hersteller des WLAN-fähigen Geräts darstellt, aus. Damit weiß Apple zumindest, von welchen Firmen Sie WLAN-fähige Geräte haben. Das kann ein schönes Fingerprinting ergeben. Es ist mir unbekannt, ob Apple diese Information für die Profilbildung verwendet. Wäre das so und Sie möchten mit dem neuen Gerät ein komplett neues Profil mit Apple eröffnen, dürften Sie das

iPhone nicht mit dem WLAN verbinden. Sie dürften das Wi-Fi Modul im iPhone zu Hause nicht mal aktivieren, weil die Geräte um Sie herum mit hoher Wahrscheinlichkeit ein einmaliges Profil an Geräten in Ihrer Umgebung darstellen. Zumal sich die Wi-Fi Netze wohl selten ändern.

Es gibt Sicherheits-bedürftige Menschen, die genau das tun: Sie verwenden das iPhone nicht zu Hause und haben dafür ein separates Gerät, dass nur zu Hause benutzt wird. Sie packen das iPhone mehrere Kilometer von zu Hause entfernt in einen Faraday-Bag, der alle Funkverbindungen unterbindet. So kennt weder Apple noch der Mobilanbieter Ihr zu Hause. Dabei muss man bedenken: In Deutschland kennt der Mobilfunkanbieter durch den Vertrag den Wohnort sowieso. Man kann das umgehen, aber das führt zu weit. Das alles ist für Sie Overkill, vielleicht. Aber es gibt Gründe für ein derartiges Verhalten. Dem können Sie mit einem GrapheneOS Handy entgehen.

Weiter mit dem iPhone.

Sobald Sie Ihr neues oder zurückgesetztes Gerät haben, können Sie alle Einstellungen konfigurieren und ein Apple-ID-Konto einrichten. Dabei gibt es eine Menge zu beachten. Wenn Sie ein neues Gerät gekauft haben, ist dies eine gute Gelegenheit, eine neue Apple-ID und ein Prepaid-Mobilfunkkonto einzurichten, um das Tracking Ihrer alten Konten zu beenden und die Datenerfassung mit anonymeren Daten neu zu starten. Installieren Sie es

im Apple Store, dort gibt es schnelle Netze und im Zweifelsfall Support.

Im nächsten Kapitel legen wir praktisch los.

INSTALLATION

Führen Sie die folgenden Schritte auf Ihrem neuen oder zurückgesetzten Gerät durch, das auf iOS 16.6 basiert. Künftige Versionen können etwas anders aussehen.

Schalten Sie das iPhone an.

- Wählen Sie die Sprache und Region aus, dann unten „Manuell konfigurieren“.
- Wählen Sie das Wi-Fi, mit dem Sie die Installation durchführen wollen und tippen auf „Weiter“. Wenn Sie einen Reboot ausführen oder diesen Schritt hier von zu Hause durchführen, weiss Apple ab hier, dass Sie der alte Kunde sind. Sie sollten dann zumindest hinter einem VPN zu Hause sein und ggf. einen anderen als den üblichen Server einstellen. Daher ist es am besten, wie beschrieben, das woanders auszuführen. Vielleicht ja im Apple Store. Die haben schnelle Netze.
- Bei der Frage nach „Daten & Datenschutz“ sagen Sie „Weiter“. Aber Sie können auch auf „Weitere Infos“ gehen und mal schauen, was Apple so alles sammelt und zu welchen Themen. Sehr unterhaltsam, für eine privatsphäre-freundliche Firma.
- Wenn Sie Touch ID oder Face ID benutzen wollen, konfigurieren Sie es entsprechend.
- Nun werden Sie nach einem Code gefragt. Tippen

Sie auf Codeptionen und wählen Sie „Eigener numerischer Code“ aus. Oftmals werde ich gefragt, wieso nicht alphanumerisch. Auf einem iPhone empfinde ich diese Eingabe etwas fehleranfällig, wenn es auch sicherer ist. Aber ein langer numerischer Code ist aus meiner Sicht auch gut.

- Nutzen Sie ein starkes Passwort. Nicht nur vier Ziffern, 0000. Nutzen Sie mehr Zeichen. Ich nehme in der Regel 12. Tippen Sie auf „Weiter“.
- Bestätigen Sie den Code und tippen Sie auf „Weiter“.
- Wählen Sie „Keine Apps und Daten übertragen“ aus.
- Wählen Sie „Passwort vergessen und noch keine Apple-ID?“ aus.
- Wählen Sie „Später in Einstellungen konfigurieren“ aus.
- Bestätigen Sie die Abfrage.
- Die Allgemeinen Geschäftsbedingungen müssen Sie „Akzeptieren“, sonst geht es nicht weiter. Lesen Sie auch hier mal durch, was der Hüter der Privatsphäre so alles meint zu schützen.
- „Automatisches Aktualisieren“ schalte ich aus, da es schon mehrmals vorkam, dass Apple Updates zurückgezogen hat oder schnell ein anderes nachschieben musste. Daher wähle ich „Nur automatisch laden“ aus.
- „Ortungsdienste deaktivieren“ ganz unten.

- Bestätigen Sie das mit „OK“.
- Bei Siri tippen Sie auf „Später konfigurieren“.
- Dasselbe bei Bildschirmzeit.
- Bei iPhone Analyse stellen Sie sicher, dass Sie diese nicht teilen.
- Wählen Sie die gewünschte Darstellung und Zoom aus.
- Wählen Sie „Los geht’s“ aus oder wischen Sie nach oben, um aus dem Menu zu kommen.
- Oftmals kommt noch ein Fenster: Konfiguration abschliessen. Tippen Sie auf „Später“.

Damit ist der erste Teil beendet. Sie haben ein neues oder zurückgesetztes Gerät aufgesetzt und die wesentlichen Sammlungen, die Sie beeinflussen können, minimiert.

EINSTELLUNGEN

Hinweis: Wenn Sie kein neues iPhone gekauft haben und Ihres auch nicht zurücksetzen wollten, können Sie hier einsteigen.

Sobald Sie im Home-Bildschirm sind, sollten Sie die App „Einstellungen“ öffnen und die folgenden Konfigurationen vornehmen. Beachten Sie, dass einige dieser Einstellungen möglicherweise Funktionen deaktivieren, die Sie für wünschenswert halten, und dass einige der hier aufgeführten Optionen auf Ihrem Gerät möglicherweise nicht vorhanden sind. Prüfen Sie alle Änderungen und nehmen Sie die Einstellungen vor, die für Ihre Verwendung am besten geeignet sind.

- Öffnen Sie die „Einstellungen“. Sie sehen bei Konfiguration abschliessen einen roten Kreis mit der Zahl 1. Ignorieren Sie das.
- Einstellungen > Bluetooth: Aus.
  Aktivieren Sie es nur, wenn Sie es benötigen. Bluetooth ist eine unterschätzte Datenquelle und Ziel von Hackern.
- Einstellungen > Mitteilungen > Geplante Übersicht: Aus.
- Einstellungen > Mitteilungen > Vorschau zeigen: „Nie“ oder „Wenn entsperrt“.
  Was habe ich im Zug schon an Nachrichten im gesperrten Bildschirm von anderen gelesen…
- Einstellungen > Mitteilungen > Bildschirm-

freigabe: Aus.

- Einstellungen > Mitteilungen > Siri Vorschläge: Alle aus.

Hinweis: Sie haben Siri nicht aktiviert und trotzdem ist hier alles scharf gestellt. Das hält Apple von Ihrer Meinung zum Datenschutz.

- Einstellungen > Mitteilungen: Deaktivieren Sie alle Mitteilungen von sensiblen Apps oder wo immer Sie das nicht wollen oder benötigen. Was für Sie sensibel ist, entscheiden Sie.
- Einstellungen > Mitteilungen: Ganz unten sehen Sie die Gefahrenwarnungen. Entscheiden Sie, ich lasse sie aktiv, ausser den Tests.
- Einstellungen > Allgemein > AirDrop: Empfangen aus.
  Ich schalte es nur ein, wenn ich es benötige. Das ist einmal im Monat oder weniger.
- Einstellungen > Allgemein > AirPlay & Handoff: Deaktivieren Sie alles. Nicht stöhnen: Wenn Sie das benötigen, weil Sie Apple TV und anderes nutzen, lassen Sie es an. Oder aktivieren Sie es nur, wenn Sie es benötigen.
- Einstellungen > Allgemein > Bild-in-Bild automatisch starten: Aus.
- Einstellungen > Siri & Suchen: Deaktivieren Sie alles.
- Einstellungen > Siri & Suchen > Für jede App: Alles deaktivieren.

Hinweis: Sie können später Einstellungen wieder aktivieren, wenn Sie Ihnen fehlen. Aber versuchen Sie doch erstmal, so wenig wie möglich zu aktivieren und Sie werden feststellen, dass Sie gar nicht so viel vermissen.

- Einstellungen > Datenschutz & Sicherheit > Ortungsdienste: Alles aus
- Einstellungen > Datenschutz & Sicherheit > Tracking: Deaktivieren

Hinweis: Fragen Sie sich, wieso das standardmässig aktiv ist?

- Einstellungen > Datenschutz & Sicherheit > Sensor- und Nutzungsdaten: Schalten Sie alles aus oder deaktivieren Sie es.
- Einstellungen > Datenschutz & Sicherheit > Bewegung & Fitness: Deaktivieren.
- Einstellungen > Datenschutz & Sicherheit > Analyse & Verbesserungen: Deaktivieren Sie alles.
- Einstellungen > Datenschutz & Sicherheit > Apple-Werbung > Personalisierte Werbung: Aus.
- Einstellungen > App Store > App-Downloads: Aus.
- Einstellungen > App Store > App-Updates: Aus.
- Einstellungen > App Store > In-App-Inhalte: Aus.
- Einstellungen > App Store > Automatische Downloads: Aus.
- Einstellungen > App Store > Automatische Videowiedergabe: Aus.
- Einstellungen > App Store > Bewertungen in

Apps: Aus.

- Einstellungen > Passwörter > Sicherheits-empfehlungen> Kompromittierte Passwörter erkennen: Aus.

Hinweis: Das ist wieder das zweischneidige Schwert zwischen Datenschutz und Sicherheit. Auf der einen Seite erhöht diese Einstellung die Sicherheit, auf der anderen Seite senden Sie Informationen an Server im Internet.

Safari ist ein grandioser Browser. Trotzdem sehr gesprächig. Hier meine Vorschläge für die Einstellungen.

- Einstellungen > Safari > Siri & Suchen: Es sollte alles deaktiviert sein, überprüfen Sie es aber nochmal.
- Einstellungen > Safari > Suchmaschine: DuckDuckGo.
- Einstellungen > Safari > Suchmaschinen-vorschläge: Aus.
- Einstellungen > Safari > Safari-Vorschläge: Aus.
- Einstellungen > Safari > Schnelle Website-Suche: Aus.
- Einstellungen > Safari > Toptreffer vorab laden: Aus.
- Einstellungen > Safari > Automatisches ausfüllen: Alles deaktivieren.
- Einstellungen > Safari > Pop-Ups blockieren: Aktivieren.
- Einstellungen > Safari > Cross-Sitetracking

verhindern: Aktivieren.

- Einstellungen > Safari > IP-Adresse verbergen: Vor Trackern.
- Einstellungen > Safari > Betrugswarnung: Aus.
- Einstellungen > Safari > Datenschutzwahrende Werbungsmessung: Aus.
- Einstellungen > Safari > Apple Pay prüfen: Aus.
- Einstellungen > Safari > Kamera: Ablehnen.
- Einstellungen > Safari > Mikrofon: Ablehnen.
- Einstellungen > Safari > Standort: Ablehnen.

Machen wir gleich mit der Karten App weiter.

- Einstellungen > Karten > Ankunftszeit teilen: Aus.
- Einstellungen > Karten > Luftqualitätsindex: Aus.
- Einstellungen > Karten > Wetterbedingungen: Aus.
- Einstellungen > Karten > Bewertungen und Fotos: Aus.
- Einstellungen > Karten > Bewertungen und Fotovorschläge: Aus.
- Einstellungen > Karten > Fotoanbietern die Nutzung deiner Fotos erlauben: Aus.

Und der Rest vom Schützenfest.

- Einstellungen > Kurzbefehle > iCloud-Synchronisierung: Aus.
- Einstellungen > Kurzbefehle > Privat teilen: Aus.
- Einstellungen > Health > Siri & Suchen: Alles deaktivieren.

- Einstellungen > Musik > Apple Music zeigen: Aus.
- Einstellungen > Kamera > QR Codes scannen: Aus.

Damit haben Sie einen weiteren Schritt zur Abgabe der Daten eingeschränkt. Manches ist invasiver als Anderes. Treffen Sie selber einen bewussten Entscheid, was Sie erlauben wollen oder nicht. Viele der Dienste bauen eine Verbinbung zu Apple Servern auf und senden Apple somit Informationen darüber, was Sie gerade tun, suchen, wohin Sie wollen usw.

STANDARD-APPS UND APPLE-ID

Entfernen Sie alle unerwünschten optionalen Standard-Apps, wie Home, Übersetzen, Bücher, iTunes Store, Uhr, Tipps, Facetime, Kalender, Mail, Notizen, Erinnerungen, Nachrichten, TV, Aktien usw. Tippen Sie dazu auf ein Icon, halten Sie es gedrückt und wählen Sie „App entfernen“ und dann „App löschen“.

Sie sollten nun ein iPhone mit benutzerdefinierten Konfigurationen haben. Sie haben jedoch noch keine Apple-ID mit Ihrem Gerät verbunden. Sie können keine Apps laden. Manche Datenschutzenthusiasten sagen, man solle einmal im Jahr eine neue Apple-ID einrichten, um die Datenerfassungssysteme von Apple ein wenig zu verwirren. Damit muss man die gekauften Apps (nicht die im Abo) nochmals kaufen. Das nervt und kann je nachdem auch teuer werden. Daher sind in diesem Fall Abos gut. Schliessen Sie mit dem neuen Handy die Abos ab, alle gleich lang, und wenn die Abos ablaufen, dann richten Sie eine neue Apple-ID ein. Ich erstelle eine neue Apple-ID und kaufe eine neue Prepaid-Mobilfunkkarte, wenn ich zu einem neuen Gerät wechsle. Ansonsten ist die Geräte ID der Wert, der Sie erkennt.

Wir werden gleich auch sehen, warum das Anlegen einer Apple-ID gleich am Anfang keine gute Idee gewesen wäre.

Apple-ID anlegen:

- Öffnen Sie die App App Store. Tippen Sie auf „Fortfahren“.
- Tippen Sie auf „Personalisierte Werbung deaktivieren“.
- Rechts oben tippen Sie auf die Person im Kreis.
- Tippen Sie auf „Neue Apple-ID erstellen“.
- Geben Sie die geforderte E-Mail-Adresse für dieses iPhone ein. Ein Alias sollte oftmals gehen.
- Geben Sie zweimal ein möglichst sicheres Passwort ein.
- Stimmen Sie den Nutzungsbedingungen zu.
- Geben Sie einen Alias-Namen ein.
- Deaktivieren Sie „Apple Updates“ und tippen Sie auf „Weiter“.
- Wechseln Sie die Zahlungsmethode zu „Keine“.
- Jetzt müssen Sie eine Adresse eingeben. Tippen Sie weiter.
- Geben Sie eine Telefonnummer ein. Tippen Sie weiter. (s.u.)
- Sie erhalten eine Bestätigung per SMS. Verfizieren Sie das.
- Verifizieren Sie ggf. den per E-Mail eingegangen Code.
- Wenn Sie fertig sind, tippen Sie auf „Weiter“.

Im Idealfall haben Sie bereits einen aktiven Mobilfunktarif für ein anderes Gerät oder Sie haben eine aktivierte physische SIM-Karte (oder eSIM) in Ihr neues iPhone eingesetzt.

Es gibt Datenschutzenthusiasten, die der Meinung sind, Apple sollte auf keinen Fall die wirkliche primäre Handynummer erhalten. Das ist in Deutschland schwierig, weil bei jeder Sim-Karten-Aktivierung eine Legitimation notwendig ist. Manche empfehlen daher, Sim-Karten aus Ländern dafür zu verwenden, wo man sich nicht ausweisen muss, wie bspw. Dänemark. Gerade Amerikaner sind der Meinung, keine primäre, echte Telefonnummer anzugeben. Dort ist es aber möglich, anonyme Sim-Karten zu erwerben und zu aktivieren. Und sie können somit auch anonyme VoIP Mobil-funknummern erhalten. Das alles ist bei uns so nicht möglich.

Außerdember: Wir wissen, dass Apple fortlaufend eindeutige Informationen vom Handy sammelt, z. B. die Seriennummer und die Telefonnummer, die mit der SIM-Karte im Gerät (oder eSIM) verbunden ist. Daher kennt Apple jederzeit die Handynummer und die eindeutige Geräte-ID. Aus diesem Grund sehe ich keinen Grund, die (anonyme Prepaid-) Nummer vor Apple zu verbergen.

Ich lege die aktivierte SIM-Karte (oder eSIM-Karte) in das iOS-Gerät ein, bestätige, dass ich Textnachrichten empfangen kann, und gebe diese Nummer bei der Erstellung des Apple-ID-Kontos im App Store an Apple weiter.

Lieber wäre mir das anders, aber so ist es heute nunmal. Auch bei dem obersten Privatsphäre-Schützer, als den Apple sich ausgibt.

Seit iOS 15 wird man bei der Anmeldung über das Standardmenü der Apple-ID in iCloud eingeloggt, ohne dass man die Möglichkeit hat, die Synchronisierung insgesamt zu deaktivieren (man kann nur einzelne Dienste deaktivieren). Das ist gefährlich, vor allem nach einem Neustart während eines Updates. Aus diesem Grund habe ich oben die Apple-ID in der App Store App erstellt. Sie sollte die minimalen Dienste aktivieren, die notwendig sind, um Anwendungen herunterzuladen und zu installieren. Wir können dies mit den folgenden Schritten testen.

- Öffnen Sie die Einstellungen und tippen Sie oben auf Ihren Kontonamen.
- Schauen Sie, ob iCloud als „Aus“ angezeigt wird.

Wenn Apple iCloud ohne Ihre Zustimmung aktiviert hat, kann dies ganz einfach korrigiert werden.

Navigieren Sie zu „Einstellungen“ und klicken Sie auf Ihr neues Apple-ID-Konto. Wenn die Option „iCloud“ „Aus“ anzeigt, müssen Sie nichts tun. Wenn etwas anderes angezeigt wird, sind Sie bei iCloud angemeldet und Apple sammelt Daten über Sie und Ihr Gerät. Wählen Sie auf diesem Bildschirm die Option „Abmelden“ und erlauben Sie Ihrem Gerät, Daten aus der iCloud zu entfernen. Kehren Sie zum App Store zurück und melden Sie sich bei Ihrem neuen Konto an. Bestätigen Sie, dass die iCloud-Einstellung „Aus“ anzeigt. Diese Einstellung sollte beibehalten werden, solange Sie iCloud nicht benötigen. Im Hauptmenü der Einstellungen sehen Sie

möglicherweise eine Warnung neben „iCloud verwenden“. Wenn dies der Fall ist, gehen Sie wie folgt vor, um dieses Ärgernis zu beseitigen.

- Tippen Sie auf „iCloud Nutzung beginnen“ und dann auf „Nicht jetzt“.

Sie mögen mein Misstrauen gegenüber iCloud in Frage stellen. Meine Sicht der Dinge ist, dass ich keinem Cloud-Speicherdienst ohne strenge E2EE (Ende-zu-Ende-Verschlüsselung) vertraue. Wir haben alle von den verschiedenen Sicherheitsverletzungen gehört, bei denen persönliche Fotos und E-Mails von Prominenten offengelegt wurden. Dies geschah aufgrund der Bequemlichkeit des kostenlosen Cloud-Speichers. Die einzige Möglichkeit, meiner Meinung nach, dies wirklich zu verhindern, besteht darin, alle Daten zu blockieren, die das Gerät verlassen. Sind Sie aufgrund ihrer Berühmtheit oder Position besonders gefährdet, empfehle ich Ihnen dringend, iCloud oder andere Cloud-Speicherlösungen vollständig zu deaktivieren.

Wie schon oft gesagt: Ich gehe davon aus, dass alles, was im Internet landet auch irgendwann öffentlich wird.

WEITERE EINSTELLUNGEN

Wir können in der App Store App noch eine weitere Einstellung vornehmen.

- Tippen Sie rechts oben auf die blaue Person im Kreis.
- Tippen Sie auf Ihren Kontonamen.
- Deaktivieren Sie „Personalisierte Empfehlungen“.
- Tippen Sie rechts oben auf fertig.

Wenn Sie bisher „Personalisierte Empfehlungen“ genutzt haben, können Sie die bisherigen Daten löschen.

Weiterhin können Sie noch in

- Einstellungen > App Store > App-Downloads, App-Update, In-App-Inhalte deaktivieren.

Damit können Sie manuell Updates durchführen. Das ist nicht für jeden geeignet, ich weiß.

Das iPhone hat keine eingebaute Firewall, wie GrapheneOS. Sie können aber etwas Ähnliches eingeschränkt erreichen. Sie können Apps den Internetzugriff verbieten, wenn Sie sich im Mobilfunknetz befinden. Blockieren Sie alle Apps und verwenden Sie Ihr iPhone nur im Mobilfunknetz, dann haben Sie ein echt teures Handy ohne Internet aber mit toller Kamera.

Sie können aber auch nur die Apps einschränken, von

denen Sie nicht wollen, dass Sie sie überwachen, während Sie unterwegs sind.

Wenn Sie fertig sind, können Sie die folgenden Änderungen vornehmen. Überlegen Sie sich die nächsten Einstellungen gut. Es geht um Kommunikation mit anderen.

- Einstellungen > Nachrichten > iMessage: Deaktivieren
- Einstellungen > Nachrichten > Namen und Foto teilen: Deaktivieren
- Einstellungen > Nachrichten > Mit dir geteilt: Deaktivieren
- Einstellungen > Nachrichten > Kontaktfotos zeigen: Deaktivieren
- Einstellungen > Nachrichten > Mitteilung an mich: Deaktivieren
- Einstellungen > Facetime > Facetime: Deaktivieren

Die meisten Menschen die ich kenne, verwenden Signal, Threema, WhatsApp und verwenden iMessage wenig oder nie.

BEZAHL-APPS UND TOUCH ID

Wenn Sie vorhaben, Apps zu kaufen, besorgen Sie sich eine vorausbezahlte iTunes-Geschenkkarte mit Bargeld in einem Lebensmittelgeschäft. Ich gebe Apple meine Kredit- oder Debitkartennummer nicht mehr, und Prepaid- und maskierte Debitkarten sind normalerweise verboten. Wahrscheinlich ist das auch nicht nötig, denn Sie sollten nur ein Minimum an Anwendungen besitzen, und auch nur solche, die unbedingt erforderlich sind. Das gilt natürlich noch mehr für proprietäre Apps die Sie bezahlen müssen. Schauen Sie sich ggf. nach Abos um, wenn Sie vorhaben, wie zuvor beschrieben, jedes Jahr die Apple-ID zu ändern.

Viele Leute fragen nach der Sicherheit der Touch ID-Option. Ich halte sie für sicher, und Apple erhält kein Bild Ihres Fingerabdrucks. Ihr Gerät erstellt einen mathematischen Wert, der auf dem Abdruck basiert, und sucht nur nach einer Übereinstimmung, wenn er verwendet wird. Es ist nur so sicher wie Ihr Passcode, da beide das Gerät entsperren können. Touch ID zu aktivieren ist eine persönliche Entscheidung, und die meisten Menschen, die ich kenne, nutzen das. Ich bitte Sie nur, die folgenden Gefahren zu bedenken.

- Erzwungener Druck: Wenn Sie unter physischen Druck gesetzt werden, könnten Sie gezwungen werden, Ihren Finger zu benutzen, um ein Gerät zu entsperren. Dies ist zwar extrem selten, aber

in den Hollywood Filmen… Ich weiss, aber ich will das Maximale darstellen. Sie können das dann immer noch abschwächen.

- Rechtliche Anforderungen: Einige Gerichte haben entschieden, dass die Angabe eines Passcodes nicht immer als Teil eines Durchsuchungsbefehls zur Durchsuchung eines Geräts erforderlich ist, ein Fingerabdruck hingegen schon. Sie können die Angabe Ihres Codes verweigern, werden aber möglicherweise gezwungen, Ihren Fingerabdruck herauszugeben.
- Wahrscheinlichere Situation: Jemand überfällt Sie, Sie sind kurz ohnmächtig, er hält Ihren Daumen auf das iPhone und hat Zugriff auf Ihr gesamtes digitales Leben. Mit einer Pin geht das nicht.
- Apple Face ID: Ich rate davon ab, so bequem es auch sein mag. Aber ich respektiere, dass viele neuen Telefone nur diese biometrische Option zulassen. Obwohl Apple Ihr Bild nicht speichert und nur Infrarotsensoren verwendet, um Ihr Gesicht lokal auf dem Gerät abzubilden (nicht auf den Servern von Apple), könnte jemand, der körperlich bedroht wird, gezwungen werden, in das Telefon zu schauen, um es zu entsperren. Selbst wenn man schläft oder im Koma liegt (siehe oben), kann damit das Handy entsperrt werden. Es liegt wiederum an Ihrem Bedrohungsprofil, was Sie verwenden wollen.

DATENAUSTAUSCH

Wie ich bereits erwähnt habe, verwende ich keinen Cloud-Speicher für sensible Daten, wie persönliche Fotos und Videos. Ich respektiere aber die Notwendigkeit, eine Sicherungskopie dieser Daten zu besitzen, insbesondere, wenn meine mobilen Geräte jedes Bild, das ich aufnehme, erstelle und speichere, besitzen. Da viele Menschen ein iPhone und einen Apple-Computer besitzen, empfehle ich ihnen, alle Inhalte manuell über ein USB-Kabel zu sichern. Die Standardanwendung von Apple für Fotosicherungen ist Fotos, aber ich ziehe es vor, sie nicht zu verwenden. Stattdessen verwende ich die mitgelieferte Anwendung „Digitale Bilder“. Diese kleine Software versucht nicht, eine Verbindung zu den Apple-Servern herzustellen, und verfügt nur über begrenzte Funktionen. Wenn ich ein iPhone mit Bildern an einen Apple-Computer anschließe, führe ich die folgenden Schritte durch.

- Verbinden Sie das iPhone via Kabel.
- Starten von „Digitale Bilder“ und dann wählen Sie links in der Liste der Geräte das angeschlossene iPhone aus.
- In der „Importieren nach:“ Option, unter der Dateiliste, wählen Sie das Verzeichnis aus, in dem die Bilder gespeichert werden sollen.
- Wählen Sie „Alle laden“ aus. Damit werden alle Bilder und Videos auf den Rechner kopiert.
- Danach können Sie alle Medien vom iPhone

löschen, in dem Sie alle Bilder und Videos auswählen, die rechte Maustaste klicken und „X Objekte löschen“ auswählen.

Wenn Sie frustriert darüber sind, dass Sie Apples iTunes- oder die Musik-App verwenden müssen, um Musik auf Ihr Gerät zu übertragen, verstehe ich Sie sehr gut.

Ich umgehe das durch die Verwendung einer Bezahl-Anwendung namens iMazing. Damit kann ich Musik, Fotos, Kontakte, Dokumente und Sicherungskopien von und auf jedes iOS-Gerät übertragen, ohne dass Apple Schwierigkeiten macht. Die Möglichkeit, neue Musikdateien zu übertragen, ohne dass dabei alle gespeicherten Songs gelöscht werden (wie mir das schon passiert ist), ist mir den Preis von €39,99 wert. Wenn Sie diese Software haben, brauchen Sie keine Apple-Apps mehr, um Daten jeglicher Art zu importieren oder zu exportieren, die mit Ihrem mobilen Gerät verbunden sind. Also auch nicht die eben erwähnte „Digitale Bilder“ Anwendung.

Während ich das schreibe, rippe ich eine CD und will diese in Apple Music speichern. Alle Apple-Verbindungen sind mit Little Snitch gesperrt. Ich hätte gerne die Titel und Künstler aus dem Internet, also gebe ich die Zugriffe auf die CDDB (Datenbank mit den meisten CDs und deren Lieder und Künstler) frei. Doch das reicht nicht, um die Titel zu laden. Ich muss auch noch Zugriffe auf Apple Server zulassen. Warum? Daher verwende ich iMazing, wenn ich Medien zwischen iPhone und Rechner

transferieren will. Andere Daten von Apps kann man meist über den Finder laden. Der Finder zeigt das iPhone an, sie klicken darauf, sehen rechts den Tab „Dateien“ und können dort die Apps auswählen und die Daten der Apps hin und her laden. Ich bin ein grosser Fan von GoodReader, da geht das beispielsweise problemlos (solange Sie keine Verschlüsselung verwenden).

Wenn Sie Ihre Fotos und Videos auf Ihrem Computer haben, hoffe ich, dass Sie Backups Ihrer Daten auf einem externen Gerät erstellen. Indem Sie alle Ihre persönlichen Daten lokal auf Geräten in Ihrem Besitz aufbewahren, eliminieren Sie vollständig die Möglichkeit für Hacker, sich in Ihre iCloud zu „hacken“ und Ihre Inhalte zu stehlen. Sie sind zwar nicht kugelsicher, aber ein Angriff wäre extrem gezielt und schwierig. Beachten Sie, dass die Verbindung Ihres iPhones mit Ihrem Apple-Computer eine bekannte Verbindung dieser beiden Geräte bei Apple herstellt. Die Risiken sind minimal, da beide Geräte hoffentlich keine Verbindung zu Ihrer wahren Identität haben, siehe vorheriges Kapitel zur Apple-ID. Außerdem rate ich von der Verwendung einer Apple-ID auf macOS-Geräten ab, was die Eindringlinge weiter einschränkt.

Wenn Sie sich auf den iCloud-Speicher verlassen müssen, nehmen Sie bitte drei wichtige Änderungen in Ihren iCloud-Einstellungen vor.

- Erstens: Deaktivieren Sie den webbasierten iCloud-Zugang. Dadurch wird verhindert, dass

jemand mit Ihren Anmeldedaten über einen Webbrowser auf Ihr iCloud-Konto zugreift. Nur Ihre Geräte haben dann noch Zugriff. Dies schließt einige häufige Sicherheitslücken durch Passwörter.

  - Einstellungen > Ihr Name oben > iCloud > Über das Internet auf iCloud-Daten zugreifen
  - „Nicht zugreifen“ antippen
- Zweitens: Wechseln Sie zu einer sichereren 2FA, z. B. einem YubiKey, der seit Anfang 2023 unterstützt wird. Wenn Sie keinen YubiKey oder Ähnliches haben, dann nehmen Sie eine Authenticator App. Jede 2FA Lösung ist besser als gar keine.
  - Einstellungen > Ihr Name oben > Passwort & Sicherheit.
  - Zwei-Faktor-Authentifizierung > Aktivieren.
  - Fortfahren, und befolgen Sie die Anweisungen auf dem Bildschirm.
  - Für einen YubiKey tippen Sie auf „Sicherheitsschlüssel“ und folgen den Anweisungen.
- Drittens: Aktivieren Sie in den Einstellungen Ihrer Apple-ID die Option „Erweiterter Datenschutz für iCloud“. Dies verschlüsselt Ihre Backups, Fotos, Notizen und andere Daten, bietet aber **keine** echte Verschlüsselung Ihrer Apple-E-Mails, Kalender oder Kontakte.

- Einstellungen > Ihr Name oben > iCloud > Erweiterter Datenschutz > Erweiterter Datenschutz aktivieren.
- Folgen Sie den Anweisungen.
- Tippen Sie dann auf Accountwiederherstellung.
- Wählen Sie eine oder beide Option aus und folgen Sie den Anweisungen.

DNS (UND VPN)

DNS ist eigentlich nur die Auflösung der Adresse, wie bspw. apple.com in eine IP-Adresse, die Computer verstehen. Damit hat der Anbieter eines DNS-Dienstes eine volle Übersicht aller Ihrer Internetverbindungen. Für mich ist das ein Problem, denn die ISPs (Vodafone etc.) kennen damit Ihr gesamtes Internetverhalten. Zumindest wissen sie, wann Sie welche Verbindung mit welchem Dienst (Browser, Mail, Chat etc.) durchgeführt haben. Daher ist es auf jeden Fall hilfreich, einen anderen DNS Server zu verwenden.

Mittlerweile haben sich Tools und Dienste etabliert, die nicht nur die Auflösung verschlüsselt gewährleisten, sondern auch unerwünschte Verbindungen verhindern, in dem sie z. B. Internet-Adressen, die Werbung oder Schadsoftware ausliefern, schlicht blockieren.

Dabei können Sie zwischen Apps, die das auf Ihrem iPhone steuern und Diensten im Internet wählen. Von mir in der Vergangenheit empfohlene Apps auf dem iPhone waren u.a. Lockdown Privacy und AdGuard Pro.

Ich empfehle die Lockdown-Firewall-Anwendung, die ich in der Vergangenheit mit Begeisterung empfohlen habe, nicht mehr. Sie hat sich zu einem Strom-verbrauchskiller entwickelt. Außerdem sagte mir ein Freund, dass er mit der Facebook App Probleme hatte. Weiterhin umgeht Apple die meisten Schutz-mechanismen mittlerweile ohnehin. So wie Google auch. Damit ist auch AdGuard

Pro nicht mehr die beste Wahl. Beide (Apple, Google) VPN Implementierungen auf den Geräten sind defekte Software, denn sie tut nicht das, was sie soll. Also nochmal im Klartext: Sowohl Google als auch Apple haben bewusst und hinterhältig die Programme zur Unterstützung von VPN kastriert, um an Ihre Daten zu kommen.

Sie dürfen sich Gedanken machen, wieso beide (!!!) das tun. Weil Ihnen Ihre Privatsphäre so wichtig ist?

Ein kurzer Abstecher:

Google's Antwort auf eine Fehlermeldung dazu ist eine arrogante Frechheit. Aber das ist bei Google zu erwarten, aber bei Apple, dem Gralshüter unserer Privatsphäre?

Google's Antwort (zur Unterhaltung, es geht hier ja um iOS):

> *We have looked into the feature request you have reported and would like to inform you that this is* ***working as intended****. We do not think such an option would be understandable by most users, so we don't think there is a strong case for offering this.*
>
> *As for disabling connectivity checks :*
>
> *-the VPN might be actually relying on the result of these connectivity checks (they are available through public APIs).*

-the VPN may be a split tunnel, letting part of the traffic over the underlying network, or only affect a given set of apps. In both these cases, the connectivity checks are still necessary for smooth operation of all the legitimate traffic that doesn't go over the VPN.

-the connectivity checks are far from the only thing exempted from the VPN ; privileged apps can also bypass the VPN and this is necessary for their operation in many cases. An example is IWLAN, or tethering traffic.

-it's unclear to us what specific privacy impact is meant. The connectivity checks reveal there is an Android device at this address, which is plenty clear from the L2 connection and from the traffic going over the VPN anyway.

Kuketz-Blog-https://www.kuketz-blog.de/warnung-android-leakt-beim-connectivity-check-daten-an-vpn-verbindungen-vorbei/

Einige Leser werden sich gleich vielleicht darüber aufregen, dass ich NextDNS gegenüber AdGuard als DNS-Filter-Anbieter gewählt habe. Meine Gründe dafür sind die folgenden.

- Für mich mittlerweile am Wichtigsten: AdGuard ist ein russisches Unternehmen, das zwar nach Zypern verlagert wurde, aber seine Infrastruktur

steht weiterhin in Russland.

- Ein russischer CEO hat eine minimale Präsenz im Internet und es gibt keine Informationen über andere Eigentümer. Gehen Sie auf deren Webseite und suchen Sie einfach mal nach einer Organisationsstruktur, einem Namen oder sonst was. Nichts! AdGuard hat einen guten Ruf, aber das Gesagte hat für mich durch den Angriffskrieg auf die Ukraine an Gewicht gewonnen.
- Ich hatte immer mal wieder Probleme mit der AdGuard Pro App in Kombination mit meinem ProtonVPN. Das beschreibe ich später.
- Oben gesagte Umgehung Apple's, die ich als Frechheit bezeichne. Apple hat bewußt die VPN Implementierung verkrüppelt. Welcher App können Sie jetzt noch vertrauen?
- Ich habe mehr Vertrauen in NextDNS. Die Gründer sind öffentlich sichtbar, Sie geben Ihre berufliche Laufbahn preis und ich weiß, wer das Unternehmen leitet. Es handelt sich meiner Meinung nach um seriöse Geschäftsleute, die sich in diesem Bereich stark engagiert haben und ihre Gründe für den Dienst transparent darlegen.
- Der Support von NextDNS ist hervorragend. AdGuard ist bisher auch gut gewesen, aber NextDNS war noch besser.

AdGuard hat vor kurzem ein neues Programm angekündigt, das angeblich NextDNS ähneln soll und benutzerdefinierte Filterung auf deren Servern und nicht

in der lokalen App ermöglicht. Wir werden sehen, was da kommt und wie es aussieht. Die benutzer-definierten Optionen von NextDNS sind gründlich getestet und geprüft worden. Ich habe lange getestet und ausprobiert, auf verschiedenen Plattformen.

Die letzte Überlegung zum Schutz der Privatsphäre im Zusammenhang mit DNS betrifft die kontobasierten (wie NextDNS, bei dem Sie ein Konto anlegen müssen) und die öffentlich zugänglichen (wie dnsforge oder dismail) Server. Ein benutzerdefiniertes NextDNS-Konto kann zwar wunderbar zum Blockieren (oder Zulassen) von Verbindungen genutzt werden, birgt aber auch ein gewisses Risiko. Da Sie über ein Konto verfügen, können alle Abfragen zu einem bestimmten Benutzer zurückverfolgt werden. Die Deaktivierung der Protokollierung der Anfragen in NextDNS sollte dies verhindern können, aber ein Gerichtsbeschluss könnte Ihre Konfiguration außer Kraft setzen. Die Verwendung eines Alias-Namens mit einer Alias-E-Mail-Adresse sollte hier Abhilfe schaffen. Wenn Sie dann noch einen VPN verwenden, wird es aufwändig, Sie zu finden. Aber nicht unmöglich.

Für die öffentlichen NextDNS-Server ist kein Konto erforderlich, sie bieten jedoch keine benutzerdefinierte Filterung. Wenn Sie nur ein paar Anzeigen ohne ein Konto filtern möchten, gibt es viele Lösungen, beispielsweise Mullvad (adblock.doh.mullvad.net), die eben genannten, aber auch AdGuard (dns.adguard.com), ohne Verwendung der App. Allerdings können Sie den Schutz

nicht ändern. Wenn eine Domäne blockiert wird, gibt es keine Möglichkeit, sie wieder freizugeben. Auch hier ist die benutzerdefinierte Filterung von NextDNS überlegen.

Und wie gesagt: Die lokalen Möglichkeiten werden von Apple teilweise umgangen. Daher ist es besser, einen Service ausserhalb des Telefons zu verwenden. Zu Hause habe ich eine Firewall (pfSense), die das alles für mich erledigt. Sie können sich pi-Hole oder eBlocker anschauen, die sind einfacher zu nutzen und sehr effektiv. Aber unterwegs benötige ich eine andere Lösung. Apple erlaubt keine einfache Änderung des DNS für das mobile Netz. Sie können nicht einfach, wie bei Android oder bei iOS für das Wi-Fi Netz, eine IP Adresse eintragen und haben einen anderen DNS Server. Und wenn Sie sicheres DNS (verschlüsselt) verwenden wollen, müssen Sie sowieso ein Profil herunterladen.

Eine Liste von Anbietern finden Sie im Internet. Bekannt und oft empfohlen sind Digitalcourage, dismail, dnsforge, mullvad (der VPN Anbieter), Quad9, Uncensored DNS. Wählen Sie einen aus.

Wenn Sie einen Anbieter gefunden haben, dann gehen Sie wie folgt vor:

- Laden Sie mit Safari die dortige Datei herunter (Endung: .mobileconfig)
- In dem sich öffnenden Pop-Up tippen Sie auf “Zulassen”
- Sie müssen das Konfigurationsprofil installieren:

Dazu gehen Sie auf
"Einstellungen > Profil geladen". Hier sollten Sie das gerade eben geladene Profil finden

- Die "Netzverkehr" Warnung bestätigen Sie und tippen auf "Installieren"
- Das zuletzt installierte Profil ist automatisch aktiv. Überprüfen Sie das in "Einstellungen" > "Allgemein-VPN & Netzwerk-DNS"
- Aktivieren Sie einmalig den Flugmodus und deaktivieren Sie ihn wieder. Damit wird der DNS Cache gelöscht und alle Anfragen werden neu über den neuen DNS aufgelöst

Alternativ können Sie die App DNSCloak verwenden oder die App von Cloudflare (die sinnigerweise 1.1.1.1 heisst).

Testen Sie, ob der DNS, den Sie eben konfiguriert haben (egal ob verschlüsselt oder nicht), verwendet wird, in dem Sie auf browserleaks.com gehen und dort IP anklicken. Weiter unten auf der Seite finden Sie

Run DNS Leak Test

Tippen Sie darauf und Sie sollten den ausgewählten DNS sehen. Alternativ können Sie auf dnsleaktest.com gehen und dort auf "Standard Test". Es dauert einen Moment, dann sollten Sie Ihren ausgewählten DNS Anbieter erkennen.

Sie können einfach nur einen anderen DNS nutzen, einen verschlüsselten (wie eben gesehen) oder einen, der

Ihnen erlaubt, selber einzugreifen und Seiten zu sperren oder zuzulassen. Wie gesagt, beim Mobilfunknetz benötigen Sie für alle Fälle ein Profil, das Sie herunterladen müssen.

Wenn Sie das aber sowieso tun müssen, dann können Sie gleich einen Anbieter wählen, der Ihnen auch hilft, bestimmte Adressen zu sperren, so wie das Lockdown Privacy oder auch AdGuard Pro können. Für mich ist dieser Anbieter NextDNS. Zuerst habe ich diesen auf meinem GrapheneOS verwendet, aber mittlerweile nutze ich ihn auf jedem mobilen Gerät. Bis zu 300.000 Anfragen im Monat sind kostenlos, danach kostet es zwei Euro/Monat. Bei GrapheneOS komme ich maximal auf 30.000 Anfragen im Monat, da die Apps und das System so gut wie keine unnötigen Verbindungen anfragen. Bei iOS habe ich sehr viel mehr, da Apple andauernd seine eigenen Adressen anpingt, die aufgelöst werden müssen, das kostet. Im wahrsten Sinne des Wortes. Aber der Service von NextDNS ist es mir wert.

Wichtig ist auch zu wissen, dass Sie NextDNS sieben Tage ohne Konto testen können. Schauen Sie in der Zeit, wieviele Anfragen Sie benötigen und rechnen das dann auf einen Monat hoch. Mich haben diese sieben Tage mit GrapheneOS überzeugt und das hat mich dann, nach Monaten, dazu gebracht, diese Lösung auch bei iPhone und iPad anzuwenden. Sie könnten mit NextDNS auch Ihr Apple TV schützen, falls Sie zu Hause nicht hinter einer Firewall sind.

Die Konfigurationsschritte sind bei Android sehr einfach, bei iOS leider nicht. Führen Sie die folgenden Schritte von Ihrem iOS-Mobilgerät aus (analog zum eben beschriebenen Artikel). Jetzt für NextDNS.

- Öffnen Sie Safari (keinen anderen Browser) und gehen Sie zu https://nextdns.io.
- Wenn noch nicht geschehen, legen Sie ein Konto an. Sie benötigen lediglich eine E-Mail-Adresse und ein Passwort. Die ersten sieben Tage benötigen Sie nicht mal das. Aber ich bin sicher, NextDNS überzeugt Sie ebenso wie mich.
- Dann gehen Sie auf https://apple.nextdns.io. Die folgenden Schritte gelten, wenn Sie ein Konto verwenden. Tun Sie das nicht, werden Standardnamen vergeben.
- Geben Sie einen Profilnamen und einen Namen für das Gerät an und tippen Sie auf „Download“.
- Tippen Sie auf „Zulassen“.
- Tippen Sie auf „Schließen“.
- Gehen Sie in die Einstellungen-App und tippen Sie direkt unter Ihrem Namen auf „Profil geladen“.
- Tippen Sie rechts oben auf „Installieren“.
- Geben Sie Ihre Pin ein.
- Tippen Sie rechts oben auf „Installieren“.
- Tippen Sie auf „Installieren“.
- Tippen Sie auf „Fertig“.
- Das zuletzt installierte Profil wird aktiv.

Alternativ können Sie auch die NextDNS App aus dem

App Store installieren. Ich weiss nicht mehr genau warum ich das nicht mehr mache, ich denke es gab einen Konflikt mit meinem VPN, weil die App den VPN belegt. Ich konnte also nur VPN oder NextDNS verwenden. Davon abgesehen finde ich die Installation von Profilen nicht so schwierig.

Ihr iPhone verwendet jetzt NextDNS für DNS-Anfragen. Im linken Tab „Einstellungen“ auf der NextDNS Seite sollte ein grüner Punkt leuchten und ein Text wie „Alles in Ordnung“ oder so erscheinen. Sie können die Protokollierung Ihrer DNS-Anfragen in Ihrem NextDNS-Portal sehen. Dies mag für einige Leser alarmierend sein. Der Tab „Logs“ (zweite von rechts) in Ihrem Portal identifiziert jede Verbindung, die von Ihrem Gerät aus hergestellt wird. Das kann ein Problem für den Datenschutz sein, hat aber auch viele Vorteile. Das sehen wir gleich.

Sie können Filter anwenden, die viele unerwünschte Verbindungen blockieren. Klicken Sie auf den Tab „Datenschutz“ und beachten Sie die automatisch angewendete Blockliste. Wenn diese nicht aktiviert wurde, fügen Sie die „NextDNS Anzeigen & Tracker Blockliste“ hinzu. Diese Datenbank blockiert über 100.000 Verbindungen, die mit Werbung, Trackern und Schadsoftware in Verbindung gebracht werden. Dadurch werden viele unerwünschte Verbindungen wie Popup-Werbung, Tracking-Code, Telemetrie und Benutzeranalysen blockiert. Sie haben jetzt einen besseren Schutz. Dieser alleine reicht für viele Menschen

schon aus und ist standardmässig meist aktiviert. Für diese Menschen: Das war's. Mehr ist nicht zu tun. Happy Surfing.

Wenn Sie sich entscheiden, mehr zu wollen, z. B. alles von Google oder Facebook zu blockieren, bietet NextDNS dafür separate Filter, die Sie zusätzlich aktivieren können. Gehen Sie auf den Tab „Datenschutz > Blocklisten" und tippen Sie auf „Fügen Sie eine Blockliste hinzu". Die Liste ist lang, spielen Sie damit. Aber nicht einfach alles aktivieren, das verlangsamt die Anfragen und bringt meist wenig Mehrwert.

Tipp: Pete Lowe's und Stephen Black's Listen haben einen sehr guten Ruf.

Sie sehen auch, dass Sie die AdGuard Blocklisten aktivieren können. Weiter unten finden Sie Listen um alle Google- oder alle Facebook-Tracker zu blockieren. Meine Welt.

Beachten Sie, dass diese Listen möglicherweise mehr blockieren, als Sie wünschen. Gelegentlich (sehr sehr selten) weigert sich der Browser meines Geräts, eine Website anzuzeigen, die ich besuchen will. Es ist nicht das Gerät, das sie blockiert, sondern NextDNS. Wenn Sie eine Website finden, die nicht geladen werden kann, ändern Sie die DNS-Option Ihres Geräts wieder auf „Automatisch" und laden Sie die Seite erneut. Wenn sie geladen wird, kennen Sie den Grund. Dies ist eine Seltenheit, aber Sie sollten wissen, was Sie tun können,

wenn Sie es brauchen.

Dazu gehen Sie in Ihrem iPhone auf

- Einstellungen > Allgemein > VPN, DNS & Geräteverwaltung > DNS und tippen Sie auf „Automatisch“.

Klicken Sie bei NextDNS auf der Webseite auf die Registerkarte „Protokolle“ und sehen Sie sich den Datenverkehr an. Hier finden Sie auch, wenn ein Filter eine Seite blockiert hat. Diese können Sie dann in die Allowlist aufnehmen und sind auf der sicheren Seite.

Sie können auch zuerst ein paar Ihrer Webseiten öffnen. Wenn Sie bisher noch keine derartigen Blocker verwendet haben, bereiten Sie sich auf einen Schock vor. Eine Seite angesurft, 50 oder mehr Einträge. Viele davon zu Werbetreibenden. Aktualisieren Sie die NextDNS-Protokollseite (Symbol mit den kreisförmigen Pfeilen) und beobachten Sie den Unterschied. Sie werden wahrscheinlich sehen, dass einige Verbindungen zugelassen und andere blockiert werden. Das ist die Filterliste in Aktion. Wenn Sie sehen, dass eine Verbindung zugelassen wird, die Sie nicht wünschen, können Sie diese Domäne kopieren und sie zur Registerkarte „Denylist“ hinzufügen. Ich habe dies für einige Domänen getan, die ich nicht wollte. Aber meist braucht man das nicht und die Liste ist auch bei mir sehr kurz. Durch tippen auf den Namen der blockierten Domäne können Sie sehen, welche Liste, wenn Sie

mehrere Nutzen, diesen Eintrag blockiert.

Wenn Sie NextDNS von nun an immer auf Ihrem(n) Gerät(en) verwenden möchten, empfehle ich Ihnen dringend, die Protokollierungsaspekte zu ändern. Klicken Sie auf den Tab „Einstellungen“ in Ihrem NextDNS-Portal und sehen Sie sich den Abschnitt „Protokolle“ an. Sie können die Protokolle vollständig deaktivieren oder den Aufbewahrungszeitraum ändern. Ich wähle Letzteres, während ich meine Geräte teste. Ich lasse die Protokolle aktiviert, deaktiviere „IP-Adressen der Clients protokollieren“, aktiviere „Domains protokollieren“ und setze die Aufbewahrungsfrist auf „1 Stunde“. Auf diese Weise kann ich immer im Portal sehen, was blockiert und zugelassen wird, aber die Protokolle werden eine Stunde nach jeder Aktivität gelöscht. Ich kann Änderungen vornehmen, während ich mein iPhone konfiguriere, und sehe die Ergebnisse sofort. Auch wenn ich neue Apps das erste Mal installiere, aktiviere ich die Protokollfunktion, bevor ich die App das erste Mal starte. Dann schaue ich, was sie treibt. Danach deaktiviere ich die Protokollfunktion wieder. Dadurch werden alle Aufzeichnungen über meine Internet-Aktivitäten über NextDNS gelöscht. Wann immer Sie wollen, können Sie alle Protokolle mit der Schaltfläche „Protokolle löschen“ löschen.

Als nächstes sollten Sie sicherstellen, dass Ihre Verbindungen verschlüsselt sind. Navigieren Sie in Safari zu https://cloudflare.com/ssl/encrypted-sni und führen Sie einen Test durch, in dem Sie auf „Browser testen“

tippen. Sie sollten neben DNSSEC und TLS ein Häkchen sehen. Wenn dies der Fall ist, verbergen Sie einen Großteil Ihres Internetverkehrs vor Ihrem ISP und Ihrem VPN (dazu im nächsten Teil mehr, denn das ist standardmässig nicht immer der Fall). Die beiden anderen Optionen auf dieser Seite gelten für den DNS-Dienst von Cloudflare. Sie können sie ignorieren. Für diesen Test ist mir nur wichtig, dass der Datenverkehr mit einer TLS-Verbindung verschlüsselt wird. DNSSEC stellt die Integrität des DNS Servers sicher.

Besuchen Sie bei geöffnetem Safari-Browser amazon.com oder focus.de oder andere und lassen Sie die gesamte Seite laden. Wenn Sie mit dieser Website vertraut sind, werden Sie feststellen, dass die meisten störenden Popups, eingebetteten Videos und blinkenden Anzeigen nicht mehr vorhanden sind. Das liegt daran, dass NextDNS diese Verbindungen blockiert hat, bevor sie Ihr Gerät erreichen. Kehren Sie dann zu Ihrem NextDNS-Portal zurück und laden Sie die Seite „Protokolle“ erneut. Es kann selten ein paar wenige Minuten dauern, bis die Ergebnisse angezeigt werden. Meist werden sie in Echtzeit angezeigt.

Der rote Balken auf der linken Seite bestätigt, welche eingehenden Verbindungen NextDNS blockiert hat. Sie können Ihre Blockliste(n) in Aktion sehen. Auf den Seiten werden Dutzende von Anzeigen und Trackern ohne unser Zutun blockiert. Wir brauchen keine Browser-Erweiterungen oder Firewall-Anwendungen. Das ist die wahre Stärke von NextDNS. Diese Implementierung ist

viel sauberer und verbraucht nur minimale Ressourcen. Sie verhindert auch Konflikte mit VPN-Anwendungen. Ich bezahle die 2€/Monat gerne, denn ich spare so viel Zeit.

Das ist alles ganz schön viel, ich weiß. Aber es ist wirklich hilfreich und das stärkste Mittel, unerwünschte Tracker und Werbung loszuwerden. In meinen Kursen ist das oftmals die einzige Einstellung, die ich mit den Teilnehmern am ersten Tag durchführe. Der Effekt war bisher immer: Wow!

Fassen wir einige der wichtigsten Erkenntnisse zusammen. Standardmäßig stellt Ihr Internet-dienstanbieter DNS-Dienste zur Verfügung und nutzt diese Daten („Vorratsdatenspeicherung“). Wenn Sie NextDNS auf Ihrem iPhone konfigurieren, verwenden Sie stattdessen den Service von NextDNS, verschlüsselt. Außerdem können die Blocklisten Anwendungen daran hindern, Telemetrie- und Analysedaten über Ihre Nutzung zu übermitteln. Theoretisch könnten Sie so die gesamte Apple Telemetrie unterbinden. Probieren Sie es aus. Funktioniert Ihr iPhone noch? Wohl kaum. Denn auch wenn Sie glauben es gekauft zu haben, es gehört Ihnen nicht.

Denken Sie an die Grenzen der kostenlosen Version. Die meisten Nutzer werden nicht mehr als 300.000 Abfragen pro Monat durchführen, aber das hängt natürlich vo Ihrer Nutzung ab. Wenn Sie mehrere Geräte haben, können Sie entweder ein Konto für jedes Gerät einrichten, müssen dann aber alle Einstellungen

mehrfach vornehmen, oder bei gesammelt mehr als 300.00 Anfragen eine geringe Gebühr von 2€/Monat für den Premium-Service von NextDNS bezahlen.

VPN und DNS

Dieser Teil behandelt das Zusammenspiel von VPN und DNS. Viele Datenschutzfreunde wollen beides verwenden. Das klappt nicht immer, nicht immer so, wie es gut wäre und daher hier Details dazu.

Wie schon beschrieben, hatte ich immer mal wieder Probleme mit AdGuard Pro und ProtonVPN. Wobei ich sagen muss, ich fand es schon gut, dass ich überhaupt beide parallel laufen lassen konnte. Der Vorteil von AdGuard Pro lag für mich auch darin, dass der eingestellte DNS in AdGuard Pro den des VPN überschreibt. Ansonsten verwenden die meisten VPN Anbieter ihre eigenen DNS Server. Was nichts Schlechtes sein muss. ProtonVPN bietet Schutz vor Malware und Phishing Seiten und blockiert Werbung. Sie können es aber nicht nach Ihren Wünschen einstellen. Mir hat das nicht gereicht. Außerdem legt man so alle Eier in einen Korb. Manche Datenschutzfanatiker bekommen dabei Gänsehaut. Auch wenn Proton einen exzellenten Ruf hat und das Risiko hierbei sicher gering ist. Aber: Sie blockieren eben nicht alles, was ich gerne blockiert hätte.

Manchmal hat die Konfiguration von ProtonVPN und AdGuard Pro dazu geführt, dass der gesamte Internetverkehr blockiert wurde. Entweder musste ich

dann AdGuard stoppen und damit waren die Werbung und die Trackings wieder da. Oder ich musste, genau in dieser Reihenfolge, erst den VPN deaktivieren, dann AdGuard, dann AdGuard wieder aktivieren und dann den VPN. Das nervte und führte bei den permanenten Verbindungen von Apple zu Datenabflüssen. Nachfragen bei Proton und bei AdGuard zeitigten dieselben Antworten: „Verwende beide nicht zusammen, sondern nur einen von beiden.“ Zu Hause war das kein Problem, aber mobil schon. Ich brauchte eine andere Lösung, nach der ich sehr lange gesucht habe.

Die meisten iOS-VPN-Apps umgehen alle benutzer-definierten DNS-Einstellungen auf dem Gerät und verwenden ihre eigenen DNS Server. Ich verwende vor allem ProtonVPN und die App erlaubt es ebenfalls nicht. Das heisst, beispielsweise dnsforge als DNS einzurichten half nicht, wenn ich ProtonVPN aktiviert hatte.

Wenn Sie die Möglichkeit haben möchten, eine VPN-Verbindung zu aktivieren, aber dennoch die Vorteile der gefilterten NextDNS-Abfragen beibehalten möchten, dann müssen Sie einen sog. DNS Leak einrichten. Das bedeutet, dass der VPN nicht mehr für Ihre DNS Abfragen verantwortlicht ist, die Daten werden also „geleakt (ein Leck)“.

Sie sollten Folgendes in Betracht ziehen:

ProtonVPN und NextDNS

Wenn Sie die iOS ProtonVPN-App verwenden, können Sie die DNS-Serveradressen für DNS-Abfragen nicht angeben. Sie müssen den DNS von Proton verwenden, der keine benutzerdefinierte Filterung bietet. Gleichzeitig umgeht Apple manche dieser Blockierer. AdGuard hat die Möglichkeit, den von ProtonVPN zu umgehen und den eigenen zu wenden. Aber: Ich wollte mich auch von AdGuard trennen, siehe oben. Die Lösung:

Sie benötigen eine Anwendung eines Drittanbieters, um die Einschränkungen von Proton mit den folgenden Schritten zu umgehen.

- Öffnen Sie den App Store, suchen Sie nach „WireGuard“, und installieren Sie die App.
- Navigieren Sie zu https://account.protonvpn.com/login und melden Sie sich an.
- Tippen Sie auf „Downloads“ und scrollen Sie nach unten zum Abschnitt „WireGuard“.
- Geben Sie als Gerätenamen „iOS“ ein und wählen Sie „iOS“.
- Wählen Sie „Keine Filterung“.
- Wählen Sie entweder einen gewünschten Server oder akzeptieren Sie die Standardoption.
- Tippen Sie auf „Erstellen“ und dann auf „Herunterladen“, wenn Sie dazu aufgefordert werden.

- Starten Sie die WireGuard-Anwendung auf dem iPhone.
- Tippen Sie auf die Schaltfläche „+“, um einen Tunnel hinzuzufügen.
- Wählen Sie „Aus Datei oder Archiv importieren“ und wählen Sie Ihre herunter-geladene Datei aus.
- Bestätigen Sie alle Aktionen und geben Sie bei Bedarf die PIN ein.
- Aktivieren Sie den Verbindungsumschalter und autorisieren Sie die Anfrage.
- Navigieren Sie zu https://my.nextdns.io und melden Sie sich mit Ihrem Konto an.
- Tippen Sie auf der Registerkarte „Einrichtung“ unter „Verknüpfte IP“ auf „IP verknüpfen“.
- Kopieren Sie den ersten DNS-Server, der oberhalb der „Verknüpften IP“ aufgeführt ist.
- Kehren Sie zur WireGuard App zurück und wählen Sie Ihre neue Verbindung aus.
- Klicken Sie auf „Bearbeiten“, um die Details zu ändern.
- Fügen Sie die NextDNS-IP-Adresse in das Feld „DNS-Server“ ein.
- Klicken Sie auf „Speichern“.

Solange diese WireGuard-Verbindung aktiviert ist, sollten Sie einen VPN-Dienst über ProtonVPN und DNS-Filterung über NextDNS haben. Testen Sie dies, indem Sie einen DNS-Leaktest online unter https://www.dnsleaktest.com durchführen. Das Ergeb-

nis sollte NextDNS identifizieren (in selten Fällen wird nur die Firma angezeigt, bei der NextDNS den Service betreibt, bspw. Misaka Networks). Öffnen Sie dann Ihr NextDNS-Portal und überprüfen Sie die Protokolle. Wenn Sie die Protokollierung aktiviert haben, sollten Sie Verbindungen und die Filterung innerhalb des iPhones sehen. Sie können auch im NextDNS Portal auf den Tab „Installation“ tippen. Der zeigt Ihnen ebenfalls an, ob Sie NextDNS verwenden. Ein grüner Kreis mit dem Text „Alles in Ordnung“ bestätigt, dass Sie NextDNS verwenden.

Die offizielle ProtonVPN-Anwendung ist nicht mehr erforderlich, es sei denn, Sie möchten andere Server ohne DNS-Filterung oder den Filtern von ProtonVPN auswählen.

Das alles funktioniert, weil wir ein ProtonVPN-Profil für einen bestimmten VPN-Server erstellt haben, der immer die gleiche IP-Adresse hat. Wir haben uns mit dieser IP-Adresse verbunden und sie mit unserem NextDNS-Konto verknüpft. Dadurch wird NextDNS angewiesen, die Filterung nur von dieser IP-Adresse aus anzuwenden, und auch nur dann, wenn der zugewiesene DNS-Server in Gebrauch ist, den wir auch WireGuard zur Verfügung gestellt haben.

Wenn Sie mehrere VPN Server in mehreren Ländern „zur Hand haben wollen“, führen Sie die oben beschriebenen Schritte mehrmals durch. Bedenken Sie aber: Wechseln Sie den VPN-Server in der WireGuard App, dann müssen

Sie in NextDNS die IP Verknüpfung neu laden.

MullvadVPN und NextDNS

Wem das mit ProtonVPN und Wireguard und NextDNS zu aufwändig oder nervig ist, dem kann ich noch MullvadVPN empfehlen.
Ich verwende zwei VPN Anbieter: ProtonVPN und MullvadVPN.
Auf einem iOS Gerät ist die Verwendung von MullvadVPN unter Verwendung von NextDNS einfacher. Sie benötigen keine zusätzliche Wireguard App und müssen auch keine Profile herunterladen.
MullvadVPN bietet an, einen eigenen DNS einzurichten.

- Laden Sie die MullvadVPN App aus dem App Store.
- Starten Sie die MullvadVPN Anwendung und loggen sich mit Ihrem Konto ein.
- Einstellungen > VPN Settings.
- MullvadVPN bietet an, bestimmte „Schädlinge“ zu blockieren. Sie haben aber keinen Einfluß darauf, welche sie blockieren. Das kann mal zu wenig, mal zu viel sein. Wenn Ihnen das aber reicht, und Sie NextDNS sowieso nicht wollen, ist das eine gute Wahl.
  - DNS Content Blocker: Wählen Sie aus, was Sie blockieren wollen. Verwenden Sie NextDNS, können Sie diese alle deaktiviert lassen.
  Der Bereich Use Custom DNS ist für uns relevant:

- Aktivieren Sie MullvadVPN.
- Gehen Sie in Ihren Safari Browser und dort auf Ihr NextDNS Konto. Dort gehen Sie auf den Tab „Installation“.
- Suchen Sie den Bereich „Verknüpfte IP“. Wenn Sie unter DNS Server „Verknüpfte IP“ ein kleines Rad rechts neben der IP Adresse sehen, dann tippen Sie darauf.
- Kopieren Sie die DNS IP Adressen darüber und tragen diese in der MullvadVPN unter „Use Custom DNS“ ein. Es ist gute Praxis, immer zwei zu verwenden. MullvadVPN verbindet sich neu.
- Gehen Sie zurück in Safari und schauen Sie unter Installation, ob Sie einen grünen Punkt und den Text „Alles in Ordnung“ sehen.

Das war es.

Wann immer Sie den VPN von Mullvad ändern, auf einen anderen Server oder ein anderes Land, müssen Sie die „Verknüpfte IP“ aktivieren, in dem Sie auf das Rad rechts neben der IP tippen. Analog zu ProtonVPN.

Fazit

Lohnt sich das alles? Das können nur Sie entscheiden. Ich selber verwende die reine ProtonVPN Anwendung fast gar nicht mehr. Ich habe mir mehrere Profile von ProtonVPN heruntergeladen, diese in WireGuard importiert, den DNS pro Profil (siehe oben) aktiviert und

bin damit zufrieden. Je nach Lust und Laune wechsle ich zwischen ProtonVPN und MullvadVPN.

Beim Wechseln des WireGuard Profils, müssen Sie die Link IP Adresse ändern, egal bei welchem VPN Anbieter.

Wenn Sie also häufig den Serverstandort ändern, aus welchen Gründen auch immer, vielleicht weil Sie in der Schweiz Dienstag und in Österreich Mittwoch Champions League schauen wollen, dann müssten Sie die verknüpfte IP Adresse in NextDNS aktualisieren. Das wollen viele nicht, Bequemlichkeit ist King. Dann ist auf jeden Fall Mullvad die etwas einfachere Lösung.

BACKUPS

Das Sichern Ihres iPhones ist viel einfacher als bei Android. Sie müssen nur den Finder auf Ihrem macOS-Computer öffnen, das Mobilgerät über USB anschließen und folgende Schritte ausführen.

- Klicken Sie im Finder auf dem Mac in der Seitenleiste auf iPhone (oder wie immer Ihr iPhone heißt).
- Aktivieren Sie die Checkbox „Lokales Backup verschlüsseln“ und geben Sie ein sicheres Passwort ein.
- Auf der rechten Seite klicken Sie den Knopf „Backup jetzt erstellen“.
- Ggf. müssen Sie Ihr iPhone entspreren.

Damit wird eine Sicherung der Betriebssystem-konfiguration und aller Apple-Daten erstellt. Es werden nicht alle Anwendungen und ihre Einstellungen oder Medien wie Musik gesichert. Wenn Sie keinen Apple-Computer besitzen, können Sie iTunes verwenden, das es auch für Windows gibt. Der Ablauf ist vergleichbar im Explorer.

Wenn Sie extreme Privatsphäre wünschen, können Sie eine virtuelle Windows-Maschine auf einem Linux-Host einrichten, jeglichen Internetzugang zur Windows-VM deaktivieren, iTunes innerhalb der Windows-VM installieren und Ihr mobiles Gerät mit der iTunes-

Installation verbinden. Aber dann sind Sie noch paranoider als ich.

Unabhängig davon, wie Sie vorgehen, ist es von großem Vorteil, eine Sicherungskopie der Einstellungen Ihres mobilen Geräts zu haben, falls Sie Ihre Konfiguration einmal auf ein zweites Gerät übertragen wollen, oder Ihr iPhone zurücksetzen müssen. Das ist vor allem auch dann wichtig, wenn Sie iCloud nicht nutzen.

KALENDER UND KONTAKTE

Apple iOS-Benutzer synchronisieren ihre Kalender und Kontakte oft gerne mit den Apple-eigenen Apps Kalender und Kontakte. Viele Drittanbieter verwenden die Frameworks von Apple, d.h. auch wenn Sie eine andere App verwenden, landen die Daten vielleicht indirekt bei Apple.

Wenn Sie Ihre Kalender und Kontakte nur auf dem iPhone haben und sie mit keinem anderen Gerät wie iPad, macOS oder einem anderen iPhone synchronisieren wollen, stellen Sie einfach iCloud ab (oder legen es gar nicht erst an, wie zuvor erwähnt). Dann bleiben die Daten auf dem Gerät. Apple verschlüsselt jetzt in der iCloud mehr, aber Mail, Kalender und Kontakte sind nicht dabei.

Die Anbieter von verschlüsselten Kalendern und Kontakten (Proton oder Tutanota) bieten ein hohes Maß an Datenschutz, sind aber nicht in der Lage, Ihre geschützten Daten innerhalb der Apple-Welt sicher zu synchronisieren. Wenn Ihre Apple Kontakte leer sind, weil Sie sie in Tutanota pflegen, und Sie erhalten einen Anruf, sehen Sie nur die Telefonnummer aber nicht den Namen aus der Tutanota App. Viele nervt das und führt dazu, dann doch die Kontakte in der hauseigenen Apple App zu pflegen.

An dieser Stelle könnte EteSync für Sie interessant sein.

Mit diesem Dienst können Sie Ende-zu-Ende verschlüsselte Kalender und Kontakte auf einem Server speichern. Der Ablauf ist folgendermassen:

Sie speichern Ihre Kontakte in der Apple Kontakte App. Diese wird wird der EteSync App verbunden. EteSync verschlüsselt diese Daten und sendet sie an einen Server. Von dort kann die EteSync App auf einem anderen Gerät die Daten holen, entschlüsseln und auf dem anderen Gerät in die Kontakte App synchronisieren. Alles Ende-zu-Ende verschlüsselt.

Gerät A Gerät B

Kontakte -> EteSync -> Server -> EteSync -> Kontakte

Damit können Sie Ihren Kalender und Ihre Kontakt direkt mit den Apple-eigenen Apps von iOS mit jedem anderen Gerät synchronisieren. Ganz ohne iCloud. EteSync ist mit einer monatlichen Gebühr von 2 US-Dollar verbunden, ist aber das einzige Unternehmen, das meiner Erkenntnis nach diesen einzigartigen Dienst anbietet. Sie installieren die EteSync App auf Ihrem iPhone. Diese synchronisiert sich dann mit Ihrem Kalender und den Kontakten und stellt die Verbindung zu den EteSync-Server her. Sie ist sozusagen der Vermittler. Sie müssen daher auf allen Geräten, mit denen Sie die Daten abgleichen wollen, EteSync installieren. Und Sie benötigen ein Konto bei EteSync, da dies der Vermittler ist.

Nach der Installation der EteSync-App aus Apple’s App Store lassen Sie alle Standardberechtigungen zu, geben

Ihre Kontoanmeldedaten ein, bestätigen die Synchronisierungsoptionen für den lokalen Kalender und die Kontakte und lassen den Synchronisierungsvorgang ablaufen. Dadurch werden Ihre lokalen Daten mit den EteSync-Servern synchronisiert und können dann auf jedem anderen Gerät aktualisiert werden. Da die Schlüssel für die Daten auf dem iPhone erstellt werden, sieht der Server von EteSync Ihre normalen Daten nicht, wie das auch bei Standard Notes für Notizen ist.

Die iOS-App für EteSync ist stabil, aber neu. Ich bin auf Fehler gestoßen, die in der Android-Anwendung nicht vorhanden waren. Wenn Sie Kalender und Kontakte über Anwendungen verschlüsselt mit einem anderen Computer oder Gerät synchronisieren müssen, ist EteSync die datenschutz-freundlichste Option. Wenn Sie diese Daten nur lokal auf Ihrem mobilen Gerät benötigen, ist dies ein Overkill. Die Nutzung der verschlüsselten Kalender- und Kontaktdienste von Proton oder Tutanota über Webbrowser oder Anwendungen auf all Ihren Geräten könnte für Sie besser sein. Ich empfehle Ihnen, ein kostenloses Testkonto bei EteSync zu erstellen, bevor Sie sich festlegen.

Sie werden sich vielleicht jetzt denken: Sagt der nicht immer, keine Daten im Netz abgeben? Richtig, das tue ich. Alles bei sich selbst zu haben, ist für mich in 99,9% der Fälle die Wahl. Viele haben aber nicht meine Ansprüche und eine Zero-Knowledge-Ende-zu-Ende-Verschlüsselung ist schon ziemlich hilfreich. Aber für die, die ähnlich wie ich ticken, hier noch zwei Tipps:

Wenn Sie das Ganze weiter treiben wollen und keine Daten in das Internet schicken möchten, oder dem EteSync Server nicht vertrauen, dann können Sie einen EteSync Server auch auf ihrem eigenen Rechner im eigenen Netz installieren. Sie synchronisieren nicht mehr mit der Firma sondern nur noch in Ihrem Netzwerk. Natürlich können Sie das auch wieder über das Internet zugänglich machen, so dass Sie flexibel sind. Ich brauche das nicht. Mir reicht es, wenn die Daten synchronisiert werden, wenn ich zu Hause bin.

Alternativ können Sie sich auch NextCloud anschauen. Während EteSync ausschliesslich Kalender, Kontakte und Notizen synchronisiert, ist NextCloud eine Mini-Cloud. Sie können darüber Kalender, Kontakte und Aufgaben synchronisieren, aber auch Daten ablegen, Medien speichern, in Gruppen arbeiten und vieles mehr. Für diese Aufgabe in diesem Kapitel ist das ein Overkill, weil es meiner Meinung nach komplexer ist, als EteSync. Wenn Sie aber sowieso eine NextCloud im Einsatz haben oder es planen, schauen Sie sich das vielleicht zuerst an und vergleichen später mit EteSync.

Hinweis: Mike Kuketz hat eine schöne Einführung zur Nextlcoud inklusive ausführlicher Installation geschrieben.

PASSWORTMANAGER

Apples iOS enthält einen eigenen Passwortmanager namens Schlüsselbund (Keychain), den ich aber nicht empfehle. Ich habe keine Probleme mit deren Verschlüsselung und Sicherheit, aber es gibt keine plattformübergreifenden Funktionen (für Android, Linux, Windows, …), und iCloud ist für die Synchronisierung erforderlich. Wenn Sie Ihr iPhone verlieren, könnten Sie Ihre Kennwörter verlieren. In der Vergangenheit habe ich über Passwörter und Passwortmanager in einer Serie geschrieben. Vielleicht lesen Sie dort nochmal nach.

Wichtig ist die Unterscheidung zwischen Offline- und Online-Passwortmanager. Die meisten Kursteilnehmer verwenden Online-Passwortmanager, weil das einfach, effizient und in vielen Fällen sehr sicher ist.

Als Online-Passwortmanager empfehle ich

Bitwarden

Wenn Sie eine einfache und kostenlose Lösung suchen, die Ihre Passwörter mit jedem Computer oder Mobilgerät synchronisiert, dann ist Bitwarden meiner Meinung nach die beste Wahl für Sie. Erfreulicher Weise grinsen mich bei diesem Thema die Kursteilnehmer an: Viele verwenden Bitwarden schon.

Bitwarden ist im kostenlosen Paket völlig ausreichend. Das Produkt wird regelmässig auditiert und die Firma ist

sehr transparent. Aber wie Sie an LastPass gesehen haben, nichts im Internet ist wirklich sicher. Auch wenn bei LastPass vieles zusammengekommen ist, für mich gilt einfach immer: Alles was im Internet passiert, wird irgendwann öffentlich. So auch die Passwörter. Sehen Sie sich Have I been Pwned (https://haveibeenpwned.com/) an. 12 Mrd Einträge.

Wenn Sie ein extremes Interesse an Ihrer Privatsphäre haben und nicht möchten, dass diese Daten verschlüsselt auf deren Servern gespeichert werden, dann ist eine Offline-Option meiner Meinung nach besser für Sie.

KeePassXC

Daher verwende ich persönlich KeePassXC auf meinen Desktop-Systemen und teile die Passwortdatei mit jedem mobilen Gerät, das ich verwende, manuell. Das heisst, Sie kopieren die Passwortdatei via Kabel oder anderen Methoden auf Ihr iPhone. Auf iPhones verlasse ich mich auf Strongbox. Strongbox bietet einen kostenlosen und verschiedene Bezahlmodelle an. Probieren Sie es aus.

Wieso jetzt beides? Ganz einfach: Es gibt KeePassXC nicht für Mobilsysteme. KeePassXC ist die App, aber das Datenbankformat für die Passwörter liegt im sog. KeePass Format vor, das als sehr sicher gilt. Daher gibt es KeePass als Programm, KeePassXC, auf Android KeePassDX und viele andere. Eben auch Strongbox, dass dieses Datenbankformat lesen kann.

Da ich das iPhone aber nur noch als Zweitphone besitze (siehe Einführung), ist der Nutzen für Strongbox für mich auf dem iPhone nur noch sehr eingeschränkt wertvoll. Vor meiner GrapheneOS Zeit habe ich Strongbox und KeePassXC verwendet.

Strongbox öffnet alle KeePassXC-Datenbanken (die enthalten Ihre Passwörter). Nach der Installation von Strongbox aus dem App Store starte ich die Anwendung und wähle „Don't Use Autofill" und „Let's Go". Ich ziehe es vor, Passwörter nach Bedarf zu kopieren und einzufügen, anstatt das Betriebssystem dies für mich tun zu lassen. Als Nächstes kopiere ich meine KeePassXC-Datenbank auf das iPhone, zum Beispiel über eine Kabelverbindung zum Computer (siehe auch Kapitel 9 Datenübertragung). Nach dem Kopieren sollten Sie die Datei in Strongbox sehen. Ich öffne die Datenbank und gebe das Passwort ein. Ich ziehe es vor, meine mobile Version der Kennwörter „schreibgeschützt" zu halten und Änderungen bei Bedarf von meinem Laptop aus vorzunehmen, daher aktiviere ich diese Option, während ich mich auf diesem Bildschirm befinde.

Warum? Weil ich sonst manchmal neue Passwörter und Kontem am Rechner und ein anderes Mal am iPhone eingebe und dann ein Problem mit der Synchronizität habe. Daher sind Tools wie Bitwarden gut, aber nicht mein Schutzprofil.

Sie können die Zeitspanne, in der die Datenbank ohne Passworteingabe freigeschaltet bleibt, je nach Ihrem

Komfort gegenüber dem manuellen Aufwand anpassen. Sie können auch eine PIN festlegen, um die Datenbank auf Ihrem mobilen Gerät zu entsperren, wenn Sie ein absurd langes Passwort haben. Für Offline-Nutzer ist Strongbox meiner Meinung nach die beste Option. Ich ermutige Sie, die kostenlose Version zu testen und herauszufinden, ob Sie die kostenpflichtigen Funktionen oder die Strongbox Zero-Option (eine minimalistische Version) benötigen.

Proton Pass

Seit ein paar Monaten gibt es als Passwortmanager Proton Pass. Vom selben Hersteller wie Proton Mail und Proton VPN. Ich vertraue Proton, ich denke, was Sicherheit angeht, wissen sie, was sie tun. Ich habe Proton Pass für iOS und in Verbindung mit dem Mac ausprobiert und werde noch nicht gänzlich umsteigen, sondern es weiter beobachten.

Für mich sind die Vorteile:

- Open Source
- Sehr gefällige Benutzerschnittstelle (Bitwarden wirkt für mich ein wenig altbacken)
- Eine fantastische Integration von E-Mail Aliasen, die das Verwalten stark vereinfacht
- Ein sehr gutes Browser AddOn

Was spricht für mich dagegen?

- Ich habe in meinen Passwortmanagern oftmals noch andere, schützenswerte Informationen. Dafür finde ich Proton Pass nicht gut geeignet.
- Es gibt noch keine Desktop App. Die reine Browserintegration ist für mich zu wenig. Wie auf dem iPhone hätte ich gerne eine App.
- Auf einem Mac gibt es keine Integration mit Safari.
- Kein Yubikey zum Schützen der Datenbank.
- Außerdem bin ich mit meiner bisherigen Lösung sehr zufrieden.

Passkey

Einige meiner Kursteilnehmer kommen seit Kurzem in den Kurs und wenn ich beginne, über das Thema Passwörter zu sprechen, dann gibt es den ein oder anderen Teilnehmer, der den Kopf schüttelt und sagt: „Kalter Kaffee. Es gibt Passkey, da brauchen wir keine Passwörter mehr."

Passkey basiert auf Technik, die es schon seit vielen Jahren gibt. Ja, es wird die altbekannten Passwörter ablösen. Aber welche Anbieter bieten Passkey heute schon an? Apple beispielsweise noch nicht. Erst mit dem Update auf iOS 17. Eine wahrscheinlich unvollständige Liste (https://www.passkey.directory/) zeigt an, wer dabei ist. Da sehen Sie auch, wer fehlt. Wenn Sie noch nie davon gehört haben, können Sie sich testweise schon mal auf Passkey vorbereiten (https://passkey.org/). Die

Seite simuliert das, was Ihnen in Zukunft auf den Seiten angeboten wird. Probieren Sie es aus, gewöhnen Sie sich daran, Sie werden die Vorzüge und die Bequemlichkeit zu schätzen lernen.

Wenn Passkey flächendeckend zur Verfügung steht und ich die Keys auch zwischen unterschiedlichen Systemen (Android und iOS beispielsweise) austauschen kann, melde ich mich wieder.

ZWEI-FAKTOR-AUTHENTIFIZIERUNG

Wenn Sie StandardNotes verwenden (was ich auf allen Plattformen als Notizendokument empfehle, nicht nur auf iOS), können Sie diese für alle 2FA Konten innerhalb von iOS (und allen anderen) verwenden. Strongbox (siehe Kapitel 13) unterstützt auch Software-Token 2FA innerhalb der App. Solange Sie damit leben können, Ihre 2FA in derselben Datenbank wie Ihre Passwörter zu haben. Ich halte das für gefährlich und würde die Passwörter immer von den 2FA Tokens trennen. Wenn Ihr Konto komprimitiert wird (wie beispielsweise bei LastPass), können Sie alle Informationen verlieren.

Ich verlasse mich auf StandardNotes für alle Software 2FA, aber verwende meinen StandardNotes 2FA Code in einer anderen App, falls ich StandardNotes entsperren muss.

Apple unterstützt mittlerweile auch Yubikeys, also einen USB Stick, der viele Möglichkeiten bietet. Doch für diese Artikelserie belasse ich das hier. Verwenden Sie eine Authenticator App, ich empfehle OTP Auth, und sichern Sie jedes Konto ab, dass das anbietet.

Wichtig: Wenn Sie 2FA aktivieren, erhalten Sie im Normalfall eine Liste von Codes, die Sie verwenden können, wenn Ihre App nicht mehr funktioniert, jemand Ihr Handy geklaut hat, es in die Badewanne gefallen oder sonstige Unpässlichkeit passiert ist. Notieren Sie sich diese. Wirklich! Das ist Ihr Rettungsring.

EINSTELLUNGEN BESTIMMTER APPS

Wir haben alle unsere Apps. In diesem Teil stellen ich die von mir empfohlenen oder weit verbreiteten vor und wie Sie diese noch ein wenig sicherer machen können.

Browser

Den meisten meiner Kursteilnehmern, die iOS bevorzugen, rate ich, Firefox Klar zu verwenden. Jedoch vermissen sie die Bookmarks und noch ein paar andere Funktionen. Ich mag Firefox Klar und nutze ihn wenn ich mein iPhone nutze. Der Standard-Webbrowser Safari ist grandios und Sie können ihn aus meiner Sicht problemlos verwenden. Ich glaube, dass er standardmäßig sicher und ziemlich privat ist. Hier hat Apple wirklich gute Arbeit geleistet, was das Unterbinden von Drittanbieter-Cookies und Privatsphäre angeht. Wenn Sie die vorherigen Einstellungen (vor allem DNS) übernommen haben, sind Sie sehr gut geschützt. Ähnlich wie Firefox blockiert Safari seitenübergreifende Cookies. Aus diesem Grund kann ich iPhone Nutzern schwer erklären, Firefox zu einem iPhone hinzuzufügen, es sei denn, Sie benötigen einen separaten Browser. Ich benötige oft zwei Browser, daher verwende ich diese beiden. Einmal pro Woche, wenn ich nach iOS- oder App-Updates suche, navigiere ich zu

- Einstellungen > Safari > Verlauf und Websitedaten löschen

und bestätigen Sie die Auswahl.

Proton Mail

Ich bin ein grosser Anhänger von Proton Produkten. Alles hat mit Proton Mail angefangen. Daher empfehle ich jedem, sich Proton Mail anzuschauen.

Standardmäßig fügt die Proton Mail App auf Ihrem iPhone eine eigene Signatur ein, die zu erkennen gibt, dass die E-Mail von einem Mobilgerät gesendet wurde. Weiterhin bietet Proton Mail die Möglichkeit, entfernte Inhalte einer E-Mail (zum Beispiel Bilder, die von einem anderen Server nachgeladen werden) anzuzeigen oder das nicht standardmässig zu tun. Je nach Land, in dem Sie sich befinden, kann das Proton Netzwerk blockiert werden. Auch hier bietet die App Abhilfe. Aber Achtung: Diese Funktion stellt eine Verbindung zu Google her. Wenn Sie, wie ich, Google in NextDNS blockieren, dann hilft Ihnen diese Funktion nicht. In Deutschland, Österreich oder der Schweiz ist das nicht notwendig.

Ich nehme daher folgende Einstellungen in der Proton Mail App vor:

- Proton Mail > Einstellungen > Konto > Signatur auf Mobilgeräten: Deaktiviert.
- Proton Mail > Einstellungen > Konto > Datenschutz > Inhalte aus externen Quellen automatisch laden: Deaktiviert.
- Proton Mail > Einstellungen > Konto >

Datenschutz > Eingebettete Grafiken automatisch laden: Deaktiviert.

- Proton Mail > Einstellungen > Konto > Datenschutz > E-Mail Tracking blockieren: Aktiviert.
- Proton Mail > Einstellungen > Konto > Datenschutz > Link-Bestätigung anfordern: Aktiviert.
  Hinweis: Für mich ein Schutzschild, falls ich mal hektisch ohne nachzudenken auf einen Link in einer E-Mail klicke. Dann geht ein Fenster auf und fragt mich, ob ich das wirklich will. Und zeigt mir den Link in Gänze an.
- Proton Mail > Einstellungen > Konto > Datenschutz > Metadaten aus Grafiken entfernen: Aktiviert.
  Hinweis: Wenn Sie Bilder versenden, können diese viele Metadaten wie Kameratyp, Ort, Datum etc. enthalten. Ich will das nicht.
- Proton Mail > Einstellungen > Alternatives Routing > Alternatives Routing erlauben: Deaktiviert.

Signal

Hinweis: Signal ist nicht mein bevorzugter Messenger. Daher kann ich hier leicht etwas übersehen. Aber für viele ist das der bevorzugte oder nach WhatsApp der alternative Messenger.

Ich ändere die folgenden Einstellungen, um den Datenschutz und die Sicherheit zu verbessern.

- Signal > Einstellungen > Chats > Link-Vorschauen erstellen: Deaktiviert
- Signal > Einstellungen > Chats > Kontakte mit iOS teilen: Deaktiviert
- Signal > Einstellungen > Chats > System-Kontaktfotos verwenden: Deaktiviert
- Signal > Einstellungen > Mitteilungen > Anzeigen: Kein Name oder Inhalt
- Signal > Einstellungen > Datenschutz > Lesebestätigungen: Deaktiviert
- Signal > Einstellungen > Datenschutz > Tipp-Indikatoren: Deaktiviert
- Signal > Einstellungen > Datenschutz > Verschwindende Nachrichten: Nach Ihrem Geschmack, aber „Aus“ geht für mich nicht.
- Signal > Einstellungen > Datenschutz > Im App-Umschalter Bildschirm verstecken: Aktivieren
- Signal > Einstellungen > Datenschutz > Bildschirmsperre: Aktivieren (ich will nicht, das jemand meine Handy im ungesperrten Zustand klaut und dann Zugriff auf alle Nachrichten hat)
- Signal > Einstellungen > Datenschutz > Zahlungssperre: Aktivieren
- Signal > Einstellungen > Datenschutz > Anrufe in Anrufliste anzeigen: Deaktiviert

Threema

Mein bevorzugter Messenger aktuell ist Threema. Matrix und das Fediverse verwenden noch weniger Menschen als Threema und nach Jahren der Überzeugungsarbeit verwenden alle mir wichtigen Kontakte Threema. Ich verbinde Threema weder mit einer E-Mail-Adresse noch mit einer Telefonnummer.

Die folgenden Einstellungen nehme ich vor.

- Threema > Einstellungen > Privatsphäre > Kontakte synchronisieren: Deaktiviert
- Threema > Einstellungen > Privatsphäre > Interaktionen teilen: Deaktiviert
- Threema > Einstellungen > Privatsphäre > Lesebestätigungen: Nicht senden.
- Threema > Einstellungen > Privatsphäre > Melden, wenn ich tippe: Nicht senden.
  Sie können beide Einstellungen in den Kontakten überschreiben. Generell will ich es aber nicht.
- Threema > Einstellungen > Benachrichtigungen > Vorschau anzeigen: Deaktiviert
- Threema > Einstellungen > Benachrichtigungen > Nickname anzeigen: Aktiviert
- Threema > Einstellungen > Medien > Medien automatisch in <<Fotos>>-App speichern: Deaktivieren.
  Hinweis: Vor allem dann, wenn Sie Ihre Fotos gegen meine Empfehlung mit iCloud in Echtzeit

synchronisieren, ist diese Einstellung wichtig

- Threema > Einstellungen > Code-Sperre > Code-Sperre aktivieren: Antippen und den Schritten folgen.
- Threema > Einstellungen > Code-Sperre > Daten löschen: Aktiviert

In den Einstellungen des Systems (also nicht in der Threema App) stelle ich noch ein, dass Siri & Suchen für alles deaktiviert sind.

- Einstellungen > Threema > Siri & Suchen: Alles deaktivieren.

FINALE

Mein letzter Gedanke in dieser Serie stammt direkt aus meiner Erfahrung mit zahlreichen Kursteilnehmern und Berichten im Internet. Wenn Sie ein iPhone mit einem aktiven iCloud-Konto verwenden, dann werden die Daten im Hintergrund automatisch mit Apples Cloud synchronisiert. Das ist bequem und funktioniert fast immer perfekt. Jedoch: In diesem Fall kann Passwort-Wiederverwendung hässliche Konsequenzen haben. Mittlerweile ist bekannt, dass viele Prominente ihre Nackbilder, Finanzdokumente, Chats etc. in der Cloud hatten und die Daten in die Öffentlichkeit gelangten. **Weil sie das Passwort an anderer Stelle auch benutzt hatten** und es dort bekannt war. Sie wurden erpresst und belästigt.

Die beste Verteidigung gegen diese Aktivitäten ist, die Daten niemals online zu synchronisieren. Wenn Ihre Fotos niemals Ihre Geräte verlassen, gibt es keine einfache Möglichkeit, auf die Daten zuzugreifen. Dies ist ein entscheidender Schritt zu mehr Privatsphäre, wenn Sie Apple-Geräte verwenden. Als zweitbeste Lösung gilt: Sehr gute, einmalige Passwörter zu verwenden. Leider kann man die 2FA nur mit iCloud verwenden. Die Prominenten habe das auf die harte Tour gelernt.

Ich habe in diesen Kapiteln viel über Apple hergezogen. Ich glaube jedoch, dass iOS sicher ist. Ich glaube, dass es deren Absicht ist, iOS für die Nutzer einfach und bequem

zu gestalten und gleichzeitig ein vernünftiges Maß an Privatsphäre zu bieten. Allerdings möchte Apple über die Standardeinstellungen alles über Sie wissen. Apple verdient mehr und mehr mit Werbung. Apple sitzt auf einem riesigen Datenberg. Sollten sie mal die Erwartungen der Analysten an der Börse nicht erreichen, massiv nicht erreichen, glaube ich, dass sie diese Daten zu Gold machen.

Wenn Sie Ihre Einstellungen wie beschrieben ändern, iCloud deaktivieren, eine anonyme Apple ID erstellen und ein Prepaid-Konto verwenden, ist das Risiko für Ihre Privatsphäre durch iOS meiner Meinung nach gering. Auf jeden Fall viel besser als ein reguläres Android, aber leider nicht so gut wie ein GrapheneOS.

ÜBER DEN AUTOR

Ich bin nur jemand, der versucht, seine Privatsphäre zu schützen und zu leben. Ich lese und höre viel und probiere alles Mögliche aus, um mein Schutzniveau zu erhöhen. Herauszufinden, was möglich ist und mit welchem Aufwand und welchen Einschränkungen ist mein Hobby. Die Erfahrungen möchte ich gerne weitergeben.