Die EU wird Ihnen bis Ende 2026 ein digitales Identitäts-Wallet aufzwingen. Pass, Führerschein, Diplome, Zugang zu öffentlichen Diensten, Bankkonten — alles in einer App.

Webologie klagt diesen Plan an. Hier ist warum. Die versprochene Souveränität ist eine technische Lüge Die deutsche Umsetzung überlässt die Kryptographie dieses Wallets Google und Apple. Zwei amerikanischen Unternehmen. Unterworfen dem CLOUD Act. Die EU schafft eine „europäische souveräne Identität“, indem sie sie in die Hände der Silicon Valley legt.

Das Risiko einer totalen Abschaltung ist real Wenn morgen eine Behörde beschließt, Ihnen den Zugang zu kappen — kein digitales Ausweispapier mehr, kein Zugang zu öffentlichen Diensten mehr, kein Bankkonto mehr, keine digitale Existenz mehr. Ohne Rechtsmittel. Ohne Verfahren. Ohne Transparenz. Ein Werkzeug, das das Leben erleichtern soll, kann durch eine einfache Verwaltungsentscheidung zu einem Mittel der totalen Ausgrenzung werden. Ein einziges Ziel für den Hack von 450 Millionen Identitäten Im April 2026 wurde die ANTS durch eine einfache Sicherheitslücke gehackt. 19 Millionen Franzosen gefährdet. Das europäische Wallet wird die vollständige Identität von 450 Millionen Bürgern zentralisieren. Pass, Bankdaten, medizinische Akte, Adresse — alles am selben Ort. Für einen staatlichen oder kriminellen Hacker ist das der absolute Jackpot. Eine einzige Lücke. 450 Millionen Opfer. Niemand hat Sie gefragt Dieses Projekt wurde ohne Referendum verabschiedet. Ohne Volksbefragung. Ohne Ihre Zustimmung. In einer Demokratie ist das Volk souverän — nicht die Technokraten aus Brüssel. Die Nutzung ist „freiwillig“ — vorerst. Aber wenn alle öffentlichen Dienste und alle Banken verpflichtet werden, es zu akzeptieren — wird die Wahl dann noch wirklich frei sein? Informieren Sie sich. Stellen Sie Fragen. Widerstehen Sie.

Europa will das Ende der Online-Anonymität. ProtectEU will VPNs zwingen, Ihre Daten zu protokollieren. Dänemark verbietet bereits VPNs ab dem 1. Juli 2026. Frankreich hat VPNs auf seine Liste der legislative Prioritäten gesetzt. Aber es gibt Tools, die niemand blockieren kann. Kein zentraler Server. Kein Unternehmen, das man zwingen kann. Keine Logs, die man verlangen kann.

Tor verschlüsselt Ihren Datenverkehr über 3 dezentralisierte RelaisI2P schafft ein Internet im Internet Shadowsocks macht Ihren Datenverkehr von HTTPS ununterscheidbar Tails OS hinterlässt keine Spuren auf Ihrem Gerät Dezentrale DNS haben keine Entität, die zensiert werden könnte Jedes vorgestellte Tool mit seinem genauen rechtlichen Status. Einschließlich dessen, was Kriminelle nutzen.

Speichern in Europa ist besser als bei AWS — aber kaum.

Die EU bereitet Chat Control vor, das EUDIW, den Krieg gegen VPNs, die verpflichtende Altersverifikation.

https://webologie.me/

Der echte Schutz ist nicht die Gerichtsbarkeit — es ist die Verschlüsselung, die Sie selbst kontrollieren.

Ein NAS bei Ihnen zu Hause mit lokaler Verschlüsselung bleibt souveräner als jede beliebige Cloud, europäisch oder nicht.

Der digitale Euro kommt 2029. Man sagt euch, es sei, um Zahlungen zu modernisieren. Hier ist, was man euch nicht sagt. Anonymität unmöglich — jede Transaktion wird aufgezeichnet Programmierbare Währung — sie kann ablaufen, begrenzt oder bedingt werden

Einfrieren von Vermögen per Klick — der kanadische Präzedenzfall hat es bereits bewiesen Niemand hat euch nach eurer Meinung gefragt Bargeld gehört euch. Der digitale Euro gehört denen, die ihn programmieren. Die eigentliche Frage ist nicht „wozu dient es“. Es ist „wem dient es“.

VPN: Europa will wissen, wer Sie sind – und das ist ernst.

Die Nutzung eines VPNs ist in Frankreich heute völlig legal.

Der Gerichtshof der Europäischen Union bestätigte dies im Januar 2026 erneut. Es gibt keinen europäischen Text, der Bürgern die Nutzung eines VPNs verbietet.

Doch was das Gesetz heute erlaubt, kann sich ändern. Und die Signale, die sich seit 2025 verdichten, deuten alle in dieselbe Richtung: Europa bereitet das Ende der Online-Anonymität vor – angefangen damit, VPNs nutzlos zu machen.

Was ist ein VPN und warum stellt es ein Problem dar?

Ein VPN (Virtual Private Network) erstellt einen verschlüsselten Tunnel zwischen Ihrem Gerät und dem Internet. Es verschleiert Ihre IP-Adresse, verschlüsselt Ihre Verbindungsdaten und verhindert, dass Ihr Internetanbieter, die Regierung oder Dritte Ihre Online-Aktivitäten einsehen können.

Genau das ist es, was die Institutionen beunruhigt.

Ein anonymer Bürger ist ein Bürger, der nicht überwacht werden kann. Und in der in Brüssel, Paris und London entstehenden regulatorischen Vision wird Online-Anonymität immer weniger als Recht, sondern immer mehr als Hindernis betrachtet.

ProtectEU: Die Strategie, die alles verändert

Im April 2025 präsentierte die Europäische Kommission **ProtectEU** – ihre Strategie für die innere Sicherheit der EU.

Das Dokument ist eindeutig: Anonymisierungswerkzeuge und verschlüsselte Nachrichten werden als **„Hindernisse für strafrechtliche Ermittlungen“** definiert .

Das erklärte Ziel ist weitreichend: Alle Online-Dienste – einschließlich VPN-Anbieter – sollen gezwungen werden, die Verbindungsmetadaten ihrer Nutzer zu protokollieren. IP-Adressen,

Zeitstempel, Sitzungsdauer, Datenvolumen – alles soll gespeichert und den Strafverfolgungsbehörden auf Anfrage zugänglich sein.

Ein formeller Gesetzesvorschlag wird bis **Mitte 2026** erwartet .

Wenn dieser Text in seiner jetzigen Form übernommen wird, würde ein VPN-Dienst, der keine Protokolle speichert – dessen einziges Argument darin besteht, keine Daten zu speichern –, in Europa faktisch illegal werden.

Mullvad, der führende schwedische Anbieter von Datenschutzlösungen, hat bereits öffentlich erklärt: Ungeachtet des endgültigen Vertragstextes wird das Unternehmen seine Architektur nicht ändern. Dies bedeutet konkret, dass es den europäischen Markt verlassen muss.

Frankreich im Rennen

Am 30. Januar 2026 bestätigte die beigeordnete Ministerin für digitale Angelegenheiten, Anne Le Hénanff, auf France Info, dass VPNs nun zu ihren **„nächsten Prioritätsthemen“** gehören .

Offizieller Kontext: um zu verhindern, dass Minderjährige das Verbot sozialer Netzwerke umgehen, indem sie eine Verbindung aus dem Ausland simulieren.

Der Subtext: die Kontrolle darüber, wer im Internet worauf Zugriff hat.

Denn die Logik ist unumstößlich. Um Minderjährigen den Zugang zu sozialen Netzwerken zu verwehren, muss man ihr Alter überprüfen. Um ihr Alter zu überprüfen, muss man den Nutzer identifizieren. Um den Nutzer zu identifizieren, muss man die Instrumente entfernen, die Anonymität ermöglichen.

VPNs geraten ins Visier. Nicht etwa, weil sie für illegale Aktivitäten genutzt werden, sondern weil sie die systematische Identifizierung von Internetnutzern verhindern.

Das Vereinigte Königreich: ein Labor für Europa

Im Juli 2025 verabschiedete Großbritannien den **Online Safety Act** – ein Gesetz, das Plattformen dazu verpflichtet, das Alter ihrer Nutzer zu überprüfen.

Die unmittelbare Folge: Die Downloadzahlen von VPNs schnellten in die Höhe. ProtonVPN verzeichnete einen Anstieg der täglichen Anmeldungen um 1.800 %, NordVPN sogar um 1.000 %.

Die Reaktion der britischen Regierung: die Nutzung von VPNs zu untersuchen – unter ausdrücklicher Androhung eines Verbots.

Im Januar 2026 stimmte das House of Lords für einen Änderungsantrag, der VPN-Anbieter dazu verpflichtet, eine obligatorische Altersverifizierung für ihre britischen Nutzer einzuführen.

Das britische Modell wird von Brüssel und Paris genau beobachtet werden.

Die Mechanismen der Steuerung – wie sie wirklich funktionieren

Um zu verstehen, was auf dem Spiel steht, muss man zwischen den Zeilen der Vorschriften lesen.

Europa sagt nicht: „Wir werden VPNs verbieten." Es sagt: „Wir werden Kinder schützen", „Wir werden den Terrorismus bekämpfen", „Wir werden den digitalen Raum sichern".

Doch die aus diesen Zielen resultierenden gesetzlichen Instrumente laufen alle auf dasselbe Ergebnis hinaus: **die obligatorische Identifizierung jedes Internetnutzers** .

Wie wir anhand des CLOUD Act analysiert haben , sind die Zentralisierung von Daten und die Identifizierung von Nutzern zwei Seiten derselben digitalen Kontrollpolitik.

Die Mechanismen sind wie folgt:

Schritt 1 — Die unbestreitbare Sache Wir wählen ein Ziel, das niemand bestreiten kann: Kinder schützen, gegen Kinderpornografie vorgehen, Terrorismus bekämpfen.

Schritt 2 — Die technische Lösung Wir schlagen eine Lösung vor, die eine Benutzeridentifizierung erfordert: Altersverifizierung, Speicherung von Metadaten, Zugriff der Strafverfolgungsbehörden auf verschlüsselte Daten.

Schritt 3 – Als Hindernisse für die Beseitigung von Anonymisierungstools werden folgende Punkte identifiziert: VPN, Ende-zu-Ende-Verschlüsselung, sichere Nachrichtenübermittlung.

Schritt 4 — Regulierung Diese Instrumente werden so stark reguliert, dass sie nutzlos oder illegal sind – ohne dass wir jemals explizit gesagt hätten, dass wir jeden überwachen wollen.

Genau dieser Prozess ist im Jahr 2026 im Gange.

Was das konkret für Sie bedeutet

Wenn die laufenden Projekte erfolgreich verlaufen:

Kommerzielle VPNs werden verpflichtet sein, Ihre Daten zu protokollieren. Ein VPN, das aufzeichnet, wer Sie sind und was Sie tun, ist kein VPN mehr – es ist ein überwachter Proxy.

Die Online-Anonymität verschwindet strukturell. Jede Verbindung wird potenziell mit einer realen Identität verknüpft, entweder über EUDIW oder andere Identifizierungsmechanismen.

Die Ende-zu-Ende-Verschlüsselung ist bedroht. Selbst wenn Chat Control in seiner ursprünglichen Form im Jahr 2026 abgelehnt wird, wird es in veränderter Form zurückkehren. Der Druck, auf verschlüsselte Kommunikation zuzugreifen, bleibt hoch.

Anbieter, die sich weigern, werden Europa verlassen. Mullvad hat dies bereits angekündigt. Andere werden folgen. Nur VPNs, die zur Kooperation bereit sind – und sich somit der Überwachung unterziehen –, werden bestehen bleiben.

Auch die Schweiz ist kein sicherer Hafen. Eine geplante Überarbeitung der Schweizer Überwachungsverordnung würde VPN-Anbieter verpflichten, jeden Nutzer anhand eines Ausweisdokuments zu authentifizieren. Der CEO von Proton hat öffentlich erklärt, dass diese Regelung „strenger als in Russland" wäre. Kein kommerzieller Anbieter ist immun, wenn der regulatorische Druck in Europa und der Schweiz gleichzeitig zunimmt.

In der Zwischenzeit bleibt Proton VPN eine der wenigen Lösungen, deren No-Logs-Architektur unabhängig geprüft wird und deren Server sich außerhalb der US-amerikanischen und europäischen Gerichtsbarkeit befinden.

Warum dies für alle ein Problem darstellt – nicht nur für paranoide Menschen

Wir hören oft: „Wer nichts zu verbergen hat, hat nichts zu befürchten."

Dies ist das gefährlichste Argument in der Geschichte der Überwachung.

VPNs werden täglich genutzt von:

- Journalisten, die ihre Quellen schützen
- Whistleblower, die Missstände aufdecken
- Opfer häuslicher Gewalt, die vor einem gewalttätigen Partner fliehen
- Aktivisten in Ländern, in denen Opposition kriminalisiert wird
- Fernarbeiter sichern ihre beruflichen Kontakte
- Millionen von Bürgern, die einfach nur möchten, dass ihre Browserdaten privat bleiben.

Massenüberwachung zielt nicht nur auf Kriminelle ab – sie zielt auf alle. Kriminelle finden jedoch immer andere Wege.

Die grundlegende Frage

Ist Online-Anonymität ein Recht oder ein Privileg?

Wenn es sich um ein Recht handelt, dann müssen die Staaten jeden Verstoß gegen dieses Recht vor einem Richter im Einzelfall mit entsprechenden Schutzmaßnahmen rechtfertigen.

Wenn es sich um ein Privileg handelt, dann können Staaten es im Namen der Sicherheit ohne Rechtsmittel, ohne Transparenz und ohne Einschränkungen abschaffen.

Diese Entscheidung wird 2026 getroffen. Nicht durch ein Referendum. Nicht durch eine Bürgerabstimmung. Sondern von Technokraten und Ministern in technischen Dokumenten, die niemand liest.

Kommerzielle VPNs sind nach wie vor die zugänglichste Lösung, um Ihre Online-Anonymität zu schützen. In einem zunehmend restriktiven regulatorischen Umfeld stellen sie jedoch nur eine vorübergehende Lösung dar – keine langfristige Garantie.

Es gibt Alternativen, die sich strukturell einer Kontrolle entziehen. Webologie wird dieses Thema in Kürze erneut aufgreifen.

Erfahren Sie mehr über Webologie

Abonnieren Sie unseren Newsletter und erhalten Sie die neuesten Beiträge per E-Mail.

Geben Sie Ihre E-Mail-Adresse ein…

Vorherige Der digitale Euro: Wem nützt er wirklich?

Ein freies Internet trotz allem: Der vollständige Leitfaden zur Umgehung der Online-Zensur

Redaktioneller Hinweis: Dieser Artikel dient ausschließlich Informationszwecken. Webologie.me befürwortet, empfiehlt oder übernimmt keine Verantwortung für die Verwendung der unten beschriebenen Tools. Einige der vorgestellten Methoden sind in bestimmten Ländern illegal – ihr rechtlicher Status wird jeweils explizit angegeben. Informationen müssen frei zugänglich bleiben. Zu wissen, wie ein Tool funktioniert, ist nicht dasselbe wie es anzuwenden.

In unserem vorherigen Artikel – VPN: Europa will wissen, wer Sie sind – haben wir analysiert, was wirklich hinter ProtectEU steht, welche Ambitionen Minister Le Hénanff verfolgt und welches dänische Gesetz am 1. Juli 2026 in Kraft treten wird. Wir kamen zu folgendem Schluss:

„Es gibt Alternativen, die sich strukturell einer Kontrolle entziehen. Webologie wird dieses Thema sehr bald wieder aufgreifen.“

Dies ist der Artikel.

Dies ist keine Anleitung zur Umgehung französischer Gesetze – die, wohlgemerkt, VPNs oder die hier vorgestellten Tools derzeit nicht verbieten. Es handelt sich vielmehr um eine vollständige, faktenbasierte und belegte Übersicht aller Möglichkeiten, **die Internetzensur zu umgehen** und einen freien und privaten Zugang zu gewährleisten – sowohl heute als auch im Falle, falls die aktuell vorbereiteten Gesetze morgen in Kraft treten sollten.

Warum herkömmliche VPNs nicht mehr ausreichen, um die Internetzensur zu umgehen

Bevor wir die Alternativen auflisten, müssen wir verstehen, warum das traditionelle VPN zu einem anfälligen Werkzeug wird – auch wenn es nach wie vor nützlich ist.

Das Geschäftsmodell eines kommerziellen VPNs basiert auf einem Versprechen: Der Anbieter speichert keine Verbindungsprotokolle (*No-Logs*). Sie vertrauen darauf, dass er nicht weiß, was Sie online tun.

Der im Juni 2025 veröffentlichte ProtectEU-Fahrplan skizzierte den Weg hin zu einer Verpflichtung für jeden Online-Dienst, einschließlich VPN-Anbieter, Verbindungsmetadaten – IP-Adressen, Zeitstempel, Sitzungsdauer, Datenvolumen – aufzuzeichnen und den Strafverfolgungsbehörden zugänglich zu machen.

Wird dieser Text unverändert übernommen, wird ein VPN *ohne Protokollierung* in Europa faktisch illegal. Das Versprechen kann nicht mehr eingehalten werden. Anbieter, die sich weigern, Protokolle zu führen, müssen den europäischen Markt verlassen – Mullvad hat dies bereits öffentlich angekündigt.

Das ist noch nicht Realität. Aber es ist die Richtung, in die es gehen wird. Und deshalb ist es wichtig, die Alternativen zu kennen – solche, die nicht von einem zentralisierten Anbieter abhängig sind, der gesetzlich dazu verpflichtet werden kann.

Stufe 1 – Ausfallsichere VPNs: Den richtigen Anbieter auswählen

Rechtsstatus in Frankreich: Legal

Nur weil VPNs unter Druck stehen, heißt das nicht, dass sie alle gleich sind. Bevor man sich komplexeren Lösungen zuwendet, sollte man Anbieter in Betracht ziehen, deren Architektur und Rechtslage strukturell eine höhere Widerstandsfähigkeit gegenüber europäischen Regulierungsauflagen bieten.

Proton VPN

Proton VPN hat seinen Sitz in der Schweiz – außerhalb der EU. Die *No-Logs*- Richtlinie des Unternehmens wurde öffentlich geprüft und durch Anfragen von Justizbehörden bestätigt, denen Proton aufgrund fehlender Daten keine Auskunft erteilen musste.

Die Situation in der Schweiz verschärft sich tatsächlich – ein Gesetzesentwurf sieht vor, dass Anbieter IP-Adressen protokollieren und Nutzer authentifizieren müssen. Als Reaktion darauf hat Proton angekündigt, einen Teil seiner Infrastruktur in die EU zu verlagern. Dennoch bleibt Proton VPN eine der zuverlässigsten Optionen für französischsprachige Nutzer: eine französische Benutzeroberfläche, Apps für alle Plattformen, das WireGuard-Protokoll und ein integrierter Kill-Switch.

Mullvad

Mullvad (Schweden) setzt technische Maßstäbe für radikale *No-Logs-Technologie* . Für die Registrierung ist keine E-Mail-Adresse erforderlich – Sie erhalten eine zufällige Kontonummer. Zahlung ist in bar oder mit Kryptowährung möglich.

Mullvad hat öffentlich erklärt, dass es Europa lieber verlassen würde, als seine Architektur an die Protokollierungsvorschriften anzupassen. Dies ist die härteste Haltung der Branche – und diejenige, die am besten zu seinem Versprechen der Anonymität passt.

Was das nicht löst

Selbst ein exzellentes VPN bleibt ein zentraler Zugangspunkt. Sie vertrauen einem Unternehmen. Ändert sich die Gesetzeslage und bleibt das Unternehmen durch die Einhaltung der neuen Bestimmungen auf dem europäischen Markt, verschwindet Ihr Schutz – ohne dass Sie es unbedingt bemerken.

Deshalb verdienen die folgenden Lösungen Beachtung.

Stufe 2 – Das selbstgehostete VPN

Rechtsstatus in Frankreich: Legal

Wir haben dies bereits in unserem Artikel „Ihr eigenes VPN in 15 Minuten“ besprochen . Die Idee ist einfach: Anstatt einen Anbieter zu bezahlen, installieren Sie Ihren eigenen VPN-Server auf einem VPS (virtuellen privaten Server), den Sie im Ausland mieten.

Der größte Vorteil: Sie müssen keinem Dritten vertrauen. Sie *sind* der Lieferant.

Zu beachtende Einschränkungen:

- Wenn der VPS in einem Land gehostet wird, das denselben Vorschriften unterliegt, sind Sie denselben Risiken ausgesetzt.
- Für Konfiguration und Wartung benötigen Sie ein Mindestmaß an technischen Kenntnissen.
- Ihre IP-Adresse auf dem VPS gehört Ihnen – wenn sie kompromittiert wird, sind Sie direkt betroffen.

Empfohlene Lösungen: WireGuard (modernes, leistungsstarkes Protokoll), Outline (basiert auf Shadowsocks, einfacher zu implementieren).

Bevorzugte Hosting-Anbieter: außerhalb der EU und außerhalb der Five Eyes — Island (1984 Hosting), Niederlande (Frantech), Schweiz (Infomaniak).

Level 3 — Tor: das Zwiebelnetzwerk

Rechtsstatus in Frankreich: Legal

Die Nutzung des Tor-Browsers ist in Frankreich völlig legal. Die Legalität hängt davon ab, welche Online-Aktivitäten Sie durchführen – der Zugriff auf legale Inhalte über Tor birgt keine rechtlichen Probleme.

So funktioniert es

Tor (*The Onion Router) ist ein dezentrales Netzwerk, das aus Tausenden von freiwilligen Servern, sogenannten Relays,* besteht . Wenn Sie eine Anfrage über Tor senden, wird diese in drei aufeinanderfolgenden Schichten verschlüsselt und durchläuft drei Relays, bevor sie ihr Ziel erreicht. Jedes Relay kennt nur das vorherige und das nächste Relay – niemals den gesamten Übertragungsweg.

Das Ergebnis: Weder Ihr Internetanbieter noch eine Regierung noch die von Ihnen besuchte Website können Ihre Identität mit Ihren Online-Aktivitäten verknüpfen. Keine zentrale Stelle. Kein Unternehmen, das man unter Druck setzen könnte. Keine Protokolle, die man anfordern könnte.

Wie man es benutzt

Am einfachsten geht es so: Laden Sie **den Tor Browser** von torproject.org herunter . Es handelt sich um eine modifizierte Version von Firefox, die bereits für die Nutzung des Tor-Netzwerks vorkonfiguriert ist. Es sind keine weiteren technischen Einstellungen erforderlich.

Für Android: **Orbot** (ermöglicht es allen Anwendungen, Tor zu passieren) oder **Tor Browser für Android** .

Für maximalen Schutz vor Internetzensur: **Tails OS** – ein Live-Betriebssystem, das *den gesamten* Netzwerkverkehr über Tor leitet und keine Spuren auf Ihrem Rechner hinterlässt. Es startet von einem USB-Stick.

Die tatsächlichen Grenzen von Tor

Tor ist keine Zauberei. Einige Punkte verdienen es, ehrlich anerkannt zu werden:

Geschwindigkeit. Drei Relais bedeuten Latenz. Tor ist langsam. Es eignet sich nicht für Streaming oder große Downloads. Es ist hervorragend geeignet für Text-Browsing, Kommunikation und Informationsabfrage.

Exit-Nodes. Der dritte Relay-Server (*Exit-Node*) empfängt unverschlüsselten Datenverkehr, wenn Sie eine Website über HTTP (ohne HTTPS) aufrufen. Auf einer HTTPS-Website bleibt der Inhalt zwar verschlüsselt, aber der Exit-Node erkennt Ihren Besuch. Daher ist die Verwendung von HTTPS unerlässlich.

Verkehrskorrelation. Ein Angreifer mit umfassender Netzwerkübersicht (ein Staat, der sowohl Ihren Internetanbieter als auch zahlreiche Tor-Knoten kontrolliert) kann theoretisch Ihre Identität durch zeitliche Analyse des Datenverkehrs rekonstruieren. Dies ist ein realer Angriffsvektor, der jedoch erhebliche Ressourcen erfordert.

Verhaltensassoziation. Die Verbindung zu Ihrem Facebook-Konto über Tor anonymisiert Sie nicht – Facebook weiß, wer Sie sind. Die Anonymität von Tor beruht auf der Trennung der Identitäten.

Tor in Ländern, die es blockieren

In einigen Ländern (China, Iran, Russland) ist der Zugriff auf öffentliche Tor-Server blockiert. In diesem Fall bietet das Tor-Netzwerk **Bridges** – nicht veröffentlichte Relays – und **austauschbare Transportprotokolle** wie **obfs4** an , die den Tor-Datenverkehr so verschleiern, dass er wie gewöhnlicher HTTPS-Datenverkehr aussieht und somit durch Deep Packet Inspection (*DPI*) nicht erkennbar ist.

In Frankreich ist das heute nicht notwendig. Es ist aber eine Fähigkeit, die genutzt werden kann, falls sich die Situation ändert.

Stufe 4 – I2P: Das Internet im Internet

Rechtsstatus in Frankreich: Legal

I2P (*Invisible Internet Project*) ist weniger bekannt als Tor, basiert aber auf einer anderen Philosophie – und in manchen Kontexten auf einer robusteren.

Der grundlegende Unterschied zu Tor

Tor ist primär für den anonymen Zugriff auf das *Clearnet* (das reguläre Internet) konzipiert. I2P ist ein *geschlossenes* Netzwerk , das die Kommunikation zwischen seinen internen Diensten ermöglicht.

I2P verwendet eine Verschlüsselungsmethode namens „Knoblauch-Verschlüsselung“ – anders als die Zwiebel-Verschlüsselung von Tor –, die mehrere Nachrichten vor dem Versand zusammenfasst und so die Analyse des Datenverkehrs erschwert. Ziele in I2P sind kryptografische Kennungen, keine IP-Adressen.

Bei I2P gibt es keinen Exit-Node – der gesamte Datenverkehr verbleibt *innerhalb* des Netzwerks. Dadurch wird die größte Schwäche von Tor (der Exit-Node) beseitigt. Allerdings kann man über I2P nicht direkt auf Google oder Wikipedia zugreifen – man nutzt stattdessen Dienste, die *innerhalb* des I2P-Netzwerks selbst gehostet werden (*z. B. Eepsites* , interne Nachrichtensysteme, Foren).

Für wen ist I2P gedacht?

I2P ist kein Tool für die breite Öffentlichkeit. Es richtet sich an Nutzer, die Folgendes wünschen:

- Kommunizieren Sie anonym mit anderen I2P-Nutzern
- Sie hosten ihre eigenen Dienste ohne Offenlegung
- Profitieren Sie von einem Netzwerk, das strukturell resistent gegen Massenüberwachung ist.

Einrichtung

I2P ist unter geti2p.net verfügbar . Die empfohlene Implementierung im Jahr 2026 ist **i2pd** (in C++), das schlanker und leistungsfähiger als die ursprüngliche Java-Version ist.

Hinweis: Das Betreiben eines I2P-Relays ist in Frankreich legal. Ein Relay gilt als einfacher Informationsträger im Sinne von Artikel 12 der europäischen Richtlinie 2000/31/EG, die in französisches Recht umgesetzt wurde.

Level 5 – Schattensocken und Verschleierung: Verkehr unsichtbar machen

Rechtslage in Frankreich: Legal. Rechtslage in Ländern mit starker Zensur (China, Iran, Russland): Grauzone bis illegal, je nach Verwendungszweck.

Shadowsocks: geboren, um die Große Firewall zu umgehen.

Shadowsocks ist ein Open-Source-Protokoll für verschlüsselte Proxys, das 2012 von einem chinesischen Entwickler mit dem Ziel entwickelt wurde, Zensur auf einfache, schnelle und äußerst unauffällige Weise zu umgehen. Anders als ein VPN ist es kein vollständiges virtuelles Netzwerk, sondern ein selektiver Proxy, der für spezifische Anwendungen konfiguriert werden kann. Das Protokoll verschleiert den Datenverkehr, sodass er wie gewöhnlicher HTTPS-Verkehr aussieht und somit für Deep-Packet-Inspection-Tools (*DPI*) nur schwer zu erkennen ist.

In der Praxis benötigt Shadowsocks einen Remote-Server (einen unzensierten VPS), auf dem die Serverkomponente installiert wird, sowie eine Client-Anwendung auf Ihrem Gerät. **Outline** , entwickelt von Jigsaw (einer Tochtergesellschaft von Alphabet), ist die einfachste Lösung für die Bereitstellung von Shadowsocks ohne fortgeschrittene Kenntnisse.

Verschleierungsprotokolle

Verschleierung geht über einfache Verschlüsselung hinaus: Sie *verbirgt* den Datenverkehr so, dass er nicht mehr nachweisbar ist.

obfs4 – der Referenz-Verschleierungstransport des Tor-Projekts. Er wandelt den Tor-Datenverkehr in einen zufälligen Datenstrom um, der nichts Erkennbares mehr erkennen lässt. Wird vom Tor Browser über das Bridges-Menü verwendet.

Shadowsocks mit dem v2ray-Plugin fügt eine WebSocket/TLS-Verschleierungsschicht hinzu. Der Datenverkehr erscheint einem CDN (z. B. Cloudflare) als normales HTTPS. Praktisch nicht erkennbar.

VLESS/XTLS (Xray) – ein von der chinesischen Anti-Zensur-Bewegung entwickeltes Protokoll. Es nutzt *uTLS* , um die TLS-Fingerabdrücke legitimer Browser perfekt nachzuahmen. Hohes technisches Niveau bei maximaler Effektivität.

Was diese Werkzeuge wirklich ermöglichen

Die Kombination aus selbstgehostetem VPN, Shadowsocks und Verschleierungs-Plugin ergibt einen Netzwerktunnel, dessen Datenverkehr für jedes Netzwerküberwachungssystem optisch nicht von Standard-HTTPS zu unterscheiden ist. Millionen von Menschen in China nutzen diese Methode täglich, um frei auf das Internet zuzugreifen – in einem Land, in dem dies offiziell illegal ist.

In Frankreich ist das heute völlig legal. Und wenn die derzeit in Arbeit befindlichen Regelungen morgen Erfolg haben, wäre es die einzige technisch tragfähige Lösung gegen fortschrittliche Filter.

Stufe 6 – Mesh- und dezentrale Netzwerke

Rechtsstatus in Frankreich: Legal

Diese Lösungen sind zwar am wenigsten bekannt, aber strukturell am widerstandsfähigsten – weil sie keinen zentralen Blockierpunkt haben.

Yggdrasil

Yggdrasil ist ein durchgängig verschlüsseltes Peer-to-Peer-Overlay-Netzwerk ohne zentrale Infrastruktur. Jeder Knoten fungiert sowohl als Client als auch als Router. Es müssen keine Server verwaltet, keine Unternehmen eingeschränkt und keine Ledger überwacht werden.

Yggdrasil ist noch experimentell und in französischer Sprache nur unzureichend dokumentiert. Seine Architektur unterscheidet sich jedoch grundlegend von allem, was von einem Nationalstaat reguliert werden kann.

Hyphanet (ehemals Freenet)

Hyphanet ist ein vollständig verteiltes Netzwerk zum Informationsaustausch. Dateien werden aufgeteilt, verschlüsselt und auf die Festplatten aller Teilnehmer verteilt. Niemand weiß, welche Fragmente welcher Dateien er speichert. Zensur ist strukturell unmöglich.

Hauptsächlich für die Veröffentlichung und Anzeige zensierter Inhalte gedacht. Sehr langsame Übertragungsgeschwindigkeit. Geeignet für Dokumente und Texte, nicht für Streaming.

IPFS (InterPlanetary File System)

IPFS ist ein Protokoll zum Speichern und Verteilen dezentraler Inhalte. Anstatt Ressourcen über ihren Speicherort (eine URL) zu adressieren, adressiert IPFS sie über ihren Inhalt (einen

kryptografischen Hash). Auf IPFS veröffentlichte Inhalte können nicht von einer zentralen Stelle gelöscht werden – sie bleiben verfügbar, solange auch nur ein einziger Knoten sie teilt.

IPFS wird bereits zur Speicherung von Archiven zensierter Websites und Publikationen genutzt, die Regierungen zu unterdrücken versucht haben.

Stufe 7 – Lösungen, die in bestimmten Ländern in einer Grauzone liegen oder illegal sind

Wichtiger Hinweis : Die folgenden Methoden sind zum Zeitpunkt der Veröffentlichung in Frankreich legal. In anderen europäischen oder außereuropäischen Ländern können sie illegal sein. Ihre Darstellung hier dient ausschließlich Informationszwecken.

Tor in einem Land nutzen, das es blockiert

Rechtsstatus: Illegal in Russland, China, Iran, Turkmenistan, Belarus, Nordkorea

In diesen Ländern ist der Zugriff auf das Tor-Netzwerk strengstens verboten. Dennoch nutzen täglich Hunderttausende Menschen die oben genannten obfs4-Bridges. Sollte Frankreich Tor morgen blockieren – ein Szenario, das derzeit noch nicht eingetreten ist, aber bis 2030 durchaus möglich sein könnte –, wären dieselben Tools weiterhin nutzbar.

Die Nutzung eines VPNs in einem Land, das dies verbietet

Rechtslage in Frankreich: Legal. Rechtslage in Dänemark ab 1. Juli 2026: Umgehung der Zensur ist illegal. Rechtslage in Russland: Technisch gesehen legal, jedoch sind Dutzende Anbieter gesperrt. Rechtslage in China: Ohne staatliche Genehmigung illegal.

Dänemark hat ein Gesetz verabschiedet, das am 1. Juli 2026 in Kraft tritt und die Nutzung von VPNs zur Umgehung der Zensur unter Strafe stellt. Dänische Staatsbürger, die ein VPN nutzen, um auf gesperrte Inhalte zuzugreifen, verstoßen damit formal gegen das Gesetz. Verschleierungstools (Shadowsocks, obfs4) wären in diesem Zusammenhang die einzige Möglichkeit, einen unentdeckten Zugriff zu gewährleisten – und wären daher, trotz formaler Illegalität, ohne Risiko praktischer Sanktionen nutzbar.

Der Tor-Exit-Node als Proxy-Server

Der Betrieb eines Tor-Exit-Nodes zu Hause ist in Frankreich legal, kann aber je nach Vertragsbedingungen Probleme mit Ihrem Hosting-Anbieter oder Internetdienstanbieter (ISP) verursachen. Es ist zwar nicht illegal, aber eine rechtliche Grauzone, die zur Kündigung Ihres Abonnements führen kann, wenn Ihr ISP dies vertraglich untersagt.

Alternative DNS- und dezentrale Auflösung

DNS-Filterung ist die gängigste Methode, mit der französische Behörden Webseiten (z. B. The Pirate Bay, illegale Streaming-Dienste) sperren. Sie lässt sich einfach und legal umgehen, indem man die DNS-Server auf die von Cloudflare (1.1.1.1), Quad9 (9.9.9.9) oder – für den größten Schutz vor Zensur – **NextDNS** mit benutzerdefinierter Filterung ändert.

Die Entwicklung dezentraler DNS-Systeme wird sich beschleunigen, um die Filterung durch DNS4EU zu umgehen, den europäischen Resolver, der mittlerweile als Instrument administrativer Blockierung missbraucht wird. Internetnutzer werden sich Blockchain-basierten

Systemen oder Peer-to-Peer-Netzwerken zuwenden, die keine zentrale Instanz haben, gegen die man klagen kann.

Handshake und **ENS** (Ethereum Name Service) sind zwei dezentrale DNS-Projekte, die bereits in Betrieb sind. Niemand kann deren Zensur anordnen.

Zusammenfassende Vergleichstabelle

Werkzeug	Benutzerfreundlichkeit	Anonymität	Geschwindigkeit	Legal FR	Regulatorischer Widerstand
Kommerzielle VPNs (Proton, Mullvad)					Durchschnitt
Selbstgehostetes VPN					Gut
Tor-Browser					Sehr hoch
Tor + obfs4					Maximal
I2P					Sehr hoch
Schattensocken					Sehr hoch
Tails OS					Maximal
IPFS / Hyphanet					Maximal
Alternative DNS-Server					Niedrig bis mittel

Webologies Empfehlungen basierend auf Ihrem Profil

Sie möchten Ihre Privatsphäre einfach nur schützen? → Proton VPN + Cloudflare DNS (1.1.1.1). Simpel, effektiv, legal. Deckt 95 % aller Anwendungsfälle ab.

Wenn Sie Journalist, Aktivist sind oder zu sensiblen Themen arbeiten, nutzen Sie den Tor Browser, HTTPS überall und Tails OS für wichtige Kommunikation. Verwenden Sie niemals ein kommerzielles VPN für Ihre Quellen.

Sie sind technikbegeistert und möchten Ihre Infrastruktur selbst kontrollieren? → Selbstgehostetes VPN auf einem VPS außerhalb der EU + Shadowsocks mit Verschleierungs-Plugin. Volle Freiheit, volle Verantwortung.

Sie erwarten strengere Regulierungen und möchten sich darauf vorbereiten? → Lernen Sie jetzt Tor + obfs4-Bridges. Es ist nicht kompliziert, aber man sollte es nicht überstürzen.

Wenn Sie in einem Land leben oder reisen, das das Internet aktiv zensiert, verwenden Sie Shadowsocks oder VLESS/Xray in Kombination mit einem Server außerhalb des jeweiligen Landes. Millionen von Menschen in China, Iran und Russland nutzen diese Methode. Informieren Sie sich vor der Nutzung stets über die geltenden Gesetze vor Ort.

Etwas, das niemand blockieren kann

Es gibt eine technische Wahrheit, die die europäischen Gesetzgeber scheinbar ignorieren – oder so tun, als würden sie sie ignorieren.

Je mehr die Behörden den Zugang zum Internet einschränken, desto stärker drängen sie die Nutzer zu verteilten Protokollen. Die weitverbreitete Nutzung des Tor-Netzwerks und unauffindbarer Bridges wird es Nutzern ermöglichen, selbst strengste Zensur zu umgehen. Der Einsatz von Verschleierungsprotokollen wie Shadowsocks wird zum Standard für die Verschleierung des Internetverkehrs selbst.

Dies ist das sogenannte Streisandsche Gesetz, angewendet auf technische Zensur: Je mehr man etwas verbietet, desto größer wird die Nachfrage nach und die Nutzung von Umgehungswerkzeugen. China investiert seit dreißig Jahren Milliarden von Dollar und Zehntausende von Ingenieuren in seine Große Firewall – und Millionen von Chinesen greifen täglich über Shadowsocks darauf zu.

Europa hat einen Regulierungsweg gewählt, der, sollte er Erfolg haben, zum selben Ergebnis führen wird: eine gespaltene Bevölkerung zwischen denen, die Überwachung standardmäßig akzeptieren, und einer technisch versierten Minderheit, die sich mithilfe unauffindbarer Protokolle frei bewegen kann. Dies ist weder ein Sieg für die Privatsphäre noch ein Sieg für die Sicherheit. Es ist eine Niederlage für alle – außer für diejenigen, die Überwachung wollten.

Die beste Verteidigung ist, diese Werkzeuge zur Umgehung der Internetzensur zu erlernen, bevor man sie braucht.

Mehr dazu erfahren Sie in unserem 15-minütigen Leitfaden zu persönlichen VPNs und in der vollständigen Analyse von ProtectEU zu VPN-Regulierungen in Europa .

Warnung: Europäische digitale Identitäts-Wallet – die Risiken

Hier ist, was Webologie über die europäische digitale Identitäts-Wallet herausgefunden hat – und was die offiziellen Texte nicht hervorheben.

Bis Ende 2026 wird jedem Bürger der Europäischen Union eine digitale Identitätsmappe zur Verfügung stehen. Personalausweis, Führerschein, Zeugnisse, Krankenversicherungskarte, Fahrzeugschein – alles in einer App auf dem Smartphone. Diese digitale Identitätsmappe basiert auf der eIDAS-2.0-Verordnung.

Die Europäische Union präsentiert dieses Projekt als Fortschritt in Richtung digitaler Souveränität und administrativer Vereinfachung. Webologie hat offizielle Texte, technische Dokumente und unabhängige Analysen geprüft. Das Bild ist differenzierter – und einige Aspekte verdienen es, öffentlich thematisiert zu werden.

Was ist die europäische digitale Identitäts-Wallet?

Das Projekt trägt den Namen EUDIW – Europäische Digitale Identitäts-Wallet. Es basiert auf der eIDAS 2.0-Verordnung (EU-Verordnung 2024/1183), die am 20. Mai 2024 in Kraft trat.

Konkret handelt es sich um eine mobile Anwendung, die Ihre offiziellen Ausweisdokumente zentralisiert und es Ihnen ermöglicht, diese digital vorzulegen – um auf öffentliche Dienstleistungen zuzugreifen, ein Bankkonto zu eröffnen, einen Vertrag zu unterzeichnen oder sich online zu authentifizieren.

Der offizielle Zeitplan:

- **Bis Ende 2026:** Jeder EU-Mitgliedstaat muss seinen Bürgern und Einwohnern mindestens eine digitale Geldbörse anbieten.
- **Bis Ende 2027** müssen Banken, Kreditinstitute, Telekommunikationsbetreiber und große Plattformen (mit mehr als 50 Millionen Nutzern) es als Identifikationsmittel akzeptieren.
- **2030:** Das erklärte Ziel ist, dass 80 % der europäischen Bürger entsprechend ausgestattet sein sollen.

In Frankreich wird die im Februar 2024 eingeführte und bereits nach eIDAS 2.0 zertifizierte Anwendung **France Identité zur offiziellen europäischen digitalen Identitäts-Wallet.**

Was das Projekt verspricht

Die offiziellen Argumente der Europäischen Kommission für die digitale Identitätsgeldbörse lauten wie folgt:

Einfachheit. Kein Scannen von Dokumenten oder erneutes Eingeben von Informationen mehr bei jedem Schritt. Starke, sofortige Authentifizierung, anerkannt in allen 27 Mitgliedstaaten.

Souveränität. Die Befreiung von der Abhängigkeit von den Identifizierungssystemen von Google und Apple – „Mit Google anmelden“, „Mit Apple anmelden“ –, die es diesen amerikanischen Unternehmen ermöglichen, Ihre Verbindungen zu verfolgen.

Kontrolle. Sie entscheiden, was Sie mit wem teilen. Der Grundsatz der „minimalen Offenlegung“ ist in den Vorschriften verankert: Sie können nachweisen, dass Sie über 18 Jahre alt sind, ohne Ihr genaues Geburtsdatum preiszugeben.

Sicherheit. Ihre Daten werden lokal auf Ihrem Gerät gespeichert, nicht auf zentralen Servern. Die Vorschriften sehen keine Nachverfolgbarkeit von Transaktionen vor.

Freiwillige Nutzung. Die Regel ist eindeutig: Niemand wird zur Nutzung der digitalen Geldbörse gezwungen. Physische Alternativen müssen erhalten bleiben.

Diese Argumente sind berechtigt. Sie verdienen es, ernst genommen zu werden. Aber sie erzählen nicht die ganze Geschichte.

Was sie Ihnen weniger erzählen

1. Google und Apple in der Technologiekette

Die EU verspricht ein souveränes System, unabhängig von den GAFAM-Unternehmen. Die technische Realität der deutschen Umsetzung – dokumentiert vom Bundesinnenministerium (BMI) selbst – zeichnet ein anderes Bild.

Um zu überprüfen, ob ein Android-Gerät vertrauenswürdig ist, bevor die Nutzung der Wallet autorisiert wird, verwendet das System **Google Play Integrity** – einen proprietären Prüfmechanismus von Google. Auf iOS übernimmt Apples **AppAttest** diese Funktion.

Konkret bedeutet dies, dass Ihr Smartphone von Google oder Apple freigegeben werden muss, bevor Sie Ihre europäische digitale Identität nutzen können. Diese Unternehmen bestätigen die Vertrauenswürdigkeit Ihres Geräts.

Die deutsche Dokumentation bestätigt dies ausdrücklich: Das `deviceIntegrity` Play Integrity-Signal beinhaltet „ein firmeneigenes Urteil von Google über kompromittierte Geräte – wir wissen nicht, was Google tatsächlich im Hintergrund tut."

Es gibt technische Alternativen, die diese Abhängigkeit umgehen würden. Entwickler haben deren Integration in das Referenz-GitHub-Repository gefordert. Diese Anfragen wurden ohne überzeugende technische Begründung ignoriert.

Es ist anzumerken, dass es sich hier um die deutsche Umsetzung handelt, die eine Vorreiterrolle einnehmen wollte. Andere Mitgliedstaaten, darunter Frankreich, könnten andere Wege gehen. Der Präzedenzfall ist jedoch besorgniserregend.

2. Das Risiko der administrativen Trennung

Die Verordnung legt fest, dass Sie die Kontrolle über Ihre Daten behalten. Unklar bleibt jedoch, was passiert, wenn der Zugriff auf Ihre Wallet gesperrt wird – sei es durch eine Verwaltungsentscheidung, einen technischen Fehler oder eine einseitige Entscheidung eines privaten Betreibers.

Wenn Ihr physischer Ausweis abläuft, werden Sie Monate im Voraus benachrichtigt. Wenn eine App gesperrt wird, kann das innerhalb von Sekunden geschehen.

Wenn morgen Ihre digitale Geldbörse den Zugang zu öffentlichen Dienstleistungen, Ihrem Bankkonto und Ihren Rezepten zentralisiert, kann selbst eine vorübergehende oder irrtümliche Sperrung Ihre administrative Existenz bedrohen. Dies geschieht ohne ein klar definiertes Beschwerdeverfahren in den Vorschriften und ohne Transparenz hinsichtlich der Sperrkriterien.

Die Frage, die offiziell niemand stellt: **Wenn Google Ihr Android-Konto sperrt, wer ist dann für den Verlust des Zugangs zu Ihrer offiziellen Identität verantwortlich?** Google, der Mitgliedstaat, der diese Infrastruktur gewählt hat, oder die Europäische Kommission, die das Modell genehmigt hat?

3. Ein beispielloses Hackerziel

Das Prinzip der europäischen digitalen Identitäts-Wallet besteht darin, Ihre sensibelsten Dokumente in einem einzigen System zu zentralisieren. Das ist ihre Stärke – und zugleich ihre Achillesferse.

Im April 2026 wurde die französische Behörde ANTS (Nationale Agentur für sichere Dokumente) aufgrund einer simplen Sicherheitslücke gehackt: Es genügte, eine Zahl in einer URL zu ändern, um auf die Daten anderer Bürger zuzugreifen. Dadurch waren potenziell 19 Millionen französische Bürger gefährdet.

Eine europäische digitale Identitätsbörse, die die Identitätsdaten von 450 Millionen europäischen Bürgern zentralisiert, stellt ein beispiellos wertvolles Ziel für kriminelle Gruppen und ausländische Geheimdienste dar. Sie müssen nicht das zentrale System angreifen – es genügt, einen einzigen Mitgliedstaat, einen einzigen zertifizierten Anbieter, ein einziges Glied in der Kette zu kompromittieren.

Die Grundregel der Cybersicherheit ist einfach: Je größer die Zentralisierung, desto attraktiver das Ziel.

4. „Freiwilliger“ – wie lange?

Die Regelung ist eindeutig: Die europäische digitale Identitäts-Wallet bleibt offiziell optional. Kein Dienst darf jemanden ablehnen, der sie nicht nutzt. Physische Alternativen müssen weiterhin bestehen bleiben.

Das trifft auch heute noch zu. Aber Folgendes trifft ebenfalls zu:

Bis Ende 2027 werden alle Banken und großen Plattformen verpflichtet sein, die digitale Geldbörse **zu akzeptieren** . Behörden, die ihre Prozesse auf die digitale Geldbörse ausrichten, werden zwangsläufig zusätzliche Hürden für diejenigen schaffen, die sie nicht nutzen.

Die Geschichte digitaler Technologien lehrt uns, dass „optional“ und „Standard“ letztendlich immer zusammenlaufen. Wenn 80 % der Bürger ein System nutzen, ist die Minderheit, die sich weigert, nicht länger geschützt – sie wird marginalisiert.

5. Die demokratische Frage

Die eIDAS 2.0-Verordnung wurde im März 2024 vom Europäischen Parlament und dem Rat der Europäischen Union verabschiedet. Dies ist ihre formale Legitimität.

Dieser Gesetzgebungsprozess fand jedoch ohne direkte öffentliche Anhörung, ohne Volksabstimmung und ohne dass das Thema vor seiner Verabschiedung im Mittelpunkt der öffentlichen Debatte stand, statt. Ein Gesetz, das die Identität von 450 Millionen Bürgern berührt, wurde von Abgeordneten beschlossen, deren Mandat dieses Thema nicht ausdrücklich umfasste.

Der Präzedenzfall des französischen Referendums von 2005 – bei dem die Bürger Nein zum Europäischen Verfassungsvertrag sagten, der dann in einer anderen Form durch den Vertrag von Lissabon ohne eine neue Volksabstimmung angenommen wurde – ist den Menschen weiterhin präsent.

In einer Demokratie sind formale Legitimität und demokratische Legitimität nicht immer dasselbe.

Was Sie jetzt tun können

Informieren Sie sich und verbreiten Sie die Nachricht. Dieses Projekt ist trotz seines potenziellen Einflusses in der Öffentlichkeit noch relativ unbekannt. Schon der Austausch darüber trägt dazu bei, seine automatische Übernahme zu verhindern.

Bewahren Sie Ihre Papierdokumente auf. Solange physische Alternativen rechtlich garantiert sind, nutzen Sie diese. Tragen Sie nicht durch Desinteresse zu deren allmählichem Verschwinden bei.

Beobachten Sie die technischen Entscheidungen der französischen Regierung. France Identité wird die französische Geldbörse sein. Die architektonischen Entscheidungen des französischen Teams – insbesondere hinsichtlich der Abhängigkeit von Google und Apple – werden entscheidend sein. Diese Informationen sind öffentlich und verdienen genaue Prüfung.

Nehmen Sie an den öffentlichen Konsultationen teil. Die Durchführungsbestimmungen, die die technischen Details festlegen, werden derzeit noch erarbeitet. Öffentliche Konsultationen finden bereits statt – sie sind zwar nicht allgemein bekannt, aber zugänglich.

Kontaktieren Sie Ihre Abgeordneten. Mitglieder des Europäischen Parlaments und nationale Parlamentarier können zu den technischen Entscheidungen und den demokratischen Garantien des Projekts befragt werden.

Abschluss

Die europäische digitale Identitätsbörse ist nicht grundsätzlich schlecht. Das Ziel der administrativen Vereinfachung ist durchaus berechtigt. Die in der Verordnung verankerten Datenschutzgarantien sind – zumindest auf dem Papier – solide.

Doch ein Projekt dieser Größenordnung – das die administrative Identität von 450 Millionen Menschen betrifft – verdient eine öffentliche Debatte, die seinem Ausmaß gerecht wird. Diese Debatte fand nicht statt.

Wir bei Webologie sind der Überzeugung, dass Technologie den Bürgern dienen und sie nicht kontrollieren sollte. Ein Tool, das Ihr gesamtes Verwaltungsleben auf einem Smartphone zentralisiert, dessen Infrastruktur von einseitigen Entscheidungen amerikanischer Unternehmen abhängt und dessen „freiwillige“ Nutzung nach und nach unverzichtbar werden wird, verdient Wachsamkeit und kritische Hinterfragung.

Sich zu informieren, Fragen zu stellen und die Kontrolle darüber zu behalten, was wir akzeptieren – das ist die Grundlage der individuellen digitalen Souveränität.

Mehr dazu: Datenpannen – was sofort zu tun ist? | Ihre persönlichen Daten sind Gold wert – so schützen Sie sie

Ihre eigene Cloud zu Hause: Was ein Heim-NAS ist und was es alles für Sie tun kann

Lesezeit: 10 Minuten

Einführung

Ein Heim-NAS ist Ihre eigene Cloud – unter Ihrer Kontrolle, zu Hause.

Jeden Monat zahlen Sie Google, Apple oder Microsoft dafür, dass Ihre Fotos, Dateien und Erinnerungen auf deren Servern gespeichert werden.

Monat für Monat vertrauen Sie darauf, dass sie Ihre Daten nicht lesen, nicht weiterverkaufen und nicht auf rechtliche Anfrage hin weitergeben.

Monat für Monat sind Sie auf sie angewiesen, um auf Ihr eigenes digitales Leben zugreifen zu können.

Es gibt eine Alternative. Sie heißt NAS.

Ein NAS ist Ihre persönliche Cloud – zu Hause, unter Ihrer Kontrolle und von überall auf der Welt zugänglich. Ihre Daten verlassen niemals Ihr Zuhause. Niemand außer Ihnen hat Zugriff darauf. Und nach der anfänglichen Investition kostet es Sie fast nichts mehr.

Dieser Artikel erklärt, was ein NAS ist, was man alles damit machen kann und warum immer mehr Menschen die Kontrolle über ihre Daten zurückgewinnen wollen.

Was ist ein Heim-NAS?

NAS steht für Network Attached Storage (Netzwerkspeicher). Ein Heim-NAS ist ein Gerät, das an Ihren Internetrouter angeschlossen ist und eine oder mehrere Festplatten enthält.

Stellen Sie sich eine externe Festplatte vor, nur viel leistungsstärker. Anstatt direkt an Ihren Computer angeschlossen zu sein, wird sie mit Ihrem WLAN-Netzwerk verbunden. Alle Ihre Geräte – Computer, Smartphone, Tablet, Fernseher – können gleichzeitig und kabellos von jedem Raum im Haus darauf zugreifen.

Und von unterwegs? Dasselbe. Im Urlaub, im Büro, auf Reisen – Sie greifen auf Ihre Dateien zu, als wären Sie zu Hause.

Äußerlich ähnelt ein NAS einer kleinen, unauffälligen schwarzen Box. Es steht auf einem Regal, wird per Ethernet mit dem Router und einer Steckdose verbunden und arbeitet geräuschlos rund um die Uhr, ohne dass man sich darum kümmern muss.

Im System läuft ein eigenes Betriebssystem. Synology, Marktführer für Heimanwender, hat DSM entwickelt – eine intuitive Weboberfläche, die einem Computer-Desktop ähnelt. Die Verwaltung erfolgt über den Browser, ohne Kommandozeilen oder spezielle technische Kenntnisse.

Die wahre Leistungsfähigkeit eines NAS liegt in den darauf installierbaren Anwendungen. Diese – sogenannten Softwarepakete – verwandeln Ihr NAS in eine vollwertige Plattform, die nahezu alle Ihre heutigen kostenpflichtigen Cloud-Dienste ersetzen kann.

Was Sie mit einem NAS machen können

Hier entfaltet das NAS sein volles Potenzial. Sehen Sie, was ein einfacher Kasten in Ihrem Regal alles für Sie leisten kann.

Sichern Sie automatisch alle Ihre Geräte

Das ist die grundlegende Funktion – und schon allein deshalb ausreichend, um den Kauf zu rechtfertigen.

Ihr NAS sichert automatisch Ihren Windows- oder macOS-Computer, Ihr Android- oder iPhone-Smartphone und alle anderen Geräte in Ihrem Heimnetzwerk. Sie müssen nichts tun. Es gibt keine monatlichen Gebühren. Die Datensicherung startet, sobald sich ein Gerät mit Ihrem WLAN verbindet.

Dies ist Stufe 2 der 3-2-1-Regel, die wir in unserem ersten Artikel dieser Reihe vorgestellt haben.

Ersetzen Sie Google Fotos oder iCloud.

Synology Photos und Immich sind zwei Anwendungen, die Ihr NAS in eine intelligente Fotogalerie verwandeln.

Gesichtserkennung, automatische Sortierung nach Datum und Ort, Zugriff vom Smartphone, Alben mit der Familie teilen – alle wichtigen Funktionen von Google Fotos, jetzt ganz bequem von zu Hause aus. Ihre Erinnerungen verlassen dabei niemals die Server von Google oder Apple.

Hinweis: Die KI-gestützten Bearbeitungswerkzeuge von Google Fotos – Zauberstab, erweiterte automatische Retusche – sind auf NAS-Systemen nicht verfügbar. Wenn Ihnen diese Funktionen wichtig sind, bietet Google Fotos in dieser Hinsicht weiterhin einen umfassenderen Funktionsumfang.

Ersetzen Sie Netflix durch Ihre eigene Medienbibliothek.

Jellyfin und Plex sind Open-Source-Medienserver. Sie speichern Ihre Filme, Serien und Musik auf Ihrem NAS und streamen sie auf jeden beliebigen Bildschirm im Haus – Fernseher, Computer, Smartphone, Tablet.

Die Benutzeroberfläche ähnelt der von Netflix. Der Unterschied: Es sind Ihre Inhalte, auf Ihrem Server, ohne Abonnement.

Ersetzen Sie Google Drive oder Dropbox.

Synology Drive und Nextcloud verwandeln Ihr NAS in einen Dateisynchronisierungsdienst. Ein Ordner auf Ihrem Computer wird automatisch mit Ihrem NAS und all Ihren anderen Geräten synchronisiert.

Sie bearbeiten ein Dokument auf Ihrem Smartphone, und es ist sofort auf Ihrem Computer verfügbar. Genau wie bei Google Drive, nur ohne das Haus verlassen zu müssen.

Verwalten Sie Ihre Passwörter unabhängig

Vaultwarden ist eine selbstgehostete Version von Bitwarden – dem weltweit beliebtesten Open-Source-Passwortmanager. Sie installieren ihn auf Ihrem NAS und greifen wie bei der klassischen Bitwarden-App von Ihrem Smartphone und Computer aus auf alle Ihre Passwörter zu.

Der entscheidende Unterschied: Ihre Passwörter werden auf Ihrem eigenen Server gespeichert, nicht auf den Servern von Bitwarden. Sie haben die volle Kontrolle.

Synchronisieren Sie Ihren Kalender und Ihre Kontakte

Mit Nextcloud auf Ihrem NAS können Sie Ihre Kalender und Kontakte auf all Ihren Geräten synchronisieren – ohne den Umweg über Google Kalender oder iCloud.

Ihre Termine, Kontakte und Aufgabenlisten bleiben auf Ihrem Computer. Kompatibel mit den vorinstallierten Apps Ihres Smartphones und Computers.

Steuern Sie Ihr Zuhause mit Home Assistant.

Home Assistant ist die weltweit beliebteste Open-Source-Plattform für Hausautomation. Installiert auf Ihrem NAS, ermöglicht sie Ihnen die zentrale Steuerung und Automatisierung all Ihrer angeschlossenen Geräte – Lampen, Steckdosen, Thermostate, Kameras und Alarmanlagen.

Eine einzige Benutzeroberfläche zur Steuerung aller Funktionen. Kein Cloud-Abonnement. Keine Übermittlung Ihrer Hausautomatisierungsdaten an Amazon, Google oder Apple.

Hosten Sie Ihre eigene Website

Ihr NAS kann eine Website, einen Blog oder eine Webanwendung hosten. Mit Tools wie dem Nginx Proxy Manager und Docker können Sie jede beliebige Webanwendung auf Ihrem eigenen Server zu Hause bereitstellen.

Dies ist die Lösung, die von vielen Entwicklern und Kreativen gewählt wird, die ein unabhängiges und kostenloses Hosting wünschen.

Hosten Sie Ihre E-Mails selbst.

Dies ist der fortschrittlichste Anwendungsfall – und der radikalste im Hinblick auf digitale Souveränität. Mit Lösungen wie Mailcow oder Mail-in-a-Box können Sie Ihren eigenen E-Mail-Server auf Ihrem NAS hosten.

Ihre E-Mails werden nicht mehr über Server von Google, Microsoft oder Yahoo geleitet. Achtung: Dies ist die komplexeste Konfiguration in dieser Liste und richtet sich an fortgeschrittene Benutzer. Wir werden ihr in einem separaten Artikel dieser Reihe einen eigenen Beitrag widmen.

Und vieles mehr

Auf einem NAS mit Synology DSM oder Docker können Hunderte zusätzlicher Anwendungen ausgeführt werden – Download-Manager, persönlicher VPN-Server, Netzwerküberwachungstools, Überwachungs-Dashboard, privater Git-Server…

Die Möglichkeiten sind nahezu unbegrenzt. Und die Online-Community ist riesig – für jedes Bedürfnis gibt es ein ausführliches Tutorial.

Heim-NAS vs. kommerzielle Cloud

Datenschutz

Das ist der grundlegende Unterschied.

Google Drive, iCloud und OneDrive verschlüsseln Ihre Daten – doch sie besitzen die Verschlüsselungsschlüssel. Auf rechtliche Anfrage können sie auf Ihre Dateien zugreifen und diese an Dritte weitergeben. Genau das ermöglicht der US Cloud Act seit 2018: US-Behörden können Zugriff auf Daten verlangen, die von US-Unternehmen gehostet werden, unabhängig davon, in welchem Land diese gespeichert sind.

Mit einem NAS verlassen Ihre Daten niemals Ihr Zuhause. Niemand außer Ihnen hat Zugriff darauf. Es gibt keine Server von Drittanbietern, auf die Behörden zurückgreifen könnten.

Die Kosten

Kommerzielles Cloud-Computing erscheint auf den ersten Blick günstig. Doch die Abonnements summieren sich.

- Google One 2 TB: 9,99 €/Monat oder **119,88 €/Jahr**
- iCloud+ 2 TB: 9,99 €/Monat oder **119,88 €/Jahr**
- Microsoft 365 Personal: 1 TB OneDrive-Speicher für **69 €/Jahr inklusive.**

Ein Einsteiger-NAS mit zwei 2-TB-Festplatten erfordert eine Anfangsinvestition von etwa 400 bis 500 Euro. Danach beschränken sich die Kosten auf den Stromverbrauch – etwa 20 bis 30 Euro pro Jahr für ein 2-Bay-NAS im Dauerbetrieb.

Über einen Zeitraum von 5 Jahren ist der Vergleich unbestreitbar:

- Google One oder iCloud 2 TB: ~600 €
- Microsoft 365 Personal: ca. 345 € (aber auf 1 TB begrenzt)
- 2-Bay-NAS + Festplatten: Einmalige Anschaffung für 400–500 €, Speicher nach Bedarf erweiterbar

Die Kontrolle

Bei kommerziellen Cloud-Diensten sind Sie vollständig vom Wohlwollen des Anbieters abhängig. Google kann seine Nutzungsbedingungen ändern, die Preise erhöhen, einen Dienst einstellen oder Ihr Konto sperren. Dies ist bereits Tausenden von Nutzern passiert.

Mit einem NAS besitzen Sie Ihre Infrastruktur. Niemand kann die Regeln in Ihrem Namen ändern. Ihre Daten gehören Ihnen allein.

Die ehrlichen Nachteile eines Heim-NAS

Ein NAS ist nicht perfekt. Wir müssen seine Grenzen offenlegen.

Die Anfangsinvestition ist höher als ein monatliches Abonnement. Die Ersteinrichtung dauert einige Stunden – moderne Benutzeroberflächen wie Synology DSM haben den Vorgang jedoch deutlich vereinfacht. Im Falle eines Hardwareausfalls sind Sie für die Fehlerbehebung selbst verantwortlich. Und im Gegensatz zu kommerziellen Cloud-Diensten bietet ein NAS keine geografische Redundanz – deshalb empfehlen wir stets, ein NAS mit einem verschlüsselten Cloud-Dienst wie Proton Drive für die externe Datensicherung zu kombinieren.

Ein NAS ist für Menschen gedacht, die die Kontrolle über ihre Daten zurückgewinnen und bereit sind, anfangs etwas Zeit zu investieren. Es ist nicht die Lösung für diejenigen, die keinerlei Aufwand und Verantwortung übernehmen wollen.

Für wen ist es gedacht?

Ein Heim-NAS ist das Richtige für Sie, wenn:

Sie besitzen jahrelang gesammelte Familienfotos und -videos, die Sie nicht verlieren und deren Eigentum Sie behalten möchten.

Sie zahlen bereits für ein oder mehrere Cloud-Abonnements und stellen fest, dass dies teuer ist für Daten, die Ihnen eigentlich nicht gehören.

Sie sind technisch neugierig – nicht unbedingt ein Experte, aber Sie scheuen sich nicht, ein paar Stunden mit der Konfiguration eines neuen Tools zu verbringen.

Sie haben mehrere Geräte in Ihrem Haushalt – Computer, Handys, Tablets – und wünschen sich eine zentrale Lösung, um alles automatisch zu sichern.

Sie legen Wert auf Datenschutz und möchten nicht, dass Ihre Daten über die Server von Google, Apple oder Microsoft geleitet werden.

Sie möchten noch weiter gehen – Hausautomation, Service-Hosting, Selbsthosting – und suchen eine Plattform, die in der Lage ist, alles zu Hause auszuführen.

Ein NAS ist weniger geeignet, wenn:

Sie wünschen sich minimalen Aufwand und keinerlei Verantwortung. Ein NAS erfordert lediglich eine einmalige Einrichtung und minimalen Wartungsaufwand – Updates, gelegentliche Festplattenprüfungen. Wenn Sie die gesamte Datenverwaltung lieber auslagern möchten, ist die kommerzielle Cloud nach wie vor die einfachere Lösung.

Sie haben ein sehr knappes Budget. Die anfängliche Investition von 400 bis 500 € für ein NAS mit Festplatten könnte abschreckend wirken. In diesem Fall empfiehlt es sich, zunächst die 3-2-1-Regel mit einer externen Festplatte und einem Proton Drive anzuwenden und später in ein NAS zu investieren.

Sie benötigen die fortschrittlichen KI-Tools von Google Fotos – Zauberradierer, automatische Retusche –, die auf einem NAS nicht verfügbar sind.

Das typische Webology-Benutzerprofil

Wenn Sie diesen Artikel lesen, haben Sie sich wahrscheinlich schon Gedanken über Ihre digitale Unabhängigkeit gemacht. Sie wissen, dass Ihre Daten wertvoll sind. Vielleicht haben Sie bereits Proton Mail installiert oder ein VPN genutzt.

Das NAS ist der logische nächste Schritt. Es ist das zentrale Element einer persönlichen und souveränen digitalen Infrastruktur – die es Ihnen ermöglicht, die vollständige Kontrolle über Ihre Daten ein für alle Mal zurückzuerlangen.

Wo soll ich anfangen?

Schritt 1 – Auswahl Ihres NAS

Für ein erstes NAS bieten sich naturgemäß zwei Möglichkeiten an.

Die **Synology DS223** ist unsere Top-Empfehlung. Mit zwei Festplatteneinschüben, einer intuitiven DSM-Oberfläche, einem umfangreichen Anwendungsangebot und einer aktiven französischsprachigen Community ist sie das einfachste NAS für Einsteiger.

Die **QNAP TS-233** ist eine solide Alternative zu einem etwas niedrigeren Preis. Sie ist anfangs weniger intuitiv als Synology-Geräte, aber nach der Konfiguration sehr leistungsfähig.

- Synology DS223
- QNAP TS-233

Schritt 2 – Auswahl Ihrer Discs

Ein NAS benötigt spezielle Festplatten, die für den Dauerbetrieb (24/7) ausgelegt sind. Festplatten für Endverbraucher sind nicht geeignet – sie verschleißen im Dauerbetrieb viel schneller.

Die **Seagate IronWolf** und die **WD Red Plus** sind die beiden führenden NAS-Systeme auf dem Markt. Zuverlässig, leise und für intensive Nutzung bestens geeignet.

Für ein 2-Bay-NAS sollten Sie zwei identische Festplatten kaufen – so können Sie RAID 1 konfigurieren, wodurch automatisch eine Spiegelkopie Ihrer Daten erstellt wird.

- Seagate IronWolf 2 TB
- Seagate IronWolf 4 TB
- WD Red Plus 2 TB
- WD Red Plus 4 TB

Schritt 3 – Fertigstellung des Protonenantriebs

Ein NAS zu Hause schützt Ihre Daten vor Ausfällen und Ransomware. Brennt Ihr Haus jedoch ab oder wird eingebrochen, sind Ihre Daten verloren.

Deshalb empfehlen wir stets die Kombination von NAS und verschlüsselter Cloud für die externe Datensicherung – Stufe 3 der 3-2-1-Regel.

Proton Drive ist die logische Wahl: clientseitige Verschlüsselung, Schweizer Rechtsprechung, Open Source. Ihre extern gespeicherten Daten bleiben genauso privat wie die Daten auf Ihrem NAS.

- Protonenantrieb
- Proton Unlimited

Und was dann?

Sie wissen nun genau, was ein NAS ist und was es Ihnen alles bieten kann. Der nächste Schritt: Wählen Sie das passende Modell für Ihre Bedürfnisse und installieren Sie es Schritt für Schritt.

Genau darum geht es im nächsten Artikel dieser Reihe – einer vollständigen Anleitung zur Installation der Synology DS223, vom Einstieg bis zu den ersten Anwendungen.

Abschluss

Die Cloud war noch nie kostenlos. Man bezahlt monatlich in Euro dafür – und ständig mit persönlichen Daten.

Ein Heim-NAS verändert alles. Sie investieren einmal, entscheiden selbst, was Sie darauf installieren, und Ihre Daten bleiben zu Hause. Nicht auf den Servern eines US-amerikanischen Unternehmens, das dem Cloud-Computing Act unterliegt. Nicht in einem Rechenzentrum, das Sie nie zu Gesicht bekommen. Zuhause. Unter Ihrer Kontrolle.

Es ist keine perfekte Lösung – das haben wir offen zugegeben. Sie erfordert einen gewissen Zeitaufwand und eine Verantwortung, die manche Menschen nicht übernehmen wollen. Doch für diejenigen, die wirklich die Kontrolle über ihr digitales Leben zurückgewinnen möchten, ist es das wirksamste verfügbare Werkzeug.

Digitale Souveränität beginnt nicht mit einem VPN oder einem Passwortmanager. Sie beginnt mit der grundlegenden Frage: Wo befinden sich meine Daten und wer hat Zugriff darauf?

Ein NAS ist die umfassendste Antwort auf diese Frage.

Installation eines Synology NAS: Ein vollständiger Leitfaden für Anfänger

Lesezeit: 11 Minuten

Dieser Leitfaden erklärt Schritt für Schritt, wie Sie ein Synology NAS installieren – vom Einlegen der Festplatten bis zu den ersten Anwendungen.

Die Installation eines Synology NAS ist viel einfacher, als Sie vielleicht denken. Keine Kommandozeile. Keine fortgeschrittenen technischen Kenntnisse erforderlich. Nur ein Webbrowser und etwa zwanzig Minuten Zeit.

Am Ende dieses Artikels ist Ihr NAS betriebsbereit, Ihre Daten sind durch RAID 1 geschützt und Sie haben von all Ihren Geräten aus Zugriff auf Ihre Dateien und Fotos.

Wir gehen es Schritt für Schritt an.

Was Sie benötigen

Bevor Sie beginnen, vergewissern Sie sich, dass Sie alles Notwendige haben.

Die Ausrüstung:

- Ihr Synology NAS, DS223 oder ein anderes Modell.
- Zwei NAS-Festplatten – Seagate IronWolf oder WD Red Plus werden empfohlen *(siehe unseren Leitfaden).(nach Wahl)*
- Ein Ethernet-Kabel zum Verbinden des NAS mit Ihrem Router
- Ein Computer oder ein Telefon mit Webbrowser
- **Eine USV (empfohlen)** schützt Ihr NAS und Ihre Festplatten vor Stromausfällen und Überspannungen. Ein plötzlicher Stromausfall während eines Schreibvorgangs kann Ihre Daten beschädigen. Für die Ersteinrichtung nicht zwingend erforderlich, aber für den Dauerbetrieb dringend empfohlen. Wir verwenden die Eaton 3S 550 – leise, kompakt und mit USB-Schnittstelle, sodass das NAS im Falle eines Stromausfalls ordnungsgemäß herunterfährt.

Was Sie nicht benötigen:

- Tastatur oder Bildschirm – die NAS-Konfiguration erfolgt vollständig über Ihren Browser.
- Schraubendreher – das NAS lässt sich ohne Werkzeug öffnen
- Spezifische technische Fähigkeiten

Geschätzte Zeit:

- Einlegen der Discs: 5 Minuten
- DSM-Installation: 15 bis 20 Minuten
- Ersteinrichtung: 10 Minuten
- Installation der ersten Anwendungen: 15 Minuten

Insgesamt: ca. 45 Minuten bis eine Stunde für ein voll funktionsfähiges NAS.

Schritt 1 – Legen Sie die Discs ein

Das Synology NAS ist so konzipiert, dass es ohne Werkzeug geöffnet werden kann. So geht's.

Stellen Sie das NAS flach auf eine stabile Oberfläche. An der Vorderseite des Geräts befinden sich zwei übereinanderliegende Schubladen. Jede Schublade enthält eine Festplatte.

Um eine Schublade zu öffnen, drücken Sie den kleinen Riegel an der Unterseite der Schublade und ziehen Sie sie zu sich heran. Die Schublade lässt sich dann leicht herausziehen.

Legen Sie Ihre Festplatte mit den Anschlüssen nach hinten in die Schublade ein. Die Festplatte gleitet automatisch in die Schienen. Für das NAS werden keine Schrauben benötigt – die Festplatte wird einfach in die Schublade eingeklickt.

Schieben Sie die Schublade so weit hinein, bis Sie ein leises Klicken hören. Wiederholen Sie diesen Vorgang für die zweite Disc in der obersten Schublade.

Wichtigste Punkte:

- Behandeln Sie Ihre Discs mit Sorgfalt – vermeiden Sie Stöße und statische Aufladung.
- Stellen Sie sicher, dass das NAS ausgeschaltet ist, bevor Sie die Festplatten einlegen.
- Die beiden Festplatten müssen identisch sein, um RAID 1 korrekt zu konfigurieren.

Schritt 2 – Verbinden und starten

Sobald die Festplatten eingesetzt sind, kann das NAS angeschlossen werden.

Die Verbindungen:

Verbinden Sie das Ethernet-Kabel zwischen dem Netzwerkanschluss auf der Rückseite des NAS und einem freien Anschluss Ihres Internetrouters. Für die Ersteinrichtung ist eine Kabelverbindung erforderlich – WLAN wird derzeit nicht unterstützt.

Schließen Sie als Nächstes das mitgelieferte Netzkabel an die Buchse auf der Rückseite des NAS und anschließend an Ihre USV oder direkt an eine Wandsteckdose an.

Wenn Sie eine USV (unterbrechungsfreie Stromversorgung) besitzen, verbinden Sie diese zusätzlich mit dem USB-Anschluss des NAS. Dadurch kann das NAS einen Stromausfall erkennen und sich ordnungsgemäß herunterfahren, bevor der Akku leer ist.

Start-up :

Drücken Sie den Netzschalter an der Vorderseite des NAS. Die LED leuchtet orange und wechselt nach einigen Sekunden auf Grün. Sie hören, wie die Festplatten hochfahren.

Warten Sie etwa 2 Minuten, bis das System vollständig initialisiert ist. Sobald die LED dauerhaft grün leuchtet, ist das NAS betriebsbereit.

Gut zu wissen: Das Synology NAS gibt beim Start einen Piepton von sich – das ist normal. Sollten Sie wiederholte Pieptöne hören, überprüfen Sie, ob die Festplatten richtig eingesetzt sind.

Schritt 3 – DSM installieren

Warum die Installation eines Synology NAS DSM erfordert

DSM (DiskStation Manager) ist das Betriebssystem für Ihr Synology-NAS. Es ist die Weboberfläche, über die Sie Ihr gesamtes NAS verwalten.

Zugriff auf die Installationsschnittstelle:

Öffnen Sie auf Ihrem Computer, der mit demselben WLAN-Netzwerk wie Ihr NAS verbunden ist, Ihren Browser und geben Sie die folgende Adresse ein:

```
web.diskstation.me
```

Synology erkennt Ihr NAS automatisch im Netzwerk und bietet die Installation an. Klicken Sie auf **Verbinden** .

Wird das NAS nicht automatisch erkannt, können Sie auch direkt auf seine lokale IP-Adresse zugreifen. Melden Sie sich dazu an der Benutzeroberfläche Ihres Internetrouters an und suchen Sie nach verbundenen Geräten – Ihr DS223 wird mit seiner IP-Adresse (üblicherweise 192.168.1.X) in der Liste angezeigt.

DSM-Installation:

Klicken Sie auf **„Jetzt installieren“** . Synology lädt automatisch die neueste Version von DSM von seinen Servern herunter. Die Installation dauert etwa 10 Minuten.

Wichtig: Trennen Sie die Stromversorgung des NAS während der Installation nicht. Das System startet nach Abschluss der Installation automatisch neu.

Erste Verbindung:

Nach der Installation von DSM startet der Einrichtungsassistent automatisch. Sie werden aufgefordert, einen Namen für Ihr NAS zu wählen, ein Administratorkonto zu erstellen und automatische Updates zu konfigurieren.

Einige Regeln für Ihr Administratorkonto:

- Wählen Sie einen anderen Benutzernamen als „admin“ – das ist der erste, den Angreifer testen.
- Verwenden Sie ein sicheres und einzigartiges Passwort – mindestens 12 Zeichen, einschließlich Großbuchstaben, Zahlen und Sonderzeichen.
- Verwenden Sie kein bereits vorhandenes Passwort wieder.

Schritt 4 – RAID konfigurieren

Dies ist der wichtigste Schritt bei der Installation eines Synology NAS. RAID 1 verwandelt Ihre beiden Festplatten in ein automatisches Datensicherungssystem.

Was ist RAID 1?

RAID 1 erstellt eine Echtzeit-Spiegelkopie zwischen Ihren beiden Festplatten. Alles, was auf Festplatte 1 geschrieben wird, wird automatisch gleichzeitig auf Festplatte 2 kopiert.

Fällt eine Festplatte aus – und das kommt vor, selbst bei hochwertigen NAS-Festplatten –, übernimmt die andere sofort. Kein Datenverlust. Keine Betriebsunterbrechung. Sie tauschen die defekte Festplatte aus, und das RAID-System wird automatisch wiederhergestellt.

Was RAID 1 nicht ist:

RAID 1 ist kein Backup. Wenn Sie versehentlich eine Datei löschen, wird sie gleichzeitig von beiden Festplatten gelöscht. Wenn Ransomware Ihre Daten verschlüsselt, werden beide Festplatten verschlüsselt. Deshalb bleibt die 3-2-1-Regel auch bei einem NAS im RAID-1-Verbund unerlässlich.

RAID 1 auf DSM konfigurieren:

In der DSM-Oberfläche gehen Sie zu **Speichermanager** → **Speicherpool** → **Erstellen** .

Wählen Sie **SHR** (Synology Hybrid RAID) oder **RAID 1** – beide bieten gespiegelten Schutz auf zwei Festplatten. SHR ist Synologys Empfehlung für Einsteiger, da es die Speicheroptimierung automatisch verwaltet.

Wählen Sie Ihre beiden Datenträger aus und klicken Sie auf **Weiter** .

Warnung: Bei diesem Vorgang werden alle Inhalte der Datenträger unwiderruflich gelöscht. Bei neuen Datenträgern besteht kein Problem. Wenn Sie bereits vorhandene Datenträger wiederverwenden, sichern Sie deren Inhalt, bevor Sie fortfahren.

Bestätigen Sie die Poolerstellung. DSM führt eine Festplattenprüfung durch, die im Hintergrund mehrere Stunden dauern kann – Ihr NAS bleibt währenddessen nutzbar.

Sobald der Pool erstellt ist, fordert DSM Sie auf, ein **Volume** zu erstellen . Übernehmen Sie die Standardeinstellungen und klicken Sie auf **„Anwenden“** .

Schritt 5 – Sicherer Zugriff

Ihr NAS ist jetzt betriebsbereit. Bevor Sie etwas installieren, nehmen Sie sich bitte fünf Minuten Zeit, um den Zugriff ordnungsgemäß abzusichern. Ein schlecht gesichertes NAS ist ein leichtes Ziel für Angreifer.

Deaktivieren Sie das Standard-Administratorkonto

DSM erstellt während der Installation automatisch ein „Administrator“-Konto. Dies ist der erste Identifikationspunkt, den Angreifer bei einem Einbruchsversuch testen.

Gehen Sie zu **Systemsteuerung** → **Benutzer und Gruppen** . Vergewissern Sie sich, dass das während der Installation erstellte Konto zur Gruppe **„Administratoren** “ gehört . Wählen Sie anschließend das Standardkonto „Admin“ aus und deaktivieren Sie es.

Aktivieren Sie die Zwei-Faktor-Authentifizierung.

Gehen Sie zu **Systemsteuerung** → **Sicherheit** → **Konten** → **Zwei-Faktor-Authentifizierung** . Aktivieren Sie diese für alle Administratorkonten.

Sie benötigen eine Authentifizierungs-App auf Ihrem Smartphone – wir empfehlen Proton Authenticator oder Aegis (Android). Beide sind Open Source und respektieren Ihre Privatsphäre.

Automatische Blockierung aktivieren

Gehen Sie zu **Systemsteuerung → Sicherheit → Kontoschutz** . Aktivieren Sie **die automatische Sperrung** – nach einer bestimmten Anzahl fehlgeschlagener Anmeldeversuche wird die IP-Adresse automatisch gesperrt.

Empfohlene Einstellungen: Blockierung nach 5 fehlgeschlagenen Versuchen innerhalb von 5 Minuten.

Automatische DSM-Updates aktivieren

Gehen Sie zu **Systemsteuerung → Aktualisieren und Wiederherstellen → DSM-Update** . Aktivieren Sie automatische Sicherheitsupdates.

Überprüfen Sie die Firewall.

Gehen Sie zu **Systemsteuerung → Sicherheit → Firewall** . Aktivieren Sie die Firewall und überprüfen Sie, ob nur die erforderlichen Ports geöffnet sind.

Schritt 6 – Synology Drive installieren

Synology Drive verwandelt Ihr NAS in einen Dateisynchronisierungsdienst – das Äquivalent von Google Drive oder Dropbox, nur eben für zu Hause.

Installation auf dem NAS:

Öffnen Sie in DSM **das Paketzentrum** . Suchen Sie nach **Synology Drive Server** und klicken Sie auf **Installieren** .

Nach der Installation öffnen Sie Synology Drive Server über den DSM-Desktop. Der Einrichtungsassistent startet automatisch. Übernehmen Sie die Standardeinstellungen, um zu beginnen.

Installation auf Ihrem Computer:

Laden Sie **den Synology Drive Client** von der offiziellen Synology-Website herunter: https://www.synology.com/fr-fr/support/download

Wählen Sie Ihr NAS-Modell aus und anschließend **Desktop-Dienstprogramme → Synology Drive Client** . Installieren Sie die Anwendung auf Ihrem Windows- oder macOS-Computer.

Beim ersten Start fragt die Anwendung nach der Adresse Ihres NAS. Geben Sie die lokale IP-Adresse Ihres Synology NAS oder dessen Netzwerknamen ein. Melden Sie sich mit Ihren DSM-Zugangsdaten an.

Synchronisierung konfigurieren:

Wählen Sie einen Ordner auf Ihrem Computer aus, der mit dem NAS synchronisiert werden soll. Alle in diesem Ordner abgelegten Dateien werden automatisch auf Ihr NAS kopiert – und umgekehrt.

Installation auf Ihrem Telefon:

Laden Sie **Synology Drive** aus dem App Store oder Google Play Store herunter. Melden Sie sich mit der IP-Adresse und den Zugangsdaten Ihres NAS an.

Gut zu wissen: Wie Sie von außerhalb Ihres Hauses auf Ihre Dateien zugreifen können, erklären wir in einem späteren Artikel dieser Reihe.

Schritt 7 – Synology Photos installieren

Synology Photos verwandelt Ihr NAS in eine intelligente Fotogalerie – das Äquivalent zu Google Fotos, aber für zu Hause, ohne Abonnement.

Installation auf dem NAS:

Öffnen Sie in DSM **das Paketzentrum** . Suchen Sie nach **Synology Photos** und klicken Sie auf **Installieren** .

Nach der Installation öffnen Sie Synology Photos über den DSM-Desktop. Die Anwendung erstellt automatisch einen **Fotos-** Ordner in Ihrem Speicherplatz.

Erstkonfiguration:

Bei der ersten Installation bietet Synology Photos zwei Modi:

- **Persönlicher Ordner** – jeder Benutzer hat seinen eigenen privaten Fotobereich
- **Gemeinsamer Bereich** – die ganze Familie hat Zugriff auf dieselben Alben.

Automatische Datensicherung vom Telefon aktivieren:

Laden Sie **Synology Photos** aus dem App Store oder Google Play Store herunter. Melden Sie sich mit der IP-Adresse Ihres NAS und Ihren DSM-Anmeldedaten an.

In der mobilen App gehen Sie zu **Einstellungen → Automatische Sicherung** und aktivieren Sie diese Funktion. Wählen Sie aus, ob die Sicherung nur über WLAN erfolgen soll – dies wird empfohlen, um Ihr mobiles Datenvolumen zu schonen.

Ab sofort wird jedes mit Ihrem Smartphone aufgenommene Foto automatisch auf Ihr NAS kopiert. Sie müssen nichts weiter tun. Kein Abonnement erforderlich. Ihre Erinnerungen bleiben bei Ihnen.

Gesichtserkennung:

Synology Fotos bietet eine Gesichtserkennung, die Fotos automatisch nach Personen gruppiert. Um diese Funktion zu aktivieren, gehen Sie zu **Einstellungen → Personenerkennung** .

Die Verarbeitung erfolgt vollständig auf Ihrem NAS – Ihre Fotos werden niemals zur Analyse an einen externen Server gesendet.

Abschluss

Herzlichen Glückwunsch – Ihr Synology NAS ist jetzt betriebsbereit.

In nur einer Stunde haben Sie Ihr Synology NAS installiert und die Kontrolle über Ihre Daten zurückgewonnen. Ihre Dateien werden automatisch synchronisiert. Ihre Fotos werden ohne Abonnement gesichert. Ihre beiden Festplatten schützen sich gegenseitig im RAID-1-Verbund. Und all das läuft rund um die Uhr zu Hause, ohne dass Sie sich darum kümmern müssen.

Das ist erst der Anfang. Ihr NAS ist eine Plattform – Sie haben gerade erst den Grundstein gelegt. Die nächsten Artikel dieser Reihe zeigen Ihnen, wie Sie noch mehr erreichen: Greifen Sie von überall auf der Welt auf Ihre Dateien zu, hosten Sie Ihre Fotos mit Immich, steuern Sie Ihre Hausautomation mit Home Assistant und verwalten Sie Ihre Passwörter mit Vaultwarden (einer selbstgehosteten Version von Bitwarden).

Stein für Stein. In Ihrem eigenen Tempo.

Greifen Sie von überall auf Ihr Synology NAS zu.

Der Fernzugriff auf Ihr Synology NAS von Ihrem Smartphone oder Computer aus ist einfacher als Sie vielleicht denken. Es gibt drei Möglichkeiten – mit sehr unterschiedlichem Sicherheitsniveau, Komplexitätsgrad und Souveränitätsanspruch.

Dieser Leitfaden erklärt, welche man auswählen sollte und wie man sie konfiguriert.

Bevor wir beginnen: das Risiko eines schlecht belichteten NAS

Wenn Sie Ihr NAS mit dem Internet verbinden, ist das, als würden Sie die Tür zu Ihrem digitalen Zuhause offen lassen. Ist diese Tür nicht richtig verschlossen, kann jeder anklopfen – und manche wissen, wie man das Schloss knackt.

Synology NAS-Geräte sind regelmäßig Ziel automatisierter Angriffe. Bots durchsuchen permanent das Internet nach ungeschützten NAS-Geräten, um Brute-Force-Angriffe durchzuführen, Ransomware zu installieren oder Dateien zu stehlen. Dies ist keine theoretische Bedrohung: In den letzten Jahren wurden massive Angriffskampagnen gegen Synology NAS-Geräte dokumentiert.

Die gute Nachricht: Ein korrekt konfigurierter Fernzugriff ist absolut sicher. Die drei in diesem Artikel vorgestellten Methoden sind alle gültig – vorausgesetzt, Sie befolgen die jeweiligen Sicherheitsregeln.

Die drei Methoden im Überblick

	QuickConnect	Schwanzschuppe	OpenVPN
Schwierigkeit	Einfach	Mäßig	Fortschrittlich
Sicherheit	Korrekt, wenn richtig	Gut	Exzellent

	konfiguriert		
Drittanbieterabhängigkeit	Synology-Server	Tailscale-Server	Keiner
Hafen wird geöffnet	NEIN	NEIN	Ja
Geschwindigkeit	Begrenzt (Staffel)	Optimal	Optimal
Frei		persönlicher Gebrauch	
Für wen	Anfänger	Die Mehrheit	Erweiterte Profile

Methode 1 – QuickConnect: die einfachste

Was es ist

QuickConnect ist der offizielle Fernzugriffsdienst von Synology. Er ermöglicht Ihnen den Zugriff auf Ihr NAS von überall aus mit einem personalisierten Login, ohne die Netzwerkeinstellungen Ihres Routers ändern zu müssen.

In der Praxis: Sie geben die Adresse `quickconnect.to/votre-identifiant` in einen Browser ein und greifen auf die DSM-Oberfläche Ihres NAS zu. Einfach, kostenlos, funktional.

Wie man es aktiviert

1. In DSM gehen Sie zu **Systemsteuerung → QuickConnect**
2. Aktivieren Sie **QuickConnect.**
3. Melden Sie sich mit Ihrem Synology-Konto an (erstellen Sie gegebenenfalls eines).
4. Wählen Sie Ihre QuickConnect-ID (z. B. `monnas-famille`)
5. Klicken Sie auf **„Anwenden“.**

Das war's. Ihr NAS ist jetzt von außen zugänglich.

Grenzen, die zu beachten sind

Relay-Durchsatz. Wenn eine direkte Verbindung nicht möglich ist (Router mit komplexem NAT oder CGNAT), wird der Datenverkehr im Relay-Modus über Synology-Server geleitet. Der Durchsatz ist dann auf ca. 1–2 Mbit/s begrenzt – ausreichend zum Durchsuchen von Dateien, aber nicht ausreichend für das Streamen von 4K-Videos.

Abhängigkeit von Synology-Servern. Wenn die QuickConnect-Server gewartet werden oder offline sind, verlieren Sie den Zugriff. Das kommt zwar selten vor, ist aber möglich.

Öffentliche Offenlegung. Ihre QuickConnect-ID ist über das Internet zugänglich. Ein Angreifer, der Ihre ID kennt, kann auf die Anmeldeseite Ihres NAS zugreifen. Deshalb ist Sicherheit unerlässlich.

Obligatorische Sicherheit

QuickConnect ohne diese Einstellungen ist wie eine halb geöffnete Tür:

1. Zwei-Faktor-Authentifizierung aktiviert: Systemsteuerung → Sicherheit → Konto → 2FA für alle Administratoren aktivieren.

2. Automatische Sperrung aktiviert: Systemsteuerung → Sicherheit → Kontoschutz → Sperrung nach 5 fehlgeschlagenen Versuchen innerhalb von 5 Minuten.

3. Beschränken Sie den Zugriff auf Apps über QuickConnect. Aktivieren Sie in den erweiterten QuickConnect-Einstellungen nur die Apps, die Sie tatsächlich nutzen (Drive, Fotos, DSM). Deaktivieren Sie alle anderen.

4. Standard-Administratorkonto deaktiviert. Überprüfen Sie, ob das generische „Administrator"-Konto tatsächlich deaktiviert ist (siehe unsere Installationsanleitung).

Für wen

QuickConnect eignet sich ideal für gelegentliche Nutzung: zum Beispiel zum Ansehen einer Datei unterwegs, zum Abrufen von Fotos von einem anderen Gerät oder zum Überprüfen des Status Ihres NAS. Wenn Sie regelmäßig große Datenmengen übertragen müssen, fahren Sie mit Methode 2 fort.

Methode 2 – Tailscale: die empfohlene Methode (Webologie-Empfehlung)

Was es ist

Tailscale ist ein modernes Mesh-VPN auf Basis von WireGuard. Es erstellt ein verschlüsseltes privates Netzwerk zwischen all Ihren Geräten – als wären sie alle mit demselben lokalen Netzwerk verbunden, egal wo auf der Welt Sie sich befinden. Es ist die schnellste Möglichkeit, Fernzugriff auf Ihr Synology NAS einzurichten, ohne Ihren Router ändern zu müssen.

Im Gegensatz zu QuickConnect leitet Tailscale Ihre Daten nicht über Zwischenserver. Die Verbindung ist direkt, Ende-zu-Ende-verschlüsselt und erfordert keine Portweiterleitung auf Ihrem Router. Sie funktioniert sogar hinter CGNAT – der Netzwerkkonfiguration, die viele Internetanbieter heutzutage verwenden.

Kostenlos für den persönlichen Gebrauch auf bis zu 100 Geräten.

Laden Sie Tailscale von der offiziellen Website herunter: tailscale.com/download

Warum dies unsere Empfehlung ist

- Ihr NAS sollte nicht öffentlich im Internet angezeigt werden.
- Direkte verschlüsselte Verbindung zwischen Ihren Geräten
- Es müssen keine Ports an Ihrem Router geöffnet werden.
- Installation in weniger als 10 Minuten von DSM
- Funktioniert auf all Ihren Geräten: Mac, Windows, iPhone, Android

So installieren Sie es auf Ihrem NAS

Auf dem NAS:

1. Öffnen Sie in DSM das **Paketzentrum .**
2. Suchen Sie nach **Tailscale** und klicken Sie auf **Installieren.**
3. Nach der Installation öffnen Sie Tailscale über den DSM-Desktop.

4. Klicken Sie auf **Anmelden** – eine URL wird angezeigt.
5. Kopieren Sie diese URL in Ihren Browser und authentifizieren Sie sich anschließend mit Ihrem Tailscale-Konto (Google, Microsoft oder GitHub).
6. Ihr NAS wird in Ihrem Tailscale-Dashboard mit einer privaten IP-Adresse angezeigt (z. B. `100.64.x.x`) .

Auf Ihren Geräten:

Laden Sie Tailscale auf jedem Gerät herunter, von dem aus Sie auf Ihr NAS zugreifen möchten:

- **iPhone/iPad** : App Store → Tailscale
- **Android** : Play Store → Tailscale
- **Mac/Windows** : tailscale.com/download

Melden Sie sich auf all Ihren Geräten mit demselben Konto an. Diese werden automatisch Ihrem privaten Netzwerk hinzugefügt.

Greifen Sie auf Ihr NAS zu:

Sobald Tailscale auf Ihrem Smartphone aktiviert ist, öffnen Sie einen Browser und geben Sie die IP-Adresse Ihres NAS-Systems (Tailscale) ein (diese wird im Tailscale-Dashboard angezeigt). Anschließend haben Sie direkten Zugriff auf DSM, genau wie zu Hause.

Eine Anmerkung zur Souveränität

Tailscale koordiniert Verbindungen über seine Server – Ihre Daten laufen jedoch nicht über diese. Die Verbindung zwischen Ihren Geräten erfolgt direkt. Dies ist ein sinnvoller Kompromiss zwischen Einfachheit und Datensouveränität.

Wenn Sie vollständige Souveränität benötigen, gibt es **Headscale** , eine selbstgehostete Version des Tailscale-Koordinierungsservers. Dies ist eine Option für fortgeschrittene Benutzer und wird in diesem Artikel nicht weiter behandelt.

Methode 3 – OpenVPN VPN: Totale Souveränität

Was es ist

OpenVPN ist über das **VPN-Server** -Paket nativ in DSM integriert . Sie betreiben Ihren eigenen VPN-Server auf Ihrem NAS. Es besteht keine Abhängigkeit von einem Drittanbieterdienst – Ihre Verbindungen laufen direkt über Ihr eigenes Netzwerk.

Dies ist die souveränste Methode. Sie ist aber auch die am komplexesten zu konfigurierende.

Installieren Sie **OpenVPN Connect** von openvpn.net

Was Sie vor Beginn benötigen

- Eine **statische IP-Adresse** von Ihrem Internetdienstanbieter oder ein **DDNS-Dienst** (Synology bietet einen kostenlosen an).
- Die Möglichkeit, einen Port an Ihrem Router zu öffnen (standardmäßig UDP-Port 1194).
- Ein gewisses Maß an Vertrautheit mit der Netzwerkkonfiguration

So konfigurieren Sie OpenVPN auf DSM

1. VPN-Server installieren

Suchen Sie im DSM-Paketcenter nach **„VPN-Server“** und installieren Sie ihn. Es handelt sich um ein offizielles Synology-Paket, das kostenlos ist.

2. Konfigurieren Sie den OpenVPN-Server

OpenVPN-Server → OpenVPN. **Aktivieren Sie den OpenVPN-Server** .

Empfohlene Einstellungen:

- Port: 1194 (UDP)
- Aktivieren Sie die Option **„Clients den Zugriff auf das LAN des Servers erlauben** “ – dies ist unerlässlich für den Zugriff auf Ihre Dateien.
- Protokoll: UDP (schneller als TCP)

Klicken Sie auf **„Anwenden“** und anschließend **auf „Konfiguration exportieren“** – Sie erhalten eine Datei `.ovpn` , die Sie auf Ihre Clientgeräte übertragen können.

3. DDNS konfigurieren (falls keine statische IP-Adresse vorhanden ist)

Systemsteuerung → Externer Zugriff → DDNS → Hinzufügen. Synology bietet einen eigenen kostenlosen DDNS-Dienst an (z. B. .synology.org `monnas.synology.me`). Aktivieren Sie ihn und notieren Sie sich Ihre Adresse.

4. Öffnen Sie den Port an Ihrem Router.

Konfigurieren Sie in der Benutzeroberfläche Ihres Internet-Routers eine Portweiterleitungsregel für UDP-Port 1194 zur lokalen IP-Adresse Ihres NAS. Die Vorgehensweise variiert je nach Internetanbieter – konsultieren Sie die Dokumentation Ihres Routers.

5. Clients konfigurieren

Auf jedem Gerät, von dem aus Sie eine Verbindung herstellen möchten:

- Installieren Sie den **OpenVPN Connect-** Client (iOS, Android, macOS, Windows).
- Importieren Sie die exportierte Datei `.ovpn` aus DSM.
- Geben Sie Ihre DSM-ID und Ihr Passwort ein.
- Einloggen

Eine Erwähnung auf WireGuard

WireGuard ist ein moderneres und schnelleres VPN-Protokoll als OpenVPN. Es wird von DSM nicht nativ unterstützt und erfordert die Installation eines Drittanbieterpakets via SSH. Wenn Sie mit der Kommandozeile vertraut sind, ist es eine hervorragende Option – geht aber über den Rahmen dieser Einsteigeranleitung hinaus.

Für wen

OpenVPN eignet sich für Nutzer, die jegliche Abhängigkeit von Drittanbietern ablehnen und die volle Kontrolle über ihre Infrastruktur behalten möchten. Es ist die Methode, die am besten mit der von Webologie vertretenen Philosophie der digitalen Souveränität übereinstimmt.

Die Sicherheitsregeln, die allen drei Methoden gemeinsam sind

Unabhängig von der gewählten Methode gelten diese Regeln stets:

Die Zwei-Faktor-Authentifizierung ist für alle Administratorkonten aktiviert. Dies ist die wichtigste Sicherheitsmaßnahme. Ein Passwort allein reicht nicht aus.

Automatische DSM-Updates sind aktiviert. Sicherheitslücken auf Synology NAS-Geräten werden regelmäßig behoben – Sie müssen die Updates aber trotzdem manuell installieren. Systemsteuerung → Aktualisieren und Wiederherstellen → Automatische Sicherheitsupdates aktivieren.

DSM-Firewall aktiviert. Systemsteuerung → Sicherheit → Firewall → Aktiviert.

Automatische Sperrung aktiviert. Nach 5 fehlgeschlagenen Verbindungsversuchen wird die IP-Adresse automatisch gesperrt.

Das Standard-Administratorkonto ist deaktiviert. Dies ist der erste Anmeldeversuch, der von Angreifern getestet wird.

Diese fünf Punkte werden bereits in unserer Synology NAS-Installationsanleitung behandelt . Wenn Sie diese Schritte bei der Installation befolgt haben, müssen Sie nichts weiter tun.

Welche Methode sollte ich wählen?

Wenn Sie Ihr NAS gerade erst installiert haben und problemlos von Ihrem Telefon darauf zugreifen möchten: **QuickConnect** , mit den oben genannten Sicherheitsregeln.

Wenn Sie Ihr NAS regelmäßig nutzen, große Dateien übertragen oder Wert auf Datenschutz legen: **Tailscale** . Es ist unsere Empfehlung für die große Mehrheit der Webologie-Nutzer.

Wenn Sie jegliche Abhängigkeit von einem Drittanbieterdienst ablehnen und mit der Netzwerkkonfiguration vertraut sind: **OpenVPN** wird auf Ihrem NAS gehostet.

Alle drei Methoden können parallel genutzt werden. Viele Anwender verwenden QuickConnect für den schnellen Zugriff auf DSM und Tailscale für die Übertragung großer Dateien.

Abschluss

Ihr NAS ist jetzt von überall auf der Welt sicher zugänglich.

Das ist das Versprechen von Self-Hosting: Ihre Daten bleiben bei Ihnen, unter Ihrer Kontrolle und jederzeit zugänglich. Kein Cloud-Abonnement. Sie müssen Ihre Dateien nicht Google, Apple oder Dropbox anvertrauen.

Regel 3-2-1: Die einfache Methode, um Ihre Daten niemals zu verlieren

Lesezeit: 9 Minuten

Einführung

Die Datensicherung ist die am meisten vernachlässigte – und gleichzeitig wichtigste – Form des digitalen Schutzes.

Sie haben wahrscheinlich Hunderte von Familienfotos auf Ihrem Handy. Wichtige Dokumente auf Ihrem Computer. Digitale Erinnerungen, die sich über Jahre angesammelt haben.

Und höchstwahrscheinlich existiert all dies nur an einem einzigen Ort.

Diesen Fehler machen 90 % der Menschen. Nicht aus Nachlässigkeit, sondern aus Unwissenheit. Wir reden uns ein, dass so etwas nur anderen passiert. Bis zu dem Tag, an dem die Festplatte ausfällt, das Handy ins Wasser fällt oder Ransomware in Sekundenschnelle alles verschlüsselt.

Dann ist es zu spät.

Die gute Nachricht: Es gibt eine einfache, bewährte Methode, die IT-Experten seit Jahrzehnten anwenden. Sie heißt 3-2-1-Datensicherung. Dafür sind keine besonderen technischen Kenntnisse erforderlich. Und sie lässt sich dieses Wochenende für unter 100 € einrichten.

Dieser Artikel erklärt, wie Sie Ihre Daten dauerhaft schützen können – und gibt Ihnen die konkreten Werkzeuge dafür an die Hand.

Was besagt die 3-2-1-Regel?

Die 3-2-1-Regel ist ein Naturschutzprinzip, das in den 2000er Jahren von dem Fotografen Peter Krogh formuliert wurde. Einfach zu merken, bemerkenswert effektiv:

- **3** Kopien Ihrer Daten
- **2** verschiedene Speichermedien
- **1** externe Kopie

In der Praxis sieht das für einen normalen Benutzer folgendermaßen aus:

- **Kopie 1** – Ihre Originaldaten auf Ihrem Computer oder Telefon
- **Kopie 2** – eine Sicherungskopie auf einer externen Festplatte zu Hause
- **Kopie 3** – eine Sicherungskopie in der Cloud oder bei einem Verwandten

Die Idee hinter dieser Regel ist einfach: Keine Katastrophe kann drei Kopien zerstören, die auf zwei verschiedenen Datenträgern an zwei verschiedenen Orten gespeichert sind.

Wenn Ihr Computer abstürzt, haben Sie die externe Festplatte und die Cloud. Wenn Ihr Haus abbrennt oder eingebrochen wird, haben Sie die Cloud. Wenn Ihre Cloud kompromittiert wird, haben Sie beide lokalen Kopien.

Es handelt sich um ein dreistufiges Sicherheitsnetz. Jede Stufe schützt vor einer anderen Bedrohung.

Warum es unerlässlich ist

Wir neigen dazu zu glauben, dass der Verlust unserer Daten selten vorkommt. Die Zahlen sprechen eine andere Sprache.

Hardwareausfälle

Eine mechanische Festplatte hat eine durchschnittliche Lebensdauer von 3 bis 5 Jahren. Laut Studien von Backblaze – einem Cloud-Speicheranbieter, der seine Zuverlässigkeitsdaten jährlich veröffentlicht – fallen jährlich etwa 5 % der Festplatten aus. Über einen Zeitraum von 5 Jahren entspricht das fast dem Ausfall jeder vierten Festplatte.

Anders als man vielleicht vermuten würde, kündigt sich ein Festplattenausfall nicht immer an. In den meisten Fällen funktioniert die Festplatte normal, bis sie plötzlich nicht mehr reagiert.

Ransomware

Ransomware ist Schadsoftware, die all Ihre Dateien verschlüsselt und ein Lösegeld für deren Wiederherstellung fordert. Sie stellt längst keine Bedrohung mehr dar, die nur Unternehmen betrifft.

Laut einem Bericht von CrowdStrike werden Ransomware-Angriffe auf Privatpersonen bis 2025 um 62 % zunehmen. Der häufigste Einstiegspunkt sind nach wie vor E-Mails mit schädlichen Anhängen oder Links – ein Fehler, der jedem unterlaufen kann.

Wenn Sie kein Offline-Backup haben, bleiben Ihnen zwei Möglichkeiten: Entweder Sie zahlen das Lösegeld – ohne Garantie auf die Wiederherstellung Ihrer Daten – oder Sie verlieren alles.

Versehentliches Löschen

Dies ist die häufigste und am meisten unterschätzte Ursache für Datenverlust: ein falscher Klick, ein misslungenes Update, eine unbeabsichtigte Formatierung. Laut einer Ontrack-Studie aus dem Jahr 2024 sind 26 % aller Datenverluste auf menschliches Versagen zurückzuführen.

Diebstahl und Naturkatastrophen

Ein Laptop wird im Café gestohlen. Eine Wohnung brennt. Es kommt zu einer Überschwemmung. Solche Szenarien kommen vor. Befinden sich Ihre Daten nur zu Hause, sind sie mit dem Ereignis verloren.

So richten Sie Ihr 3-2-1-Backup ein

Ebene 1 – Die lokale Kopie: die externe Festplatte

Das ist der Ausgangspunkt. Eine externe Festplatte, die über USB mit Ihrem Computer verbunden ist und auf die Sie regelmäßig Ihre wichtigen Daten kopieren.

Dies ist die schnellste und günstigste Backup-Lösung. Eine externe 1-TB-Festplatte kostet zwischen 50 und 80 Euro und ist für die meisten Nutzer mehr als ausreichend.

Zwei wichtige Punkte:

Manuelle Backups sind in der Regel unzuverlässig. Menschen vergessen Dinge. Daher ist Automatisierung unerlässlich. Unter Windows eignet sich dafür der integrierte Dateiversionsverlauf. Unter macOS ist Time Machine die ideale Lösung. Beide Programme sind kostenlos und bereits auf Ihrem Rechner installiert.

Zweitens muss die externe Festplatte getrennt bleiben, wenn keine Datensicherung durchgeführt wird. Ransomware, die Ihren Computer infiziert, verschlüsselt auch angeschlossene Laufwerke. Eine getrennte Festplatte ist geschützt.

Empfohlene Ausrüstung:

- Seagate Expansion 1 TB – zuverlässig, kompakt, erschwinglich
- WD My Passport 2 TB – ideal für alle, die viele Fotos und Videos haben.

Stufe 2 – Das NAS: Automatische Datensicherung zu Hause

Ein NAS (Network Attached Storage) ist ein kleiner Speicherserver, der mit Ihrem Internetrouter verbunden ist. Er ist von all Ihren Geräten – Computer, Smartphone, Tablet – über WLAN zugänglich, ohne dass ein Kabel angeschlossen werden muss.

Dies ist das zweite Speichermedium für Ihre 3-2-1-Regel. Und es ist das Herzstück der Artikelserie, die wir auf Webologie veröffentlichen – im nächsten Artikel widmen wir ihr eine ausführliche Anleitung.

Merken Sie sich zunächst das Wichtigste: Ein NAS mit zwei Festplatten im RAID-1-Verbund erstellt automatisch eine Spiegelkopie Ihrer Daten. Fällt eine Festplatte aus, übernimmt die andere ohne Datenverlust.

Synology und QNAP dominieren den Markt für NAS-Systeme für Endverbraucher. Sie sind zuverlässig, gut dokumentiert und verfügen über einfache Benutzeroberflächen.

Empfohlene Ausrüstung:

- Synology DS223 – ideal für Einsteiger, 2 Festplatteneinschübe, einfache Benutzeroberfläche
- QNAP TS-233 – eine gute Alternative, ausgezeichnetes Preis-Leistungs-Verhältnis

Informationen zu kompatiblen Festplatten für Ihr NAS finden Sie in unseren Empfehlungen im Abschnitt „Welche Hardware wählen?“ weiter unten.

Stufe 3 – Die verschlüsselte Cloud: Externes Kopieren

Dies ist die wichtigste Stufe für Ihre Sicherheit. Eine Kopie Ihrer Daten wird extern gespeichert und ist von überall aus zugänglich.

Aber Vorsicht: Nicht alle Cloud-Dienste sind in puncto Datenschutz gleich.

Google Drive und OneDrive verschlüsseln Ihre Dateien – die Verschlüsselungsschlüssel liegen jedoch in ihrem Besitz. Auf rechtliche Anfrage können sie auf Ihre Daten zugreifen und diese an Dritte weitergeben, ohne Sie unbedingt darüber zu informieren.

Proton Drive funktioniert anders, wie wir in unserem Vergleich von Google Drive, OneDrive und Proton Drive ausführlich erläutern . Die Verschlüsselung erfolgt clientseitig: Ihre Dateien werden auf Ihrem Gerät verschlüsselt, bevor sie an die Server gesendet werden. Selbst Proton kann Ihre Dateien nicht lesen. Es unterliegt Schweizer Recht, ist Open Source und wird unabhängig geprüft.

Für eine datenschutzfreundliche 3-2-1-Datensicherung ist Proton Drive die logische Wahl.

→ Erste Schritte mit dem Protonenantrieb

Welche Ausrüstung auswählen?

Externe Festplatten

Für eine erste lokale Datensicherung stechen zwei Optionen deutlich hervor.

Die **Seagate Expansion** ist eine zuverlässige Wahl. Kompakt, zuverlässig und mit Speicherkapazitäten von 1 TB bis 4 TB erhältlich, benötigt sie kein externes Netzteil – ein einziges USB-Kabel genügt. Ideal zum Sichern von Dokumenten, Fotos und Musik.

Die **WD My Passport** ist etwas hochwertiger. Ihr Hauptvorteil: Sie beinhaltet eine automatische Backup-Software und bietet Hardware-Verschlüsselung mit Passwortschutz. Empfehlenswert, wenn Sie Ihre Festplatte regelmäßig transportieren.

Für die meisten Nutzer ist 1 TB ausreichend. Wer eine große Sammlung an Videos oder hochauflösenden Fotos besitzt, sollte sich gleich für 2 TB entscheiden.

- Seagate Expansion 1 TB
- Seagate Expansion 2 TB
- WD My Passport 1 TB
- WD My Passport 2 TB

NAS

Ein NAS ist zwar eine größere Investition, aber die umfassendste Lösung für die automatisierte Datensicherung zu Hause.

Die **Synology DS223** ist unsere Top-Empfehlung für Einsteiger. Sie verfügt über zwei Festplatteneinschübe, eine intuitive DSM-Benutzeroberfläche und die Synology Drive Mobile App für den Zugriff auf Ihre Dateien per Smartphone. Sie ist kompatibel mit Seagate IronWolf- und WD Red-Festplatten, die speziell für den Dauerbetrieb in einem NAS entwickelt wurden.

Die **QNAP TS-233** ist eine solide Alternative zu einem etwas niedrigeren Preis. Ihre Benutzeroberfläche ist etwas weniger intuitiv als die von Synology, aber ihre Funktionen sind für den normalen Heimgebrauch vergleichbar.

Wählen Sie für die Festplatten in Ihrem NAS NAS-spezifische Modelle. Die **Seagate IronWolf** und die **WD Red Plus** sind für den Dauerbetrieb ausgelegt. Sie sind vibrationsfest und haben eine längere Lebensdauer als herkömmliche Festplatten für Endverbraucher.

- Synology DS223
- QNAP TS-233
- Seagate IronWolf 2 TB
- Seagate IronWolf 4 TB
- WD Red Plus 2 TB
- WD Red Plus 4 TB

Die verschlüsselte Wolke

Für das Kopieren außerhalb des Standorts bietet Proton Drive verschiedene Optionen an.

Der **Proton Free** -Tarif beinhaltet 1 GB Speicherplatz – ausreichend für wichtige Dokumente, aber nicht für Fotos.

Der Proton Drive- Tarif für 3,99 €/Monat bietet 200 GB Speicherplatz – ausreichend für die Mehrheit der Nutzer, die Dokumente, wichtige Fotos und Arbeitsdateien sichern möchten.

Der Proton Unlimited -Tarif für 9,99 €/Monat umfasst 500 GB Speicherplatz und Zugriff auf die gesamte Proton-Suite: Mail, VPN, Pass und Kalender. Er ist die umfassendste Lösung, wenn Sie Ihre digitale Privatsphäre zentral verwalten möchten.

Aktuell bietet Proton Drive einen Rabatt von 40% auf Jahresabonnements an.

- Protonenantrieb
- Proton Unlimited

Wo soll ich heute Abend anfangen?

Schritt 1 — Heute Abend (kostenlos, 30 Minuten)

Beginnen Sie damit, festzustellen, was Sie sich nicht leisten können zu verlieren.

Familienfotos. Verwaltungsunterlagen. Berufliche Projekte. Kontakte. Machen Sie sich eine mentale Liste.

Aktivieren Sie als Nächstes die automatische Datensicherung auf Ihrem Smartphone, falls noch nicht geschehen. Auf dem iPhone finden Sie diese Option in iCloud – gehen Sie zu „Einstellungen“ → Ihr Name → „iCloud“ → „iCloud-Backup“. Auf Android-Geräten ist es Google Fotos oder Google One – stellen Sie sicher, dass die automatische Synchronisierung aktiviert ist.

Dies ist keine endgültige Lösung – es handelt sich um die Cloud von Apple oder Google, daher gibt es keine clientseitige Verschlüsselung. Aber es ist besser als nichts, während Sie auf die Einrichtung Ihres ordnungsgemäßen 3-2-1-Backups warten.

Schritt 2 — Dieses Wochenende (50 € bis 80 €, 1 Stunde)

Kaufen Sie eine externe Festplatte und konfigurieren Sie die automatische Datensicherung.

Unter Windows: Schließen Sie Ihr externes Laufwerk an, gehen Sie zu Einstellungen → Update und Sicherheit → Sicherung → Laufwerk hinzufügen. Der Dateiversionsverlauf erledigt den Rest.

Unter macOS: Schließen Sie Ihr externes Laufwerk an. macOS bietet Ihnen automatisch an, es mit Time Machine zu verwenden. Bestätigen Sie. Time Machine erstellt dann stündlich im Hintergrund ein Backup, ohne dass Sie sich darum kümmern müssen.

Trennen Sie das Laufwerk zwischen den Datensicherungen und bewahren Sie es in einer Schublade auf.

Sie haben nun zwei Kopien Ihrer Daten auf zwei verschiedenen Speichermedien. Das ist schon viel besser als die Ausgangssituation.

Schritt 3 — Innerhalb des Monats (ab 3,99 €/Monat)

Mit Proton Drive können Sie auch extern kopieren.

Installieren Sie die Proton Drive-App auf Ihrem Computer und Smartphone. Richten Sie die automatische Synchronisierung Ihrer wichtigsten Ordner ein – Dokumente, Fotos, Desktop.

Ihre Daten werden nun clientseitig verschlüsselt, in der Schweiz gespeichert und sind von jedem Gerät aus zugänglich. Selbst im Falle von Diebstahl, Brand oder einem kompletten Systemausfall bei Ihnen zu Hause sind alle Daten wiederherstellbar.

→ Erste Schritte mit dem Protonenantrieb

Und was dann?

Wenn Sie noch einen Schritt weiter gehen möchten – beispielsweise die automatische Datensicherung all Ihrer Geräte zu Hause, den Zugriff auf Ihre Dateien von überall ohne Abhängigkeit von einer Cloud eines Drittanbieters oder das Hosting eigener Dienste – dann ist NAS der nächste Schritt.

Genau darum geht es im nächsten Artikel dieser Reihe.

Abschluss

Datenverlust ist kein Pech. Er ist eine Frage der Vorbereitung.

Eine Festplatte fällt aus. Ein Handy geht kaputt. Ransomware schlägt zu. Solche Dinge passieren – gar nicht so selten, wie man vielleicht denkt. Der einzige Unterschied zwischen denen, die sich innerhalb von Minuten erholen, und denen, die jahrelange Erinnerungen und Arbeit verlieren, ist das Vorhandensein oder Fehlen eines Backups.

Die 3-2-1-Regel ist nicht nur etwas für Experten. Es ist eine einfache, bewährte Methode, die jeder anwenden kann. Drei Kopien: zwei physische Kopien und eine digitale Kopie. Sie können noch heute Abend mit dem beginnen, was Sie bereits haben.

Sie entscheiden selbst, welchen Schutz Sie wählen. Eine externe Festplatte für 60 € ist immer noch deutlich besser als gar keine. Ein NAS mit Proton Drive ist die Komplettlösung für alle, die die volle Kontrolle über ihre Daten zurückgewinnen möchten.

In jedem Fall war der beste Zeitpunkt für die Einrichtung eines Backups vor einem Jahr. Der zweitbeste Zeitpunkt ist jetzt.

Physischer Sicherheitsschlüssel: Der ultimative Schutz vor Kontodiebstahl

Geschätzte Lesezeit: 12 Minuten

Letzte Aktualisierung: März 2026

Ein Datenleck. Eine abgefangene SMS. Ein Google-Konto, das innerhalb von 48 Stunden leergeräumt wurde.

Dieses Szenario passiert täglich Tausenden von Menschen, die sich durch die aktivierte Zwei-Faktor-Authentifizierung (2FA) geschützt wähnten. Das Problem? Nicht alle 2FA-Methoden sind gleich sicher. Manche lassen sich sogar umgehen, ohne dass man es merkt.

Es gibt eine Lösung, die Hacker aus der Ferne nicht stehlen können, selbst wenn sie Ihr Passwort kennen, selbst wenn sie Ihre Telefonnummer kontrollieren: den **physischen Sicherheitsschlüssel** .

In diesem Leitfaden erfahren Sie, warum Ihre aktuelle Zwei-Faktor-Authentifizierung möglicherweise Schwächen aufweist, wie ein physischer Schlüssel funktioniert und welchen Sie entsprechend Ihrem Profil auswählen sollten.

Teil 1 – Warum Ihre aktuelle Zwei-Faktor-Authentifizierung nicht ausreicht

SMS: die am häufigsten genutzte… und riskanteste Methode

Wenn Ihnen eine Website einen Code per SMS zur Bestätigung Ihrer Verbindung sendet, wirkt das sicher. Tatsächlich weist dieses System jedoch zwei gravierende Schwächen auf.

SIM-Swapping : Ein Krimineller kontaktiert Ihren Mobilfunkanbieter, gibt sich als Sie aus und beantragt die Übertragung Ihrer Rufnummer auf eine neue, von ihm kontrollierte SIM-Karte. Dadurch landen alle Ihre SMS und Ihr Zwei-Faktor-Authentifizierungscode bei ihm. [Ich habe

dem Thema SIM-Swapping einen eigenen Artikel gewidmet, falls Sie mehr darüber erfahren möchten.]

SS7-Abfangen : Das globale Telefonnetz basiert auf einem 40 Jahre alten Protokoll (SS7), das mit den entsprechenden Werkzeugen das Abfangen von SMS-Nachrichten aus der Ferne ermöglicht. Das ist keine Science-Fiction – Journalisten demonstrierten es 2017 live im deutschen Fernsehen.

Das Urteil : 2FA per SMS ist zwar unendlich viel besser als gar nichts, bietet aber keinen soliden Schutz, wenn man selbst Ziel eines Angriffs ist.

Die TOTP-App (Google Authenticator, Aegis…): besser, aber nicht unfehlbar

Apps, die alle 30 Sekunden einen 6-stelligen Code generieren (TOTP), sind SMS deutlich überlegen. Sie haben jedoch eine Schwachstelle: Wenn Ihr Telefon mit Schadsoftware infiziert ist, kann der Angreifer diese Codes in Echtzeit auslesen.

Es gibt auch Echtzeit-Phishing-Angriffe, bei denen eine gefälschte Website Ihren TOTP-Code während der Eingabe abfängt und ihn unmittelbar vor Ablauf seiner Gültigkeit verwendet.

Der physische Schlüssel: etwas, das ein Hacker aus der Ferne nicht besitzen kann.

Ein physischer Sicherheitsschlüssel (YubiKey, OnlyKey) ist ein kleines USB- oder NFC-Gerät, das Sie an Ihr Smartphone anschließen oder in dessen Nähe halten, um sich zu authentifizieren. Sein grundlegendes Merkmal: **Der Schlüssel muss physisch vorhanden sein, damit die Verbindung funktioniert** .

Kein Hacker am anderen Ende der Welt kann Ihnen den Schlüssel aus der Ferne stehlen. Nicht einmal, wenn er Ihr Passwort kennt. Nicht einmal, wenn er Ihre SMS abgefangen hat. Solange Sie den Schlüssel nicht in der Hand halten, bleibt die Tür verschlossen.

Die Grundlage vor dem Schlüssel: ein Passwortmanager

Bevor man überhaupt über physische Schlüssel spricht, gibt es eine oft übersehene Voraussetzung: **Ihre Passwörter selbst** .

Ein physischer Schlüssel schützt den Zugriff auf Ihre Konten. Wenn Sie aber überall Passwörter wie „März2024!“ verwenden, lösen Sie nur die halbe Wahrheit. Ein Passwort-Manager generiert und speichert für jeden Dienst einzigartige, komplexe Passwörter – ohne dass Sie sich diese merken müssen.

Ich empfehle ProtonPass : Open Source, Ende-zu-Ende-verschlüsselt, mit Sitz in der Schweiz und jetzt auch mit E-Mail-Alias-Generierung zum Schutz Ihrer echten Adresse. Es funktioniert auf all Ihren Geräten.

Die optimale Kombination: **Proton Pass für sichere Passwörter + ein physischer Schlüssel für den Zugang** = Sie gehören zu den 1 % der am besten geschützten Nutzer.

Teil 2 – Wie ein physischer Schlüssel funktioniert

Die FIDO2- und WebAuthn-Protokolle einfach erklärt

Hinter physischen Sicherheitsschlüsseln verbergen sich zwei offene Standards: **FIDO2** und **WebAuthn** . Man muss sich diese Namen nicht merken – entscheidend ist, was sie ermöglichen.

Bei der Registrierung Ihres Schlüssels auf einer Website werden zwei Elemente generiert: ein **privater Schlüssel** (der ausschließlich auf Ihrem physischen Schlüssel gespeichert und niemals weitergegeben wird) und ein **öffentlicher Schlüssel** (der an die Website gesendet wird). Nach dem Login sendet die Website eine mathematische Aufgabe, die nur mit Ihrem privaten Schlüssel gelöst werden kann. Ist Ihr physischer Schlüssel nicht vorhanden, kann niemand diese Aufgabe lösen.

Das Besondere an diesem System ist, dass der private Schlüssel das physische Gerät niemals verlässt. Selbst wenn die von Ihnen genutzte Website gehackt wird, erhalten die Angreifer lediglich den öffentlichen Schlüssel – der ohne den physischen Schlüssel nutzlos ist.

Was geschieht tatsächlich?

1. Sie geben Ihren Benutzernamen und Ihr Passwort ein.
2. Die Website fordert Sie auf, dies mit Ihrem Schlüssel zu bestätigen.
3. Sie stecken Ihren YubiKey ein und drücken den Knopf (oder Sie bringen Ihren OnlyKey in die Nähe).
4. Der Schlüssel signiert die Verbindung kryptografisch.
5. Zugriff gewährt

Dauer des Vorgangs: 3 Sekunden.

Teil 3 – YubiKey vs. OnlyKey: Welchen soll man wählen?

YubiKey – Der Marktmaßstab

Der von Yubico (einem schwedisch-amerikanischen Unternehmen) hergestellte YubiKey ist der weltweit am häufigsten verwendete Sicherheitsschlüssel. Er wird von Google, US-amerikanischen Regierungsbehörden und Millionen anspruchsvoller Nutzer eingesetzt.

Hauptmerkmale:

- Maximale Kompatibilität (praktisch alle Dienste, die FIDO2 unterstützen)
- Außergewöhnliche Robustheit (beständig gegen Wasser, Druck und Stöße)
- Verfügbare Formate: USB-A, USB-C, NFC
- Für den grundlegenden Gebrauch ist weder Batterie noch Softwareinstallation erforderlich.
- GrapheneOS-kompatibel (über NFC oder USB-C)

Schwachpunkt:

- Der Quellcode ist teilweise geschlossen (die Firmware ist nicht Open Source).
- Preis: ca. 69 € je nach Modell

Welches Modell soll ich wählen?

- **YubiKey 5 NFC / 5C NFC** (USB-A oder USB-C + NFC): der vielseitigste, funktioniert an PC und Smartphone — auf Amazon ansehen (~69 €)
- **YubiKey 5 Nano** : ultrakompaktes Format, das ständig eingesteckt bleibt – erhältlich bei Amazon (ca. 81 €)

Für die überwiegende Mehrheit der Nutzer ist der YubiKey 5 NFC oder 5C NFC die beste Wahl.

OnlyKey – Die Open-Source-Alternative

Der von CryptoTrust (einem amerikanischen Unternehmen) hergestellte OnlyKey zeichnet sich durch eine einzigartige Funktion aus: Er kann auch **Passwörter speichern und diese automatisch** über ein direkt in das Gerät integriertes PIN-Code-Tastenfeld eingeben.

Hauptmerkmale:

- Vollständig Open Source (Hardware und Firmware)
- Speichert bis zu 24 Konten mit Benutzername + Passwort + TOTP
- Physische PIN am Gerät (12 Tasten) – keine Eingabe am Computer
- Selbstzerstörung nach X falschen PIN-Eingaben

Schwächen:

- Weniger breite Kompatibilität als YubiKey
- Komplexere Konfigurationsschnittstelle
- Keine NFC-Version

Für wen ist es gedacht? Für den Benutzer, der maximale Kontrolle wünscht und vollständig Open Source bevorzugt.

OnlyKey ist bei Amazon erhältlich (ca. 67 €).

Schnellvergleichstabelle

	YubiKey 5 NFC	OnlyKey
Preis	~€69	~€67
Open Source	Teilweise	Gesamt
NFC (Smartphone)	✅	❌
Passwortspeicherung	❌	✅
Benutzerfreundlichkeit	★★★★★	★★★
Kompatibilitätsdienste	★★★★★	★★★
GrapheneOS-kompatibel	✅	✅

Zusammenfassend lässt sich sagen: Wer die einfachste und kompatibelste Lösung sucht, sollte sich für einen YubiKey entscheiden. Wer mit den technischen Aspekten vertraut ist und bei dem Open Source ein absolutes Muss ist, für den ist der OnlyKey eine hervorragende Wahl.

Teil 4 – Kompatibilität: Wo kann ein physischer Schlüssel verwendet werden?

Kompatible Dienste

Die Liste der Dienste, die FIDO2/WebAuthn unterstützen, wächst jährlich. Hier sind die wichtigsten:

Messaging und Produktivität:

- **Proton Mail, Proton Drive, Proton VPN** – Proton unterstützt FIDO2-Schlüssel auf allen seinen Diensten
- Gmail / Google Workspace
- Microsoft / Outlook
- GitHub
- Bitwarden

Soziale Netzwerke und andere:

- X (Twitter) (Nur für Premium-Abonnenten)
- Facebook / Instagram
- Dropbox
- 1Password

Was noch fehlt: Die meisten französischen Banken akzeptieren noch keine FIDO2-Schlüssel für die Anmeldung (sie verwenden ihre eigenen PSD2-Systeme). Das ändert sich jedoch.

Smartphone-Kompatibilität

iPhone (iOS 16+): Kompatibel über NFC und Lightning/USB-C. Safari unterstützt WebAuthn nativ.

Android: Kompatibel über NFC und USB-C. Chrome und Firefox unterstützen WebAuthn.

GrapheneOS: Vollständig kompatibel über NFC (YubiKey) und USB-C. Keine spezielle Konfiguration erforderlich – GrapheneOS entspricht den Android-Standards für WebAuthn.
[Falls Sie GrapheneOS noch nicht kennen, finden Sie hier eine ausführliche Anleitung .]

Teil 5 – Was ein physischer Schlüssel NICHT leistet

Dieser Abschnitt ist wichtig. Ein physischer Schlüssel ist ein mächtiges Werkzeug, aber er ist keine Magie.

Es bietet keinen Schutz, wenn:

- Sie verlieren ihn, weil Sie keinen Backup-Schlüssel eingerichtet haben (speichern Sie immer 2 Schlüssel für jedes wichtige Konto).
- Die von Ihnen verwendete Website unterstützt kein FIDO2 (einige ältere Dienste unterstützen nur SMS oder TOTP).
- Ihr Computer ist bereits bei der Ersteinrichtung mit einem Keylogger infiziert.
- Ihr Schlüssel UND Ihr Handy werden gleichzeitig gestohlen.

Es ersetzt nicht:

- Ein guter Passwortmanager (die beiden ergänzen sich)
- Gute allgemeine digitale Hygiene (Updates, Wachsamkeit gegenüber Phishing)
- Ein VPN in öffentlichen Netzwerken

Praktischer Tipp: Bestellen Sie immer **zwei Schlüssel** gleichzeitig. Der erste ist Ihr Hauptschlüssel. Der zweite ist Ihr Backup-Schlüssel, den Sie an einem sicheren Ort aufbewahren. Bewahren Sie beide Schlüssel für jedes wichtige Konto auf. So bleiben Sie auch bei Verlust des Hauptschlüssels auf dem Laufenden.

Fazit – Der optimale Schutzstapel

Ein physischer Sicherheitsschlüssel ist eine der besten Entscheidungen, die Sie für Ihre digitale Sicherheit treffen können. Er verhindert praktisch alle Fernzugriffsangriffe auf Konten.

Die empfohlene Stack-Kombination basierend auf Ihrem Profil:

Einsteigerprofil: Beginnen Sie mit Proton Pass für Ihre Passwörter und fügen Sie dann einen YubiKey 5 NFC für Ihre sensibelsten Konten hinzu (E-Mail, Bank, falls kompatibel, soziale Netzwerke).

Erweitertes Profil: Proton Pass + YubiKey 5C NFC (primär) + YubiKey 5 NFC (Backup). Aktivieren Sie den Schlüssel für Proton Mail, GitHub, Google und alle wichtigen Dienste.

Open-Source-Maximalist-Profil: OnlyKey + Proton Unlimited für Mail, Passwörter, Drive und VPN in einem einzigen verschlüsselten Ökosystem.

Das Prinzip ist einfach: Ein Hacker kann Ihr Passwort von der anderen Seite der Welt stehlen. Er kann aber keinen physischen Gegenstand stehlen, der sich in Ihrer Tasche befindet.

Übernehmen Sie wieder die Kontrolle.