Schieb Report

Ausgabe 2022.09

Datenaustausch mit Android per Web: Airdroid

Android-Geräte sind offen für alles, auch für den Zugriff auf das Dateisystem zur Datenübertragung. Die geht sogar einfacher als über den Explorer oder Finder!

Normalerweise nutzt ein Android-Gerät eine Kabelverbindung, um die Daten auf einen PC oder Mac zu bekommen. Durch den integrierten Treiber meldet sich das Smartphone am stationären Rechner als Massenspeicher an, der wie ein USB-Stick oder eine externe Festplatte nutzbar ist.

Unübersichtliche Dateistruktur

Android basiert auf Unix, und das merkt man vor allem an der Verzeichnisstruktur: Wer sie durchschaut, der kommt schnell damit klar und findet die gesuchten Dateien, alle anderen müssen sich mühsam daran gewöhnen. Das wird deutlich besser, wenn die Dateien grafisch aufbereitet und kategorisiert werden - wie Android es für den Benutzer macht. Hier setzt die kostenlose App AirDroid an.

Kabellos und grafisch

Nach der Installation der App und dem kostenlosen Anlegen eines Benutzerkontos ist kein Kabel und keine schwer zu konfigurierende Verbindung nötig: Ruft einfach http://web.airdroid.com/ auf und scannt mit der Kamera des Smartphones den angezeigten QR-Code. Smartphone und PC verbinden sich miteinander, und das über eine lokale Verbindung, die Daten verlassen nicht das eigene Netzwerk.

Der Browser stellt eine Oberfläche dar, wie Android sie nicht schöner hinbekommen könnte. Die Dateien sind nach Kategorien sortiert, auch ein Zugriff auf die Nachrichten, das Rufprotokoll und die Kamera ist möglich. Jede Datei kann auf den PC heruntergeladen werden, indem sie einfach auf Desktop oder Schreibtisch oder in einen Ordner im Explorer gezogen wird.

KJM beschließt Sperrung von xHamster

Landesmedienanstalten verpflichten Internetanbieter zur Blockierung des Porno-Portals xHamster. Damit wird eine Netzsperre durchgeführt. Eine Methode, die nicht unumstritten ist.

Die Kommission für Jugendmedienschutz (KJM) hat im Verfahren gegen das Porno-Portal xHamster einstimmig entschieden, dass Internetanbieterinnen das Angebot für den Abruf aus Deutschland sperren müssen. Ein Schritt, der sich schon vor längerer Zeit angekündigt hat und damit alles andere als übereilt erfolgt. Das Mittel der Netzsperre ist allerdings umstritten.

xHamster weigert sich, Altersverifikation einzubauen

Auf der Seite sind pornografische Angebote frei zugänglich – ohne dass sichergestellt ist, dass Kinder und Jugendliche keinen Zugang dazu erhalten. Das verstößt gegen den Jugendmedienschutz-Staatsvertrag (JMStV) und ist damit gesetzeswidrig.

Nach einer vorherigen Entscheidung der KJM im März 2020 hatte die zuständige Landesanstalt für Medien NRW die Anbieterin von xHamster, das Unternehmen Hammy Media Ltd., bereits damals dazu aufgefordert, die Seite gesetzeskonform zu gestalten und eine Altersüberprüfung vorzunehmen.

xHamster wird blockiert

Daher müssen nun als Erstes die fünf größten deutschen Internetanbieterinnen den Abruf der Seite „de.xhamster.com“ blockieren. Die Landesmedienanstalten, die gemäß des Sitzes der Anbieter zuständig sind – die Bayerische Landeszentrale für neue Medien (BLM), die Landesanstalt für Medien NRW (LFM NRW), die Medienanstalt Berlin-Brandenburg (mabb) sowie die Medienanstalt Rheinland-Pfalz – haben entsprechende Bescheide zugestellt.

Dr. Marc Jan Eumann, Vorsitzender der KJM: „Pornos sind kein Kinderprogramm. Unser gesetzlicher Auftrag ist es, Kinder und Jugendliche vor Inhalten zu schützen, die nicht ihrem Entwicklungsstand entsprechen. Pornografie stellt eine erhebliche Gefahr für ihre seelische und sexuelle Entwicklung dar".

Netzsperren sind umstritten

Nachvollziehbar - auch, wenn es dazu unterschiedliche Ansichten gibt. Aber die Landesanstalten haben nunmal die Aufgabe, geltendes Recht auch durchzusetzen. Ein Porno-Angebot für Erwachsene ist so lange kein Problem, wie technische Schutzvorkehrungen die gesetzlichen Standards zum Schutz von Kindern und Jugendlichen sicherstellen.

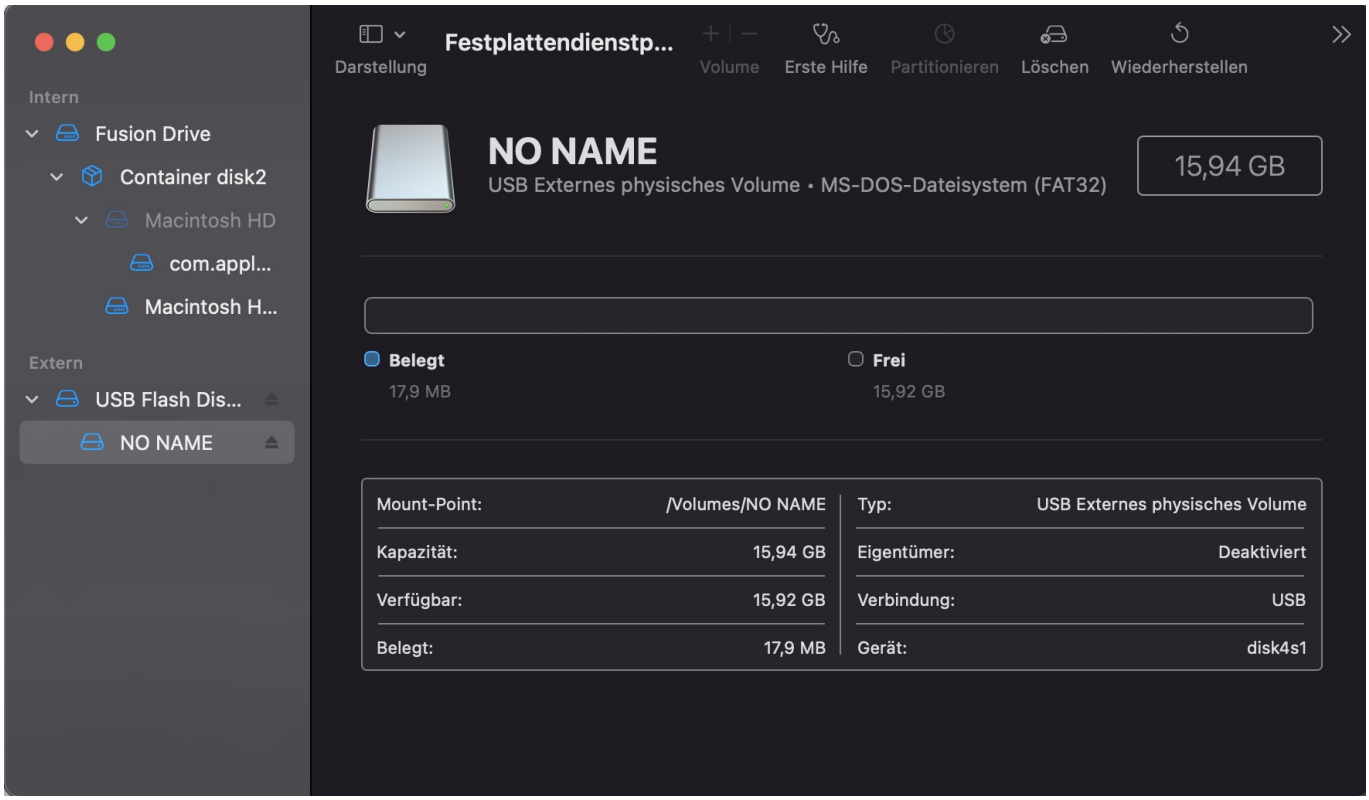
Da xHamster das nicht tut, greifen die Landesanstalten für Medien nun als letztes Mittel auf Sperrverfügungen zurück. Sie schützen damit Kinder, nicht das Geschäftsmodell der Pornoindustrie.

Ein konsequenter Schritt. Angebote, die sich an ein deutsches Publikum richten, müssen sich auch an den deutschen Jugendmedienschutz halten. Und dann ist es auch egal, wenn der Firmensitz sonstwo ist.

Wenn SD-Karten bei macOS nicht funktionieren

Mittlerweile sind wieder in so gut wie allen macOS-Geräten SD-Karten-Slots eingebaut. Super, wenn sie funktionieren. Was aber, wenn nicht?

Auf einem stationären Mac sind SD-Karten meist nur eine zweiweise Erweiterung. Beispielsweise, wenn die Bilder einer Digitalkamera auf den Mac kommen sollen. Bei einem Macbook ist das schon anders: Micro-SD-Karten können mit einem Adapter so eingelegt werden, dass sie unauffällig im Gerät bleiben können und so den eher begrenzten SSD-Speicher dauerhaft ergänzen. In den meisten Fällen sind die Daten, die darauf gespeichert sind, genauso wichtig wie die auf der Festplatte. Was, wenn die SD-Karte nicht mehr gefunden wird?



Der erste Schritt sollte immer die Kontrolle der Karte sein. Oft hat diese sich durch den Transport gelockert und steckt nicht mehr ganz im Slot. Hilft das nicht weiter, dann ist das **Festplattendienstprogramm** von macOS die beste Anlaufstelle. macOS zeigt die SD-Karten und USB-Sticks in einem eigenen Bereich **Extern** an. Klickt den jeweils unteren Eintrag eines Datenträgers an, dann zeigt die App alle Eigenschaften (wie beispielsweise die Formatierung und Kapazität) im Detailbereich an.

Erste Hilfe versucht das Laufwerk wieder verfügbar zu machen, ohne die Daten zu verändern. Im Idealfall müssen nur automatisch ein paar Parameter angepasst werden, und das Laufwerk erscheint wieder im Finder. **Wiederherstellen** geht dann schon einen Schritt weiter und versucht den Datenträger in seiner Formatierung wiederherzustellen. Die Daten sind dabei aber oft nicht mehr rekonstruierbar.

Hilft auch **Löschen** nichts mehr, dann bleibt als letzter Versuch eine Formatierung unter Windows. Klingt komisch, schafft es aber oft, eine SD-Karte oder einen USB-Stick wiederzubeleben.

Teilnehmer aus einer Teams-Sitzung entfernen

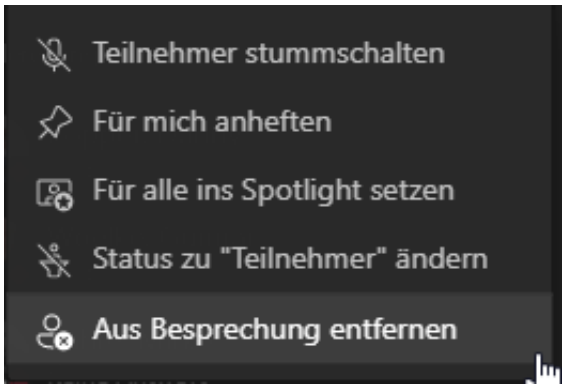
Microsoft Teams schafft einen virtuellen Raum für Besprechungen. Was aber, wenn jemand darin ist, der da nicht hingehört? Raus mit ihm!

Selten wird eine Teams-Besprechung spontan einberufen. Der Link zur Besprechung ist meist in dem Termin erhalten, den alle Teilnehmer bekommen haben. Jeder Teilnehmer kann dann durch einen Klick darauf in die Besprechung gelangen. Je mehr Teilnehmer aber im Verteiler sind, desto eher schleicht sich mal ein Tippfehler oder eine Verwechslung ein. Kurz: Im Termin ist plötzlich jemand, der da gar nicht hingehört.

Löschen von Teilnehmern

Aus der Situation zu entkommen, ist eigentlich leicht: Die freundliche Bitte an den ungebetenen Gast, die Besprechung zu verlassen, bewirkt meist Wunder. Wenn es sich denn um eine Person aus Fleisch und Blut handelt! Manche Teilnehmer in Terminen sind das nicht: Raumsysteme beispielsweise, die mehrere Teilnehmer mit Kamera und Mikrofon an dem Termin teilnehmen lassen. Die lassen sich

leider nicht durch gutes Zureden davon überzeugen, die Besprechung zu verlassen.



Das Problem ist Teams nicht fremd, und so bietet die App auch die Möglichkeit, Teilnehmer zu entfernen. Allerdings nicht da, wo der Anwender es vermuten würde! Statt in den Teilnehmerbildern der Besprechung müsst Ihr auf das Symbol mit der kleinen Figur oben rechts im Teams-Bildschirm klicken, dann auf die drei Punkte. Im sich öffnenden Menü entfernt dann ein Klick auf **Aus Besprechung entfernen** den Teilnehmer sowohl aus der Besprechung selbst als auch aus dem Besprechungs-Chat.

Vorsicht beim OneDrive-Papierkorb

Speichern Sie Ihre Dateien in OneDrive und verlassen sich darauf, dass die auf allen Rechner verfügbar sind? Dann achten Sie genau darauf, welche Dateien Sie löschen!

OneDrive dient vor allem als zentraler Speicher für Dateien in der Cloud. Der Cloudspeicher ist immer führend: Die Version der Datei, die darauf gespeichert ist, ist die aktuelle Version. Ändern Sie sie auf einem der Geräte, die mit dem OneDrive synchronisieren, dann wird die Änderung in die Cloud synchronisiert. Jedes Ihrer Geräte lädt dann zeitnah die aktualisierte Version herunter.

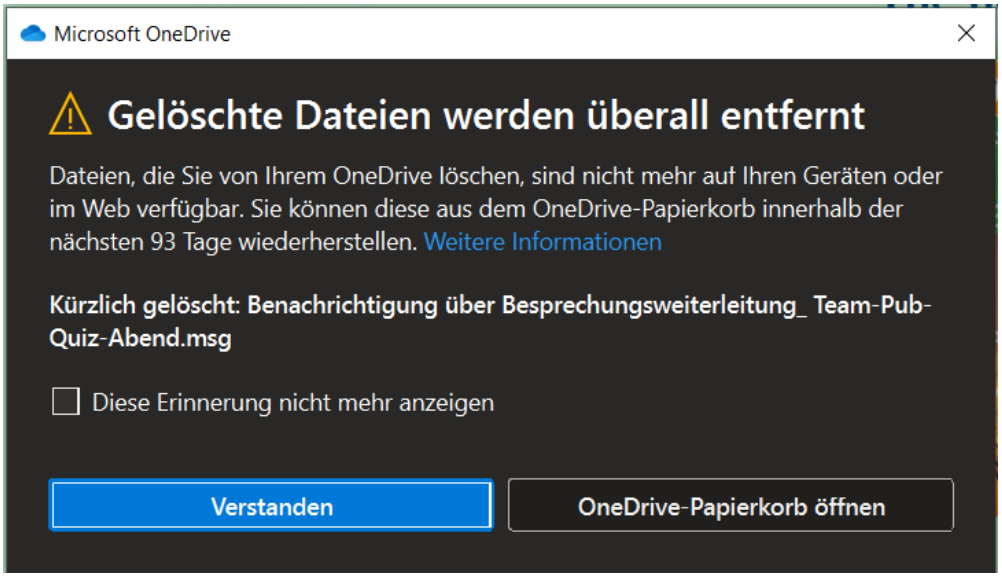
OneDrive ist führend

Sollten zeitgleich Änderungen an der selben Datei von mehreren Rechnern vorgenommen worden sein, dann meldet die OneDrive-App einen Konflikt. Sie können dann festlegen, ob eine Datei behalten werden soll. Wenn beide Änderungen wichtig, dann können Sie beide Dateien behalten. In diesem Fall werden beide Versionen auf alle Geräte synchronisiert.

Wenn Sie Dateien löschen, dann verschwinden diese auch von jedem Gerät, das mit Ihrem OneDrive synchronisiert.

Zentraler Speicher, lokaler Papierkorb?

Sie brauchen eine Datei nicht mehr? Dann löschen Sie sie. Ganz konsequent synchronisiert OneDrive auch diese Änderung in die Cloud. Die Datei wird in ihrem lokalen Windows-Papierkorb gespeichert. Daraus können Sie sie jederzeit wiederherstellen, solange Sie diesen nicht geleert haben.



Nun ist der Windows-Papierkorb nur auf dem jeweiligen Rechner verfügbar. Wenn Sie feststellen, dass Sie die Datei trotzdem benötigen, dann können Sie auch auf einem der anderen Geräte noch darauf zugreifen, denn OneDrive hat einen eigenen Papierkorb, den Sie als Ordner links in der Ordnerliste finden.

Vorsicht dabei aber: Die Dateien werden daraus innerhalb von 30 Tagen (normales OneDrive) bzw. 93 Tagen (OneDrive for Business) gelöscht und sind dann nicht mehr verfügbar!

Gericht kippt NetzDG: Verstoß gegen EU-Recht

Google und Meta haben gegen Teile des NetzDG geklagt. Jetzt haben sie einen ersten Erfolg erzielt: Die Meldepflicht im NetzDG verstoße gegen das Herkunftslandprinzip, meint das Verwaltungsgericht Köln.

Eigentlich soll seit Anfang Februar das neue NetzDG gelten: Portale wie Facebook, Tiktok oder Youtube müssen nicht nur Posts löschen, wenn sie von strafbaren Inhalten erfahren, sondern entdeckte Posts mit strafbaren Inhalten samt IP-Adresse an eine zentrale Meldestelle beim BKA melden. Das soll mehr Strafverfolgung ermöglichen - und den Druck auf jene User erhöhen, die sich nicht davon abhalten lassen, immer wieder Hass und Hetze zu verbreiten.

Portale wie Facebook, Youtube und andere klagen

Doch dazu ist es nicht gekommen, da einige Portale wie Meta, Tiktok und andere

gegen das Gesetz geklagt haben. Nun hat das Verwaltungsgericht Köln zu den Eilanträgen von Google und Meta entschieden: Die müssen vorerst keine Meldungen ans BKA machen (was die Portale ohnehin unterlassen haben). Nach Ansicht des Gerichts verstoße die Regelung aus § 3a NetzDG gegen EU-Recht, heißt es in einer Mitteilung des Gerichts.

Es geht um das sogenannte **Herkunftslandprinzip**. Entsprechend der E-Commerce-Richtlinie regelt derjenige Staat bestimmte Anforderungen an die Anbieter, in dem dieser seinen Sitz hat. Und der liegt bei Google und Meta nicht in Deutschland, sondern in Irland. Das sind juristische Details - aber eben in solchen Situationen relevant.

Auf diesen Umstand haben in der jüngsten Vergangenheit schon viele Experten und Juristen hingewiesen. Ein Problem, das sogar in einem Gutachten der Wissenschaftlichen Dienste des Bundestags benannt ist.

Bedeutet konkret: Das Herkunftslandprinzip macht es prinzipiell erforderlich, dass Irlans - als Herkunftsland - Meldepflichten jeder Art regelt. Genau das macht es nun problematisch, ein NetzDG zu formulieren, das Irland umgeht. Ändern könnten das erst neue EU-Regeln wie sie aktuell in Vorbereitung sind, etwa mit dem **Digitale Dienste Gesetz** (Digital Services Act).

Weitere Klagen von Twitter und Tiktok

In einem Eilantrag ging es auch um die geplante Vorschrift, dass Anbieter sogenannte Gegenvorstellungsverfahren durchführen müssen. Bedeutet konkret: Nutzer müssen widersprechen können, wenn Postings durch die Portale gelöscht werden. Es könnte sich ja um eine irrtümliche oder unrechtmäßige Löschung handeln. Deshalb sollen User widersprechen und eine Prüfung verlangen können.

Neben Google und Meta haben auch Twitter und Tiktok Klagen eingereicht. Für sie steht eine Entscheidung noch aus.

Digitale Proteste gegen den Krieg nehmen zu

Russen können keine iPhones mehr kaufen: Apple hat in Russland den Verkauf vollständig eingestellt. Es gibt nach dem Aufruf von Ukraines Vize Fedorov auf Twitter jede Menge Solidarität, öffentliche Proteste und auch gezielte Aktionen gegen Russland im Netz. Nicht alle sind ungefährlich.

Apple hat am Dienstag einen vorübergehenden Verkaufsstopp für alle Produkte in Russland angekündigt. Auch in Russland populäre Hardware wie iPhones, iPads oder Macs sind in Russland vorerst nicht mehr erhältlich. Schon vergangene Woche hat der Konzern seine Lieferungen an russische Verkaufskanäle gestoppt. Eigene Apple Stores hat das Unternehmen in Russland nicht – und der Apple-Store erlaubt in Russland keine Einkäufe mehr.

Keine Apple-Produkte mehr in Russland

Damit verzichtet der Konzern aus Solidarität zur Ukraine auf erhebliche Umsätze. Das ist mehr als nur eine symbolische Geste und vermutlich eine Reaktion auf den Hilferuf des ukrainischen Vizepräsidenten. Vor einigen Tagen hat Mykhailo Fedorov, Vize-Premier der Ukraine und gleichzeitig Minister für Digitalisierung des Landes, auf seinem Twitter-Account diverse Tech-Konzerne konkret um Hilfe und Boykott Russlands gebeten, darunter Apple und Netflix. Apple hat nun entschlossen reagiert.

In einem anderen Tweet hat Fedorov aber auch offen jeden dazu aufgerufen, sich einer „IT-Armee“ anzuschließen. Fedorov hat das sogar so genannt. Dem extra für diesen Zweck eingerichteten Kanal auf Telegram folgen bereits über 270.000 Menschen aus aller Welt. Hier werden allerlei Angriffe auf russische Ziele ausgeheckt und besprochen. Insbesondere sogenannte „Denial of Service“-Attacken (DDoS).

Dabei werden bestimmte Server mit einer nicht mehr zu bewältigenden Anzahl gleichzeitiger Anfragen heillos überfordert. Sie gehen in die Knie – und sind dann für die Öffentlichkeit nicht mehr erreichbar. Betroffen von solchen Angriffen waren und sind die Webseite des Kremls, sowie die Onlineangebote der Sberbank, des

Staatssenders Russia Today sowie das Gasunternehmen Gazprom. Auch die deutsche Webseite ist aktuell nicht erreichbar.

Aufruf des Hacker-Verbunds „Anonymous“

Die hohe Bereitschaft, an solchen Angriffen mitzuwirken, lässt sich auch mit dem offiziellen Aufruf der Hackergruppe „Anonymous“ erklären. Die hat vor wenigen Tagen Russland quasi offiziell den Krieg erklärt. Dadurch fühlen sich Hacker in aller Welt berufen, Ziele in Russland anzugreifen, vor allem Ziele, die zur Regierung und dem Machtbereich Putins gehören. So ist es Anonymous nach eigenen Angaben gelungen, das russische Verteidigungsministerium und den belarussischen Waffenhersteller Tetraedr zu attackieren und lahmzulegen.

Laut Anonymous geht es nicht darum, die russische Bevölkerung zu treffen. „Putin, der Hackertruppen und Troll-Armeen gegen westliche Demokratien einsetzt, bekommt einen Schluck seiner eigenen bitteren Medizin“, heißt es in einer Stellungnahme. Neben gezielten Störungen ist ein weiteres Ziel, die IT-Experten und Hackergruppen mit der Abwehr zu beschäftigen, damit sie sich nicht um Angriffe in der Ukraine und des Westens kümmern können. Die Angriffe erfüllen also verschiedene Zwecke.

Angriffe auf russische Infrastruktur sind riskant

Angriffe auf kritische Infrastruktur, etwa Atomkraftwerke oder Verkehr, sind allerdings ein gefährliches Unterfangen, wie auch Vertreter von Anonymous selbst sagen. Daher muss unbedingt vermieden werden, dass relevante digitale Infrastruktur in Russland zerstört wird oder sogar Menschenleben fordert. Denn das wäre nicht nur unvertretbar, sondern würde Putin die nötige Rechtfertigung liefern, ungehemmt zurückzuschlagen – wozu die gut trainierten und finanziell bestens ausgestatteten Hackertruppen aus Russland zweifellos in der Lage sind.

Deshalb engagierten sich Anonymous-Aktivisten auch proaktiv dafür, dass Menschen in der Ukraine trotz akuter Störungen des Internets beständig online bleiben können. Um das zu gewährleisten, werden VPN-Dienste bereitgestellt, die unter Umgehung der ukrainischen Infrastruktur direkt Zugriff aufs Internet bieten.

Erfolgreiche Petition in Russland selbst

Aber auch in Russland regt sich Widerstand gegen den Krieg. Eine russischsprachige Online-Petition des Aktivisten und Oppositionspolitikers Lew Ponomarjow gegen den Krieg in der Ukraine haben bislang mehr als 1,1 Millionen Menschen unterzeichnet. Unter anderem wird ein sofortiger Rückzug der russischen Streitkräfte vom "Territorium des souveränen Staates Ukraine" verlangt.

https://youtu.be/K6dPg5iT1DE

Was bedeutet eigentlich der Begriff "Pentest"?

Wer wissen will, ob seine digitale Infrastruktur (Server, Netzwerk, PCs, Datenbanken) sicher vor Angriffen durch Hacker oder Bots muss, sollte einen "Penetration Test" machen (kurz "Pentest"). Eine Art gezielter und koordinierter Belastungstest: Was hält die eigene Infrastruktur aus?

IT-Sicherheit war selten so wichtig wie in diesen Tagen. Es vergeht kaum eine Woche, in der nicht über einen erfolgreichen Hack-Angriff berichtet wird. Die weniger erfolgreichen und unentdeckten bleiben natürlich unerwähnt. Vor allem Unternehmen und Geschäftsbetriebe sollten daher immer die Sicherheit ihrer IT-Infrastruktur immer im Blick behalten.

Das Problem ist, dass die meisten keine Fachleute im eigenen Team haben und somit überhaupt nicht wissen, ob sie richtig geschützt oder womöglich sogar ein leichtes Ziel für Hacker sind.

Ein Sicherheits-Audit kann hier Abhilfe schaffen. Der sogenannte Pentest ist in Deutschland eine sinnvolle Methode. Doch was bedeutet dieser Begriff genau?

Was ist der Pentest?

Der Pentest - oder auch "Penetration Test as a Service" ist ein Begriff aus der IT-Sicherheit.

Bei einem solchen Penetrationstest geht es darum zu prüfen, ob ein System vor einem potenziellen Hack-Angriff geschützt ist oder nicht.

Dabei gibt es verschiedene Möglichkeiten, die sich nach Art, Umfang und auch der Aggressivität der Prüfung unterscheiden. **Je nachdem, für welche Möglichkeit man sich entscheidet, unterscheiden sich auch die Ergebnisse des Tests, was Risiken für den Betrieb mitbringen könnte.**

Vor einem Pentest sollte immer ein IT-Experte befragt werden, der das potenzielle Risiko am besten einschätzen kann. Die verschiedenen Abstufungen sind umfangreich. Dabei geht es unter anderem um die Häufigkeit der Durchführung des Pentests aber auch die durchsuchten Systeme oder die gewünschten Ergebnisse.

Die Durchführung selbst ist das größte Problem, denn viele Pentests passen mit ihren Anforderungen nicht zu dem jeweiligen Unternehmen. Ein professionelles Audit ist daher unumgänglich, wenn man kein unnötig hohes Risiko generieren möchte.

Faktor Informationsbasis

Bei einem Pentest kann man grundsätzlich zwischen einem Black-Box- und einem White-Box-Test unterscheiden. Bei der ersten Variante geht es um einen Test, bei dem vorab keine Informationen über das getestete System vorliegen.

Damit simuliert man einen tatsächlichen Hacker-Angriff, denn diese müssen meist auch bei Null starten. **Der Nachteil liegt darin, dass man mit relativ hohen Kosten nur begrenzte Ergebnisse erzielen kann.** So wird z.B. die Gewinnung von IP-Adressen lange dauern und Geld kosten, obwohl man im Grunde sofort intern darauf zugreifen könnte.

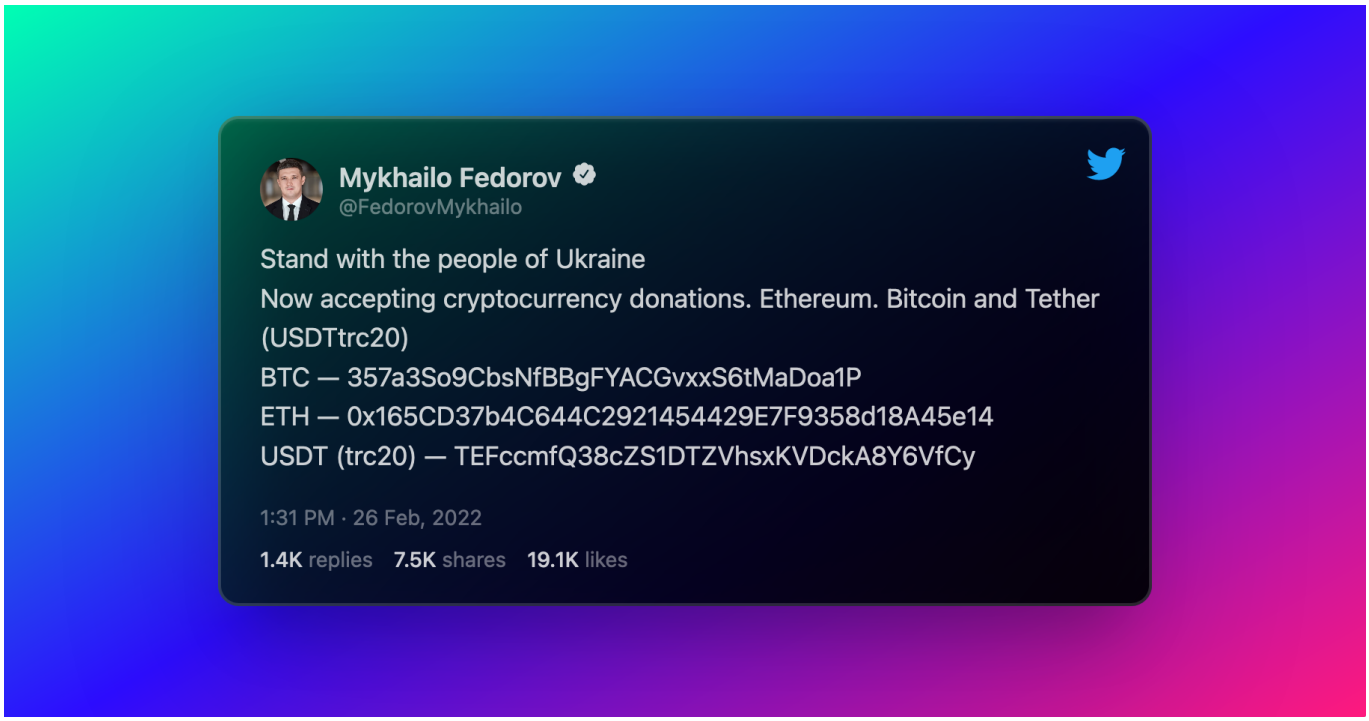
Beim White-Box-Test beginnt man derweil mit einer Datengrundlage, anhand derer man gezielt weiterarbeiten kann. Man erzielt schneller Ergebnisse, man kann den ausbleibenden Teil der Informationsbeschaffung aber nicht auswerten. Bei der Wahl einer der beiden Varianten sollte man sich also vor Augen führen, wie viel Zeit und Geld man einsetzen und welche Art von Ergebnissen man am Ende erhalten möchte.

Aggressives Vorgehen

Bei einem Pentest ist der Grad der Aggressivität sehr wichtig. Bei einem passiven Vorgehen werden die gefundenen Fehler nicht genutzt. **Mittelmäßig aktiv ist man, wenn man gefundene Schwachstellen teilweise ausnutzt, wenn sie z.B. das gesamte System beeinflussen könnten.** Bei einem aggressiven Vorgehen sollen möglichst alle Schwachstellen ausgenutzt werden, selbst wenn dabei ein erhöhtes Risiko entsteht.

Man kann also sagen, dass mit steigender Aggressivität beim Pentest auch das Risiko für Schäden und Ausfälle steigt. Ob die gewonnenen Informationen das Risiko wert sind, muss individuell entschieden werden. Wichtig ist dabei, dass man neue Fehler finden möchte, die dann in der Folge ausgebessert werden können. Nur dann haben Zeit und Aufwand für den Pentest einen Sinn.

Hybride Kriegsführung: Auch im Netz wird gekämpft



Das Internet spielt im Ukraine-Konflikt eine große Rolle. Ukraines Vize Fedorov ruft über Twitter offen Tech-Konzerne zur Hilfe auf. Während Google gezielt Dienste abschaltet, stellt Elon Musk in der Ukraine sein Satelliten-Internet zur Verfügung.

Mykhailo Fedorov, Vize-Premierminister der Ukraine ist gleichzeitig Minister für Digitalisierung des Landes – und spielt gekonnt auf der Klaviatur der digitalen Medien. Minister Fedorov hat auf seinem Twitter-Account diverse Tech-Konzerne konkret um Hilfe und Boykott Russlands gebeten: Apple solle doch in Russland seine Stores schließen, Netflix seinen Streaming-Dienst in Russland einstellen.

Google schaltet Verkehrsdienst ab

Nicht mit allen Wünschen und Forderungen dringt Fedorov durch. Mit einigen aber schon. So hat Youtube den umstrittenen Sender „Russia Today“, der vor allem auf Youtube sendet, von Werbeeinnahmen ausgeschlossen. Zwar hätte sich Fedorov ein Ausschließen des gesamten Kanals gewünscht, so fließt aber

zumindest kein Geld mehr an den Sender.

Außerdem hat Google in seinem Kartendienst Google Maps die Verkehrshinweise in der Region Ukraine abgeschaltet. Was auf den ersten Blick wenig zu bringen scheint, hat einen ernsten Hintergrund: Ein IT-Experte hatte am 24. Februar festgestellt, dass aufgereihte LKW und Militärfahrzeuge um morgens 3.15 Uhr als „Stau“ in Google Maps verzeichnet waren.

Die eingeschalteten Smartphones der mit den Fahrzeugen auf der Straße stehenden Soldaten waren für Googles Algorithmus ein Verkehrsstau - auch die Smartphones der Ukrainer, die nur langsam oder gar nicht am Konvoi vorbei kamen. Um solcherlei taktische Informationen nicht weiter öffentlich zu machen, hat Google den Dienst abgeschaltet.

Bitte um Spenden auf Krypto-Konten

Fedorov ruft aber auch zu Spenden in Kryptowährungen auf: Die Ukraine hat Krypto-Wallets für Bitcoin, Ethereum und Tether eröffnet – und es sollen schon Millionenbeträge aus anonymen Quellen gespendet worden sein. Umgekehrt fordert Fedorov Krypto-Börsen auf, russische Konten zu sperren/blockieren.

Auch an den Tech-Milliardär Elon Musk hat sich Fedorov gewandt. Denn bei kriegerischen Aktivitäten in der Ukraine ist beeits digitale Infrastruktur beschädigt, teilweise sogar zerstört worden (etwa ein eigenes Satelliten-Kommunikationssystem). Nicht auszuschließen, dass das russische Militär gezielt die gesamte digitale Infrastruktur zerstören will – oder, wer weiß, später auch „besetzen“ und auf diese Weise kontrollieren möchte. In Russland gibt es kein freies Internet.

Elon Musk schaltet Satelliten-Internet für Ukraine frei

Darum der Fedorovs Tweet an Elon Musk: Während Musk den Mars kolonisieren wolle, versuche Russland, die Ukraine zu besetzen, schreibt er. "Wir bitten Sie, die Ukraine mit Starlink-Stationen zu versorgen und vernünftige Russen zum Aufstehen aufzufordern".

Zum Hintergrund: Elon Musk gehört das Unternehmen SpaceX, das den Satelliten-Internetdienst Starlink betreibt. Rund 2.000 Satelliten umkreisen bereits den

Globus – in einer vergleichsweise geringen Höhe von 350 bis 1.000 Kilometer. Es sollen noch deutlich mehr werden. Die Satelliten kommunizieren per Laser miteinander und erlauben, von so ziemlich jeden Fleck der Erde aus ins Internet zu gehen. Nutzer können dann mit erstaunlich hoher Bandbreite surfen, E-Mails verschicken, Videos hochladen.

Eigentlich ist Starlink dazu gedacht, schlecht angebundene, ländliche Gebiete mit Internetzugang zu versorgen. Die Satellitenschüssel kostet 500 Dollar, der Online-Zugang 100 Dollar im Jahr. Bislang wurde die Ukraine nicht von Starlink versorgt. Das hat Elon Musk in seiner Hilfsaktion geändert – und „Terminals“ auf den Weg gebracht. Satelliten-Antennen, die notwendig sind, um mit den Satelliten Kontakt aufzunehmen. Darüber können Regierung, Militär und Zivilisten ungehindert mit der Außenwelt kommunizieren.

Das Internet als Kriegsschauplatz

Doch es zeichnet sich auch im Internet eine Eskalation ab. Minister Fedorov ruft auf seinem Twitter-Kanal alle Menschen mit IT-Kenntnissen dazu auf („We are creating an IT army“), sich aktiv am Kampf gegen russische Propaganda und auch russischen Hack-Angriffen zu engagieren. Über den Messenger-Dienst „Telegram“ sollen die Aufgaben („Tasks“) koordiniert werden.

Auch der Hacker-Verbund „Anonymous“ hat Russland den Krieg erklärt: Die im Verbund lose verbundenen Hacker aus aller Welt wollen russische IT-Infrastruktur angreifen. Ein gefährliches Vorhaben, da russische Hacker sehr erfahren, trainiert und mächtig sind. Bei einer Kriegsführung im Internet drohen Attacken auf westliche Infrastruktur – und das kann schnell fatale Folgen haben. Etwa beim Ausfall von wichtigen Verkehrssystemen oder wenn Krankenhäuser lahmgelegt werden.

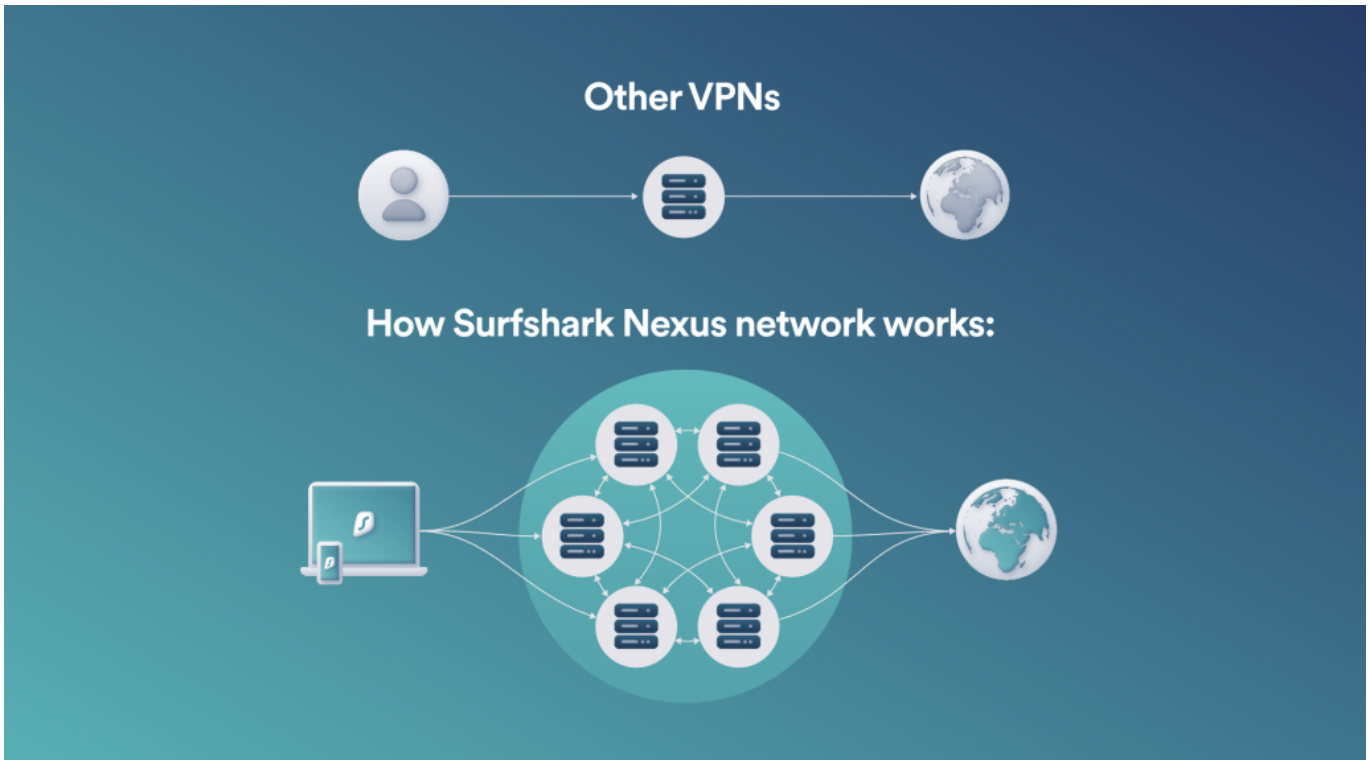
Schon seit Wochen greifen russische Hacker-Kollektive die digitale Infrastruktur der Ukraine an: Webseiten werden lahmgelegt, Server angegriffen und gezielt Daten gelöscht. Rechte: WDR/Schieb

VPN-Dienst mit mehr Tempo und Sicherheit: Surfshark Nexus

VPN-Dienste werden bei den Usern immer beliebter. Sie verschleiern die eigene Identität und erlauben auch den aktuellen Standort virtuell zu verändern. Der niederländische VPN-Anbieter Surfshark setzt dabei jetzt auf ein interessantes neues Konzept, da mehr Privatsphäre und Tempo verspricht.

Die meisten VPN- Dienste folgen ein und demselben Prinzip: Der Nutzer stellt eine Verbindung von seinem Gerät mit einem VPN-Server her, der baut einen verschlüsselten Datentunnel auf und erledigt dann alle Webseiten-Anfragen und teilweise auch andere Anfragen im Netz. Dadurch wird die gesamte Kommunikation sicher verschlüsselt und auch die eigene Identität verschleiert.

Auch der Anbieter Surfshark hat dieses Prinzip bislang verfolgt. Doch jetzt hat der Anbieter aus den Niederlanden eine Art Turbo für seinen VPN-Dienst eingeführt: Mit Surfshark Nexus verbinden sich Nutzer bei Aktivieren des VPN-Netz nicht mehr mit einem VPN-Server aus dem Surfshark-Netzwerk, sondern gleich mit allen. Das sorgt für mehr Datentempo - und noch mehr Privatsphäre.



Surfshark Nexus: Rotierende IP-Adressen

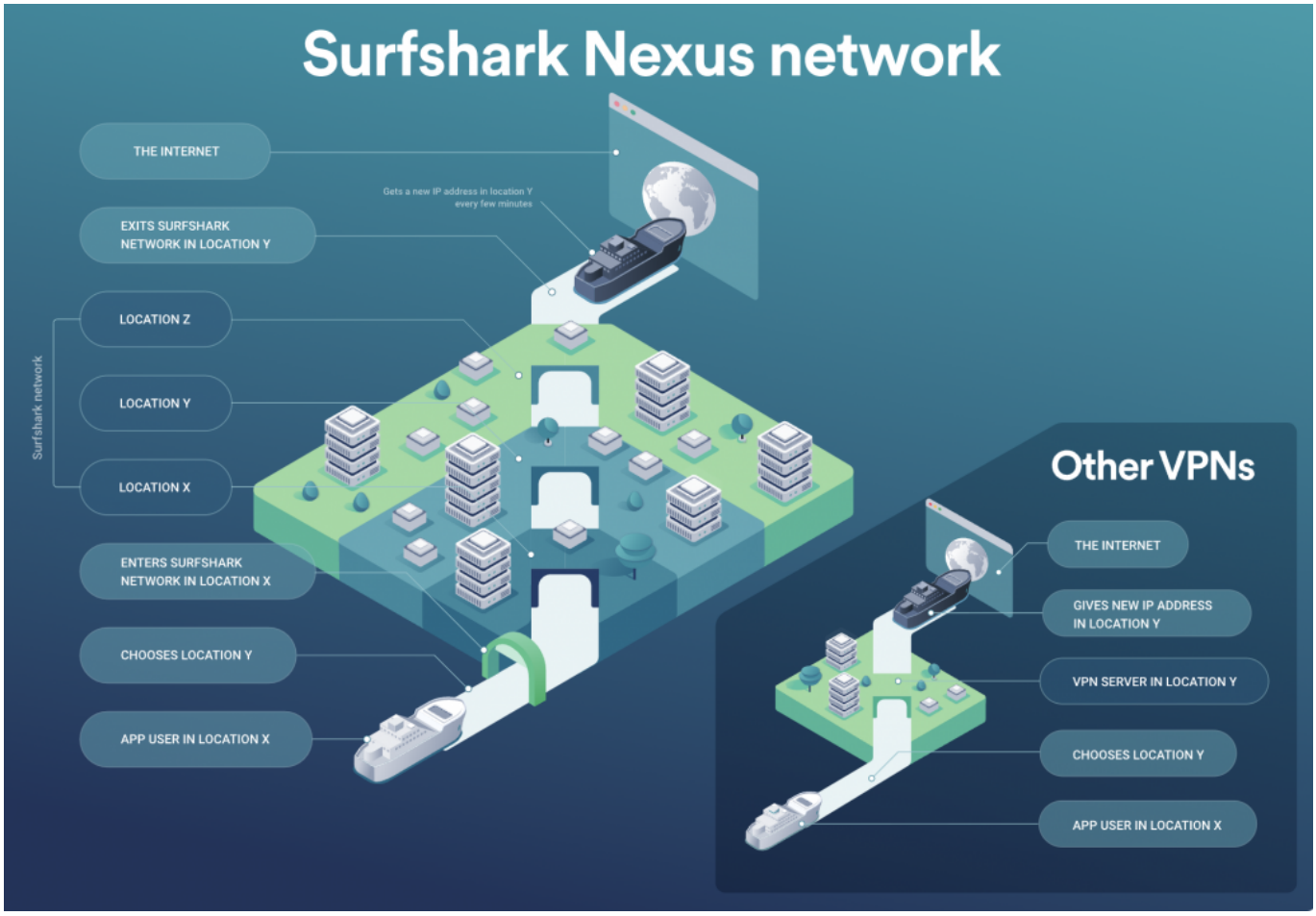
Der Hersteller verspricht insgesamt mehr Datentempo, stabilere Verbindungen und eine noch bessere Sicherheit. Die entsteht schon allein dadurch, dass die Surfshark-Software einen IP-Rotator aktiviert. Die IP-Adresse der eigenen Verbindung verändert sich alle paar Sekunden von ganz alleine, sie "springt" sozusagen. Das macht es Werbenetzwerken und anderen Diensten deutlich schwerer (teilweise sogar unmöglich), einen User bei seiner Surftour zu verfolgen.

Etwas Vergleichbares bieten andere Anbieter wie HMA (Hide My Ass) zwar auch schon etwas länger an, allerdings mit einem entscheidenden Unterschied: Dort wird die VPN-Verbindung kurz unterbrochen, um die jeweils neue IP-Adresse zu aktivieren. Surfshark Nexus macht das eleganter: Es erfolgt keine Unterbrechung der Verbindung. Das Surfen bleibt immer schnell - und trotzdem verändern sich die IP-Adressen im Hintergrund. Die User bemerken das nicht mal.

Für den einzelnen Nutzer ändert sich nicht viel: Er oder sie aktiviert das VPN-Netwerk - und fertig. Alles andere erledigt die Software im Hintergrund. Wer mag, legt einen Ort oder eine Region fest, aus der IP-Adressen ausgewählt werden sollen. Beispielsweise ausschließlich IP-Adressen aus Großbritannien.

Ein solcher IP-Wechsel empfiehlt sich nicht beim Streamen von Filmen oder

Serien, da kann das eher schädlich sein. Beim Surfen im Netz hingegen steigert es die Privatsphäre enorm, wenn die IP-Adressen sich in regelmäßigen Abständen ändern.



Weitere neue Funktionen bis Ende 2022

Hersteller Surfshark hat weitere neue Features angekündigt, die bis Ende 2022 eingebaut und aktiviert werden sollen. Darunter einen **IP Randomizer**: Hier bekommt ein User beim Surfen gleich mehrere IP-Adressen zugewiesen. Beim Ansteuern einer jeweils neuen Webseite bekommt das Gerät (das kann ein PC Tablet oder Smartphone sein) von Nexus eine neue IP-Adresse zugewiesen.

Nicht die einzige Neuerung, die geplant ist. Surfshark erweitert auch sein Multi-Hop-Verfahren: **Dynamic Multi Hop** heißt das Konzept. Hier wählt der User die einzelnen Stationen (VPN Locations) manuell aus und entscheidet, in welcher Reihenfolge sie angesteuert werden sollen. Also erst in Neuseeland, dann in Australien, gefolgt von Singapur, Österreich und Paris. Ganz so, als wäre man mobil. Das erlaubt gewissermaßen eine Art "Hakenschlagen" beim Surfen. Das

allerdings ist nur in wenigen Situationen wirklich sinnvoll und nötig, eher nichts für Menschen, die einfach nur unbescholten im Netz unterwegs sein wollen.

Surfshark bietet sei VPN-Netzwerk und die Serviceleistungen drumherum zu günstigen Preisen an: Mit dem Gutscheincode **sharkstart** kostet das Jahresabo aktuell nu 2,22 EUR pro Monat. Die Software dazu gibt es für Mac und Windows, für Android und iOS. Ein Konto reicht, um all Deine Geräte mit Surfsharb abzusichern (sehr wichtig!).

VPN auf einem Mobilgerät installieren

Ein Virtual Privat Network (VPN) bietet deutlich mehr Schutz und Privatsphäre - insbesondere beim Surfen. Viele denken, diesen Schutz gäbe es nur auf Desktop-PCs. Doch das ist unzutreffend. Es gibt heute gute und komfortable Lösungen, auch für Mobilgeräte - und da ist der Schutz häufig besonders dringend erforderlich.

Ein Virtual Privat Network (VPN) kann die Sicherheit beim Surfen erhöhen - etwa in einem offenen WLAN. Aber auch generell. Denn wer ein VPN nutzt, stellt keine direkte Verbindung zwischen seinem Gerät und einem Web-Server her, sondern geht immer den "Umweg" über einen VPN-Server. Der übernimmt ab da die Aufgabe, ruft den gewünschten Web-Server, holt die Daten ab und liefert sie ab.

Das ist zwar ein Zwischenschritt und dauert etwas länger, bietet dafür aber ein enormes Plus an Sicherheit.

Denn zum einen erfährt der Web-Server nicht, wer da Kontakt aufgebaut hat (das VPN verschleiert die eigene IP), zum anderen erfolgt die gesamte Kommunikation verschlüsselt in einem Datentunnel. Das erschwert Abhören und macht es teilweise sogar nahezu unmöglich.

In der Praxis haben sich die VPN-Dienste von Surfshark (niederländischer Anbieter) bewährt. Unter https://surfshark.com/de/ gibt es Infos zum Produkt und auch Preisinformationen. Wer noch kein Kunde ist und die App auf seinem Mobilgerät installiert, kann auch darüber ein Abo abschließen.

Wichtig zu wissen: Niemand braucht immer ein VPN immer. Wer nur Informationen auf einer gewöhnlichen Nachrichten-Seite abruft oder bei Wikipedia, ist nicht gefährdet. Wer jedoch viele Webseiten besucht, wird von der Werbe-Industrie beobachtet. Es gibt zwar auch andere Mittel und Werkzeuge, um sich der Überwachung zu entziehen - ein VPN ist aber auch einer, und zwar ein recht bequemer.

Einfache Installation unter iOS und Android

Ein VPN lässt sich nicht nur auf einem Desktop-PC nutzen, sondern durchaus auch auf einem Mobilgerät. Der Vorteil des niederländischen Anbieters Surfshark ist, dass man all seine persönlichen Geräte mit VPN schützen kann. Auch die Mobilgeräte.

Die Installation ist einfach:

1. Im Mobilgerät den App-Store aufrufen, also Google Play Store oder Apple Store.
2. Dort der Einfachheit halber nach "Surfshark" suchen.
3. Den Eintrag "Surfshark Proxy by Surfshark" auswählen - und öffnen.
4. Wenn es noch kein Konto gibt, jetzt eins eröffnen. Die ersten 7 Tage sind kostenlos - zum Test. Anschließend kostet das VPN für das Mobilgerät knapp 50 EUR im Jahr. Wer mehr Geräte schützen will, schließt ein größeres Paket ab und kann dann auch seinen Desktop-PC absichern.
5. Die App ist installiert.

Die Installation ist wirklich einfach. Beim ersten Start muss man der App ausdrücklich erlauben, seine Aufgaben als VPN-Dienst zu erledigen. Sowohl unter iOS wie unter Android sind dazu entsprechende Sicherheitseinstellungen erforderlich. Die App fordert einen auf, die nötigen Korrekturen vorzunehmen. Wer sich daran hält, hat diesen wichtigen Teil schnell erledigt. Das muss auch nur einmal gemacht werden!

Standort automatisch oder manuell wählen

Ab diesem Moment steht der VPN-Service jederzeit zur Verfügung. Solltet Ihr den Schutz benötigen - und das ist keineswegs immer der Fall -, aktiviert Ihr der Einfachheit halber die Surfshark-App und wählt aus, mit welchem Server Ihr Euch verbinden wollt. Standardmäßig ist es ein Server in der näheren Umgebung, um ein höheres Datentempo zu gewährleisten.

Wenn Ihr aber Euren Standort komplett verändern wollt, etwa um auf Dienste zugreifen zu können, die nur im Ausland zur Verfügung stehen, wählt Ihr einen Standort im Ausland. Unter "**Standorte**" steht eine lange Liste mit Standorten im Ausland zur Verfügung. Ihr habt freie Wahl.

Hohes Datentempo beim Surfen

Surfshark bietet sehr gutes Tempo im Download: Nach Aktivieren des VPN-Service konnte ich selbst über die Nodes (Knotenpunkt) in New York oder Tokio deutlich über 100 MBit/Sekunde erreichen. Der Upload war schwächer mit unter 10 MBit/Sekunde. Doch das spielt beim Surfen in der Rege keine so große Rolle, wichtiger ist der Download.

Vorsicht bei Leihwagen und Freisprecheinrichtungen

Telefonieren im Fahrzeug ohne Freisprecheinrichtung ist teuer. Wer einen Leihwagen nutzt, koppelt gerne das Smartphone mit dessen Freisprecheinrichtung. Das sollte allerdings bei Abgabe des Autos auch wieder rückgängig gemacht werden!

Früher kostenpflichtiges Zubehör, heute Standard in so gut wie jedem Fahrzeug: Die Freisprecheinrichtung sorgt über eine Bluetooth-Verbindung zwischen Fahrzeug und Smartphone dafür, dass beim Telefonat keine Hände nötig sind (daher auch der englische Begriff "Handsfree") und beide Hände am Lenkrad bleiben können.

Die Bluetooth-Kopplung

Die Verbindung muss einmalig hergestellt werden. Wie bei jeder anderen Bluetooth-Verbindung tauschen Fahrzeug und Telefon einen Schlüssel aus, der am Gerät oder am Fahrzeug bestätigt werden muss. Wie das bei dem speziellen

Fahrzeug geht, ist meist im Unterhaltungssystem ersichtlich oder findet sich im Handbuch. Die Kopplung macht aber meist noch mehr als eine Telefonie-Verbindung herzustellen. Kontakte werden ins Telefonbuch des Fahrzeugs synchronisiert, Nachrichten können vom Telefon auf das Display des Fahrtzieles übertragen werden und mehr. Kurz: Die eigenen Daten kommen auf ein fremdes Gerät!

Daten gehören zur Bluetooth-Partnerschaft

Nun ist es nicht so, dass die Daten für jeden Fahrer frei zugreifbar wären: Alle Daten und Funktionen können nur bei bestehender Verbindung mit dem gekoppelten Telefon verfügbar. Nichtsdestotrotz sind sie im Speicher des Fahrzeugs, der ausgelesen werden kann, und werden nach Abgabe des Fahrzeugs nicht mehr benötigt.Wie immer in solchen Fällen ist dann das Löschen der Daten die beste Lösung!

Im Bluetooth-Menü des Fahrzeuges findet sich die Übersicht aller gekoppelten Telefone. Wird eines davon angewählt, dann kann es dort direkt gelöscht werden.

WinGet: Schnelle Installation von Programmen in Windows 11

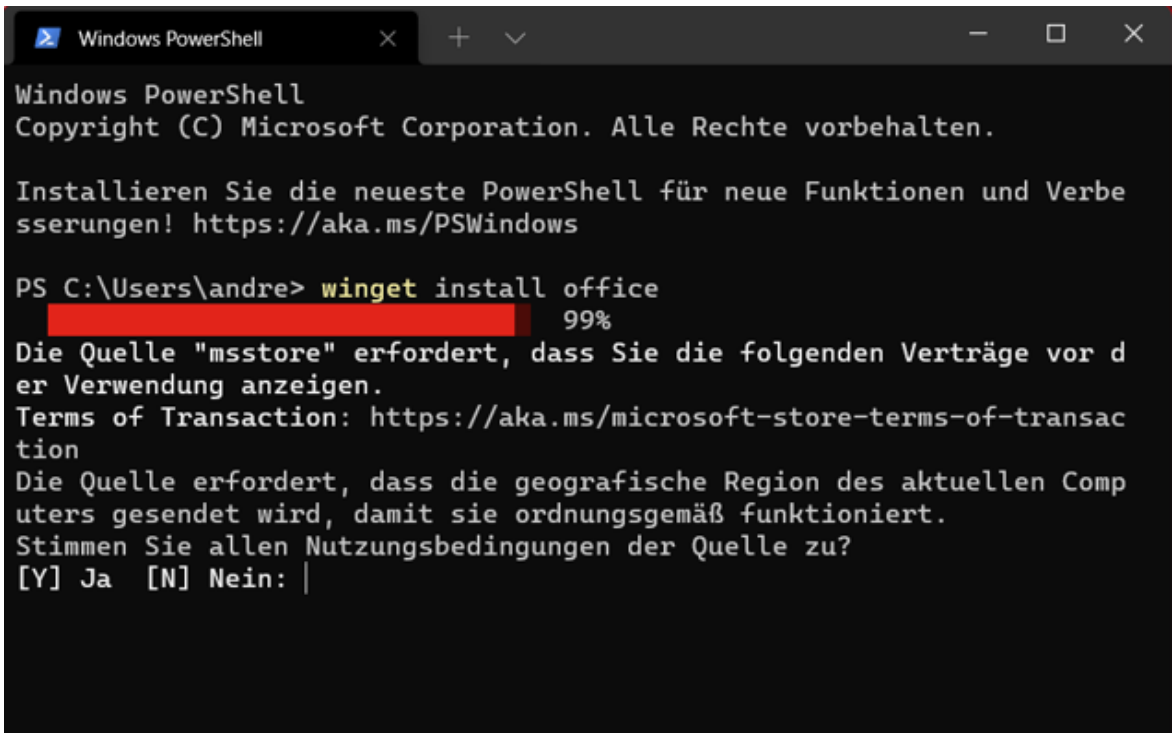
Die Installation von Programmen unter Windows funktioniert im Standard über den Store oder Webseiten. Es geht in vielen Fällen aber auch schneller!

Programme sind das Salz in der Suppe von Windows. Normalerweise führt der Weg dahin über Internetseiten oder den Windows Store, braucht also einige Klicks. Das mag bei spezieller Software, für die vorher eine intensive Suche nötig ist, sinnvoll sein. Bei Standardprogrammen weiß das Betriebssystem aber schon genau, wo es die Software herbekommt. Aus diesem Grund hat Windows 11 eine versteckte Abkürzung mit an Bord, die erstaunlich oft eine Menge Zeit spart.

Installation über die PowerShell

Die Funktion verbirgt sich in der Windows PowerShell, die sich durch die Tastenkombination **Windows** + **X** und einen Klick auf **Windows Terminal** starten

lässt.



Der Befehl **winget install** (wobei der letzte Parameter ersetzt werden muss durch den Namen des gewünschten Programmes) lässt Windows 11 nun diverse Softwarequellen nach dem gewünschten Programm durchsuchen. Dazu gehört der interne Windows Store, aber auch andere vertrauenswürdige Quellen, die Microsoft nicht vollständig offen legt.

Die PowerShell sucht die App heraus, wenn keine passende gefunden wird, erscheint eine Fehlermeldung auf dem Bildschirm. I, positiven Fall startet die Installation nach einer Bestätigung durch den Benutzer. Selbst die Lizenzvereinbarung, die bei der Installation des Programmes zwingend zu akzeptieren ist, kann PowerShell einholen! Windows 11 führt die Installation des Programmes dann durch, als wäre es manuell aus dem Store heruntergeladen worden.