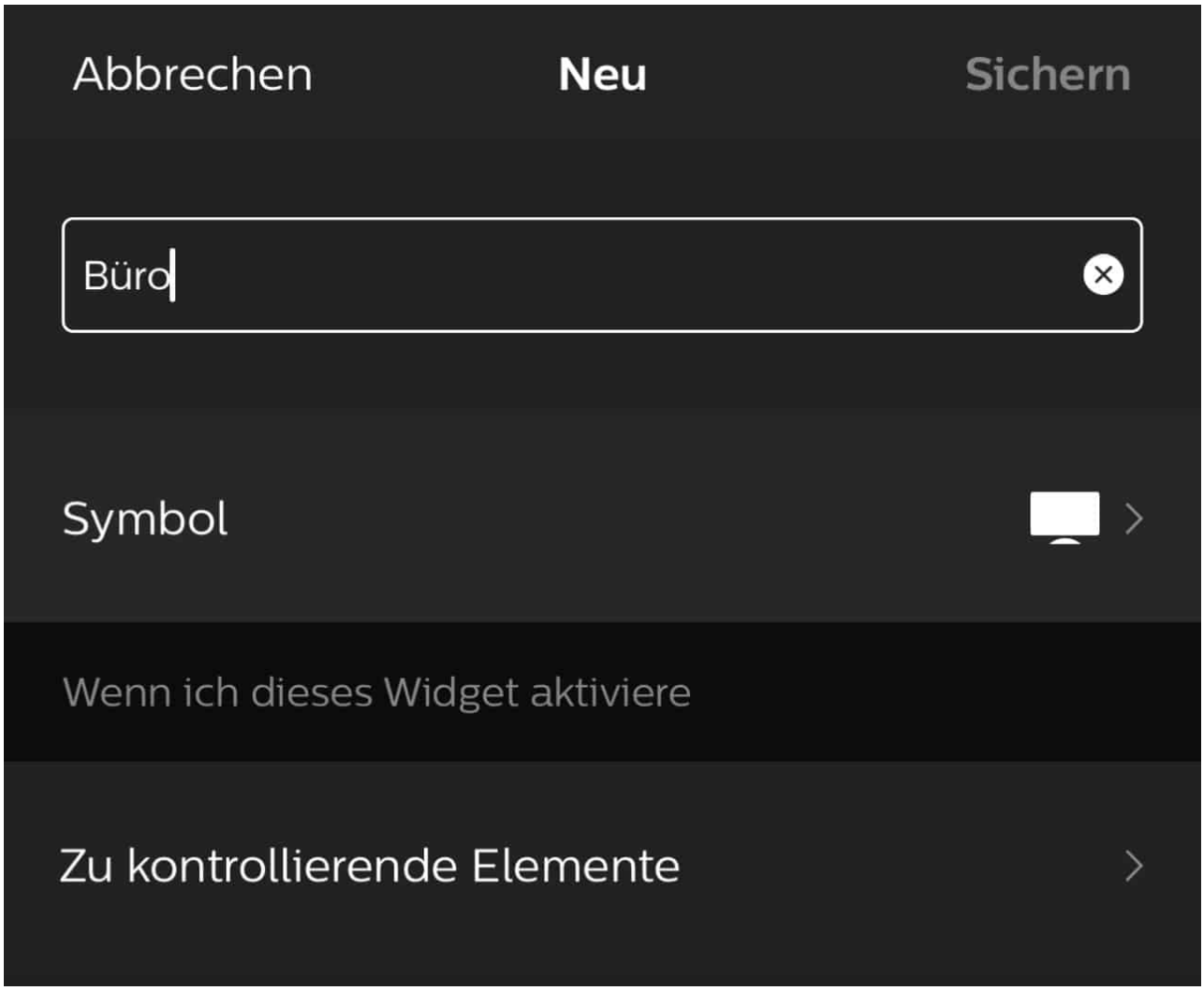
Schieb Report

Ausgabe 2020.49

Anlegen von Widgets für Hue-Lampen

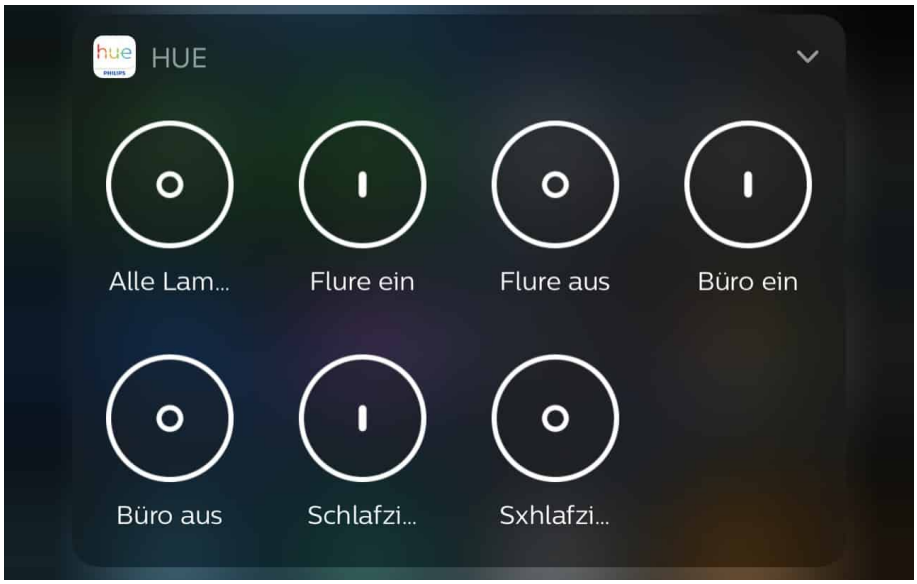
Unser Zuhause verwandelt sich mehr und mehr zu einer Bühne für elektronische Spielereien. Wer steht heute noch von der Couch auf und schaltet das Licht ein oder aus? Smarte Beleuchtung wie Philips Hue und entsprechende Apps erleichtern uns das Leben durchaus. Wenn auch um den Preis der weniger werdenden Bewegung! iOS und iPadOS 14 gehen jetzt noch einen Schritt weiter und ersparen Ihnen durch Widget sogar den Start der Hue-App!

Wie so oft hat Apple uns Funktionen als revolutionär neu verkauft, die anderenorts schon lange bekannt sind. Die Widgets, kleine, bedienbare Informationsfelder auf dem HomeScreen, gehören bei Android schon lange zum Standard. Für Apple-Geräte sind sie aber neu. Um diese zu Steuerung Ihrer Lampen verwenden zu können, müssen Sie zuerst in die Einstellungen der Hue-App gehen und dort auf **Widgets & Apple Watch** tippen.



Dort tippen Sie auf **Widget erstellen** und geben dem neuen Widget einen **Namen** und ein **Symbol**. Wählen Sie nun die Zimmer aus, die über das Widget ein- oder ausgeschaltet werden sollen. Wenn Sie das getan haben, dann können Sie die Szene auswählen, die geschaltet werden soll. Das kann eine vordefinierte Szene sein, aber auch das Ausschalten der Lampen in dem Raum.

Sinnvollerweise erstellen Sie immer zwei Widgets: Einmal eines zum Einschalten des Raumes, ein anderes zum Ausschalten. Achten Sie auch auf die Reihenfolge der Anlage: Die Widgets erscheinen dann im HomeScreen des iPhones oder iPads in der Reihenfolge, in der Sie sie angelegt haben. Das lässt sich später nicht mehr verändern.


HUE
Alle Lam...
Flure ein
Flure aus
Büro ein
Büro aus
Schlafzi...
Sxhlafzi...

Die Corona-Warn-App im Ausland

Eine der wichtigen Empfehlungen der Behörden in Zeiten der Pandemie: „Bleiben Sie zuhause“, oder formeller: „vor nicht notwendigen, touristische Reisen wird gewarnt“. Was bei einem Wochenendabstecher an die See noch vernünftig und nachvollziehbar erscheint, ist in anderen Bereichen kaum machbar. Wie funktioniert die Corona-Warn-App im Ausland?

Wer im Grenzland wohnt, fährt zur Arbeit oder zur Familie in ein anderes Land. Unternehmen mit Niederlassungen im Ausland können nicht alle Tätigkeiten per Videokonferenz erledigen und vieles mehr. Es macht also Sinn, die Begegnungen mit anderen Menschen und deren Smartphones mit der Corona-Warn-App auch grenzübergreifend abzugleichen. Das war nicht von Anfang an vorgesehen, sondern ist erst mit der Version 1.5 der App implementiert worden.

Die gute Nachricht: Für diesen grenzübergreifenden Datenaustausch brauchen Sie keine separate App zu installieren, sondern einfach nur über ein Update Ihre deutsche Corona-App aktualisieren.

Verschiedene Modelle

Die Basis für den Datenaustausch ist der sogenannte European Federation Gateway Service, das EU-Datenabgleichssystem. Für dessen Entwicklung waren ebenfalls die Deutsche Telekom und SAP verantwortlich, die ja auch federführend bei der Entwicklung der Corona-App selbst waren.

Für den Austausch der Daten gibt es drei Modelle. Welches davon verwendet wird, entscheidet jeweils die in einem Land zuständige national Behörde, in Deutschland also das Robert Koch-Institut.

Modell 1: Die Benutzer teilen und empfangen Daten Europaweit.

Modell 2: Die Nutzer entscheiden, ob ihre Kennungen nur national oder auch international geteilt werden sollen.

Modell 3: Die nutzen können entscheiden, mit welchen Ländern – zusätzlich zum Heimatland – die Daten geteilt werden.

In Deutschland findet das effektivste Modell 1 Anwendung. Das kann sich mit kommenden App-Updates aber natürlich mit der Zeit ändern.

Welche Staaten sind dabei?

Die Version 1.5 der Corona-Warn-App, mit der der Europäische Datenaustausch möglich ist, ist Anfang Oktober veröffentlicht worden. In dieser ersten Version war der Austausch nur zwischen Deutschland, Italien und Irland möglich.

Mittlerweile sind weitere Länder hinzugekommen, mit dem Ziel, möglichst viele Länder in diesen Datenaustausch aufzunehmen. Das geht natürlich nur, wenn die Technik identisch ist und sich das jeweilige Land für die dezentrale Speicherung der Daten entschieden hat. Eine Zusammenarbeit mit Frankreich fällt damit zum Beispiel schon einmal aus: Die französische Corona-App setzt auf die zentrale Speicherung der Begegnungsdaten.

Sie können direkt in der App nachschauen, welche Länder aktuell an der länderübergreifenden Risikoermittlung teilnehmen. Dazu tippen Sie auf den Link zur **Risiko-Ermittlung** im Hauptbildschirm der App. Dann tippen Sie auf **Länderübergreifende Risikoermittlung/Teilnehmende Länder** und die App

zeigt Ihnen die teilnehmenden Länder der aktuellen App-Version an.

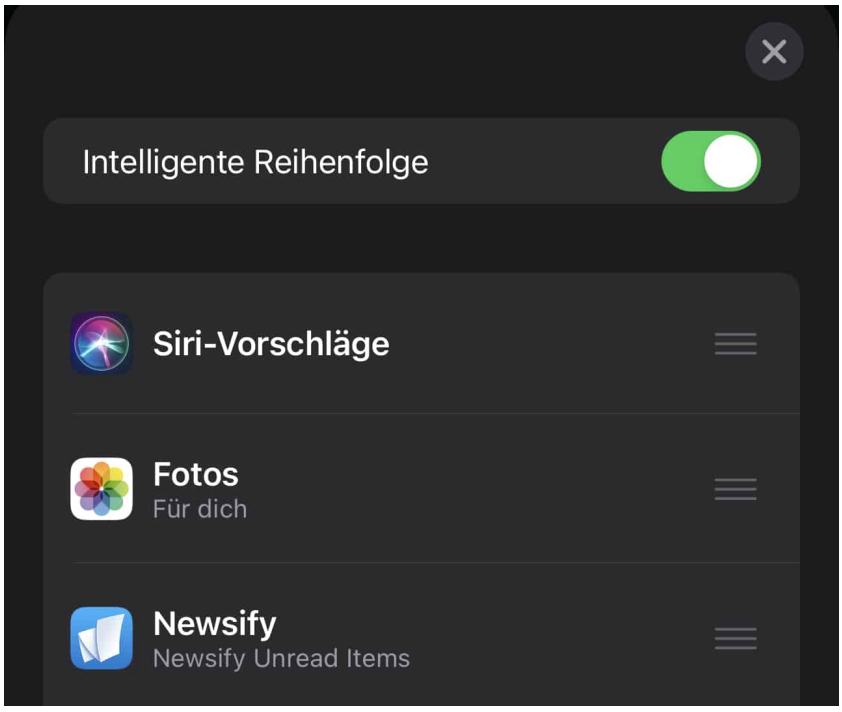
Erzeugen von Smart-Stapeln bei iOS und iPadOS

Widgets sind seit iOS und iPadOS 14 eine der Neuerungen auf Apple-Geräten. Im Gegensatz zu Android, wo es diese Funktion schon seit Jahren gibt, ist die Umsetzung bei iOS noch rudimentär. Vor allem, weil noch nicht allzu viele Apps Widgets unterstützen. Trotzdem können Sie auf Ihrem iPhone und iPad einiges damit machen, wenn Sie die Smart-Stapel nutzen.

Die Idee ist einfach: Sie wollen so wenig wie möglich Platz auf dem HomeScreen verschwenden, aber gleichzeitig so viele Informationen wie möglich unterbringen. Bei Apps gibt es dazu die Stapel, wo sich in einem Symbol mehrere Apps verbergen. Für Widgets funktioniert das ähnlich:

Halten Sie den Finger auf einem freien Bereich eines HomeScreens, bis dieser in den Wackelmodus geht. Dann tippen Sie auf das **Plus-Zeichen** oben links. Wählen Sie ganz oben den Smart-Stapel aus und legen Sie seine Größe fest.

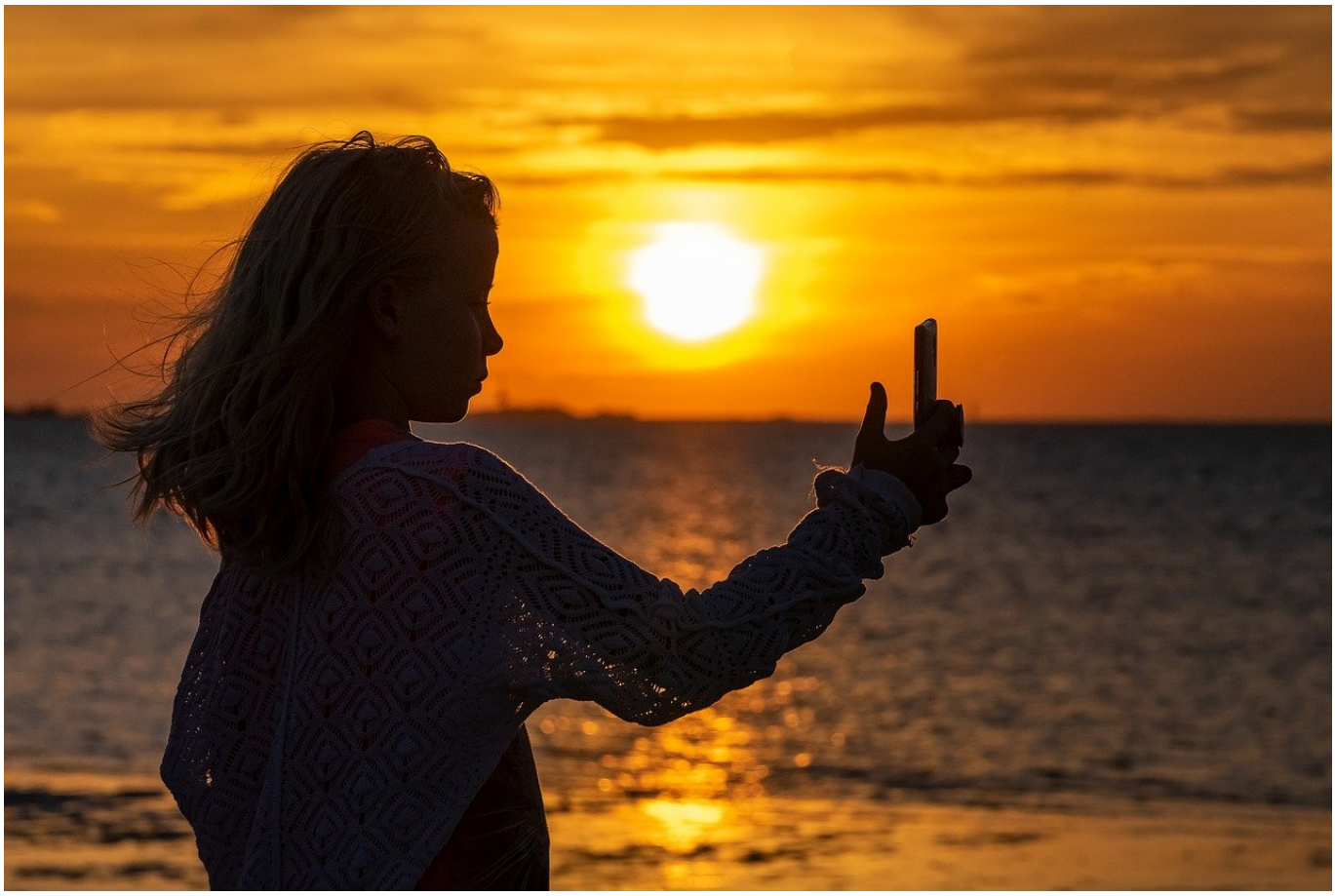
Im Standard sind schon verschiedene Widgets im Smart-Stapel. Wie bei Apps können Sie nun beliebige Widgets in den Smart-Stapel schieben. Um diesen Smart zu machen, bearbeiten Sie ihn. Dazu halten Sie den Finger einen Moment auf das Symbol, dann wählen Sie **Stapel bearbeiten**.



Aktivieren Sie Intelligente Reihenfolge, dann wählt iOS in der Anzeige immer das Widget aus, was anhand unterschiedlicher Faktoren (wie Ihrem

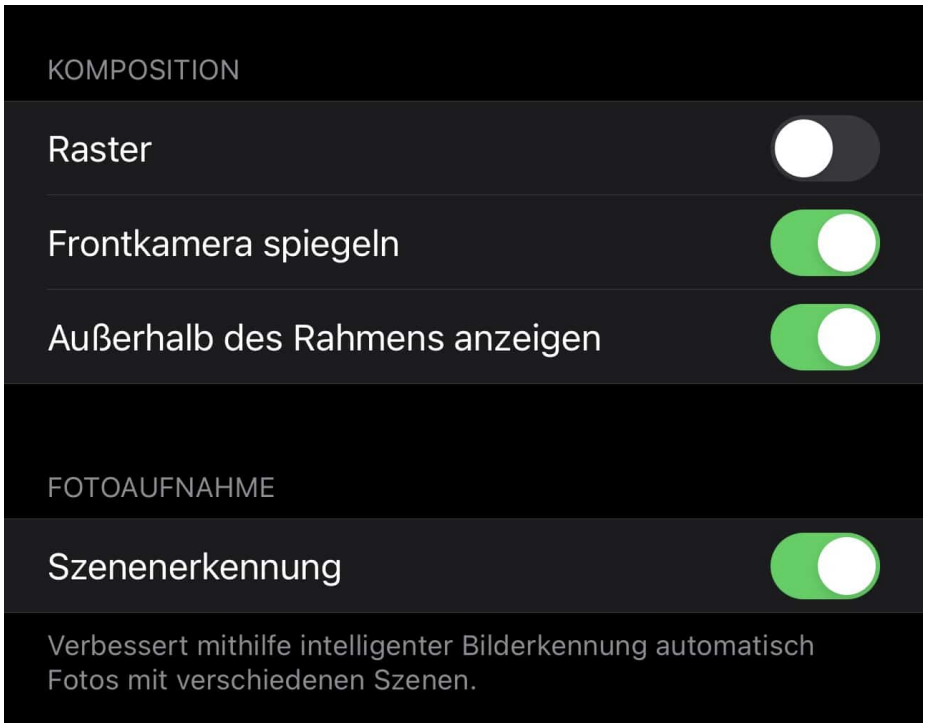
Nutzungsverhalten, Tageszeit, neue Inhalte) gerade wichtig erscheint.

Wenn das Selfie-Bild spiegelverkehrt ist



Sie einen sehen es als Unsitte, die anderen als erweiterten Teil ihrer Persönlichkeit: Das Selfie. So gut wie jedes Smartphone hat neben der Fotokamera im Display eine zweite Kamera, die von Linse und Sensor speziell für Aufnahmen der Personen vor dem Display ausgelegt ist. Ob Foto oder Facebook Live-Video, die Bilder sollten der Realität entsprechen und nicht spiegelverkehrt sein. Wir zeigen Ihnen, wie Sie bei iOS Einfluss nehmen können.

Wenn Sie Ihr eigenes Bild auf dem Display durch die Frontkamera sehen, dann ist dieses gespiegelt. Das fällt auf den ersten Blick nicht auf, nur dann, wenn Sie einen Text im Hintergrund haben oder eine Frisur, bei der der Scheitel in die eine oder andere Richtung geht. Wichtig ist hier aber vor allem, dass das Endergebnis (also das geschossene Foto oder der Video-Feed) stimmt. Wenn das auch nicht stimmt, dann können Sie das in den Kameraeinstellungen ändern.



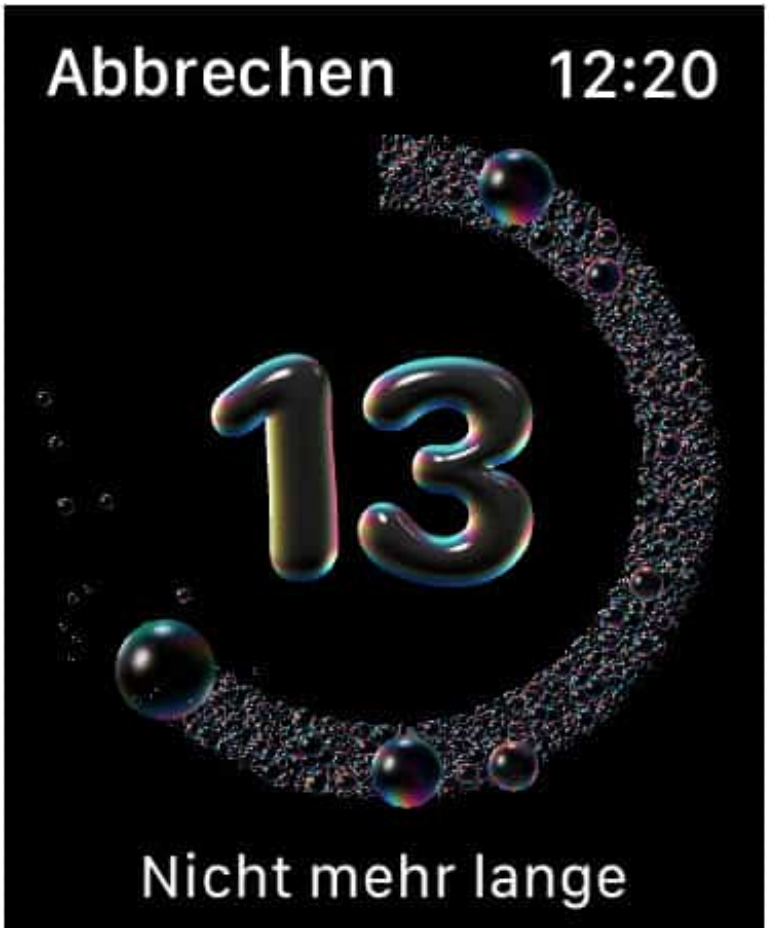
Unter **Einstellungen** > **Kamera** finden Sie einen Schalter **Frontkamera spiegeln**. Ist dieser ausgeschaltet, dann sollte das Bild/Video nicht gespiegelt (und damit wie im Original) sein. Wenn eine App aber manuell das Bild spiegelt, dann ist die Darstellung gegebenenfalls trotzdem falsch. Ändern Sie dann an die Schalterstellung und versuchen Sie es erneut!

Smartes Händewaschen mit der Apple Watch

Das regelmäßige Waschen der Hände ist und bleibt eines der zentralen Hilfsmittel, um eine Ansteckung mit dem Corona-Virus zu vermeiden. Auch wenn das schon vor der Pandemie eine Selbstverständlichkeit war, so können Sie sich noch nicht freisprechen, es immer mal wieder zu vergessen.

Auch die richtige Länge des Waschvorgangs ist ein Thema: Immer wieder finden Sie als Tipp, einfach zweimal „Happy Birthday“ zu singen. Das dauert erfahrungsgemäß 20-30 Sekunden und damit lange genug, um die Hände auch richtig gewaschen zu haben.

Alles unnötig, wenn Sie eine Apple Watch haben. Die kann nämlich erkennen, wenn Sie Ihre Hände waschen und dann einen automatischen Timer starten. Noch besser: Wenn Sie es wollen, erinnert die sie auch umgehend daran, wenn Sie zuhause angekommen sind und nicht nach kurzer Zeit Ihre Hände gewaschen haben. Komfortabler geht es kaum!



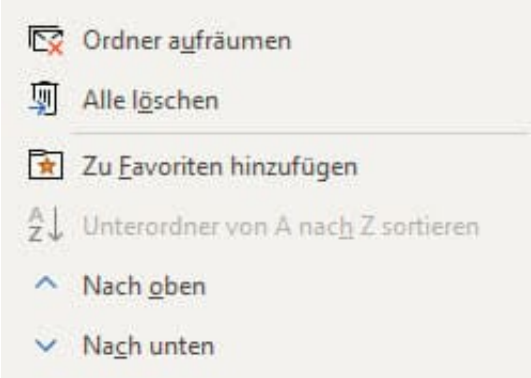
Zur Aktivierung der Funktion müssen Sie einmal auf dem iPhone in die Apple Watch-App gehen und dort unter Meine Watch relativ weit unten auf **Händewaschen** tippen. Aktivieren Sie Timer fürs Händewaschen, damit Ihre Apple Watch beim Erkennen des Händewaschens automatisch einen 20 Sekunden-Timer startet. Ist der abgelaufen, dann bekommen Sie sowohl ein Ton- als auch ein Vibrationssignal.

Aktivieren Sie zusätzlich **Erinnerungen fürs Händewaschen**, dann müssen Sie einmalig die Positionsnutzung freigeben. WatchOS wartet dann bei Erreichen Ihres Heimatortes einen Moment ab und schickt Ihnen dann eine Erinnerung ans Waschen der Hände, wenn der Vorgang nicht erkannt wird. So können Sie das regelmäßige Händewaschen kaum mehr vergessen!

Verwalten von Outlook-Favoriten

Je mehr und je länger Sie mit Outlook arbeiten, desto mehr wird es wichtig, Ordnung zu halten. Ein Posteingang, der ungefiltert alle E-Mails enthält, ist schnell unübersichtlich. Wenn Sie eine bestimmte E-Mail suchen, dann kostet Sie das unnötig Zeit. Die Lösung: Legen Sie Favoriten an, auf die Sie schneller zugreifen können.

Favoriten sind Platzhalter für Ordner in der Ordnerstruktur von Outlook, vergleichbar mit den Verknüpfungen im Explorer und dem Desktop von Windows. Um einen Ordner zum Favoriten zu erklären, klicken Sie mit der rechten Maustaste auf seinen Namen und dann auf **Zu Favoriten hinzufügen**. Der Ordner taucht dann zusätzlich zu seinem Originalort auch noch einmal unter **Favoriten** auf.



Alternativ ziehen Sie einen Ordner aus dem normalen Ordnerbereich in den Bereich Favoriten. Hier sollten Sie aber vorsichtig sein: Wenn Sie die Maustaste versehentlich zu früh loslassen, verschieben Sie gegebenenfalls den Originalordner!

Um einen Favoriten wieder zu entfernen, klicken Sie in mit der rechten Maustaste an und dann auf **Aus Favoriten entfernen**. Dadurch wird der Originalordner natürlich nicht verändert oder gelöscht!

Wenn Dokumente in Teams zu klein sind

Termine nicht mehr vor Ort, sondern per Videokonferenz durchzuführen, gehört zur neuen Realität. Programme wie Zoom oder Microsoft Teams erlauben nicht nur die Kommunikation zwischen den Teilnehmern, sondern auch die gemeinsame Diskussion über Dokumente. Teilen Sie den Bildschirm und schon reden alle Teilnehmer über das selbe. Dumm nur, wenn Sie das Dokument kaum lesen können, weil es zu klein ist. Wir zeigen Ihnen, wie Sie bei Teams die Darstellung verbessern können.

Der erste Schritt ist meist die Frage an den Vortragenden, ob er die Darstellung vergrößern kann. Das geht über die Zoom-Funktionen der Programme und Apps, mit denen das Dokument dargestellt wird. Oft ist das aber nicht der richtige Weg: Eine Vergrößerung der Darstellung bedeutet gleichzeitig eine Verringerung des sichtbaren Details. Das ist unnötig, solange Teams noch Bildschirmplatz mit eigenen Elementen verschwendet. Die großen Symbole oder Videobilder nehmen unnötig Platz weg, ebenso die Symbolleisten. Entfernen Sie diese in den Einstellungen von Teams.

Klicken Sie dazu auf die drei Punkte, dann auf **Vollbild**, um die Symbole von Teams zu minimieren. Klicken Sie im selben Menü auf **Fokus**, um das Dokument vergrößert darzustellen. Dieses nimmt dann den maximal verfügbaren Platz auf dem Desktop ein.

Wie nachhaltig ist Digitalisierung eigentlich?

Das Schlagwort "Digitalisierung" ist in aller Munde: Auch die Kanzlerin fordert mehr Tempo bei der Digitalisierung. In einiger Hinsicht will man ihr da auch zustimmen - aber nicht in jeder Hinsicht. Denn es geht nicht nur um ein Mehr von allem. Manchmal geht es auch um ein weniger. Vor allem, wenn es um die Nachhaltigkeit geht. Denn dieser Aspekt wird häufig vernachlässigt.

Digitalisierung und Nachhaltigkeit: Das sind die beiden Schwerpunktthemen auf dem Digitalgipfel dieses Jahr, der heute (01.12.2020) endet. Es geht vor allem darum, wie Digitalisierung helfen kann, unsere Alltagsaufgaben besser zu lösen.

Etwa: Können Drohnen in der Landwirtschaft helfen, lassen sich mit KI Verkehrsströme optimieren - und kann man so Energie sparen? Es gibt zweifellos viele interessante Ansätze. Es geht darum, die Richtigen rauszupicken und loszumarschieren.

Digitalisierung birgt auch viele Nachteile

Gleichzeitig ist Digitalisierung aber auch eine enorme Herausforderung - denn es sind auch viele Nachteile damit verbunden. Allen voran der enorme

Energiebedarf: Rechenzentren verbrauchen sehr viel Energie. Jetzt schon rund 2,7% des europäischen Strombedarfs. Tendenz: Steigend. Die EU will das ungebremste Wachstum des Energiehungers eindämmen. Aus ökologischen Gründen. Das ist richtig und wichtig - und damit auch Thema auf dem Digitalgipfel.

Viel zu wenig beachtet bislang ist aber auch die Frage, wo all die Rohstoffe herkommen, die in moderner Technologie verbaut sind: Seltene Erden und seltene Metalle vor allem. Sie werden teilweise unter räuberischen Bedingungen abgebaut, in China, in Chile, in Afrika. Mit umweltzerstörerischen, gesundheitsschädlichen und menschenverachtenden Methoden.

Niemand spricht über Ressourcenverschwendung

Die uneingeschränkt empfehlenswerte Dokumentation auf ARTE belegt: Wir belügen uns alle selbst, wenn wir glauben, den ökologischen Wandel gäbe es wirklich. Moderne Technologie - und auch die Digitalisierung - fordern ihren Tribut. Und die Politik schaut weg. Das gehört zur Nachhaltigkeit zweifellos dazu, ist aber auf dem Digitalgipfel vermutlich kein Thema. Denn mit den Fragen des

Ressourcenabbaus und der Ressourcenverschwendung beschäftigt sich Politik nicht gerne.

Dafür in diesem Jahr mit einem anderen Aspekt (denn dafür gibt es Applaus): Der bessere Schutz von Plattform-Beschäftigen. Die Digitalisierung sorgt für viele prekäre Beschäftigungen, ob im Lieferbetrieb oder als Uber-Fahrer.

Nachhaltigkeit: Nicht nur Umweltschutz

Es gibt heute viele sogenannnte "Solo-Selbständige" (auch so ein Unwort, weil es nach Freiwilligkeit und Selbstbestimmung klingt, nicht nach Ausbeutung und sozialem Verfall), die von Plattformen abhängig, aber dort nicht richtig beschäftigt sind. Und auch Mitarbeiter von Amazon werden überwacht - und sind nicht unbedingt in jeder Hinsicht zu beneiden. Digitalisierung bedeutet allzu häufig Turbokapitalismus pur: Die einen verdienen, die anderen zahlen die Zeche. Umwelt inklusive.

Es ist richtig und wichtig, da genau hinzuschauen. Ich habe zwar ernsthafte Zweifel, dass sich am Wesen der Probleme wirklich etwas ändern. Aber genau das muss dringend passieren.

Amazon bespitzelt Mitarbeiter, Partner und Kunden

Online-Security in Unternehmen kann nicht hoch genug priorisiert werden

Wer im Internet unterwegs ist, der muss sich absichern. Das gilt erst recht für Unternehmen, die mit eigenen Webangebotem im Netz vertreten sind - oder vielleicht sogar auch noch anderweits ans Netz angebunden sind. Die Gefahren sollten auf keinen Fall unterschätzt werden: Cyberkriminelle nutzen früher oder später jedes Sicherheitsleck.

Dass Online-Tools, Cloud-Dienste, eine Website und eine gute technische Infrastruktur heute zur Grundausstattung praktisch jedem Unternehmens gehören, dürfte klar sein. Leider werden dabei allerdings Security-Aspekte nach wie vor deutlich unterschätzt. Grundsätzlich gilt: Jede Website muss heute angemessem abgesichert sein. Ein Hackerangriff kann heute einfach zu großen Schaden anrichten. Suchmaschinen wie Google strafen gehackte Webseiten ab.

Auch, wenn Unternehmen für Cyberattacken sensibilisiert sind, bleibt dies oft eine

Sache der Chefetage. Dabei sollten Programmierer und auch das Online-Marketing das Thema ebenfalls auf dem Schirm haben. Doch was ist dabei zu beachten und wie lässt sich Online-Security durchsetzen?

Abbildung 1: Online-Security wird für Unternehmen mehr und mehr zur Überlebensfrage. doch was ist dabei zu beachten?
Bildquelle: @ Philipp Katzenberger / Unsplash.com

Studie: Wie steht es um KMUs und Mittelständler?

Ein genauer Blick auf die Lage in Sachen Cyber-Security bei KMUs und Mittelständlers zeigt, wie ernst die Lage ist. So berichten laut einer Studie des GDV 30% der befragten Unternehmen von wirtschaftlichen Schäden durch Cyberattacken. Zusätzlich ergab sich, dass die Größe des Unternehmens in Zusammenhang mit dem Erfolg von Cyberattacken steht: Je kleiner das Unternehmen, desto eher kommen die Angreifer durch. Die wirtschaftlichen Schäden nehmen dabei ganz unterschiedliche Formen an:

- Kosten für Aufklärung und Datenwiederherstellung (59%)
- Unterbrechung des Betriebsablaufs (43%)

- Reputationsschaden (14%)
- Diebstahl von Kunden- oder Kreditkartendaten (11%)

Trotzdem sehen sich 73% aller Unternehmen ausreichend gegen Cyberattacken geschützt. Hier zeigt sich, dass diese Einschätzung nicht in jedem Fall den Tatsachen entspricht und noch Nachholbedarf besteht.

Häufige Angriffe im Bereich Cyber-Kriminalität

Das Instrumentarium von Hackern für Cyberattacken zeigt sich mittlerweile als außerordentlich vielseitig. Zu den häufigsten Aktionen gehören:

- Social Engineering (Phishing und betrügerische Websites)
- Typ der Malware-Infizierung: Serverkonfiguration
- Typ der Malware-Infizierung: SQL-Einschleusung
- Typ der Malware-Infizierung: Code-Einschleusung
- Typ der Malware-Infizierung: Fehlervorlage
- Websiteübergreifende Malware-Warnungen
- Typ des Hacks: Code-Einschleusung
- Typ des Hacks: Einschleusung von Inhalten
- Typ des Hacks: URL-Einschleusung

Phishing per Mail und auch das Nachstellen bekannter Websites zum Datenabgriff dürften den meisten Mitarbeitern mittlerweile bekannt sein. Trotzdem fallen nach wie vor recht viele Geschädigte darauf herein. Dies mag aber auch an der Tatsache liegen, dass die Angriffe immer besser werden und professioneller aussehen.

Was sagt Google zum Thema Cybersicherheit?

Wer sich mit Suchmaschinenoptimierung (SEO) beschäftigt, weiß mittlerweile, dass eine grundlegende Absicherung der Website ein Ranking-Kriterium darstellt. Leider verstehen die meisten darunter lediglich die Einrichtung eines Sicherheitszertifikates (SSL). Doch diese Maßnahme ist allein nicht ausreichend. Auch eine grundlegende Absicherung wird mittlerweile vorausgesetzt. Im Umkehrschluss bedeutet das: Gehackte Websites werden von Google abgestraft, weil sie für Nutzer eine negative Nutzererfahrung mit sich bringen.

Beispiel in Kurzform

Ein Beispiel zeigt sich an folgendem Screenshot:

Das Unternehmen wurde bereits wenige Tage nach dem launch Opfer eine Hacker-Attacke und wurde deshalb von Google deindexiert. Somit waren die Kosten für die Entwicklung der Website nur der Anfang. Zusätzlich musste großer Aufwand betrieben werden, um den Fehler zu finden. Ohne Backups entsteht zudem das Problem, dass man nicht einfach zu einem vorigen Punkt zurückspringen kann.

Darüber hinaus besteht danach das Google-Problem zunächst weiter. Nach der Bereinigung müssen betroffene Unternehmen für die eigene Website zunächst einen Reconsideration Request stellen. Dabei prüft Google erneut, ob alle Probleme ausgeräumt wurden. Ist das der Fall, wird die Seite erneut freigegeben. Dies kann mitunter mehrere Wochen dauern, wenn man auf die Hilfe von Profis verzichtet. Doch hier gilt: Zeit ist Geld!

Wichtig: *Schädliche Dateien von Hacker lassen sich nicht immer so einfach finden. Mitunter schlummern diese Schadprogramme mehrere Wochen, bevor sie zum Einsatz kommen. Aus diesem Grund ist es sinnvoll, täglich Backups anzufertigen und im Notfall auch einmal auf ein Backup von vor mehreren Wochen zurückzugreifen. Das ist immer noch günstiger, als komplett von vorn beginnen zu müssen.*

Geeignete Schutzmaßnahmen für Unternehmen

Wenn Unternehmen das Thema Online-Security richtig angehen wollen, muss dieser Aspekt von Anfang Teil der Website- und Shop-Entwicklung sein. Vorsicht ist besser als Nachsicht und hilft dabei, Hackangriffe deutlich zu erschweren. Bei der Beauftragung eines Programmierers sollte die Security gleich Teil des Angebots sein. Zusätzlich sollten Unternehmen eine genaue Erklärung einfordern, wie das Ganze sichergestellt wird. Somit lässt sich sicherstellen, am Ende auf seriöse Anbieter zu setzen, die wirklich im Sinne der Sicherheit des Unternehmens handeln.

Zusätzlich sind folgende Maßnahmen sinnvoll:

- **Regelmäßige Überprüfung:** Eine regelmäßige Prüfung der Online-Security der eigenen Website sollte als Standard im Unternehmen implementiert wird. Nur so lässt sicherstellen, dass die Sicherheitsmechanismen noch greifen. Da Hacker sich auch immer weiterentwickeln, ist es sinnvoll, durch eine Überprüfung mögliche Lücken frühzeitig zu entdecken und zu schließen. Hierbei sind auch Tools wie der Website Security Check der OSG hilfreich, die einen kostenlosen Check ermöglichen. So lassen sich Schwachstellen schnell und sicher identifizieren.
- **Mit Rechtervergabe arbeiten:** Eine gute Praxis bei der Rechtevergabe sorgt dafür, dass nur sachkundige Personen systemrelevante Änderungen durchführen dürfen. Dies bleibt dann zum Beispiel der IT-Abteilung vorbehalten, während der Praktikant zum Beispiel nur eine Freigabe für seinen Arbeitsbereich erhält. Dies erfordert vorher natürlich eine genaue Planung, wer wann welche Zugangsberechtigungen benötigt.

Wer diese Maßnahmen beachtet, kann eine gute Basis in Sachen Online-Security legen und somit zum Teil hohe wirtschaftliche Schäden vom eigenen Unternehmen abwenden.

Abbildung 2: Wird der Sicherheitsgedanke bereits bei der Programmierung beachtet, lassen sich Sicherheitslücken deutlich besser abdecken. Bildquelle: @ Markus Spiske / Unsplash.com

Fazit: Online-Security niemals unterschätzen

Die obigen Studien zeigen sehr eindrucksvoll, welche Schäden ein Hackerangriff auf die Website oder den Shop eines Unternehmens haben können. Darüber hinaus existiert jedoch eine erschreckend hohe Zahl an Unternehmen, die sich in Sachen Sicherheit gut aufgestellt sehen und das Problem zu unterschätzen scheinen.

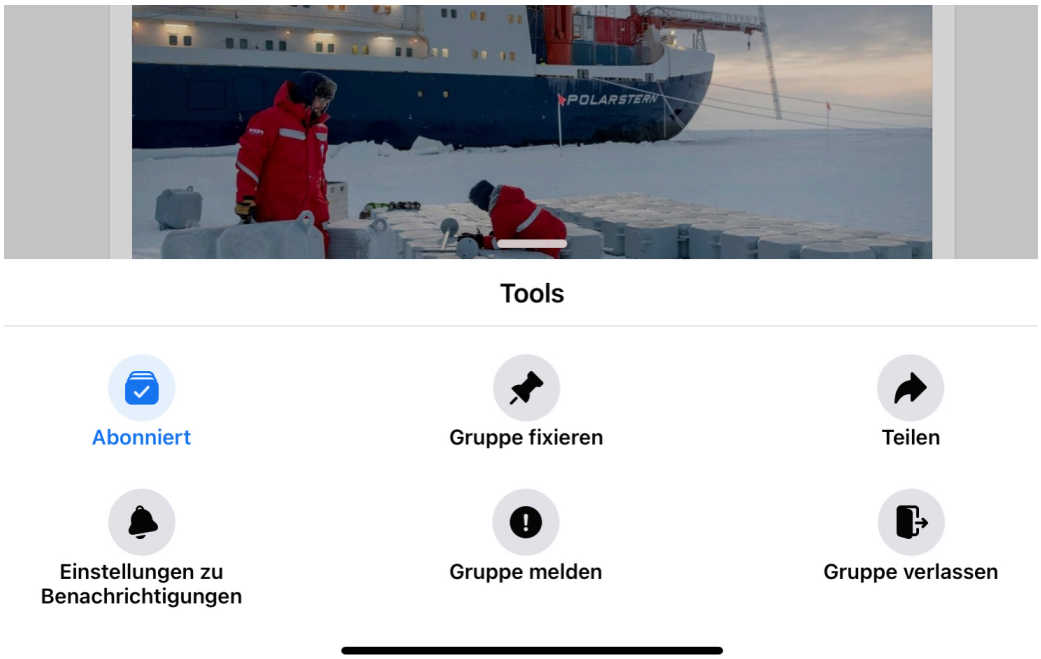
Die Erfahrung zeigt jedoch, dass Online-Security nicht hoch genug auf der Prioritätenliste stehen kann. Wer diesen Gedanken gleich bei der Erstellung von Website oder Online-Shop einfließen lässt, regelmäßig Überprüfungen durchführt und zudem die Zugangsrechte geschickt vergibt, kann bereits eine gute Basis in Sachen Security legen. Dies ist zusätzlich auch im Hinblick auf SEO wichtig, da die entsprechenden Bereiche sich auch auf das Ranking auswirken können. Bei einer Online Marketing Agentur erhält man eine kompetente Beratung rund um

alle Bereiche der Online-Security.

Wenn Facebook-Beiträge in Gruppen nicht funktionieren

Facebook-Gruppen haben schon lange die Funktion der virtuellen Kneipe um die Ecke übernommen: Sie schauen vorbei, halten ein kurzes Schwätzchen, schauen sich an, was es Neues gibt. Sie schaffen es nicht, vorbeizuschauen? Dann helfen Ihnen die automatischen Benachrichtigungen über neue Beiträge. Was aber, wenn diese nicht funktionieren?

Die Benachrichtigungen für neue Beiträge in einer Gruppe sind im Standard vorgegeben, Sie können sie aber selber ändern. Das sollte auch nur durch Sie erfolgen, manchmal greift Facebook aber ohne Information an die Benutzer ein. Das führt dazu, dass Sie plötzlich weniger Benachrichtigungen bekommen und gegebenenfalls interessante Beiträge verpassen.



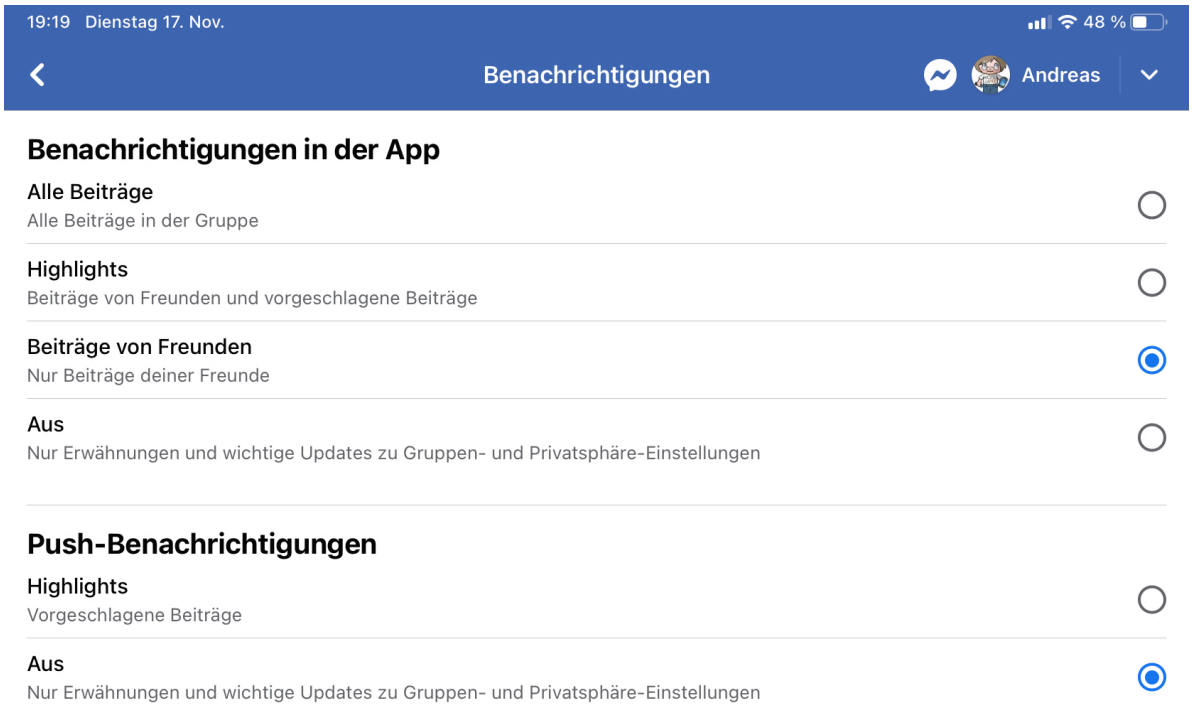
Zur Kontrolle und zur Änderung wechseln Sie in die Gruppe, dann tippen Sie auf die drei Punkte oben rechts in der Facebook-App. Tippen Sie dann auf **Einstellungen für Benachrichtigungen**. Darin finden Sie einen Bereich **Benachrichtigungen in der App**. Hier haben Sie vier Einstellmöglichkeiten:

Alle Beiträge: Sie erhalten eine Nachricht für jeden neuen Gruppenbeitrag.

Highlights: Diese Einstellung präferiert Facebook. Sie bekommen Beiträge von Freunden angezeigt plus Beiträge, die Facebook als interessant einordnet.

Beiträge von Freunden: Sie bekommen in den Benachrichtigungen nur Beiträge von Freunden angezeigt.

Aus: Facebook schickt keine Benachrichtigungen für Gruppenbeiträge.



Die Zahl der angezeigten Benachrichtigungen nimmt von oben nach unten ab. Probieren Sie einfach aus, welche die für Sie richtige Einstellung ist.

Sicheres Surfen im VPN zu Sonderpreisen

Es hat sich mittlerweile herumgesprochen: Ein Virtual Private Network (VPN) schützt beim Surfen im Netz. Der Datenverkehr ist abhörsicher (sogar im offenen WLAN), die eigene Identität ist verschleiert (weniger Tracking und Nachverfolgung) und außerdem können User so ihren Aufenthaltsort ändern. Praktisch, um auf Inhalte zuzugreifen, die nur für bestimmte Regionen zur Verfügung stehen. Wer noch kein VPN hat, kann rund um den Black Friday zu besonders günstigen Konditionen ein VPN einrichten. Cyberghost VPN zum Beispiel gibt es für 2 EUR im Monat - und drei Monate kostenlos.

Früher haben nur Menschen ein VPB benutzt, wenn sie im Homeoffice gearbeitet oder von unterwegs in den Firmenrechner mussten. Heute verwenden viele ein VPN, denn es sind so viele Vorteile damit verbunden.

Wer per VPN im Web surft, setzt sich quasi eine "Tarnkappe" auf: Die Identität lässt sich verschleiern und der Datenverkehr ist weitgehend abhörsicher. Wichtige Vorteile, die man zwar nicht immer braucht - aber wenn, lässt sich das VPN per Mausklick einschalten. Und das nicht nur auf dem PC zu Hause oder auf dem

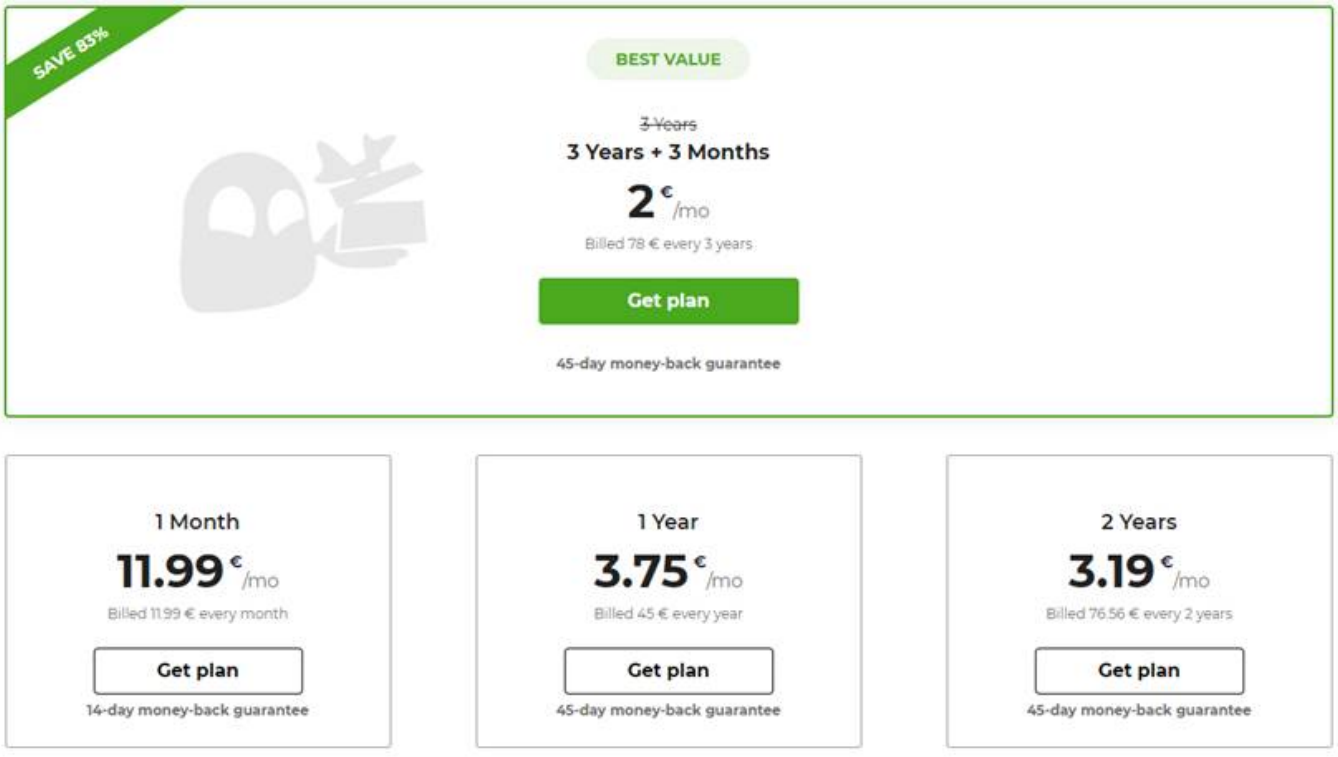
Notebook, sondern selbstverständlich auch auf Mobilgeräten wie Smartphones oder Tablets.

Cyberghost VPN bietet viele Vorteile

In einem VPN wird der Datenverkehr komplett **verschlüsselt**, was ihn abhörsicher macht – sogar in einem offenen WLAN. Zudem wird die eigene Identität verschleiert, weil die eigene IP-Adresse verschwindet. Darüber hinaus lassen sich in einem VPN Inhalte nutzen, die sonst geblockt sind. Eine Menge Vorteile – und einfach handhabbar sind VPNs heute auch.

- Abhörsicher kommunizieren
- Die eigene Identität verschleiern (IP-Adresse)
- Den Aufenthaltsort verschleiern
- Torrent Netzwerke absichern
- Geo-Blocking umgehen
- Zugriff auf 35 Streamingdienste mit Geo-Blockaden weltweit
- Sicher digital bezahlen

Niemand braucht ununterbrochen VPN-Dienste. Aber es gibt immer wieder Situationen, in denen sie nützlich und hilfreich sind.



Die guten VPNs sind kostenpflichtoge Angebote. Die meisten kosten einige EUR pro Monat (wichtig: Nur die guten VPNs verfügen über ausreichend Kapazitäten, damit es beim Surfen nicht zu Beeinträchtigungen beim Tempo kommt). Cyberghost VPN bietet rund um den Black Friday einen wirklich erheblichen Discount von über 80% an (wenn man sich gleich auf drei Jahre festlegt).

ç

Geo-Blocking bei Videos, Audios und Streaming-Diensten

Das Phänomen kennt wohl jeder: “Dieses YouTube-Video ist in Ihrem Land nicht erreichbar”. Oder man kann sich auf Netflix nicht die neuesten Serien anschauen, weil sie in Deutschland noch nicht gezeigt werden dürfen. Oder man bekommt die guten BBC-Sendungen nicht als Stream zu sehen, weil man nicht in England ist.

Das Internet ist eben doch nicht so international und grenzübergreifend wie man immer denkt. Viele Inhalte stehen nur in bestimmten Ländern zur Verfügung.

Hier hilft ein VPN weiter. Wer einen VPN-Anbieter nutzt, kann “so tun als ob”.

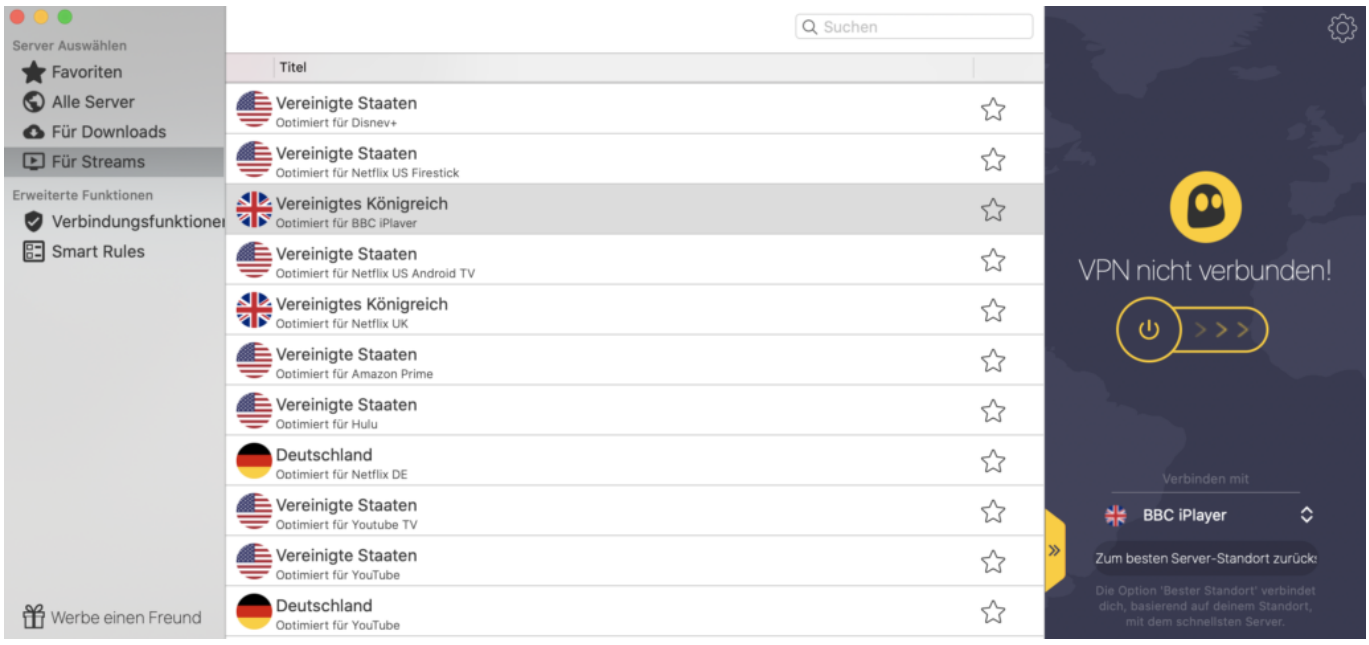
Man kann sich per Mausklick in ein anderes Land begeben, denn man bekommt eine IP-Adresse in einem Land seiner Wahl zugewiesen: USA, Großbritannien, Frankreich, England – wo man will. Vorteil: Schon hat man Zugriff auf Inhalte, die man sonst nicht zu sehen bekommt.

Wer unbedingt die neuesten Serien schauen will, die in den USA deutlich früher starten als hier bei uns in Deutschland/Europa, kennt das Problem: Kein Zugriff. Doch mit einem geeigneten VPN-Dienst wie Cyberghost VPN ist es kein großes Problem mehr: VPN-Dienst starten, die USA als virtuellen Aufenthaltort auswählen - und Netflix präsentiert andere Serien und Filme als in Deutschland.

In Deutschland gibt es nur 20% der Inhalte zu seheb, die Netflix in den USA anbietet. In dieser Übersicht kann man wunderbar nachschauen, wie es ganz konkret aussieht - wie viele Serien und/oder Filme in jedem einzelnen Land zu sehen sind. Wer einen VPN-Dienst nutzt, kann sich schnell und leichter überall "hin beamen" - und so andere Inhalte anschauen.

Zugriff auf Inhalte der BBC

Ich persönlich bin ein Fan der BBC. Leider kann man nur noch auf wenige Audio- und Video-Inhalte der BBC zugreifen, wenn man sich nicht aktuell im Vereinigten Königreich aufhält. Das ist sehr schade, denn es gibt hervorragende Sendungen - auch Talk-Sendungen, die es auf jeden Fall lohnt anzuschauen.



Ich habe mehrere VPN-Anbieter durchprobiert. Nur einer scheint aber auf diese

Situation optimal vorbereitet: CyberGhost VPN. Es gibt sogar eine eigene Einstellung dafür: Wer BBC schauen will, wählt einfach dafür in der Server-Kategorie "Für Streams" aus - und dort den VPN-Server in UK, der speziell für BBC-Streams vorgesehen ist. Und schon ist es möglich, über den BBC iPlayer aktuelle Fernsehsendungen abzurufen - wirklich klasse.

Mehr Sicherheit durch VPN - auch in offenen WLANs

Offene WLANs sind in der Regel ungesichert. Jeder kann rein – ohne Nachfrage, ohne Passwort und auch ohne jede Verschlüsselung. Das macht die Sache zwar sehr einfach – aber leider auch ziemlich riskant. Denn weil die Daten nicht verschlüsselt werden, kann theoretisch jeder im WLAN ohne großen Aufwand alles mithören und mitlesen. Auch sensible Daten.

Wenn man nur ein paar Webseiten ansteuert, ein paar Artikel liest: Kein Problem. Aber sobald man sich irgendwo einloggt oder sensible Daten eingibt, ist Vorsicht angebracht. Bankgeschäfte sollte man im offenen WLAN also besser nicht erledigen. Denn man weiß nie, wer mitliest. Man bekommt es nicht mal mit, wenn jemand in einem offenen WLAN spioniert.

Deshalb Mein Tipp: In offenen WLANs unbedingt ein VPN verwenden. Denn in einem VPN werden alle Daten sicher verschlüsselt. Es gibt Profilösungen, die bieten eine Menge Komfort und erlauben, alle Daten sicher zu verschlüsseln. Doch diese Lösungen kosten Geld und sind nicht immer ganz einfach zu handhaben. Einmal eingerichtet - ob auf dem PC oder Mobilgerät - bemerkt man als Nutzer gar nicht mehr, dass ein VPN einen schützt.

Das ist allerdings nur dann gewährleistet, wenn der VPN-Anbieter eine große Auswahl an Server-Standorten bietet - und diese leistungsfähig genug sind, die Daten schnell weiterzureichen und zu verschlüsseln. Kostenlose oder kleinere VPN-Dienste sind meist langsam. Es ist zu spüren, dass alles langsamer und träger passiert. Wer Pech hat, kann nicht mal mehr Videos ruckelfrei anschauen. Gute VPN-Anbieter haben diesen Nachteil nicht: Hier ist man (fast) genauso schnell unterwegs wie ohne VPN, aber deutlich besser abgesichert.

CyberGhost VPN: Schneller VPN-Dienst mit vielen Funktionen

Nachdem wir uns wirklich viele VPN-Dienste angeschaut haben, empfehlen wir

derzeit CyberGhost VPN. Der Dienst hat mittlerweile 36 Mio. Anwender - und deckt nahezu alle Bedürfnisse ab, die man bei einem VPN-Dienst haben kann.

- Eigene Apps/Software für alle Plattformen: Windows, macOS, Linux, iOS, Android und Apple TV, Amazon Fire TV&FireStick, Xbox, PlayStation und sogar für Router
- Rund 6300 dedizierte VPN-Server in 90 Ländern - also eine riesige Auswahl und Tempo!
- Ein CyberGhost-VPN-Nutzer kann bis zu sieben (7) Geräte gleichzeitig schützen
- Ausprobieren leicht gemacht: Es gibt eine 45-tägige Geld-zurück-Garantie
- Besonders wichtig: Der Anbieter gibt an - keine Logs. Es wird also nichts protokolliert

schieb.de Leser/innen bekommen CyberGhost VPN schon ab 2 EUR.