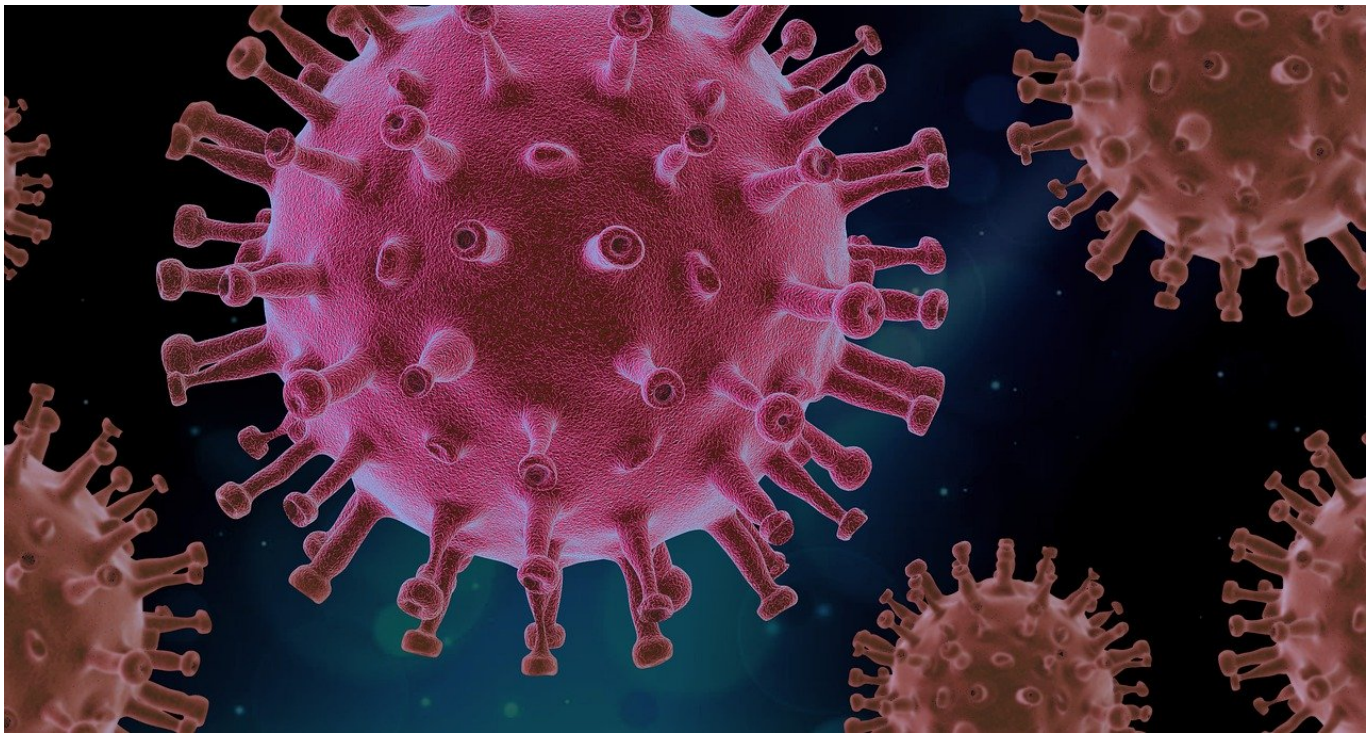
# Schieb Report

Ausgabe 2020.47

# Die Corona-Warn-App und Bluetooth



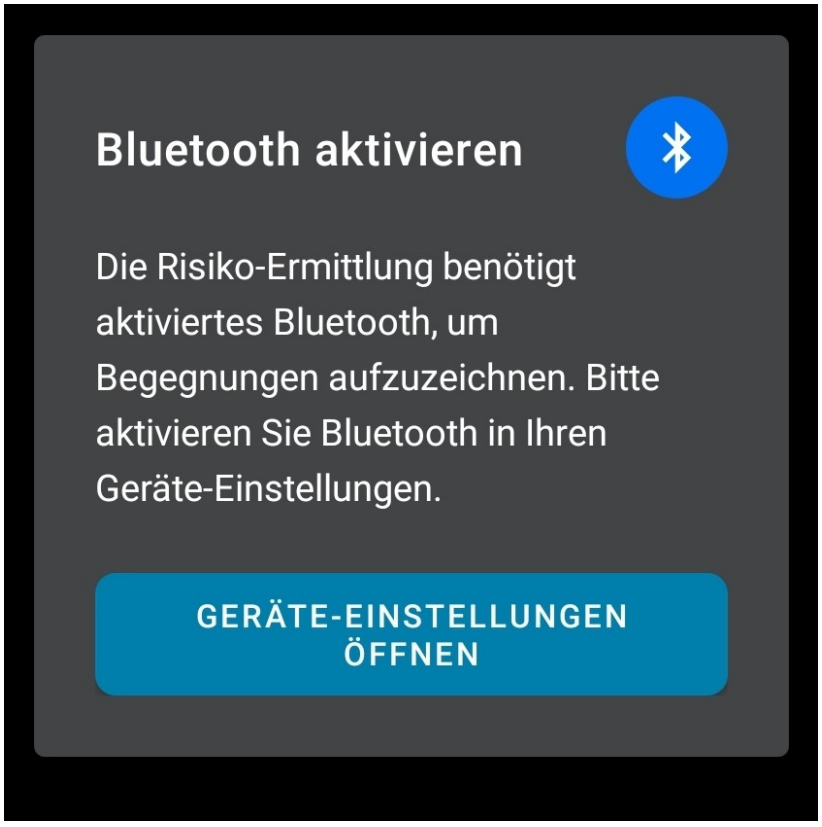
Bluetooth dient im Standard dazu, über kurze Strecken Daten zwischen zwei Geräten auszutauschen. Im Gegensatz zu WLAN bedarf es dazu keiner zusätzlichen Infrastruktur: So gut wie jedes Smartphone hat Bluetooth integriert, und die Kommunikation über Bluetooth ist „Point to Point“, also direkt zwischen den Geräten. Dies ist auch die Basis für die Corona-Warn-App. Aber wie funktioniert das?

Sind zwei Smartphones nahe beieinander, dann können diese sich sehen und sogar auf Grund der Signalstärke eine Abschätzung vornehmen, wie nah sie sich sind. Hinter den Smartphones verbergen sich deren Besitzer. Sie können also mit hoher Wahrscheinlichkeit davon ausgehen, dass bei einer Begegnung der Smartphones die Besitzer nahe beieinander waren. Stellt sich später heraus, dass davon einer mit Corona infiziert war, besteht ein Risiko für den anderen Benutzer.

Je näher die beiden Geräte sich sind, desto stärker ist das Signal, was empfangen werden kann. Dies lässt einen Rückschluss darauf zu, wie hoch das Risiko einer Infektion betrachtet werden muss: Je höher die Signalstärke, desto näher die Geräte und deren Benutzer, entsprechend höher ist das Risiko einer Infektion.

Die Herausforderung: Jeder Funksender verbraucht Strom, und gerade bei Smartphones ist der Akku sowieso schon einer der kritischen Faktoren: Die Mobilfunkverbindung, Apps, die im Hintergrund laufen und Strom verbrauchen, der Bildschirm, der bei der Benutzung beleuchtet ist, all diese Geräte verbrauchen Akkukapazität. Je nach Smartphone ist es schon eine Herausforderung, mit einer Akkuladung über den Tag zu kommen.

Diese Gedanken sind auch bei der Entwicklung der Corona-Warn-App wichtig gewesen. Damit Begegnungen aufgezeichnet werden können, muss der Bluetooth-Sender immer eingeschaltet sein und auf der Suche nach anderen Geräten. Der Stromverbrauch soll so gering wie möglich sein, darum unterstützt die App nur Geräte, die den neuen Bluetooth LE (für **L**ow **E**nergy)-Standard unterstützen.




Die Konsequenz: Kritik an den Herstellern, dass man ja nur neue Geräte absetzen wollte, die diesen Standard unterstützen. Diese Argument ist aber wenig stichhaltig: Würden alte Geräte unterstützt, dann wäre der Akkuverbrauch durch die alten, nicht optimierten Bluetooth-Standards so hoch, dass der Akku im Handumdrehen leer wäre. In der Folge würde die App kaum genutzt und könnte damit ihre Funktion nicht erfüllen.

Grundvoraussetzung für die Nutzung der Kontaktverfolgung in der Corona-Warn-App ist, dass Bluetooth eingeschaltet ist. Diese Funktion finden Sie sowohl im Benachrichtigungscenter Ihres Smartphones als auch in den Einstellungen unter **Bluetooth**.

Wenn Sie Bluetooth ausgeschaltet haben, dann kann die App die Kontaktverfolgung nicht mehr vornehmen. Sie bekommen in der App eine Warnung angezeigt. Tippen Sie auf Geräte-Einstellungen öffnen, um Bluetooth wieder einzuschalten.

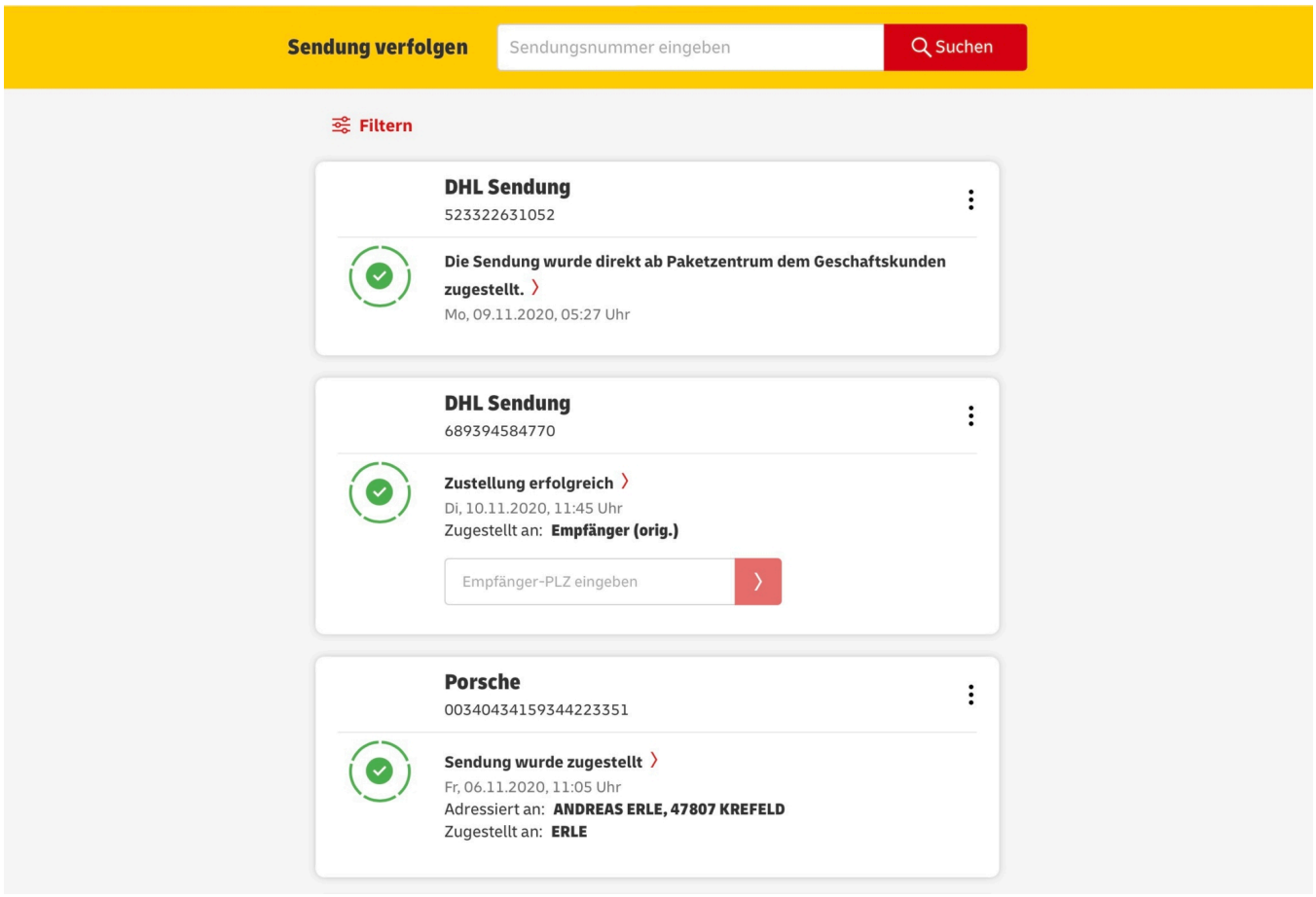
Die bisher erfassten Daten beeinflusst das nicht, nur die Erfassung neuer Begegnungen ist ohne eingeschaltetes Bluetooth nicht mehr möglich.

Einige ältere Geräte bieten die Möglichkeit, Ihr Gerät nach außen sichtbar zu machen. Das ist so, als würde es in die Welt hinausrufen „Hier bin ich! Koppelt Euch mit mir!“. Diese Funktion ist für die Corona-Warn-App nicht nötig. Schalten Sie sie aus, denn die bedeutet ein potentielles Sicherheitsrisiko.

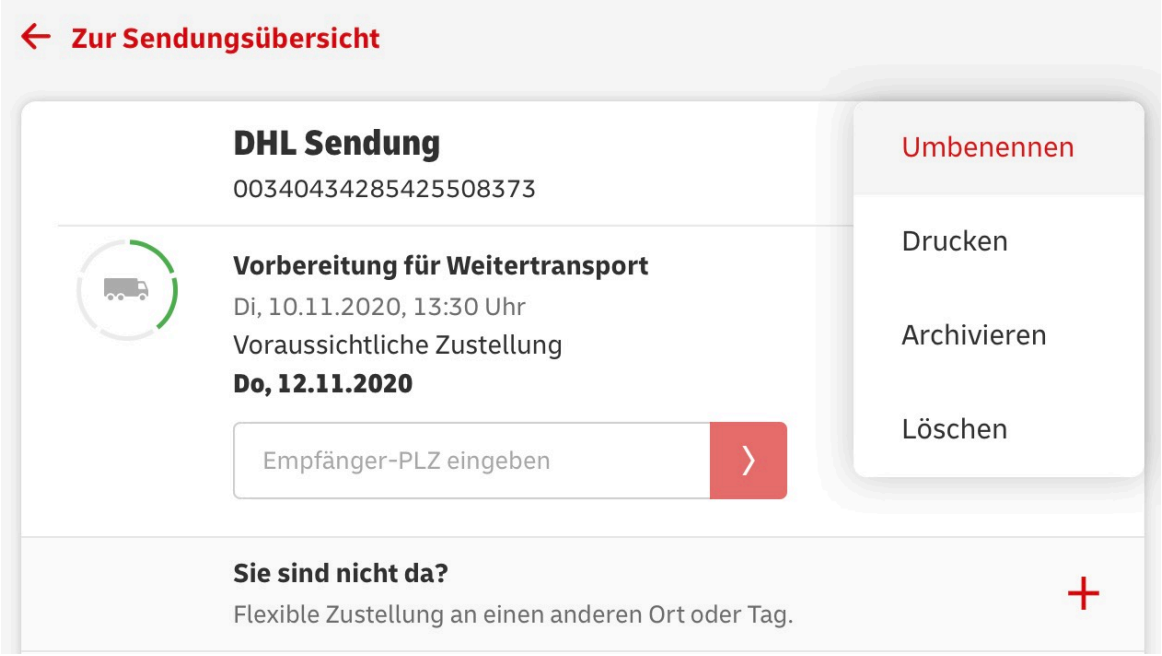
# DHL-Pakete ohne Zusatzsoftware tracken


Sie verschicken ein Paket, und der Empfänger möchte wissen, wo es gerade ist.Ihr Lieblings-Online-Händler hat endlich die heiss ersehnte Ware verschickt, und Sie wollen wissen, wann diese zugestellt wird. Die Paketverfolgung per App bedarf einer Installation. Für DHL können Sie das auch ohne App direkt auf der Webseite machen, inklusive der Sendungshistorien.

Dazu müssen Sie sich nur einmal ein kostenloses Konto auf de Paketverfolgungs-Webseite von DHL anlegen. Das können Sie auf Wunsch dann auch nutzen, um Pakete online zu frankieren oder Abholungen zu buchen. Melden Sie sich auf allen Geräten dann mit diesem Konto auf der Webseite an. Das führt dazu, dass Sie Seite weiß, wer Sie sind und damit alle ihre Suchen und selbst versendeten Pakete kennt.

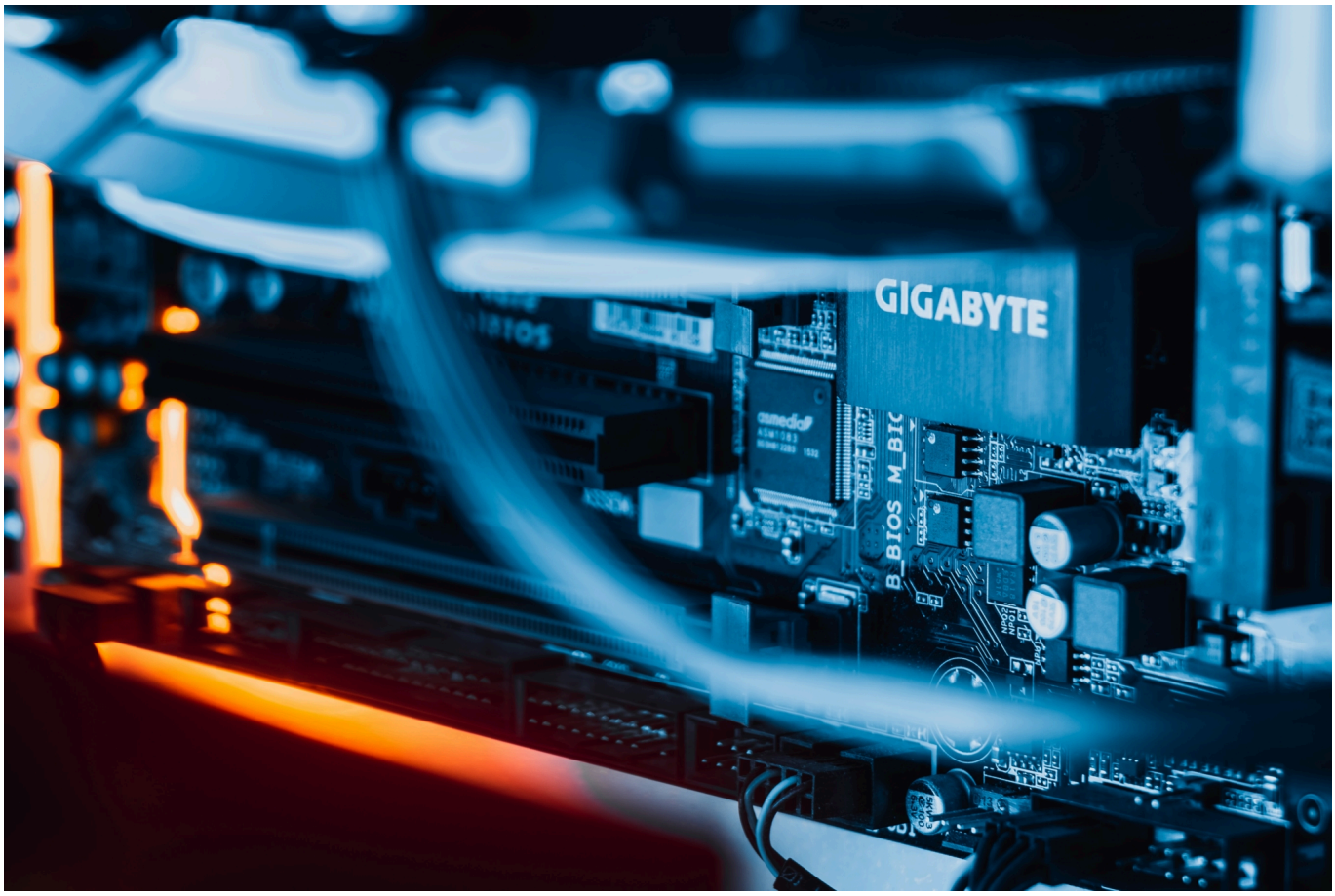



Um ein neues Paket zu tracken, geben Sie dessen Paketnummer unter **Sendung verfolgen** ein. Die Webseite zeigt Ihnen nun den aktuellen Status und den Sendungsverlauf. Wenn dieser schon vorliegt, dann auch den voraussichtlichen Liefertermin. Dieser erscheint, wenn die Sendung das Startpaketzentrum verlassen hat.




Alle Pakete werden automatisch unter Ihrem Konto weitergeführt. Sie müssen also die Paketnummer nicht mehr manuell eingeben, sondern finden das Paket automatisch in der Liste Ihrer Sendungen weiter unten auf der Seite. Klicken sie auf die drei Punkte neben dem Titel des Pakets, dann können Sie ihm einen sprechenderen Namen geben oder es aus der Liste löschen.

# Die Vorteile einer Microsoft Azure Cloud




**Wer als Privatmensch seine Daten und Anwendungen in die Cloud bringen will, kommt mit den üblichen Standarddiensten wie Dropbox, iCloud, Google Drive oder OneDrive bestens aus. Anders sieht es für kleine, mittelständische und erst recht große Unternehmen aus. Sie brauchen anspruchsvollere Lösungen, um den individuellen Anforderungen gewachsen zu sein. In diesem Zusammenhang spricht man von einer Business-Cloud.**

Auch für professionelle Ansprüche gibt es eine große Auswahl an Anbietern: Amazon mit seinen Amazon Web Services (AWS) ist einer der größten. Auch Google bietet Cloud-Dienste an. Sehr stark in diesem Segent ist aber auch Microsoft.

Microsoft Azure ist eine Business-Cloud, die zu mehr Flexibilität in der Unternehmens-IT führt. Zudem lassen sich damit Kosten reduzieren. Die skalierbare Cloud-Plattform erlaubt den Betrieb beliebig vieler Anwendungen, den Test von Neuentwicklungen und die Abbildung ganzer Server.

## Kombination von Business Cloud und On-Premise-Lösung

In jedem Unternehmen gibt es Gegner einer Public Cloud, die Bedenken wegen der Datensicherheit äußern. Azure von Microsoft ist aber eine hybride Cloud und kombiniert damit die Business Cloud mit einer On-Premise-Lösung. Die IT-Abteilung der Firma behält die Kontrolle darüber, wo die eigenen Daten gespeichert werden. Selbst das Land für das Hosting kann sie wählen. Wer sich in der EU sicherer fühlt, wählt einen hiesigen Serverstandort.

## Die Architektur von Microsoft Azure

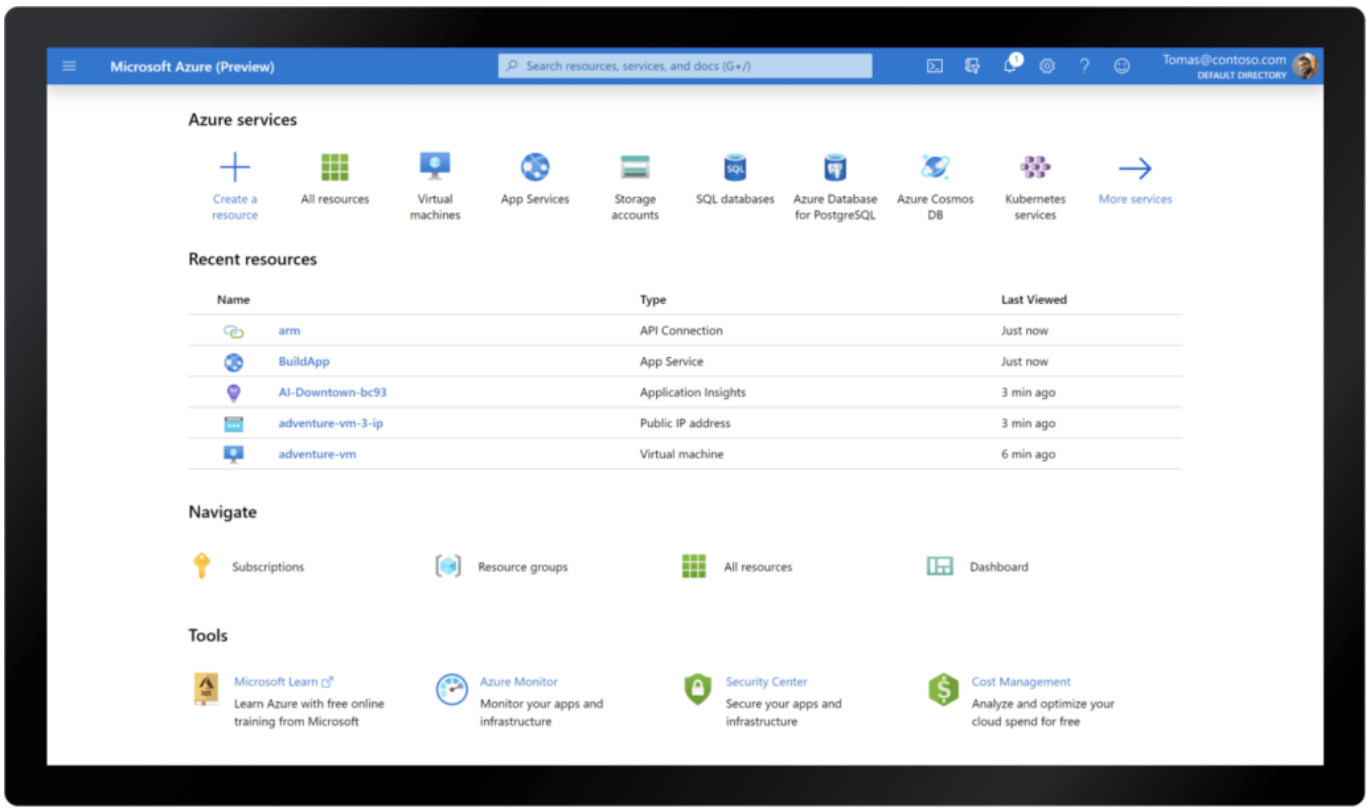
Die skalierbare, individuell anpassbare Plattform für das Cloud-Computing erlaubt die Datenspeicherung teilweise lokal und ebenso in der Cloud. Mit den lokal gespeicherten Daten lassen sich gleichzeitig Azure-Programme nutzen. Diese ermöglichen die Verwaltung der Daten, die Abbildung einer virtuellen Umgebung und die Entwicklung von Anwendungen und Apps. Der Zugriff auf die Business Cloud ist über Windows und Linux möglich. Azure von Microsoft ermöglicht es, sich Dienste und Programme selbst zusammenzustellen. Das ist nicht bei jeder Cloud-Plattform möglich.

Die Microsoft-Cloud lässt sich an die individuellen Geschäftsprozesse jedes Unternehmens anpassen. Die Zusammenstellung nehmen die IT-Verantwortlichen direkt bei Microsoft vor. Darüber hinaus ist Azure beliebig konfigurierbar und kann sowohl als SaaS als auch als PaaS oder IaaS genutzt werden. Das gewählte Betriebsmodell erlaubt die Bereitstellung unterschiedlichster Services, darunter:

- VM (Virtual Machines unter Windows oder Linux)
- SQL-Datenbanken
- App Services
- Storage
- Backups
- Active Directory
- uvm.

Zur Architektur von Azure gehört auch die mehrschichtige Sicherheit in den Rechenzentren, der Software selbst und den betrieblichen Infrastrukturen. Microsoft hat in seine Cloudlösungen in den letzten Jahren über eine Milliarde US-Dollar investiert und beschäftigt 3.500 Sicherheitsexperten, welche die Cloud permanent auf Sicherheitsrisiken scannen. Nach Angaben des Konzerns aus

Redmond soll Azure die vertrauenswürdigste Cloud schlechthin sein.




## Business Cloud für komplexe Compliancevorgaben

Unternehmen sind stets bestrebt, ihre Compliance zu optimieren. Azure von Microsoft bietet die branchenweit umfangreichste Complianceabdeckung: Über

90 Complianceangebote sind integriert. Das schafft kein anderer Anbieter. Auf die Datensicherheit können sich die Anwender verlassen. Das wichtigste Prinzip des Azure-Datenschutzes lautet, dass die Anwender Besitzer ihrer Daten bleiben. Selbstverständlich werden diese von Microsoft niemals für Marketingzwecke verwendet.

## Nahtloser Hybridbetrieb

Mit Azure können die Firmen lokal, am Edge oder über mehrere Clouds verteilt arbeiten. Die Tools und Dienste wurden speziell für die hybride Cloud entwickelt. Das schafft eine unglaubliche Flexibilität und ermöglicht es, die Azure- Verwaltung für die gesamte eigene IT-Infrastruktur zu verwenden. Mit dem Azure-Remoting können die Mitarbeiter orts- und geräteunabhängig arbeiten. Dazu trägt die cloudbasierter App- und Desktopvirtualisierung bei. Azure ist vollständig für

Windows 10 optimiert und arbeitet nahtlos mit MS Office zusammen. Die Cloudlösung lässt sich binnen Minuten auf jede gewünschte Anwendungsgröße skalieren.

## Microsoft Azure: Lizenzvorteile

Anwender von Azure können ihre schon vorhandenen Lizenzen für Windows- und SQL-Server mit Azure weiter nutzen und erhalten einen Rabatt von bis zu 40 % für die Hybridcloud Azure. Diese wurde als hybride Lösung extra so entwickelt, dass sie auf den bereits vorhandenen Lösungen aufsetzen kann. Die bestehenden Lizenzen bleiben vollumfänglich erhalten.

Azure von Microsoft lässt sich darüber hinaus relativ leicht migrieren. Die skalierbare Cloudlösung gilt als sehr zukunftssicher.

# Zehn Jahre Google Streetview in Deutschland


**Zehn Jahre Google Streetview in Deutschland: Die Deutschen nutzen den Dienst zwar gerne, um sich in anderen Ländern umzuschauen - doch die eigene Häuserfassade wollen viele nicht im Netz sehen. Ein Proteststurm hat dazu geführt, dass Google in Deutschland keine neuen Aufnahmen macht. Der Widerstand ist verständlich - entlädt sich aber an der falschen Stelle.**

Vor zehn Jahren Stand Deutschland Kopf: Weil Google-Autos über deutsche Straßen rollten und mit ihren Dachkameras Häuser fotografierten. Für Google Streetview, jenen Onlinedienst, der zu Google Maps gehört und das Betrachten einer Umgebung mit 360-Grad-Panoramen ermöglicht.

In über 90 Ländern war Google Streetview bereits unterwegs, aber in Deutschland war die Empörung groß. Ein unangemessener Eingriff in die Privatsphäre sei das, ein Verstoß gegen den Datenschutz. Manche fühlten sich überrumpelt, dass ein IT-Konzern seine Virtualität verließ, mit echten Autos durch echte Straßen rollte und echte Häuser fotografierte. Da hörte der Spaß für viele auf.

## Proteste trotz Panoramafreiheit

Ich habe diese Aufregung nie teilen können. In Deutschland gilt die Panoramafreiheit. Alles, was ein Fußgänger oder Radfahrer oder Autofahrer sehen kann, darf bildlich wiedergegeben werden. An einer Hausfassade ist nun wirklich nichts Privates. Warum also diese Aufregung?

Vermutlich, weil die Menschen vor zehn Jahren zum ersten Mal begriffen, dass die großen IT-Konzerne tatsächlich in ihr Leben eindringen. Am PC oder auf dem Smartphone merken sie es eher nicht. Wenn die Konzerne hier Daten sammeln, ist nicht unmittelbar zu merken. Doch wenn Autos durch die Straßen rollen, dann wird die Sache greifbar. Und die Wut entlädt sich ausgerechnet dort, wo es am wenigsten angebracht ist.

## Normaler Reflex: Zu viele Demütigungen

Wir kennen das alles aus dem Alltag: Wir ertragen 100 Demütigungen, kleine Ärgernisse und Provokationen durch Familie, Freunde oder Kollegen. Beim 101. Mal bricht der Frust durch, an einer Stelle, wo Beobachter vielleicht sagen: Was hat sie denn nur, was stört ihn denn?

So ähnlich verhält es sich bei Google Streetview. 244.000 Häuserfassaden in

Deutschland wurden komplett oder teilweise verpixelt. Das verdirbt einem den Spaß an der Sache, weil diese Pixelmatsche bescheuert aussieht - und zu verrückten Konsequenzen führt: Zieht ein Pixel-Aktivist wieder aus, kann ein Haus nicht mehr entpixelt werden. Die Daten wurden ja gelöscht. Das hat Google den Spaß an der Sache verdorben - deshalb gibt es seit 2011 bei Google Streetview in Deutschland keine Aktualisierungen mehr. Nur im Rest der Welt.


## An der richtigen Stelle protestieren

Viel klüger und angemessener wäre es, sich über die wirklichen Eingriffe aufzuregen - und sich dagegen zu wehren. Das mehr oder weniger klammheimliche Datensammeln von Google, Amazon und vor allem Facebook. Und insbesondere das Verquicken der Daten und das gnadenlose Ausschlachten von Gewohnheiten, Eigenheiten und persönlichen Merkmalen. Das ist privat. Aber keiner merkt's, weil keine Google-Autos oder Facebook-Bikes durch die Wohnung rollen.

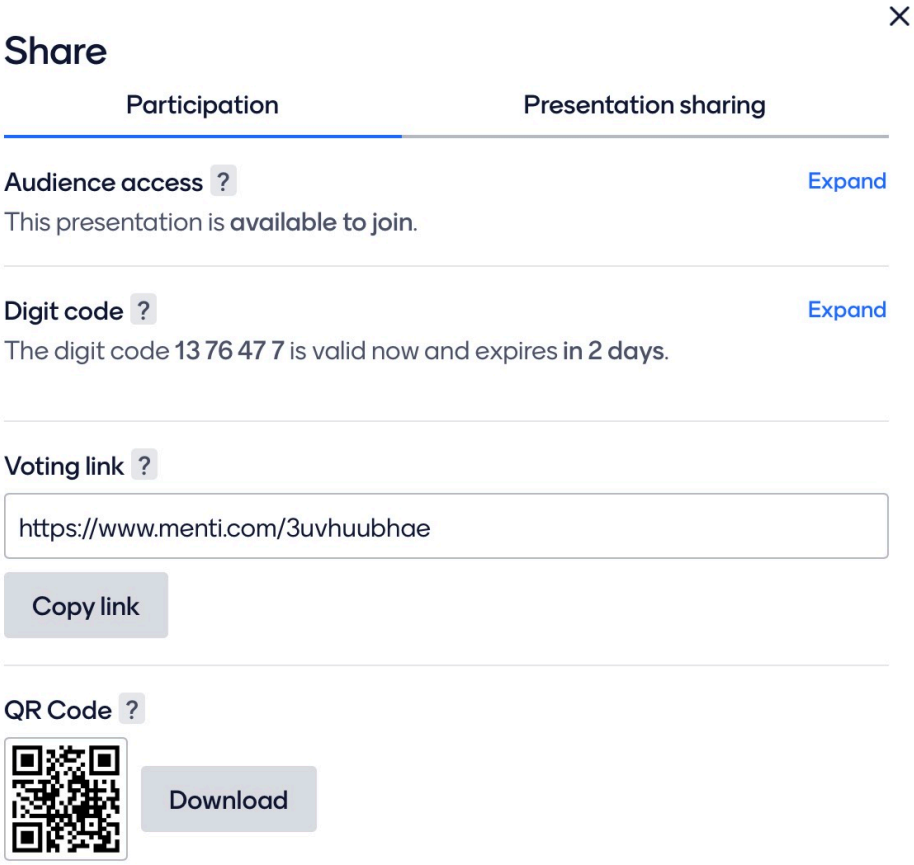
Eine trügerische Sicherheit. Kanalisieren wir unseren Ärger und unseren Widerstand doch lieber richtig.

*Zehn Jahre Google Streetview: Vom Onlinedienst zum Schreckgespenst*

# Interaktive Wortwolken: Mentimeter

Gerade in Zeiten der eingeschränkten Kontakte sind Präsentationen oft langweilig: Einer redet und zeigt Folien, die anderen Teilnehmer konsumieren - meist stumm. Fragen bleiben meist unbeantwortet, weil viele Menschen einfach ungerne in der ungewohnten Umgebung reden. Mentimeter ist ein kostenloser Dienst, der hier helfen kann!

Mentimeter versucht, die in einer persönlichen, lebhaften Diskussion unweigerlich vorkommenden Zwischenrufe in die Präsentation aufzunehmen. Dazu legen Sie sich zuerst ein kostenloses Konto an und können dann schon loslegen: Legen Sie eine neue Präsentation an, dann wählen Sie als Typ **WordCloud**. Geben Sie die Frage ein, auf die die Teilnehmer antworten sollen, dann bekommen Sie einen generierten Link. Noch einfacher: Auf Wunsch stellt die Webseite auch einen QR-Code bereit, den die Teilnehmer einfach vom Bildschirm mit der Kamera-App eines Android- oder iOS-Gerätes abscannen können und dann automatisch auf die Webseite der Umfrage geleitet werden. Den QR-Code können Sie in Ihre PowerPoint-Präsentation aufnehmen.




Zum Zeitpunkt der Umfrage stellen Sie die Mentimeter-Seite auf dem Bildschirm dar. Die Teilnehmen gehen mit Ihren Smartphones auf den Link und können ihre Begriffe eingeben. Sobald diese abgeschickt sind, erscheinen sie auf Ihrer Umfrageseite. Je mehr Teilnehmer es sind desto mehr wächst die Wortwolke nach und nach und bietet dann eine tolle Diskussionsgrundlage.

Go to **www.menti.com** and use the code **92 90 23 3**

# Wie gefällt Euch schieb.de?

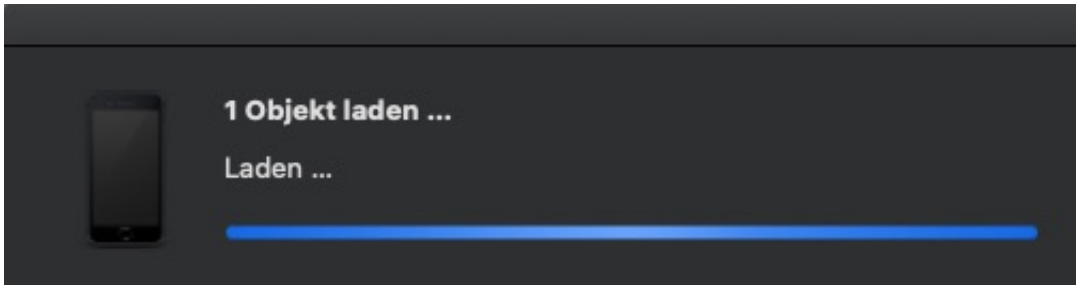
Mentimeter

# Fehler bei der Verbindung eines iPhones beheben


Die Verbindung eines iPhones oder iPad mit PC oder Mac sollte das Einfachste von der Welt sein. Ist es auch... meistens.  Manchmal aber will der Rechner nicht so recht, und meist passiert das, wenn Sie gar keine Zeit haben. Die Lösung ist meist einfach und kosten nur geringen Zeitaufwand!

Die Fehlermeldung "Um eine Verbindung zu Ihrem iPhone herzustellen, ist ein Softwareupdate erforderlich", hat eine einfache Ursache: Updates von iOS verändern manchmal die Art, wie iPhone und Windows bzw. macOS die Verbindung zueinander aufbauen. Die alte Version von iTunes bzw. Music kommt dann nicht mehr mit der neuen Version von iOS klar.


Klicken Sie auf **Installieren**, dann lädt Ihr Rechner die neue Version der Software herunter, installiert sie und baut dann die Verbindung zum Gerät auf. Wenn das nicht automatisch klappt, dann ziehen Sie einmal den Stecker aus der USB-Buches des Rechners und schließen Sie das iPhone/iPad einmal neu an. Die Verbindung wird damit zurückgesetzt und neu aufgebaut.



# Wenn WLAN auf dem iPad/iPhone nicht stabil ist

Nicht alle Geräte haben eine eingebaute SIM-Karte und so ist Wireless LAN (WLAN) die am häufigsten verwendete Verbindungsmethode bei mobilen Geräten. Egal, ob es sich dabei um ein Smartphone, ein Tablet oder ein Notebook handelt. Dumm, wenn WLAN nicht funktioniert. Die Ursache bei iOS-Geräten ist allerdings oft sehr einfach. Wir zeigen Ihnen, was Sie tun können, um wieder online zu kommen!

Es kann immer mal wieder vorkommen, dass die WLAN-Verbindung zusammenbricht und gegebenenfalls manuell wieder hergestellt werden muss. Der erste Check: Ist das Gerät weit vom Router entfernt? Wird die Verbindung stabiler, wenn der Abstand verringert wird? Wenn ja, dann kann Ihnen ein Repeater helfen.

Wenn nicht, dann löschen Sie einmal die WLAN-Verbindung: Unter **Einstellungen** > **WLAN** sehen Sie eine Liste aller WLANs. Tippen Sie daneben auf das **i**. durch ein Tippen auf **Dieses Netzwerk ignorieren** löschen sie die gespeicherten Zugangsdaten. Sie können dann direkt das WLAN wieder antippen, die Zugangsdaten eingeben und erneut verbinden. Oft ist das Problem damit gelöst.

Wenn das nichts hilft, dann starten Sie das Gerät einmal über die spezifische Tastenkombination (beispielsweise den Einschalter und die Home-Taste gleichzeitig mehrere Sekunden gedrückt halten). Damit wird das Gerät komplett neu gestartet (was mehr erreicht als ein Ein- und Ausschalten). Das hilft, nicht einwandfrei laufende Dienste zu beenden.

# App-Updates bei macOS manuell installieren


Nicht nur macOS, auch die Apps aus dem macOS App Store bekommen regelmässig Updates spendiert. Neue Funktionen, Fehlerbeseitigungen, es macht Sinn, diese auch zu installieren. Das passiert im Normalfall in regelmässigen Abständen auch automatisch. Wenn Sie aber eine App dringend sofort aktualisieren müssen, dann müssen Sie diesen Prozess manuell starten. Wir zeigen Ihnen, wie!

Alle Updates auf dem Mac können Sie durch einen Klick auf den Apfel oben links am Bildschirmrand erreichen: Unter **Systemeinstellungen** sehen Sie die Zahl der macOS-Updates. Klicken Sie darauf und Sie gelangen in die Einstellungen und können die OS-Updates direkt installieren.

Darunter finden Sie mit **App Store** einen Link zum App Store. Spannenderweise heisst das Fehlen einer Zahl von vorhandenen Updates - die dort durchaus manchmal zu finden ist - nicht, dass keine vorhanden sind. Klicken Sie auf den Link, dann in der Liste links ganz unten auf **Updates**.

macOS zeigt Ihnen dann rechts neben der Liste die vorhandenen App-Updates an. Diese können Sie durch einen Klick direkt starten. Darunter finden Sie eine Liste der Apps, die gerade erst aktualisiert wurden und die Änderungen, die das Update jeweils gebracht hat.

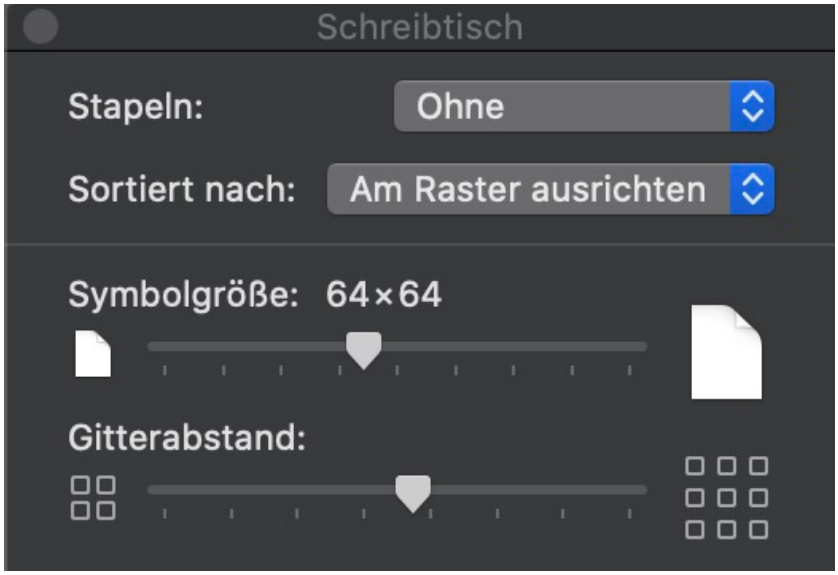
# Darstellungsoptionen einblenden beim macOS Finder

Es gibt zwei Arten von Benutzern: Die einen arbeiten alleine in ihren Programmen und nutzen nur die Dateiablage des Betriebssystems, die anderen beziehen auch den Schreibtisch oder Desktop mit ein. Letzteres ist nicht ganz ungefährlich, Sie können schnell die Ordnung verlieren. MacOS bietet Ihnen hier einige Möglichkeiten, das zu vermeiden.

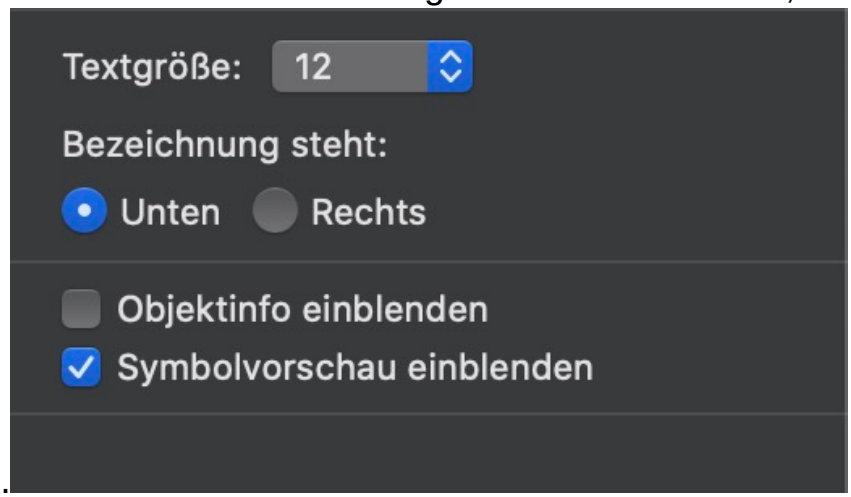
Wenn Sie Dateien geordnet und damit einfacher wieder aufzufinden darstellen wollen, dann können Sie die Funktion der Stapel nutzen.

Um die Symbole zu ändern, klicken Sie mit der rechten Maustaste in einen freien Bereich des Schreibtisches und dann auf **Darstellungsoptionen einblenden**. Hier können Sie sehr fein einstellen, wie die Symbole auf dem Schreibtisch dargestellt werden sollen und wie sie angeordnet sind.Über die **Symbolgröße** legen Sie in mehreren Schritten fest, wie groß das Symbol sein soll. Hier macht es Sinn, ein wenig mit den Einstellungen zu spielen, denn es gibt Alternativen, die wir im nächsten Abschnitt vorstellen.

Mac OS ordnet die Symbole in einem virtuellen Gitter an, dessen Größe Sie unter **Gitterabstand** festlegen können. Je größer der Wert, desto weiter sind die aneinandergrenzenden Symbole voneinander entfernt.



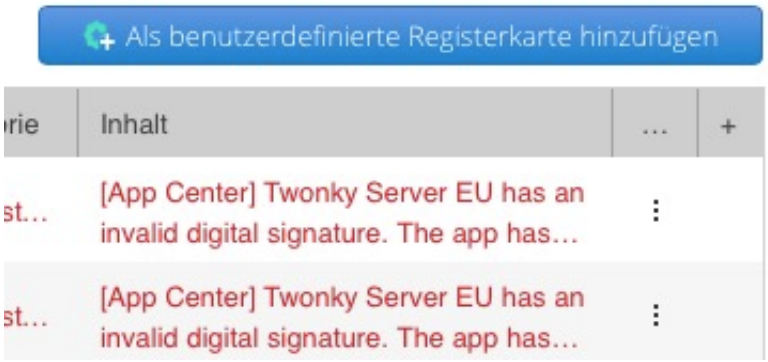

Weiterhin können Sie einstellen, ob die **Bezeichnung**, also der Text des Symbols, unten oder rechts steht und wie die **Textgröße** der Beschriftung sein soll. Vor allem die letzte Einstellung kann dazu führen, dass Sie deutlich stressfreier arbeiten können, denn je besser Sie die Bezeichnungen erkennen können, desto kürzer müssen Sie suchen.



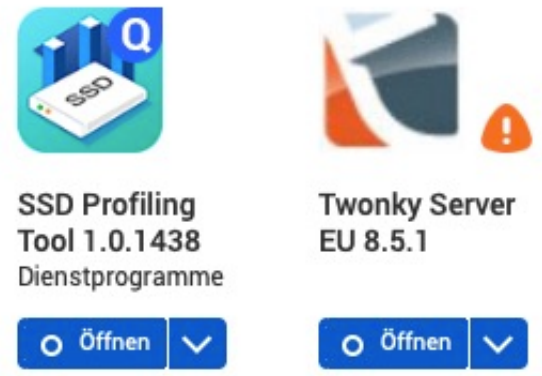
# Wenn Apps auf einem QNAP-NAS beendet werden

Eine Netzwerkfestplatte wie die von QNAP oder Synology sind weit mehr als Festplatten mit Netzwerkanschluss. Der Speicher befindet sich ein einem Gehäuse, das einen nahezu vollwertigen PC enthält. Der hat zwar ein QNAP-eigenes Betriebssystem, erlaubt aber die Installation von vielen zusätzlichen Apps. Die können entweder aus dem hauseigenen AppStore stammen, aber auch aus anderen Quellen. Wenn eine App immer wieder automatisch beendet wird, hat das oft eine einfache Ursache!

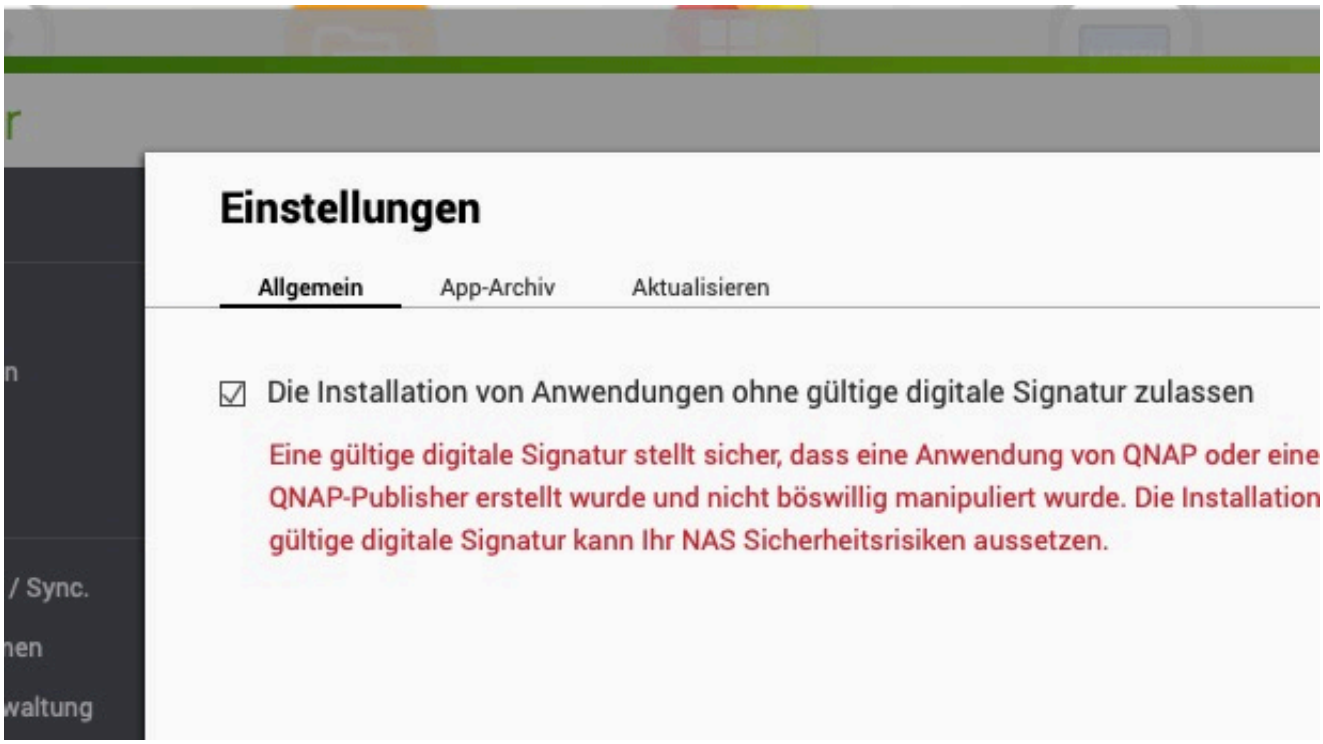
Vor allem bei von Geräten außerhalb des NAS genutzten Apps wie dem Twonky-DLNA-Server ist das ein PRoblem: Sie schalten den Fernseher ein, normalerweise scheint Ihr NAS als Quelle. Plötzlich ist es nicht mehr zu sehen, und bei der Kontrolle auf dem NAS finden Sie folgende Fehlermeldung:




QNAP hat in einem Update den Security Counsellor, die interne Sicherheits-App, so eingerichtet, dass Apps, die keine gültige digitale Signatur haben, nicht zulässig sind. Für Apps, die Sie neu installieren, ist das kein Problem: Das NAS lässt die Installation gar nicht erst zu bzw. fordert Sie auf, die Freigabe explizit zu erteilen. Bei vor dem Update installierten Apps ist die Freigabe nicht erteilt, und der Counsellor beendet die Apps bei jeder Ausführung.




Eine Appp ohne gültige Signatur erkennen Sie im App Center auf dem NAS durch ein orangenes Ausrufezeichen neben dem Symbol. Sie können die App manuell starten, indem Sie auf **Starten** klicken. Um das Beenden zu vermeiden, klicken Sie auf das Zahnrad im App Center und setzen Sie einen Haken neben **Die Installation von Anwendungen ohne gültige digitale Signatur zulassen**. Das sollten Sie aus Sicherheitsgründen aber nur tun, wenn Sie für jede einzelne App die Hand ins Feuer legen, dass diese keinen Schaden anrichtet!


Einstellungen
Allgemein
App-Archiv
Aktualisieren
Die Installation von Anwendungen ohne gültige digitale Signatur zulassen
Eine gültige digitale Signatur stellt sicher, dass eine Anwendung von QNAP oder eine
QNAP-Publisher erstellt wurde und nicht böswillig manipuliert wurde. Die Installation
gültige digitale Signatur kann Ihr NAS Sicherheitsrisiken aussetzen.

# Überwachungsfotos bestellen? Kein Problem

**Zunehmende Digitalisierung bedeutet nicht nur Fortschritt, sondern auch zunehmende Risiken. Das belegt ein aktuelles Beispiel aus Russland: Hier ist es möglich, über dubiose Kanäle auf Telegram sich Fotoaufnahmen aus Überwachungskameras der Stadt Moskau zu besorgen. Über eine Gesichtserkennung lassen sich gezielt Personen aufspüren.**

Fast überall hängen in Großstädten Überwachungskameras. Mal besser, mal gar nicht zu sehen. Wir haben uns daran gewöhnt - und nehmen sie deshalb nicht mehr wirklich wahr.

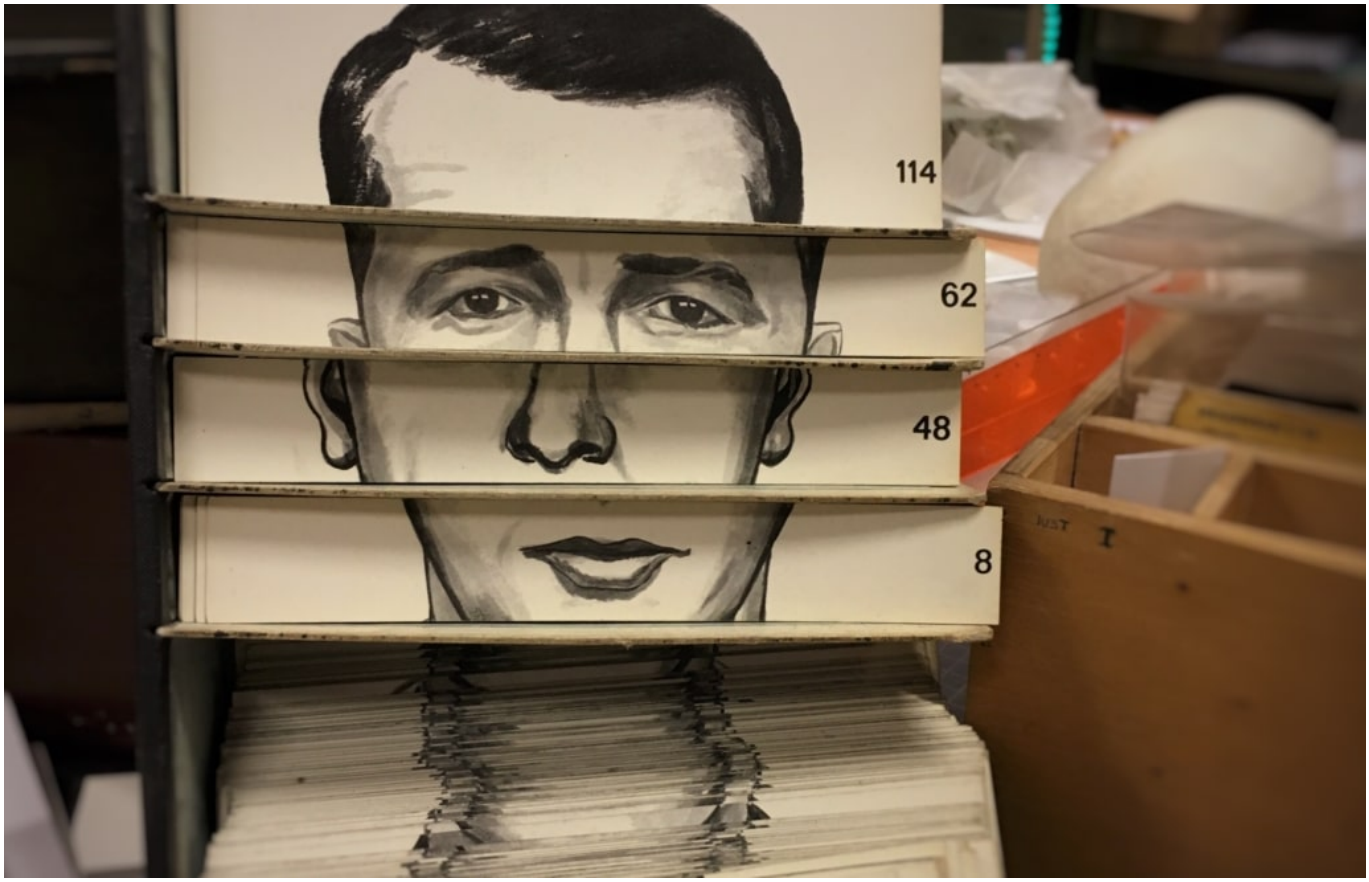
Aus dem "Tatort" oder aus anderen Filmen wissen wir: Die Polizei besorgt sich schon mal gerne Aufnahmen solcher Kameras. Und Hollywood erweckt mitunter den Eindruck, Hacker könnten die Kameras jederzeit mühelos fernsteuern und eine Person dabei beobachten, wie sie von A nach B geht.

Leider ist die Wahrheit nicht weit von Hollywoods Einfallsreichtum entfernt. Wie die auf Menschenrechte spezialisierte britische Thomson Reuter Stiftung jetzt berichtet, ist es offensichtlich gar kein Problem, auf die Überwachungssysteme einer Großstadt zuzugreifen.

## Fotos aus Überwachungssystemen

Eine 20-jährige Russin hat sich im Auftrag der Aktivistengruppe Roskom Swoboda bei einer zwielichtigen Kontaktperson auf Telegram gemeldet. Die hat in dem Messengerdienst versprochen, Zugriff auf Fotos aus Überwachungskameras in Moskau zu haben. Mehr als das: Auftraggeber können der Kontaktperson ein Foto geben - und die sucht dann mit Hilfe von Gesichtserkennung nach passenden Überwachungsbildern. Ein Fahndungsinstrument also.

Für 16.000 Rubel (etwa 175 Euro) bekam die Aktivistin laut dem Bericht schließlich 79 Fotos von sich selbst. Aufgenommen an verschiedenen Orten in Moskau, auch in U-Bahn-Stationen und Bussen. Und das über einen Zeitraum von vier Wochen. So etwas ist nur möglich, wenn dauerhaft die Aufnahmen von sehr vielen Kameras zur Verfügung stehen und auf einem Server gespeichert sind. Dann eine Gesichtserkennung darüber laufen zu lassen, um eine bestimmte Person zu finden, ist heute technisch keine besondere Herausforderung mehr. Cloud-Dienste wie Amazon Web Services (AWS) bieten solche Systeme und Dienste schlüsselfertig an.



*Mit geeigneter Software nach Gesichtern zu suchen, ist heute einfach geworden*

## Die Privatsphäre ist dahin

Kriminelle benötigen also nur eine Sicherheitslücke, schon lassen sich Aufnahmen von Überwachungskameras missbrauchen. Die Privatsphäre ist dahin. Je größer das Überwachungssystem, desto größer das Problem - und das Risiko. Wie das Beispiel des polnischen Foto-Suchangebots PimEyes zeigt, können die Folgen fatal sein.

Wenn etwa Geheimdienste auf solche Systeme zugreifen, wissen sie ohne jeden Aufwand sofort Bescheid: Wo wohnt eine Person, welchen Tagesablauf hat sie, wen trifft sie, wo geht sie essen oder arbeiten? Sicher kein beruhigender Gedanke für russische Dissidenten, Oppositionelle oder Journalisten, die häufig bedroht werden.

Aber auch wir sollten Lehren aus dem Beispiel von Roskom Swoboda ziehen. Die Sicherheitsstandards für Kamerasysteme können gar nicht hoch genug sein.

*So funktioniert das Einsammeln von Fotos und Gesichts-Scans im großen Stil*

# EU will energiesparsame Rechenzentren


**Rechenzentren bei Providern, Cloud-Diensten oder großen Plattformen verbrauchen eine Menge Energie. Tendenz: Rasant steigend. Damit die EU ihre Klimaziele erreichen kann, hat sie nun auch einen Blick auf den Energiebedarf der Rechenzentren. Denn der ist enorm - und nimmt zu. Mit geeigneten Mitteln soll der Energiebedarf reduziert werden.**

Für die meisten von uns ist Internet ein bisschen wie Magie. Wir zücken das Smartphone oder klappen das Notebook auf - und im Display erscheint die ganze Welt. Nachrichten, Meldungen, Webseiten, Fotos, Videos - nur einen Mausklick entfernt. Und kaum einer macht sich Gedanken darüber, wie das eigentlich funktioniert.

Möglich machen das Rechenzentren. Jede Menge davon. Bei den großen IT-Giganten wie Google, Facebook, Microsoft. Bei den Streamingdiensten. Bei den Providern. All diese Rechenzentren und Cloud-Dienste sind extrem energiehungrig. Rund 2,7% der europäischen Strombedarfs geht auf das Konto solcher Rechenzentren. Tendenz: Steigend. Schon 2030 sollen es 3,2 Prozent

sein. Und das sind nur die Rechenzentren. Der Energiebedarf der Geräte der Nutzerinnen und Nutzer kommt noch dazu.

*CO2-Ausstoß in Rechenzentren muss reduziert werden*[/caption]

## EU will Stromverbrauch beschränken

Doch die EU hat sich ehrgeizige Klimaziele gesetzt. Deshalb müssen auch die Rechenzentren sparen. Energie vor allem, um den CO2-Ausstoß zu reduzieren.

Die EU hat deshalb einen Katalog an Vorschlägen und Anforderungen vorgelegt, die Rechenzentren ab einer bestimmten Größe künftig erfüllen müssen. Besonders wichtig bei Rechenzentren: die Kühlung. Denn überall, wo viele Computer am Stück rechnen, wird viel Wärme produziert, und damit die Chips nicht durchschmoren braucht es starke Kühlsysteme. Die erfordern aber einen hohen Energieeinsatz, insbesondere bei warmen Außentemperaturen. Es müssen also effizientere Kühlungssysteme her.

## Rechenzentren optimieren - das lohnt sich

Gleichzeitig kann und soll die Abwärme der Rechenzentren genutzt werden, etwa zur Heizung oder um Energie zurückzugewinnen. Besonders wichtig ist natürlich auch der Einsatz erneuerbarer Energien.

Last not least können und müssen Rechenzentren aber auch optimiert werden, damit sie weniger Energie verbrauchen. Außerdem spielt es auch eine Rolle, wo Rechenzentren stehen. In Südeuropa ist nicht der ideale Ort: Dort ist es ohnehin warm – da produziert die Kühlung einen höheren CO2-Ausstoß. In Norwegen muss man dagegen nur die Fenster öffnen ... Im Ernst: Es gibt Rechenzentren am Meer, die kühlen mit Meerwasser. Es gibt also Ideen, die müssen nun umgesetzt werden.

[caption id="attachment_772280" align="alignnone" width="1030"]

*KlickScham: Der Energieverbrauch von Google und Co. ist enorm*

## Selbst Energie sparen - das geht!

Irgendwann wird es sicher in Europa Zertifikate geben, auf die man achten könnte. Aber so weit sind wir noch nicht. Ganz generell wichtig zu wissen: Streaming – vor allem Filme und Serien – verbraucht eine Menge Energie. Wer da auf seinen CO2-Fußabdruck achten möchte, wählt keine 4K-Auflösung, wenn HD völlig reicht.

Auch ist es besser, zu Hause per DSL zu streamen – oder Filme downzuloaden – als diese unterwegs im Mobilfunknetz zu streamen. Mobilfunknetze verbrauchen viel mehr Energie. Und bei Videoschalten mit den Kollegen, kann man auch einfach mal das eigene Videobild abschalten und nur zuhören, wenn man nichts zu sagen hat.