

A portrait of a man with short brown hair and a slight smile, wearing a teal button-down shirt. He is positioned on the left side of the frame, with his arms crossed. The background is dark. The text 'Schieb Report' is overlaid on the right side in a large, white, sans-serif font.

Schieb Report

Ausgabe 2019.32

Refurbished IT: Lohnen sich generalüberholte Geräte?

Heutzutage gibt es kaum noch einen Haushalt ohne technisches Equipment. Laut aktuellen Studien hatten 2018 bereits [90 Prozent aller Haushalte in Deutschland](#) einen PC. Im Bereich der Mobiltelefone, darunter herkömmliche Handys und Smartphones, sind es sogar 96,7 Prozent. Doch wer sich mit [Hardware](#) versorgen will, muss nicht zwangsweise immer zu Neugeräten greifen.

Die Anschaffung neuer, hochwertiger Geräte, insbesondere PCs, Laptops, Notebooks, Tablets und Smartphones, kann ohne Weiteres ein großes Loch in den Geldbeutel reißen. Während die Kosten von Zubehör wie [Kopfhörer](#), Maus und Co. für die meisten Menschen noch erschwinglich ist, sieht das bei der Anschaffung größerer Hardware anders aus.

Leider sind immer wieder Anschaffungen nötig - denn keine Hardware hält ewig.

Ungefähre Lebensdauer der Hardware eines PC

- **Lithium Akkus von Notebooks und Handys:** 300 bis 800 Ladezyklen, theoretisch sieben bis 15 Jahre haltbar, praktisch jedoch zwei bis fünf Jahre;
- **Blei Akkus von USV-Anlagen:** 400 bis 600 Vollzyklen, vier bis sechs Jahre;
- **Desktop PC:** vier bis sechs Jahre;
- **Notebook:** drei bis fünf Jahre;
- **Server wie HP oder Supermicro:** fünf bis acht Jahre
- **andere Server und Eigenbau:** vier bis fünf Jahre
- **Laserdrucker:** drei bis zehn Jahre
- **Tintenstrahldrucker:** vier bis zehn Jahre



Was sind Refurbished IT-Geräte?

Eine gute Alternative sind Geräte, die nicht fabrikneu sind, sondern generalüberholt. Also gebrauchte Hardware, die vom Hersteller oder einem Anbieter eingesammelt, unter die Lupe genommen und wieder auf Vordermann gebracht wird. Wie neu - aber eben nicht neu. "Refurbished", ist der Fachbegriff dafür.

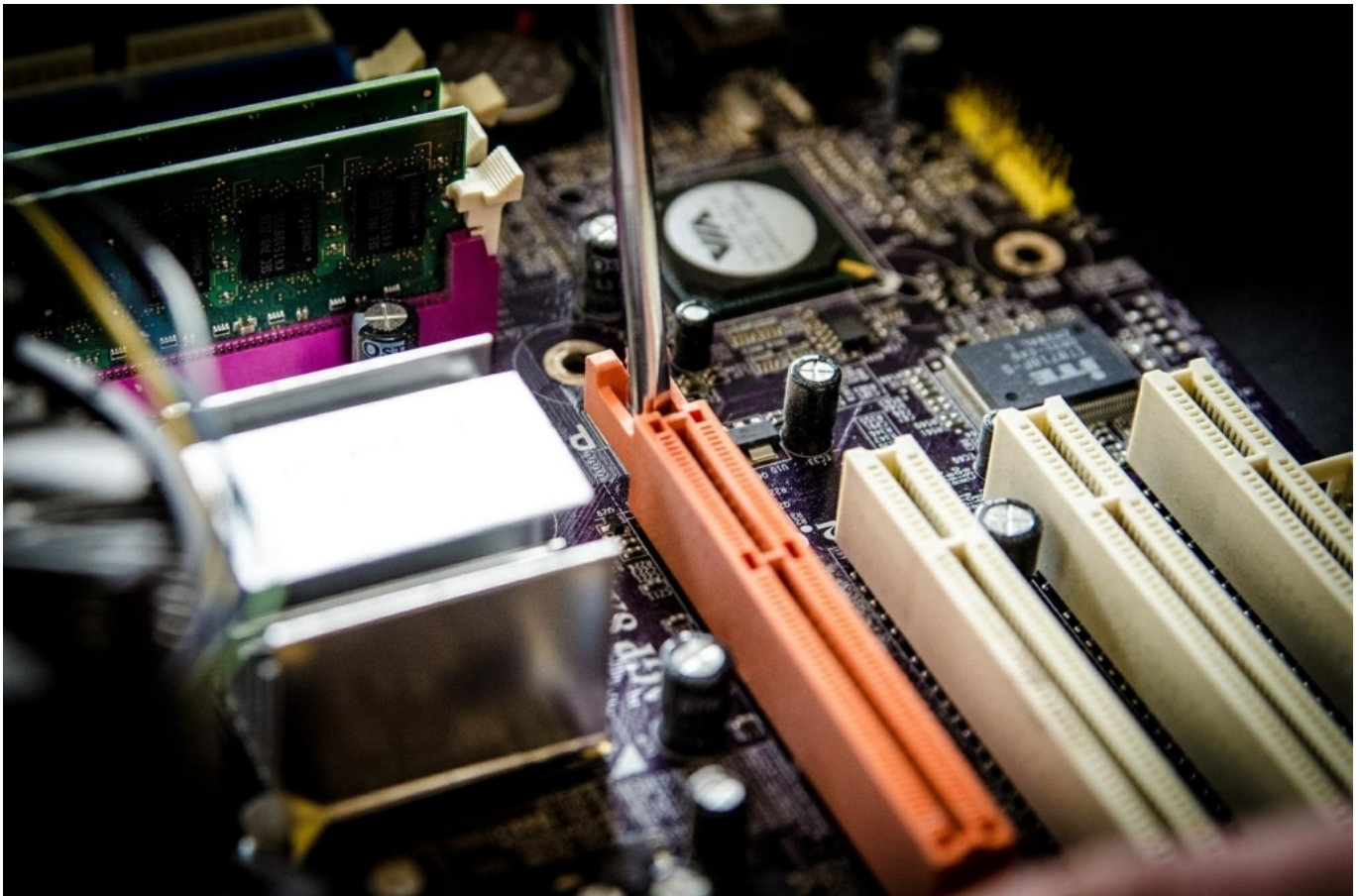
Oft handelt es sich dabei um Business-Geräte aus beendeten Leasingverträgen. Büros geben die Geräte zurück, nicht weil sie altersschwach oder defekt wären, sondern weil sie routinemäßig durch neue ersetzt werden. Nach der Rücksendung schließt sich ein sogenannter Audit-Prozess an, der sowohl die Überprüfung als auch eine detaillierte Beschreibung über die technische Ausstattung und die optische sowie technische Qualität enthält. Zum Audit-Prozess zählen unter anderem

- die Reinigung der Geräte innen und außen,
- die Datenlöschung,
- ein ausführlicher Test der Hardware,
- eventuelle Reparaturen einzelner Komponenten und
- die Erfassung der Geräte im Bereich Technik und Qualität.

Manche Refurbished Produkte sind so gut wie neu

Durch das Rückgaberecht für Verbraucher wird es diesen leicht gemacht, technische Geräte wegen eines Defekts oder einfach wegen Nichtgefallens wieder zurückzugeben. Damit fällt die Neuware unter gebrauchte Produkte, auch wenn diese vielleicht überhaupt nicht oder nur wenig genutzt wurde.

Auch Refurbished Business-Geräte aus einem Leasingbestand sind aufgrund ihrer Hochwertigkeit und Langlebigkeit oftmals noch über einen langen Zeitraum nutzbar.



Einteilung der Refurbished Geräte in Stufen

Nach dem Auditprozess werden die Geräte in verschiedene Stufen eingeteilt, die sich wie folgt darstellen:

1. **Demoware** – Diese stammt aus Messe- und Ladenausstellungen, Insolvenzen und ähnlichem. Sie sind absolut neuwertig und wurden entweder nur wenig oder noch gar nicht benutzt. Bevor die Demoware auf den Ladentisch kommt, erfolgt eine technische Überprüfung, Reinigung und die Werkeinstellungen werden zurückgesetzt.
2. **Neuware Sonderposten** – Hierbei handelt es sich um neue, originalverpackte Geräte, die beispielsweise schon über einen längeren Zeitraum zum Lagerbestand gehören. Sie verfügen teilweise über keine Herstellergarantie, der Verbraucher erhält jedoch eine zweijährige Gewährleistung auf Neuware Sonderposten.

3. **Gebrauchte A-Ware** – Diese Stufe beinhaltet Geräte, die professionell aufbereitet wurden und refurbished sowie technisch geprüft sind. Sie können leichte Gebrauchsspuren aufweisen.
4. **Gebrauchte B-Ware** – Die Geräte erfüllen die gleichen Voraussetzungen wie A-Ware, jedoch können sie stärkere Gebrauchsspuren, die zu einem optischen Mangel führen, aufweisen. Eine Beeinträchtigung des Produkts in der Performance und der Funktion liegt nicht vor.

Vorteile von Refurbished IT-Geräten

Der **deutlich günstigere Preis** steht an erster Stelle bei Refurbished Produkten. Durch die gründliche Überprüfung, Reinigung und eventuelle Instandsetzung erhält man für weit weniger Geld als bei einem Neukauf ein nahezu gleichwertiges Gerät, insbesondere was die Technik anbetrifft.

Befürworter von generalüberholten Waren führen zudem an, dass ein gebrauchtes Gerät – im Gegensatz zu einem neuen – einer zusätzlichen Kontrolle beziehungsweise Prüfung unterzogen wurde. Eventuelle Schwächen oder Fehler wurden bereits vom Erstnutzer erkannt, was zur Rückgabe führte. Bei Refurbished Produkten wurden diese beseitigt. Dies führt zu einer geringeren Schadenshäufigkeit.

Nachteile von Refurbished IT-Geräten

Aufgrund der Tatsache, dass Refurbished IT häufig neuwertig ist und darüber hinaus mögliche Fehler bereits behoben wurden, entsteht beim Kauf im Prinzip kein Nachteil. Manche Menschen stören sich möglicherweise daran, dass in der Regel nicht die neusten Geräte in generalüberholter Form auf den Markt kommen.

Weist es deutliche Gebrauchsspuren auf, wirkt es sich ausschließlich nachteilig auf die Augen des Betrachters aus. Dies liegt jedoch in der Hand des Käufers, der ebenso viele Produkte ohne äußerliche Beschädigungen im Angebot findet. Als nachteilig kann angesehen werden, dass teilweise eine reduzierte Garantiedauer vorliegt.

Vorsicht beim Kauf von Refurbished IT-Geräten

Als problematisch für den Verbraucher stellt sich heraus, dass die Begriffe „refurbished“ und „generalüberholt“ nicht geschützt sind. Praktisch jeder Laden versteht darunter etwas anderes. Es ist wichtig, einen vertrauensvollen Händler aufzusuchen, da es sonst passieren kann, dass man ein Gerät erhält, welches möglicherweise nur äußerlich kurz gereinigt wurde.

Ein guter Shop bietet auf seine Refurbished IT-Geräte eine **mindestens einjährige Garantie** an. Grundsätzlich haben Käufer ein 14-tätiges Rückgaberecht. In dieser Zeit empfiehlt es sich, das Produkt ausführlich zu testen. Ein besonderes Augenmerk sollte dabei auf dem Akku

liegen. Liegt die Leistung noch auf etwa 90 Prozent, ist eine der Voraussetzungen für lange Haltbarkeit erfüllt.

Tipp: Es muss nicht immer eine Neuanschaffung sein. Vermeintlich defekte Geräte wie Smartphones, Tablets oder PCs lassen sich häufig auch [kostengünstig reparieren](#).

Also: Wer auf das neuste Modell verzichten kann und nicht aus emotionalen Gründen an einem Neugerät festhält, ist mit einem Refurbished IT-Gerät bestens bedient. Die Nachteile sind gering und werden problemlos von der Einsparung beim Kauf überwogen. Voraussetzung ist allerdings eine gute Recherche, um einen vertrauensvollen Händler mit einem individuell passenden Produkt zu finden.

Viel Erfolg, Kommissar KI!

In NRW testen Behörden eine KI-Software, um im Bereich der Kinderpornografie im Netz erfolgreicher zu fahnden. Ein Pilotprojekt, an dem sich Fachleute, Wissenschaftler und auch Microsoft beteiligen. Ein zweifellos sinnvoller Einsatz von KI. Aher wie funktioniert's?

Fotos und Videos mit sexueller Gewalt an Kindern gab es vermutlich schon immer. Doch niemand kann ernsthaft bestreiten, dass die Digitalisierung und vor allem das Internet der solchen Videos Vorschub leisten, wie keine andere Kulturtechnologie zuvor. Es war noch nie so einfach und günstig, Fotos und Videos zu machen - und sie so bequem und effektiv an perverse Abnehmer in aller Welt zu verteilen.

Kein Zoll, der Päckchen anschaut. Kein Fotostudio, das auffällige Aufnahmen meldet. Im Darknet lässt sich zu allem Überfluss auch noch alles im Schatten der Anonymität abwickeln. Kein Wunder, dass dieser Schandfleck der Menschheit wächst und wächst.



Täterinnen und Täter agieren im Schatten der Anonymität

Gleichzeitig ist es für Polizei und Behörden sehr schwierig, Täter und Abnehmer ausfindig zu machen - eben weil es im Netz so einfach ist, sich (weitgehend) anonym zu bewegen. Das "Angebot" und damit das Problem explodieren regelrecht: Rund drei Petabyte Daten kursieren Experten zufolge im Netz. Schier unvorstellbare Mengen an perversen Bildmaterial.

Ein Beamter kann sich maximal 500 Bilder pro Stunde anschauen. Es bräuchte vermutlich ein Sonderkommando von der Größe eines ganzen Landes, um überhaupt nur annähernd alles relevante Material zu sichten. Die Strafverfolgung ist dann noch ein ganz anderes Thema. Deshalb ist KI (Künstliche Intelligenz) die einzige Lösung. Microsoft entwickelt schon lange Algorithmen, um KI-gestützt kinderpornografische Aufnahmen (Fotos und Videos) im Netz zu entdecken. Und um gesuchte Personen zu identifizieren.



Forschungsprojekt will Fahndung verbessern

Außerordentlich begrüßenswert also, dass in NRW nun ein digitales Forschungsprojekt startet: Behörden wie die Staatsanwaltschaft Köln, Forscher der Universität des Saarlandes und Softwareexperten von Microsoft sowie von einigen anderen engagierten Stellen experimentieren mit "Kommissar KI".

Ganz ehrlich: Ich kann mir kaum einen sinnvolleren Einsatz für KI vorstellen. Jede/r einzelne

Täter/in weniger (es sind auch Frauen, die solche Angebote ermöglichen) und vor allem jede/r Abnehmer/in weniger ist ein Erfolg. KI kann helfen, den Fahndungsdruck erheblich zu erhöhen.

Allein die Sorge, in Zukunft wahrscheinlicher und schneller entdeckt zu werden, könnte bei dem ein oder anderen genug Druck aufbauen, es lieber zu lassen. Man kann dem Projekt also wirklich nur die Daumen drücken!

<https://vimeo.com/331395648>

Fassaden verpixeln oder nicht?

Verpixelte Häuserfassaden in Google Streetview: Das gibt es nur in Deutschland - und droht nun auch der geplanten Alternative Apple Look Around. Doch es stellt dich die Frage: Wieso überhaupt Fassaden verpixeln? Als Widerstand gegen die Datensammelwut - oder gibt es vernünftige Gründe?

Als Google Street View vor etwa zehn Jahren in Deutschland gestartet ist, gab es heftige Diskussionen um die Frage, ob Häuserfassaden nun für jeden auf der Welt sichtbar veröffentlicht werden dürfen oder nicht. Die Verpixelungs-Front hat gesiegt: Wenn Hausbesitzer oder Mieter es nicht wollen, kommt ein "Blur" (Unschärfefilter) über die entsprechende Fassade - und schon sieht Street View an dieser Stelle vermatscht aus.



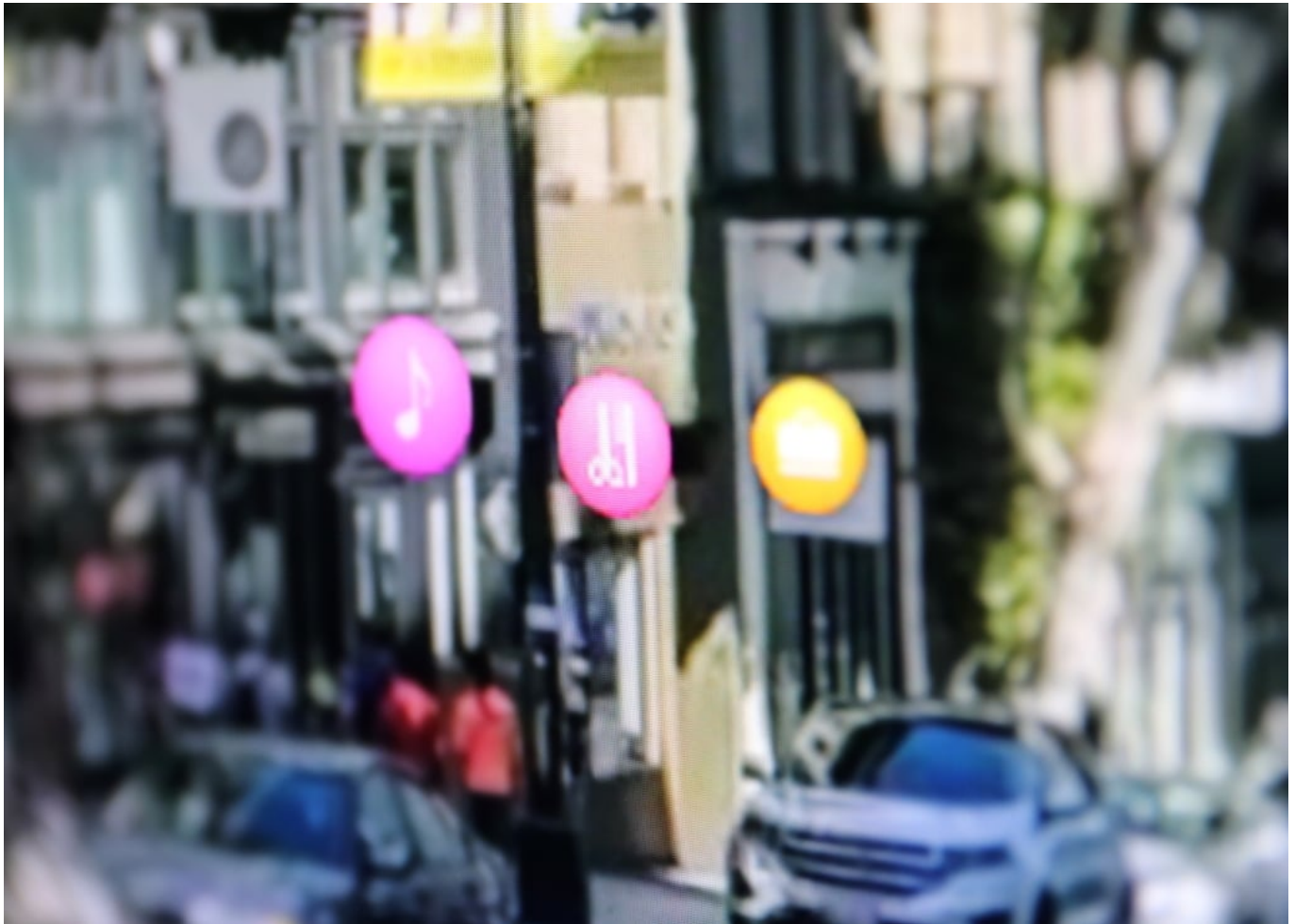
Noch unsicher, ob Aufnahmen aus Deutschland veröffentlicht werden

Bei Apples Look Around wird es genauso sein. Zwar sind die Proteste nicht mal ansatzweise so laut wie vor zehn Jahren - was möglicherweise daran liegen könnte, dass sich die Menschen an überall und ständig alles fotografierende Passanten gewöhnt haben.

Aber es ist interessant: Apple will nun mehr oder weniger dasselbe machen wie Google vor zehn Jahren - doch Widerstand gibt es wenig. Vielleicht auch deshalb, weil Apple von vorneherein sagt: Wir wissen um die besondere Situation in Deutschland und bieten schon Monate vor Veröffentlichung der Aufnahmen die Möglichkeit, eine Verpixelung zu beantragen

(per E-Mail).

Dabei ist - Stand heute - nicht mal klar, ob Apple die Aufnahmen, die die rund 80 Spezialfahrzeuge derzeit machen, überhaupt im Look Around-Dienst veröffentlicht werden. Erst im kommenden Jahr will Apple entscheiden, ob die Aufnahmen gezeigt werden sollen oder nicht. Sie werden vor allem gemacht, um das Kartenmaterial selbst zu optimieren (in Apple Maps). Der Look Around-Dienst mit seinen Panoramabildern ist nur ein (möglicher) Bonus.



Warum ein Recht auf Verpixelung?

Klar, dass sich [Apple](#) nicht festlegen möchte - nach den Erfahrungen, die Google in Deutschland gemacht hat. Wegen der juristischen Auseinandersetzungen und der zahllosen verpixelten Fassaden hat Google in Deutschland die Lust verloren: Seit zehn Jahren gibt es keine neuen Aufnahmen. Und neue Orte, die von Street View abgebildet werden, gibt es auch nicht. Der Zustand von Street View ist in Deutschland eingefroren - während im Rest der Welt ständig neue und aktualisierte Aufnahmen dazu kommen.

Ich bin immer für Datenschutz und den Schutz der Privatsphäre. Aber der öffentliche Raum gehört allen - nicht einzelnen. Klar, dass Gesichter und Autokennzeichen verpixelte gehören.

Aber doch keine Häuserfassaden. Die sind nun mal da. Wirklich gute Gründe, wieso es ein Recht auf Verpixelung geben sollte, konnte mir auch der Jurist Michael Terhaag nicht liefern (siehe Video).

Terhaag erklärte mir: Die auf den Spezialfahrzeugen montierten Kameras (egal ob Google, Apple oder denen anderer Anbieter) sind etwas höher als die Augenhöhe eines typischen Passanten. Das strapaziert die [Panoramafreiheit](#) (die urheberrechtliche Freiheit bestimmte Bauwerke fotografieren zu dürfen) schon mal. Dann wäre es schon etwas anderes, wenn in einer Datenbank **alle** Hausfassaden eines Ortes oder Landes gespeichert werden.

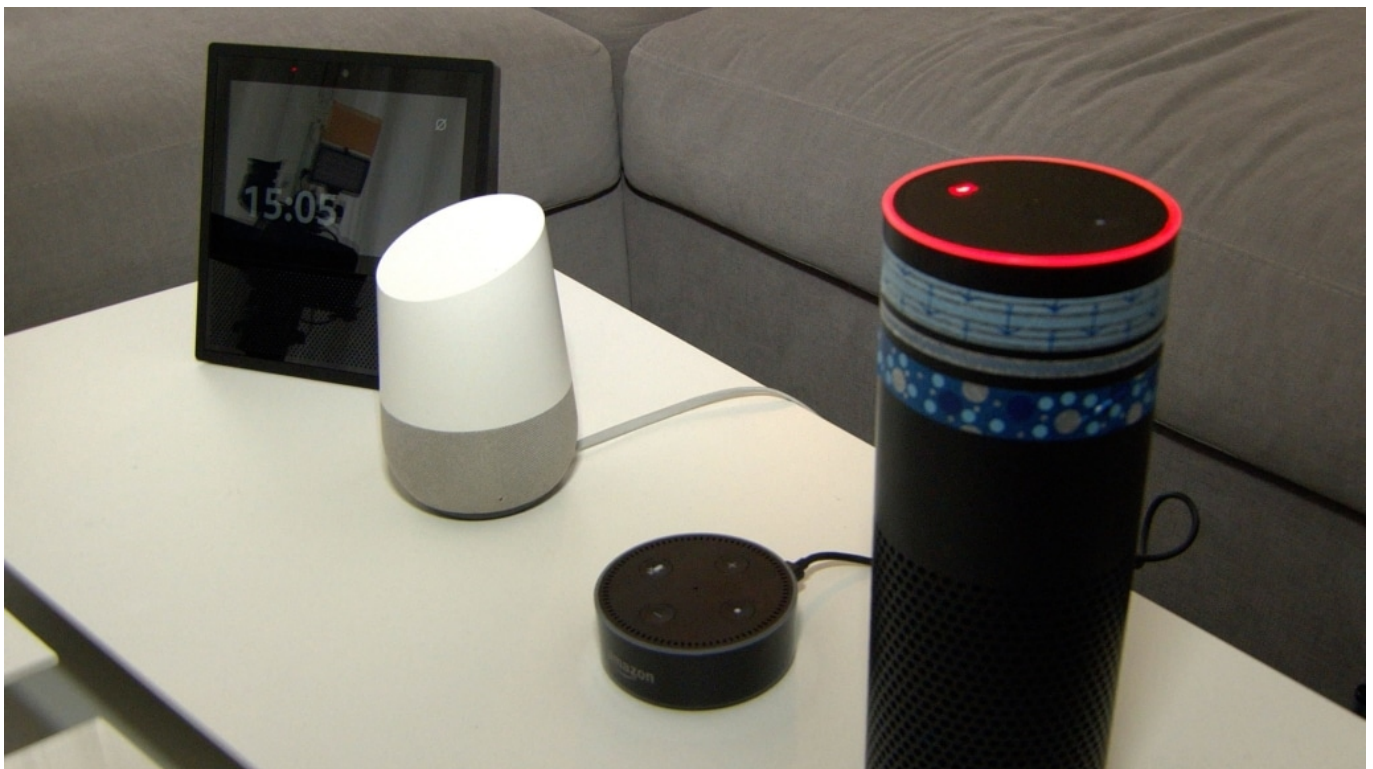
Stimmt. Aber wem schadet das im Alltag tatsächlich? Ein Blick in den Hintergarten-Pool oder nicht? - mit Google Earth ist im Zweifel viel indiskreter. Das stört aber niemanden.

<https://vimeo.com/351786011>

Bei Apple Siri hören keine Menschen mehr zu!

Stichprobenartig hören Menschen aus Fleisch und Blut in ausgewählte Gesprächsfetzen hinein, die Digitale Assistenten wie Siri, Alexa, Cortana oder Google Assistant nicht verstanden haben. Um die Qualität zu verbessern. Das Problem: Die meisten User ahnen nichts davon - und es macht einen Unterschied, ob Menschen oder Maschinen mithören. Apple hat die Praxis jetzt erst mal gestoppt.

Heute schon ein paar Worte mit [Alexa](#), Cortana, Google Assistant oder Siri gewechselt? Den meisten ist gar nicht klar, was passiert, nachdem das Schlüsselwort ("Alexa", "Google", "Siri") gefallen ist. Die Geräte stellen blitzschnell eine Online-Verbindung zu den Servern des jeweiligen Anbieters her, übertragen das Gesagte und warten auf die Auswertung durch die KI-Software. Das geschieht in der Regel derart schnell, dass die Menschen denken, das Smartphone oder die Box hätte den Job erledigt. Ist aber nicht so.



Echte Menschen hören Gespräche ab

Doch nicht immer "verstehen" die Algorithmen, was gesagt wurde. Unter anderem auch deshalb, weil häufig versehentlich Sprachfetzen übertragen werden, die gar nicht für den Assistenten gedacht waren. Dann gehen einzelne Wörter oder Sätze an die Server - obwohl das Schlüsselwort nicht gefallen ist.



Von Amazon, Apple und Google wissen wir, dass sich deshalb echte Menschen aus Fleisch und Blut einige dieser Sprachfetzen anhören - und analysieren, warum die Algorithmen das nicht verstanden haben. Sie schreiben Protokolle, was gesagt wurde. So soll das "Verstehen" verbessert werden, indem unterschiedliche Aussprachen und Dialekte trainiert werden.

Das Problem: Die User wissen nichts davon - sie wurden auch nicht wirklich gefragt. Denn wenn eine Maschine zuhört, ist das eine Sache. Wenn echte Menschen etwas anhören, was ich gesagt habe - auch wenn ich sie nicht kenne und die Gesprächsfetzen angeblich anonymisiert untersucht werden -, so hat das doch eine ganz andere Qualität. Den meisten Menschen ist das schlichtweg unangenehm. Verständlicherweise.

User müssen besser informiert werden

Google hat deshalb schon im Juli das Abhören von Sprachdateien beim Google Assistant in Europa ausgesetzt. Jetzt hat auch Apple nachgezogen - und [verzichtet vorerst ebenfalls darauf](#), Anweisungen oder Gespräche von echten Menschen analysieren zu lassen. Allerdings nur, weil Siri-User davon nichts wissen. Künftig sollen sie besser informiert und um Erlaubnis gebeten werden. Das ist natürlich eine enorme Verbesserung der Situation.

Was auch geklärt werden müsste: Was bedeutet es konkret, wenn Unternehmen wie Amazon, Apple, Google und Microsoft behaupten, die Daten würden anonymisiert, bevor sie von Menschen ausgewertet werden? Ist das wirklich zuverlässig? Außerdem: Wer wertet die Gesprächsfetzen aus? Die meisten Unternehmen lassen nicht nur eigene Mitarbeiter ran, sondern auch Mitarbeiter in externen Unternehmen - was ein zusätzliches Sicherheitsproblem darstellt.

Darüber hinaus hilft alle Anonymisierung nichts, wenn sich anhand der aufgezeichneten

Gesprächsfetzen ableiten lässt, wer da mit wem spricht - und worüber. Das ist in Einzelfällen durchaus möglich.

Es gibt also viele gute Gründe, die Sprachassistenten (auch) kritisch zu sehen.

<https://vimeo.com/351578604>

Wenn Internetseiten nicht erreichbar sind: Der DNS-Server

Eine immer wieder vorkommende Störung beim Aufruf von Internetseiten ist die Namensauflösung. Wenn Sie <http://www.schieb.de> als Internet-Adresse eingeben, dann wird dieser Name – der für das Internet nur eine Buchstabenwolke ist – in die IP-Adresse umgesetzt. Funktioniert das nicht, dann findet der Browser die gewünschte Seite nicht.

Das können Sie nachvollziehen, indem Sie in einer Eingabeaufforderung den Befehl **ping** eingeben. Ersetzen Sie dabei durch die Adresse der Webseite.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.557]
(c) 2018 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\andre>ping schieb.de

Ping wird ausgeführt für schieb.de [54.93.189.161] mit 32 Bytes Daten:
Antwort von 54.93.189.161: Bytes=32 Zeit=13ms TTL=52
Antwort von 54.93.189.161: Bytes=32 Zeit=12ms TTL=52
Antwort von 54.93.189.161: Bytes=32 Zeit=12ms TTL=52
Antwort von 54.93.189.161: Bytes=32 Zeit=12ms TTL=52

Ping-Statistik für 54.93.189.161:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 12ms, Maximum = 13ms, Mittelwert = 12ms

C:\Users\andre>
```

Wenn die Namensauflösung funktioniert, dann wird die URL in die zugehörige IP-Adresse umgesetzt. Sie sehen dann die IP-Adresse neben dem Text „Ping wird ausgeführt für...“. Funktioniert sie aber nicht, dann ist es kein Wunder, dass sie keine Internetseiten aufrufen können! Hier können Sie versuchen, den DNS-Server zu verändern. Der ist für die Namensauflösung zuständig.

Der DNS-Server wird vom Internetanbieter vorgegeben, ist also im Standard vorangestellt. Wenn Sie diesen manuell ändern wollen, dann öffnen Sie die Konfigurationsoberfläche Ihres Routers. In den Interneteinstellungen bei den Zugangsdaten finden Sie einen Reiter DNS-Server. Hier tragen Sie beispielsweise 1.1.1.1 (für den schnellen Cloudflare-DNS-Server)

FRITZ!Box 7490

Internet > Zugangsdaten

Internetzugang

IPv6

LISP

AVM-Dienste

DNS-Server

Hier können Sie auswählen, ob für die Namensauflösung von Internet-Adressen die vom Internetanbieter verwendet werden sollen.

DNSv4-Server

- Vom Internetanbieter zugewiesene DNSv4-Server verwenden (empfohlen)
- Andere DNSv4-Server verwenden

Bevorzugter DNSv4-Server: . . .

Alternativer DNSv4-Server: . . .

DNSv6-Server

- Vom Internetanbieter zugewiesene DNSv6-Server verwenden (empfohlen)
- Andere DNSv6-Server verwenden

Bevorzugter DNSv6-Server

Alternativer DNSv6-Server

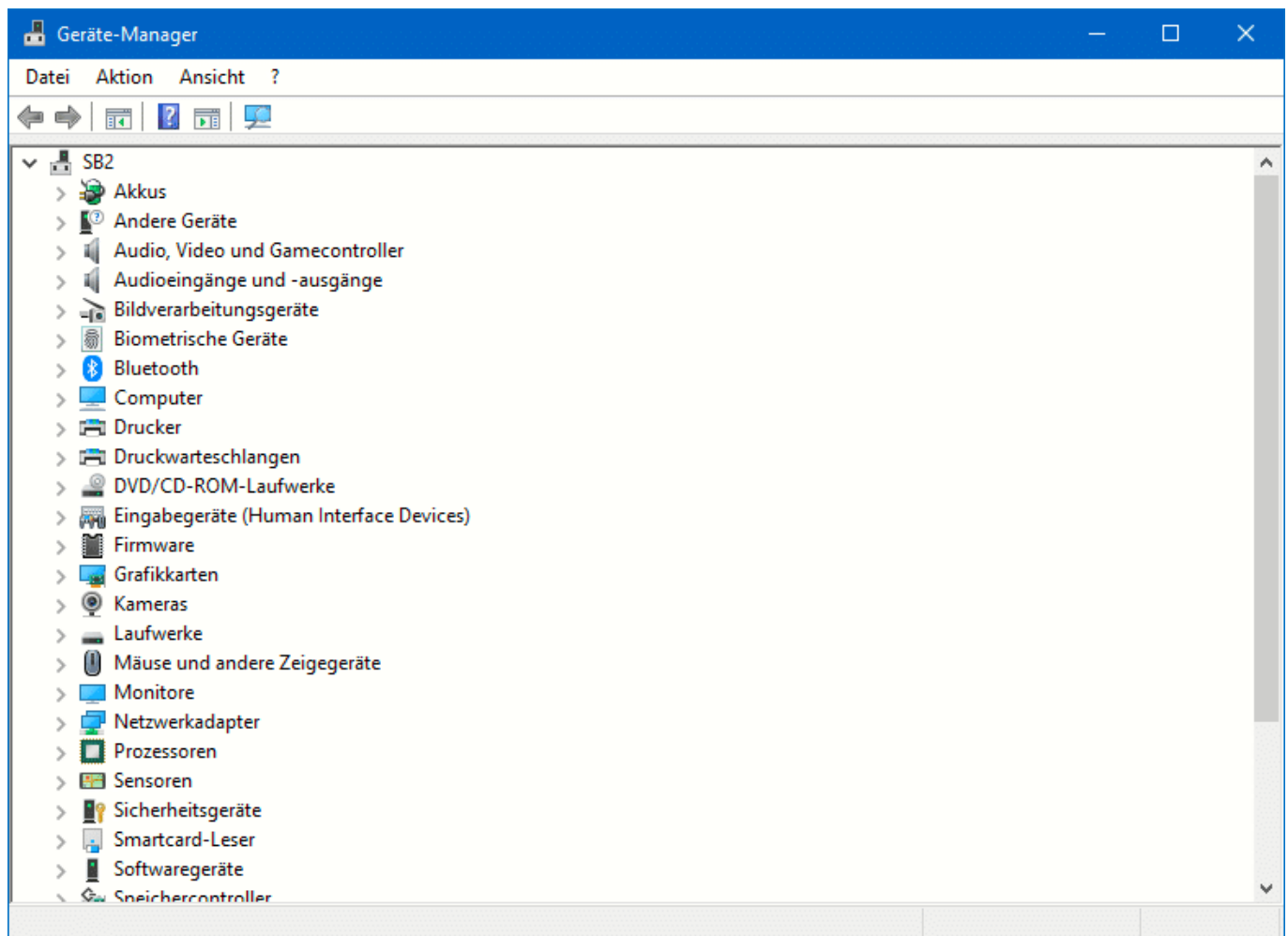
Eine Liste von DNS-Servern finden Sie unter anderem unter <https://www.ungefiltert-surfen.de/nameserver/de.html>.

Sie sollten sicher sein, dass der DNS-Server vertrauenswürdig ist. Ist dieser in den Händen von Cyber-Bösewichten, dann können diese Ihre Anfrage umleiten auf eine beliebige Seite. Diese sieht dann genauso aus wie die echte Seite, hat nur Viren und Trojaner für Sie im Angebot. Und da Sie ja die richtige URL eingegeben haben, sind Sie nicht misstrauisch!

Hardwareprobleme im Gerätemanager lösen

Auch wenn Sie heute meist ein komplett fertiges Gerät anschaffen: Ein PC besteht aus einer Vielzahl von Komponenten, die zusammenarbeiten müssen. Oft sehen Sie diese gar nicht, weil sie sich auf der Hauptplatine befinden. Ist aber nur einer dieser Komponenten gestört, defekt oder wird nicht richtig angesprochen, dann sind die Auswirkungen groß. Der Geräte-Manager kann die Lösung bieten!

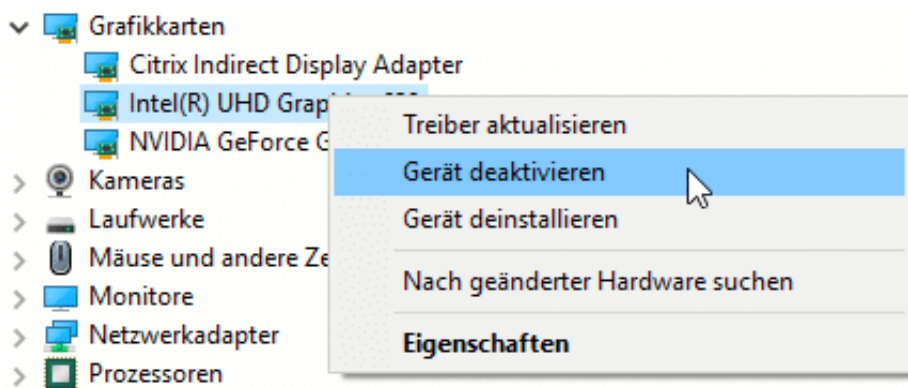
Die erste Anlaufstelle bei Hardwareproblemen ist der Geräte-Manager. Diesen erreichen Sie, indem Sie im Suchfeld **Gerätemanager** eingeben und diesen dann durch einen Klick starten.



Windows 10 zeigt Ihnen nun nach Kategorien geordnet alle Geräte an, die es erkannt hat. Klicken Sie auf den kleinen Pfeil vor einer Kategorie. Dann bekommen Sie alle Geräte darin angezeigt. Wenn eine Störung vorliegt, das Gerät nicht erkannt wird oder nicht angesprochen werden kann, dann sehen Sie an seinem Symbol ein Ausrufezeichen in einem gelben Kreis. Klicken Sie doppelt darauf, um eine Fehlerbeschreibung zu kommen.



Wenn ein Problem dauerhaft Probleme bereitet, dann kann die Deaktivierung eine Hilfe sein. Im Standard versucht Windows kontinuierlich, mit angeschlossenen Geräten zu kommunizieren. Damit erhalten Sie wieder und wieder Fehlermeldungen.



Um ein Gerät zu deaktivieren, klicken Sie mit der rechten Maustaste hinein, dann auf **Gerät deaktivieren**. Windows weiß nun, dass es das Gerät nicht mehr ansprechen soll.

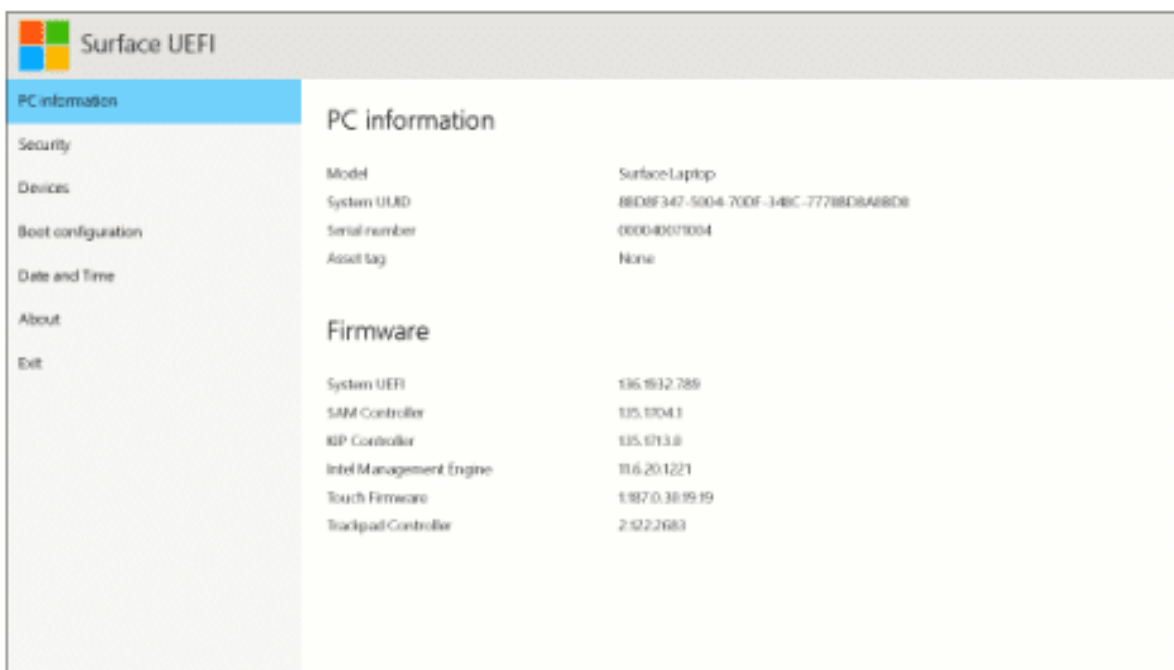
Es kann damit zwar nicht mehr verwendet werden, produziert aber auch keine Fehlermeldungen mehr.

Booten eines Surface/Notebooks im UEFI-Modus

Wenn Ihr PC einwandfrei startet, dann ist kein Eingriff nötig. Wenn allerdings Windows nicht mehr laden will, der Bootvorgang hängen bleibt, kryptische Fehlermeldungen auf dem Bildschirm angezeigt werden, dann sieht es schon anders aus: Früher war in solchen Fällen das BIOS der Ort der Fehlerbehebung, mittlerweile vermehrt das UEFI (Unified Extensible Firmware Interface), die Schnittstelle zwischen der Hardware Ihres Rechners und Windows.

Um dort hinein zu gelangen, sind einige Handgriffe nötig. Bei den meisten moderneren Geräten funktioniert folgendes Vorgehen:

1. Fahren Sie das Gerät herunter (wenn das noch geht) oder schalten Sie es durch längeres Drücken des Power-Schalters aus.
2. Warten Sie 10 Sekunden.
3. Halten Sie die Lauter-Taste des Gerätes gedrückt. Parallel dazu schalten Sie es ein.
4. Halten Sie die Taste so lange gedrückt, bis der UEFI-Bildschirm erscheint.



Um den UEFI-Modus aus dem System zu erreichen, gehen sie wie folgt vor:

1. In den Windows 10-Einstellungen klicken Sie auf **Update & Sicherheit > Wiederherstellung > Erweiterter Start > Jetzt neu starten**.
2. Wählen Sie auf dem Bildschirm **Option auswählen** die Option **Problembehandlung** aus.
3. Dann klicken Sie auf **Erweiterte Optionen** **> UEFI-Firmware-Einstellungen > Neu starten** aus.

Erweiterter Start

Starten Sie von einem Gerät oder Datenträger (beispielsweise von einem USB-Laufwerk oder einer DVD), ändern Sie die Firmwareeinstellungen Ihres PCs, ändern Sie die Windows-Starteinstellungen, oder stellen Sie Windows mithilfe eines Systemimage wieder her. Dadurch wird Ihr PC neu gestartet.

Jetzt neu starten

vorher sollen Sie alle Programme beendet und alle Dateien gespeichert haben, damit Sie keinen Datenverlust erleiden.

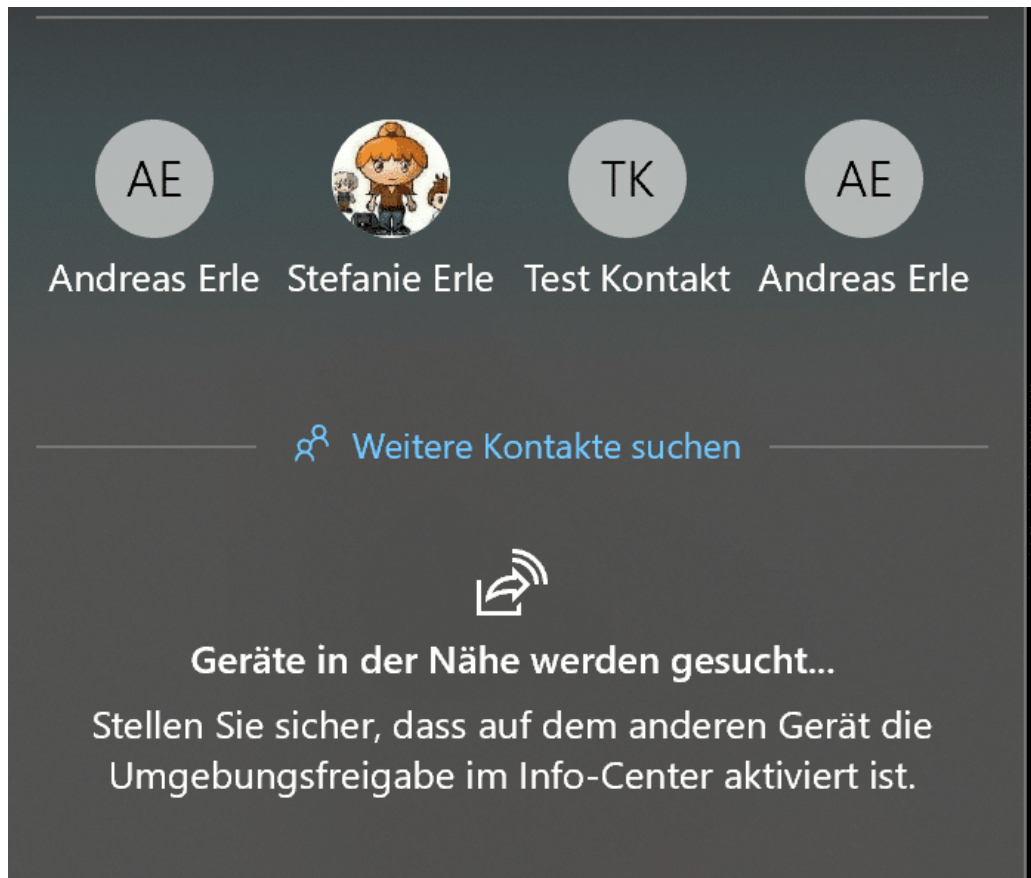
Schnelles Freigeben von Elementen unter Windows 10

Gerade in der Arbeitswelt werden Sie nur noch in den seltensten Momenten alleine und ohne Andere arbeiten. Kollaboration ist das Wort der Stunde. Und so ist der Austausch von Informationen und Dokumenten etwas ganz Normales. Statt nun immer wieder eine E-Mail mit Anhang zu verschicken, verwenden Sie doch einfach die Umgebungsfreigabe.

Die Umgebungsfreigabe ist fester Bestandteil von Windows. Sie funktioniert so ähnlich wie das von macOS bekannte [Airdrop](#): Die Umgebung wird nach Geräten durchsucht, die empfangsbereit wären. Grundvoraussetzung: Sie aktivieren auf jedem Gerät im InfoCenter die Umgebungsfreigabe durch Aktivieren der Schaltfläche. Nur dann ist ein Gerät auch sichtbar für andere Geräte.

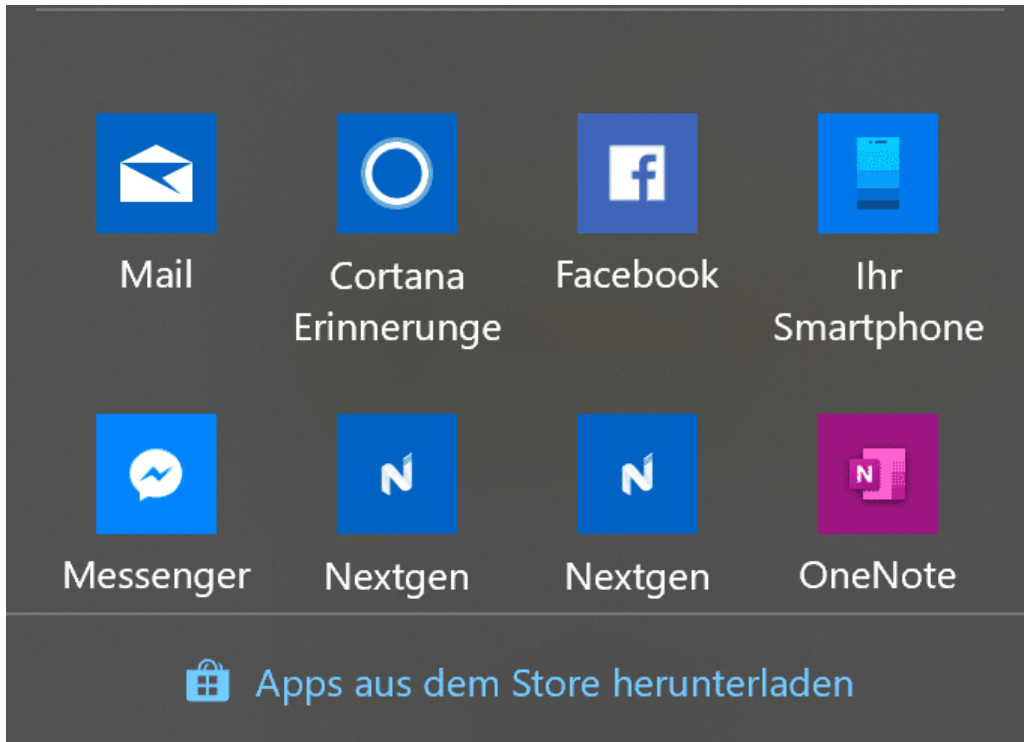


Um ein Element (das kann eine Webseite, ein Word-Dokument, ein Bild sein) zu teilen, klicken Sie auf das Teilen-Symbol im jeweiligen Programmfenster. Windows 10 durchsucht jetzt die Umgebung nach empfangsbereiten Geräten.



Wählen Sie aus der Liste dann einfach dasjenige aus, an das das Element geschickt werden soll. Ohne weiteres Zutun bauen die beiden Geräte nun eine Verbindung miteinander auf und das Element wird versendet.


Wenn Sie kein Gerät finden, dann stellt Ihnen Windows 10 gleich die Standardmethoden zur Verfügung. Wählen Sie aus der Liste aus, ob Sie per E-Mail, Facebook, dem Smartphone etc. den Versand vornehmen wollen. Das ist zwar vom Arbeitsablauf her ein wenig aufwändiger, funktioniert aber auch.



The image shows a screenshot of a Windows Start menu with a dark grey background. It features two rows of application tiles. The first row contains four tiles: Mail (blue square with a white envelope icon), Cortana Erinnerunge (blue square with a white circle icon), Facebook (blue square with a white 'f' icon), and Ihr Smartphone (blue square with a white smartphone icon). The second row contains four tiles: Messenger (blue square with a white speech bubble icon), Nextgen (blue square with a white 'N' icon), Nextgen (blue square with a white 'N' icon), and OneNote (purple square with a white 'N' icon). Below the tiles is a dark grey bar with a shopping bag icon and the text "Apps aus dem Store herunterladen".

Mail Cortana Erinnerunge Facebook Ihr Smartphone

Messenger Nextgen Nextgen OneNote

 Apps aus dem Store herunterladen

Den abgesicherten Modus als Verknüpfung anlegen

Wenn Sie häufiger an Ihrem Rechner Veränderungen vornehmen, dann kann es durchaus vorkommen, dass Sie häufiger im abgesicherten Modus starten müssen. Statt nun mit viel Aufwand durch Menüs zu klicken machen Sie es sich einfacher: Legen Sie sich doch einfach eine Verknüpfung auf dem Desktop dazu an!

Viele der Funktionen von Windows sind nichts anderes als ein Programm, das tief in den Systemverzeichnissen schlummert. Diese Programme können auf vom Benutzer aufgerufen werden. Allerdings verwenden sie eine Vielzahl von Parametern, die erst die Funktionen richtig zur Anwendung bringen.

Für ein solches Programm können Sie auf dem Desktop eine Verknüpfung anlegen. Diese ruft das Systemprogramm mit den richtigen Parametern auf. Sie selbst müssen die Verknüpfung dann einfach nur noch starten.

Dazu klicken Sie mit der rechten Maustaste auf einen freien Bereich des Desktops, dann auf **Neu > Verknüpfung**.



Für welche Elemente möchten Sie eine Verknüpfung erstellen?

Mit diesem Assistenten können Sie Verknüpfungen mit lokalen oder vernetzten Programmen, Dateien, Ordnern, Computern oder Internetadressen erstellen.

Geben Sie den Speicherort des Elements ein:

Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.

Geben Sie nun den Befehl **shutdown.exe /r /o /f /t 00** ein und klicken Sie auf **Weiter**. Geben Sie der Verknüpfung einen Namen. Beispielsweise Abgesichert. Unter diesem Namen wird die Verknüpfung auf dem Desktop gespeichert. Voila: Nun müssen Sie nur noch den Doppelklick machen und schon startet Ihr Rechner im abgesicherten Modus!

Unterwegs nicht auf ein Multimonitor-Setup verzichten

Der Mensch ist ein Gewohnheitstier. Kaum hat er sich an etwas gewöhnt, mag er es nicht mehr missen. Im Büro, ja auch zuhause haben Sie sich mittlerweile daran gewöhnt, mindestens zwei, wenn nicht gar mehr Monitore zur Verfügung zu haben. Der Platz auf dem Desktop kann nicht groß genug sein. Wenn Sie sich unterwegs jetzt auf einen einzigen Monitor beschränken müssen, dann fehlt etwas. Schließlich hat das Notebook nur einen Bildschirm, und im Reisegepäck ist ein externer Monitor kaum tragbar. Die Lösung kommt von Asus.

Die Zenscreens sind portable USB-C-Monitore mit Full HD-Auflösung. Sie sind von Größe und Gewicht her vergleichbar mit dem Display eines Notebooks und passen damit wunderbar in eine Notebooktasche. Die Diagonale von knapp 15 Zoll entspricht der eines Standard-Laptops. Der Clou: Sie brauchen keine Stromversorgung, denn USB-C bringt diese ja automatisch mit.



Um das Gerät nun ohne Fuß hingestellt zu bekommen, gibt es zwei Möglichkeiten: Zum einen haben die ZenScreens eine magnetische Tasche, die an der Hinterseite des Displays hält. Verschiedene Faltpositionen erlauben - wie bei normalen Tablet-Taschen - verschiedene Winkel und Positionen. Zum anderen hat jeder ZenScreen ein Loch unten rechts, in das ein Stift

eingelegt werden kann. Der dient dann als Standfuß.

Wer kein USB-C zur Verfügung hat, der findet mit dem [ZenScreen GO](#) eine Alternative: Der bringt ein Adapter von einem Standard USB-A-Anschluss auf das USB-C des Display mit. Um das Problem der Stromversorgung zu lösen, hat er einen integrierten Akku. Dieser schafft ungefähr vier Stunden Laufzeit. Die ZenScreens gibt es je nach Modell für zwischen EUR 220 und EUR 320 im wohlsortieren Einzelhandel und online.

Wenn echte Menschen Gespräche mit Assistenten abhören

Viele haben heute „smarte Lautsprecher“ wie Alexa, Google Home, Apple HomePod oder vergleichbare Geräte stehen. Oder sie sprechen im Auto mit dem Assistenten, mit Alexa, Siri, Cortana oder Google Assistant. Und im Smartphone sind auch welche eingebaut. Doch was viele nicht wissen: Gelegentlich hören Menschen aus Fleisch ab, was wir mit den Assistenten gesprochen haben – teilweise auch ungewollt aufgenommene Sprachfetzen. Apple hat jetzt angekündigt, das einzustellen.

Wichtig zu wissen: Wenn das jeweilige Schlüsselwort fällt – also je nach Hersteller „[Alexa](#)“, „Google“, „Siri“, „Cortana“ oder was auch immer –, geht alles, was danach gesprochen wird, an einen Server des jeweiligen Anbieters. Also zu Google, Amazon, Apple, Microsoft.

Denn hier wird mit KI versucht, blitzschnell das Gesprochene zu interpretieren: Eine Frage, eine Anweisung, ein Wunsch? Es ist nicht einfach, gesprochene Befehle zu verstehen, deswegen geht alles zu Servern und wird nicht im Gerät erledigt. Die Antwort kommt dann zurück. Nur: Das klappt nicht immer.

Es gibt häufig Probleme. Um herauszufinden, woran es liegt, dass die KI-Software nicht richtig versteht, hören gelegentlich echte Menschen in die Audioaufnahmen hinein – und versuchen so, der Maschine das Zuhören beizubringen.



Wer hört denn da genau zu – und was hören sie an?

Ausgewählt zum Probehören durch Menschen werden Gesprächsfetzen, die Schwierigkeiten bei der Analyse gemacht haben. Etwa, weil genuschelt wurde, weil mehrere Leute gleichzeitig geredet haben, ein Akzent oder Dialekt dabei war – oder einfach, weil aus Versehen etwas aufgezeichnet wurde, was gar nicht für die Assistenten gedacht war.

Echte Menschen können das dann viel besser verstehen. Sie machen sich Notizen und sollen so helfen, die KI-Systeme zu verbessern. Es sind Mitarbeiter der jeweiligen Unternehmen, also Amazon, Google, Apple und Co. – oder Mitarbeiter von Unternehmen, die dafür bezahlt werden, also in externen Firmen. Wer das genau macht, weiß man nie. Aber alle Unternehmen machen solche Stichproben.



Und die wissen dann und hören dann, was jemand sagt oder fragt?

Im Grunde schon. Allerdings versichern Apple, Amazon und Google, dass die Sprachfetzen anonymisiert sind. Das heißt, die Abhörexperten wissen nicht, von wem sie da etwas hören. Ob das stimmt, können wir nicht wissen und auch nicht kontrollieren. Außerdem gibt es Situationen, da erschließt sich schon aus dem aufgezeichneten Gespräch, wer redet, mit wem oder über wen. Da hilft die ganze mögliche Anonymisierung nichts.

Apple setzt Abhören vorerst aus

Apple hat das stichprobenartige [Abhören durch echte Mitarbeiter vorerst eingestellt](#). Google ebenso vor einigen Tagen – allerdings nur in der EU, wo strengere Datenschutzrichtlinien bestehen.

Der Hintergrund: Bislang war den meisten unbekannt, dass es zu stichprobenartigem Abhören durch Menschen kommt. Den meisten ist es – verständlicherweise – unangenehm zu wissen, dass möglicherweise echte Menschen Anweisungen oder versehentlich aufgezeichnete Gespräche aufzeichnen.

Das ist jetzt bekannt geworden – und viele User haben sich beschwert. Vor allem, weil über

diesen Sachverhalt gar nicht aufgeklärt wird. Apple will aber nicht vollständig darauf verzichten: Künftig werden die User informiert – und können sich entscheiden, ob sie ggf. zur Verbesserung des Services ein Abhören durch echte Menschen zustimmen wollen.



Alles gut jetzt bei Google und Siri?

Immerhin haben Google und Apple reagiert – und unternehmen etwas. Das finde ich positiv. Amazon zeigt sich wie immer unbeeindruckt und macht mit dieser Praxis erst mal weiter. Allerdings wird sich das nicht mehr lange durchhalten lassen: Die Aufmerksamkeit nimmt zu. Immer mehr Menschen wird klar, dass die Digitalen Assistenten ein Sicherheitsrisiko für die Privatsphäre darstellen. Ganz sicher werden auch die Vorschriften verschärft. "Sicher" ist kein Digitaler Assistent. Denn die Anweisungen werden dauerhaft auf Servern gespeichert

teilweise auch versehentlich aufgezeichnete Gesprächsfetzen.

Da stellt sich natürlich jeder die Frage: Kann ich das denn unterbinden, etwa wenn ich mit meinem Chef spreche oder als Journalist ein vertrauliches Interview führe?

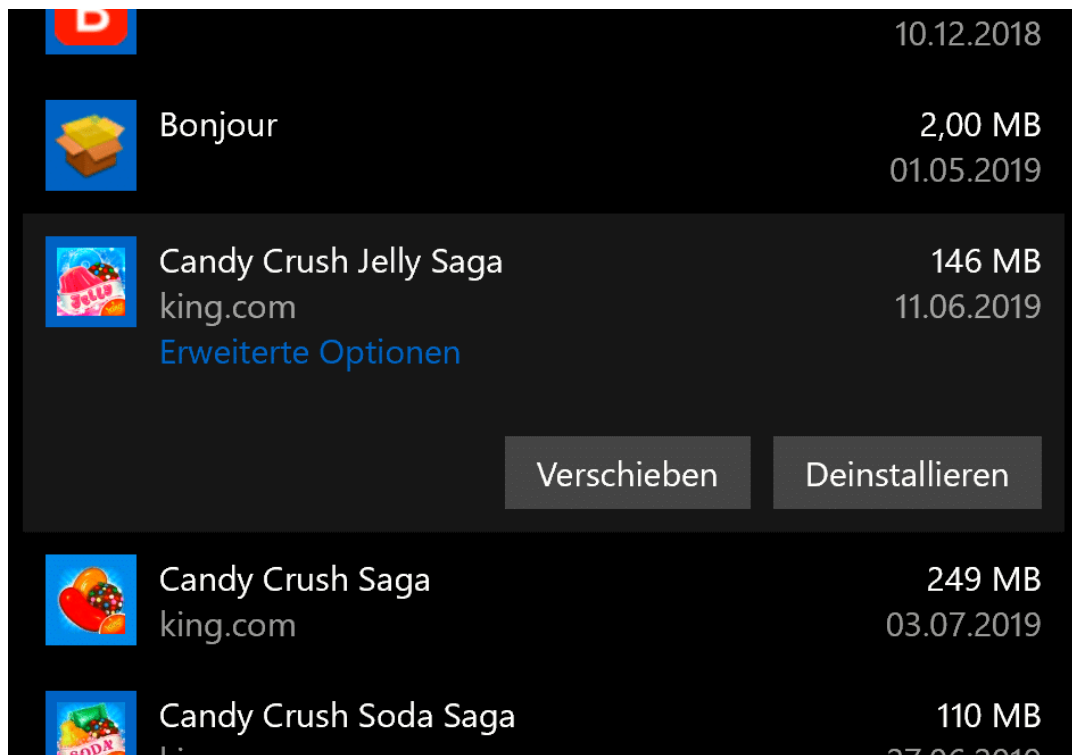
Die Antwort: Jein. Wer die Assistenten nutzt, muss immer damit rechnen, dass das gesprochene Wort auf Server geschickt und gespeichert wird. Wer Diskretion will: Stecker ziehen – ausschalten.

Und bei Siri und Co. auf dem Smartphone: Hier die Funktion deaktivieren, dass sie auf Schlüsselwort reagieren. Besser, man drückt den entsprechenden Button.

Apps & Programme auf eine Speicherkarte verschieben

Besonders auf mobilen Geräten wie Tablets und Notebooks ist der Speicher knapp. Neben Windows selbst, all Ihren Daten, Offlinekopien von Dateien sind auch die Programme auf der Festplatte oder SSD gespeichert. Das frisst Speicher. Und der wird irgendwann knapp. In der Regel erweitern Sie ihn durch Speicherkarten. Programme darauf zu verlagern ist einfacher, als Sie vielleicht denken!

Programme lassen sich nicht einfach von einem Ort zum anderen kopieren. Zumindest nicht so, dass sie dann auch noch laufen. Während der Installation werden diverse Dateien an verschiedenen Stellen des Systems abgelegt. Wenn diese woanders hingelegt werden, muss das Programm das mitgeteilt bekommen. Windows 10 hat dafür einen eigenen Mechanismus zur Verfügung.



Klicken Sie in den Einstellungen auf **Apps > Apps & Features**. Windows zeigt Ihnen nun eine Liste aller installierter Apps und Programme an. Diese können Sie sich nach Namen, aber auch nach Größen sortieren lassen. Klicken Sie nun die App an, die auf ein anderes Laufwerk verschoben werden soll.



Ein Klick auf **Verschieben** öffnet einen Dialog, in dem Sie das Ziellaufwerk, auf das das Programm verschoben werden soll, auswählen können. Wichtig dabei: SD-Karten und andere externe Datenträger sind noch nicht sofort beim Systemstart verfügbar. Wenn ein automatisch gestartet werden soll, dann lassen Sie es besser auf der internen Festplatte!

Speicher auf einem iOS-Gerät freimachen

Mit der Zeit sammelt sich auf einem mobilen Geräte eine Menge an Daten an. Nicht nur die über iTunes übertragenen Daten und die Dokumente, die Sie erzeugt haben. Es gibt viele Programme, mit denen Sie auf dem Gerät selbst Inhalte herunterladen können. Beispielsweise Netflix, das das Herunterladen von Filmen und Serienfolgen erlaubt. Die nehmen auf dem Gerät Platz weg, der dringend benötigt wird. Ohne direkten Speicherzugriff oder den PC können Sie die kaum unterwegs löschen. Allerdings versteckt iOS eine dazu hilfreiche Funktion in den Einstellungen.

Auch wenn iOS (noch) keinen wirklichen Zugriff auf den Speicher des iPads bietet, so hat das System doch einen Überblick, welche App welche Daten verwaltet. Das ist auch bei den Fotos und Videos der Fall. Diese Optimierungsmöglichkeiten bietet Ihnen iOS nur dann an, wenn der Speicher eng wird. Tippen Sie auf **Einstellungen** > **Allgemein** > **iPhone-/iPad-Speicher**. iOS zeigt Ihnen dann die Optimierungsmöglichkeiten an.



Fotos optimieren

[Aktivieren](#)

1,44 GB einsparen - Fotos und Videos in vollständiger Auflösung werden sicher in iCloud gespeichert und auf dem iPad werden Versionen in geringerer Auflösung verwendet.










iTunes-Videos prüfen



Bis zu 36,84 GB einsparen - Zeige alle aus iTunes geladenen Videos an und entferne sie bei Bedarf.

Wenn Sie viele Videos auf dem iPad haben, dann klicken Sie auf **iTunes-Videos prüfen**. Die Videos samt ihrer Größe werden angezeigt und Sie können sie mit einem Wischen nach links und **Löschen** vom Gerät entfernen.

EIGENE VIDEOS		29,44 GB
	Aquaman	3,98 GB
	Bumblebee	3,88 GB
Deadpool 2	834,9 MB	Löschen
	Escape Plan 2 - Hades	1,35 GB
	Jumanji.Willkommen.im.Dschungel.201...	806,6 MB
	klassentreffen.2019.german.1080p.bluray...	3,91 GB
	Spiderman - A New Universe	4,54 GB
	Star Wars Episode 7 - Das Erwachen der...	5,35 GB

Wenn Sie Videos mit einer App (wie beispielsweise [Netflix](#)) geladen haben, dann werden diese unter **Geladene Videos** angezeigt. Diese können Sie auf dem selben Weg vom Gerät entfernen und so Platz frei machen.

[← Zurück](#)

Geladene Videos

[Bearbeiten](#)

NETFLIX



St. 1: Flg. 10 – The Umbrella Academy

Noch nicht angesehen

260,8 MB

Wenn das WLAN Probleme macht

Oft ist nicht die die Internetverbindung an sich das Problem, sondern die WLAN-Verbindung. Diese ist stark abhängig davon, wo der Router ist und wo Sie sich befinden. Je mehr Mauern zwischen Ihnen und dem Router sind, desto schlechter das WLAN. Mit ein wenig Hilfe können Sie das Problem relativ schnell in den Griff bekommen.

Um einen Überblick zu bekommen, laden Sie sich das kostenlose Tool [Wireless Network View](#) herunter. Das nimmt die WLAN-Hardware Ihres Gerätes und durchsucht damit die Umgegend nach der empfangbaren WLANs ab. Die gefundenen WLANs werden dann in einer Liste dargestellt. **Last Signal** und **Average Signal** zeigen die Qualität des WLAN-Empfangs an. Je näher der Wert bei 100% ist, desto besser.

SSID	Last Signal	Average Si...	Detection ...	% Detection	Security En...	Connectable	Authentication	Cipher
(e) [SSID]	33%	35%	2	100.0%	Yes	Yes	802.11 Open	WEP
(e) AirTies_Air4...	76%	76%	2	100.0%	Yes	Yes	RSNA-PSK	CCMP
(e) AirTies_Air4...	54%	53%	2	100.0%	Yes	Yes	RSNA-PSK	CCMP
(e) AirTies_Air4...	90%	89%	2	100.0%	Yes	Yes	RSNA-PSK	CCMP
(e) AirTies_Air4...	30%	30%	1	100.0%	Yes	Yes	RSNA-PSK	CCMP
(e) CHESS	28%	29%	2	100.0%	Yes	Yes	RSNA-PSK	CCMP
(e) devolo-30d3...	24%	24%	1	50.0%	Yes	Yes	RSNA-PSK	CCMP
(e) DIRECT-b51...	30%	29%	2	100.0%	Yes	Yes	RSNA-PSK	CCMP
(e) DIRECT-ikC1...	57%	57%	2	100.0%	Yes	Yes	RSNA-PSK	CCMP
(e) FRITZ!Box 75...	37%	43%	2	100.0%	Yes	Yes	RSNA-PSK	CCMP
(e) Telekom_FON	28%	29%	2	100.0%	No	Yes	802.11 Open	None
(e) WOPPC_Spe...	80%	82%	3	100.0%	Yes	Yes	RSNA-PSK	CCMP
(e) WOPPC_Spe...	93%	94%	3	100.0%	Yes	Yes	RSNA-PSK	CCMP
(e) WOPPC_Spe...	39%	39%	3	100.0%	Yes	Yes	RSNA-PSK	CCMP
(e) WOPPC_Spe...	62%	60%	3	100.0%	Yes	Yes	RSNA-PSK	CCMP
(e) WOPPC_Spe...	82%	83%	3	100.0%	Yes	Yes	RSNA-PSK	CCMP
(e) WOPPC_Spe...	87%	89%	3	100.0%	Yes	Yes	RSNA-PSK	CCMP

22 Wireless Networks, 1 Selected
 NirSoft Freeware. <http://www.nirsoft.net>

Wenn Sie die Möglichkeit haben, dann stellen Sie den Router so auf, dass Sie an den Stellen möglichst guten Empfang haben, wo Sie surfen.

Nun wird das aber nicht immer einfach zu realisieren sein. Die Position des Routers hängt vor allem von der der Kabel ab. Und die wiederum wird durch die Steckdose in Ihrer Wohnung festgelegt. Für dieses Problem gibt es aber eine technische Lösung, die so genannten [WLAN-Repeater](#) (oder Range Extender). Wie auch immer sie heißen, eines haben sie gemeinsam: Sie werden in die Steckdose gesteckt, nehmen das WLAN des Routers auf und verstärken es. Sie können mehrere Repeater hintereinanderschalten und damit das ganze Haus mit stabilem

WLAN versorgen.