Schieb Report

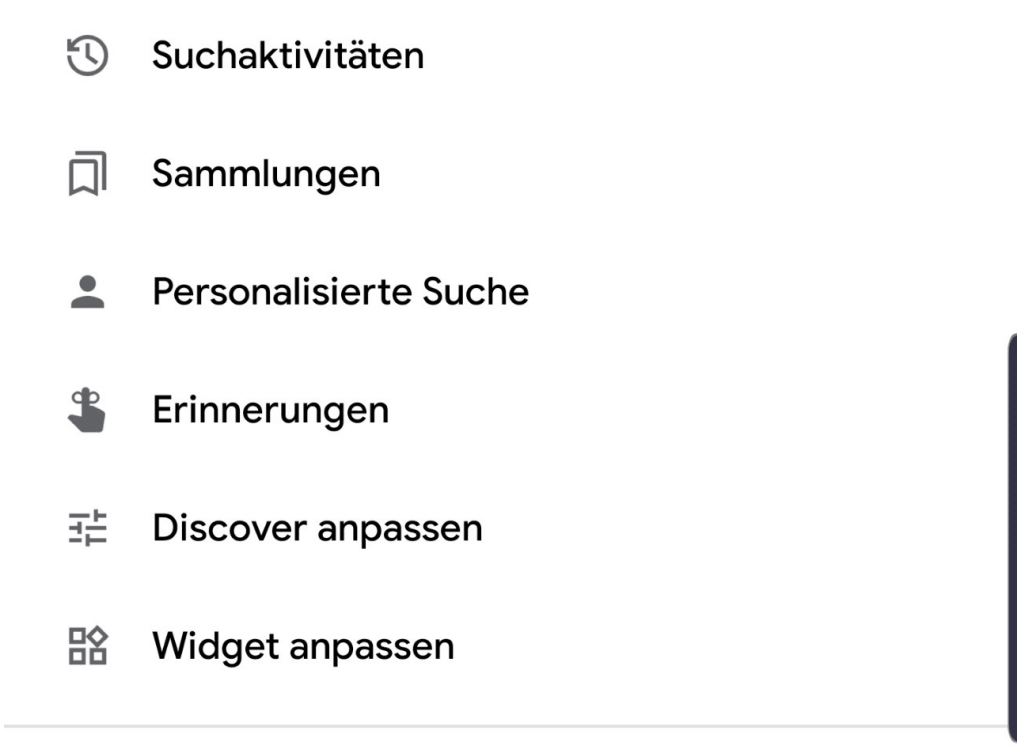
Ausgabe 2022.05

Konfiguration des Suchwidgets in Android

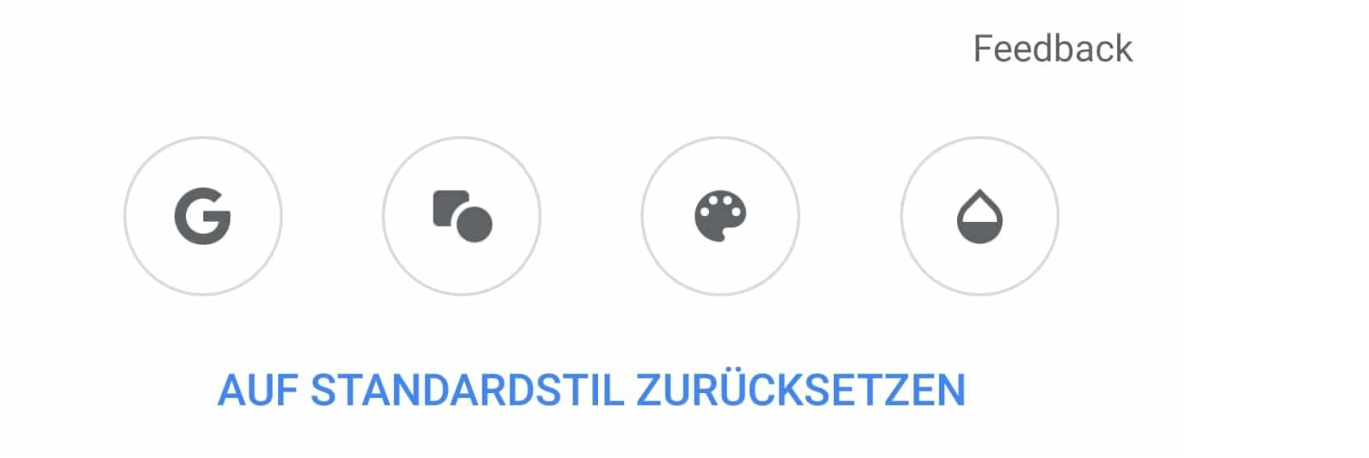
Bei so gut wie jedem Android-Telefon finden Sie im Standard auf der Startseite das Suchwidget von Google, das kleine Suchfeld. Dessen Aussehen müssen Sie aber so nicht hinnehmen. Verändern Sie es einfach nach Ihren Bedürfnissen!

Sollten Sie das Such-Widget nicht sehen, dann halten Sie den Finger einen Moment auf eine freie Stelle des Displays gedrückt. Tippen Sie dann auf **Widgets**, dann suchen Sie es hinaus und platzieren Sie es auf dem Startbildschirm.

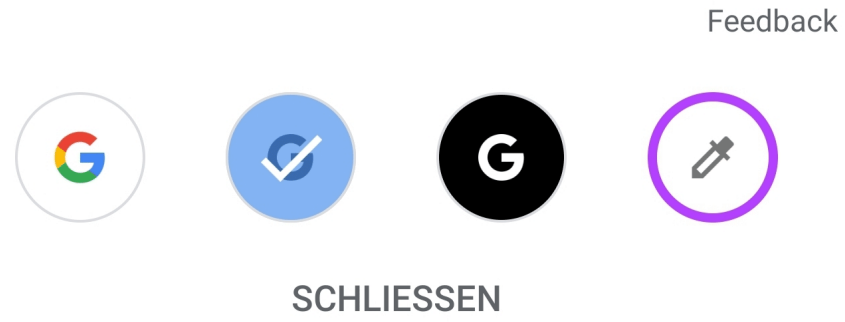
Um es nun vom Aussehen her zu verändern, tippen Sie es einmal an. Tippen Sie auf einen beliebigen Text in der Anzeige, um die Bildschirm-Tastatur zu schließen. Unten rechts am Bildschirm können Sie nun mit **Mehr** die Einstellungen öffnen und tippen darin auf **Widget anpassen**.

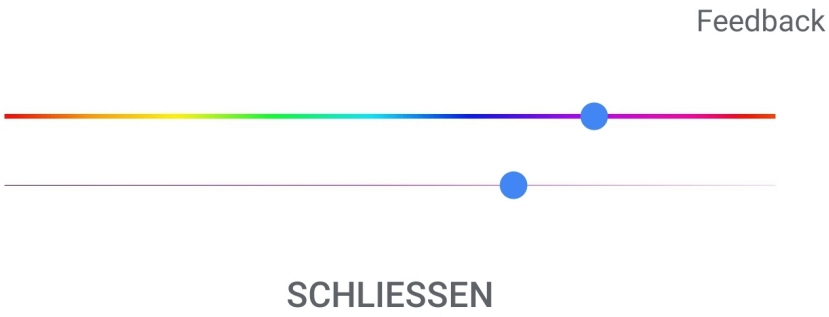


Am unteren Bildschirmrand finden Sie nun vier Symbole, die die einzelnen Anpassungsmöglichkeiten symbolisieren. Über das ganz linke Symbol können Sie festlegen, ob nur das G oder das Wort Google im Widget angezeigt werden soll.



Mit dem zweiten von links können Sie die Form des Suchfelds von eckig bis abgerundet verändern. Das Symbol mit der Farbpalette erlaubt Ihnen das Festlegen der Färbung des Widgets. Je nach Startseiten-Hintergrund können Sie es hell oder dunkel einfärben. Wenn Ihnen das nicht individuell genug ist, dann tippen Sie auf die Pipette und wählen Sie über den Farbregler eine beliebige Farbe aus.


Feedback
SCHLIESSEN

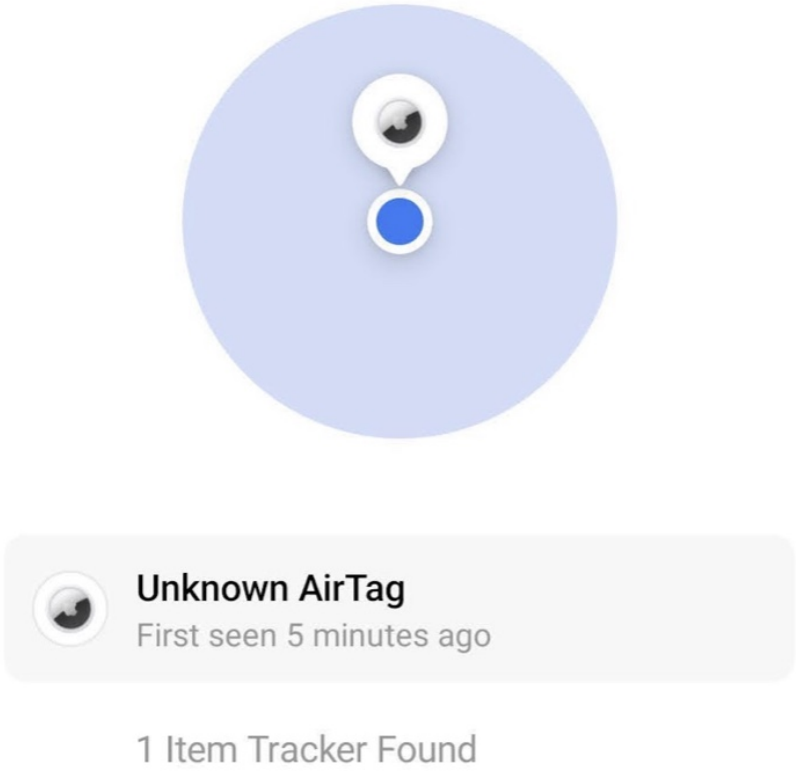

Feedback
SCHLIESSEN

Fremde Airtags mit Android-Geräten aufspüren

Die Apple AirTags sollen dem einfachen Auffinden von Gegenständen dienen. Das Risiko: Wer Ihnen ein AirTag unterschiebt, kann Sie damit auch tracken! Hier hilft die Tracker Detect App für Android.

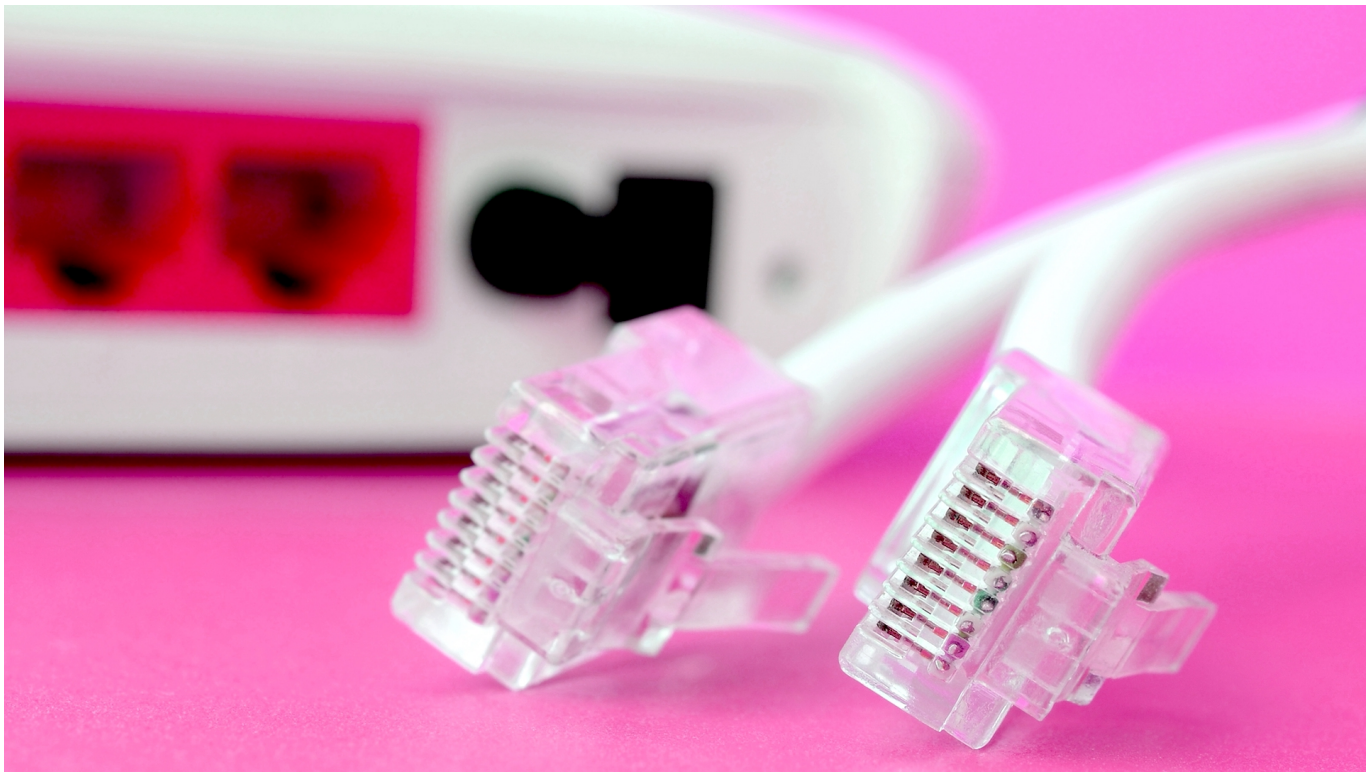
Sie suchen Ihren Schlüssel? Starten Sie die Wo ist-App auf Ihrem iPhone und lassen Sie sich die Position des AirTags anzeigen, das daran hängt. Wenn Sie selber ein iPhone verwenden, dann bemerken Sie schnell, dass ein fremdes AirTag sich mit Ihnen bewegt: Das AirTag wird von Ihrem Smartphone als nicht zu Ihnen gehörend identifiziert und gibt mehrfach einen Ton aus. Parallel dazu zeigt Ihr iPhone eine Meldung an, dass sich ein fremdes AirTag mit Ihnen bewegt.

Android unterstützt im Standard keine AirTags, damit existiert diese Funktion nicht. Apple hat nach langen Diskussionen eine kostenlose App herausgebracht, die zumindest die manuelle Suche nach fremden AirTags erlaubt.



Die Voraussetzung: Das AirTag muss sich 15 Minuten außerhalb der Reichweite des iPhones befinden, zu deren Apple ID es gehört. Klicken Sie in der App auf **Scan**, dann durchsucht sie die Umgebung nach AirTags, die zurückgelassen wurden. Hat Ihnen jemand heimlich untergeschoben, dann erscheint dieses in der Liste. Ist es länger als 10 Minuten in Reichweite Ihres Smartphones, dann können Sie durch ein Tippen auf **Play Sound** einen Ton wiedergeben lassen. Dieser erleichtert es, das AirTag dann auch physisch zu orten.

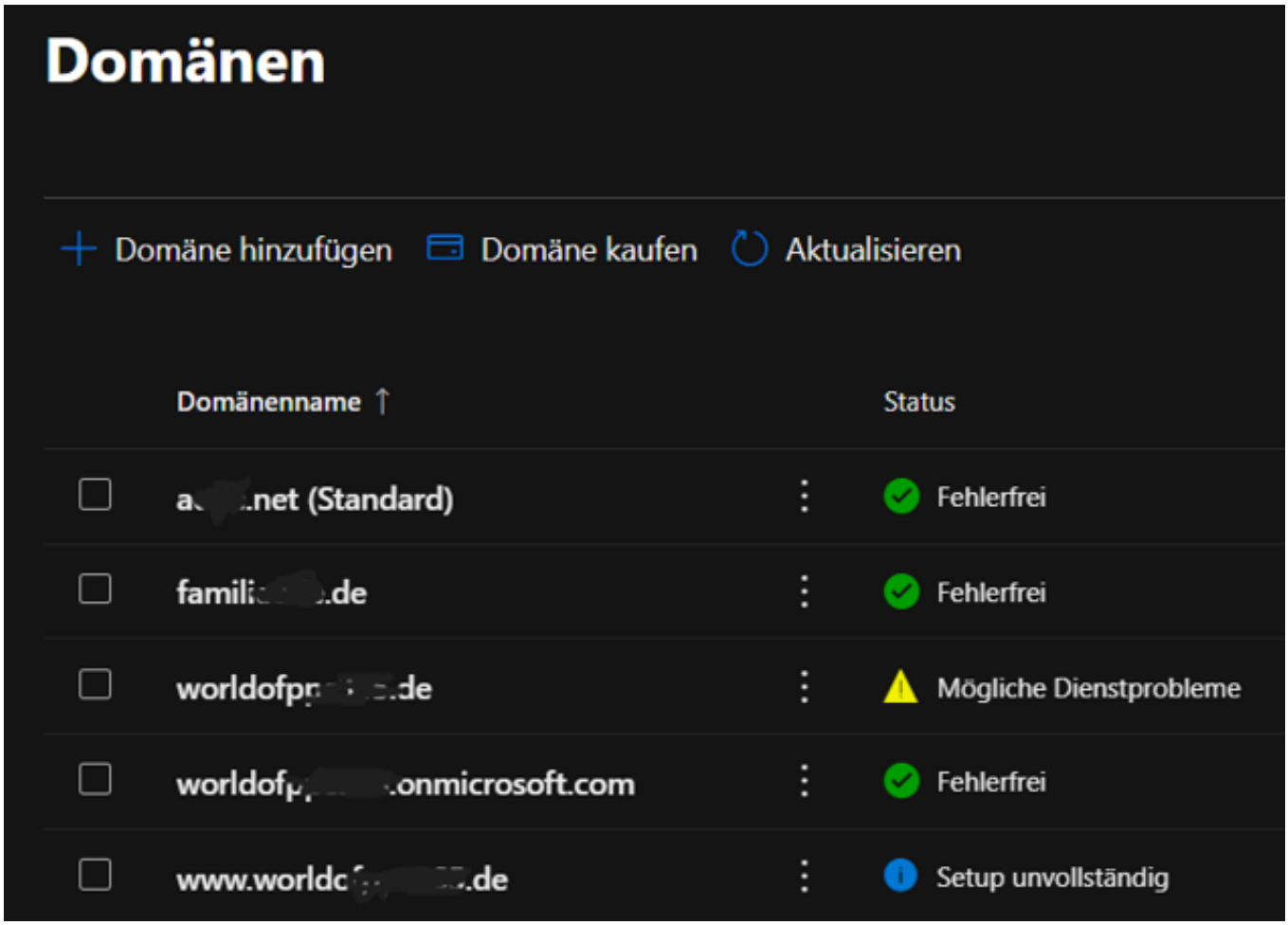
Hinzufügen einer eigenen Domäne bei Microsoft 365



Die Business-Pläne von Microsoft 365 erlauben es Ihnen, eine eigene Domain zu hinterlegen und sich auch mit Ihren E-Mail-Adresse komplett von den Namensvorgaben von Microsoft zu lösen. Wir zeigen Ihnen, wie das geht!

Im Standard geben Sie bei Anmeldung eines Microsoft 365-Business-Plans einen Namen für Ihre Organisation ein, beispielsweise **meineorganisation**. Da die einzelnen Benutzer Ihrer Organisation automatisch auch ein E-Mail-Postfach bekommen, bekommen Sie von Microsoft automatisch eine Domäne **meineorganisation.onmicrosoft.com**. Dieser Name ist natürlich meist nicht sonderlich schön. Abhilfe schaffen können Sie direkt in der Administrationskonsole von Microsoft 365 (die existiert nur in den Business-Plänen):

- Melden Sie sich unter http://admin.microsoft.com an der Admin-Konsole an.
- Klicken Sie auf **Alle anzeigen** > **Einstellungen** > **Domänen**.



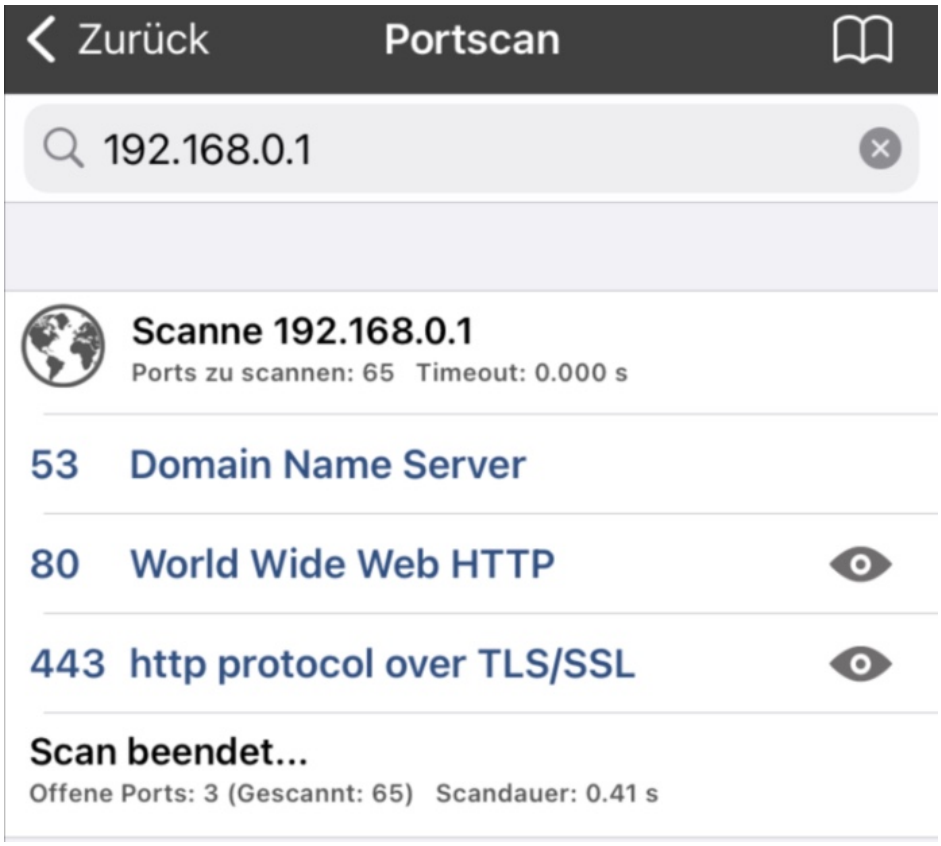
- Über **Domäne kaufen** können Sie direkt aus der Konsole nach freien Domains suchen lassen, diese registrieren und korrekt konfigurieren lassen. Das muss kein Firmenname sein, auch **meinefamilie.de** ist eine Option!
- Wenn Sie bereits eine Domäne besitzen und diese einbinden wollen, gehen Sie nach dieser Anleitung

Warum ist dieser Schritt so wichtig? Wenn Sie Benutzer anlegen wollen, dann müssen Sie diese einer Domäne zuordnen. Dafür muss diese Microsoft 365 bereits bekannt sein!

Informationen über Netzwerkgeräte am iPad bekommen

Smartphones, Tablets, Fernseher, Smarthomegeräte, alle verbinden sich in Ihrem Zuhause mit dem WLAN. Das führt dazu, dass Sie kaum Überblick über die Geräte und Dienste im WLAN bekommen. Abhilfe kann hier die App iNet Pro für iOS schaffen.

Die Herausforderung im Netzwerk sind meist die nicht sprechenden Namen der Netzwerkgeräte. Nur wenige Geräte identifizieren sich mit nachvollziehbaren Namen wie "Fritz!Box" im Netzwerk. Oft sehen Sie nur die Mac-Adresse (die weltweit einmalige Hardwareadresse des Geräts) oder die IP-Adresse im Netzwerk. Das macht das Identifizieren eines potentiellen Sicherheitslecks nicht einfacher.



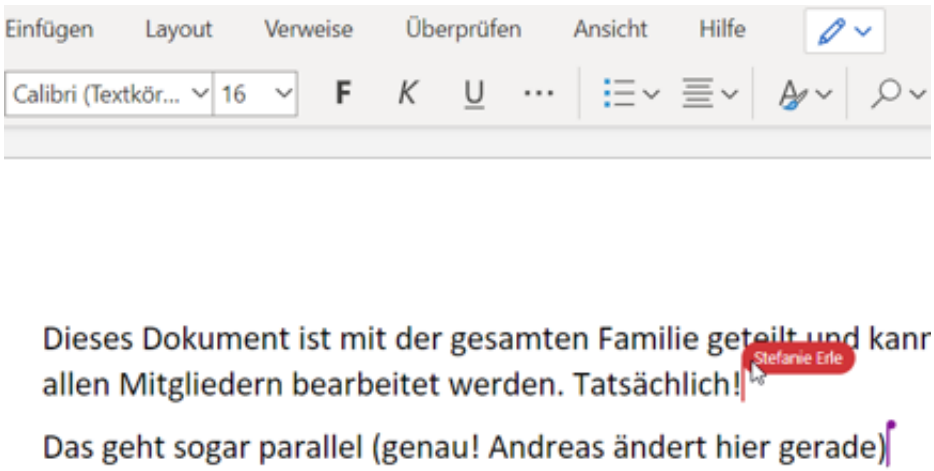
In der App klicken Sie im Übersichtsmenü auf **Netzwerkscanner**, um eine Analyse Ihres WLANs zu starten. Die App zeigt Ihnen nun alle gefundenen Geräte an, entweder mit deren Namen oder mit der IP-Adresse. Darunter finden Sie auch die Zahl der Dienste, die das jeweilige Gerät bereitstellt. Klicken Sie auf ein Gerät, beispielsweise auf eines, das Sie nicht kennen. Unter **Weitere Informationen** zeigt die App Ihnen weitere bekannt Infos zum Gerät an. Da wird dann schnell aus einer unleserlichen Zeichenkette ein Drucker mit Modellnamen oder eine Webcam!

Klicken Sie unten in der Übersicht auf **Scanne nach offenen Ports**, um eine Übersicht der Netzwerkports zu bekommen, über die das Gerät aus dem Netzwerk erreichbar sind. Diese können - und sollten - Sie abschalten, wenn sie nicht nötig sind. Dazu müssen Sie die jeweilige Konfigurationsoberfläche des Gerätes aufrufen.

Paralleles Bearbeiten von Dateien unter Microsoft 365

Im Gegensatz zur Bearbeitung von Dokumenten auf einem Datenträger erlaubt Microsoft 365 die gleichzeitige Bearbeitung durch mehrere Personen. Wir zeigen Ihnen, wie Sie das optimal nutzen können!

Sie sind mit mehreren Personen an der Erstellung einer Präsentation, eines Dokumentes oder einer Tabelle betraut. Wie immer stehen Sie unter Zeitdruck und müssen möglichst parallel arbeitet statt das Dokument immer wieder hin- und herzuschicken. Das funktioniert, wenn die Datei auf einem OneDrive oder SharePoint liegt.



- Öffnen Sie den Link in der E-Mail, die der Eigentümer Ihnen zum Dokument geschickt hat.
- Wenn bereits andere Anwender das Dokument bearbeiten, dann sehen Sie oben rechts in der Menüleiste kleine runde Symbole für jeden Benutzer.
- In der selben Farbe sehen Sie im Text farbige Markierungen, die die aktuelle Position des jeweiligen Bearbeiters im Text anzeigen. Damit können Sie sicherstellen, nicht parallel genau die selbe Stelle im Dokument anzugehen.
- Änderungen werden – abhängig von der Qualität der Internetverbindung - bei jedem Bearbeiter nahezu in Echtzeit angezeigt.

Die Datei wird bei der gleichzeitigen Bearbeitung automatisch gespeichert, sobald ein Bearbeiter eine Änderung vornimmt.

Hinzufügen eines freigegebenen Postfachs in Outlook

Wenn Sie mit anderen Anwendern zusammenarbeiten, dann müssen Sie oft schnell auf E-Mails reagieren. Auch, wenn ein Kollege abwesend ist. Dazu kann dieser Ihnen das Postfach freigeben. Wir zeigen Ihnen, wie Sie das freigegebene Postfach einbinden können.

Die Freigabe des Postfaches ist ein Teil der Merkmale des Postfachs. Sie als Benutzer sind dort hinterlegt, damit können Sie das Postfach über Ihr Outlook verbinden. Dazu klicken Sie in Outlook auf **Datei** > **Kontoeinstellungen** > **Kontoeinstellungen**.

Outlook zeigt Ihnen jetzt die aktuell geöffneten Postfächer an. Das sind keine Stellvertretungen, sondern ihre eigenen Postfächer. Klicken Sie jetzt auf das Postfach, zu dem Sie das freigegebene Postfach zuordnen wollen. Klicken Sie dann auf die Registerkarte **Ändern**.

Im sich öffnenden Fenster klicken Sie auf **Weitere Einstellungen** und auf die Registerkarte **Erweitert**.

Unter **Zusätzlich diese Postfächer öffnen** klicken Sie auf **Hinzufügen**. Outlook öffnet jetzt eine Eingabemaske, in der Sie die E-Mail-Adresse des freigegebenen Postfachs eingeben können. Diese muss zwingend auf dem selben Server liegen (Exchange Server oder Microsoft 365-Organisation).

Drücken Sie die Eingabetaste. Kommt keine Fehlermeldung, dann ist das freigegebene Postfach erfolgreich eingebunden. Sie können den Dialog jetzt durch Klicken auf die Kreuze verlassen.

Das eingebundene Postfach finden Sie links im Verzeichnisbaum in Outlook ganz unten.

Fall Künast und NetzDG: Wer im Netz beleidigt oder bedroht, muss vermehrt mit Strafen rechnen

Renate Künast hat vor dem Bundesverfassungsgericht einen Sieg eingefahren: Facebook muss der Politikerin mitteilen, wer sie da auf Facebook aufs Übelste beleidigt hat. Eine Trendumkehr, da Opfer nun mehr Möglichkeiten haben, sich zu wehren. Gleichzeitig wurde das NetzDG verschärft.

Die Grünen-Politikerin Renate Künast wurde und wird auf Facebook und anderen Plattformen immer wieder beleidigt und sogar bedroht.

Anders als andere Politiker geht Renate Künast aber damit sehr offensiv um und auch immer wieder juristisch dagegen vor. Sie wehrt sich. Sogar bis zum Bundesverfassungsgericht. Diese Woche ist dort ein Urteil ergangen, das man eindeutig als Sieg für Renate Künast bezeichnen kann. Demnach muss Facebook der Politikerin mitteilen, wer sie da eigentlich aufs Übelste beleidigt hat. Denn diese Auskunft hat das Netzwerk bislang verweigert. In der Branche wird das

Urteil als wegweisend betrachtet.

Übelste Beleidigungen - Meinungsfreiheit?

Renate Künast hat in der Vergangenheit immer wieder gegen Beleidigungen im Netz geklagt – und keineswegs immer Recht bekommen.

Der Politikerin wurden schon viele Beleidigungen auf Facebook und anderswo zugemutet: „Drecksau“, „Schlampe“, „Sondermüll“ – oder einfach „ein Stück Scheiße“. Und das sind noch die harmloseren Varianten. Die Politikerin hat oft geklagt. Das Zivilgericht in Berlin hatte vor einigen Jahren geurteilt, als Politikerin müsse sie sich die meisten der Beleidigungen gefallen lassen, etwa „ein Stück Scheiße“.

Oder auch diverse sexististische Posts. Ehrlich gesagt muss man sich dann nicht wundern, wenn Menschen in den Netzwerken immer noch eins drauf legen und immer aggressiver werden, wenn deutsche Gerichte solche Urteile fällen.

Renate Künast hat sich aber nicht unterkriegen lassen, sogar ein Buch geschrieben („Hass ist keine Meinung“) und immer wieder geklagt. Sogar bis zum Bundesverfassungsgericht. Das hat anders als einige Gerichte davor die Ansicht vertreten, auch Politiker hätten Persönlichkeitsrechte – und müssten sich derartige ausfällige Beleidigungen nicht gefallen lassen. Renate Künasts Anwälte hätten Anspruch darauf, von Facebook zu erfahren, wer die Beleidigungen geschrieben hat. Diese Auskunft hatte Facebook bislang nämlich stets verweigern.

Facebook muss Urheber von Hass-Posts verraten

Ein Urteil, an dem sich andere Gerichte nun werden orientieren müssen, da das Bundesverfassungsgericht den Rahmen zurechtgerückt hat.

Obwohl die Beleidigungen bereits Jahre zurückliegen, weiß die Politikerin nicht, wer sie geschrieben hat. Das wäre aber für ein Strafverfahren oder auch eine Zivilklage wichtig. Sie kennt also gar nicht die Täterinnen oder Täter. Das wird sich jetzt ändern, denn die Gerichte sind angewiesen, anders zu entscheiden – und könnten und werden vermutlich auch Facebook vorschreiben, Daten herauszugeben.

Erst dann könnte Renate Künast gegen diese Personen vorgehen. Ein Problem, das ja alle Menschen haben, die auf Plattformen wie Facebook oder Instagram beleidigt oder bedroht werden. Sie müssen sich immer erst mit den Plattformen auseinandersetzen, die praktisch nie konkrete Daten rausrücken. Wenn sich das jetzt ändert, könnten Opfer in Zukunft gezielt Strafanzeige stellen und auch Schmerzensgeld oder Schadenersatz fordern. Das hebt die Anonymität ein wenig auf.

Auch das NetzDG ist seit 1. Februar verschärft

Apropos Strafverfahren: Wir haben ja ein Netzwerkdurchsetzungsgesetz (NetzDG) - und das ist seit dieser Woche verschärft.

Bislang hat das NetzDG Anbieter großer Plattformen – also insbesondere Google, Facebook, Instagram, TikTok, Twitter etc. – verpflichtet, Postings mit Hass, Hetze und offensichtlich strafbaren Inhalten zu löschen. Aber nicht pro-aktiv, sondern immer erst, wenn den Netzwerken eine Meldung gemacht wird. Das hat auch einiges gebracht. Eine aktuelle Studie stellt fest, dass es auf Twitter rund 10% weniger Hass und Hetze gibt, seitdem das NetzDG in Deutschland in Kraft ist.

Aber Beleidigungen wie die gegen Renate Künast deckt das Gesetz nicht ab. Jetzt ist das Gesetz verschärft worden. Die Netzwerke müssen offenkundig strafbare Inhalte auch aktiv an eine „Zentrale Meldestelle für strafbare Inhalte“ (ZMI) melden, die extra beim Bundeskriminalamt (BKA) eingerichtet wurde.

Rund 200 Beamte arbeiten dort und sollen künftig Meldungen entgegennehmen. Die Netzwerke sollen die Postings melden, aber auch gleich einige Daten, etwa wer das gepostet hat, IP-Adresse etc. Die Beamten entscheiden dann, ob Strafverfahren eröffnet werden.

Was bringt das neue NetzDG?

Stellt sich die Frage: Wird das denn etwas bringen, würde da in Fällen wie Renate Künast helfen?

Persönliche Beleidigungen sind durch das NetzDG eher nicht abgedeckt. In Fällen wie bei Renate Künast bringt das NetzDG keinen Fortschritt. Experten rechnen

aber damit, das rund 250.000 Fälle aktiv von den Netzwerken an das BKA gemeldet werden könnten. Bei der Zentralen Meldestelle arbeiten 200 Beamte. Rund 150.000 Strafverfahren könnten dadurch entstehen – wenn die Justiz überhaupt in der Lage ist, so viele Fälle zu bearbeiten.

Aber das würde eindeutig den Druck erhöhen, da es gefährlicher wird, öffentlich in den Netzwerken Hass und Hetze zu verbreiten. Allerdings haben Google, Facebook, Twitter und TikTok gegen das Gesetz geklagt. Sie wollen sich nicht zum Erfüllungsgehilfen der Justiz machen und haben auch Datenschutzbedenken.

Das muss erst geklärt werden, denn in der Tat haben selbst Institutionen wie HateAid, die gegen Hass und Hetze im Netz vorgehen wollen, Bedenken, dass so viele Daten aus den Netzwerken an das BKA gehen sollen. Das bedeutet: So lange die Klagen laufen, fließen auch keine Daten an das BKA. Wir werden abwarten müssen, wie Gerichte entscheiden.

Ändere-dein-Passwort-Tag: HPI-Sicherheitsforscher klären auf über Cyberangriffe und Passwortsicherheit

Am Ändere-Dein-Passwort-Tag werden wir daran erinnert, sorgsamer mit unseren Passwörtern umzugehen. Das Hasso Plattner Institut (HPI) bietet interessante Hilfen dazu an.

Der "Ändere-dein-Passwort-Tag" am 1. Februar ist der jährliche Aufruf, die eigenen Passwörter zu aktualisieren.

Denn das Risiko, als Unternehmen oder Privatperson gehackt und Opfer eines Cyberangriffs zu werden, ist groß. "Die Frage ist nicht, ob es passiert, sondern wann", betonen die Sicherheitsexperten des Hasso-Plattner-Instituts (HPI).

Auch im vergangenen Jahr hat der Diebstahl digitaler Identitäten weiter zugenommen. Der HPI Identity Leak Checker ermöglicht mittlerweile den Abgleich mit rund 13 Milliarden gestohlener und im Internet frei verfügbarer Identitätsdaten.

Die Überprüfung, ob man selbst Opfer eines Datendiebstahls geworden ist, ist mit dem kostenlosen Service, den das HPI seit 2014 betreibt, denkbar einfach. Mehr als 8 Millionen geleakte Details zu Bankverbindungen seien beispielsweise in Verbindung mit der E-Mail bereits gefunden worden. Über diese Risiken, die schwache und damit unsichere Passwörter verursachen können, klärt das HPI auf und veröffentlicht jedes Jahr die "Top 10"-Passwörter der Deutschen.

Rechner können Passwörter immer schneller knacken

Den meisten ist gar nicht bewusst, wie schnell die Rechenleistung der Server und Computer geworden ist. Bei den sogenannten Brute-Force-Angriffen können Milliarden von Kombinationen innerhalb einer einzigen Sekunde ausgespielt werden. Da ist die Trefferquote groß.

Neben den bereits bestehenden Tipps für sichere Passwörter, empfiehlt es sich, möglich lange Passwörter zu erstellen. Dahinter steckt einfache Mathematik. Wenn man sich die Kombinationsmöglichkeiten anschaut, vervielfacht jedes weitere Zeichen die Zeit, die es braucht, um das Passwort knacken zu können. Für die Passwortsicherheit besteht somit ein enormer Unterschied, ob ein Passwort zwölf, vierzehn oder sechzehn Zeichen umfasse.

Tipps zur Passwortwahl

Bei der Passwortwahl empfiehlt das Hasso-Plattner-Institut daher:

- Lange Passwörter (> 15 Zeichen)
- Verschiedene Zeichenklassen verwenden (Groß-, Kleinbuchstaben, Zahlen, Sonderzeichen)
- Keine Wiederverwendung von gleichen oder ähnlichen Passwörtern bei unterschiedlichen Diensten
- Verwendung von Passwortmanagern
- Passwortwechsel bei Sicherheitsvorfällen und bei Passwörtern, die die obigen Regeln nicht erfüllen
- Zwei-Faktor-Authentifizierung aktivieren, wenn möglich

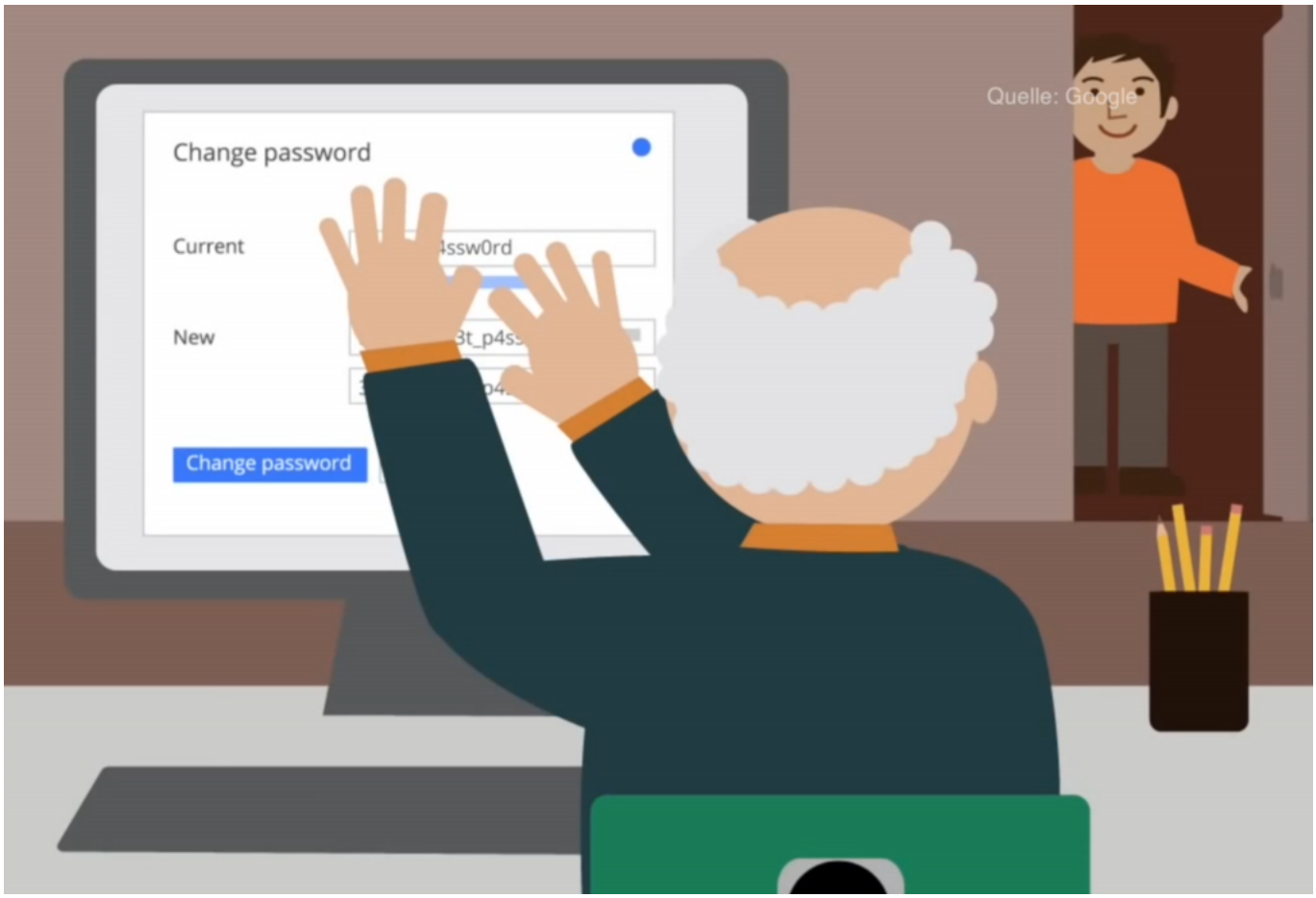
Der Identity Leak Checker

Ob man Opfer eines Datendiebstahls geworden ist, lässt sich mit dem Identity Leak Checker, einem Online-Sicherheitscheck des Hasso-Plattner-Instituts (HPI), sehr leicht überprüfen. Seit 2014 kann dort jeder Internetnutzer unter https://sec.hpi.de/ilc kostenlos durch Eingabe seiner E-Mail-Adresse prüfen lassen, ob Identitätsdaten von ihm frei im Internet kursieren und missbraucht werden könnten.

Die Sicherheitsforscher ermöglichen den Abgleich mit mittlerweile mehr als 12,8 Milliarden gestohlener und im Internet verfügbarer Identitätsdaten. Dabei liegt der Fokus auf Leaks bei denen deutsche Nutzer betroffen sind. Das Angebot ist in Deutschland einzigartig.

Insgesamt haben mehr als 16,5 Millionen Nutzer mithilfe des Identity Leak Checkers die Sicherheit ihrer Daten in den letzten fünf Jahren überprüfen lassen. In mehr als 4,2 Millionen Fällen mussten Nutzer darüber informiert werden, dass ihre E-Mail-Adresse in Verbindung mit anderen persönlichen Daten im Internet offen zugänglich war.

Ändere Dein Passwort Tag: Bitte nicht wörtlich nehmen



Am 01. Februar ist nationaler "ÄndereDein-Passwort-Tag". Das solltet Ihr aber nicht zu wörtlich nehmen. Denn regelmäßiges Ändern des Passworts ohne Anlass wird gar nicht mehr offiziell empfohlen.

Ändere Dein Passwort Tag: Früher galt unter Experten die unbedingte Empfehlung, sein Passwort alle paar Wochen zu ändern. Dazu rät das Bundesamt für Sicherheit in der Informationstechnik (BSI) schon länger nicht mehr.

Experten des BSI sind davon längst abgerückt. Demnach könnte ein Passwort auch jahrelang genutzt werden, wenn es die richtigen Kriterien erfüllt. Das Passwort ändern sollen Menschen aber natürlich nach wie vor dann, wenn das eigene Passwort geknackt oder in fremde Hände geraten ist.

Ein gutes und solides Passwort wählen

Viel wichtiger ist es, ein gutes, solides Passwort zu verwenden. Das ist mindestens acht Zeichen lang, besser deutlich länger, es enthält Groß- und Kleinbuchstaben, Ziffern **und** Sonderzeichen.

Es enthält keine Namen, keine Zeichenfolgen wie **abcd** oder **1234** und vor allem - und das ist wichtig! - auch keine Wörter, die im Wörterbuch stehen. Denn Hacker machen es sich einfach: Sie probieren alles aus, was in einem Wörterbuch steht – auch Kombinationen daraus.

Wie gut das eigene Passwort ist und wie schnell ein Hacker mit einem normalen PC ein Passwort knacken könnte, kann jeder unter checkdeinpasswort.de ausprobieren. Einfach mal machen.

Und noch besonders wichtig – wenn auch unbequem: In jedem Onlinekonto ein anderes Passwort verwenden. Damit ein Hacker, der mal ein Passwort geklaut oder gehackt hat, damit nicht überall reinkommt.

Passwort-Manager helfen!

Aber überall ein anderes Passwort zu benutzen: Das ist schwierig bis unmöglich. Wie sinnvoll und sicher sind denn Passwort-Manager?

Passwort-Manager – ob im Browser eingebaut oder zusätzlich installiert – sind sehr sinnvoll. Denn sie ermöglichen es, in jedem Onlinekonto ein anderes sicheres Passwort zu verwenden. Der Benutzer muss die Passwörter beim Login dann ja nicht mehr eingeben.

Die guten Passwort-Manager machen die eigenen Passwörter bequem überall verfügbar, auf PCs, Tablets und Smartphones. Sie warnen auch, wenn Sicherheitslücken oder kompromittierte Onlinekonten entdeckt wurden. In solchen Fällen unbedingt sofort handeln.

Wer auf Nummer Sicher gehen will, geht noch einen Schritt weiter – und setzt auf die sogenannte Zwei-Faktor-Authentifizierung. Eine zusätzliche Sicherheitsstufe, die sich fast überall aktivieren lässt, ob bei Microsoft, Google, Apple, Facebook, Twitter oder Amazon.

Zusätzlich zum Passwort muss dann noch ein individueller Code eingegeben werden, der in der Regel im eigenen Smartphone erzeugt wird. Die Folge: Bekommt ein Hacker mein Passwort in die Hände, kann er sich trotzdem nicht einloggen.

Deutsche nutzen stoisch simple Passwörter

Die Top 10 der deutschen Passwörter, die das Hasso-Plattner-Institut jüngst gemeldet hat: “123456”,, “123456789”, “1234”, “12345678”, “hallo”, “passwort”, “1234567”, “11111” und “hallo123”. Ernsthaft? Damit loggen sich die Deutschen also am liebsten ein? Eigentlich kaum zu glauben, denn mittlerweile müsste sich doch wirklich auch bis zum ignorantesten User rumgesprochen haben, dass solche Passwörter gar nicht gehen.

Trotzdem sind sie nicht nur beliebt, sondern sogar im großen Stil im Einsatz. Da muss man sich nicht wundern, wenn immer wieder Systeme geknackt und Daten geklaut werden.

Allerdings kann ich uns User auch verstehen. Es werden doch unmenschliche Dinge erwartet: Wir sollen Passwörter benutzen, die nicht im Wörterbuch stehen, die nicht zu kurz sind, die Groß- und Kleinschreibung enthalten und natürlich Sonderzeichen.

BGH-Urteil zu Facebook und Pseudonymen

Laut BGH dürfen Menschen, die vor Mai 2018 ein Konto eröffnet haben, ein Pseudonym verwenden - alle anderen müssen Klarnamen verwenden. Wieso ist das so?

Der Bundesgerichtshof (BGH) hat sich vor einigen Tagen mit Facebook beschäftigt. Und zwar ganz konkret mit einem Aspekt hier im Netzwerk: Nutzer müssen bei Facebook einen Klarnamen verwenden, sie dürfen kein Pseudonym benutzen. Also nicht **RevengerHolger**, sondern bitte mit echtem Namen unterwegs sein.

Ein Name, der mit dem echten Namen weitgehend übereinstimmt. Doch dagegen hatten zwei User geklagt, die nicht mit ihrem echten Namen im Netzwerk präsent sein wollten. Sie wollten Pseudonyme verwenden. Dürfen sie, sagt der BGH – unter bestimmten Umständen.

Warum ist Klarname bei Facebook Pflicht?

Facebook argumentiert, das Netzwerk sei vor allem dazu da, dass sich Menschen

finden und verbinden. Da wäre es kontraproduktiv, nicht den eigenen Namen zu benutzen. Klar: Wenn ich mich Snoopy123 nenne, finden mich meine Klassenkameraden aus der Grundschule natürlich nicht. Das Argument ist schlüssig. Außerdem seien Menschen, die ihren Klarnamen verwenden, achtsamer, wenn sie mit anderen Menschen umgehen. Das allerdings ist eine umstrittene Position. Es gibt Studien, die das Gegenteil belegen.

Auf jeden Fall hat Facebook in seinen Nutzungsbedingungen die Vorschrift, Klarnamen zu benutzen. Wenn jemand dagegen verstößt und ein Pseudonym verwendet, fordert Facebook ihn früher oder später auf, das zu ändern. Weigert sich jemand konsequent, wird auch schon mal das Konto gesperrt. Genau das ist zwei Personen passiert: Ein Mann und eine Frau haben dagegen geklagt. In den ersten Instanzen hat Facebook auch Recht bekommen. Jetzt beim BGH aber nicht mehr. Die beiden dürfen ihr Pseudonym verwenden. Eine Regelung, die für sie gilt – aber längst nicht für alle.

Warum das nicht für alle gilt

Jetzt können keineswegs alle Facebook-Nutzer ein Pseudonym verwenden. Die Entscheidung des BGH gilt nicht für alle. Für wen gilt die Entscheidung?

Der BGH hat einen Fall entschieden, der schon einige Jahre zurückliegt. Und da sah die Welt noch anders aus als heute. Vor Mai 2018 gab es die Datenschutzgrundverordnung noch nicht, dafür aber ein Telemediengesetz, das ausdrücklich das Recht vorsieht, dass Menschen sich auch pseudonym oder anonym in einer Plattform müssen anmelden können.

Ein verbrieftes Recht, nicht zum Klarnamen gezwungen sein zu müssen, könnte man sagen. Seit die DSGVO in Kraft ist, das ist seit Mai 2018, sieht die Sache anders aus: Die DSGVO sieht kein solches Privileg auf ein Pseudonym vor. Deshalb kann Facebook seitdem tatsächlich die Verwendung eines Klarnamens verlangen. Das bedeutet in der Praxis: User, die ihr Konto schon vor Mai 2018 bei Facebook eröffnet haben, können nun auf ein Pseudonym bestehen. Alle anderen, die ihr Konto nach Mai 2018 eröffnet haben, sind gezwungen, einen Klarnamen zu benutzen, da Facebook das in seinen Nutzungsbedingungen von den Nutzern erwartet.

Gilt das auch für andere Netzwerke?

Nicht explizit. Jedes Netzwerk hat seine eigenen Regeln. Unter ähnlichen Bedingungen würde vermutlich aber genauso entschieden: Vor Mai 2018 hatten wir alle ein Recht auf die Verwendung eines Pseudonyms, seit Mai 2018 aber nicht mehr. Die meisten anderen Netzwerke wie Instagram, Twitter oder TikTok bestehen aber sowieso nicht auf einen Klarnamen, sondern akzeptieren auch Fantasienamen und Pseudonyme. Dort gibt es das Problem also gar nicht. Es wäre im übrigen durchaus möglich, dass ein Netzwerk bei der Registrierung auf die Angabe der echten Daten besteht, muss diese aber ja nicht im Netzwerk anzeigen.

Ungeklärt: Klarname oder Pseudonym besser?

Wieso gibt es überhaupt immer wieder Streit darüber, ob Klarnamen Pflicht sein sollten?

Das liegt daran, dass man davon ausgeht, dass Menschen sich achtsamer ihren Mitmenschen gegenüber verhalten, wenn sie mit echtem Namen auftreten und einfacher zu identifizieren sind. Also die Annahme, dass ich eher lautstark polemisiere, beleidige oder auch Hass und Hetze verbreitet, wenn ich anonym in einem Netzwerk unterwegs bin. Allerdings ist das eine anfechtbare These.

An der ETH Zürich wurde dazu geforscht. Mit dem Ergebnis: Es wird immer häufiger unter Realnamen Hass und Hetze verbreitet. Das alleine scheint also keine Lösung zu sein. Außerdem versprechen sich viele Politiker auch eine einfachere Strafverfolgung, wenn Klarnamen vorgeschrieben sind. Allerdings ist das auch nicht richtig. Viel wichtiger wäre dann, dass sich Menschen mit ihrer Handynummer oder echten Adresse registrieren; es ist nicht entscheidend, dass dafür auch der Klarname angezeigt wird.

Cyberkriminologe empfiehlt "Polizeiwachen im Netz"

Hass, Hetze und Morddrohungen im Netz gehören längst zum Alltag. Die Politik reagiert mit Druck und Verboten. Bundesinnenministerin Faeser will Telegram aus dem App Store verbannen. Das NetzDG wird Anfang Februar verschärft: Facebook und Co. müssen Straftaten dann direkt melden. Aber gibt es denn wirklich keine andere Ideen und Konzepte, um der Lage Herr zu werden? Doch, die gibt es: Die Polizei müsse umstrukturieren - und Wachen im Netz aufmachen, erklärt mit ein Cyberkriminologe im Gespräch.

Wenn ich bei Rot über die Ampel gehe, verstoße ich gegen die Straßenverkehrsordnung. In der Regel passiert nichts. Aber: Das Risiko besteht. Könnte ja die Polizei sehen. Also bin ich vorsichtig.

Doch Regelverstöße im Netz bleiben meist folgenlos. Keiner, der aufpasst. Kein Kläger. Kein Richter. Keine Strafen. Und deswegen leider auch – eine weitgehend völlige Enthemmung.

Ruth Moschner frustriert mangelnde Strafverfolgung

TV-Moderatorin Ruth Moschner hat sich dieser Tage in einem offenen Brief und

Video an die Öffentlichkeit gewandt: Sie wurde mehrfach auf Instagram belästigt, hat das zur Anzeige gebracht. Aber ein Täter wurde nicht ermittelt.

Ruth Moschner hat völlig Recht, wenn sie das öffentlich anprangert. Es ist tatsächlich ein Armutszeugnis, wenn Straftaten im Netz nicht geahndet und Straftäter bestraft werden. Wir beschäftigen uns ja schon sehr lange mit Hass, Hetze, Beleidigungen, sogar Morddrohungen im Netz, die zu einem immer größeren Problem werden.

Da muss man sich schon fragen, wieso das so ist. Und vor allem, was geeignete Gegenmittel sein könnten.

Bundesinnenministerin Faeser droht damit, Telegram aus den Stores verbannen zu lassen.

Als ob das eine Lösung wäre. Alle, die mit Hass und Hetze auf Telegram nichts zu tun haben, würden mitbest

Polizeiarbeit anders denken

Es gibt aber Ansätze, die ich interessant und vielversprechend finde. Und einer lautet: Polizeiarbeit ganz anders zu denken.“

Wie wäre es, wenn die Polizei im Netz Streife fahren würde. So wie im richtigen Leben auch. Denn wer Polizei sieht, fühlt sich als Bürger in der Regel sicherer – und die Abschreckungswirkung ist nicht zu unterschätzen. Das zumindest ist die zentrale Forderung von Thomas Rüdiger, Cyberkriminologe aus Brandenburg, der auch Polizisten schult.

Cyberkriminologe Thomas Gabriel Rüdiger sagt mir dazu im Gespräch; „Man muss zunächst sagen: Eigentlich ist es für uns so, dass die Sichtbarkeit der Polizei ein essenzieller zB auch im Straßenverkehr. Und ich glaube, dass die Polizeit genauso Bestandteil sein muss dieses öffentlichen digitalen Raums wie im Straßenverkehr.“

Da kommen natürlich auch merkwürdige Gefühle auf, denn da gibt es bislang ja nicht. Wirkt das nicht wie ein Polizeistaat und führt zu Widerstand?

Dazu sagt Thomas Rüdiger „Ich glaube das Grundproblem im Netz ist in dieser

Situation eher, dass wir bislang gar keine Überwachung durch die Polizei hatten, sondern wir hatten eher eine Unterwachung.“

"Bislang haben wir keiner Überwachung im Netz, sondern eine Unterwachung."
Thomas Gabriel Rüdiger, Cyberkriminologe

Unterwachung statt Überwachung

"Unterwachung statt Überwachung": So kann man es auch formulieren. Polizei, die im Netz patrouilliert: Das erfordert allerdings ein völliges Umdenken, auch bei den Innenministern, sagt Rüdiger. Alle bei der Polizei müssten Medienkompetenz entwickeln – und Tausende von Beamten sich schwerpunktmäßig mit Kriminalität im Netz beschäftigen. Denn da findet Kriminalität heute vor allem statt.

Das erscheint mir ein folgerichtiger Ansatz zu sein. Denn Werkzeuge wie Telegram verbieten zu wollen, das ändert überhaupt nichts an der Situation. Dann wird irgend eine andere offene App zum neuen Tummelplatz.

Wie so eine Ausgestaltung genau aussehen könnte, das müsste natürlich erst mal besonnen diskutiert werden. Auch, was als öffentlicher Raum im Netz gilt und was strikt privat ist, natürlich.

Wir sollten jedoch unbedingt auch an die schwächsten in der Gesellschaft denken: unsere Kinder. Die sind allzu oft völlig wehrlos im Netz unterwegs – und brauchen dringend mehr Hilfe.“

Vorschlag: Kinderwachen im Netz

Stichwort: **Cybergrooming**. Erwachsene locken Kinder und Jugendliche online in Fallen. Oft mit dem Ziel, sexualisierter Gewalt an Kindern. Ein riesiges und leider wachsendes Problem.

Häufiger Tatort: Online-Games. Junge Menschen verbringen hier sehr viel Zeit. Aber hier passt niemand auf. Nicht nur deswegen schlägt Thomas Rüdiger spezielle Kinderwachen im Netz vor, an die sich junge Menschen und Opfer wenden können.

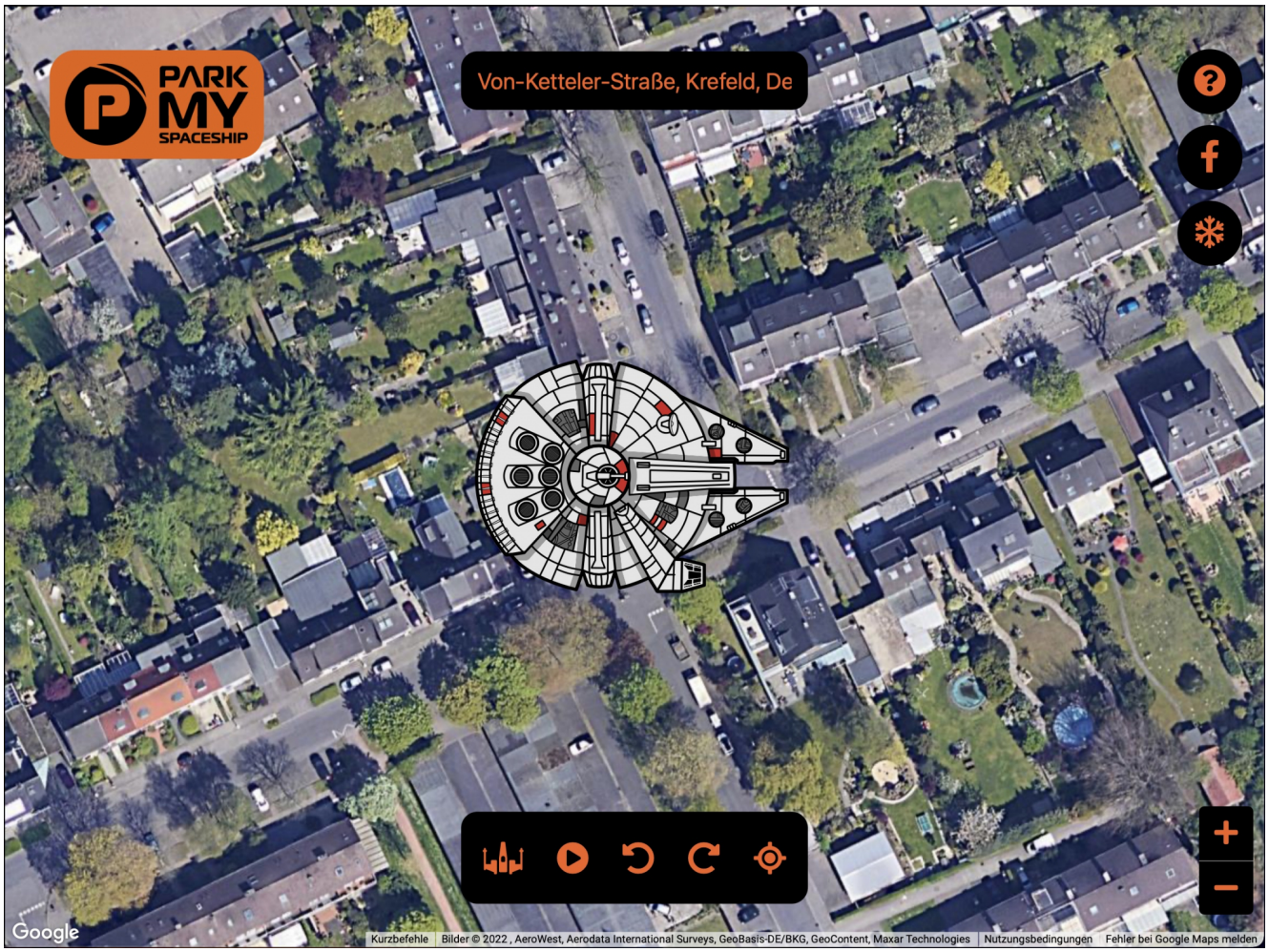
Der Wunsch des erfahrenen Cyberkriminologen wäre, dass wir eine Art Kinder-Online-Wache kreieren, wo Polizisten mit Pädagogen, Lehrern, Ärzte rund um die Uhr für Kinder in einer virtuellen, spielerischen Umgebung zur Verfügung stehen und Chat-Möglichkeiten anbiete. Damit sie die Kinder in der Welt, in der sie unterwegs sind, im digitalen Raum, Möglichkeiten hätten, sich an die Polizei zu wenden.

Lösungsansätze, mal völlig anders gedacht – und das gefällt mir daran. Wir müssen Kinder und Jugendliche schützen. Und am Ende auch uns alle. Der Auftrag an die Politik ist klar: Kriminalität verlagert sich von der physischen in die Onlinewelt. Also muss auch die Polizei Personal umschichten.

Park my Spaceship: Der Todesstern im Vorgarten

Wollten Sie immer schon mal wissen, wie groß die bekannten Raumschiffe Ihrer Lieblings-Science-Fiction-Serie sind? Dann können wir Ihnen helfen: Ob Enterprise, Todesstern oder das Mutterschiff aus "Independence Day", stellen Sie sie mit Park my Spaceship einfach in Ihren Vorgarten!

Die Webseite Park my Spaceship können Sie von jedem Gerät mit einem halbwegs aktuellen Webbrowser aufrufen. Beim ersten Aufruf fragt Sie sie nach der Berechtigung für das Auslesen der Position. Wenn Sie die nicht erteilen wollen, dann ist das kein Problem: Geben Sie die Adresse einfach im Suchfeld am oberen Bildschirmrand ein. Die Seite nutzt die Google Maps als KArtenb asis und legt eine eine Oberfläche darüber.



Klicken Sie in der Symbolleiste am unteren Bildschirmrand auf das linke Symbol mit dem Raumschiff, dann können Sie nach Kategorien (wie Star Wars, Star Trek, Battle Star Galactica etc.) das gewünschte Raumschiff auswählen. Dieses stellt die Seite entsprechend des Zoomfaktors der Kartenansicht in der "Originalgröße" dar. Klicken Sie auf den Wiedergabe-Button in der Symbolleiste, um es über die Karte fliegen zu lassen.

Wenn das Macbook sich im Standby entlädt

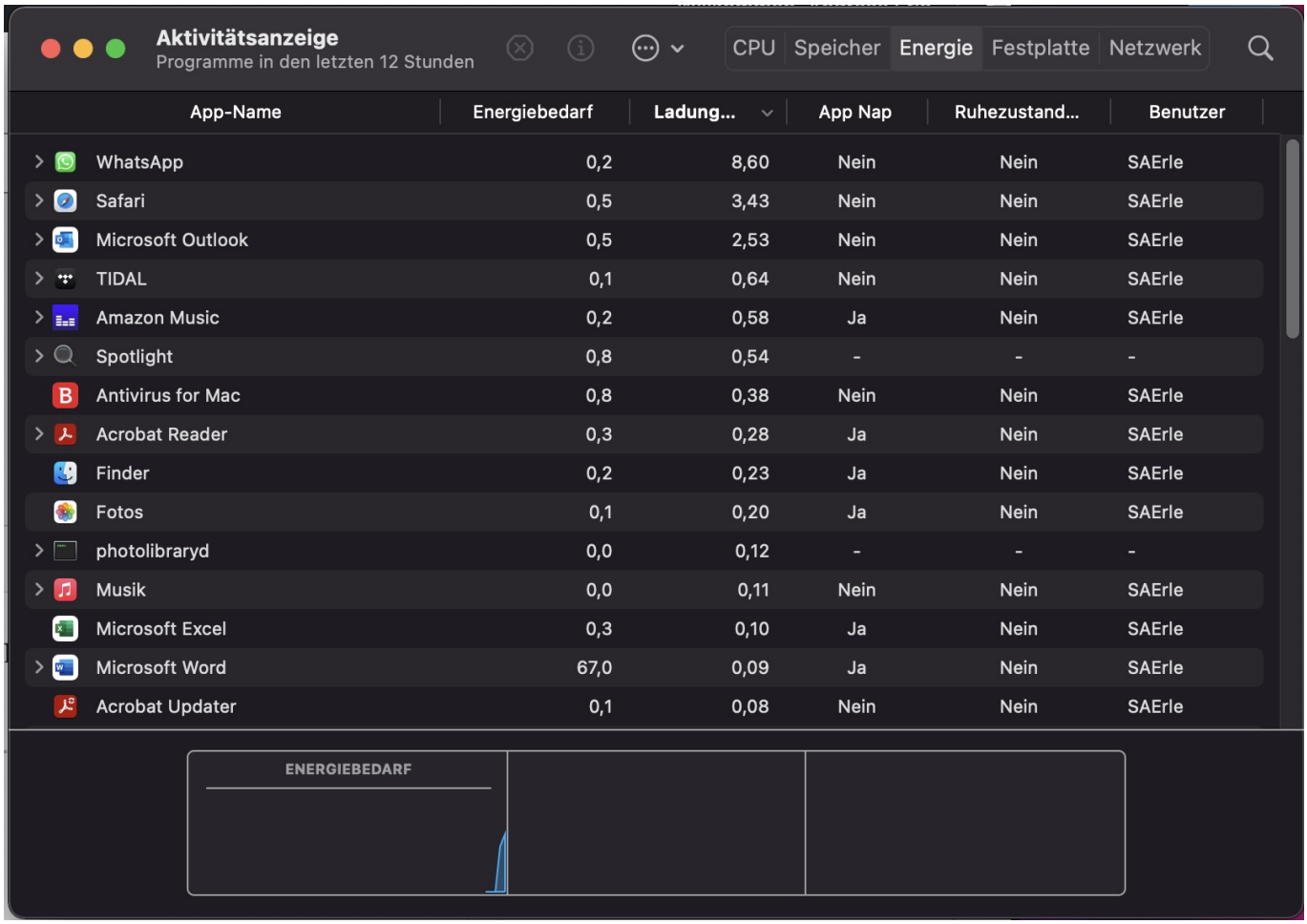
Die Akkulaufzeiten der aktuellen Macbooks sind bemerkenswert. Bei normaler sporadischer Nutzung kommen Sie in den meisten Fällen über einige Tage. Allerdings nur, wenn das Gerät korrekt in den Standbymodus geht und dort Strom spart. Wenn das bei Ihnen nicht der Fall ist, lesen Sie weiter!

Zwei Kernprobleme können dafür sorgen, dass Ihr Macbook auch bei zugeklapptem Deckel weiter Strom verbraucht und den Akku unnötig entladen. Das ist insbesondere unangenehm, wenn Sie beim Beenden der Arbeit am Vortrag noch genug Kapazität hatten und den Akku nicht geladen haben. Sie klappen das Gerät am nächsten Morgen auf und der Akku ist nahezu leer!

Apps, die den Standby verhindern

Es kann Apps geben, die einfach laufen wollen und Ihren Mac daran hindern, in den Standby-Modus zu gehen. Die können Sie einfach identifizieren: Starten Sie die **Aktivitätenanzeige** über Spotlight und klicken Sie auf den Reiter **Energie**. Sie

finden darin eine Spalte **Ruhezustand verhindern**. Steht neben einer der Apps in diese Spalte ein **Ja**, dann beenden Sie die App.



App-Name	Energiebedarf	Ladung...	App Nap	Ruhezustand...	Benutzer
WhatsApp	0,2	8,60	Nein	Nein	SAErle
Safari	0,5	3,43	Nein	Nein	SAErle
Microsoft Outlook	0,5	2,53	Nein	Nein	SAErle
TIDAL	0,1	0,64	Nein	Nein	SAErle
Amazon Music	0,2	0,58	Ja	Nein	SAErle
Spotlight	0,8	0,54	-	-	-
Antivirus for Mac	0,8	0,38	Nein	Nein	SAErle
Acrobat Reader	0,3	0,28	Ja	Nein	SAErle
Finder	0,2	0,23	Ja	Nein	SAErle
Fotos	0,1	0,20	Ja	Nein	SAErle
photolibraryd	0,0	0,12	-	-	-
Musik	0,0	0,11	Nein	Nein	SAErle
Microsoft Excel	0,3	0,10	Ja	Nein	SAErle
Microsoft Word	67,0	0,09	Ja	Nein	SAErle
Acrobat Updater	0,1	0,08	Nein	Nein	SAErle

Zu lange Zeit bis zum Standby

Die Standby-Zeit können Sie nicht über Einstellung direkt im System verändern. Ist diese zu lang, dann geht das System gar nicht ins Standby, bei einem macOS-Update waren es beispielsweise im Standard 86400 Sekunden (was 24 Stunden, also einem ganzen Tag, entspricht). Um das zu korrigieren, starten Sie das **Terminal** über **Spotlight** und geben Sie dann folgende Befehle ein:

sudo pmset -a hibernatemode 25

sudo pmset -a standby 1

sudo pmset -a standbydelaylow 60

sudo pmset -a standbydelayhigh 60

Die 60 ersetzen Sie über die gewünschte Zahl an Sekunden, bis das Gerät automatisch in den Standby-Modus wechselt.