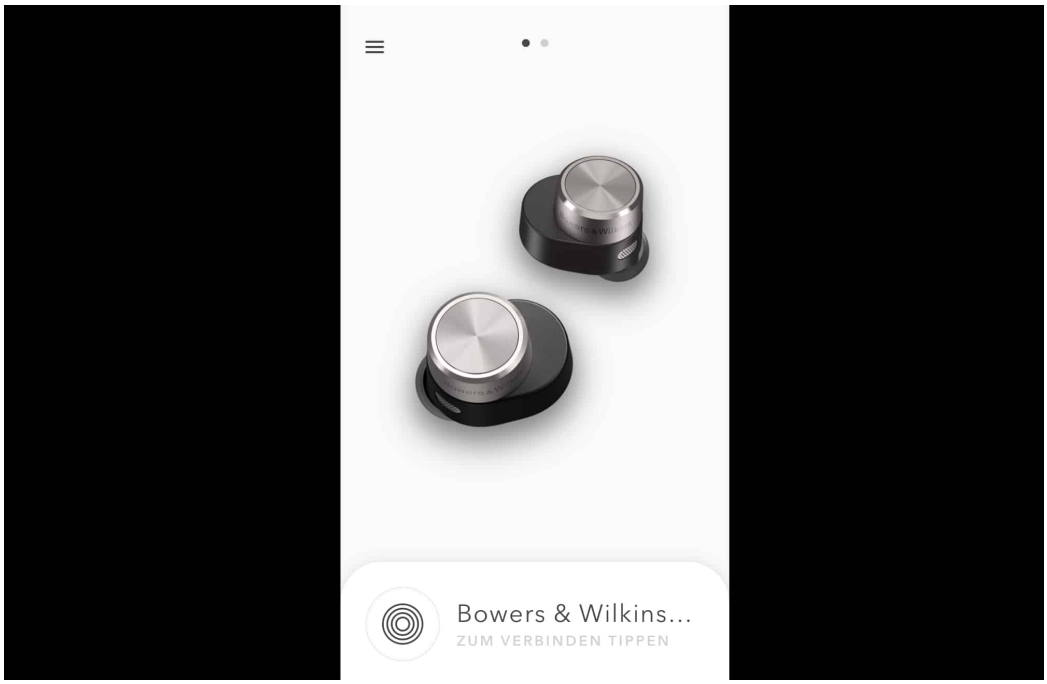
Schieb Report

Ausgabe 2021.29

Aussetzer bei Bowers & Wilkins PI7 vermeiden

Die Bowers & Wilkins PI7 sind vielen Aussagen nach mit die besten Bluetooth-In Ears. Auf Grund der variablen Übertragungsrate schaffen diese es, dem Quellmaterial und der Verbindungsart nach die qualitativ beste Übertragungsart zu wählen. Das soll dafür sorgen, dass Sie jederzeit ununterbrochenen Musikgenuss haben. Dumm nur, wenn Aussetzer den Hötgenuß stören. Wir zeigen Ihnen. was Sie dagegen machen können.

Der wichtigste Faktor für ungestörten Musikgenuss ist die ununterbrochene Übertragung. Aussetzer, auch wenn sie nur kurz sind, fallen direkt auf und stören einfach. Die Ursachen sind oft einfach: Der Sender (meist das Smartphone) und der Empfänger (die In Ears) sind entweder zu weit auseinander oder werden durch Störsender in der Nähe beeinträchtigt. In einem solchen Fall bringen Sie die Geräte näher zueinander.



Bei den B&W PI7 kommt noch ein weiterer Faktor hinzu: Auch wenn die nah am Smartphone/Tablet sind, unterbricht die Verbindung manchmal für mehrere Sekunden. Wenn Sie davon betroffen sind, dann hilft meist folgender Trick: Gehen Sie auf Ihrem Smartphone/Tablet in die Übersicht der laufenden Apps (bei neuen Android- und iOS-Versionen wischen Sie mit dem Finger von unten nach oben und dann nach rechts über den Bildschirm). Dann schliessen Sie die Headphone-App von Bowers & Wilkins, die normalerweise für die Einrichtung der InEars benutzt wird. Sobald diese nicht mehr im Hintergrund läuft, hören die Aussetzer auf.

Native Instruments Maschine+ mit Akku betreiben

Native Instruments ist mit seinen Maschine-Controllern in vielen Heim-Studios vertreten. Klassischerweise benötigen diese einen PC oder Mac, auf dem die Software läuft und die die entsprechenden Expansions zuordnet. Im Gegenzug versorgt das Gerät den Controller dadurch mit Strom. Beim Maschine+ ist das anders: Das Gerät funktioniert als komplette Standalone-Lösung - braucht aber ein Netzteil und ist damit nicht da nutzbar, wo Sie es gerade wollen. NI bietet keinen Akku an, aber wir können Ihnen eine Alternative präsentieren!

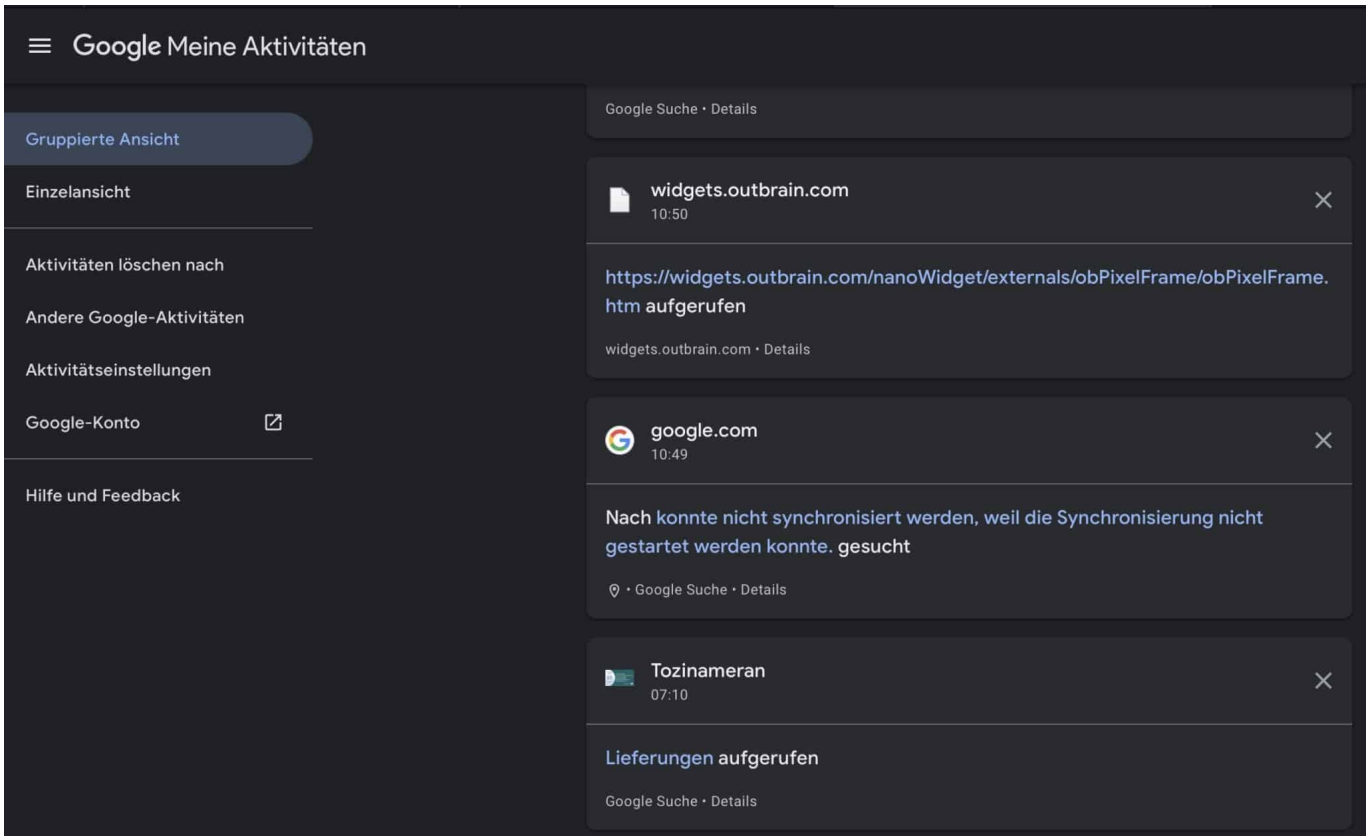
Native Instruments spricht selbst von der Möglichkeit, externe Akkupacks zu verwenden, bietet diese aber nicht an. Die Herausforderung: Das Maschine+ braucht 15V, während die normalen Akkupacks meist nur 5V bieten. Die Alternative: Das Omnicharge 20+, das Sie bei diversten Online-Händlern angeboten bekommen. Das hat neben den normalen USB-A und USB-C-Anschlüssen auch einen Netzteilanschluss, der zwischen 15 und 18 Volt eingestellt werden kann. Mit 15 Volt lässt sich das Maschine+ wunderbar betreiben.

Dazu brauchen sie allerdings noch ein Kabel mit zwei Rundsteckern. Omnicharge bietet das als Set mit diversen Steckergrößen an, das geht aber auch einfacher: Besorgen Sie sich ein Kabel mit kombiniertem 5,5*2,1 und 5,5*2,5 Kabel wie das hier. Das bekommen sie für deutlich unter 10 Euro!

Historie der Google-Suche finden

Kennen Sie das? Sie habe in einer intensiven Internetrecherche alle möglichen Webweiten gefunden. Nicht alle haben Sie als Lesezeichen abgelegt, und plötzlich brauchen Sie eine davon erneut. Kein Problem: Sie können ja erneut danach suchen. Leider ist Google sehr empfindlich auf die Begriffe und deren Reihenfolge, wenn Sie diese nicht exakt so verwenden wie beim ersten Mal, dann fällt das Suchergebnis anders aus. Da hilft die Suchhistorie!

Voraussetzung ist, dass Sie mit Ihrem Google-Konto angemeldet sind. Sobald Sie das einmal gemacht haben, bleibt die Verknüpfung zwischen Ihren Suchen und dem Konto gespeichert. Das sehen Sie unter anderem daran, dass oben rechts im Google-Fenster Ihr Kontobild angezeigt wird. Klicken Sie darauf, dann auf **Google-Konto verwalten**.



Unter **Daten & Personalisierung** > **Web- & App-Aktivitäten** klicken Sie auf **Aktivitäten verwalten**. Google zeigt Ihnen jetzt nach Datum sortiert Ihre Suchanfragen an. Wenn Sie eine davon erneut ausführen wollen, dann klicken Sie sie einfach an. Das Suchergebnis wird nicht zu 100 Prozent identisch, denn die Suche wird immer wieder aktuell durchgeführt. Je näher Sie vom Zeitpunkt her an der ursprünglichen Suche sind, desto höher sind Ihre Chancen, dass die gesuchte Seite (noch) dabei ist.

Probleme mit Bitdefender und iTunes lösen

Jede Synchronisation mit einem mobilen Gerät ist potentiell ein Sicherheitsrisiko. Das sorgt dafür, dass auch die Antivirenprogramme wie Bitdefender diese Kommunikation überwachen. Was auf der einen Seite Sicherheit gibt, weil damit die Verbreitung von Schadsoftware unterbinden wird, kann auch zu Problemen führen: Wenn iTunes/Musik nicht mehr synchronisiert, dann muss schnell eine Lösung her. Die zeigen wir Ihnen hier!

Wenn nach einem Update von Bitdefender bei der Synchronisation Ihres iPhones (oder iPads) die Meldung

Das iPhone MeiniPhone konnte nicht synchronisiert werden, weil die Synchronisierung nicht gestartet werden konnte.

und parallel dazu eine Meldung von Bitdefender kommt, dass mobile Geräte zentral über Bitdefender Central verwalten werden können, dann gehen Sie wie folgt vor:

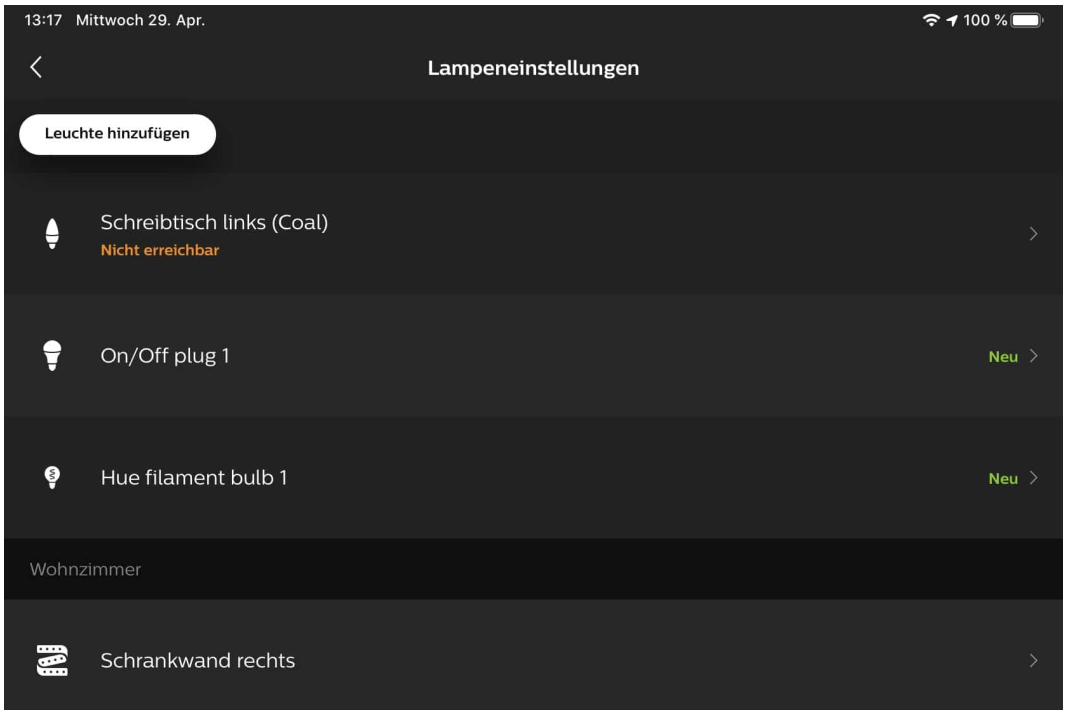
Deinstallieren Sie Bitdefender, indem Sie über den macOS Finder aus **Programme** > **Bitdefender** klicken und den **BitDefender Uninstaller** ausführen. macOS deinstalliert alle Programmodule, das kann einige Minuten dauern. Nach der Erfolgsmeldung starten Sie Ihren Mac neu.

Nach dem Neustart sollten Sie nichts anderes machen, als das iPhone/iPad anzuschliessen und einmal die Synchronisation zu starten. Denken Sie daran: Aktuell sind Sie ohne Virenschutz! Dann rufen Sie Bitdefender Central auf und installieren Sie von dort aus Bitdefender neu.

Nutzen von innr-Geräten mit Hue-Bridges

Smart Lighting, die Kunst der optimalen Raumbeleuchtung mit durch das Smartphones und das Tablet steuerbaren Lampen und Steckdosen, ist schon lange keine Nischenanwendung mehr. Da wundert es nicht, dass sich neben Philips mit seiner Hue-Reihe immer mehr Anbieter ein Stück des Kuchens sichern. Diese Produkte gilt es dann in das bestehende System zu integrieren. Wir zeigen Ihnen, wie.

Wichtig ist schon bei der Anschaffung ein genauer Blick auf die Kompatibilität. Kaufen Sie nur Lampen und Steckdosen, die mit Ihrem Hue-System kompatibel sind. Ein Beispiel dafür sind die Geräte von innr. Andere Konkurrenzprodukte, beispielsweise von TP-Link, sind auch per App bedienbar. Allerdings nur mit der eigenen, nicht mit der Hue-App. Da bleibt Ihnen dann nur die Verwendung eines übergeordneten Systems, dass mit beiden Herstellern klarkommt. Amazons Echo-Geräte können da helfen.



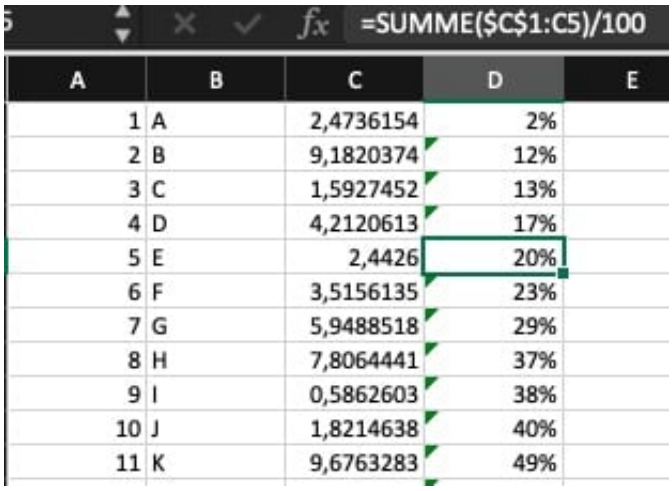
Smarte Glühbirnen lassen sich relativ einfach ins das Hue-System integrieren: Schrauben Sie sie in die Fassung, dann suchen Sie in der Hue-App unter **Einstellungen** > **Lampeneinstellungen** > **Leuchte hinzufügen** nach neuen Lampen. Auch die innr-Lampen werden dann - wie die Hue-Originale - angezeigt und können konfiguriert werden.

Bei den innr-Steckdosen gibt es eine Besonderheit: Stecken Sie diese noch nicht ein, sondern starten Sie erst wie oben beschrieben die Suche nach neuen Geräten. Erst wenn diese läuft, stecken Sie die Steckdose ein. Nach wenigen Sekunden wird diese angezeigt.

Zellen aufsummieren in Excel

Eine häufige Anwendung in Excel ist die Verwaltung von Anteilen. Wie viele Menschen haben schon gewählt? Wie viele verwenden prozentual betrachtet welches Produkt? Der Prozentsatz berechnet sich dann aus dem Anteil des jeweiligen Wertes an der Gesamtsumme, das ist schnell umgesetzt. Wie aber summieren Sie Werte auf? Wir zeigen es Ihnen!

Eine Formel für das Aufsummieren von Zellen suchen Sie in Excel vergeblich. Das macht aber nichts, denn mit einem kleinen Trick können Sie die schnell selbst bauen. Dabei nutzen Sie aus, dass es in Excel relative und absolute Zellbezüge gibt: **Relative Zellbezüge** werden aktualisiert, wenn Sie die Zelle in eine andere Zeile oder Spalte kopieren. Als Beispiel: Die Formel *=A1B1 wird automatisch zu =A2B2* geändert, wenn Sie sie eine Zeile nach unten kopieren, damit jeweils die Zellen der aktuellen Zeile verwendet werden.



	A	B	C	D	E
1	A		2,4736154	2%	
2	B		9,1820374	12%	
3	C		1,5927452	13%	
4	D		4,2120613	17%	
5	E		2,4426	20%	
6	F		3,5156135	23%	
7	G		5,9488518	29%	
8	H		7,8064441	37%	
9	I		0,5862603	38%	
10	J		1,8214638	40%	
11	K		9,6763283	49%	

Bei **absoluten Zellbezügen** stellen Sie der Zeilen- und/oder Spaltenangabe ein $ voran. Damit bleib die entsprechende Referenz unverändert, egal, wohin Sie die Zelle in der Tabelle bewegen. Als Beispiel: **A1** bleibt immer **A1**.

Das machen Sie sich beim Aufsummieren zu Nutze. Geben Sie der Zelle, in der die Aufsummierung stehen soll, eine Summenformel der Form =Summe(C1:C1): Die erste Zelle der Summe ist ein absoluter Bezug, die letzte Zelle die aktuelle. Wenn Sie die Zelle nun weiter nach unten kopieren, dann wird die Endzelle der Summenbildung immer angepasst auf die aktuelle Zelle, die Anfangszelle bleibt aber unverändert. Anders gesagt: Die Zelle enthält immer die Summe von der ersten Zelle bis zu aktuellen, kurz: Eine Aufsummierung aller Zellen bis zur aktuellen.

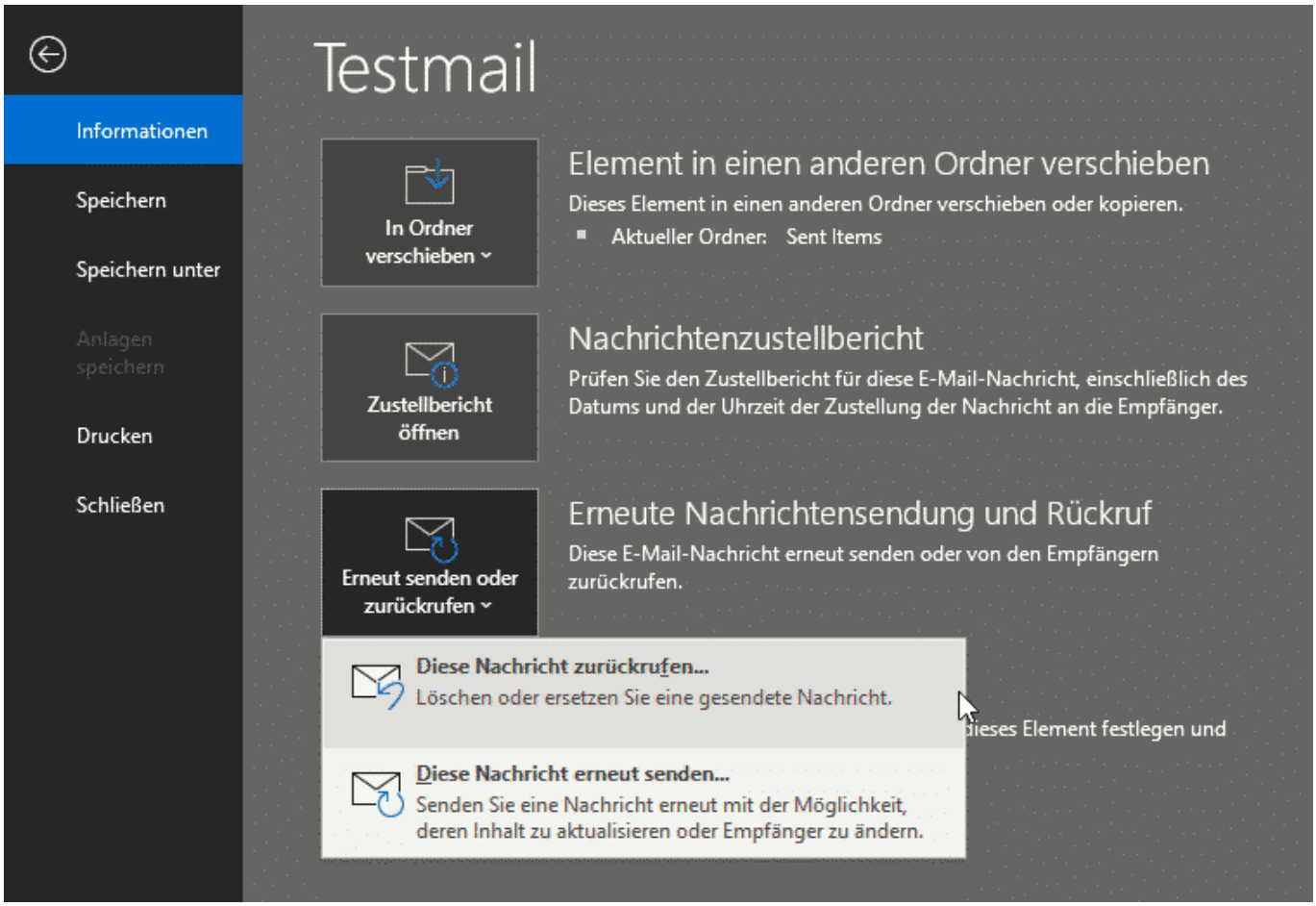
Zurückziehen einer E-Mail in Outlook

Sie kommunizieren täglich mit einer Vielzahl von Personen, oft laufen die Konversationen gleichzeitig. Da passiert es schnell, dass Sie eine E-Mail noch nicht ganz fertig haben uns sie versehentlich verschicken. Oder Sie klicken aus Versehen auf "Allen Antworten" statt nur dem einen Adressaten zu schreiben, für den Ihr Kommentar gedacht ist. Unterbestimmten Bedingungen haben Sie die Möglichkeit, eine bereits versendete E-Mail zurückzurufen.

Der Rückruf einer E-Mail löscht diese aus dem Posteingang des Empfängers, dieser bemerkt gar nicht, dass er eine E-Mail bekommen hat, die dann plötzlich weg ist. Tatsächlich geht das aber nur, wenn dieser die Nachricht noch nicht gelesen hat, sein E-Mail-Programm also die Mail noch nicht abgerufen hat oder der Empfänger sie noch nicht geöffnet hat.

Noch wichtiger: Ein Rückruf funktioniert nur dann, wenn Sender und Empfänger auf dem selben E-Mail-Server (meistens also in der selben Firma/Organisation) sind. Wenn Sie die E-Mail an andere Server geschickt haben, sollten Sie den Rückruf gar nicht erst versuchen: Neben der eigentlichen E-Mail bekommt der

Empfänger dann nämlich noch eine zweite, die ihn über den Rückrufversuch informiert. Das ist eher peinlich als nützlich!



Um eine E-Mail in Outlook zurückzurufen, klicken Sie auf den Ordner für gesendete E-Mails und öffnen Sie die E-Mail mit einem Doppelklick. Klicken Sie dann auf **Datei** > **Erneute Nachrichtensendung und Rückruf**. Im sich öffnenden Auswahlfenster klicken Sie auf **Diese Nachricht zurückrufen** und dann auf OK. Outlook versucht den Rückruf und teilt Ihnen für jeden Empfänger als separate E-Mail mit, ob der Rückruf erfolgreich war oder nicht.

Pegasus: Der Lieblingstrojaner für Schnüffelstaaten

Über die Schnüffel-Software "Pegasus" wird immer mehr bekannt: Viele Staaten sind Kunden beim israelischen Unternehmen NSO und lassen Menschenrechtler, Anwälte, Journalisten und Aktivisten bespitzeln - mit Hilfe eines schwer abzuschüttelnden Trojaners. Die Methoden sind abstoßend - die Folgen teilweise dramatisch.

Wir leben in einer komplizierten Welt. Auf der einen Seite ist den meisten von uns ihre Privatsphäre wichtig. Andererseits bedienen viele rund um die Uhr "Soziale Netzwerke" und geben damit gleich doppelt ihre Privatsphäre auf: Durch die Inhalte, die sie posten - und vor allem durch die Unmengen an Daten, die sie bei den großen Onlinekonzernen abliefern. Das ist eine allgemein bekannte Bedrohung - und jeder geht damit anders um.

Diffuse Gefahr: Ausspähung durch Trojaner

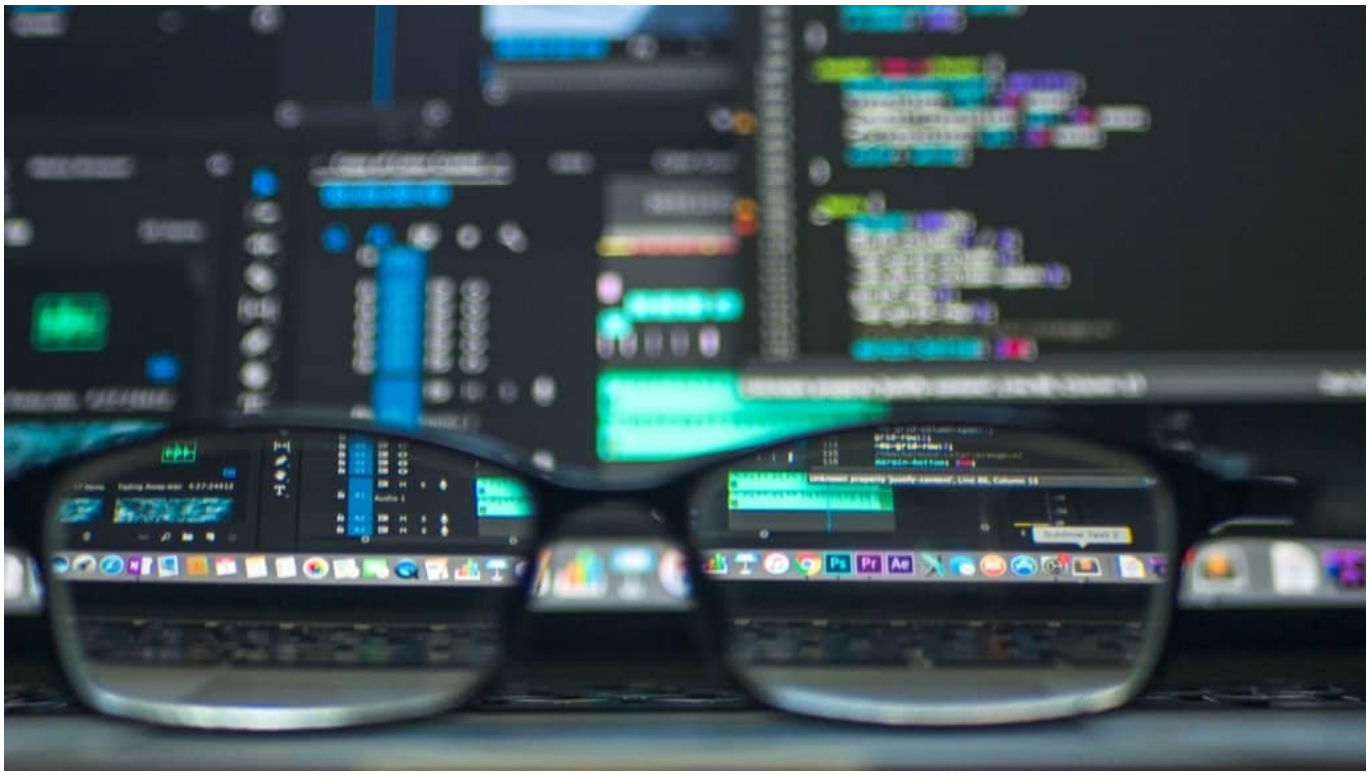
Dann gibt es aber auch noch diffuse Gefahren. Viele sorgen sich, der Staat könnte sie bespitzeln. In Deutschland tendenziell eine eher unbegründete Sorge - jedenfalls für die meisten Bürger -, aber doch nicht völlig unbegründet. Das belegen die aktuellen Recherchen von WDR, NDR, ZEIT und Süddeutscher Zeitung.

Dabei geht es um den Spitzel-Trojaner "Pegasus", den die israelische Firma NSO entwickelt und betreibt. Eine - wie es scheint - überaus potente Software, die so ziemlich alles ermöglicht: Mitlesen von Chat-Nachrichten (auch verschlüsselten), Mithören von Gesprächen, unbemerktes Aktivieren von Kamera und Mikrofon (das Handy wird zur fernsteuerbaren Wanze) und vieles andere mehr.

Ausnutzen von Sicherheitslücken

Betreiber NSO nutzt sogenannte "Zero Day Exploits" aus, Sicherheitslücken, die noch nicht bekannt, zumindest aber noch nicht gestopft sind, um den Trojaner aus der Ferne aufzubringen. Etwa, durch einen Anruf per WhatsApp oder Facetime. Das Opfer muss den Anruf nicht mal annehmen. Es sind solche Sicherheitslecks, die gnadenlos ausgenutzt werden.

Die israelische Firma arbeitet für viele Behörden in vielen Ländern. Angeblich, um dabei zu helfen, Kriminelle und Terroristen auszuspähen. Doch laut den Recherchen des nicht-kommerziellen Journalistenverbands Forbidden Stories und 16 Medienhäusern bespitzelt NSO auch Politiker, Journalisten, Menschenrechtler, Anwälte und Medienschaffende. Es kursiert eine Liste mit 50.000 Handy-Nummern potenzieller Opfer, darunter auch der französische Staatschef Emmanuel Macron.



Es braucht politischen Druck

Was bedeutet das? Der Aufwand ist vergleichsweise hoch, eine Person zu bespitzeln. Aber es ist machbar - und viele Staaten, darunter Saudi-Arabien, Bahrain, Mexiko oder das EU-Mitglied Ungarn zahlen dafür, dass NSO eigentlich besonders geschützte Menschen ausspäht.

Die Pegasus-Affäre zeigt: Es ist technisch möglich, aus der Ferne Smartphones auszuspähen. Und: Es wird auch gemacht. Wer es sich leisten kann und will, kann die Dienste von NSO nutzen.

Es ist wohl allerhöchste Zeit, politischen Druck auszuüben: Das Ausspionieren von Menschenrechtlern, Anwälten, Journalisten und Politikern sollte tabu sein. Alle Staaten sollten sich verpflichten, so etwas zu unterlassen - und

Unternehmen, die derartige Dienstleistungen anbieten, juristisch zu belangen.

https://vimeo.com/577962131

Bund stellt Autobahn-App vor - aber wozu bloß?

Die neue Autobahn-App kann nicht so recht überzeugen: Ein echtes Navisystem ist nicht enthalten - und Experten beklagen Sicherheits- und Datenschutzprobleme, weil die App Zugriff auf Webcams entlang der Autobahnen gewährt - und man so theoretisch die Bewegung eines Autos nachvollziehen kann. Dazu müssten Webcams und App aber tadellos funktionieren - und das tun sie nicht.

Deutsche Autobahnen sorgen überall auf der Welt für Gesprächsstoff, zumindest bei Menschen, die sich für Autos begeistern können - denn auf deutschen Autobahnen gibt es keine Geschwindigkeitsbegrenzung (theoretisch) und der Zustand der Autobahnen selbst ist auch ganz ordentlich, verglichen mit dem Rest der Welt. Aber über eins wird man sich in der Welt eher totlachen: unsere neue Autobahn-App.

Die App zeigt Staumeldungen und Verkehrsbehinderungen

Wieder mal ein Projekt von Bundesverkehrsminister Andreas Scheuer (CSU), das nach Steuerverschwendung aussieht. Denn die App bietet kaum einen Nutzen. Gut, wenn Andreas Scheuer auf dem Rücksitz seiner Limousine Platz nimmt und sich chauffieren lässt, kann er vielleicht mal einen Blick über den Verkehrsfluss "seiner" Autobahnen werfen. Aber sein Chauffeur wird die App eher nicht nutzen. Denn sie ist weitgehend sinnlos.

Die App, die es für iOS und Android gibt, zeigt zwar Staumeldungen und andere aktuelle Hindernisse an und kann auch eine Route planen - ist aber keine Navigationshilfe. Denn natürlich möchte man den Navisystemen am Markt keine Konkurrenz machen. Deshalb lässt sich eine mit der Autobahn-App geplante Route an die Navisysteme von Google und Apple übergeben (an andere nicht).

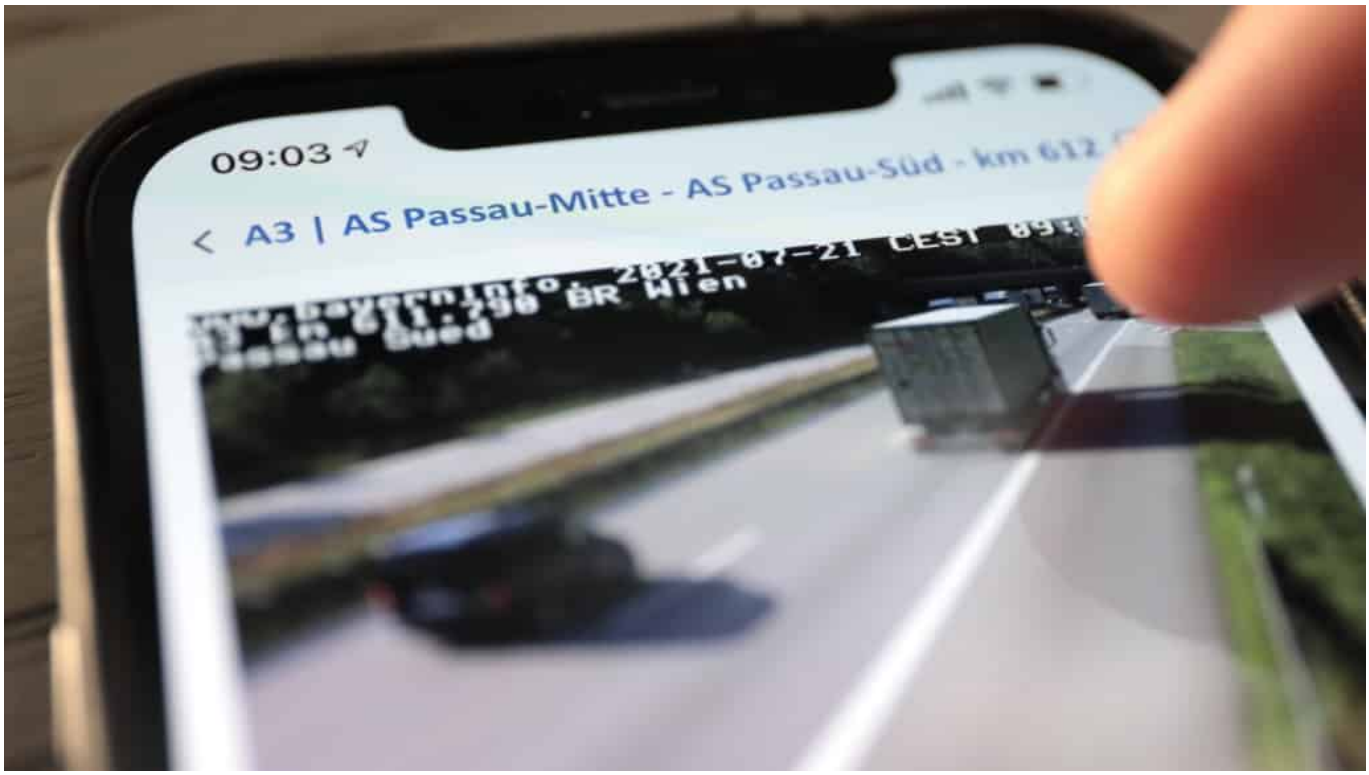
Nur: Wozu? Routen planen können die selbst - und auch sie kennen heute Staus, Sperrungen und vor allen Umgehungen und planen sie sofort ein.

Die App zeigt 1.000 Webcam-Bilder

Zwar zeigt die App auch an, wo es Raststätten gibt, wo Parkplätze oder Ladesäulen für E-Autos sind - aber ob die Parkplätze belegt sind, das zeigt die App nicht an. Das wäre zumindest für Brummi-Fahrer mal interessant. Aber das hätte die App nützlich gemacht, deshalb wurde darauf lieber verzichtet.

So ziemlich das einzige, was die Autobahn-App kann und bewährte Navisysteme nicht, ist das Anzeigen von Webcam-Bildern. Es gibt rund 1.000 Webcams an deutschen Autobahnen - und deren aktuelle Bilder lassen sich in der App anschauen. Damit man sehen kann, ob der Verkehr fließt.

Andreas Scheuer kann das auf seinem Platz im Fond nutzen. Sein Chauffeur nicht. Der muss auf die Straße schauen.



Eine völlig sinnlose Anwendung

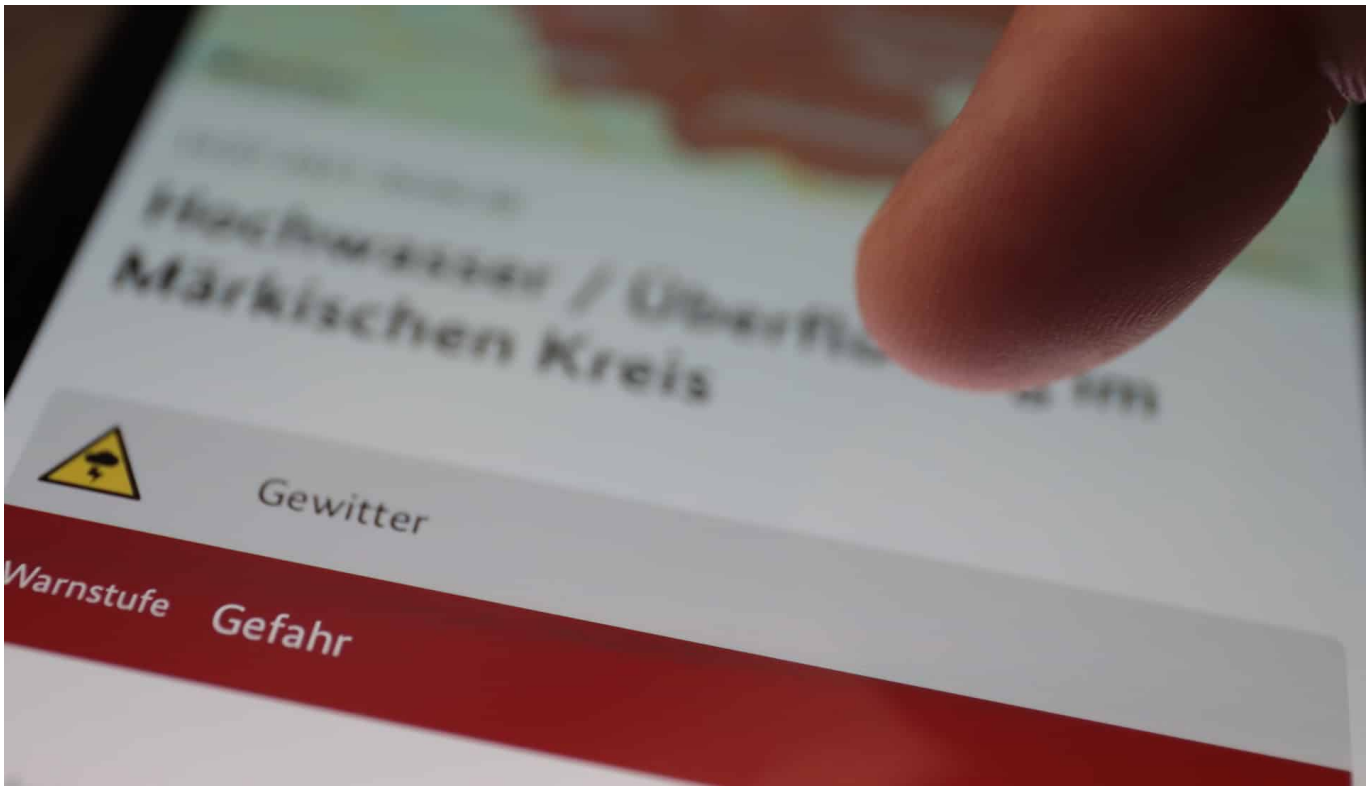
Ich will es gerne auf den Punkt bringen: Die App ist vollkommen nutzlos - und zeichnet ein erbärmliches Bild davon, wie Politik sich Digitalisierung vorstellt. Ich frage mich, wieso Dorothee Bär als Digitalisierungsbeauftragte der Bundesregierung ihrem CSU-Kollegen da nicht in den Lenker gegriffen hat ...

So ein sinnfreies Projekt. Sinnvoll wäre es zum Beispiel, die Autobahnen mit Sensoren und von mir aus auch mit Webcams auszustatten - und alle Daten der

Allgemeinheit zur Verfügung zu stellen. Dabei kommen dann sinnvolle und nützliche Apps raus.

Die Autobahn-App bietet im Alltag keinen wirklichen Nutzen

Katastrophenschutz: Warn Apps müssen besser werden



Wir haben zwei Warn-Apps in Deutschland, die vor Unwettern, Katastrophen, großen Unfällen und sogar Terroranschlägen warnen: NINA und Katwarn. Doch es wird Kritik laut, denn die Apps funktionieren nicht immer zuverlässig - und auch der Mobilfunk ist nicht so robust, wie er sein sollte.

Warnung, Bergung, Rettung und Versorgung: Darauf kommt es in Katastrophen an - und das alles will gut organisiert (und auch geübt) sein.

Um die Bevölkerung zu warnen, setzen Behörden auf einen Mix von Methoden: So wird nicht nur über Radio, Fernsehen und Internet vor Gefahren gewarnt, sondern auch mit Sirenen (aber immer weniger) - oder über Apps. Zwei sind dabei besonders erwähnenswert: Die bundesweit verfügbare und aktive Warn-App Nina vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) sowie die von Fraunhofer Fokus entwickelte Katwarn-App.

Zwei Apps im Einsatz: Nina und Katwarn

Nina hat im Unwetter mancherorts ganz gute Dienste erwiesen: Wer in Erftstadt und Umgebung wohnt und die App im Einsatz hat, wurde vergangenen Mittwoch von der Leitstelle gewarnt. "Bleiben Sie möglichst zu Hause", lautete die Bitte. Einen Tag später wurde über die App erneut gewarnt: "Dammbruch: Extreme Gefahr". In Ahrweiler gab es solche Warnhinweise in der Nina-App wohl nicht. Dafür aber über die Katwarn-App.

Es kann also besser werden, das Konzept, per App zu warnen. Es sollte keine Rolle spielen, für welche Warn-App man sich entscheidet: Zumindest die wichtigen Warnungen sollten alle erreichen.

Rund 10 Prozent der Deutschen haben Nina oder Katwarn installiert. Nicht schlecht, lässt sich aber zweifellos noch verbessern. Zum Vergleich: Die Corona Warn App haben deutlich mehr Menschen auf ihrem Smartphone.

Mobilfunknetze ausfallsicherer machen

Natürlich hat längst nicht jeder ein Smartphone - deshalb kann die Warnung per App nicht die einzige Maßnahme sein. Umgekehrt ist es aber auch kein Grund, auf eine App-Lösung zu verzichten. Denn die Apps haben einen riesigen Vorteil: Jeder User kann selbst entscheiden, welche Gebiete in Deutschland für ihn relevant sind. Also, ob man nur im aktuellen Aufenthaltsbereich oder zum Beispiel auch bei Warnungen in einem bestimmten Gebiet gewarnt werden möchte. Wichtig, wenn man mitbekommen möchte, ob etwa im Wohnort von Freunden oder Familie etwas passiert.

Und es gibt eine weitere Hürde: Fällt der Strom und/oder das Mobilfunknetz aus, funktionieren Warn-Apps nicht mehr - zumindest nicht mehr flächendeckend. Ein funktionstüchtiger Mobilfunk ist heute elementar, auch in der Organisation von Rettung und Hilfen. Denn längst nicht alle verfügen über Funksysteme.

Lassen sich Mobilfunkeinheiten besser absichern - und auch mit Notstromaggregaten ausstatten? Solche Fragen müssen wohl beantwortet werden.

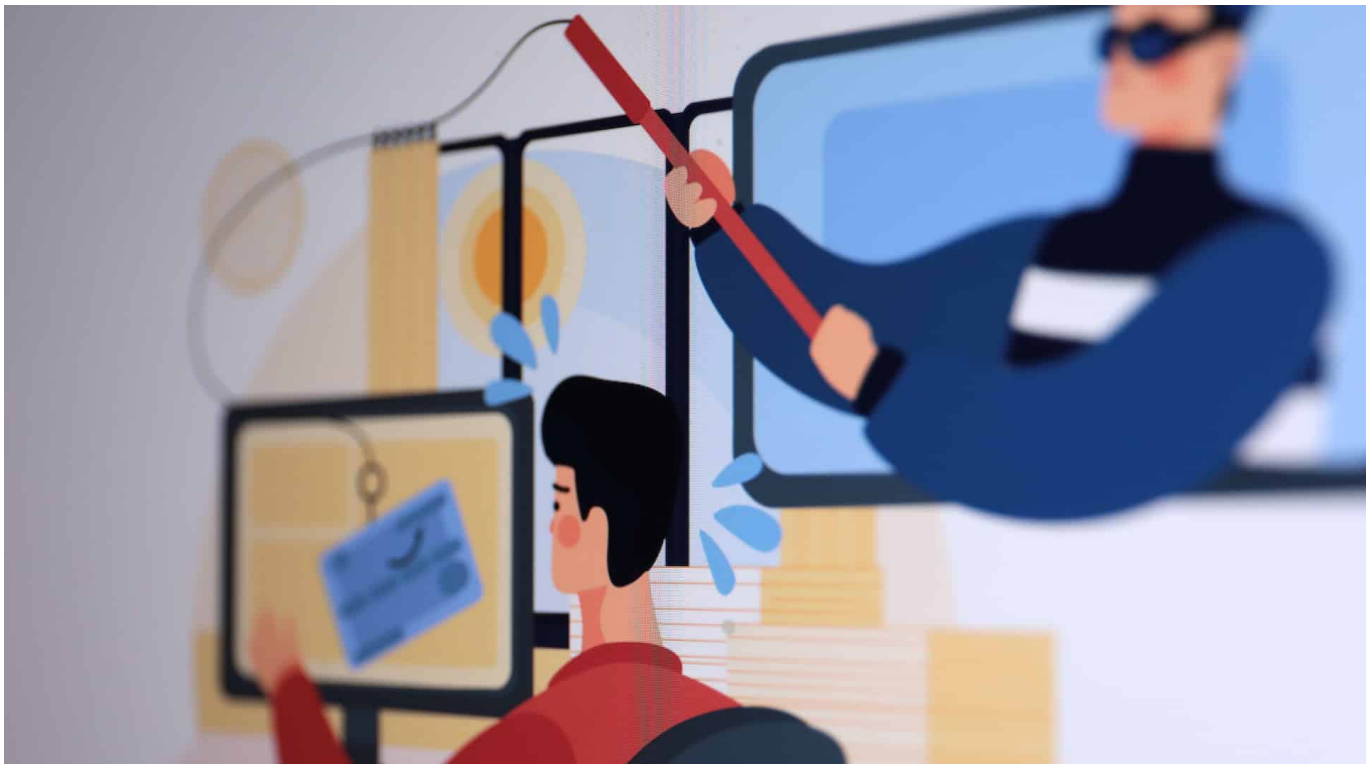
Vorschlag: Nina Opensource und erweitern

Und ich hätte noch eine Bitte: Die Corona Warn App wurde stets weiter entwickelt - orientiert am jeweiligen Bedarf. Es wäre sicher klug, auch die Nina-App neu zu denken. OpenSource wäre gut, damit andere Systeme andocken können. Und damit Experten Erweiterungen entwickeln können. Es ist zwar löblich, dass Facebook einen "Crisis Reponse" Dienst hat, in dem sich Menschen in Krisengebieten als "Ich bin in Sicherheit!" melden können. Aber Hilfen sollten nicht unbedingt über Facebook organisiert werden, sondern besser über nicht-kommerzielle Systeme. Die Nina-App könnte und sollte entsprechend ausgebaut werden.

Das geht nicht von heute auf morgen, ist aber ein wichtiges Projekt.

https://vimeo.com/576736973

Immer mehr Phishing-Angriffe auf Messengern - vor allem auf WhatsApp



Zwar sind die meisten Chat-Verläufe in modernen Messengern verschlüsselt - und daher weitgehend abhörsicher. Allerdings gibt es andere Gefahren. Cyberbetrüger nutzen mittlerweile vor allem Messenger wie WhatsApp, um ihre betrügerischen Nachrichten zu verteilen. Wer da nicht aufpasst, könnte in eine Phishing-Falle tappen. Besonders gefährdet: WhatsApp.

Cyberkriminelle gehen immer den Weg, der am meisten Erfolg verspricht. Früher waren Windows-Rechner das beliebteste Angriffsziel, heute sind es andere Plattformen. Wie die Experten beim Sicherheitsunternehmen Kaspersky ermittelt haben, nutzen die Cyberangreifer immer häufiger Messenger, um Menschen in Fallen zu locken.

WhatsApp ist aktuell die populärste Plattform von Cyberbetrügern

Die meisten Cyberbetrügereien über Messenger

Naheliegend, weil heute fast jeder Messenger benutzt (weltweit 2,7 Milliarden Menschen). Trotzdem ist das neu: Früher erfolgten die meisten Betrugsversuche über Mail, in den letzten Jahren in den Sozialen Netzwerken - und nun stehen zum ersten Mal Messenger ganz oben auf der Liste. Besonders brisant dabei: Wer Nachrichten von Freunden oder bekannten Unternehmen erhält, erwartet keine Betrugsversuche.

Doch da sollte sich niemand so sicher sein. Die Betrüger versenden - etwa über gekaperte Nutzerkonten - Nachrichten an Freunde, um sie zum Beispiel auf manipulierte Webseiten zu locken - und dort sensible Daten abzugreifen. Am häufigsten geschieht das über WhatsApp - das ist nun mal der beliebteste Messenger der westlichen Welt.

Laut Kaspersky werden hier derzeit mit Abstand am häufigsten Menschen betrogen: durch Phishing, Scamming und Pharming.

Android besonders gefährdet

Am ehesten gefährdet sind Menschen, die das Handy-Betriebssystem Android verwenden - denn Android bietet Angreifern mehr Möglichkeiten. Durch nicht gestopfte Sicherheitslecks, aber auch durch die Tatsache, dass Android weniger restriktiv ist als Apples iOS. In punkto Sicherheit ist das ein Nachteil.

WhatsApp ist also am gefährlichsten - und das gilt insbesondere für Android-Nutzer. iPhone-User sind seltener betroffen: Das mobile Betriebssystem bietet weniger Freiheit und damit auch weniger Angriffsfläche.

Auch Nachrichten von Freunden können Betrugsversuche enthalten

Wer selbst nicht zum Opfer werden will, sollte wachsam sein: Links besser genau prüfen, ob sie richtig geschrieben sind (vor allem die Adressen) und ob sie überhaupt Sinn ergeben. Auf keinen Fall der Aufforderung nachkommen, eine Nachricht weiterzuverbreiten - da stecken besonders häufig Betrugsmaschen dahinter.

Leider müssen Nutzer sogar bei Nachrichten aus dem Freundes- und

Bekanntenkreis wachsam sein, mahnt Kaspersky: Messenger-Konten könnten gehackt worden sein. Ungewöhnliche Nachrichten, die nicht zum typischen Kommunikationsverhalten einer bekannten Person passen, sollten immer die Alarmglocken läuten lassen.

Wer Sicherheits-Software wie Virenschutz etc. installiert, kann sich vor einigen Angriffen und Betrugsmaschen schützen. Denn solche Software erkennt bekannte Webseiten mit betrügerischer Absicht, überprüft automatisch Zertifikate und achtet auch auf Auffälligkeiten.

Wichtig ist aber zu wissen: Messenger sind längst kein geschützter Raum mehr. Im Gegenteil: Sie sind aktuell der beliebteste Tummelplatz für Cyberbetrüger aus aller Welt (vor allem aus Russland, Indien und Brasilien).

Scammer gehen gnadenlos vor: Ein Profi hat sie bei der Arbeit beobachtet