„Digitale Selbstverteidigung“

DaSou-Podcast-Folge mit Marius Melzer

Karina Filusch: Hallo und herzlich Willkommen beim DaSou-Podcast. Wir sind Rechtsexpertinnen und sprechen in jeder Folge über Datensouveränität, abgekürzt DaSou. Ich bin Karina Filusch, Datenschutz-Anwältin und externe Datenschutzbeauftragte.

Aileen Weibeler: Ich bin Aileen Weibeler und angehende Juristin.

Karina Filusch: Wir beschäftigen uns in unserem Büro täglich mit Datenschutz und haben in letzter Zeit Fragen erhalten, was die perfekte Alternative zu WhatsApp wäre.

Aileen Weibeler: Eigentlich war es geplant, dass WhatsApp seine AGB zum 8. Februar ändert, daraus wurde dann doch erst der 15. Mai. Grundsätzlich soll es dann möglich sein, dass WhatsApp unsere Daten an Facebook weitergibt und individualisierte Werbung geschaltet werden kann.

Karina Filusch: Ja und ich habe aus Versehen den neuen WhatsApp-AGBs zugestimmt. Ich war in Eile und da ist dieses kleine Fenster aufgeploppt auf meinem Handy, ich habe gar nicht gelesen, was das ist und habe einfach auf „ja“ gedrückt, ich ärgere mich total.

Aileen Weibeler: Oje, aber mach dir nichts draus, das passiert vielen Leuten, wenn sie in Eile sind. Man macht sich auch meistens nicht die Mühe, Änderungen in irgendwelchen Cookie-Bannern vorzunehmen.

Karina Filusch: Ja genau. Gut, dass du Cookie-Banner ansprichst. Unser heutiger Gast stellt uns DIE Lösung für dieses Problem vor und wir gehen der Frage auf den Grund, was ist besser Apple oder Android.

Heute ist Marius Melzer bei uns. Er ist Diplom-Informatiker und engagiert sich seit vielen Jahren im Chaos Computer Club Dresden. Der Chaos Computer Club ist eine Vereinigung von Hackerinnen und Hackern, die sich dafür einsetzt, dass Digitales und Technik zum Wohle der Menschen eingesetzt wird. Marius Melzer macht beim Projekt „Chaos macht

Schule“ mit und klärt Schülerinnen und Schüler über Privatsphäre im Internet auf. Und er hat ein total cooles Ende-zu-Ende-verschlüsseltes Video-Konferenz-Tool entwickelt: Palava TV. Ich habe es schon genutzt und kann es nur empfehlen.

Aileen Weibeler: Alle Infos dazu findet ihr in den Shownotes.

Karina Filusch: Marius, was ist für dich denn eigentlich DaSou und warum ist das so wichtig?

Marius Melzer: Das sind natürlich zwei unterschiedliche Fragen. Zum einen, was ist das? Ich würde sagen, das bedeutet, dass ich weiß, wo meine Daten sind und, dass ich bestimmen kann, wie damit umgegangen wird. Das bedeutet nicht unbedingt, dass meine Daten nirgendwo gespeichert sind. Dann kann ich ja in einer vernetzten Welt sehr wenig machen, auch wenn ich denke, dass die meisten Dienste mit weniger Daten durchaus genauso gut funktionieren würden. Aber ich denke, dass es wichtig ist. Und da sind wir sehr weit weg von, dass wir zum einen überhaupt eine Übersicht haben, wo unsere Daten landen. Wenn ich zum Beispiel Microsoft Teams benutze, da gab's einen sehr schön Blogpost von jemanden, der das mal durchexerziert hat, wo seine Daten von dieser Videochat-Applikation eigentlich im Endeffekt landen, bei welchen Firmen. Und das hat er irgendwie rausgefunden, indem er immer und immer wieder Anfragen gemacht hat, zum Beispiel auf Basis von der Datenschutzgrundverordnung und ähnlichen Gesetzen. Und das ist niemandem bewusst, glaub ich. Die Datenspuren, die man hinterlässt, wenn man sich irgendwo im Internet bewegt. Egal welche Website man benutzt. Manche besser, manche schlechter, die Daten landen immer an Stellen, wo man sie nicht erwarten würde. Und das ist für mich ein Teil von Datensouveränität, dass man solche Sachen weiß, wo sie landen und, dass es ein Default gibt, dass meine Daten nicht einfach weitergegeben werden, außer an Stellen, wo ich es explizit erlaubt habe.

Karina Filusch: Dann gehen wir jetzt mal ans Eingemachte. Und zwar wollte ich mit dir über Anti-Tracking in Browsern sprechen. Was tracken unsere Browser denn alles über uns?

Marius Melzer: Unsere Browser selbst tracken erst einmal hoffentlich nichts. Zumindest kann man das bei manchen Browsern explizit sagen, die natürlich Open Source sind, in die man reingucken kann, zum Beispiel Firefox. Was ein Browser ist, der von einer Stiftung, der Mozilla-Stiftung gemacht wird und der explizit mit der Idee dahinter entwickelt wird, dass die Daten von den Nutzern möglichst geschützt werden. Aber tracken tun vorrangig Teile von Websites. Also in den meisten Fällen kommt ein Tracker, ein Tracker ist ein kleines Programm, was nach Hause telefoniert, was zu irgendeiner Firma die Informationen liefert, dass ich und ich werde identifiziert anhand von zum Beispiel meiner IP-Adresse, also der Adresse, mit der ich mich im Internet bewege. Aber auch manchmal mit zum Beispiel den Eigenschaften meines Browsers oder wenn ich mich irgendwo eingeloggt habe, bei Facebook oder bei Google, von denen kommt die meiste Werbung, die ich im Internet sehe, auch auf anderen Websites. Dann werde ich darüber identifiziert und dann wird nach Hause telefoniert, welche Website ich besucht habe.

Also es gibt da große Werbe-Netzwerke und das sind die Netzwerke, die am meisten solche Tracker benutzen. Es gibt auch andere Firmen, die Tracker machen aus anderen Gründen, aber der Hauptteil sind die Werbe-Netzwerke. Also die großen Werbe-Netzwerke gehören zu Facebook und Google, aber es gibt auch noch andere. Und wenn man sich zum Beispiel so eine Website wie Spiegel-Online anguckt, es gibt ein Firefox-Plugin, ich muss dann nochmal kurz überlegen, wie das hieß, Lightbeam heißt das Plugin. Damit kann ich das visualisieren. Das installiere ich. Das macht mir selbst eine eigene Website auf, die aber lokal läuft. Also die sendet keine Daten oder sowas und die ist am Anfang leer und dann kann ich meine Lieblings-Websites ansurfen und dann werden die mir visualisiert, als so kleine runde Kugeln und dann gibt's kleine Dreiecke und das sind wiederum die Tracker, die verbunden sind mit den Websites. Und das Problem sind eben die Tracker, die bei einem Großteil der Websites, die ich an Servern eingebunden sind. Jetzt ist natürlich die Frage, wie kann ich dagegen vorgehen, dass das passiert? Und das Gute ist, dass diese Werbe-Netzwerke und diese Tracker, sind bekannt. Da gibt's Listen im Internet. Und natürlich, je problematischer und größer so ein Tracker ist, desto sicherer ist das, dass der auf solchen Listen landet. Und da gibt's eben Plugins für diverse Browser. Das bekannteste meiner Meinung nach ist „disconnect.me“. Und das ist auch denke ich das Beste, weil das zweite Ghostery ist zum Beispiel nicht Open Source und man kann da nicht reingucken, was es macht, aber wenn man den Firefox benutzt, dann braucht man gar kein Plug-in. Die haben nämlich mittlerweile das eingebaut, und zwar im Endeffekt die gleiche Technologie, die auch die disconnect.me- Plugin für andere Browser benutzt. Und das ist standardmäßig momentan erst einmal nur in diesem privaten Modus an, dass der dann dieses Tracking unterbindet. Also im Endeffekt kennt er die Tracker und unterbindet einfach das nach Hause telefonieren. Das Schöne daran ist, würde ich sagen, dass auch diese ganzen nervigen Popups, die immer kommen, die rechtlich da sein müssen, Cookies erlauben und so weiter und so fort, dass ich die im Endeffekt einfach ignorieren kann. Da kann ich überall, ich klicke da immer auf „allow all“, ums schnell wegzumachen, weil eben ich weiß, dass die problematischen Tracker, die Cookies benutzen, um mich wieder zu identifizieren, dass die zwar diese Cookies immer noch auslesen können, aber die können nicht mehr nach Hause telefonieren. Also Cookies gibt's natürlich überall im Internet und werden für ganz viele legitime Sachen auch verwendet, also zum Beispiel, wenn ich mich irgendwo einlogge, dann wird immer ein Cookie gesetzt. Aber es wird eben auch dafür verwendet, mich wiederzuerkennen, auf einer neuen Website, zum Beispiel durch einen Tracker, der dann so ein Cookie setzt. Und wenn aber der Tracker zwar das Cookie setzen kann, aber dann nicht mehr nach Hause telefonieren kann, dann macht es nichts mehr.

Karina Filusch: Marius, hast du uns gerade die Lösung für die ganzen Cookie-Pop-Ups gebracht? Ach, bin ich froh, dass du jetzt gerade die Lösung für dieses Cookie-Problem gegeben hast. Das wird uns allen natürlich den Alltag im Internet erleichtern, also vielen Dank! Das ist ein echt guter Tipp.

Marius Melzer: Im Firefox ist es ja schon installiert. Standardmäßig drin, wenn ich den auf meinem Computer habe und verwende. Und da kann ich auch einfach in den Einstellungen variieren, weil normalerweise ist das nur erst einmal im privaten Modus momentan. Da kann ich einfach in die Einstellungen gehen und dann unter Datenschutz und kann da klicken auf Aktivitäten, Verfolgung oder Anti-Tracking. Ich glaube Aktivitäten-Verfolgung heißt es. Und da kann ich das aktivieren. Das ist nicht nur im privaten Modus, sondern auch immer alles. Und dann sieht man links oben neben der Adressleiste, sieht man ein kleines Schild dann. Und dann machte er das Gleiche, was dieses Plugin auch macht. Und das Coole daran ist, dass das auch im Firefox auf Android zum Beispiel geht. Und auf diesem, bei diesem Firefox-Klar-Browser für iOS. Das heißt, da sind diese Sachen auch schon mit drin. Das kann ich genauso einstellen. Und ich habe das sozusagen auch auf dem Handy unterbunden, das Tracking erst einmal im Browser über Websites. Beim Handy gibt es halt noch die zweite Sache, dass dieses Tracking, das gibt's auch für Apps. Und das ist sowohl in Android als auch in iOS-Geräten möglich. Aber genau, das ist sozusagen ein weiteres Thema.

Karina Filusch: Ja, wir können gleich darüber sprechen. Auf Handys heißt das oft Werbe-ID. Das ist so dieses Schlagwort, was ich oft höre. Man soll diese Werbe-ID ausschalten und dann wird man nicht mehr getrackt. Ist das richtig so?

Marius Melzer: Also das ist ja wie bei jedem Tracking, geht es den Trackern, also den Überwachern erst einmal darum, dass sie ein Wiedererkennen im Web eben über diverse Websites hinweg und auf dem Handy über App-Grenzen hinweg und dann im Browser werden Cookies gesetzt, die eben auch positiv sein können, aber für den Einsatzzweck würde ich sagen, sind sie negativ, um jemanden identifizieren zu können. Und bei Apps ist das in den großen Handy-Betriebssystemen schon fest eingebaut, dass der Benutzer in einer App eine eindeutige ID bekommt, die sozusagen über das gesamte Gerät gleichbleibt und Firmen dann das miteinander verbinden können, dass ich zum Beispiel der Gleiche bin, der WhatsApp mit einem bestimmten Account verwendet wie eine andere App.

Karina Filusch: Ist diese Werbe-ID also dafür zuständig, dass wenn ich Alpaka bei Google eintippe und suche, dass ich dann für Alpakas Werbung bei Facebook zum Beispiel bekomme?

Marius Melzer: Das kann gut passieren und es ist natürlich auch so, dass zusätzlich, wenn man jetzt ein Android-Gerät hat, dass diese Werbe-ID, die natürlich von Google kommt und, dass dann Google wiederum weitere Informationen bekommt, über was ich auf dem Handy mache und was ich auf dem Computer mache, was ich sozusagen im Web mache und das miteinander verbinden kann. Und das ist auch ein grundsätzliches Problem.

Auf dem Handy kann man das nur ein bisschen schwerer, würde ich sagen, verhindern, da muss man da bei einem Android, muss man ja immer ein Google-Konto angeben, es sei denn, man hat so ein freies Android installiert. Aber auch im Browser ist es so, wenn ich da zum Beispiel bei Facebook noch angemeldet bin oder wenn ich bei Google noch angemeldet bin und auf eine andere Website gehe, die überhaupt nichts mit Facebook oder Google zu tun hat und das entweder zum Beispiel Werbungen von denen drin oder alternativ, dass irgendwie sonst so ein Like-Button von Facebook mit drin, das ich anklicken kann oder so ein Google-Ding zum Beispiel. Dann bin ich angemeldet weiterhin. Dann weiß eben Facebook, dass ich derjenige bin, der da angemeldet ist. Auch da, auch über solche Sachen funktioniert so eine Identifizierung.

Karina Filusch: Ich habe mal so eine Frage an dich. Ich lese immer wieder, dass Apple so viel besser sein soll im Vergleich zu Android-Geräten, weil Apple ja nicht so viel tracken würde und so viel sicherer sei, dass sogar sensible Berufsgruppen wie Journalistinnen und Journalisten auf Apple setzen, weil es heißt, es sei so viel sicherer und würde so weniger tracken. Ist das wahr? Kannst du das bestätigen?

Marius Melzer: Da muss man vielleicht zum einen zwischen Sicherheit und Datenschutz ein bisschen trennen. Ich glaube, die Sicherheit der Geräte an sich, da nehmen sich die Systeme heutzutage nicht viel. Da gibt's von beiden Seiten große Anstrengungen, das möglichst sicher zu gestalten. Also sicher im Sinne von einem Angreifer von außen zum Beispiel, der das eigene Gerät übernehmen möchte. Und dann gibt's den Datenschutzaspekt. Und da gibt es natürlich auf der einen Seite, gibt es einfach den Unterschied, dass Google mit meinen Daten Geld macht, und das würde ich sagen ein primärer Entwicklungsgrund für Android gewesen ist, dass man auch auf mobilen Geräten noch mehr Daten sammeln kann, von den Leuten. Das gibt es in dem Sinne bei Apple erst einmal nicht. Die Geräte sind so teuer, dass die schon auch ihren Hauptteil des Geldes einfach mit den Geräten selbst machen und hinter den Daten momentan keine Einnahmequelle sehen. Aber er ist auch so, dass bei Apple-Geräten das alles Closed Source ist. Also, dass man da erstmal nicht reinsehen kann, wie es funktioniert und es gab in den letzten Monaten auch immer mal so Berichte darüber, wo sich Apple einige Fauxpas geleistet hat.

Unter anderem war es so, dass die immer wenn eine App gestartet wurde, dass die da so Telemetrie gesandt haben, also die Informationen, dass ein Programm benutzt, wird zum Beispiel und das ist nicht okay. Und das haben sie, glaube ich, jetzt auch abgeschaltet, weil es da irgendwie einen großen Aufschrei gab. Aber das zeigt auch, dass sie in solchen Sachen natürlich experimentieren und dass man nicht per se sagen kann, benutze ein Apple-Produkt und ihr seid sicher. Aber es gibt natürlich den Unterschied, dass sie momentan nicht damit ihr Geld verdienen. Dafür sind die Geräte eben sehr viel geschlossener und bei Android ist es so, dass ein großer Teil des Grundsystems ist Open Source und in die kann man reingucken. Und das sorgt dafür, dass es für Android-Geräte häufig alternative Android-Systeme gibt, die man natürlich erstmal installieren muss, um vielleicht ein paar zu nennen, es gibt dieses LineageOS, was würde ich sagen, das Standardsystem da ist. Es gibt mittlerweile auch einfachere zu installierende und benutzenden sicherheitsfokussierte Systeme und da gibt's CalyxOS, das ist sozusagen einfach ein alternatives Android. Das kann ich auf mein System machen und habe die ganzen Google Sachen erstmal nicht und hab von Grund auf erst einmal ein Handy, was mich nicht belauscht und wo ich auch reingucken kann. Das heißt, so etwas hier ist auf jeden Fall, auch wenn es vielleicht erst ein kleiner Aufwand ist, ist es viel besser als zu sagen, ich kauf mir einfach ein Apple-Gerät, meiner Meinung nach.

Karina Filusch: Ja, und wie funktioniert das? Ich benutze Android. Ich oute mich mal. Gehe ich da jetzt einfach auf den Store und lade mir dieses System herunter?

Und dann ist alles gut. Funktioniert das so einfach?

Marius Melzer: Das ist leider ein bisschen schwieriger.

Karina Filusch: Schade!

Marius Melzer: Gut ist, dass es mittlerweile für fast jedes Handy eine ganz gute Anleitung dafür gibt. Aber das grundsätzliche Prozedere ist, dass man sein Handy mit einem USB-Kabel an den Computer macht. Auf dem Computer dieses neue System herunterlädt, das auf das Handy spielt, auf eine SD-Karte zum Beispiel, da drauf oder in den internen Speicher. Und dann installiert man vom Computer heraus einen Bootloader, nennt sich das, einen neuen, den man starten kann, wenn man das Handy startet, gibt man hier so eine Kombination an Tasten ein. Meistens ist es der Aus-Knopf und die Lautstärke-Runter-Taste, die dann nicht das normale System startet, sondern diesen neuen Bootloader. Und über den kann man dann das System installieren, das ist nicht so einfach wie eine App zu installieren.

Karina Filusch: Und denkst du so eine 08/15-Nutzerin wie ich kriege das hin mit einer Anleitung?

Marius Melzer: Ich glaube bei diesem bei diesem CalyxOS ist das nochmal ein bisschen einfacher gestaltet. Und ich denke das kriegt man durchaus auch mit so einer Anleitung hin. Bei dem LineageOS, was den Vorteil hat, dass es für fast alle Geräte verfügbar ist, ist manchmal ein bisschen schwieriger. Es gibt aber mittlerweile, da muss man sich natürlich ein neues Gerät besorgen, aber es gibt Projekte, die einem sowas schon einspielen. Und zwar gibt es dieses /e/Phone, also nicht iPhone, sondern mit E im Deutschen. Das wird /e/ geschrieben. Das ist wie dieses CalyxOS, ein Privatsphäre schützendes Android ohne die ganzen Google Sachen und die verkaufen zum Beispiel refurbished, gebrauchte Handys sozusagen, wo sie das Aufspielen schon für die Leute, die sich das nicht trauen, das selbst zu machen.

Karina Filusch: Ach cool, dann tut man dem Klima was Gutes und seinen Geldbeutel und gleichzeitig schützt man seine Daten noch. Das ist ja perfekt. Vielen Dank. Das Projekt kannte ich noch gar nicht. Wir verlinken das alles natürlich. Und für diejenigen, die gerade nicht mitschreiben können.

Marius Melzer: Wo wir gerade bei Klima sind, ist auf jeden Fall., also es ist natürlich gut, seine Geräte so lange wie möglich zu benutzen. Und ich würde sagen, auch da hilft Open Source weiter, weil dieses freie Android zum Beispiel, also dieses LineageOS, häufig hat das noch Updates, lange nachdem die eigentlichen Hersteller keine Updates für das Gerät mehr liefern. Und man kann auch alte Handys von sich wieder zum Leben erwecken mit sowas und wieder eine frische Software drauf spielen. Genau, und zum anderen ist es aber andersherum auch sehr wichtig, dass man so alte Geräte weggibt, damit irgendwie die Bauteile da drin weiterverwendet werden können. Das wissen, glaube ich, die meisten nicht, die fünf alte Handys noch drin haben. Eigentlich wichtiger ist, die alten Geräte wieder im Kreislauf hineinzugeben, als sich nicht das neue Handy zu kaufen.

Karina Filusch: Mist, hätten wir mal vor ein paar Monaten gesprochen, als ich alle Handys, die in meiner Schublade gelegen haben, verkauft habe, dann hätte ich das vielleicht nochmal umsetzen können und die noch verwenden können.

Also Klimaschutz trifft Datenschutz. Das hängt so eng beieinander, dass hätte ich gar nicht erwartet. Also einfach nochmal eine ganz neue Perspektive, denke ich, die wir da aufgemacht haben. Marius, bevor wir weiter zu Open Source gehen, weil wir das jetzt schon öfter angesprochen haben. Und apropos das Handy, das mithört. Es sind ja nicht nur Google Dienste und andere von anderen Firmen, die mithören, sondern auch tatsächlich Apps, die mittracken. Ich hab neulich auf Twitter gelesen, da hat eine Nutzerin geschrieben, jetzt könnte man so ein Handy-Frühjahrsputz machen und doch mal alle überflüssigen Apps entfernen. Warum ist das so wichtig, sich solcher Sachen zu entledigen, ab und zu mal?

Marius Melzer: Also da ist es natürlich zum einen wichtig, dass man vielleicht einen kleinen Überblick hat, welche Apps denn überhaupt welche Daten über mich sammeln. Und das ist natürlich schwer zu sagen. Es gibt aber einen, würde ich sagen, Anhaltspunkt. Also es gibt sowohl in dem Playstore von Google als auch im App Store von Apple mittlerweile bei jeder App, wenn man ein bisschen runter scrollt, die Berechtigung und aber auch eine Übersicht über die Daten, die diese App sammelt über einen. Und das ist relativ detailliert und das ist auch sehr interessant. Wenn man sich zum Beispiel mal unterschiedliche Messenger anguckt, kommen wir ja wahrscheinlich noch zu, dass wenn man das mal vergleicht. So ein Signal Messenger, der da einen einzigen Eintrag hat, den mit Daten, die sie eigentlich gar nicht verwenden. Und wenn man sich den Facebook Messenger anguckt, der eine Palette von sicherlich 40, 50 Datenpunkten hat, die dieser Messenger über einen verrät.

Das heißt, das ist der erste Punkt. Wenn ich mir meine Apps angucke, dann würde ich zuerst einmal gucken, was sammeln die überhaupt für Daten über mich? Und dann ist es natürlich, wenn man sich nach Alternativen umguckt, ist es schlau, auch da auf Open Source zu setzen, also auf Apps, die einsehbar sind und die in den meisten Fällen auch gar nicht das Interesse haben, Daten zu sammeln. Und dann kann ich vor allem unter

Android den F-Droit Store empfehlen. Das ist sozusagen eine Alternative zu dem Google Play Store, kann man auf f-droit.org runterladen. Kann man nicht im Play Store finden, natürlich, weil sie das nicht wollen. Aber direkt auf dieser Website kann man auf Download klicken und den einmal runterladen. Dann alle Apps, die man daraus installiert sind Open Source.

Karina Filusch: Um was gibt es da so für Open Source Apps in diesem F-Droit-Store?

Marius Melzer: Alles Mögliche, würde ich sagen. Das Coole ist, dass es in vielen Fällen eben nicht die Apps sind von einer bestimmten Firma. Wenn ich jetzt mal das Beispiel von so Transport Apps nehme, wo ich gucken kann, wie ich mit einem Bus von einem Ort zum anderen komme in meiner Stadt, dann gibt's da eben nicht die DVB oder die BVG App drin, unbedingt, weil das eben nicht so bekannt ist. Aber dann gibt's da Apps drin, die Open Source sind und die mit ganz vielen unterschiedlichen lokalen ÖPNVs funktionieren und wo man es einfach einstellt. Ich bin hier in Dresden gerade und dann funktioniert das genauso. Und wenn ich dann nach Köln reise zum Beispiel, dann kann ich es umstellen und dann funktioniert es auch da, die gleiche App.

Karina Filusch: Kann ich diese App auch benutzen, wenn ich ein ganz normales Android benutze, also ich brauche nicht dieses andere Betriebssystem, sondern kann auf dem normalen Android diese alternative Öffi-App nenne ich sie mal, benutzen?

Marius Melzer: Genau, das geht auf jeden Fall und es geht auch parallel zum Play Store, also wenn es Apps gibt, auf die ich gar nicht verzichten kann, weiß nicht, sowas wie Spotify oder so was, dann kann ich die eben aus dem originalen App Store nehmen. Das zumindest ein einfacher Schritt, wo man erstmal nicht viel ändern muss.

Karina Filusch: Ja, ich hab noch eine grundständige Frage. Wenn diese großen Unternehmen, was sammeln sie denn da so für Daten? Ich lese immer wieder was von Metadaten. Was sind das für Daten? Und warum ist das eigentlich so schlimm, dass diese großen Unternehmen, diese Daten von uns bekommen?

Marius Melzer: Also es gibt, würde ich sagen, diese zwei Arten von Daten. Es gibt die Inhaltsdaten und die Metadaten. Die Inhaltsdaten sind jetzt bei einem Messenger das, was ich schreibe oder bei Videotelefonie, mein Bild und mein Ton, den ich versende, das ist der Inhalt. Und das ist natürlich das erste, was ich schützen möchte, rein aus Reflex würde ich sagen, dass niemand meine private Kommunikation mithören kann. Und das ist auch total wichtig. Da gibt es verschiedenste Arten von Verschlüsselung, um dem entgegen zu treten. Da gibt es zum einen die Transport-Verschlüsselung. Das ist, wenn ich eine Website aufrufe und oben in der Adresszeile „https" steht, steht statt „http" und meistens noch so ein zugeschlossenes Schloss, dann ist die Verbindung verschlüsselt. Aber auf dem Server selbst, wo diese Website liegt, die können natürlich noch sehen, was ich da hochlade oder sowas. Und wenn ich aber mit jemand anderem kommuniziere, zum Beispiel über einen Messenger oder Videochat, also immer eine direkte Kommunikation zwischen Leuten, dann kann ich eine viel stärkere Form der Verschlüsselung, wählen, nämlich die Ende-zu-Ende-Verschlüsselung und das bedeutet, dass meine Inhaltsdaten auf meinem Handy oder auf meinem Rechner verschlüsselt werden, also eingepackt werden in ein Paket, das niemand öffnen kann. Und das kann dann durchs Internet gehen, wie es will, bei wahrscheinlich einem Anbieter von der App oder von der Website vorbeigehen und dann zu dem anderen gelangen, mit dem ich kommuniziere. Und erst der kann diese Verschlüsselung wieder entschlüsseln. Und ist es wichtig, dass man so für die Kommunikation mit Menschen, würde ich mal sagen, auf Apps und Programme ausweichen, die das machen, die Ende zu Ende Verschlüsselung.

Karina Filusch: Ja, da fällt mir ein Programm ein, dass das macht. Ich erinnere mich, vor einiger Zeit hatte WhatsApp so eine Nachricht aufploppen lassen bei den Nutzerinnen und Nutzern. Und da hieß es „wir verschlüsseln jetzt Ende-zu-Ende". Also das ist etwas Gutes.

Aber mit WhatsApp gibt es noch ein anderes Problem, denn kürzlich hat WhatsApp die AGBs geändert und gibt an, dass jetzt die Daten mit Facebook verbunden werden sollen. Ich bin der Überzeugung, es ist schon vorher passiert, aber jetzt machen sie es offiziell in den AGBs und wer da ablehnt, der kann WhatsApp nicht mehr benutzen. Das bedeutet friss oder stirb. Also entweder du gibst dem ganzen Konzernen deine Daten oder du kannst unser Produkt nicht weiter nutzen. Deswegen gibt es jetzt gerade so eine Flucht von WhatsApp und ich wollte deshalb mit dir auch noch über Messenger-Dienste sprechen, was es da so für gute Alternativen gibt. Was benutzt du denn für einen Messenger?

Marius Melzer: Also ich benutze schon seit langer Zeit ausschließlich Signal. Einen anderen Messenger hab ich gar nicht installiert.

Karina Filusch: Und warum?

Marius Melzer: Das hat mit ganz vielen unterschiedlichen Sachen zu tun. Ich kann mal versuchen, das aufzulisten. Das hängt zum einen mit Transparenz wieder zusammen. Bei Signal ist sowohl die App auf meinem Handy, die ich benutze, als auch der im Server-Code, beides ist Open Source und in beides kann man reingucken, weil es ist transparent und Signal ist vom Unternehmens-Typ sozusagen, ist kein Unternehmen, sondern ist eine Stiftung, die hat in ihren Statuten, dass sie keinerlei Datensammeln, eben bis auf die zwei, drei kleinen Sachen, die sie brauchen, um es weiterzuleiten. Und das kann man wiederum auch in dem Source-Code überprüfen, dass sie nichts anderes machen. Und das heißt, sie sind politisch und finanziell relativ unabhängig. Und die App ist schon mal Open Source und der Server ist Open Source. Und das sind schon mal finde ich ziemlich wichtige Dinge. Und dann ist eben noch der zusätzliche Punkt, da waren wir eben stehengeblieben, dass es eben noch die Metadaten gibt. Und die Metadaten sind Daten über meine Daten. Außerdem die ganzen anderen W-Fragen, also wer kommuniziert mit wem, in welcher Art und Weise? Und manchmal spielen solche Sachen wie das Wo noch eine Rolle, was auch ein ganz wichtiges Datum ist, wo ich mich aufhalten, weil ja super viele Apps jetzt nicht unbedingt nur Messenger Apps, aber so super viele Apps können auf den Standort zugreifen und haben hinterher ein komplettes Profil darüber, wo ich mich bewege, wann ich wo, war, zu welchen Ärzten ich gehe, ob ich irgendwie in irgendeine Kirche gehe… Über solche Dinge kann man wahnsinnig viel über eine Person herausfinden. Wie tickt die Person, ist es ein Frühaufsteher? Hat sie eine Beziehung? Hat sie vielleicht eine Affäre, ob man schwanger ist. Alles.

Karina Filusch: Unglaublich. Und diese Daten geben wir gratis Google und Co.

Marius Melzer: Genau und das ist eben der Punkt, dass selbst wenn WhatsApp angibt, dass sie Ende-zu-Ende-Verschlüsselung machen, was ich leider noch nicht einmal überprüfen kann, weil ja die App nicht Open Source ist. Das heißt, da können sie versprechen, wie sie wollen. Das kann niemand nachprüfen. Dann gibt es immer noch die Metadaten, das heißt, mein gesamtes Kontaktbuch wird, wenn ich anfange WhatsApp zu benutzen, wird an Google gesandt, zum Beispiel. Und dann auch jede Kommunikation, die ich mache, das landet alles in den Facebook-Datenbanken, natürlich. Also wann ich mit wem, wie viel, vor allem auch in Kontakt stehe, darüber können sie zu Sozialgraphen machen. Die können sehen, in was für Gemeinschaften bin ich? Bin ich zum Beispiel in einem Fußballverein oder so. Da kann man weitere Schlüsse draus ziehen, aus solchen Metadaten. Und das bedeutet, auch wenn eine App Ende-Ende-Verschlüsselung macht, was schon mal, würde ich sagen, bei einem Messenger das Must-Have-Feature ist, dann gibt's immer noch diese Metadaten, die fallen trotzdem an. Und das heißt, es muss trotzdem meinem Anbieter in irgendeiner Art und Weise vertrauen können. Und da kommt eben wieder rein, dass Signal eben auf der Ebene alles richtig macht, würde ich sagen. Also da gibt's natürlich noch andere Messenger, Threema oder Telegram.

Karina Filusch: Ja, Threema ist ja mein Liebling. Wir haben in der Vorbereitung ein bisschen darüber geschrieben und ich habe Marius ganz stolz in der E-Mail geschrieben, hast du schon gesehen, dass seit Dezember Threema Open Source ist? Und dann kam die Ernüchterung, denn Open Source ist nicht Open Source, nicht wahr?

Marius Melzer: Also Open Source ist Open Source, aber es ist leider nur die App Open Source, das heißt, man kann da immerhin reingucken und weiß, dass die Verschlüsselung irgendwie was Ordentliches macht. Das ist schon mal schön, aber der Server-Code ist nicht Open Source, das heißt, ich weiß zum Beispiel nicht, was sie mit den Metadaten machen, auch wenn es gut ist, dass die natürlich in der EU angesiedelt sind und damit mindestens unter die DSGVO erst einmal selbst fallen als Anbietern. Es ist trotzdem so, dass sie eine Firma sind und natürlich auch, dadurch würde ich sagen, ein bisschen angreifbarer sind als die Signal-Foundation. Aber zumindest durch diesen Schritt, dass mindestens die App schon mal Open Source ist, würde ich sagen es ist jetzt eine App, die man auch durchaus benutzen kann. Was meiner Meinung nach im Gegensatz zu Telegram steht, was ja viele als sicher ansehen.

Karina Filusch: Ja, da gibt's viel in Social-Media so an Posts gerade „Nehmt Telegram statt WhatsApp“ ganz viel kursiert das gerade rum.

Marius Melzer: Genau, das ist leider Quatsch. Ich würde sagen, das Hauptproblem ist, dass sie die Gruppen nicht verschlüsseln, das heißt, alle Kommunikation darüber ist komplett ungesichert, das heißt, dass es ist im Zweifel sogar schlechter als WhatsApp, würde ich sagen.

Karina Filusch: Wow.

Marius Melzer: Und, dass wir relativ viele Daten, wenn man eben nicht diese konkret verschlüsselten Verbindungen macht, die man ja sogar auswählen muss „geheimer Chat“ oder sowas. Dann laden sie halt auch so den gesamten Chatverlauf zu sich hoch. Klar, das ist sicherlich auch ein Feature, das wir wollen, wenn jemand Telegram woanders installiert, dass man die Daten wieder da hat sozusagen. Aber es ist auf jeden Fall einen

Datenschutz-Anti-Feature. Und dazu kommt noch also, dass es unter anderem gegründet wurde von dem russischen Kontakte-Gründer, also von diesem russischen Facebook sozusagen. Die sind zwar aus Russland weg gegangen, Telegram, um da sozusagen keine offensichtlichen Verzweigungen zu haben, aber es ist trotzdem so, dass ich jetzt per se erst einmal dieser Stiftung Signal sehr viel mehr vertrauen würde als einer Firma, die von jemandem, der das russische Facebook gemacht hat.

Karina Filusch: Vor allem weil die ja noch Server dort in Russland stehen haben, laut Website.

Marius Melzer: Also von daher. Ich denke mittlerweile, jetzt wo die App Open Source ist kann man Threema durchaus nutzen. Telegram sollte man nicht nutzen. Mein Tipp wäre, Signal zu nutzen. Noch cooler wäre es natürlich, wenn es eine dezentrale Lösung gäbe, die jeder auch selbst betreiben kann. Da gibt es dieses Element, was man vielleicht schon mal gehört haben könnte…

Karina Filusch: Ja.

Marius Melzer: …wenigstens mal mit nennen. Ich schätze mal in der Zukunft, wenn sich nochmal Änderungen ergeben, welche Messenger wir benutzen. Und wer weiß, ob Signal so positiv bleibt, wie es das jetzt gerade scheint. Dann ist das auf jeden Fall eine Alternative. Das ist einfach eine Open Source Software, die ich auch selbst betreiben kann, wo meine Schule das betreiben kann oder mein Verein das betreiben kann, so miteinander verbinden kann.

Karina Filusch: Da kann man mal sehen, was im Internet eigentlich so für Quatsch kursiert. Ich habe auf Social-Media so oft gelesen, dass Telegram angeblich eine gute Alternative für WhatsApp sein soll

Aileen Weibeler: Ja, ich habe auch schon versucht mich nach Alternativen umzuschauen, aber um ehrlich zu sein war mir das etwas zu komplex, weshalb ich echt froh bin, dass wir jetzt einen Experten dahatten. Mit dem wir außerdem über sichere Passwörter gesprochen haben. Das findet ihr aber nicht in dieser Folge.

Karina Filusch: Ja genau, wir haben euch das als super mega special Material aufbereitet mit Schritt für Schritt Anleitungen, also falls ihr Lust habt euch da noch mit zu beschäftigen hört da doch mal rein.

Aileen Weibeler: In der nächsten Folge geht es dann um die beliebten Sprachassistenten wie Siri und Alexa und was die im Alltag vielleicht an der ein oder anderen Stelle so aufschnappen.

Karina Filusch: DaSou ist eine Produktion der Kanzlei Filusch. Mehr Infos findet ihr auf unserer Website www.dasou.law. Der Jingle wurde komponiert von Mauli, die Idee zu DaSou hatte Axel Jürs, das Cover hat Hélène Baum erstellt, beraten wurden wir von Susan Stone.

Aileen Weibeler: Falls ihr Fragen zu DaSou habt, schickt uns eine Mail an hallo@dasou.law oder einfach eine Twitter-Nachricht.

Karina Filusch: Danke fürs Zuhören. Bis zum nächsten Mal!

Aileen Weibeler: Bis nächstes Mal!