Alptraum Handy-Wanze

Smartphone-Spionage-Apps als Stalker-Werkzeuge

Sie sind die Erfüllung der Träume von eifersüchtigen (Ex-)Partnern oder Stalkern: Komplett-Sets aus Handy-Spyware und Cloudservice ermöglichen es, Standortdaten, Chat-Verläufe, Fotos, Gespräche und vieles mehr in Echtzeit zu überwachen. Der Einsatz von FlexiSpy, mSpy und Co. ist verboten, doch das schert viele Kunden nicht.

Von Holger Bleich

Wenn Eifersucht im Spiel ist, schieben misstrauische Partner mitunter alle moralischen Bedenken beiseite. Dann werden Schubladen durchwühlt, Freunde heimlich befragt oder gar Detektive engagiert. Steht die ungeteilte Zuneigung in Frage, führt der Argwohn dazu, dass der legitime Anspruch der oder des Liebsten auf Privatsphäre mit Füßen getreten wird. Niedere Instinke verdrängen die Vernunft.

Genau auf diese Instinkte setzen dubiose Anbieter von Spionage-Apps für Smartphones, und das offenbar sehr erfolgreich: „Wenn Sie in einer festen Beziehung sind, haben Sie ein Recht zu wissen!“ So wirbt der thailändische App-Hersteller Vervata für sein bedienungsfreundliches Handy-Trojaner-Set FlexiSpy. Nachdem man knapp 200 US-Dollar überwiesen hat, kann man drei Monate lang „lautlos alle Unterhaltungen, Standorte, und Nutzerverhalten eines Smartphones von sämtlichen Webbrowsern aus“ überwachen, lockt Vervata auf seiner Homepage.

Offensichtlich lockt er auch hierzulande erfolgreich: Geleakte Kundendaten aus diesem und dem vergangenen Jahr zeigten, dass Vervata allein in Deutschland über 1000 zahlende Kunden hat. Das Online-Magazin Vice bekam diese Daten in die Finger. Man habe unter anderem „Rechtsanwälte, Firmengründer, Mitarbeiter von Reinigungsfirmen, Sicherheitsunternehmen, Party-Veranstalter, Friseurinnen und Internisten“, gefunden, berichtete Vice. Die Mehrzahl der Kunden seien Männer, doch immerhin mehr als ein Drittel seien Frauen.

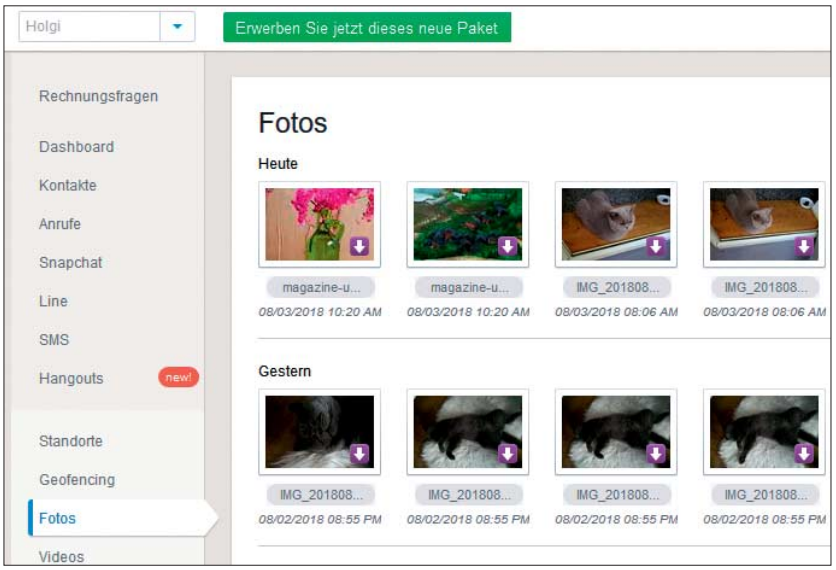
Diese Zahlen mögen nicht allzu hoch erscheinen. Bedenkt man aber, dass hinter jedem einzelnen Account eines oder gar mehrere Schicksale von Personen stehen, deren Privat- und vielleicht auch Intimsphäre über eine Handy-Wanze ausspioniert werden, lässt das erschaudern. Hinzu kommt, dass das Urgestein FlexiSpy mittlerweile zig Mitbewerber hat, die ebenso um die Gunst von eifersüchtigen Ehepartnern, Stalkern, übersorgenden Eltern oder kontrollsüchtigen Arbeitgebern buhlen. Der populärste davon ist mSpy des US-amerikanischen Herstellers My Spy, der mindestens eine ähnlich große Kundenzahl wie Vervata haben dürfte und mit lediglich 100 Euro pro drei Monaten vergleichsweise günstig daherkommt.

Der Funktionsumfang beider Trojaner-Services unterscheidet sich nicht erheblich. Beide bieten nur bei gerooteten Android-Smartphones vollen Remote-Zugriff. Die versteckte Installation auf nicht gerooteten Android-Geräten beschränkt Möglichkeiten und erleichtert Opfern das Aufspüren der Spionage-App (siehe S. 84). Vervata unterstützt iOS 11, allerdings wegen der restriktiven Rechte auf Apple-Geräten nur mit Jailbreak. My Spy bietet dagegen mSpy auch für aktuelle iOS-Versionen ohne Jailbreak an.

Wege aufs Handy

Die Anmeldung und Bezahlung bei den Services klappt problemlos, sofern man der englischen Sprache mächtig ist: Um hiesige Kunden anzulocken, scheinen alle Werbetexte mittels Translator-Services in radebrechendes Deutsch übersetzt worden zu sein, an vielen Stellen haben Vervata und My Spy ganz drauf verzichtet. Die Spyware-Lizenzen gestatten es lediglich, ein einziges Gerät zu verwanzen. Möchte der Stalker ein zweites Gerät anmelden, muss er das bisherige abmelden oder eine zweite Lizenz erwerben.

Die Spionage-Software landet je nach Betriebssystem auf unterschiedlichen Wegen auf dem Handy. Bei ungerooteten Android-Versionen etwa installiert man das APK-Paket entweder via USB oder über den Download mit dem Browser. Erforderlich ist auf jeden Fall der physische, entsperrte Zugang zum Gerät. Die Anbieter erläutern mit Schritt-für-Schritt-Anleitungen, welche Sicherheitsbarrieren und Stealth-Modi aktiviert werden müssen, damit die App nicht sofort vom Betriebssystem entdeckt wird. mSpy nutzt auf iPhones ohne Jailbreak zur Datenausleitung das iCloud-Backup. Der Möchtegern-Spion muss also die



Das mSpy-Panel zeigt, wie gerne der überwachte Autor dieses Artikels seine Katzen knipst.

Illegale Überwachung

Von Joerg Heidrich

Vom Einsatz versteckter Überwachungs-Apps sollte man unbedingt die Finger lassen. Nur in ganz wenigen Fällen kann man sie überhaupt legal einsetzen. Eine ganze Reihe von Strafvorschriften stehen der Handy-Spionage entgegen. Zudem kann die Verletzung des Persönlichkeitsrechts zusätzlich auch Unterlassungs- und in besonders schwerwiegenden Fällen auch Schmerzensgeldansprüche nach sich ziehen. Darüber hinaus ist das Erfassen, Speichern oder die Weitergabe fremder Daten – dazu zählen auch Fotos von Personen – ohne Zustimmung des Betroffenen ein Verstoß gegen geltendes Datenschutzrecht.

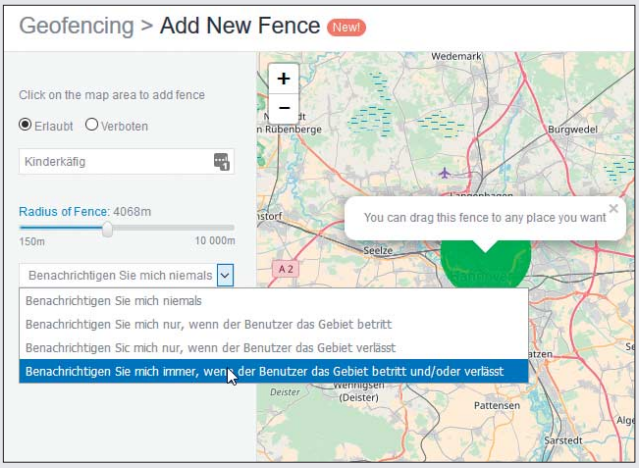
Mehrere Bestimmungen im Strafgesetzbuch (StGB) schützen die Vertraulichkeit von Wort, Foto- und Filmaufnahmen oder Daten. Paragraf 201 StGB sieht eine Freiheitsstrafe von bis zu drei Jahren oder eine Geldstrafe vor, wenn eine Person „unbefugt das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt“. Strafbar ist also jede Aufzeichnung eines Gesprächs und natürlich auch Telefonats ohne Kenntnis und Zustimmung *aller* beteiligten Personen.

Relevant sind auch die Paragrafen 202a StGB („Ausspähen von Daten“), und 202b StGB („Abfangen von Daten“). Diese schützen Informationen vor unbefugtem Zugriff entweder durch das Überwinden eines Zugangsschutzes oder auf dem Transportweg. Darunter fällt, dass fremde Handys ausspioniert werden, falls es etwa um E-Mails, WhatsApp-Nachrichten, Kontakte oder Gesprächsinformationen geht. Nach Paragraf 202c StGB beginnt die Strafbarkeit schon mit dem Kauf oder der Miete einer Spionage-App. Dies gilt dann, wenn man sich oder anderen eine Software verschafft, deren Zweck Ausspähen und Abfangen von Daten ist. Strafbar machen sich in vielen Fällen auch die Anbieter von Spionage-Apps.

Eltern

Eltern kann es erlaubt sein, eine Spionage-App auf dem Smartphone des Kindes zu platzieren, denn Eltern verfügen über eine Befugnis, in die Privatsphäre ihrer Kinder einzugreifen. Dies ergibt sich aus den Paragrafen 1626 und 1631 des Bürgerlichen Gesetzbuchs (BGB) („Elterliche Sorgfaltspflicht“). Die Internetnutzung oder den Aufenthaltsort eines Zehnjährigen ohne dessen Kenntnis mit einer Spionage-App zu kontrollieren dürfte daher rechtmäßig sein.

Allerdings sehen diese Vorschriften auch vor, dass die Eltern die „wachsende Fähigkeit und das wachsende Bedürfnis des Kindes zu selbständigem verantwortungsbewusstem Handeln“ zu berücksichtigen haben. Hieraus ergibt sich auch ein mit dem Alter wachsendes Recht des Nachwuchses auf Privatsphäre. Laut EU-Datenschutz-Grundverordnung (DSGVO) etwa ist ein Jugendlicher ab 16 in der Lage, selbständig in die Verarbeitung seiner Daten einzuwilligen. Bei der Handy-Überwachung kann die Altersgrenze darunter liegen – je nach Entwicklungsstands des Kindes. Ohnehin umfasst die elterliche Sorge nur Belange des eigenen Kindes. Sobald von der Lauschaktion Dritte involviert sind, ist die Grenze der Strafbarkeit bereits erreicht – also etwa beim heimlichen Abhören eines Telefonats mit den Großeltern.



Mit mSpy kann man den Bewegungsradius der Zielperson mit Geofencing überwachen.

Stalking

Unzulässig ist es, via Spionage-App den Lebenspartner ohne dessen Einverständnis zu überwachen. Neben den bereits benannten Paragrafen zum Lauschen, Filmen oder Auslesen von Daten dürfte auch der relativ neue Paragraf 238 StGB einschlägig sein. Er stellt „Nachstellen“ unter Strafe – Stalking also. Danach handelt derjenige strafbar, der einer anderen Person „in einer Weise unbefugt nachstellt, die geeignet ist, deren Lebensgestaltung schwerwiegend zu beeinträchtigen“. Dazu zählt unter anderem die beharrliche Verwendung von Telekommunikationsmitteln oder sonstigen Mitteln der Kommunikation.

So wurde Ende 2015 ein 20-Jähriger verurteilt, der seine Ex-Freundin per Handy-App überwacht und unter anderem ihre SMS und WhatsApp-Mitteilungen mitgelesen hatte. Nur der Tatsache, dass der Hobby-Spion noch nach Jugendstrafrecht verurteilt wurde und er geständig war, dürfte er es zu verdanken haben, dass die vom Amtsgericht Heilbronn ausgesprochene Strafe bei lediglich 30 Arbeitsstunden lag.

Arbeitsplatz

Nicht nur Unternehmen mit einer ausgeprägten amerikanischen Arbeitsethik neigen dazu, die eigenen Mitarbeiter intensiv überwachen zu wollen. Eine verdeckte Überwachung ist aber allenfalls in extremen Ausnahmefällen möglich, etwa im Rahmen von Videoüberwachung wegen eines konkreten Strafverdachts. In einzelnen Jobs, etwa bei Gefahrguttransporten, ist es außerdem erlaubt, die Mitarbeiter räumlich zu orten.

Für eine versteckte Überwachung des Dienst-Handys ist kein legal möglicher Einsatz erkennbar. Nicht einmal eine offene, dauerhafte Überwachung dürfte im Arbeitsverhältnis zulässig sein. Denn dafür ist eine Einwilligung des Arbeitnehmers erforderlich, die freiwillig sein muss. Zumindest bei einer Vollüberwachung ist es jedoch mehr als fragwürdig, ob diese Freiwilligkeit jemals vorliegen kann. Zudem müsste auch ein vorhandener Betriebsrat zustimmen.

Apple-ID und das Passwort des Opfers kennen und iCloud-Backup heimlich aktivieren.

Anything goes

Ist die Spionage-App installiert und über ein Kennwort mit dem Dienst vernetzt, beginnt sie, Daten abzugreifen und laufend in die Cloud zu pumpen. Zu FlexiSpy und mSpy gehören komfortable Web-Dashboards, die diese Daten aufbereiten. Die Standorte etwa stellen beide Anbieter als Bewegungshistorie auf einer zoombaren Open-Streetmap-Karte dar. Über Geofencing-Funktionen lassen sich Gebiete festlegen. Verlässt oder betritt das Opfer den definierten Radius, alarmiert der Dienst seinen Kunden.

Zu den Basisdaten, die von jedem Smartphone ausgelesen werden können, zählen außerdem aufgenommene Töne, Bilder und Videos, Kontakt- und SMS-Datenbanken, die Anrufhistorie mit ein- und ausgehenden Nummern, Daten aus der Kalender-App sowie Browser-Verläufe und Bookmarks. Haben die Trojaner Root-Rechte, können sie aber wesentlich mehr. Dann leiten sie in Echtzeit Chat-Verläufe von Messengern wie WhatsApp, Facebook, Instagram, Snapchat oder Tinder aus. FlexiSpy schneidet auch VoIP-Calls über Skype, Facebook, Whatsapp und anderen Clients mit. Beide Apps verfügen über einen Keylogger. Wird er aktiviert, ersetzen sie die Standard-Tastatur durch ihre eigene, die jeden Tastenanschlag mitschneidet.

FlexiSpy enthält in der teureren „Extreme-Edition“ außerdem die ultimative Wanzen-Funktion: Im Frontend kann man über die Option „Live Listening“ eine Mobilnummer für ein „Monitor-Gerät“angeben. Telefoniert das Spyware-Opfer, bekommt der „Monitor“ ein Signal und kann das Gespräch am eigenen Handy unbemerkt mitverfolgen. Außerdem kann er mit einem stillen Anruf das Mikrofon des Opfer-Smartphones aktivieren und live die Umgebung abhören.

Kaum Unrechtsbewusstsein

Der Einsatz all dieser Funktionen ist in Deutschland streng verboten, sofern die Zielperson nichts davon weiß und in die Spionage nicht ausdrücklich eingewilligt hat (siehe Kasten „Illegale Überwachung“). Die dubiosen Anbieter schwurbeln in ihren Beschreibungen gekonnt um den heißen Brei herum. Meist ist verharmlosend von „Kinderschutz-Funktionen“ oder „Mitarbeiter-Kontrolle“ die Rede. Erst im Kleingedruckten, bei FlexiSpy etwa in einer verlinkten „Legalen Verzichtserklärung“ [sic], erfährt der Kunde, dass sich die Firma von jeder Verantwortung für eine illegale Nutzung der Spionage-App freispricht – was rechtlich kaum zu halten ist.

Aus den Support-Foren zu den Apps wird deutlich, dass kaum jemand diese Spionage-Toolsets zu legalen Zwecken einsetzt. Das Online-Magazin Vice hat sich die Mühe gemacht, viele der im bereits erwähnten FlexiSpy-Datenbank-Leak gefundenen Kunden anzuschreiben und nach ihren Motiven zu fragen. Das Magazin veröffentlichte einzigartige Einblicke in die Abgründe von Stalker-Seelen, deren feuchte Träume mit FlexiSpy und Co. in Erfüllung gingen.

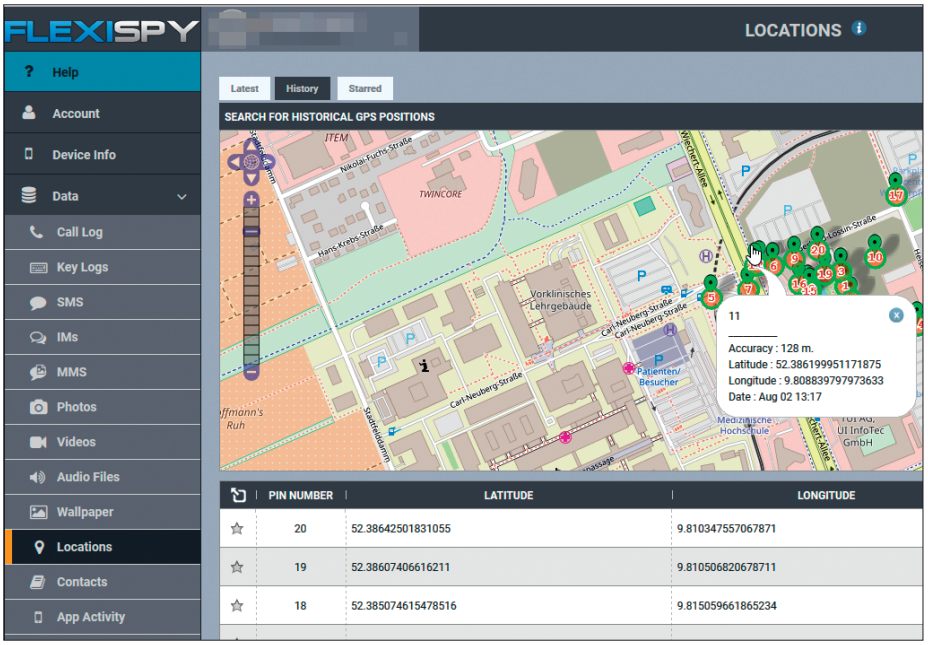
Zum Beispiel Alex (Name von Vice geändert). Er habe seine Frau knapp drei Monate ausspioniert und ganze Tage damit verbracht, das aufgezeichnete Material zu sichten. Und er fühle sich auch heute noch im Recht, weil er herausfand, dass seine Frau ihn betrog: „Manche bringen sich dann vielleicht um oder knallen ihre Familie ab. Ich habe die Scheidung eingereicht“, zitierte Vice. Laut Vice herrsche bei den Nutzern der App kaum ein Unrechtsbewusstsein. „Ist doch normal, ein Mann will eben manchmal einfach wissen, was seine Frau macht“, gab einer zu Protokoll.

Prophylaxe

In der Öffentlichkeit hört man wenig zu dem Thema. Eine stichprobenhafte Nachfrage von c’t bei den zuständigen Landeskriminalämtern von Niedersachsen und Berlin ergab, dass es in den vergangenen Jahren kaum Ermittlungsverfahren wegen des strafbaren Einsatzes von Spionage-Apps gab, geschweige denn Strafprozesse. Vieles spricht allerdings für eine hohe Dunkelziffer (siehe Interview „Krankhaft eifersüchtige Partner“).

Geschädigte haben ein doppeltes Nachweisproblem: Zeigen sie die Straftat an, müssen sie ihr Smartphone inklusive aller privaten Daten zur forensischen Analyse der Polizei aushändigen. Selbst wenn die Ermittler die Spionage-App finden, gilt es, dem mutmaßlichen Täter die Überwachung nachzuweisen. Ohne Hausdurchsuchung und Analyse seiner Geräte dürfte das schwer gelingen – doch für solche Maßnahmen liegt die juristische Schwelle hoch, was auch die Opfer wissen. Weil sie dieses Procedere mit ungewissem Ausgang meiden – oder schlicht aus Scham oder Furcht vor Racheaktionen –, dürften viele Geschädigte auf den Gang zur Polizei verzichten.

Am besten also, man beugt der Smartphone-Spionage vor. Dazu gehört, alle Geräte mit einem sicheren Zugangsschutz zu versehen. PINs und Passwörter müssen geheim bleiben, auch vor dem Ehepartner. Fingerabdruck-Sicherung bie-



Im Dashboard von FlexySpy lässt sich die Standorthistorie des überwachten Handys nachverfolgen.

„Krankhaft eifersüchtige Partner“

Im Interview betont die ehemalige Kriminalkommissarin Sandra Cegla, dass Handy-Spionage auch gefestigte Menschen massiv erschüttern kann.

Foto: Frauke Brenne/Brennweite

Sandra Cegla berät Stalking-Opfer.

Sandra Cegla war 14 Jahre lang bei der Berliner Polizei beschäftigt, unter anderem als Kriminalkommissarin. In Kreuzberg und Neukölln habe sie „tiefe gesellschaftliche Einblicke erhalten“ und sich „acht Jahre lang auf die Schwerpunkte Stalking und Intimpartnergewalt spezialisiert“, erklärt sie selbst. 2015 gründete sie SOS-Stalking, eine kommerzielle „Sicherheitsagentur“, die Stalking-Opfer berät und unterstützen soll.

c’t: Können Sie aus Ihrer Beraterpraxis abschätzen, wer Spionage-Apps in welchem Umfeld nutzt?

Sandra Cegla: Im Zusammenhang mit dem Phänomen Stalking wird Spyware unserer Erfahrung nach häufig im häuslichen Umfeld eingesetzt. Wir beobachten dabei krankhaft eifersüchtige Partner, die schon während der Partnerschaft eine Spyware auf dem Handy ihrer Partnerin installiert haben oder ihr sogar ein Handy mit bereits vorinstallierter Spyware geschenkt haben. Dieser Kontrollzwang scheint besonders bei Männern ausgeprägt zu sein, denn eine weibliche Täterin, die Spyware verwendet hat, ist bei uns noch nicht vorgekommen.

Allerdings kommt die Verwendung von Spyware auch im beruflichen Kontext vor. In unseren Fällen gibt es auch hier immer einen Stalking-Hintergrund, also Ablehnung und Kränkung. Das kann der Chef gegenüber einer Mitarbeiterin sein, ein Kollege gegenüber einer Kollegin oder ein ehemaliger Mitarbeiter gegenüber dem Chef. Es ist allerdings auch denkbar, dass Spyware unter Konkurrenten in der Wirtschaft eingesetzt wird.

c’t: Können Sie ein konkretes Beispiel aus dem privaten Umfeld nennen?

Cegla: Ja, wir hatten etwa einen Fall, in dem einer jungen Frau innerhalb ihrer Partnerschaft eine Spyware auf dem Handy installiert wurde. Durch eine Äußerung, die sie gegenüber einem Freund in einem persönlichen Gespräch getätigt hatte, war ihr Partner so gekränkt, dass wenige Minuten später am Telefon daraus ein heftiger Streit entstand. Hier wurde ihr deutlich, dass er Insiderwissen hatte, das er wirklich nicht hätte haben können.

Wie sich herausstellte, hat er also nicht nur alle ihre Telefonate mitgehört, ihre Chatverläufe und sonstige Korrespondenz gelesen, sondern auch Gespräche im Raum direkt mitgehört. Ohne es zu wissen, trug sie über mehrere Wochen eine Wanze mit sich herum. In einer späteren Konfrontation gab er zu, die Spyware installiert zu haben. Das verursachte eine massive seelische Erschütterung bei unserer Klientin, die ich als taff und bodenständig erlebt habe.

c’t: Warum gibt es so wenig Strafverfolgung in diesem Deliktbereich?

Cegla: Die Gründe, warum der Einsatz von Spyware nur selten angezeigt und der Strafverfolgung zugeführt wird, kann ich nur vermuten. Man muss verstehen, dass der Einsatz von Spyware in unseren Fällen sehr häufig aus einem komplexen, meist gestörten Beziehungsgeflecht hervorgeht. Da spielen Abhängigkeiten, Schuld und Scham eine Rolle. Die Betroffenen suchen oft viele Jahre die Schuld für das destruktive Verhalten des Täters bei sich selbst. Sehr häufig sind alle Spuren schon verwischt, wenn die Spyware auffliegt. Der Täter hat schließlich alles mitgehört. Und der Weg zur Polizei ist ein schwerer. Ich persönlich weiß, dass es gute und engagierte Polizisten gibt, die gute Arbeit leisten. Unsere Klientinnen berichten jedoch immer wieder davon, dass sie sich von der Polizei nicht ernst genommen fühlen.

Ein weiterer wesentlicher Punkt, warum den Behörden die Taten gar nicht erst bekannt werden, ist, dass gerade im Bereich der Beziehungstaten, die auch Sexualdelikte einschließen, die Dunkelziffer sehr hoch ist. In diesen Fällen haben die Frauen oft eine derart lange Leidensgeschichte hinter sich, dass sie dem Druck eines Strafverfahrens nicht standhalten können. Auch hier bleiben weitere Fälle im Verborgenen, in denen mit Spyware gearbeitet wurde. Insgesamt habe ich jedoch den Eindruck, dass die Fälle, in denen Spyware vermutet wird, erheblich höher ist als die Zahl von Fällen, in denen Spyware tatsächlich verwendet wurde.

tet wohl den besten Schutz, Wischgesten den miesesten – sie können abgeschaut oder mitgefilmt werden. Wo immer möglich sollte eine Zwei-Faktor-Authentifizierung aktiviert sein. Das gilt insbesondere für wichtige Services, allen voran die Google-ID (Android) und die Apple-ID (iOS).

In den folgenden Artikeln geben wir Ihnen weitere Grundlagen an die Hand, um Smartphone-Spionage vorzubeugen und wirksam begegnen zu können. Wir erläutern, welche Einfallstore es gibt. Anschließend finden Sie in zwei separaten Artikeln konkrete Anleitungen und Checklisten, wie Sie unter Android und iOS Spyware enttarnen und eliminieren können. Dies gilt natürlich nicht nur fürs eigene Gerät, sondern auch für die Smartphones von Familienmitgliedern oder Bekannten, denen Sie dann hilfreich zur Seite stehen können. *(hob@ct.de)* c't