Alptraum Handy-Wanze: Vorsicht vor diesen Spionage-Apps

c't Sonderheft

c't Android

Der Smartphone-Praxis-Guide

So wird Ihr Smartphone sicher

Checklisten für Android, WhatsApp, Google und Ihre Passwörter

schlank

Dieser Trick entfernt vorinstallierte Apps auch ohne Rooten

schnell

Kaufberatung: Mittelklasse-Handys schlagen Highend-Modelle

Smartphones umziehen

Wie Sie mit Apps und Hersteller-Tools alle Daten auf Ihr neues Handy bringen

Editorial

Liebe Leserin, lieber Leser,

das Smartphone ist Ihr Alltagsbegleiter voller wichtiger und intimer Daten. Wie Sie diese wertvollen Informationen schützen und wie Sie noch mehr aus Ihrem Smartphone herausholen, zeigt Ihnen unsere Auswahl an aktualisierten Android-Artikeln aus der c't.

Falls Sie den Verdacht hegen, dass Sie jemand ausspioniert, erklären wir Ihnen, wie Sie etwaige Spionage-Apps enttarnen und entfernen. Sie erfahren, wo weitere Risiken drohen und wie Sie Ihr Handy samt Google- und WhatsApp-Account absichern – und dass Passwortmanager und Zwei-Faktor-Authentifizierung gar nicht so kompliziert zu bedienen sind, wie es den Anschein hat.

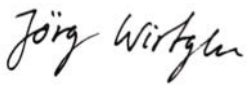
Wir zeigen Ihnen die wichtigsten Einstellungen beim Einrichten eines neuen Smartphones und verraten einen Trick, wie Sie lästige vorinstallierte Bloat-Apps loswerden. Mit unseren Tipps übertragen Sie alle Daten, Fotos, Apps und Einstellungen vom alten aufs neue Handy – naja, fast alle jedenfalls …

Oder können Sie sich noch gar nicht für ein Wunschmodell entscheiden? Wir diskutieren die Vorzüge von High-End-Modellen aus dem Vorjahr, die auf verlockende Preise gefallen sind, und erklären, was hinter Android One steckt. Sie erfahren, welcher Handy-Prozessor wie leistungsfähig ist.

Neues App-Futter: Physik-Apps machen aus dem Handy einen Tricorder, mit OCR-Apps bekommen Sie Ihre Papierflut digitalisiert, RSS-Reader bereiten News auf. Auch für Kinder haben wir Tipps für drinnen und draußen parat.

Wenn Sie in die Programmierung von Apps einsteigen möchten: Eine Übersicht von Crossplattform-Tools zeigt, welche Frameworks Ihnen beim Entwickeln für Android und iOS helfen. Googles Android- und iOS-Framework Flutter widmen wir ein mehrteiliges Tutorial.

Viel Spaß beim Lesen,



Jörg Wirtgen

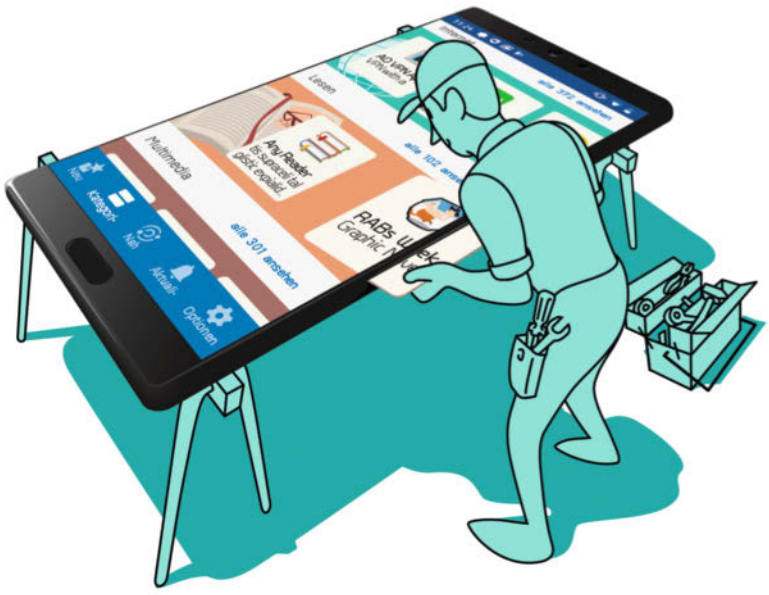
Inhalt

Spionage

Security

Umziehen und einrichten

Smartphones



Apps

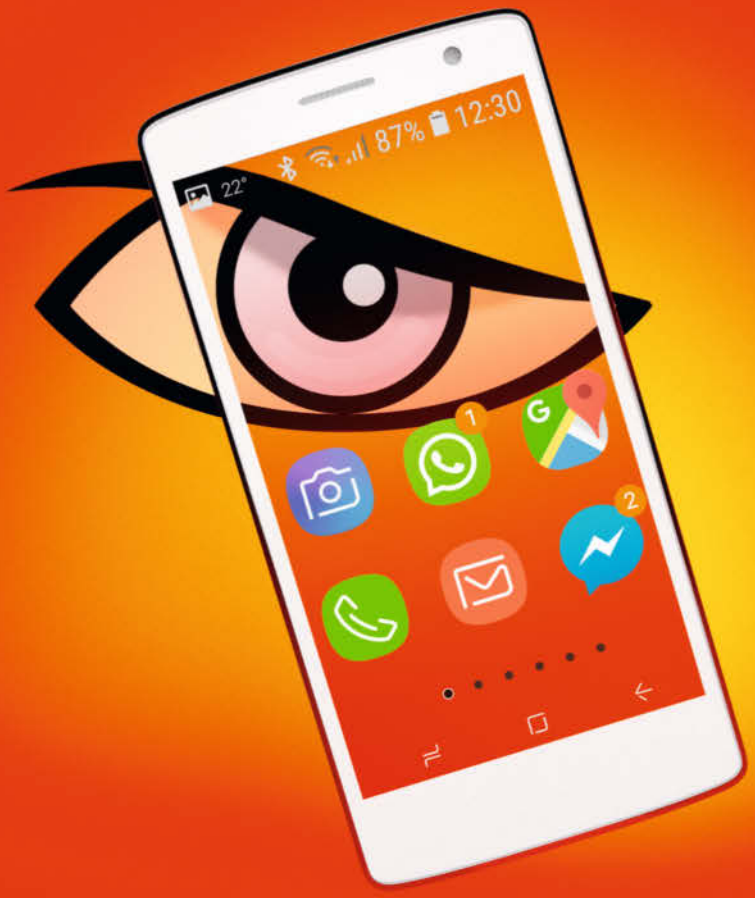
Playstore ohne Google

Programmieren

Zum Heft

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 Instinkte 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 2017 und 2018 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.

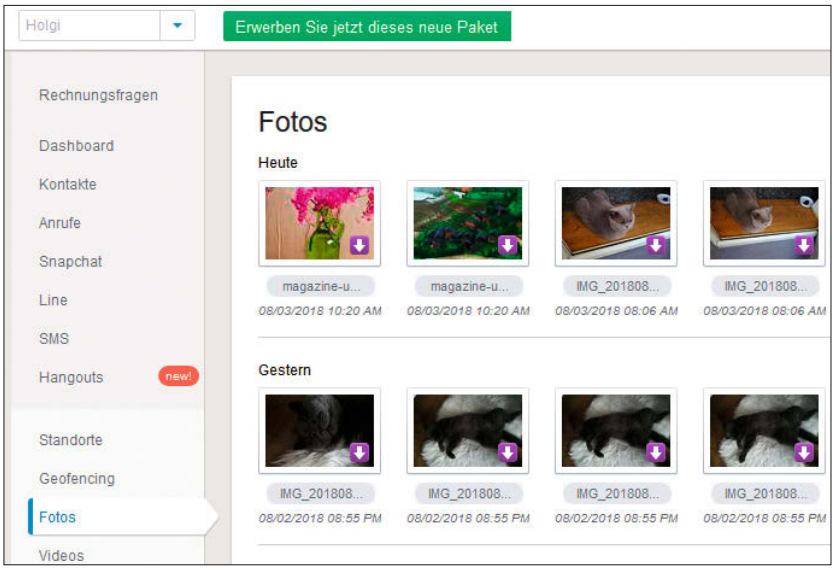
Diese Zahlen mögen nicht allzu hoch erscheinen. Bedenkt man aber, dass hinter jedem einzelnen Account eines oder gar mehrere Schicksale von Personen stehen, deren Privat- und vielleicht auch Intimsphäre über eine Handy-Wanze ausspioniert werden, lässt das erschaudern. Hinzu kommt, dass das Urgestein 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. 14). 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.



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.

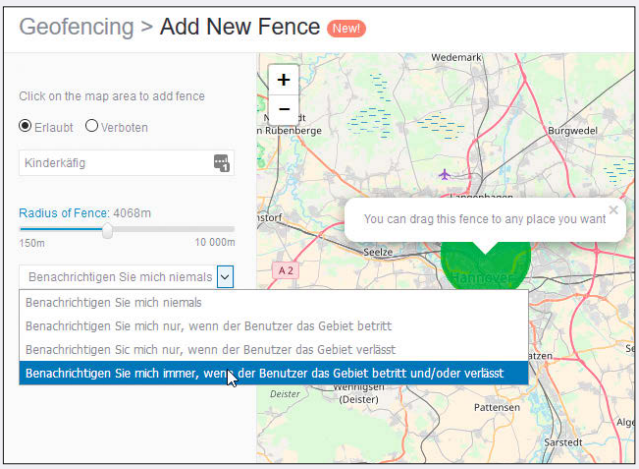
Mehrere Bestimmungen im Strafgesetzbuch (StGB) schützen die Vertraulichkeit von Wort, Foto- und Filmaufnahmen oder Daten. Paragraf 201 StGB sieht eine Freiheitsstrafe von bis zu drei Jahren oder eine Geldstrafe vor, wenn eine Person „unbefugt das nichtöffentlich gesprochene Wort eines anderen auf einen 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 Entwicklungsstand 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.

Der Möchtegern-Spion muss also die 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 andere 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.

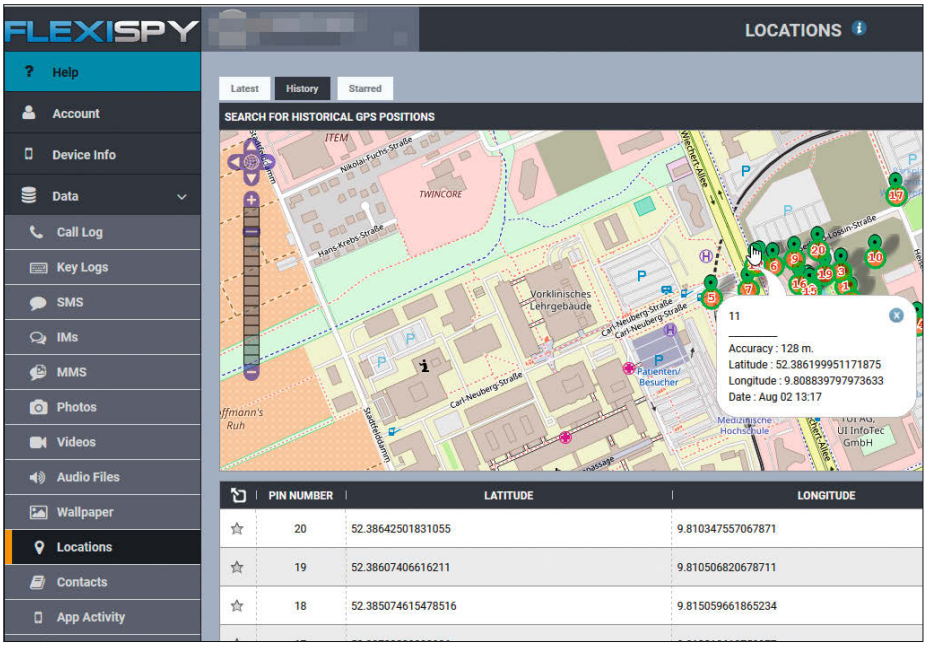
Zum Beispiel Alex (Name von Vice geändert). Er habe seine Frau knapp drei Monate ausspioniert und ganze Tage damit verbracht, das aufgezeichnete Material zu sichten. Und er fühle sich auch heute noch im Recht, weil er herausfand, dass seine Frau ihn betrog: „Manche bringen sich dann vielleicht um oder 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 zunächst, welche Einfallstore es gibt. Anschließend finden Sie eine konkrete Anleitung mit Checkliste, wie Sie unter Android 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

VOICE THEMENFORUM

für IT-Entscheider

VOICE CIO Service GmbH

heise Events

7. März 2019, DB Systel GmbH in Frankfurt

DevOps – Wandel der Firmenkultur meistern

DevOps erfordert einen Wandel in der Firmenkultur. Die Entwicklung vom Expertensilo zu kleinen, autonom arbeitenden agilen Teams erfordert die Überwindung des traditionellen Konflikts zwischen Entwicklung und Betrieb. Beim Aufbau und Management flexibler Microservices-Architekturen erleichtert Automatisierung die Qualitätssicherung und das Testen. Zu einem der wichtigsten Faktoren für den Erfolg zählt aber nicht zuletzt das Vertrauen innerhalb des Teams.

IMPULSVORTRÄGE – INTERAKTIVES ARBEITEN – NETWORKING

Das erwartet Sie:

Das 7. VOICE THEMENFORUM erarbeitet, welche Möglichkeiten DevOps bietet. Wie erreichen Sie eine effektivere und effizientere Zusammenarbeit der Bereiche Entwicklung, IT-Betrieb und Qualitätssicherung? Vertiefen Sie auf diesem Forum auch die Ergebnisse des VOICE ENTSCHEIDERFORUM 2018.

Auszug aus dem Programm:

Impulsvortrag: *„Need for Speed" – warum der Innovationsdruck DevOps unausweichlich macht* // Dr. Martin Strunk, Fachbereichsleiter Individualentwicklung für den Personenverkehr, DB Systel GmbH

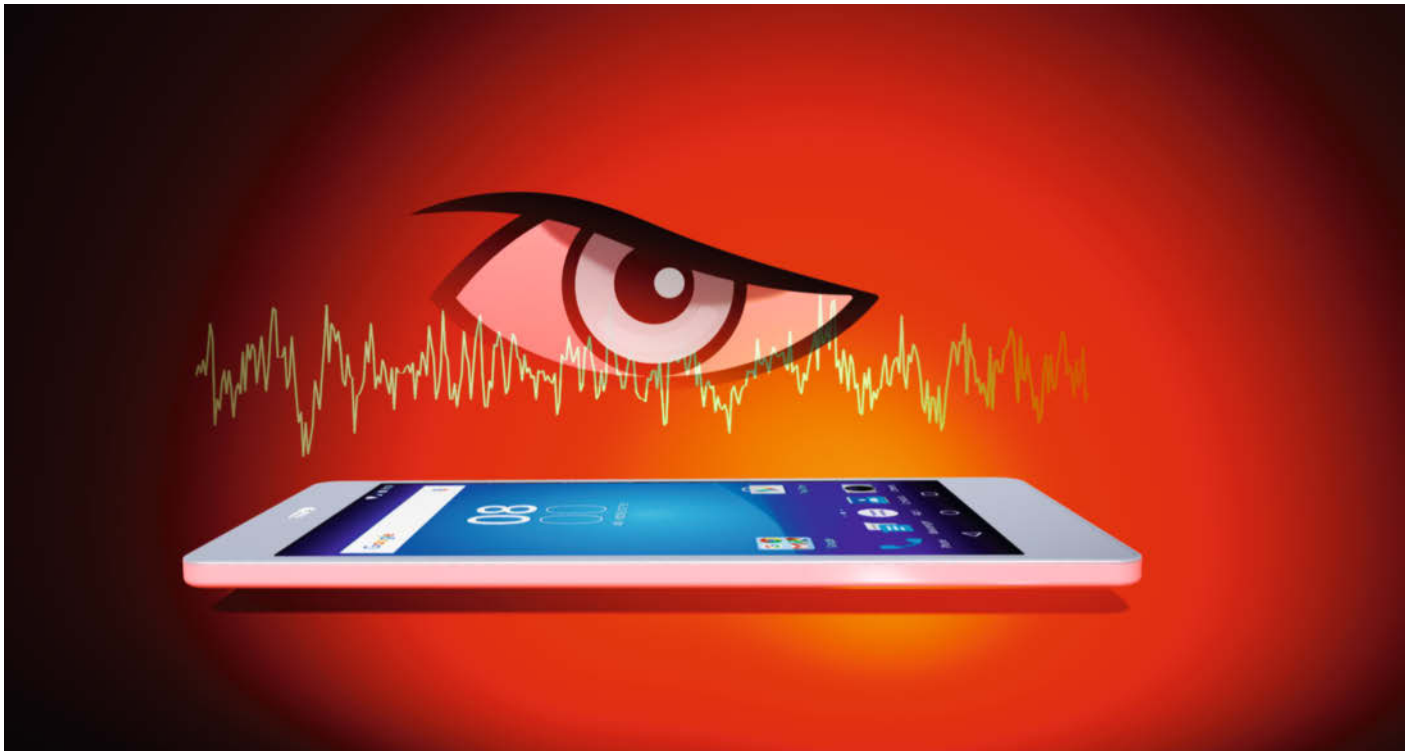
Gastgeber des VOICE THEMENFORUM ist die DB Systel GmbH, die als Anbieter von Informations- und Telekommunikationsdiensten der Deutschen Bahn fungiert.

Teilnahmegebühren: 199,00 Euro (inkl. MwSt.)

Sponsoren: MT AG, redhat.

Weitere Informationen und Anmeldung unter:

www.heise-events.de/voice_themenforum



Spionage entzaubert

So funktioniert Spyware auf Smartphones

Das Ausspionieren von Handys hat nichts Magisches. Spyware ist ganz normale Software – häufig sogar ziemlich schlechte. Wenn man versteht, wie sie arbeitet, kann man sie enttarnen und unschädlich machen.

Von Michael Spreitzenbarth

Damit ein Spionage-Programm Daten einsammeln und verschicken kann, muss es erst mal aufs Handy der Zielperson kommen. Das ist für Strafverfolger, die einen Verdächtigen überwachen wollen, durchaus ein Problem, da sie keinen direkten Zugang zum Smartphone haben. Und wenn sie es in die Hände bekommen, ist das Gerät meist auch noch über eine PIN beziehungsweise andere Sperrmechanismen geschützt. FBI und bald wohl auch das deutsche ZITiS kaufen deshalb schon mal für sechsstellige Summen Exploits ein, mit denen sich diese Hürde nehmen lässt.

Bei kommerziellen Spionage-Apps wie FlexySpy, mSpy und Co übernimmt der eifersüchtige Partner die schmutzige Arbeit: Er installiert den Trojaner in einem unbeobachteten Moment. Den erforderlichen Code hat er entweder, oder er greift sich das Gerät, wenn es gerade entsperrt ist. Selbst Fälle, in denen der Finger des schlafenden Opfers auf den Entsperr-Button gelegt wird, sind schon vorgekommen. Noch einfacher: Er verschenkt ein Gerät, das er vorher in aller Ruhe präpariert hat. Der Rest ist einfach – die Hersteller der Software liefern eine Schritt-für-Schritt-Installations-Anleitung.

Die beschreibt dann unter anderem, welche Sicherheitsmaßnahmen außer Kraft gesetzt werden müssen, damit die Software überhaupt eingespielt werden kann. Auf einem iPhone läuft das auf einen Jailbreak hinaus. Denn mit dem lässt sich auch Software ohne Apples digitale Signatur am offiziellen App Store vorbei einspielen. Bei Android geht das leichter, indem man das Einspielen von Software aus beliebigen Quellen gestattet.

Das ist erforderlich, weil es die kommerzielle Spionage-Software nicht in den offiziellen Stores von Apple und Google gibt. Apple etwa prüft vor der Freigabe, auf welche Daten eine App zugreift, ob das zu den beschriebenen Eigenschaften der App passt und ob dies auch transparent dem Nutzer angezeigt wird. Das entspricht natürlich nicht den Anforderungen von Flexispy und mSpy, die ja gerade heimlich im Hintergrund auf alles zugreifen wollen.

Google hat ähnliche Tests für den Play Store. Selbst aus anderen Quellen installierte Apps kann Google nachträglich löschen, wenn sie sich als bösartig entpuppen. Dieses Feature nennt sich „Google Play Protect“. Dazu scannt das System regelmäßig alle installierten Apps. Findet es dabei bösartige Exemplare, werden diese gelöscht und der Anwender erhält eine Warnung. Auch hier setzen FlexiSpy und Co nicht auf Hightech-Tricks, sondern weisen den Stalker an, diesen Schutz bei der Installation zu deaktivieren.

Im Folgenden will das Spionage-Programm auf alle möglichen Daten des Nutzers zugreifen. Doch Smartphones haben deutlich weitergehende Sicherheitskonzepte als etwa ein Windows-PC. Bei dem

kann jedes einmal aktive Programm im Wesentlichen auf alle Daten des Anwenders zugreifen, sofern diese nicht explizit verschlüsselt sind. E-Mails, Kontakte, Dokumente, Surf-Historie – alles frei zugänglich. Der PC-Spionage-Trojaner kann das einfach einsammeln und übers Netz verschicken.

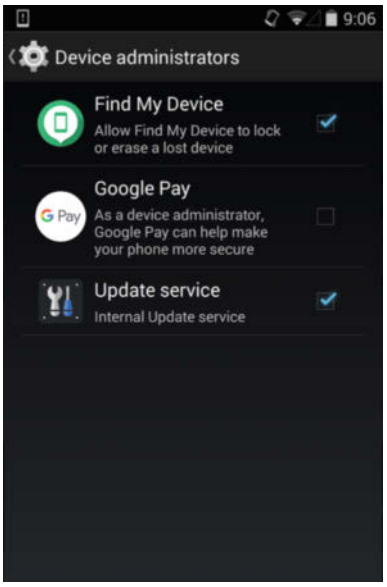
Grenzüberschreitung

Bei den heutigen mobilen Betriebssystemen ist es hingegen gängige Praxis, dass jede App in einer eigenen gesicherten Umgebung läuft – der sogenannten Sandbox. Innerhalb dieser Sandbox kann sie nur über definierte APIs mit dem Betriebssystem selbst sprechen, bleibt aber von anderen Apps oder Prozessen abgeschottet. Hiermit wird gewährleistet, dass die Daten von WhatsApp auch nur von WhatsApp gesehen und bearbeitet werden.

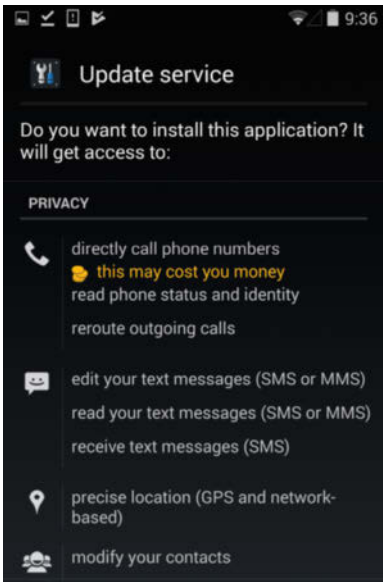
Am einfachsten und gründlichsten umgeht eine Spionage-Software diese Hürden, indem es die Schutzmechanismen des Systems außer Kraft setzt und sich selbst zum absoluten Herrscher aufschwingt. Bei Android-Systemen nennt man das „rooten“, also sich die Rechte des nahezu allmächtigen Root-Accounts zu verschaffen. Bei iOS firmiert das Ausbrechen aus dem Rechte-Gefängnis als „jailbreaken“. Hat der Besitzer das bereits selbst erledigt, hat der Stalker leichtes Spiel. Ansonsten muss er nachhelfen. Gerade auf iOS führt daran kaum ein Weg vorbei, wenn eine andere App etwa auf WhatsApp-Daten zugreifen will.

Zumindest theoretisch gibt es einen weiteren Angriffspunkt: In Firmen werden Geräte in aller Regel über ein zentrales Mobile Device Management (MDM) administriert. Ein solches MDM bietet dann auch Möglichkeiten zur Spionage. Erst kürzlich deckte Cisco Talos einen gezielten Spionage-Angriff in Indien auf, der sich das zunutze machte. Dabei wurden mehrere iPhones einem von Angreifern betriebenen MDM unterstellt und dann von diesem unter anderem mit trojanisierten Versionen von WhatsApp und Telegramm versehen. Für den Einsatz in kommerziellen Tools für einen Massenmarkt eignet sich diese Vorgehensweise jedoch nicht, da mit jedem aufgedeckten Spionagefall die involvierten Zertifikate und MDMs „verbrannt“ sind.

Bei Android gibt es jedoch eine Art „MDM light“, bei der eine App zum Geräteadminstrator ernannt wird. Damit bekommt diese App auch ganz ohne Rooten des Geräts besondere Rechte. Sie kann damit auf Funktionen wie GPS-Ortung, Anrufweiterleitung, Proxy-Einstellungen et cetera zugreifen und diese auch ändern. Des Weiteren kann Spyware dann im Nachgang auch weitere Apps installieren oder löschen. Das nutzen etwa Spionageprogramme von OmniRAT und FlexiSpy, um ihren vollen Funktionsumfang ausschöpfen zu können.



Hinter dem angeblichen „Update service“ verbirgt sich das Spionage-Programm mSpy.



Schon die erste von fünf Seiten zeigt: Der angebliche „Update Service“ will auf alles zugreifen.

Außerdem hat das Sandbox-Konzept gewollte Löcher. Setzte man es strikt um, wäre es schon unmöglich, ein gerade aufgenommenes Foto via WhatsApp an einen Freund zu schicken. Deshalb kann eine App mit zusätzlichen Berechtigungen, die der Entwickler explizit (wie im Fall von Android) oder implizit (wie bei iOS) anfordert, auf bestimmte Daten anderer Apps zugreifen. Diese Rechte muss man sich zwar vom Anwender genehmigen lassen – aber das kann der Stalker auch bei der Installation gleich mit absegnen. Sowohl Android als auch iOS zeigen diese Rechte allerdings auch später noch an.

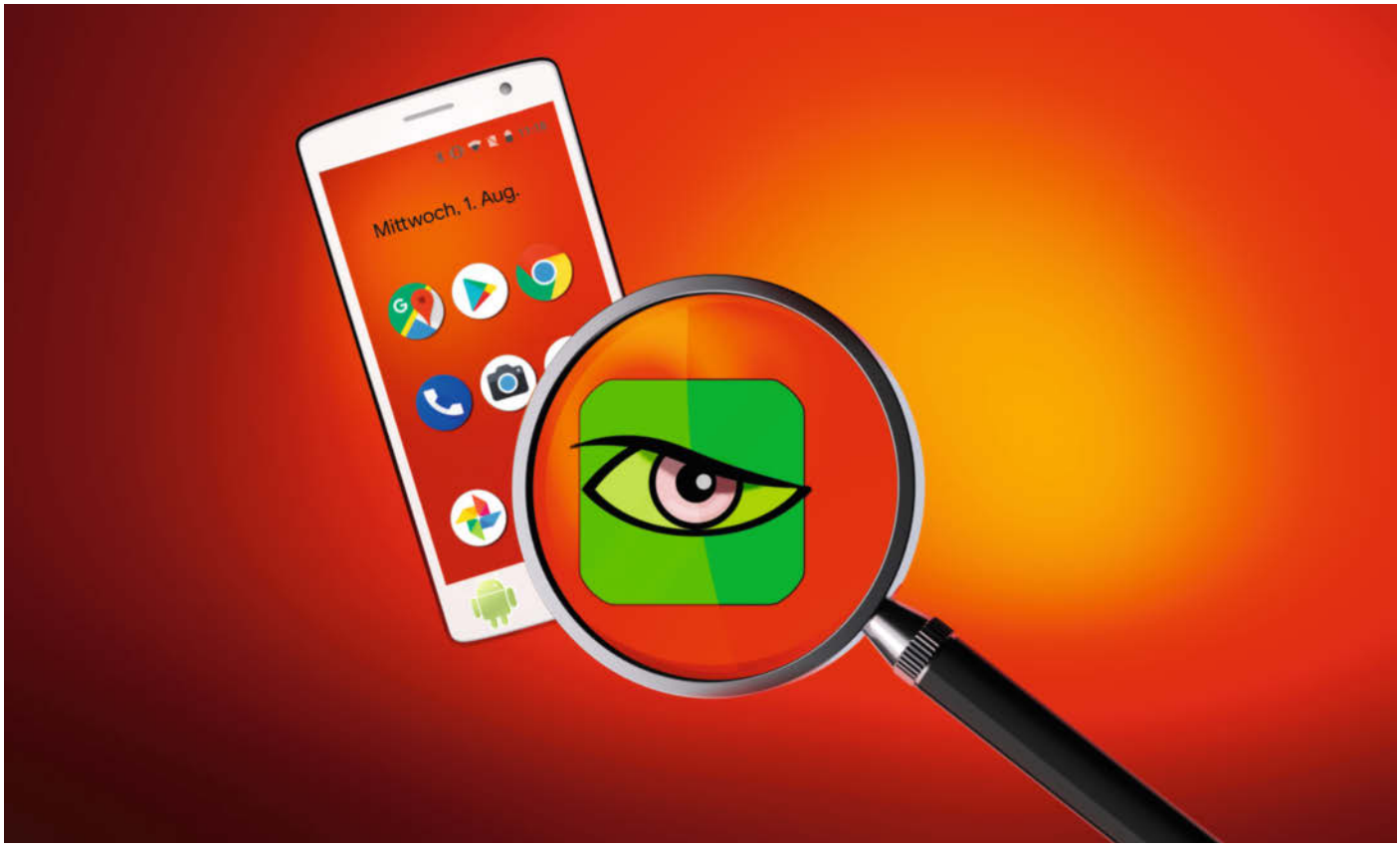
Der Königsweg zur Spionage erfordert gar keine oder minimale Eingriffe in das System. Denn sowohl Android als auch iOS drängen es dem Anwender förmlich auf, ein Backup in der hauseigenen Cloud des Herstellers zu sichern. Ist es auf dem Handy des Opfers ausgeschaltet, kann ein Stalker das Cloud-Backup mit wenigen Handgriffen aktivieren.

Die Backups enthalten dann alle Daten des Geräts und sind mit den Zugangsdaten des Nutzers zugänglich. Ist das Cloud-Passwort bekannt, können sich Spionage-Tools die Daten aus der Cloud herunterladen, die gewünschten Informationen extrahieren und dem Stalker nett aufbereitet präsentieren. Natürlich funktioniert dies nicht wie bei der Spionage auf dem Gerät quasi in Echtzeit. Da die Backups aber in aller Regel täglich aktualisiert werden, gibt es keinen großen zeitlichen Versatz. Diesen Umweg über die iCloud nehmen etwa die iOS-Versionen von FlexiSpy und mSpy, wenn sie ohne Jailbreak auskommen müssen.

Spionage light

Mit den Zugangsdaten zu Accounts kann man auch ganz ohne zusätzliche Tools auf viele Informationen zugreifen. Dienste wie Facebook oder Google Hangouts kann man bequem im Webbrowser mitverfolgen. Und bei fast allen E-Mail-Diensten kann man stille Weiterleitungen von Kopien aller eintreffenden Mails einrichten. Moderne Messenger wie WhatsApp oder Signal kann man mit Desktop-Apps oder einem Browser koppeln, die dann oft über Wochen oder Monate alles mitlesen können. Der Stalker muss dazu nur in einem unbeobachteten Augenblick mit dem Handy einen QR-Code scannen.

Natürlich hinterlassen all diese Aktivitäten Spuren. Wie Sie diese systematisch finden und richtig interpretieren, zeigt Ihnen der folgende Artikel. *(ju@ct.de)* c't



Wurmkur für Androiden

Spionage-Software erkennen und entfernen

Ein Angreifer benötigt Ihr Handy nur für ein paar unbeobachtete Minuten, um darauf eine Spionage-App zu verstecken. Etwas mehr Handgriffe sind vonnöten, um die Infektion zu erkennen und die Überwachung zu stoppen.

Von Michael Spreitzenbarth

Wenn Sie den Verdacht hegen, dass Sie jemand ausspioniert, sollten Sie zuerst überprüfen, ob Ihr Handy gerootet ist. Denn auf einem gerooteten Handy kann ein Angreifer ein Spionagetool so verstecken, dass es mit den hier beschriebenen Methoden nicht zu entdecken ist – auch wenn Sie selbst den Root aus gutem Grund durchgeführt haben [1].

Durchsuchen Sie Ihr Gerät unter „Einstellungen/Apps“ nach Tools, die klassischerweise zum Rooten verwendet werden. Dazu zählen unter anderem SuperSu, BusyBox oder KingRoot. Außerdem überprüfen Sie mit der App Root-Checker direkt, ob Ihr Handy gerootet ist.

Die von uns untersuchten Spionage-Pakete mSpy und FlexiSpy nutzen derzeit zwar keine besonderen Root-Tricks, um sich zu verstecken. Sie werden also von den folgenden Maßnahmen auch auf gerooteten Systemen entfernt. Aber das kann sich mit jedem Update ändern, zudem könnte Ihr Angreifer weitere Schädlinge installiert haben, die sich besser verbergen. Letztlich können Sie einem gerooteten Handy nicht mehr vertrauen.

Hegen Sie auf einem gerooteten Gerät einen konkreten Verdacht, haben Sie zwei Optionen: Zum einen können Sie das Gerät wie weiter unten beschrieben auf die Firmeneinstellungen zurücksetzen, was auch den Root-Zugang entfernt und die Standard-Sicherheitsfunktionen wieder in Kraft setzt. Das Handy ist dann wieder sauber, aber das neue Einrichten des Systems ist mühselig.

Zum anderen können Sie das gerootete System reparieren. Das bedeutet viel Arbeit, doch Sie finden genauer heraus, welche Daten der Angreifer geklaut hat. Es empfiehlt sich, jemanden hinzuzuziehen, der mit gerooteten Systemen Erfahrung hat. Einen Einstieg in die Android-Forensik vermitteln der nachfolgende Artikel und ct.de/w7bc, wir gehen hier nicht weiter darauf ein.

Gerätemanager

Im Folgenden gehen wir davon aus, dass Ihr Gerät nicht gerootet ist und somit alle von Ihnen ermittelten Diagnoseinformationen zuverlässig sind. Zuerst überprüfen Sie die sogenannten Geräteadministrator-Apps, denn sie bekommen unter Android besonders viele Zugriffsrechte. Die finden Sie in den Einstellungen unter „Sicherheit & Standort/Apps zur Geräteverwaltung“, auf manchen Geräten unter

„Gerätesicherheit/Andere Sicherheitseinstellungen“ oder ähnlich.

Hier sollten Sie im Normalfall nur „Mein Gerät finden“ (manchmal „Find My Device“ genannt) und „Google Pay“ sehen und – je nach Einsatzzweck des Telefons – noch das Mobile Device Management Ihrer Firma oder den Eintrag einer Mail-App mit Exchange-Zugang wie „E-Mail“ von Nine. Entdecken Sie an dieser Stelle andere Einträge, so haben Sie ein starkes Indiz für eine Infektion. Deaktivieren Sie die verdächtigen – im Zweifel alle – Geräteadministratoren.

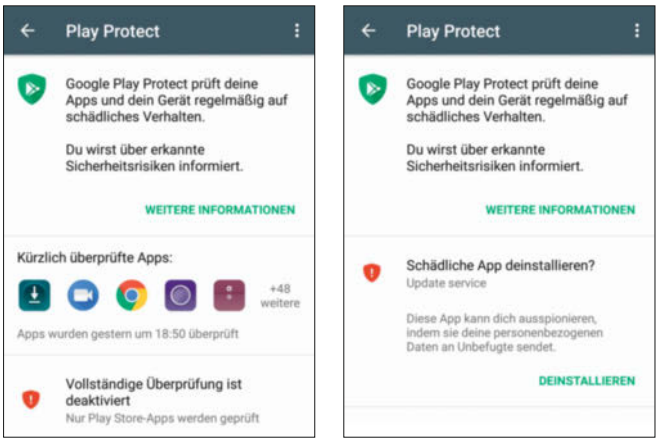
Sie können die Geräteadministratoren hier nur deaktivieren. Zum Löschen müssen Sie die zugehörige App deinstallieren. Doch ärgerlicherweise dürfen Apps ihren Eintrag in dieser Liste der Geräteadministratoren beliebig bezeichnen, sodass Sie nicht immer wissen, von welcher App er stammt. Die Spionagesoftware mSpy trägt sich hier beispielsweise mit „Update Service“ ein, FlexiSpy mit „System Update“. Einige Spionage-Apps verweigern die Deinstallation, solange Sie als Geräteadministrator eingetragen sind.

Play Protect einschalten

Als Nächstes kontrollieren Sie die eingebauten Sicherheits-Features von Android – diese erkennen die meisten Schädlinge nämlich, weswegen Angreifer sie deaktiviert haben dürften. Unter dem Namen Play Protect überprüft Android inzwischen alle Apps auf dem Gerät, und das auch unter älteren Android-Versionen [2]. Sie finden Play Protect am Einfachsten in der App Play Store im Hamburger-Menü.

Die Option „Gerät auf Sicherheitsbedrohungen prüfen“ muss eingeschaltet sein und der letzte Scan darf nur ein paar Tage her sein. Falls nicht, ist das ein deutlicher Hinweis auf eine Infektion. Ist die zweite Option „Erkennung schädlicher Apps verbessern“ darunter aktiviert, lädt Play Protect unbekannte Apps zu Google hoch und lässt sie dort in der Cloud scannen. Obwohl sinnvoll, ist sie standardmäßig ausgeschaltet und liefert daher keinen Hinweis auf eine Infektion.

Schalten Sie Play Protect und das „Verbessern“ ein und führen Sie bei aktiviertem Internet-Zugang mit dem Reload-Knopf darüber einen sofortigen Scan aller Apps durch. Die Spionage-Tools mSpy und FlexiSpy werden dabei erkannt und können rückstandslos deinstalliert werden. Die folgenden Kontrollen sollten Sie dennoch zusätzlich durchführen.



Androids eingebauter Virenscanner darf nicht deaktiviert sein (links), die letzte Überprüfung sollte nicht zu weit zurückliegen. Der Scanner erkennt nämlich durchaus gängige Spionage-Apps (rechts), auch wenn sie sich als „Update Service“ verstecken.

Weil Googles Play-Store-Scanner viele Spionage-Apps erkennt, sind sie dort nicht erhältlich. Der Angreifer muss sie als Datei aufs Smartphone laden und manuell installieren. Dazu muss er die Sperre abschalten, die normalerweise vor Apps aus solchen Fremdquellen schützt.

Bei älterem Android finden Sie diese Sperre in den Einstellungen unter „Sicherheit/Unbekannte Herkunft“ oder ähnlich. Bei aktuellem Android gibt es keine zentrale Sperre mehr, sondern man erlaubt es gezielt einzelnen Apps wie FileManager, Browser oder Dropbox, Fremd-Apps zu installieren. Die Liste der Apps finden Sie in den Einstellungen unter „Apps & Benachrichtigungen/Spezieller App-Zugriff/Unbekannt“ oder ähnlich; hier sollte bei keiner App „zulässig“ stehen.

In beiden Fällen bedeutet eine deaktivierte Sperre, dass ein Spionageangriff stattgefunden haben kann. Umgekehrt ist eine eingeschaltete Sperre keine Versicherung für ein sauberes System, denn der Angreifer kann sie nach Installation des Schädlings einfach wieder aktivieren.

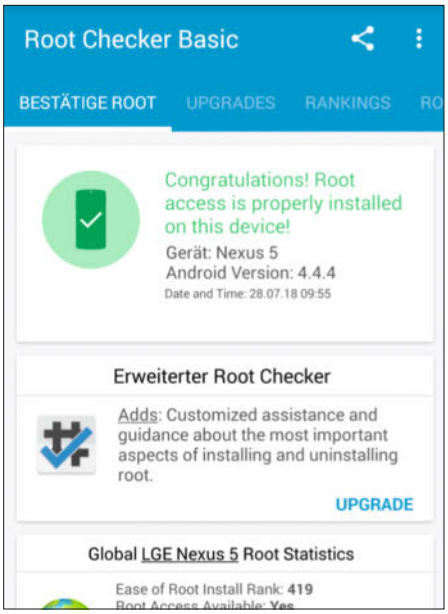
Verdächtige Apps

Verlassen Sie sich im Verdachtsfall nicht auf Play Protect, sondern überprüfen Sie alle installierten Apps. Öffnen Sie dazu in den Einstellungen den Punkt „App-Berechtigungen“, meist unter „Apps“ oder „Apps & Benachrichtigungen“ oder ähnlich zu finden, auf manchen Geräten im Drei-Punkte-Menü der Apps-Anzeige oben rechts. Dort kontrollieren Sie, welche Apps auf persönliche Daten zugreifen dürfen.

Hier sollten unter den Punkten Kontakte, SMS, Kamera und Standort keine Apps auftauchen, die Sie nicht installiert haben oder von denen Sie nicht wissen, was sie machen. Deinstallieren Sie unbekannte Apps, notieren Sie sich aber (auch bei den folgenden Deinstallationen) vorher den Paketnamen, um Ihre Arbeiten nachvollziehen zu können. Wenn einige Apps mit einem zusätzlichen Schloss-Symbol doppelt erscheinen: Das ist eine Auswirkung einer unkritischen Funktion einiger Samsung- und Xiaomi-Geräte, mit der Sie Apps mit einem zweiten Konfigurationssatz starten können.

Dann durchsuchen Sie die Liste aller installierten Apps nach unbekannten oder verdächtigen Apps. Welche Berechtigungen eine App anfordert, verrät ein Antippen der App. Daraus kann ein erfahrener Nutzer oft schon eine erste Tendenz erkennen, ob etwas faul ist.

Allerdings fordern auch einige harmlose Apps eine Vielzahl an Berechtigun-



Mit Root Checker finden Sie heraus, ob Ihr Gerät gerootet ist. Die Meldung „Congratulations!“ bedeutet in Ihrem Fall „Vorsicht! Verseuchungsgefahr!“

Checkliste zum Prüfen von Android-Geräten

- ist das Gerät nicht gerootet?
- unbekannte Geräteadministratoren deaktivieren
- Play Protect einschalten und Gerät scannen
- verdächtige Apps entfernen
- Passwörter aller Dienste (Google, Banking, Facebook, Evernote, Dropbox, ...) ändern
- Web-Zugriff von Messenger-Apps sperren
- notfalls auf Werkseinstellungen zurücksetzen

gen an – etwa weil die Entwickler fragwürdige Bibliotheken zur Werbeeinblendung nutzen. Unschön, aber aus Spionage-Sicht unkritisch, sofern Sie die App wissentlich selbst installiert haben. Denn dass gerade diese App eine echte Schwachstelle hat und dass Ihr Angreifer genau diese ausnutzt, ist unwahrscheinlich. Andererseits schadet es nichts, im Rahmen dieser Diagnose direkt alle anderen kritischen oder ungenutzten Apps zu deinstallieren.

Wichtig ist auch ein Blick auf die Quelle der App, gerade falls bei Ihnen die Installation aus Fremdquellen zugelassen war. Neuere Android-Versionen zeigen das in dieser App-Detailansicht unter den Berechtigungen an. Dort steht etwa „Von Google Play Store geladene App“ (im Allgemeinen unkritisch) oder „Von Galaxy Apps geladene App“ (Vorinstallation von Samsung). Höchst verdächtig ist hingegen eine „Vom Paket-Installer geladene App“, sie stammt aus einer fremden Quelle. Wenn Sie sie nicht selbst aus gutem Grund installiert haben: Weg damit! Weil nicht alle Smartphones Fremd-Apps so klar auszeichnen, schauen Sie zuerst kurz, wie eine unverdächtige App ausgezeichnet ist.

Allerdings dürften Sie auch eine Reihe Fehlalarme bekommen, denn viele Hersteller installieren Apps, deren Sinn sich gar nicht oder zumindest nicht aus dem Namen erschließt. Diese aus Spionage-Sicht unverdächtigen Apps erkennen sie daran, dass in der App-Detailansicht der Knopf fürs Deinstallieren fehlt und Sie sie stattdessen höchstens deaktivieren können. Sie sind im Allgemeinen unbedenklich, sofern nicht schon ab Werk oder vom Zwischenhändler eine Malware installiert wurde (siehe ct.de/w7bc).

Die üblichen Spionage-Apps dürften Sie mit diesen Maßnahmen gefunden und von Ihrem System verbannt haben. Weitere Indizien für eine Spionage-Infizierung finden Sie in der Tabelle unten. Wenn Sie den Verdacht haben, dass gewieftere Angreifer hinter Ihnen her sind, die hartnäckigere Schadsoftware installiert haben, sollten Sie einen Reset auf Werkseinstellungen vornehmen – oder einen Experten zu Rate ziehen, da es auch Schädlinge gibt, die ein Reset überleben oder die in der Firmware lauern.

Accounts schützen

Falls Sie einen erfolgreichen Angriff befürchten, sind nach dem Säubern des Geräts weitere Maßnahmen ratsam. Sie müssen davon ausgehen, dass auch Ihr Google-Account kompromittiert ist.

Unter https://myaccount.google.com/device-activity finden Sie heraus, welche Geräte Ihren Google-Account nutzen und wann der letzte Zugriff stattgefunden hat. Verdächtige Geräte löschen Sie einfach durch einen Klick auf „Entfernen“. Ändern Sie dann Ihr Passwort. Wir empfehlen, bei dieser Gelegenheit auch die Bestätigung in zwei Schritten zu aktivieren (siehe S. 44).

Das Gleiche gilt auch für alle anderen Cloud-Dienste, die Sie nutzen: Dropbox, Evernote, Facebook – und, wichtig, vom Smartphone aus genutztes Internet-Banking. Kontrollieren Sie die Zugriffe, ändern Sie im Zweifel die Passwörter, aktivieren Sie wenn möglich die Zweifaktor-Authentifizierung und löschen Sie verdächtige registrierte Geräte.

Bei WhatsApp, Signal und einigen weiteren Messengern droht eine zusätzliche Falle: Sie bieten inzwischen die Möglichkeit, die App auch über Browser zu bedienen und somit an alle Nachrichten und Fotos zu gelangen. Der Zugriff bleibt, einmal eingerichtet, auch nach Säuberung Ihres Handys aktiv. Diese Zugänge finden Sie bei WhatsApp unter „WhatsApp Web“, bei Signal unter „Verknüpfte Geräte“, bei Threema unter „Threema Web“ – löschen Sie sie alle.

Werkseinstellungen

Die letzte Rettung – vor allem wenn das Gerät gerootet sein sollte – ist der Factory Reset, also das komplette Zurücksetzen auf Werkseinstellungen. Falls Sie Ihr Gerät für hoffnungslos befallen und verwanzt halten, führen Sie die obigen Passwort-Änderungen erst nach dem Reset oder von einem anderen Gerät aus durch, denn sonst erfährt ein möglicherweise noch installierter Keylogger die neuen Passwörter. Der Reset löscht alle Daten vom Handy, bringen Sie also vorher alles Wichtige wie Fotos, Adressen und Termine in Sicherheit und notieren Sie sich wichtige Elemente Ihrer Konfiguration.

Sie stoßen den Reset in den Einstellungen in „System/Optionen zurücksetzen/Alle Daten löschen“ an, auf einigen Systemen „Allgemeine Verwaltung/Zurücksetzen/Auf Werkseinstellungen zurücksetzen“ oder ähnlich genannt.

Achten Sie beim erneuten Einrichten des Telefons darauf, es als „neues Gerät“ einzurichten und nicht etwa aus einem Backup zu installieren. Denn Sie laufen sonst in Gefahr, dass Ihr Gerät aus dem Backup direkt wieder infiziert wird. Denken Sie auch unbedingt daran, den Zugang zum Gerät zu sperren, entweder per Fingerabdruck, Gesicht oder Passwort, mindestens aber mit einer vier- oder besser sechsstelligen PIN. *(jow@ct.de)* c't

Literatur

[1] Schwierige Wurzelbehandlung, Root-Zugriff und Custom-ROMs mit Android, Alexander Spier, c't 4/2018, S. 100
[2] Android sichtbar geschützt, Googles Schutzpaket Play Protect für Android, Ronald Eikenberg, c't 23/2017, S. 142

Android-Forensik: ***ct.de/w7bc***

Bekannte Spyware und deren Erkennung

Spyware	Hinweise auf eine Infektion
mSpy	Wählen von #000* öffnet das User-Interface von mSpy
FlexiSpy	FSXGAD_\<versionsnummer>.apk auf der SD-Karte; in /data/app/ liegt com.mobilefonex.mobilebackup-1.apk; http://djp.cc bleibt oft im Browserverlauf zurück; Wählen von *#900900900 öffnet das User-Interface von FlexiSpy
PhoneSheriff	hinterlässt alle abgefangenen Daten und Einstellungen unter /data/com.studio.sp2/
MobileSpy	Wählen von #123456789* öffnet das User-Interface von MobileSpy
OmniRAT	erzeugt Geräte-Administrator com.android.engine.Deamon