c't wissen

Überwachung

Das Praxishandbuch gegen Schnüffler

c't Überwachung abwehren

Smartphones abdichten

Schnüffel-Apps ganz einfach zügeln
Lösungen für Unternehmen

Wirklich sicheres Online-Banking

Abhörsicher mailen

Sichere Mail-Services getestet
Komfortabel verschlüsseln mit PGP

Facebook und WhatsApp bändigen

www.ctspecial.de

Sofort abtauchen!

Jetzt für nur 12,90 € inklusive VR-Brille bestellen.

shop.heise.de/ct-wissen-vr ✉ service@shop.heise.de
Auch als eMagazin erhältlich unter: shop.heise.de/ct-wissen-vr-pdf

Generell **portofreie Lieferung** für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 15 €

heise shop
shop.heise.de/ct-wissen-vr

Editorial

Zeit, aktiv zu werden!

Software-Hersteller, Dienste-Betreiber, Werbebranche und die Geheimdienste sowieso – offenbar bedienen sich bald alle nach eigenem Gutdünken an unseren Daten. Was ungeschützt rumliegt oder durchs Netz geht, das kann man doch wohl auch nutzen, oder?

Nein! Damit ist jetzt Schluss. Wir erobern uns die Hoheit über unsere Daten zurück und fordern unsere vom Grundgesetz garantierte Selbstbestimmung wieder ein: „Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."

Da jedoch kaum damit zu rechnen ist, dass NSA, Admob & Co. künftig freiwillig auf das Sammeln und Auswerten von Daten verzichten werden, haben wir für Sie dieses Praxishandbuch gegen die grassierende Totalüberwachung zusammengestellt. Es zeigt Ihnen, wo überall spioniert wird und vor allem: was Sie ganz konkret dagegen tun können.

Viel Spaß beim Lesen und gutes Gelingen bei der Umsetzung

Jürgen Schmidt

Inhalt

APPS BÄNDIGEN

Ohne Abnicken aller geforderten Rechte keine App-Installation? Gegen allzu neugierige Apps helfen die richtigen Einstellungen und spezielle Privacy-Apps.

MESSAGING OHNE LAUSCHER

Wer per WhatsApp, Facebook oder Videotelefonie kommuniziert, macht Unbefugten den unbemerkten Zugriff auf die eigene Privatsphäre oft unnötig leicht.

E-MAIL PRIVAT

Sicher sind E-Mails nur, wenn man die Verschlüsselung auch konsequent nutzt. Das gelingt am besten mit Programmen, die einem das Leben nicht unnötig schwer machen.

ONLINE-BANKING SICHER

TAN, PIN oder doch lieber HBCI? Nicht jedes Sicherheitsverfahren der Banken schützt bei Online-Buchungen gleich gut vor Cyber-Dieben.

BYOD MANAGEN

Mit dem privaten Smartphone auf Firmendaten zuzugreifen ist weit verbreitet. Dabei gilt es Betriebsgeheimnisse zu sichern, ohne die private Nutzung zu beschränken.

ZUM HEFT

Smartphone-Schnüfflern auf der Spur

Sobald sich ein Smartphone mit dem Internet verbindet, fließen die Daten: Viele dieser Übertragungen werden heimlich vollzogen, enthalten vertrauliche Daten und führen zu Webseiten, von denen Sie noch nie gehört haben.

Von **Achim Barczok**

Wenn die Beschreibungstexte von Android-Apps wirklich alles aufführen würden, was sie tun, dann könnten viele Entwickler die Downloads vermutlich an zwei Händen abzählen. „Wir senden Ihre genauen Standortdaten kombiniert mit E-Mail-Adresse, Telefonnummer und anderen persönlichen Daten an unsere Server“ müsste es zum Beispiel bei PayPal heißen.

Der Text des Bilderdiensts PicsArt und des Spiels Trivia Crack hätte den Zusatz: „Wir schicken Ihre Ortsdaten regelmäßig unverschlüsselt durchs Netz – an unseren gemeinsamen Werbepartner.“

Die Security-Suites von Avira, Bitdefender und AVG würden werben mit: „Dank unseres Diebstahlschutzes wissen wir immer, wo Sie sind. Auch wenn Sie ihn gar nicht aktiviert haben.“

Egal ob bewusste Weitergabe, unnötige Sammelei oder sorgloses Hantieren mit persönlichen Daten – Schnüffeln ist bei Android-Apps kein Einzelfall, sondern die Regel. Statt dem Gebot der Datenarmut zu folgen, scheinen sich viele Entwickler und ihre Partner dem Grundsatz verschrieben zu haben, vorsichtshalber alles mitzuschneiden, was sie abgreifen können und was für sie oder andere in

Zukunft interessant sein könnte. Google trägt dabei Mitschuld: Das Unternehmen weiß seit Jahren um die Schwächen von Android, die das Datensammeln im Verborgenen erleichtern. Dagegen getan hat Google so gut wie nichts.

Wer seine Daten schützen will, darf deshalb nicht auf Google hoffen: Es ist Zeit, selbst aktiv zu werden. Bauen Sie eine Sicherheitsbarriere um Ihr Handy, kontrollieren Sie Datenflüsse und ertappen Sie Datensammler auf frischer Tat. Wie das geht, erklären wir Ihnen in diesem und nachfolgenden Artikeln.

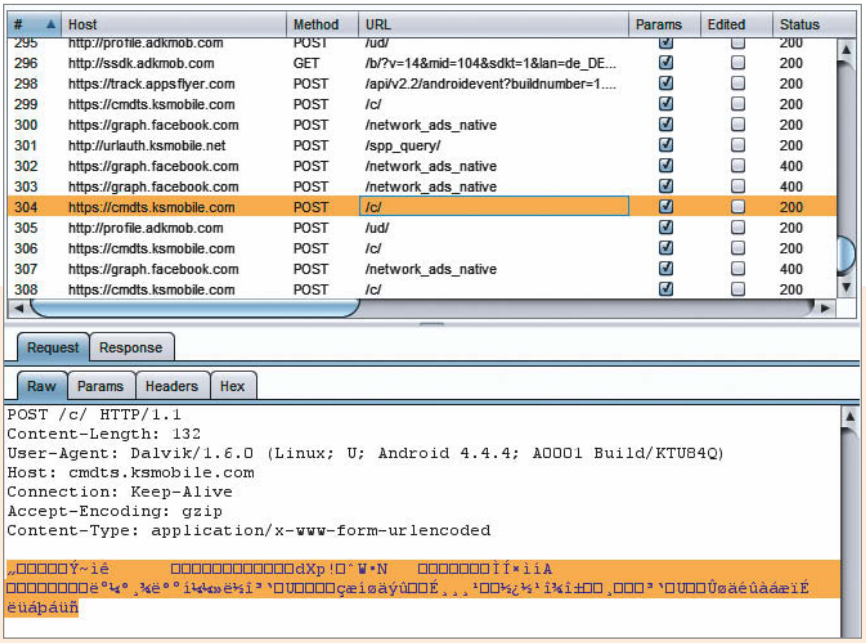
Datenhort Smartphone

Für viele haben Smartphones den PC als Speicher der wichtigsten und privatesten Daten ersetzt: Dort lagern Unterlagen, persönliche Fotos, Kontodaten, der Browser-Verlauf, jeglicher Kommunikationsaustausch mit Freunden, Familie und Arbeitskollegen sowie hunderte Adressen, Telefonnummern und Kalendereinträge. Dank vielfältiger Sensoren und Funktionen erfassen Smartphones außerdem vieles aus ihrer direkten Umgebung: Fotografien, Ton, den Standort.

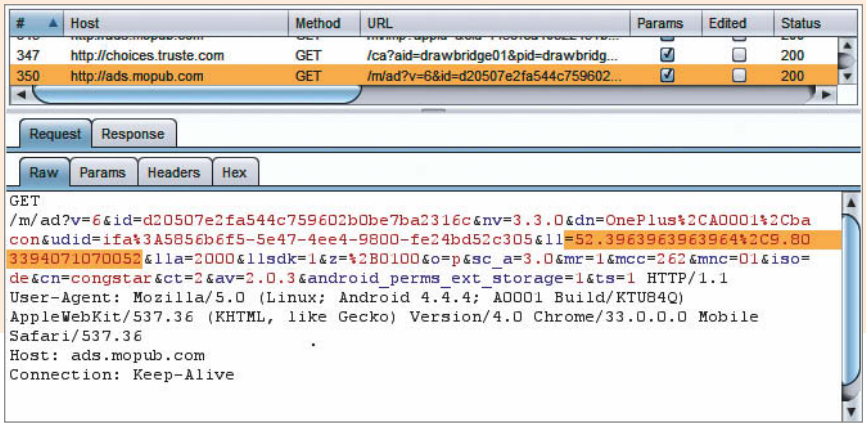
Schon ein kleiner Teil dieser Informationen zeichnet, zentral zusammengefügt, ein detailliertes Profil des Nutzers: Wer ist er, wo ist er, was hat er sich gekauft und was wünscht er sich zu seinem nächsten Geburtstag. Anonym zu bleiben ist unmöglich: Schon eine Handvoll Ortsdaten identifizieren zuverlässig, wo man wohnt und arbeitet. Wie viel man aus den Daten eines Handys lesen kann, bewies vor Kurzem der Taxi-Dienst Uber: Er rechnete anhand der Bewegungsprofile seiner Nutzer aus, in welchen US-Städten besonders viele One-Night-Stands stattfinden.

Datentresor Android?

Prinzipiell bringt Android alles mit, um diese sensiblen Informationen zu schützen und ein guter Datentresor zu sein, sogar ein besserer als der PC. Installierte Apps leben in einer Sandbox und sind so vom Rest des Smartphones abgetrennt. Auf persönliche Daten, den aktuellen Standort, Systemeinstellungen oder auch die SD-Karte darf eine App erst zugreifen, wenn man es ihr explizit erlaubt hat.



Clean Master sendet ständig verschlüsselte Daten nach Hause und zu Werbenetzwerken – auch wenn die App im Hintergrund läuft.

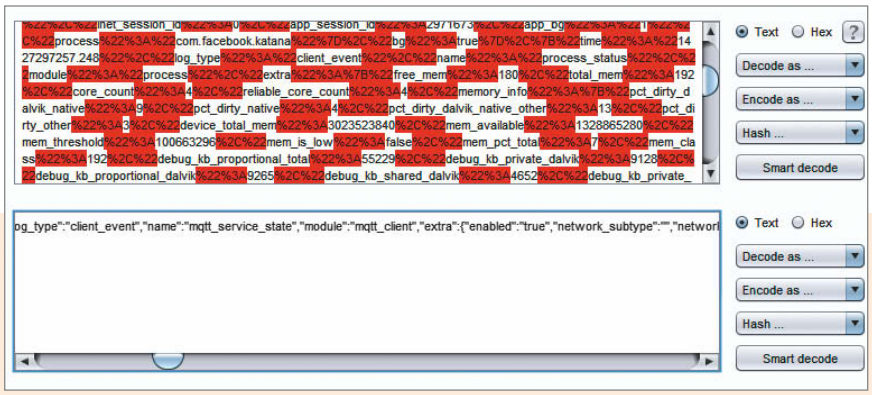


Viele werbefinanzierte Spiele schicken Ortsdaten in Kombination mit der Werbe-ID des Smartphones unverschlüsselt an ihren Werbepartner MoPub.

Doch dieses System funktioniert nur, wenn der Anwender die Kontrolle behält und sinnvoll entscheiden kann, welcher App er den Zugang zu welchen Daten gewährt. Genau das ist jedoch bei Android derzeit noch nicht möglich. Welche Daten eine App nutzen oder gar ins Netz versenden darf, muss der Anwender pauschal bei der Installation abnicken. Er kann weder einzelne Rechte wie den Zugriff auf SMS oder Internet verbieten, noch kann er sie nachträglich entziehen. Der DB Navigator beispielsweise benötigt für durchaus sinnvolle Extra-Funktionen den Zugriff aufs Adressbuch und die Ortsdaten; nur muss man ihm diese Rechte auch dann geben, wenn man die Zusatzfunktionen nicht benutzen will. Die Security-Pakete von Avira, Bitdefender und AVG bieten einen Diebstahlschutz, der das Gerät lokalisiert, wenn es geklaut wurde oder verloren gegangen ist. Die Ortsdaten senden die Apps aber auch dann nach Hause, wenn man nur den Malware-Scanner der Apps verwendet. Bitdefender sammelt zusätzlich die Liste aller WLAN-Hotspots in der Umgebung.

Undurchsichtig bleibt auch, ob eine App die ihr anvertrauten Daten nur für den angegebenen Zweck nutzt oder sie heimlich missbraucht. PicsArt beispielsweise fordert Ortsdaten für die lokale Bildersuche an, reicht sie dann aber auch an Werbenetzwerke weiter.

Diese Probleme um Android und die Datensicherheit sind nicht neu. Seit vielen Jahren bemühen sich Datenschützer und IT-Sicherheitsleute, dem Treiben einen Riegel vorzuschieben. Dass man etwas tun kann, hat Apple bei iOS gezeigt: Den Zugriff auf Ortsdaten und Kontakte kann der Nutzer dort jederzeit



Der Facebook-Client sammelt detaillierte Infos zum Smartphone und führt ein sekundengenaues Logbuch, in welchen WLANs oder Mobilfunknetzen sich der Anwender eingebucht hatte.

Bitdefender und andere Security-Suites informieren ihre Server für eine Diebstahlschutzfunktion regelmäßig, wo sich das Handy befindet – auch wenn man die Funktion gar nicht nutzt.

für jede App einzeln an- und ausschalten. An die meisten persönlichen Kennnummern kommt eine App nicht ran. Beispielsweise ist die MAC-Adresse für sie nicht lesbar und Werbepartner müssen als Identifikationsnummer eine Werbe-ID benutzen, die der Anwender jederzeit zurücksetzen kann.

Google zieht bei der im Herbst 2015 erscheinenden Android-Version 6.0 (Marshmallow) zwar endlich nach. Doch wer sich aktuell ein Handy kauft, muss davon ausgehen, diese Version verspätet oder im schlimmsten Fall gar nicht für sein Smartphone zu bekommen. Bisher hat sich Google beim Datenschutz hauptsächlich auf echte Malware konzentriert: Der Play Store wird auf bekannte Schad-Software kontrolliert und Apps werden ausgesperrt, die ohne Wissen des Nutzers SMS verschicken oder Telefonate führen.

Wer aber persönliche Daten ohne offensichtlichen Schaden für den Anwender sammelt, muss keine Konsequenzen fürchten. Eine zurücksetzbare Werbe-ID wie bei Apple hat Google nur halbherzig eingeführt. Laut den Entwicklerbestimmungen von Google ist sie zwar seit einiger Zeit für Werbetreibende Pflicht. Dennoch bedienen sich dutzende Apps und Werbedienstleister weiterhin unveränderlicher Kennnummern wie der IMEI (Kennziffer des Geräts) oder der Android ID, die erst beim Zurücksetzen des Geräts gelöscht wird.

Detaillierte Nutzerbilder entstehen

Viele Datenschutzverstöße wirken auf den ersten Blick unbedeutend, führen aber in der Summe und

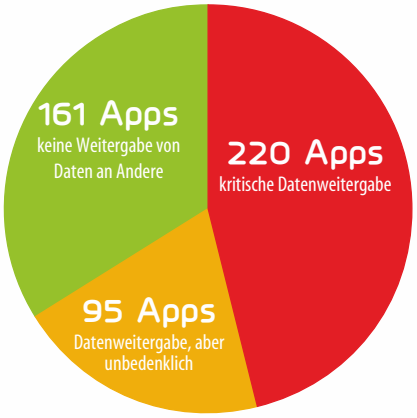
vor allem über längere Zeiträume hinweg zu extrem detaillierten Nutzerprofilen. Die meisten Daten sammeln die App-Entwickler nicht einmal für sich selbst, sondern für andere Schnüffler, die dem Nutzer komplett verborgen bleiben: für Werbenetzwerke und Analysedienste. Fast alle kostenlosen und viele kostenpflichtige Apps nutzen solche Netzwerke und haben deren Schnittstellen in ihre Apps integriert. Wie zahlreich diese Verbindungen inzwischen sind, zeigt das Schaubild rechts. Es stellt alle Verknüpfungen dar, auf die wir im Code der beliebtesten 50 Kostenlos-Apps in Deutschland gestoßen sind.

Werbenetzwerke wollen durch die Datensammelei möglichst passgenaue Anzeigen an die Nutzer ausliefern. Einige dieser Dienste belohnen Entwickler sogar mit höheren Einnahmen, je mehr Daten sie über ihre Nutzer verraten. Gleichzeitig bekommen die Netzwerke ein extrem gutes Bild darüber, wer ein Nutzer ist und was er tut. Ein Anbieter wie MoPub, dessen Code in 8 der 50 beliebtesten deutschen Apps steckt (Stand: März 2015), kann einzeln noch harmlos erscheinende Daten aus den unterschiedlichsten Quellen unbemerkt sammeln und zusammenführen. So könnte aus der einen App der Standort kommen, aus einer anderen detaillierte Geräteinformationen, aus der dritten E-Mail-Adresse und eindeutige Kennnummern: Dank Werbe-ID sind diese drei Häppchen auf einen gemeinsamen Nutzer zurückzuführen. Setzt der Nutzer seine Werbe-ID zurück, kann MoPub die Daten über die verbleibenden Kennnummern immer noch verbinden. Oft gehen solche Datensätze zu allem Überfluss unverschlüsselt durchs Netz, sodass sie auf dem Weg von Smartphone zum Netzwerk von jedem mitgehört werden können.

Manchmal verschwimmen die Grenzen zwischen Entwickler-Tools und Werbeschnüfflern. Das größte Analysenetzwerk Flurry, das 16 der von uns überprüften 50 Apps integriert haben, agiert gleichzeitig auch als Werbeanbieter. Viele Apps bieten an, sich per Facebook bei ihnen einzuloggen; gleichzeitig sammelt das soziale Netzwerk Daten für sein eigenes mobiles Werbenetzwerk. Die Spiele-Engine Unity hat ebenfalls einen Werbekanal integriert und holt sich aus den mit Unity entwickelten Spiele-Apps Nutzerdaten.

Keine Einzelfälle

Was c't immer wieder in kleinen App-Stichproben findet, wird auch von Dienstleistern wie Mediatest Digital bestätigt. Das Unternehmen überprüft in regelmäßigen Abständen hunderte Apps auf Sicherheitsrisiken und Datenschutzprobleme. Von den knapp 500 Android-Apps aus ihrem Pool stellte Mediatest bei zwei Dritteln aktive Kontakte zu Werbe- oder Analysenetzwerken fest. Und die Mehrheit davon stufte Mediatest als datenschutztechnisch bedenklich ein, weil sie persönliche Daten unverschlüsselt versendeten oder beispielsweise die IMEI oder Standortdaten mitschickten. Die Mediatest-Sammlung enthält vor allem Apps für Webdienste, Nachrichtenseiten, Office-Tools und Kommunikationsanbieter. Die gerne als Parade-Schnüffler genannten werbefinanzierten Spiele kommen in der Liste noch nicht mal vor. (acb) c't



Quelle: Mediatest Digital

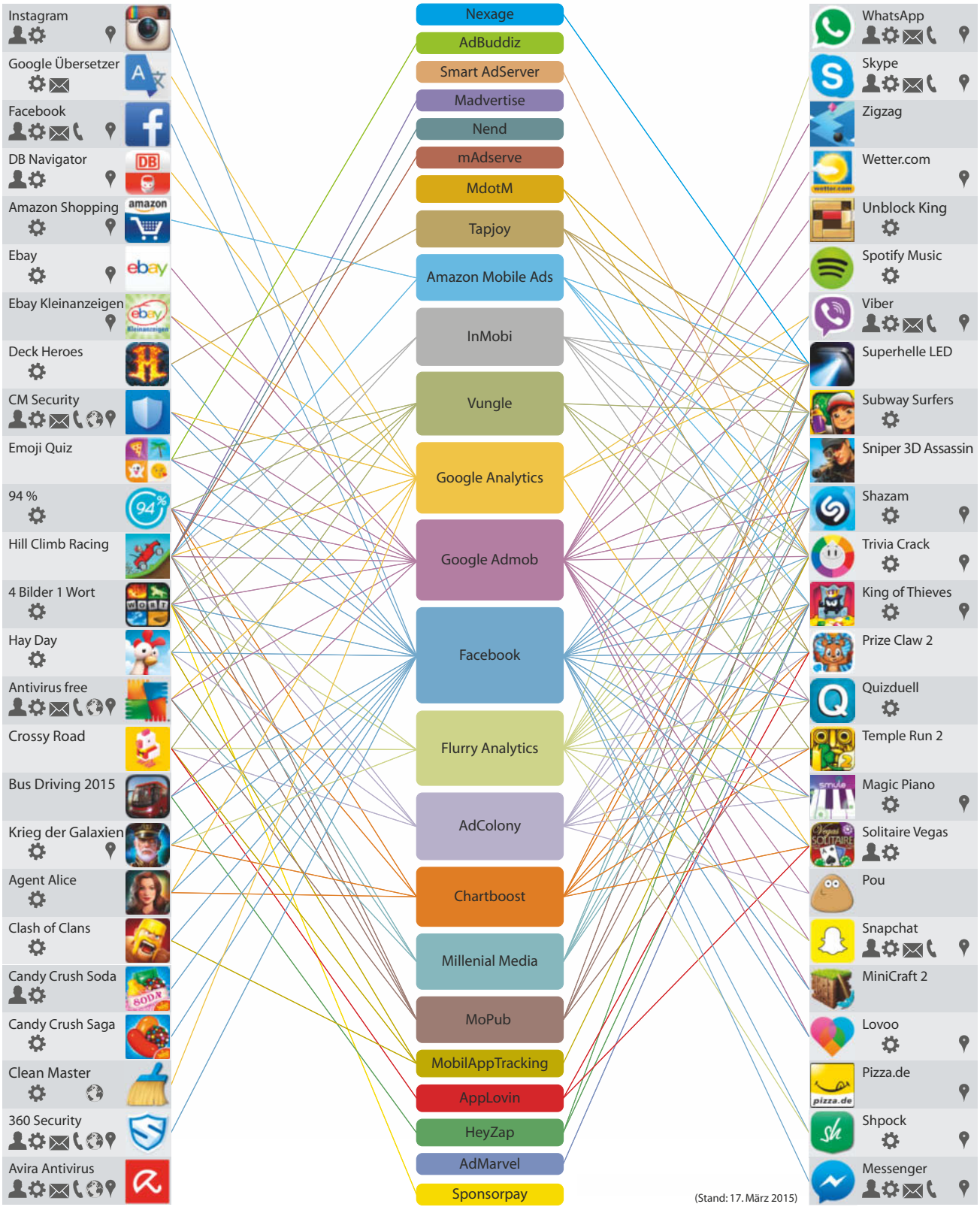
Datenversand an Werbe- und Analysenetzwerke

Der Dienstleister Mediatest untersucht für Unternehmen, welche Apps für den Gebrauch auf geschäftlichen Smartphones datenschutzrechtlich unbedenklich sind. Die Grafik zeigt, wie viele Apps aus ihrem Testpool Daten an Werbe- und Analysenetzwerke weitergeben.

Verbindung zwischen Apps und Werbenetzwerken

Android-Apps offenbaren in ihrer Manifest-Datei die Namen ihrer Java-Komponenten, die Rückschlüsse auf Kooperationen mit Werbe- und Analyse-Netzwerken zulassen. Das Schaubild zeigt, welche Verbindungen zwischen den 50 kostenlosen Top-Apps (links, rechts) und Netzwerken (Mitte) wir im Code gefunden haben.

Zugriff auf vertrauliche Daten
- Kontakte
- Benutzerkonten (Liste)
- SMS, E-Mail etc.
- Telefonie- u. SMS-Funktionen
- Webseitenverlauf
- Ortsdaten



(Stand: 17. März 2015)

Schnüffel-Apps durchleuchten

Um Schnüffel-Apps einen Riegel vorschieben zu können, muss man sie erst einmal identifizieren. Zur Überführung verdächtiger Programme kann man deren Internetverkehr filtern oder einen Blick in den Code werfen. Beides geht einfacher, als es klingt.

Von **Achim Barczok, Ronald Eikenberg** und **David Wischnjak**

Mit den richtigen Werkzeugen ist eine grobe Einteilung in harmlose und gefährliche Apps schnell getroffen – aufwendiger ist es, die Übeltäter in flagranti zu erwischen. In diesem Artikel führen wir Sie in drei Schritten in die Sicherheitsanalyse von Apps ein. Dabei kommen Methoden zum Einsatz, wie sie auch professionelle Sicherheitsunternehmen verwenden.

- **Schritt 1:** Verdächtige Apps identifizieren
- **Schritt 2:** Datenverkehr mit Server abhören
- **Schritt 3:** Code-Analyse

Der erste Schritt erfordert wenig Arbeit oder Vorkenntnisse und hilft, Apps auf ihre Risiken hin einzuschätzen. Haben Sie einen Verdächtigen identifiziert, können Sie im zweiten Schritt den Datenverkehr des Smartphones über einen PC umleiten und dort gezielt abhören. Über einen Man-in-the-Middle-Eingriff lässt sich sogar verschlüsselte Kommunikation mitlesen. Diese dynamische Analyse deckt allerdings nur auf, was die App im Lauf der aktiven Testphase verschickt – es gibt keine Garantie, dass Schnüffeleien zu einem späteren Zeitpunkt auftreten können. Im dritten Schritt dekompilieren wir deshalb die App und versuchen, im Code das Einlesen, Übergeben und Verschicken von persönlichen Daten nachzuvollziehen. Dieser Ansatz wirft am meisten ab, dauert aber auch am längsten. Wir haben uns in diesem Artikel auf Android konzentriert – hier gibt es die meisten Übeltäter, aber auch die meisten Werkzeuge, um ihnen entgegenzuwirken. Das Abhören über einen Server (Schritt 2) lässt sich aber auch recht einfach für iOS und WindowsPhone umsetzen.

Schritt 1: Verdächtige Apps identifizieren

Wie am PC ist auch am Android-Smartphone oder -Tablet die erste und wichtigste Regel, bei der Auswahl neuer Apps genau hinzuschauen. Viele negative Bewertungen im Play Store können beispielsweise auf problematische Apps hindeuten, oft beschreiben Bewertungen auch konkrete Fehlverhalten der Apps.

Während des Installationsdialogs sollten Sie zudem überprüfen, welche Rechte die App einfordert: Eine Taschenlampe benötigt keinen Zugriff auf Ortsdaten; ein Spiel muss keine SMS verschicken. Die Überprüfung solcher Berechtigungen hat Google