DIVSI
Deutsches Institut für Vertrauen und Sicherheit im Internet

P R E S S E I N F O R M A T I O N

Wissenswertes über den Umgang mit Smartphones

Aktuelle DIVSI-Studie:
Android, iOS, BlackBerry und Windows Phone auf dem Prüfstand

- **So erfahren Hersteller - oft unbemerkt vom Nutzer - Details über ihre Kunden.**
- **Meist nur beschränkte Einwirkungsmöglichkeiten der Nutzer**
- **Was geschieht mit meinen Daten und wo werden sie gespeichert?**

Hamburg, 04. November 2014 – Längst zahlen die Nutzer mobiler Geräte mit ihren persönlichen Angaben – oft, ohne es überhaupt zu ahnen. Denn die globale Währung in der Smartphone-Ökonomie sind heutzutage Daten. Der einzelne Kunde hat dabei meist kaum eine Chance zur Selbstbestimmung. Das hat eine aktuelle DIVSI Studie ergeben, in der die vier meistgenutzten Betriebssysteme für Smartphones auf dem deutschen Markt überprüft wurden: Android, iOS, BlackBerry und Windows Phone. Realisiert wurde die Untersuchung vom Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC) im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI).

DIVSI Direktor Matthias Kammer: „Die Technologie von Smartphones besser verstehen und durchschauen zu können, wird von Monat zu Monat wichtiger, da mobile Betriebssysteme auf immer weiteren alltäglichen Geräten wie digitalen Fitnessarmbändern, Datenbrillen oder in Autos zum Einsatz kommen. Die neue Studie leistet einen Beitrag dazu, Zusammenhänge zwischen Funktionalität und Informationsfreigabe besser verstehen und einordnen zu können."

Ausgangsfrage der Studie war eine aktuelle Leitidee des DIVSI: „Was geschieht mit meinen Daten?". Wesentliches Ziel war, das Bewusstsein des einzelnen Nutzers dafür zu stärken, was kritische Daten überhaupt sind, wie darauf zugegriffen wird und welche Einflussmöglichkeiten der Nutzer bei den unterschiedlichen Systemen selbst hat, den Schutz der eigenen Daten zu gewährleisten. Und dies mit Einstellungen und auf Wegen, die nachvollziehbar sind und nicht auf „Hacking" oder tiefstem technischen Expertenwissen basieren.

Die praktisch unbegrenzten Einsatzmöglichkeiten der Smartphones sind geradezu dafür prädestiniert, Gewohnheiten ihrer Nutzer zu erkennen, unbemerkt weiter zu melden und ein genaues Profil zu erstellen, vor allem weil die Geräte praktisch permanent online sind. Ortungsdienste und Sprachsteuerung dienen den Herstellern dabei meist als wertvolle Datenquellen, ebenso wie Nutzungs- und Diagnosedaten.

Datenschutzbestimmungen mit Interpretationsspielraum

Welche Daten die einzelnen Betriebssysteme sammeln und welche Rechte der Nutzer dem Hersteller in Bezug auf diese Daten einräumt, steht grundsätzlich in den Datenschutzbestimmungen. Diese gestatten jedoch einen weitgefächerten Interpretationsspielraum. Für den Nutzer sind die Regeln jedoch praktisch nicht vollständig nachvollziehbar, das Ausmaß der Zustimmung wird ihm nicht bewusst.

Unklar, wo die Daten bleiben

Wo genau Daten gespeichert werden, erfährt der Nutzer bei keinem der getesteten Betriebssysteme konkret. Die Datenschutzbestimmungen weisen lediglich darauf hin, dass die Speicherung und Verarbeitung personenbezogener Daten in zahlreichen Ländern auf der ganzen Welt erfolgen kann.

Unbemerkte Verbindungen

Die Studie zeigte auch, dass alle vier Betriebssysteme bereits aktiv werden, bevor Nutzer überhaupt das erste Telefonat führen oder eine erste Nachricht versenden. In einer technischen Untersuchung zeigte sich, dass die Geräte direkt nach Inbetriebnahme, bei Auswahl einer minimalen Konfiguration, automatisch eine Vielzahl von Netzwerkverbindungen mit verschiedenen Servern im Internet herstellen.

Datenzugriffe durch Dritt-Apps

Apps von Drittanbietern erweitern die Funktionen eines Smartphones im Auslieferungszustand erheblich. Sie werden in den jeweiligen App-Stores der Hersteller zum Download angeboten, oftmals kostenlos. Möchte man Apps auf seinem Gerät installieren, ist in der Regel ein Kundenkonto erforderlich.

Mit Installation und Nutzung solcher Apps verlässt der Nutzer allerdings den Raum der Datenschutzbestimmungen des Herstellers. Fortan gelten für die Benutzung der App die rechtlichen Bedingungen der Drittanbieter. Dadurch setzen sich die Nutzer einem weiteren Risiko aus.

Es gibt zum Teil erhebliche Unterschiede bei den Betriebssystemen, inwieweit ein Nutzer Datenzugriffe durch Dritt-Apps erkennen, verstehen und kontrollieren kann. Ob und wann Zugriffe auf private Daten erfolgen, ist für Nutzer dabei kaum nachvollziehbar. Android und iOS bieten zumindest bei Standortdaten die Möglichkeit an, dass der Nutzer einsehen kann, welche Anwendungen zuletzt auf die Daten zugegriffen haben. Einmal erteilte Zugriffsrechte können Anwender nur bei iOS und BlackBerry wieder rückgängig machen.

Die Studie möchte die Nutzer aufklären und sensibilisieren, welche und wie viele Daten durch die Verwendung eines Smartphones anfallen und verarbeitet werden. In einem Katalog der zehn wichtigsten Fragen und Antworten informiert das DIVSI leicht verständlich und übersichtlich, was Nutzer bei der Verwendung ihres Smartphones mit den Betriebssystemen Android, BlackBerry, iOS oder Windows Phone wissen sollten. Gleichzeitig gibt der Fragenkatalog Hilfestellung für den alltäglichen Umgang mit den eigenen Daten auf dem Smartphone - ohne auf Annehmlichkeiten bei der Nutzung verzichten zu müssen.

Die Studie ist kostenlos erhältlich als Download unter www.divsi.de

Pressekontakt:

DIRK METZ Kommunikation
www.dirk-metz.de

Bockenheimer Landstraße 51-53 - 60325 Frankfurt

Tel.: 069/2400 84 45/46 - Fax: 069/2400 8415

Mail: info@dirk-metz-kommunikation.de

Fraunhofer AISEC ist eine der international führenden Einrichtungen für angewandte Forschung im Bereich IT-Sicherheit. Mehr als 80 hochqualifizierte Mitarbeiterinnen und Mitarbeiter arbeiten an maßgeschneiderten Sicherheitskonzepten und Lösungen für Wirtschaftsunternehmen und den öffentlichen Sektor. Dazu zählen Lösungen für eine höhere Datensicherheit sowie für einen wirksamen Schutz vor Cyberkriminalität wie Wirtschaftsspionage und Sabotageangriffe. Das Kompetenzspektrum erstreckt sich von Embedded Security, über Automotive, Network und Smart Grid Security bis hin zum Schutz vor Produktpiraterie und Industrial Security sowie die Absicherung von Cloud-Diensten. Zudem bietet Fraunhofer AISEC in seinen modernen Testlaboren die Möglichkeit zur Evaluation der Sicherheit von vernetzten und eingebetteten Systemen, von Hard- und Software-Produkten sowie von Web-basierten Diensten und Cloud-Angeboten.

Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI)
Mittelweg 142 • 20148 Hamburg • Telefon +49 (0) 40 226 36 98 98 • Fax +49 (0) 40 226 36 98 93 • info@divsi.de • www.divsi.de

Zu den Kunden von Fraunhofer AISEC gehören Hersteller, Zulieferer und Anwender aus den Bereichen der Chipkartensysteme (u.a. Infineon Technologies, Giesecke & Devrient), Telekommunikation (u.a. Deutsche Telekom), dem Automobilbau (u.a. BMW) und deren Zulieferindustrie sowie Logistik und Luftfahrt, Maschinenbau und Automatisierungstechnik, dem Gesundheitswesen, der Software-Industrie wie auch dem öffentlichen Sektor.

Weitere Informationen unter www.aisec.fraunhofer.de.

Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI)
Mittelweg 142 • 20148 Hamburg • Telefon +49 (0) 40 226 36 98 98 • Fax +49 (0) 40 226 36 98 93 • info@divsi.de • www.divsi.de