Aufgabe für App-Anbieter
Transparenz für Android App-Nutzer herstellen!

In den vergangenen Monaten erreichten den Hessischen Datenschutzbeauftragten (HDSB) zahlreiche Beschwerden bzgl. der Funktionsweise von bestimmten Apps unter dem Betriebssystem Android.

Die Beschwerdeführer erklärten, bestimmte Apps würden auf den Standort, den Kalender und die Kontaktdaten des Gerätes zugreifen. Sie hatten den Verdacht, dass ihre persönlichen Daten verdeckt ausspioniert werden.

Wenn bei den Benutzern Zweifel am rechtmäßigen Umgang mit personenbezogener Daten einer App entstehen, kann es der Reputation der App, der damit verbunden Dienstleistungen und nicht zuletzt der Reputation des verantwortlichen Unternehmens massiv schaden. Dies ist in der Regel mit wirtschaftlichen Nachteilen verbunden. Im internationalen Vergleich sind datenschutzfreundliche Apps aus Deutschland ganz klar ein Wettbewerbvorteil, da insbesondere außerhalb der Europäischen Union oft kein ausreichendes Schutzniveau herrscht.

Es war deshalb zu klären, ob diese Apps unzulässig personenbezogene Daten nutzen oder die Bedeutung und Funktionsweise von systeminternen Berechtigungen – die eine App unter Android-OS benötigt – von den Betroffenen missverstanden wird.

Weiterführende Informationen bietet die „Orientierungshilfe Apps“ [1], in der Rahmenbedingungen für eine gesetzeskonforme Entwicklung und Nutzung von Apps dargestellt werden.

Persönliche Daten auf Smartphones und Tablet-Computern

Smartphones und Tablet-PCs sind leistungsfähige Computer, deren Daten für Angreifer und die Wirtschaft zum Teil viel interessanter sind, als Daten klassischer Personal-Computer, weil sie noch mehr personenbezogene Daten von ihren Besitzern, deren Freunden und anderen Personen preisgeben können.

Zum Beispiel:

- Kontakte (Namen, Telefonnummern, E-Mail-Adressen, Anschriften, Geburtsdaten uä.)
- Geräteinformationen (Rufnummer, eindeutige Geräte-ID)
- Fotos, Musik, Videos, Dokumente uä.
- Nachrichteninhalte von SMS, E-Mails uä.
- Aufenthaltsorte
- Kalender/Termine
- Telefonate (vergleichbar mit einem Einzelverbindungsnachweis)
- Informationen zum Surfverhalten (Anmeldedaten, Passwörter, Chroniken, Lesezeichen uä)

Diese Daten lassen sich für wirtschaftliche Zwecke sehr gut nutzen. Deshalb versuchen Gerätehersteller, Provider und vor allem App-Anbieter diese Daten zu erhalten.

Gustav-Stresemann-Ring 1 • 65189 Wiesbaden • Telefon 0611 1408 0 • Telefax 0611 1408 900
E-Mail poststelle@datenschutz.hessen.de • Internet http://www.datenschutz.hessen.de

„Heimtückische“ Apps übertragen diese sogar einfach ungefragt, unverschlüsselt und nicht anonym auf die Server der App Betreiber. Datenschutzgerechte Apps nutzen nur die Daten, die zum Betrieb der App erforderlich sind und nur nach Rückfrage mit dem Betroffenen.

Android App-Berechtigungen

Damit Apps nicht eigenmächtig auf alle Daten zugreifen können, existieren unter Android-OS systeminterne Berechtigungen. Dadurch soll der Benutzer erkennen können, welche persönlichen Daten eine App verarbeiten will. Die benötigten Berechtigungen werden im Idealfall vor der Installation zur Zustimmung oder Ablehnung angezeigt. Stimmt der Benutzer den Berechtigungen nicht zu, lässt sich die App nicht installieren.

Teilweise verlangen Apps nach Berechtigungen, die sie zur Funktionserfüllung nicht benötigen. In solchen Fällen ist Vorsicht geboten. Es besteht die Gefahr, dass die eigenen Daten unberechtigt als Ware gehandelt werden.

Typischerweise erscheinen für Apps des Öfteren Updates. Gründe dafür sind Fehlerbeseitigungen, Sicherheitsupdates und Weiterentwicklung der Funktionalität. Updates werden i.d.R. über den Google Play Store installiert. Benötigt die neue Version der App Berechtigungen, die ihr Vorgänger noch nicht benötigt hat, muss der Nutzer diesen und den bisher benötigten Berechtigungen noch einmal explizit zustimmen.

Beispiel Navigations App

Eine Navigations- App zeigt beispielhaft in der Praxis anzutreffenden Probleme. Kern-Funktionalität einer Navigations- App ist die Routenführung. Dazu benötigt die App die Angabe einer

- Adresse als Reiseziel und
- den aktuelle Standort.

Neben der manuellen Eingabe einer Adresse, kann der Benutzer auch komfortabel eine Adresse aus den Kontakten des Gerätes wählen.

Außerdem kann die App Standortinformationen über das Mobilfunknetz, WLAN oder GPS beziehen und arbeitet mit Kartenmaterial, das auf dem Gerät gespeichert wurde.

Bei ihrer Installation werden folgende Berechtigungen angefordert:

Nr	Systemberechtigung	Beschreibung im Google Play Store
1	Genauer Standort (GPS- und Netzwerkbasiert)	Ermöglicht der App, Ihre genaue Position anhand von GPS-Daten oder über Netzwerkstandortquellen wie Sendemasten oder WLAN zu ermitteln. Standortdienste müssen auf Ihrem Gerät verfügbar und aktiviert sein, damit die App sie verwenden kann. Apps können Ihren Standort anhand dieser Daten ermitteln und verbrauchen eventuell zusätzliche Akkuleistung.
2	Ungefährer Standort (netzwerkbasiert)	Ermöglicht der App, Ihren ungefähren Standort zu ermitteln. Diese Standortangabe stammt von Standortdiensten, die Netzwerkstandortquellen wie etwa Sendemasten oder WLAN verwenden. Diese Standortdienste müssen auf Ihrem Gerät verfügbar und aktiviert sein, damit die App sie verwenden kann. Apps können Ihren ungefähren Standort anhand dieser Daten ermitteln.
3	Anruflisten lesen	Ermöglicht der App, das Anrufprotokoll Ihres Geräts zu lesen, einschließlich der Daten über ein- und ausgehende Anrufe. Diese Berechtigung

		ermöglicht Apps, Daten Ihres Anrufprotokolls zu speichern.
4	Kontakte lesen	Ermöglicht der App, auf Ihrem Tablet gespeicherte Daten zu Ihren Kontakten einschließlich der Häufigkeit zu lesen, mit der Sie bestimmte Personen angerufen, an sie eine E-Mail gesendet oder auf andere Weise mit ihnen kommuniziert haben. Diese Berechtigung ermöglicht Apps das Speichern Ihrer Kontaktdaten und schädliche Apps können Kontaktdaten ohne Ihr Wissen weitergeben.
5	USB-Speicherinhalte ändern oder löschen	Ermöglicht der App, in den USB-Speicher zu schreiben.

Die Benutzer können leicht die Notwendigkeit der Berechtigungen Nr. 1, 2 und 4 nachvollziehen. Bei den Berechtigungen Nr. 3 und 5 entstehen bei aufmerksamen Benutzern jedoch Zweifel, ob diese benötigt werden. Sie stellen sich aller Voraussicht nach folgende Fragen:

- Greift die App auf meine Dokumente, Bilder, Musik, Videos usw. zu, die sich auf der externen Speicherkarte befinden?
- Warum interessiert sich die App für meine Anrufliste? Sie ist schließlich mit einem Einzelgesprächsnachweis vergleichbar.
- Werden diese Daten lokal verarbeitet oder an einen Server übermittelt und gespeichert?

Exkurs: Interner und Externer Speicher bei Android Geräten

Der Interne Speicher von Android- Geräten ist in der Regel fest verbaut. Er enthält das Betriebsystem und installierte Apps inklusive ihrer Daten. Apps können nicht auf die Daten des Betriebsystems und auf die Daten anderer Apps zugreifen.

Externe Speicher von Android-Geräten sind in der Regel austauschbare Speicherkarten. Die installierten Apps und das Betriebsystem können grundsätzlich darauf zugreifen.

Viele Bürgerinnen und Bürger sind oft zu Recht misstrauisch, wenn Apps bei der Installation Berechtigungen erhalten, um auf ihre persönlichen Daten zugreifen zu können. In den letzten Jahren sind viele Missbrauchsfälle aufgedeckt worden. Die Enthüllungen von Edward Snowden sorgen zusätzlich (zurecht) für Verunsicherung.

Überdies sind viele Berechtigungen so definiert, dass sie mehrere einzelne Rechte zusammenfassen. Beispielsweise erlaubt die Berechtigung "Ungefährer Standort" einer App die Ermittlung von Standortinformationen nicht nur über die Sendemastern des Mobilfunkanbieters, sondern auch über WLAN. Die Berechtigung "Genauer Standort" fast sogar drei einzelne Rechte zusammen: Die Ermittlung von Standortinformationen per GPS, WLAN und über die Sendemastern des Mobilfunkanbieters.

Benötigt die App davon aber nur ein Teilrecht, muss trotzdem die Zugriffsberechtigung für alle eingeräumt werden, da die zusammengefassten Rechte nicht teilbar sind. Für die Benutzerinnen und Benutzer ist es aber nicht ersichtlich, warum der Zugriff auf die in der Berechtigung zusammengefassten, nicht benötigten Rechte erlaubt werden soll.

Gleichzeitig sind die detaillierten Beschreibungen der Berechtigungen so formuliert, dass möglichst viele – so genannte „schädliche“ – Anwendungsfälle beschrieben werden. Viele Nutzerinnen und Nutzer glauben dann, dass die App, die gerade installiert werden soll, alle beschriebenen Rechte genau so nutzt.

Ausschlaggebend für die datenschutzrechtliche Bewertung ist aber nicht die Beschreibung der Verwendungsmöglichkeiten dieser Berechtigungen, sondern die tatsächliche Verwendung der eingeräumten Berechtigungen.

Für das Beispiel der Navigations-App könnte eine datenschutzrechtliche Bewertung wie folgt aussehen:

Die Berechtigung Nr. 5 (USB-Speicherinhalte ändern oder löschen) erlaubt der App den Zugriff auf die Externe Speicherkarte. Sie existiert experimentell erst seit Android OS 4.1 und hat noch keine praktische Relevanz, da Apps auch auf die Externe Speicherkarte zugreifen können, wenn Sie diese Berechtigung nicht haben. Diese Berechtigung wird erst in zukünftigen Versionen (aktuell Android OS 4.4.x) so funktionieren, wie sie tatsächlich beschrieben ist.

Die Notwendigkeit der Berechtigung Nr. 3 (Anruflisten lesen) ist technisch bedingt. Sie ist mit der Berechtigung 4 (Kontakte lesen) bis einschließlich der Android OS Version 4.0.x. gekoppelt. Obwohl momentan Android OS 4.4.x aktuelle Version ist, hat die Version 4.0.x noch einen hohen Verbreitungsgrad. Damit die App zu dieser Version abwärtskompatibel bleibt, müssen weiterhin beide Berechtigungen angefordert werden, obwohl die Berechtigung Nr. 3 (Anruflisten lesen) für die Softwarefunktionalität nicht notwendig ist.

In einem konkreten Fall erklärte der Datenschutzbeauftragte des App-Anbieters, dass die Routenberechnung und -führung vom Gerät selbst durchgeführt wird und keine personenbezogenen Daten vom Gerät weder an einen eigenen Server, noch an einen Server eines Dritten übermittelt werden.

Bei einer Prüfung haben sich auch keine Anhaltspunkte ergeben, die diesen Aussagen widersprechen, deshalb bestanden für die App keine datenschutzrechtlichen Bedenken.

Empfehlung

Diese Problematik zeigt deutlich die Wichtigkeit der Transparenz als eines der „neuen Datenschutzziele“ (s.a. M. Rost, A. Pfitzmann: Datenschutz-Schutzziele – revisited, DuD, 2009 S. 353).

Deshalb sollten Anbieter in der Beschreibung der App im Google Play Store detailliert und vollständig folgende Angaben machen oder darauf verlinken:

- Welche Berechtigungen werden für welche Softwarefunktionalität gebraucht?
- Wie werden die dadurch gewonnen Daten verarbeitet?

Dabei sollten keine standardmäßigen Berechtigungsbeschreibungen - wie man Sie aus dem Google Play Store kennt - verwendet werden, da sie in ihrer Abstraktheit nicht konkret zur Softwarefunktionalität der App passen. Diese Beschreibung sollte immer auf dem aktuell zu Installation angebotenen Versionsstand basieren. Durch veraltete Beschreibungen entstehen andernfalls Missverständnisse.

Zusätzlich sollten diese Angaben auch Teil der Datenschutzerklärung der App sein, die ebenfalls im Google Play Store verlinkt sein muss.

Dann können die App-Nutzer erkennen, dass ihre persönlichen Daten nicht verdeckt ausspioniert werden.

Weiterführende Informationen und Links

[1] Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter:
http://www.datenschutz.hessen.de/download.php?download_ID=314&download_now=1

Weiterführende Informationen zum Thema Mobile Geräte finden Sie auf unserer Seite: http://www.datenschutz.hessen.de/ft-mobilegeraete.htm