Deutscher Bundestag **Drucksache 17/11276**

17. Wahlperiode 30. 10. 2012

Kleine Anfrage

der Abgeordneten Jan Korte, Dr. Rosemarie Hein, Ulla Jelpke, Jens Petermann, Dr. Petra Sitte, Frank Tempel, Halina Wawzyniak und der Fraktion DIE LINKE.

Angriffe auf Smartphones

Smartphones haben sich mittlerweile zu leistungsfähigen Mini-PCs entwickelt, die neben vielfältigen Kommunikationsdiensten wie Telefonie, E-Mail und Instant Messaging auch als Speicherplatz für sensible Dokumente und persönlichen Daten dienen. Laut dem BITKOM (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.) stiegen die Verkaufszahlen von Smartphones im Jahr 2011 im Vorjahresvergleich um 31 Prozent auf 11,8 Millionen an. Mittlerweile besitzen fast zwei Drittel der Deutschen ein Smartphone, das geht aus einer repräsentativen Umfrage hervor, die die Bundesministerin für Ernährung, Landwirtschaft und Verbraucherschutz, Ilse Aigner, am 24. Oktober 2012 vorstellte.

Dass die im Betriebssystem der sogenannten mobilen Endgeräte vorinstallierten Sicherheitsmechanismen jedoch kaum ausreichend sind, um vertrauliche Daten angemessen zu schützen, wussten vor nicht allzu langer Zeit noch die wenigsten Nutzerinnen und Nutzer. Noch im Jahr 2011 stellte das Bundesamt für Sicherheit in der Informationstechnik (BSI) in dem Papier „Wie sicher sind Smartphones? Sicherheitsrisiken und Schutzmaßnahmen bei der Nutzung von Mobilen Endgeräten“ fest, dass in diesem Bereich noch immer großer Informationsbedarf herrsche. Die Behörde kam damals im Rahmen einer Befragung zu dem Schluss, dass ein Drittel der Smartphonenutzer nicht wissen, dass ihr Smartphone exakt die gleichen Schutzmaßnahmen wie ihr PC benötigt. Das hat sich offenbar im Laufe der Zeit geändert. In der aktuellen Umfrage des Bundesministeriums für Ernährung, Landwirtschaft und Verbraucherschutz (BMELV) gaben 80 Prozent der Befragten an, auf bestimmte Anwendungen zu verzichten, um sich vor Angriffen auf ihr Smartphone zu schützen.

Das scheint auch notwendig zu sein, denn manipulierte Apps stellen noch immer und in zunehmendem Maße ein großes Sicherheitsrisiko dar. Jedes fünfte der rund 48 000, für das von Google entwickelte Betriebssystem Android, angebotenen Apps ist mit Viren oder Trojanern versehen (Quelle: Studie SMobile Systems). Installiert ein Nutzer unwissend solch eine manipulierte App auf seinem Telefon, verschafft sich diese sogleich Zugriff auf das gesamte Betriebssystem und somit auch auf alle persönlichen Ressourcen. Zugleich erhielten die deutschen Mobilfunkanbieter ein vernichtendes Urteil, als sie vom Securtity Research Lab auf den Schutz vor Spionage getestet wurden. T-Mobile und Vodafone wurden dabei mit mangelhaft bewertet, E-Plus und O_2 sogar mit ungenügend. Das scheint wenig verwunderlich, denn keiner der Anbieter hat die zum Schutz vor Spionage notwendige A5/3 Verschlüsselung eingerichtet (Quelle: WirtschaftsWoche Ausgabe 29/2012).

Die bisher bekanntesten Smartphone-Viren ZitMo, DroidDream und Droidsheep hatten die Fähigkeit, Smartphones so zu steuern, dass es möglich war, Passwörter und für das Onlinebanking notwendige TANs auszuspähen, Bewegungsprofile zu erstellen, sich ohne Kenntnis der Betroffenen in soziale Netzwerke einzuklinken, ja sogar Telefongespräche abzuhören, SMS einzusehen und zu versenden.

Die Daten, die durch solche Programme unbemerkt erworben werden, sind aber nicht nur für Kriminelle interessant. Auch die Anbieter und Entwickler der Smartphone-Apps profitieren von den Daten ihrer Kundinnen und Kunden. Nicht selten werden diese dann zu Werbe- und Analysezwecken genutzt oder an Dritte weiterverkauft. Apple reagierte bereits auf diese Entwicklung. So ist es mit dem Update auf IOS6 notwendig geworden, beim Öffnen einer Anwendung derselben eine Nutzungserlaubnis zu erteilen. Dabei wird explizit genannt, worauf die jeweilige App zugreifen möchte – beispielsweise auf Fotos, den Standort oder das Adressbuch. Ebenso neu ist die Rubrik Datenschutz in den Grundeinstellungen des Telefons.

Das Potential, welches Smartphones zur Spionage der jeweiligen Nutzerin oder des Nutzers bieten, haben mittlerweile auch Staatsregierungen und Ermittlungsbehörden entdeckt. Neben dem bereits in die öffentliche Kritik geratenen Trojaner FinFisher der Firma Gamma International GmbH, mit dem die Rechner von Oppositionellen während der arabischen Revolution bespitzelt wurden, gibt es nun auch eine mobile Version des Trojaners. Demzufolge ist es längst möglich, Skype-Telefonate oder Facebook-Chats, die über das Smartphone betrieben werden, auszuspionieren.

Tatsächlich scheint sich auf diesem Gebiet ein neuer Markt zu öffnen. So arbeitet die Telekom Deutschland GmbH laut Medienberichten zurzeit an abhörsicheren Smartphones, um Regierung und Großunternehmen vor Übergriffen von Hackern und Spionen zu schützen.

Trotz all dieser Vorkommnisse und entgegen der vom Bundeskriminalamt (BKA) gemachten Feststellung einer „beginnende[n] Fokussierung auf das Zielfeld mobile Endgeräte“ (Cybercrime-Bundeslagebericht 2010) durch Kriminelle meint der Präsident des BKA, Jörg Zierke, dass von Angriffen auf Smartphones derzeit keine echte Gefahr ausgeht, und merkt aber zugleich an, dass sich die Bedrohungslage in Zukunft jedoch verschärfen wird.

Wir fragen die Bundesregierung:

1. Liegen der Bundesregierung Statistiken über die Entwicklung der Nutzung von Smartphones vor?

   Wenn ja, welche, wie bewertet die Bundesregierung diese, und was sagen sie aus über

   a) die Anzahl von Smartphone-Nutzern,

   b) die Entwicklung von Angriffen auf Smartphones durch Viren oder Malware (bitte Statistiken der Antwort beilegen)?

2. Wie bewertet die Bundesregierung die Bedrohung durch manipulierte Apps, Viren und Malware für Smartphones?

3. Welche Hersteller, Betriebssysteme und Modelle waren nach Kenntnis der Bundesregierung bisher wie oft von Angriffen durch welche manipulierten Applikationen betroffen (bitte nach Hersteller, Betriebssystem, Modell und manipulierter App aufschlüsseln)?
4. Ist der Bundesregierung bekannt, wie viele Nutzer bisher von manipulierten Apps und deren Konsequenzen betroffen sind (wenn ja, bitte die Anzahl angeben)?
5. Wie viele und welche manipulierten Apps mit welchen Funktionsweisen sind der Bundesregierung seit wann bekannt (bitte nach manipulierter App, Funktionsweise und Datum des Bekanntwerdens aufschlüsseln)?
6. Welche Daten wurden nach Kenntnis der Bundesregierung bisher mit welchen Konsequenzen für den Smartphonenutzer durch welche Apps ausgespäht?
7. In wie vielen Fällen wurde nach Kenntnis der Bundesregierung mit durch manipulierte Apps errungenen Daten Kreditkartenbetrug begangen?
8. Wird die Bundesregierung Konsequenzen aus den Angriffen auf Smartphones ziehen?

   Wenn ja, wie sehen diese aus?

   Wenn nein, warum nicht?
9. Setzt die Bundesregierung manipulierte Apps, Viren oder Malwaresoftware für Smartphones zu Ermittlungszwecken ein?

   Wenn ja,

   a) wie oft war das bisher der Fall,

   b) in welchem Zusammenhang wurde diese Technik genutzt,

   c) auf welcher gesetzlichen Grundlage und

   d) mit welchem Ergebnis?
10. Setzen Ermittlungsbehörden nach Kenntnis der Bundesregierung manipulierte Apps, Viren oder Malwaresoftware zu Ermittlungszwecken ein?

    Wenn ja,

    a) welche,

    b) wie oft war das bisher der Fall,

    c) in welchem Zusammenhang wurde diese Technik genutzt,

    d) auf welcher gesetzlichen Grundlage und

    e) mit welchem Ergebnis?
11. Ist der Bundesregierung bekannt, welche Möglichkeiten die Bürgerinnen und Bürger haben, sich vor Angriffen auf Smartphones zu schützen?

    Wenn ja, welche sind dies?
12. Welche Maßnahmen schlägt die Bundesregierung vor, und welche hat sie bereits durchgeführt, um auf die Bedrohung durch manipulierte Apps aufmerksam zu machen?
13. Will die Bundesregierung den immer häufiger auftretenden Angriffen auf Smartphones entgegenwirken?

    a) Wenn ja, wie?

    b) Wenn nein, warum nicht?

14. Wird die Bundesregierung die Vertreiber von Applikationen auffordern, entsprechende Schritte gegen die Verbreitung von manipulierten Apps einzuleiten und ihr Angebot besser zu kontrollieren?

    Wenn ja, wie sehen diese aus?

    Wenn nein, warum nicht?

Berlin, den 30. Oktober 2012

Dr. Gregor Gysi und Fraktion

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333