Deutscher Bundestag **Drucksache 17/11539**

17. Wahlperiode 20. 11. 2012

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Jan Korte, Dr. Rosemarie Hein, Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 17/11276 –

Angriffe auf Smartphones

Vorbemerkung der Fragesteller

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. Zu-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 15. November 2012 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

gleich 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.

Vorbemerkung der Bundesregierung

Die von der Bundesministerin für Ernährung, Landwirtschaft und Verbraucherschutz, Ilse Aigner, vorgestellte Verbraucherumfrage „Sicherheit und Datenschutz bei Smartphones“ wurde durch die Arbeitsgruppe 4 (AG 4) „Vertrauen, Datenschutz und Sicherheit“ des IT-Gipfels initiiert. Die Studie wurde von Bundesministerin Ilse Aigner und dem Co-Vorsitzenden der AG 4, Dr. Ottenberg, am 24. Oktober 2012 vorgestellt. Nach Aussage des Bundesministeriums für Ernährung, Landwirtschaft und Verbraucherschutz hat Bundesministerin Ilse Aigner am 24. Oktober 2012 mitgeteilt, dass laut Angaben des Branchenverbandes BITKOM von August 2012 70 Prozent der verkauften Handys inzwischen Smartphones sind.

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,

Circa 28 Prozent aller Deutschen verfügen über ein Smartphone, das sind ca. 22 Millionen Menschen. Laut Angaben des Branchenverbandes BITKOM vom August 2012 sind 70 Prozent der verkauften Handys inzwischen Smartphones.

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

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beobachtet und bewertet Bedrohungen auf Smartphones. Anders als bei PC-Systemen werden für Smartphones aktuell keine Angriffe beobachtet, die ohne Interaktion des Nutzers durchgeführt werden (wie z. B. Drive-By-Exploits).

Stattdessen besteht eine Bedrohung durch Apps, die der Nutzer selbst herunterlädt und die Missbrauch mit seinen persönlichen Daten treiben. Eine andere Bedrohung sind trojanisierte (bzw. manipulierte) Apps, die der Nutzer aus nicht vom Anbieter voreingestellten Quellen (wie z. B. dem AppStore oder Google-Play) herunterlädt und die Schadcodes enthalten. Schadprogramme, die auf Smartphones beobachtet werden, sind vor allem sogenannte Premium-Dialer (die SMS an teure Rufnummern versenden) oder die als Nebenkomponente eines Banking-Trojaners auf dem PC dienen (und beispielsweise Bestätigungs-SMS des mTAN-Verfahrens abgreifen). Eine quantitative Betrachtung ist allerdings nicht möglich, da Nutzer diese Fälle häufig nicht bemerken und noch öfter nicht zur Anzeige bringen.

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

Generell ist zu beobachten, dass Kriminelle stets neue Technologien angreifen und ausnutzen, wenn damit Geld zu verdienen ist. Durch die große Verbreitung lohnt sich der Aufwand für Angriffe durch manipulierte Apps und Malware. Mechanismen, die dem Smartphone-Nutzer transparent darstellen, welche Risiken mit der Installation von Apps aus nicht vom Anbieter voreingestellten Quellen verbunden sind, etablieren sich erst langsam.

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)?

Hierzu führt das BSI keine systematische Erhebung durch. Es liegen keine detaillierten Zahlen vor. Grundsätzlich ist davon auszugehen, dass über geschicktes Social Engineering alle Hersteller, Betriebssysteme und Modelle bedroht sind.

4. Ist der Bundesregierung bekannt, wie viele Nutzer bisher von manipulierten Apps und deren Konsequenzen betroffen sind (wenn ja, bitte die Anzahl angeben)?

Hierzu liegen der Bundesregierung keine Erkenntnisse vor. Weder das BSI noch das Bundeskriminalamt (BKA) erheben entsprechende Informationen.

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)?

Hierzu nimmt das BSI keine systematische Erhebung vor. Grundsätzlich sind Applikationen mit Schadfunktionen möglich, die den Verlust der Vertraulichkeit, der Integrität/Authentizität (Identitätsdiebstahl) und der Verfügbarkeit der Daten auf dem Smartphone zum Ziel haben können.

Zu der Anzahl manipulierter Apps wird auf die Antwort zu Frage 4 verwiesen.

6. Welche Daten wurden nach Kenntnis der Bundesregierung bisher mit welchen Konsequenzen für den Smartphonenutzer durch welche Apps ausgespäht?

Für derartig mobile Endgeräte gelten den bisherigen Feststellungen zufolge die gleichen Risiken wie für stationäre Rechner. Auf dem beschriebenen Weg dürfte es somit möglich sein, alle auf dem Endgerät verfügbaren Daten auszuspähen. Es werden solche Daten ausgespäht, die Kriminellen Nutzen bringen. Dies beinhaltet u. a. Adressdaten von Kontakten, Bankzugangsdaten, Kreditkartendaten, Lokalisierungsdaten (siehe auch Antwort zu Frage 1b).

7. In wie vielen Fällen wurde nach Kenntnis der Bundesregierung mit durch manipulierte Apps errungenen Daten Kreditkartenbetrug begangen?

Zu der Anzahl manipulierter Apps und deren Folgen wird auf die Antwort zu Frage 4 verwiesen.

8. Wird die Bundesregierung Konsequenzen aus den Angriffen auf Smartphones ziehen?

   Wenn ja, wie sehen diese aus?

   Wenn nein, warum nicht?

Das Beschaffungsamt des Bundesministeriums des Innern (BMI) hat im Auftrag des BSI die Ausschreibung von Rahmenverträgen über die Lieferung von sicheren mobilen Endgeräten für Sprach- und Datenkommunikation für den Einsatz in der Bundesverwaltung eingeleitet.

Das BKA trägt der Entwicklung im Bereich Cybercrime mit einer entsprechenden Schwerpunktsetzung in der Abteilung „Schwere und Organisierte Kriminalität“ Rechnung. Die im Rahmen der originären bzw. Zentralstellen-Aufgabenwahrnehmung gewonnenen Erkenntnisse werden mit anderen Sicherheitsbehörden ausgetauscht und in diesem Kontext auch für präventive Zwecke aufbereitet.

Maßnahmen zum Schutz der Verbraucher sind durch die dafür zuständigen Institutionen zu ergreifen.

Im Übrigen wird auf die Antwort zu Frage 12 verwiesen.

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?

Ermittlungen werden grundsätzlich von Ermittlungsbehörden geführt. Auf die Antwort zu Frage 10 wird verwiesen.

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?

Die Ermittlungsbehörden auf Bundesebene setzen keine Apps, Viren oder Malware zu Ermittlungszwecken auf Smartphones ein.

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

    Wenn ja, welche sind dies?

Bürger können folgende Schutzmaßnahmen zur Reduzierung der Angriffswahrscheinlichkeit auf ihren Smartphones umsetzen:

- Betriebssystem-Software aktuell halten
- Sicherheitsmechanismen des Betriebssystems nutzen (nicht „Rooten“ oder Jailbreaken“);
- nur tatsächlich benötigte Applikation, aus vertrauenswürdiger Quelle, installieren;
- ggf. Sicherheitssoftware auf dem Smartphone installieren.

12. Welche Maßnahmen schlägt die Bundesregierung vor, und welche hat sie bereits durchgeführt, um auf die Bedrohung durch manipulierte Apps aufmerksam zu machen?

Das Bundesministerium des Innern hat auf die zunehmende Bedeutung des Themas „Mobile Sicherheit“ reagiert und es in den Fokus des diesjährigen IT-Gipfelprozesses gerückt. So beschäftigt sich eine Unterarbeitsgruppe der durch Bundesinnenminister Dr. Hans-Peter Friedrich gemeinsam mit Dr. Ottenberg, dem Vorsitzenden der Geschäftsführung von Giesecke&Devrient, geleiteten AG 4 „Vertrauen, Sicherheit und Datenschutz“ mit der Thematik Mobile Sicherheit. Im Rahmen dieses Prozesses wurde die Umfrage initiiert, auf der die Fragestellung basiert.

Die Thematik stellte einen Schwerpunkt des diesjährigen IT-Gipfels am 13. November in Essen dar. So diskutierten im Rahmen einer Podiumsdiskussion der

Bundesminister des Innern, Dr. Hans-Peter Friedrich, die Bundesbeauftragte für Informationstechnik, Staatssekretärin Rogall-Grothe, Schaar (BfDI), Dr. Ottenberg (G&D), Koederitz (IBM), Streibich (Software AG) und Witt (Student am HPI) zum Thema „Mobile Sicherheit – Mobiles Leben".

Im Rahmen des IT-Gipfels starteten die Bundeskanzlerin Dr. Angela Merkel und die Staatssekretärin Rogall-Grothe „GovApps", eine Informationsplattform für öffentliche mobile Anwendungen.

Darüber hinaus bilden Hinweise auf die Gefahren und Handlungsempfehlungen bei der Nutzung von Smartphones einen Schwerpunkt in der Informations- und Sensibilisierungsarbeit des BSI (vgl. www.bsi-fuer-buerger.de, Hauptnavigationspunkt: Sicher bewegen im mobilen Netz). Dies wird im Bedarfsfall ergänzt durch aktuelle Warnungen über den E-Mail-Newsletter Bürger-CERT (www.buerger-cert.de) bzw. Pressemeldungen des BSI, z. B. bei akuten Angriffswellen oder bei neu gewonnener Erkenntnis über Sicherheitslücken in Betriebssystemen oder Anwendungsprogrammen mit Bezug zu Smartphones.

Das BSI greift anlassbezogen aktiv die Thematik im Rahmen seiner Öffentlichkeits- und Pressearbeit auf, z. B. mit Handlungsempfehlungen (Pressemeldung vom 1. Juni 2012 und Themenseiten in www.bsi-fuer-buerger.de) wie „Sommer, Sonne, Strand und Meer – sicheres Surfen im Ausland: Wie Sie Ihre mobilen Geräte während Ihres Urlaubs schützen."

Zudem setzt das BSI bei Veranstaltungen u. Ä. Druckschriften zur Unterstützung der Sensibilisierungsarbeit zum Thema Mobile Sicherheit ein (vgl. www.bsi-fuer-buerger.de/BSIFB/DE/Wissenswertes_Hilfreiches/Service/Downloads/Broschueren/broschueren_node.html) und stellt auf seiner Internetseite zu aktuellen Themen Überblickspapiere zur Verfügung, wie: „Überblickspapier Smartphone" (www.bsi.bund.de/DE/Themen/ITGrundschutz/Ueberblickspapiere/Ueberblickspapiere_node.html)

Auch die vom Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz geförderte Internetseite des Verbraucherzentrale Bundesverbandes e. V. „surfer-haben-rechte" hält Informationen zu Smartphones bereit (vgl. www.surfer-haben-rechte.de/cps/rde/xchg/digitalrechte/hs.xsl/1479.htm).

13. Will die Bundesregierung den immer häufiger auftretenden Angriffen auf Smartphones entgegenwirken?

    a) Wenn ja, wie?

    b) Wenn nein, warum nicht?

Das BSI ist in Kontakt zu Herstellern, Netzbetreibern und Sicherheitsunternehmen, um die Maßnahmen gegen Angriffe auf Smartphones auf verschiedenen Ebenen zu verbessern. Darüber hinaus informiert und sensibilisiert das BSI die Nutzer von Smartphones (vgl. Antwort zu Frage 12).

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?

Große Vertreiber von Apps haben bereits Maßnahmen zur Überprüfung von Apps etabliert. Diese werden kontinuierlich angepasst. Die konkreten Maßnahmen können jedoch nicht national festgelegt werden, da diese Vertreiber ihre Apps weltweit anbieten. Im Übrigen verweise ich auf die Antwort zu Frage 13.

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