Deutscher Bundestag **Drucksache 16/9947**

16. Wahlperiode 09. 07. 2008

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Hartfrid Wolff (Rems-Murr), Gisela Piltz, Christian Ahrendt, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 16/9705 –

Mobiltelefone als Zielobjekt und Spionagewerkzeug

Vorbemerkung der Fragesteller

Vermehrt wird das Thema Mobilfunksicherheit in den Medien diskutiert. Die Zahl der bekannt gewordenen Missbrauchsfälle steigt stetig an. Mittlerweile ist entsprechende „Spionagesoftware“ im Internet allgemein zugänglich. Beispiele hierfür sind das Produkt FlexiSPY und die auf der Seite von „ehebruch24.de angebotenen Mobilfunkortungssysteme. Wird die Software unbemerkt auf fremde Mobilfunkgeräte gespielt, können Unbefugte sich Zugriff auf die dort vorhandenen bzw. eingehenden Daten und Telefonate verschaffen.

1. Welche Maßnahmen wurden seitens der Regierung bislang für die Mobilfunksicherheit ergriffen?

2. Welche Rolle spielt dabei das Bundesamt für Sicherheit in der Informationstechnik?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat Publikationen wie z. B. das Grundschutzhandbuch, Informationsbroschüren und Technische Richtlinien zur Mobilfunksicherheit erstellt, die regelmäßig angepasst werden.

Für die Übertragung eingestufter Informationen sind die Festlegungen der Verschlusssachenanweisung des Bundes (VSA) zu beachten. Daraus ableitend sind je nach Einstufungsgrad dieser Informationen zertifizierte bzw. zugelassene IT-Produkte zu verwenden.

Mit § 109 des Telekommunikationsgesetzes (TKG) sind auch die Mobilfunkdiensteanbieter im Übrigen verpflichtet, u. a. das Fernmeldegeheimnis und personenbezogene Daten sowie Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubten Zugriff zu schützen.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 7. Juli 2008 übermittelt.

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

3. Seit wann ist der Bundesregierung die Spionagesoftware bekannt?

Die Software Flexispy ist der Bundesregierung seit Mitte 2006 bekannt.

4. Wie wird die Mobilfunksicherheit bei Bundeseinrichtungen, insbesondere dem Kanzleramt, den Ministerien und den Sicherheitsbehörden, gewährleistet?

Auf die Antworten zu den Fragen 5 und 6 wird verwiesen.

5. Ist gewährleistet, dass die von den Mitgliedern der Bundesregierung und den Beamtinnen und Beamten des Bundes eingesetzten Mobilfunkgeräte, insbesondere bei den Behörden und Organisationen mit Sicherheitsaufgaben (BOS), keine Spionagesoftware oder Ortungssysteme enthalten?

   Wenn ja, wie?

Handelsübliche mobile Endgeräte bieten keinen den Anforderungen der VSA genügenden Schutz gegen das Einbringen von Schadsoftware. Eingestufte Daten dürfen daher nicht mit diesen Geräten übertragen werden.

Soweit erforderlich stehen in der Bundesverwaltung deshalb vom BSI zugelassene Kryptohandys zur Verfügung.

6. Gibt es für die von Beamtinnen und Beamten des Bundes genutzten Mobilfunkgeräte ein regelmäßiges Kontrollsystem, das verhindert, dass sich Spionage- und Ortungssoftware auf diesen Geräten befindet?

Nein, da dienstlich genutzte, handelsübliche Mobilfunkgeräte nur für nicht eingestufte Inhalte verwendet werden dürfen.

Bei konkreten Verdachtsmomenten auf Schadsoftware erfolgt im Einzelfall eine Geräteprüfung durch das BSI.

7. Inwieweit lässt sich der Verkauf von sog. Spionagesoftware, wie z. B. FlexiSPY, wirksam unterbinden?

Der Verkauf von Computerprogrammen, deren Zweck die Begehung eines strafbaren Ausspähens von Daten (§ 202a StGB) oder Abfangens von Daten (§ 202b StGB) ist, wurde durch das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität vom 7. August 2007 (BGBl. I S. 1786), das am 11. August 2007 in Kraft getreten ist, als Vorbereitung des Ausspähens und Abfangens von Daten (§ 202c StGB) unter Strafe gestellt. Der Missbrauch von Computerprogrammen, die nicht in den Anwendungsbereich von § 202c StGB fallen, kann nach den §§ 202a bzw. 202b StGB strafbar sein.

Der Vertrieb von Spionageprogrammen erfolgt überwiegend aus dem Ausland über das Internet und kann daher nicht wirksam unterbunden werden.

8. Steht die Bundesregierung im Dialog mit Mobilfunkanbietern und -herstellern?

   Wenn ja, was ist Gegenstand des Dialogs, und welche Ergebnisse wurden bislang erzielt?

Das BSI als zentraler IT-Sicherheitsdienstleister des Bundes unterhält diverse Kontakte zu Mobilfunknetzbetreibern und Geräteherstellern. Im Ergebnis dieser Kontakte zur Verbesserung der IT-Sicherheit ist z. B. das Kryptohandy TopSec 700 entstanden.

Die AG Telekommunikation der obersten Bundesbehörden steht im ständigen Dialog mit den Mobilfunkbetreibern. Sie wird sich dafür einsetzen, dass Daten zur Lokalisierung von Handys nicht herausgegeben werden, so dass Ortungsmöglichkeiten ausgeschlossen werden.

Auf die Pflichten gemäß § 109 TKG wird hingewiesen.

9. Findet zum Thema Mobilfunksicherheit Aufklärungsarbeit seitens der Regierung oder der Unternehmen gegenüber der Bevölkerung statt?

   Wenn ja, in welchem Maße?

   Wenn nein, ist sie geplant, und in welcher Form?

Ja. Auf den Portalen www.bsi.de und www.bsi-fuer-buerger.de werden umfangreiche Informationen zum Thema IT-Sicherheit inklusive Mobilfunksicherheit für die Wirtschaft und die Bürger bereitgestellt sowie regelmäßig überarbeitet.

Gemeinsam mit Unternehmen, Branchenverbänden, Vereinen und einer Hochschule hat die Bundesregierung zudem den Verein „Deutschland sicher im Netz“ gegründet, der darauf abzielt, Bürger und Unternehmen noch stärker als bisher für den sicheren Umgang mit Informationstechnik zu sensibilisieren und gegenseitige Verantwortung aufzuzeigen.

10. Wird auf dem Sektor der Mobilfunksicherheit Forschung betrieben?

    Wenn ja, durch wen, und mit welchen bisherigen Ergebnissen?

Ja. Das BSI kooperiert auf dem Sektor Mobilfunksicherheit im Rahmen diverser Studien mit unterschiedlichen Universitäten und forschungsnahen Einrichtungen.

Die Erforschung von Sicherheitsfragestellungen für den Endnutzer bei Mobilfunkzugangstechnologien war bisher kein Gegenstand der Projektförderung des Bundesministeriums für Bildung und Forschung (BMBF).

Im Forschungs- und Entwicklungs-Programm „Informations- und Kommunikationstechnologien 2020“ des BMBF, das im Jahr 2007 gestartet wurde, wird nunmehr besonderes Gewicht auf die Forschung zur IT-Sicherheit gelegt.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Amsterdamer Str. 192, 50735 Köln, Telefon (02 21) 97 66 83 40, Telefax (02 21) 97 66 83 44
ISSN 0722-8333