Deutscher Bundestag **Drucksache 17/1072**

17. Wahlperiode 17. 03. 2010

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Jan Korte, Ulla Jelpke, Wolfgang Neskovic, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 17/864 –

Sicherheit im Mobilfunk

Vorbemerkung der Fragesteller

Nachdem das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Juli 2009 gewarnt hatte, dass die „Kommunikation mit GSM-Mobiltelefonen […] ohne hinreichende Sicherheitsmaßnahme als unsicher anzusehen“ sei, schloss das Bundesbeschaffungsamt mit den drei deutschen Firmen Secusmart, Rohde & Schwarz sowie T-Systems Großaufträge für die Ausstattung von Bundesbeamten mit sicheren Handys ab (heise online am 29. Oktober 2009). Die drei Rahmenverträge sollen „tausende Handys“ und „mehrere Millionen Euro“ umfasst haben. Das Geld stamme aus dem Konjunkturpaket II, in dem 500 Mio. Euro für Informationstechnik reserviert waren. Insgesamt seien 21 Mio. Euro für Krypto-Handys ausgegeben worden, wovon mehr als die Hälfte T-Systems für seine Simko2-Geräte eingenommen habe (ebenda).

Auch der Chaos Computer Club (CCC) hält es nicht mehr für verantwortbar, sensible Informationen über Mobiltelefone im GSM-Netz als Gespräch oder Kurznachricht auszutauschen. (Quelle: 26. Chaos Communication Congress (26C3) vom 27. bis 30. Dezember 2009 in Berlin).

Der 20 Jahre alte Verschlüsselungsalgorithmus, der von über 200 Mobilnetzen weltweit eingesetzt und von der Industrievereinigung der GSM-Mobilfunkanbieter (GSMA) vertreten wird, sei auf dem 26C3 ohne großen finanziellen oder technischen Aufwand gehackt worden.

Die meisten der Verschlüsselungslösungen für Smartphones seien allerdings nutzlos, berichtet der Newsletter „Sichere Kommunikation“ (Ausgabe 02/10). Zu diesem Schluss komme zumindest der in der Szene bekannte Hacker Notrax in seinem Blog (http://infosecurityguard.com). Er habe 16 Tools unter die Lupe genommen und bislang 12 davon knacken können. Unter den „gehackten“ sei nach eigenen Angaben auch die SecuVoice-Lösung des Düsseldorfer Anbieters Secusmart. Lediglich an drei Varianten habe sich der IT-Security-Experte bislang die Zähne ausgebissen, er weise jedoch ausdrücklich darauf hin, dass eine durch ihn nicht gefundene Schwachstelle nicht bedeute, dass ein Produkt auch wirklich sicher sei.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 16. März 2010 übermittelt.

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

1. Hat die Bundesregierung Kenntnis von dem erfolgreichen Angriff auf den GSM-Algorithmus, und wenn ja, wie bewertet sie diesen?

Aktive und passive Angriffsverfahren auf die GSM-Luftschnittstelle (Global System for Mobile) sind der Bundesregierung seit langem bekannt. Für ein missbräuchliches Abhören bedurfte es jedoch bisher eines erheblichen finanziellen und technischen Aufwandes. Auf dem 26. Chaos Communication Congress (26C3) vom 27. bis 30. Dezember 2009 wurde in Berlin nun ein neues Projekt zum passiven Angriff auf den GSM-Verschlüsselungsstandard dargestellt. Die Projektergebnisse und damit der erfolgreiche Angriff des GSM-Algorithmus sind realistisch und dahingehend zu bewerten, dass ein missbräuchliches Abhören nunmehr deutlich einfacher und erstmals ohne großen finanziellen/technischen Aufwand möglich ist.

2. Wird die Bundesregierung Konsequenzen aus dem erfolgreichen Angriff auf den GSM-Algorithmus ziehen?

   Wenn ja, wie sehen diese aus?

   Wenn nein, warum nicht?

Als Konsequenz des erfolgreichen Angriffs auf den GSM-Algorithmus verstärkt die Bundesregierung ihre bereits seit geraumer Zeit abgegebene Empfehlung, für die sensible mobile Kommunikation Krypto-Handys zu nutzen. Die mobile Kommunikation der Bundesregierung wird daher bereits mit Krypto-Handys abgesichert.

3. Ist der Bundesregierung bekannt, dass Kritik am GSM-Verschlüsselungsalgorithmus bereits kurz nach seiner Einführung laut wurde, und wie hat sie gegebenenfalls auf den Vorwurf der mangelnden Sicherheit reagiert?

Die Kritik am GSM-Verschlüsselungsalgorithmus war der Bundesregierung bekannt, beispielsweise durch konkrete Beschreibungen von Lauschangriffen in der Fachliteratur. Die Bundesregierung wies auf die Gefahren u. a. im Rahmen der Öffentlichkeitsarbeit und in Informationsbroschüren hin. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfahl bereits zu diesem Zeitpunkt für die sichere mobile Sprachkommunikation den Einsatz von Krypto-Handys.

4. Wird die Bundesregierung die GSMA auffordern, entsprechende Schritte einzuleiten, den gebrochenen Standard durch einen zeitgemäßeren und sicheren auszutauschen?

   Wenn nein, warum nicht?

GSM-Mobilfunkgeräte fallen in den Anwendungsbereich der Richtlinie 1999/05/EG. Artikel 3 der Richtlinie legt die grundlegenden Anforderungen für alle hiervon erfassten Geräte fest. Diese enthalten keine Anforderungen an die Verschlüsselung von Funkverbindungen. Die EU-Mitgliedstaaten können keine nationalen Regelungen schaffen, die über die grundlegenden Anforderungen der Richtlinie hinausgehen. Insofern hat die Bundesregierung keinen direkten Einfluss auf die Standardisierung. Das Bundesministerium für Wirtschaft und Technologie wird jedoch prüfen, inwieweit auf EU-Ebene ein sichererer Standard gefördert werden kann.

5. Hat die Bundesregierung zur Sicherung ihrer eigenen mobilen Kommunikation entsprechende Handys angeschafft, und wenn ja, welchen Umfang hatte die Anschaffung, und aus welchen Mitteln wurde sie bestritten (bitte nach Auftragnehmer, Anzahl, Modell, Verschlüsselungssoftware, Kosten und jeweiligen Empfängern aufschlüsseln)?

Für die sichere mobile Kommunikation setzt die Bundesregierung technische Lösungen ein, die vom BSI zugelassen sind. Derzeit verfügen die Produkte TopSec Mobile der Firma Rohde & Schwarz SIT und Secuvoice der Firma Secusmart über eine Zulassung bis VS-NfD. Die Produkte bestehen aus von der jeweiligen Herstellerfirma entwickelter Soft- und Hardware.

Mit Mitteln des IT-Investitionsprogramms im Rahmen des „Gesetzes zur Sicherung von Beschäftigung und Stabilität in Deutschland“ beschaffte die Bundesregierung bisher 499 TopSec Mobile und 1 500 Secuvoice zur Sicherung der mobilen Sprachkommunikation und Ablösung von Altgeräten. Die ressortweise Verteilung der Geräte ist unterer Tabelle zu entnehmen. Die Ausstattung nachgeordneter Behörden und konkreter Empfänger erfolgt in eigener Zuständigkeit der Ressorts, zentrale Vorgaben bestehen nicht.

	Secuvoice, Firma Secusmart	**TopSec Mobile, Firma Rohde & Schwarz**
AA	90	
BK	140	75
BMAS	30	
BMBF	5	
BMF	140	
BMFSFJ	8	
BMG	80	
BMI	500	203
BMJ	50	
BMU	50	
BMVBS	50	
BMVg	142	200
BMWi	175	5
BMZ	6	
BPA	2	10
BPrA	12	6
BRH	10	
BT	10	

Ergänzend werden aus der Maßnahme noch rund 3 250 zusätzliche Geräte beschafft und auch weiteren Bundesministerien und Behörden bereitgestellt. Die Kosten pro Stück betragen für TopSec Mobile ohne kompatibles Mobilfunkgerät 1 260 Euro netto, für Secuvoice ohne kompatibles Mobilfunkgerät 1 200 Euro netto.

6. Hat die Bundesregierung Kenntnis davon, dass die angeblich abhörsicheren Secusmart-Handys gehackt wurden?

   Wenn ja,

   a) seit wann weiß die Bundesregierung davon,

   b) sind eventuell auch andere von der Bundesregierung angeschaffte Krypto-Handys von den erfolgten Hacks betroffen, und wenn ja, welche (bitte nach Anzahl, Modell, Verschlüsselungssoftware, Kosten und jeweiligen Empfängern aufschlüsseln),

   c) welche Maßnahmen hat sie diesbezüglich ergriffen?

Die Bundesregierung erhielt am 29. Januar 2010 Kenntnis von einem anonymen Internetbeitrag über die angeblich erfolgreiche Schadsoftware-Installation auf einem Secuvoice-Handy. Das BSI informierte die IT-Sicherheitsbeauftragten der Bundesverwaltung über die Meldung sowie über bei der mobilen Kommunikation grundsätzlich notwendigen Sicherheitsmaßnahmen.

Versuche und Analysen konnten die behaupteten Angriffe nicht verifizieren. Das BSI bewertet Secuvoice und TopSec Mobile weiterhin als sicher, die erteilte Zulassung bis VS-NfD gilt uneingeschränkt.

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