

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Matthias Büttner, Andreas Mrosek, Frank Pasemann, Martin Reichardt und der Fraktion der AfD
– Drucksache 19/3676 –

Verschlüsselung von Patientendaten bei Rettungsdiensten

Vorbemerkung der Fragesteller

Einem starken Datenschutz muss nach Auffassung der Fragesteller in Zeiten der Digitalisierung und der damit einhergehenden einfacheren Verbreitung und Missbrauch von sensiblen Daten ein hoher Stellenwert eingeräumt werden.

Nach Auffassung der Fragesteller ist es die Aufgabe der Behörden, hier eine Vorreiterrolle zu übernehmen und den restlichen Gesellschaftsbereichen vorzuleben, wie Datenschutz so sicher und einfach wie nötig und möglich umgesetzt werden kann.

In Bezug auf das E-Health-Gesetz heißt es im Koalitionsvertrag zwischen CDU, CSU und SPD für die 19. Legislaturperiode „Grundlagen für den sicheren Austausch sensibler Daten und Informationen sowie die digitale Patientenakte sind eine verlässliche und vertrauenswürdige Telematikinfrastruktur und höchste Datenschutz- und Datensicherheitsstandards“ und „Es wird sichergestellt, dass die Datenspeicherung den strengen Anforderungen des Datenschutzes unterliegt. Die gespeicherten Daten sind Eigentum der Patientinnen und Patienten.“

Nicht nur die Speicherung der Daten muss sicher erfolgen, auch die Übertragung sensibler Daten muss so gestaltet sein, dass Dritte diese nicht unverschlüsselt auslesen können. In einem Artikel auf golem.de (www.golem.de/news/behoerdenfunk-patientendaten-von-rettungsdiensten-ungeschuetzt-im-internet-1807-135622.html) wird berichtet, dass im Landkreis Recklinghausen „Funksprüche von Rettungsdiensten mit Namen und Adressen von Betroffenen [...] über ein unverschlüsseltes Protokoll namens Pocsag verschickt werden.“ Weiter führt der Artikel aus: „Doch im öffentlichen Bereich wird Pocsag nach wie vor eingesetzt – und das oft unverschlüsselt.“ Im Artikel wird weiterhin auf einen Bericht des NDR verlinkt (www.ndr.de/der_ndr/presse/mitteilungen/Datenleck-Hamburger-Feuerwehr-sendet-unverschluesst-sensible-Personendaten,presse-meldungndr17688.html), aus dem Jahr 2016, in dem ein ähnliches Datenleck in Hamburg gefunden wurde.

Vorbemerkung der Bundesregierung

Die Bundesregierung unterstreicht ausdrücklich den hohen Stellenwert des Datenschutzes insbesondere im hier vorliegenden Bereich der Gefahrenabwehr. Aus diesem Grund betreibt die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS), finanziert von Bund und Ländern, den abhörsicheren Digitalfunk BOS.

Der Digitalfunk BOS ist das bundesweit einheitliche digitale Sprech- und Datenfunksystem für die Einsatzkräfte von Polizeien und Feuerwehren, Rettungskräften sowie Katastrophen- und Zivilschutzbehörden von Bund, Ländern und Kommunen.

Der Betrieb des Digitalfunks BOS erfolgt gemeinsam mit Bund und Ländern. Die BDBOS übernimmt hierbei die Gesamtkoordination und treibt die Weiterentwicklung des Funknetzes gemäß den Anforderungen der Nutzer voran.

Mit den derzeit über 4 600 Basisstationen werden rund 99 Prozent der Fläche der Bundesrepublik Deutschland abgedeckt und die Kommunikation der Einsatzkräfte im Alltag und in Großlagen gesichert. Beim BOS-Digitalfunknetz handelt es sich somit um das weltweit größte und mit einer Verfügbarkeit von 99,97 Prozent zugleich zuverlässigste Digitalfunknetz seiner Art.

Die Anzahl der im Digitalfunk BOS registrierten Nutzer steigt weiter an. Derzeit sind es über 800 000 Nutzer, davon rund 517 000 aus nichtpolizeilichen Organisationen. Pro Monat werden mit dem BOS-Digitalfunk über 50 Mio. Funksprüche abgewickelt und ca. 300 Millionen Kurznachrichten versandt.

Neben der sicheren, hochverfügbaren Sprachkommunikation realisiert das BOS-Digitalfunknetz eine schmalbandige Datenkommunikation. Sie ermöglicht beispielsweise die Alarmierung von Einsatzkräften der Rettungsdienste.

In den vom Fragesteller angeführten Beispielen aus Hamburg und Recklinghausen wurde jedoch nicht der Digitalfunk BOS, sondern das unverschlüsselte Protokoll POCSAG genutzt.

1. In welchen Kommunen und Gemeinden werden nach Kenntnis der Bundesregierung unverschlüsselte Systeme für den Behördenfunk (Feuerwehr, Rettungsdienste, Katastrophenschutz etc.) verwendet?

Über den Einsatz von unverschlüsselten Systemen auf Ebene der Kommunen und Gemeinden liegen der Bundesregierung keine Informationen vor.

2. In welchen Kommunen und Gemeinden werden nach Kenntnis der Bundesregierung verfälschte Informationen im Behördenfunk als Datenschutzmaßnahme in den Nachrichten genutzt?

Dazu liegen der Bundesregierung keine Informationen vor.

3. Wer ist für den Datenschutz im Behördenfunk zuständig?

Welche Protokolle werden für den Behördenfunk in Deutschland genutzt?

Die Nutzung des Digitalfunks erfolgt durch Nutzer auf Ebene von Bund, Ländern und Kommunen. Jeder dieser Akteure ist für den im jeweiligen Zuständigkeitsbereich liegenden Datenschutz im Digitalfunk BOS verantwortlich.

Die BDBOS ist verantwortlich für die Verarbeitung personenbezogener Daten, die im Zusammenhang mit dem Betrieb des Digitalfunks stehen. Dies betrifft insbesondere die Verarbeitung von Verkehrsdaten, die bei der Erbringung des Telekommunikationsdienstes im Digitalfunk BOS entstehen.

4. Welche Protokolle empfiehlt die Bundesregierung, um Datenschutz zu gewährleisten?

Ein wesentlicher Vorzug des Digitalfunks BOS ist die Abhörsicherheit. Der TETRA-Standard beinhaltet als Sicherheitsfunktion bereits eine Luftschnittstellenverschlüsselung. Die genutzte Verschlüsselung basiert auf dem TETRA Encryption Algorithms (TEA-2). Diese schützt den Übertragungsabschnitt zwischen mobilem Endgerät und Basisstation. Sie gewährleistet jedoch keinen Schutz für die dahinter liegende Netzinfrastruktur. Aus diesem Grund wird der Funkverkehr im Digitalfunk BOS durch den Einsatz einer sogenannten Ende-zu-Ende-Verschlüsselung zusätzlich geschützt. Diese Technik stellt die Verschlüsselung des Funkverkehrs vom sendenden Endgerät über die gesamte Netzinfrastruktur hinweg zum empfangenden Endgerät sicher.

5. Welche Maßnahmen sind von der Bundesregierung geplant, um den Datenschutz im Behördenfunk zu stärken?

Mit dem von der Bundesregierung geplanten Entwurf eines Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 sollen entsprechend den europäischen Vorgaben der Datenschutz der Nutzerinnen und Nutzer des Digitalfunks BOS an die neue Rechtslage angepasst werden.

6. Welche Fördermaßnahmen der Bundesregierung bestehen, um den Datenschutz im Behördenfunk zu stärken?

Grundsätzlich dienen alle Maßnahmen zur Sicherung des Digitalfunks BOS an sich zugleich auch der Erhöhung des Datenschutzniveaus. Daher sind derzeit keine dedizierten Förderungsmaßnahmen geplant.

7. Können Kommunen Fördergelder im Rahmen der Digitalisierung abrufen, um den Behördenfunk zu verschlüsseln?

Wenn ja, wie viele Kommunen haben Fördergelder für die Verschlüsselung ihres Behördenfunks

- a) beantragt und
- b) ausgezahlt bekommen?

Da der verschlüsselte Digitalfunk BOS gemeinsam von Bund und Ländern finanziert wird, erübrigt sich die Bereitstellung von Fördergeldern für Verschlüsselungen.

8. Welche Maßnahmen wurden seitens der Bundesregierung seit 2016 getroffen, als das Problem durch den Vorfall in Hamburg bekannt geworden ist?

Der Digitalfunk BOS steht als sicheres Sprech- und Datenfunksystem bundesweit zur Verfügung. Daher waren neben der Bereitstellung des Digitalfunk BOS aus Sicht der Bundesregierung keine weiteren Maßnahmen erforderlich.

9. Welche Fälle sind der Bundesregierung bekannt, in denen es zu Datenlecks im Behördenfunk gekommen ist?

Wie hat die Bundesregierung von diesen Datenlecks Kenntnis erhalten?

Der Bundesregierung sind keine Datenlecks im Digitalfunk BOS bekannt.

10. Wird das Bundesamt für Sicherheit in der Informationstechnik (BSI) standardmäßig informiert, wenn es zu Vorfällen dieser Art kommt?

Wie ist die Vorgehensweise?

Das BSI fungiert als Nationale Meldestelle für IT-Sicherheitsvorfälle und hat zu diesem Zweck Meldewege u. a. mit Bundesbehörden, Landesbehörden und Unternehmen etabliert. Je nach Vorfall erhält das BSI auch Meldungen von Sicherheitsforschern, Journalisten oder Kunden. Das BSI unterstützt dann die Betroffenen im Rahmen seiner Zuständigkeit bei der Herstellung eines sicheren Betriebszustandes.

Bevor ein Sicherheitsvorfall an das BSI gemeldet wird, muss dieser jedoch erst festgestellt werden. Beim Abhören von unverschlüsselten Nachrichten, die mittels POCSAG-Protokoll übermittelt werden, ist dies selten der Fall. Sollte das BSI, wie im auf Golem geschilderten Fall, Kenntnis von öffentlich zugänglichen Sammlungen von sensiblen Daten erlangen, nutzt es die etablierten Kanäle, um den Vorfall zu beheben.

11. Welche Maßnahmen oder Hilfestellungen ergreift die Bundesregierung, und über welche Behörden, sobald sie Wissen von einem Datenleck erhält?

Die Maßnahmen und Hilfestellungen würden im Rahmen der sog. Sicherheitsvorfallbearbeitung erfolgen. Dies bedeutet im Grundsatz die sofortige Ergreifung von technischen Gegenmaßnahmen, falls ein Datenabfluss durch technische Fehleinstellungen oder Manipulationen erfolgt wäre. Würden bei Log-Datenauswertungen Abweichungen mit Hinweis auf unbekannte Datenverkehre festgestellt werden, würden ebenfalls konkrete Untersuchungen an den betroffenen Baugruppen bzw. Netzelementen erfolgen.