Deutscher Bundestag **Drucksache 20/7420**

20. Wahlperiode 22.06.2023

Antwort

der Bundesregierung

auf die Kleine Anfrage der Fraktion der CDU/CSU
– Drucksache 20/7135 –

Sicherheitslücken im Mobilfunknetz

Vorbemerkung der Fragesteller

Am 11. Mai 2023 berichtete das Nachrichtenmagazin „DER SPIEGEL“ über Sicherheitslücken im Mobilfunknetz, die für das gezielte Ausspionieren und die Überwachung von Menschen missbraucht werden könnten (www.spiegel.de/netzwelt/handy-spaehattwie-ein-schweizer-it-unternehmer-weltweite-ueberwachung-ermoeglicht-a-f252d8e2-5697-42c8-8b75-bee73fb4eaa5). Die Schwachstellen lägen demnach im Signalling System 7 (Signalisierungssystem Nummer 7 – SS7), welches die weltweite Zustellung von Anrufen und SMS zwischen verschiedenen Komponenten von Mobilfunknetzen ermöglicht. Jedoch würden SS7-Angriffe auch für das Hacken von Telegram-Konten, Airbnb-Accounts und E-Mail-Postfächer genutzt. Laut Recherchen des „DER SPIEGEL“ stelle insbesondere das Schweizer IT-Unternehmen Fink Telecom Services Cyberkriminellen die dafür entscheidende Infrastruktur zur Verfügung. Inzwischen hat der internationale Verband der Mobilfunkunternehmen (GSMA) Telefonunternehmen dazu geraten, die Zugänge dieses Unternehmens ins Netz zu kappen (www.spiegel.de/netzwelt/netzpolitik/andreas-fink-mobilfunkverband-geht-gegen-schweizer-ss7-dienstleister-vor-a-d012c1dd-afb7-4ead-9571-59653abc17e1). Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnte vor „Schwachstellen in der SS7-Signalisierung“ (S. 40, www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?__blob=publicationFile&v=3).

1. Wie beurteilen die Bundesregierung aktuell, insbesondere das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Bundesnetzagentur, die Einschätzung des „DER SPIEGEL“, wonach „gravierende Schwachstellen im internationalen Mobilfunknetz“ vorliegen (www.spiegel.de/netzwelt/handy-spaehattwie-ein-schweizer-it-unternehmer-weltweite-ueberwachung-ermoeglicht-a-f252d8e2-5697-42c8-8b75-bee73fb4eaa5)?

   a) Gibt es aus Sicht des Bundesministeriums für Digitales und Verkehr (BMDV) Handlungsbedarf, und wenn ja, welchen?

   b) Gibt es aus Sicht des BSI Handlungsbedarf, und wenn ja, welchen?

   c) Gibt es aus Sicht der Bundesnetzagentur Handlungsbedarf, und wenn ja, welchen?

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Digitales und Verkehr vom 21. Juni 2023 übermittelt.

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

7. Welche Sicherheitsmaßnahmen, wie etwa Plausibilitäts-Checks und die Nutzung von SS7-Firewalls, ergreifen die Mobilfunkbetreiber in Deutschland nach Kenntnis der Bundesregierung, um SS7-Attacken zu verhindern?

9. Wie bewerten die Bundesregierung, insbesondere das BSI und die Bundesnetzagentur, die Effektivität dieser Maßnahmen zur Verhinderung von SS7-Attacken?

10. Was hat die Bundesnetzagentur bisher getan, um eine Ausnutzung von SS7-Schwachstellen in Deutschland zu verhindern?

11. Wie unterstützen die Bundesregierung, insbesondere das BSI und die Bundesnetzagentur, Mobilfunkprovider und weitere Unternehmen bei der Prävention von SS7-Attacken?

12. Welche Planungen bestehen nach Kenntnis der Bundesregierung in der Branche zur Ablösung des SS7-Protokolls, und inwiefern unterstützen das BSI und die Bundesnetzagentur eine Ablösung des SS7-Protokolls?

Die Fragen 1, 7 und 9 bis 12 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Nach Kenntnis der Bundesregierung sind den deutschen Mobilfunknetzbetreibern die Schwachstellen der SS7-Signalisierung – auch aufgrund entsprechender Hinweise des Bundesamtes für Sicherheit in der Informationstechnik (BSI) – bekannt. Sie haben Sicherheitsvorkehrungen getroffen, um das Risiko im Zusammenhang mit SS7 zu reduzieren. Diese Vorkehrungen werden regelmäßig überprüft und soweit notwendig angepasst.

Die Bundesnetzagentur (BNetzA) hat im Einvernehmen mit dem BSI und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) einen Katalog von Sicherheitsanforderungen erstellt, der den Betreibern und Anbietern Schutzmaßnahmen und sonstige Vorkehrungen empfiehlt, um u. a. SS7-Attacken und deren Auswirkungen zu minimieren.

Die BNetzA prüft im Rahmen der Überprüfung des Sicherheitskonzepts nach § 166 des Telekommunikationsgesetzes (TKG) und dessen Umsetzung auch, ob die Betreiber entsprechende Maßnahmen ergriffen haben, um Gefährdungen durch SS7 zu minimieren.

Darüber hinaus ist das BSI in diesem Zusammenhang in der GSM Association (GSMA) tätig und berät die Arbeitsgruppen der GSMA zur Förderung der Sicherheit in Hinblick auf die Signalisierungsinfrastruktur der Mobilfunknetze, inklusive SS7. Bekannte Angriffe können mit speziellen SS7-Firewalls erkannt und abgewehrt werden. Hierzu befindet sich das BSI mit Unternehmen im Austausch.

Eine Weiterentwicklung des internationalen Mobilfunkstandards könnte die Sicherheit weiter erhöhen. Die Bundesregierung setzt sich hierfür aktiv ein. Unter anderem beteiligt sich das BSI an den laufenden Aktivitäten zu den Signalisierungsprotokollen für das 5G-Roaming, welche langfristig das SS7-Protokoll ablösen werden.

Nach Kenntnis der Bundesregierung wird das SS7-Protokoll in näherer Zukunft voraussichtlich nicht vollständig abgelöst, da es in absehbaren Zeiträumen einen Bedarf geben wird, Inbound- sowie Outbound-Roamer in 2G-Netzen mit Mobilfunk zu versorgen. Es wird erwartet, dass das SS7-Netz schrittweise kleiner wird. Für das 5G Roaming wurde bereits eine Lösung standardisiert, die langfristig das SS7 Protokoll ablösen wird. Weitere Verbesserungen daran sind

aktuell in Diskussion und Arbeit, die von der BNetzA begleitet und unterstützt werden.

2. In welchem Umfang fanden nach Kenntnis der Bundesregierung, insbesondere des BSI, SS7-Attacken in Deutschland statt (bitte für die Jahre 2021 und 2022 aufführen)?

   In welchem Umfang wurden dabei Aufenthaltsdaten von Nutzern erspäht und Gespräche und Textnachrichten abgefangen?

   In welchem Umfang wurden dabei insbesondere Accounts von Online-Plattformen und Messenger-Apps, E-Mails-Accounts gehackt und Zugang zu Bankkonten erlangt?

Es wird auf die im Internet veröffentlichten Informationen auf der Webseite des BSI verwiesen, abrufbar unter:

www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Smishing_SMS-Phishing_141021.html.

Darüber hinaus liegen der Bundesregierung keine eigenen Informationen vor.

3. In welchem Umfang fanden nach Kenntnis der Bundesregierung SS7-Attacken in Deutschland durch SS7-Zugänge ausländischer Mobilfunkbetreiber statt (bitte für 2021 und 2022 angeben)?

Hierzu liegen der Bundesregierung keine eigenen Informationen vor.

4. War nach Kenntnis der Bundesregierung Fink Telecom Services auch in Deutschland tätig, und sind Zusammenhänge zur illegalen Ausnutzung von SS7-Aktivitäten bekannt?

Das genannte Unternehmen ist nicht nach § 5 TKG als Betreiber öffentlicher Telekommunikationsnetze oder Betreiber öffentlich zugänglicher Telekommunikationsdienste gemeldet. Darüber hinaus liegen der Bundesregierung keine eigenen Informationen vor.

5. Welche Unternehmen in Deutschland bieten nach Kenntnis der Bundesregierung Drittunternehmen und Privatpersonen Zugänge über das SS7-Protokoll an?

6. Für welche Dienstleistungen nutzen diese Drittunternehmen nach Kenntnis der Bundesregierung Zugänge zum SS7-Protokoll?

Die Fragen 5 und 6 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Hierzu liegen der Bundesregierung keine eigenen Informationen vor.

8. Welche Sicherheitsmaßnahmen ergreifen in Deutschland Online-Plattformen, Messenger-Apps, E-Mail-Provider, Banken und weitere Unternehmen, um SS7-Attacken zu verhindern?

Die Verhinderung von SS7-Angriffen liegt nicht im Einflussbereich von Online-Plattformen, Messenger-Apps, Email-Providern und Banken.

Zur Vermeidung von Gefährdungen bei der Nutzung von SMS-basierten Authentisierungsverfahren werden alternative Verfahren zur Multifaktor-Authentisierung angeboten:

- bei Online-Plattformen und E-Mail-Provider sind dies u. a. softwarebasierte Verfahren wie „Time-based one-time password“ (TOTP),
- bei Messenger-Apps (z. B. Signal, WhatsApp) PINs für die Verifizierung in zwei Schritten,
- bei Banken sowohl software- als auch hardwarebasierte Verfahren (insbesondere PushTAN und chip-TAN),
- und bei weiteren Unternehmen (z. B. Versicherungen) hardwarebasierte Verfahren (z. B. Personalausweis).

Sofern Anbieter keiner besonderen Regulierung unterliegen (z. B. PSD2-Richtlinie), sind diese derzeit nicht verpflichtet, grundsätzlich eine Multifaktor-Authentisierung oder eine Alternative zu einer bestehenden Multifaktor-Authentisierung zur Verfügung zu stellen.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, 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