

Kleine Anfrage

der Abgeordneten Matthias Büttner, Andreas Mrosek und der Fraktion der AfD

Nationale Sicherheit und digitale Infrastruktur

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

Die Fragesteller vertreten die Ansicht, dass bei sensibler Netzinfrastruktur sicherzustellen ist, dass die digitale Souveränität gewahrt bleibt. Nach Ansicht der Fragesteller gehört Telekommunikation (unter anderem Mobilfunk- und Glasfasernetze) zur kritischen Infrastruktur des Landes. Die australische Regierung ist hier der Ansicht, dass es mit der nationalen Sicherheit nicht vereinbar ist, Mobilfunkkomponenten von Huawei Technologies Co. Ltd. und ZTE Corp in ihrem 5G-Mobilfunknetz zu verbauen. Laut der „IT-TIMES“ sind Regierungsvertreter in Beijing verärgert und bezeichnen das Vorgehen als schlechte Ausrede, ein chinesisches Unternehmen vom Markt gänzlich auszuschließen (www.it-times.de/news/australien-sperrt-huawei-und-zte-als-5g-technologie-lieferanten-nokia-und-ericsson-durfte-das-freuen-129629/).

Die australische Regierung teilt in ihrer Pressemitteilung mit, dass sie die nationalen Sicherheitsrisiken in Bezug auf 5G-Netze intensiv geprüft hat und dass 5G hier Änderungen benötigt im Vergleich zu früheren Mobilfunknetzen (www.minister.communications.gov.au/minister/mitch-fifield/news/government-provides-5g-security-guidance-australian-carriers).

Vor Australien hatten bereits die Vereinigten Staaten von Amerika Huawei und ZTE von ihrem 5G-Ausbau ausgeschlossen (www.focus.de/digital/handy/nach-den-usa-australien-verbietet-zte-und-huawei-5g-ausbau_id_9474378.html).

Alle drei großen in Deutschland tätigen Mobilfunk- und Internet-Service-Provider setzen überwiegend aus dem Ausland eingekaufte Produkte ein, die sie nur an der Oberfläche verstehen können (www.techrepublic.com/blog/it-security/researchers-create-nearly-undetectable-hardware-backdoor/). Ein Zugriff auf alle spezifischen Hardwarekomponenten oder auf die Firmware ist nur durch den Systemhersteller möglich. Nach Kenntnis der Fragesteller bestehen seitens Mitarbeitern der Deutschen Telekom AG Bedenken, dass im Mobilfunk mehr als zwei Drittel der Technikprodukte von Huawei zum Einsatz kommen und beim 5G-Ausbau Huawei ebenfalls den Löwenanteil erhalten wird. Nach Kenntnis der Fragesteller dürfte bei anderen Providern die Größenordnung ähnlich, eher noch höher sein (www.wiwo.de/unternehmen/it/huawei-aufstieg-mit-spionage/21115020.html).

Wir fragen die Bundesregierung:

1. Gehören für die Bundesregierung Mobilfunk- und Glasfasernetze zu den sicherheitskritischen Infrastrukturen?

2. Hat die Bundesregierung eine umfassende Überprüfung der nationalen Sicherheitsrisiken für 5G-Netze durchgeführt?

a) Wenn ja:

Welche Tätigkeiten wurden durchgeführt (bitte nach Datum und Behörde listen)? Welchen Einfluss hatten die Ergebnisse der Tätigkeiten auf die 5G-Strategie der Bundesregierung? Welche konkreten Maßnahmen wurden auf Grund der Überprüfungen getroffen? Welchen Einfluss hatten die Ergebnisse der Tätigkeiten auf die Glasfaserstrategie der Bundesregierung? Welche konkreten Maßnahmen wurden auf Grund der Tätigkeiten getroffen?

b) Wenn nein:

Warum hat so eine Überprüfung noch nicht stattgefunden? Ist eine Überprüfung in Planung? Wurde die 5G-Strategie der Bundesregierung formuliert, ohne den Aspekt nationale Sicherheit der verbauten Hardwarekomponenten zu beachten? Wurde die Glasfaserstrategie der Bundesregierung formuliert, ohne den Aspekt nationale Sicherheit der verbauten Hardwarekomponenten zu beachten?

3. Teilt die Bundesregierung die Ansicht der australischen Regierung, dass 5G eine Änderung der Funktionsweise der Mobilfunknetze im Vergleich zu früheren Generationen von Mobilfunknetzen darstellt und diese Änderungen die Bedrohungspotentiale für Telekommunikationsnetze erhöhen?

a) Wenn ja:

Welche Maßnahmen hat die Bundesregierung getroffen um die Bedrohungspotentiale zu klassifizieren? Welche Bedrohungspotentiale sieht die Bundesregierung? Wie viele Mitarbeiter der Bundesregierung sind mit dem Aufgabenfeld Bedrohungspotentiale in Bezug auf Telekommunikationsnetze betraut (bitte getrennt nach Behörde listen)?

b) Wenn nein:

Wo weicht die Ansicht der Bundesregierung von der Sicht der australischen Regierung ab?

4. Teilt die Bundesregierung die Ansicht der Regierungsvertreter in Beijing, dass es sich bei der Vorgehensweise der australischen Regierung um eine Ausrede handelt, um chinesische Unternehmen vom Markt auszuschließen?
5. Teilt die Bundesregierung die Ansicht der australischen Regierung, dass es keine Kombination von technischen Sicherheitskontrollen gibt, die die neu auftretenden Risiken ausreichend mildern?

Wenn nein, welche Kombination bzw. Maßnahme wird aus Sicht der Bundesregierung als erfolgreich angesehen?

6. Teilt die Bundesregierung die Ansicht der australischen Regierung, dass die Beteiligung von Hardwareanbietern, die wahrscheinlich außergerichtlichen Anweisungen einer ausländischen Regierung unterliegen, die mit nationalem Recht kollidieren, das Risiko bergen, dass der Netzbetreiber das 5G-Netz nicht ausreichend vor unbefugtem Zugriff oder Eingriffen schützen kann?

a) Wenn ja, welche Schlussfolgerungen, Anweisungen und Maßnahmen ergeben sich daraus für die Bundesregierung und für private Internetunternehmen in Deutschland?

b) Wenn nein, warum nicht?

7. Die Hardware welcher Anbieter für Mobilfunk- und Glasfaserhardware ist nach Kenntnis der Bundesregierung in den Telekommunikationsnetzen in Deutschland verbaut (bitte nach Technik, Prozentzahl und Anbieter listen)?
Wenn nicht beantwortet werden kann, welche Hardware verbaut ist, wie wurde die Überprüfung der Telekommunikationsnetze auf Übereinstimmungen mit den Zielen digitale Souveränität und nationale Sicherheit durchgeführt?
8. Welcher Anbieter von Hardware ist nach Kenntnis der Bundesregierung für den 5G-Ausbau relevant?
9. Welche Hardware welcher Anbieter wird nach Kenntnis der Bundesregierung in den digitalen Testfeldern (www.bmvi.de/DE/Themen/Digitales/Digitale-Testfelder/Digitale-Testfelder.html) genutzt (bitte getrennt nach Projekt auflisten)?
10. Ist die Bundesregierung der Ansicht, dass durch das Verbauen von Hardware des Anbieters Huawei Technologies Co. Ltd. in Glasfasernetzen ein Risiko für die nationale Sicherheit oder digitale Souveränität ausgeht?
11. Ist die Bundesregierung der Ansicht, dass durch das Verbauen von Hardware des Anbieters Huawei Technologies Co. Ltd. in 5G-Mobilfunknetzen ein Risiko für die nationale Sicherheit oder digitale Souveränität ausgeht?
12. Ist die Bundesregierung der Ansicht, dass durch das Verbauen von Hardware des Anbieters ZTE Corp. in Glasfasernetzen ein Risiko für die nationale Sicherheit oder digitale Souveränität ausgeht?
13. Ist die Bundesregierung der Ansicht, dass durch das Verbauen von Hardware des Anbieters ZTE Corp. in 5G-Mobilfunknetzen ein Risiko für die nationale Sicherheit oder digitale Souveränität ausgeht?
14. Gibt es Hersteller von Hardware, bei denen die Bundesregierung der Ansicht ist, dass ein Verbauen ihrer Technologie in Mobilfunk- oder Glasfasernetzen ein Sicherheitsrisiko in Bezug auf die nationale Sicherheit oder digitale Souveränität darstellt (bitte alle betroffenen Hersteller getrennt nach Land listen)?
15. Hat die Bundesregierung geprüft, ein Verbot für die Nutzung von Hardware bestimmter Hersteller beim Aufbau von Mobilfunk-, 5G- und Glasfasernetzen in Deutschland auszusprechen?
 - a) Wenn ja:
War die Prüfung allgemeiner Natur? War die Prüfung konkret auf Hardware einiger Hersteller bezogen?
 - b) Wenn nein:
Ist so eine Prüfung in Planung? Wenn eine Prüfung in Planung ist, wird diese Prüfung allgemeiner Natur sein, oder sich konkret auf Hardware einiger Hersteller beziehen?
16. Die Hardware welcher Hersteller für Mobilfunk-, 5G-, und Glasfaserausbau ist nach Kenntnis der Bundesregierung am preisgünstigsten und würde erwartungsgemäß den Zuschlag bei öffentlichen Ausschreibungen erhalten (bitte nach Herkunft des Herstellers nach Preis aufsteigend listen)?

Berlin, den 5. September 2018

Dr. Alice Weidel, Dr. Alexander Gauland und Fraktion

