PDF

PARTEI DES FORTSCHRITTS

Positionspapier der PdF zur Sicherheit in der kritischen Netzwerkinfrastruktur

1. 5G-Netzausbau und Sicherheitsbedenken

Im Zuge des 5G-Netzausbaus werden zunehmend Sicherheitsbedenken gegen die Verwendung von Komponenten chinesischer Hersteller laut. Nachdem Großbritannien schon 2020 einen Bann gegen 5G-Technik von Huawei verhängt hatte (1), gab es in den USA im November 2022 einen Importstopp für Geräte der Hersteller Huawei, ZTE, Hytera Communications, Hangzhou Hikvision Digital Technology und Dahua Technology (2).

2. Diskussion um Importverbote und Einfluss autoritärer Staaten

Es wird diskutiert, ob man angesichts dieser Verbote generell auch in Deutschland auf Importe von 5G-Komponenten und eventuell generell auf Kommunikationstechnologie aus Staaten mit eingeschränkten demokratischen Strukturen verzichten sollte, da die Herstellerfirmen oft unter dem Einfluss der jeweiligen Regierungen stehen. Erst jüngst wurde z. B. bekannt, dass Geheimdienste aus China systematisch Telekommunikation in USA und anderen Ländern abhören (3).

3. Europäische Kontrollmechanismen und Zertifizierung

Als Reaktion auf solche Sicherheitsrisiken wird zurzeit im europäischen Raum an Kontrollmechanismen gearbeitet. Unter der sperrigen Abkürzung NESAS CCS-GI (Network Equipment Security Assurance Scheme, Cybersecurity Certification Scheme - German Implementation) bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Zertifizierung kritischer Komponenten in der Telekommunikation an, die in Zukunft verpflichtend werden soll (4). Erste Zertifizierungen wurden schon im Jahr 2023 vorgenommen, z. B. wurde der chinesische Hersteller ZTE vom TÜV Nord zertifiziert (5). Es existieren allerdings erst wenige anerkannte Prüfstellen.

An einer allgemeineren Form zur Zertifizierung sogenannter „Trusted Chips“ wird schon seit 2023 auf europäischer Ebene gearbeitet.

4. Unser Standpunkt

Die PdF vertritt angesichts dieser Entwicklungen die Meinung, dass in Zukunft in kritischer Netzwerkinfrastruktur nur Kommunikationskomponenten verwendet werden sollten, wenn diese nach den vorgenannten Verfahren als sicher zertifiziert wurden. Ein pauschales Verbot von Produkten aus bestimmten Herkunftsländern lehnen wir ab. Bei der Zertifizierung sollte auch der gesamte Lebenszyklus des Produktes bewertet werden, inklusive Fehlerkultur und Transparenz im Umgang mit Sicherheitslücken. Außerdem sollten gleiche Zertifizierungsverfahren europaweit gültig sein.

Darüber hinaus sollte die Entwicklung und Produktion zertifizierter Komponenten europäischer Hersteller gezielt gefördert werden, um technologische Souveränität zu stärken und Abhängigkeiten zu verringern. Dies entspricht auch den Zielen des ‚European Chips Act', der eine resistentere europäische Halbleiterindustrie anstrebt.

5. Quellen:

1. 5G: Großbritannien verbietet Huawei-Netzwerktechnik ab September - DER SPIEGEL
   https://www.spiegel.de/netzwelt/netzpolitik/5g-grossbritannien-verbietet-huawei-netzwerktechnik-ab-september-a-b6e296f3-d4b5-4d43-8ece-734c0c5c788d
2. USA verbannen Huawei und ZTE – DW – 26.11.2022
   https://www.dw.com/de/usa-verbannen-huawei-und-zte/a-63895829
3. our telephone networks are cooked.
   https://www.youtube.com/watch?v=tRATnT577Aw&t=41s
4. BSI - Zertifizierung nach NESAS CCS-GI
   https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-NESAS/NESAS-CCS-GI_node.html
5. TÜVIT prüft 5G-Produkt von ZTE erfolgreich nach NESAS - Pressemitteilungen | TÜViT
   https://www.tuvit.de/de/aktuelles/pressemitteilungen/pressemitteilungen-detail/article/tuevit-prueft-5g-produkt-von-zte-erfolgreich-nach-nesas/
6. European Chips Act
   https://digital-strategy.ec.europa.eu/en/policies/european-chips-act