SPD Fraktion im Bundestag

Ein digital souveränes Europa mit sicheren 5G-Netzen

Positionspapier der SPD-Bundestagsfraktion vom 17. Dezember 2019

Wir leben in Zeiten schneller und tiefgreifender Veränderungen. Das gilt nicht nur für technologische, sondern auch für politische Entwicklungen. Wenn wir über digitale Souveränität sprechen, müssen wir diese beiden Aspekte zusammen denken. Umfassende digitale Souveränität kann nur mit einem europäischen Ansatz erreicht werden. Auf einzelstaatlicher Ebene ist digitale Souveränität nicht erreichbar.

Die Diskussion um die digitalen Netze zeigt schon heute die globalen Entwicklungen auf, die uns in Zukunft sehr intensiv beschäftigen werden. Die Beziehungen zwischen den USA und China werden zunehmend konfrontativ. Beide Länder befinden sich in einem Technologiekonflikt, bei dem 5G wohl nur der Anfang ist. Gleichzeitig bezeichnet die EU China mittlerweile als politischen und wirtschaftlichen Systemwettbewerber. Angesichts der neuen geostrategischen Auseinandersetzungen muss sich auch Europa positionieren. Deshalb muss die Frage beantwortet werden, wie Europa seine digitale Souveränität sicherstellen kann, um nicht in ungewollte Abhängigkeiten zu geraten. Digitale Souveränität bedeutet die Fähigkeit, die Hoheit über die Netzwerktechnik des Cyberraums der Europäischen Union zu behalten. Das setzt die industrielle Fähigkeit voraus, kritische digitale Infrastruktur zu schaffen und zu betreiben. Des Weiteren setzt es auch die Fähigkeit voraus, den Zugriff außereuropäischer Mächte auf die kritische Infrastruktur gegenwärtig und zukünftig zu unterbinden. Kaum einer anderen Technologie werden aktuell so weitreichende Veränderungspotentiale für Gesellschaft und Wirtschaft zugeschrieben wie der Einführung von 5G-Mobilfunkangeboten. 5G als digitales Nervensystem wird die mobile Datenübertragung schneller, intelligenter und modularer machen. Dabei ändert sich die Funktionsweise der Netzarchitektur mit 5G im Vergleich zu 4G (LTE) massiv. Ehemals zentrale Funktionen werden deutlich dezentralisiert. Ebenso nimmt die Bedeutung von Softwarekomponenten deutlich zu. Damit wird das Netz eine deutlich höhere Komplexität aufweisen, stärker auf die Identifizierung von Sicherheitslücken und damit auf permanente Software-Aktualisierungen angewiesen sein. Auch „wandert“ die Intelligenz der Netze bis in die Antenne und immer mehr Funktionen aus dem Kernnetz in das Radio-Access-Network (RAN) in der Netzperipherie. Insgesamt ergibt sich damit eine viel größere Angriffsfläche, was insbesondere auch für die Sicherheit nachgelagerter Systeme gilt.

Durch eine schnellere Vernetzung, größere Kapazitäten und den sich daraus ergebenden neuen Anwendungsfällen vertieft sich die Integration der vernetzten Elemente; unabhängig davon, ob es sich um das Internet der Dinge, die industrielle Nutzung, private oder sonstige Nutzungsfälle handelt. Die Daten aus Produktions- und Logistikprozessen der Industrie 4.0 werden damit also genauso übertragen werden, wie der alltägliche Konsum von neuen Inhalten der privaten Nutzerinnen und Nutzer. Wirtschaftliche Geschäftsprozesse aller Art verlaufen vernetzter und auch die Steuerung von Infrastruktur wie z.B. Verkehr oder der Stromerzeugung und -netze wird durch 5G digital erfolgen. Die Digitale Infrastruktur (sowohl festnetz- wie funkbasiert) wird daher zwangsläufig zum Bestandteil der kritischen Infrastruktur Deutschlands.

Damit wird die Sicherheit dieser Netze auch zu einer Frage der nationalen und europäischen Sicherheit, sowie der digitalen Souveränität. Entsprechend muss sichergestellt sein, dass für

diese Netze höchste Sicherheitsanforderungen vorliegen. Hierbei sind grundsätzlich drei Risikokategorien zu identifizieren:

1. Spionage:

Menschen, Unternehmen, Forschungseinrichtungen und die Verwaltung müssen darauf vertrauen können, dass alles Machbare dafür getan wird, damit ihre Daten und Kommunikationswege nicht ausspioniert werden.

2. Manipulation und Sabotage:

Die digitale Infrastruktur ermöglicht neben der persönlichen Kommunikation auch die Steuerung von intelligenten Maschinen und Fahrzeugen sowie die Kommunikation in Krisenfällen. Als kritische Infrastruktur müssen die Netze bestmöglich vor Sabotage geschützt sein. Dies umfasst nicht nur das Risiko eines (tendenziell unwahrscheinlichen) „Kill Switch“ (Abschaltung) sondern vor allem weniger auffällige Szenarien wie das Verlangsamen, Umleiten oder Verändern von Informationsflüssen (Manipulationen).

3. Industriepolitische und technologische Abhängigkeit:

Zur langfristigen Sicherheit gehört auch die Fähigkeit Europas, 5G Netze selbst bauen und betreiben zu können und die Entwicklung künftiger Technologien in diesem Bereich selbst in der Hand zu haben. Es geht um die Rückgewinnung der digitalen Souveränität. Andernfalls entsteht eine technologische Abhängigkeit, die unsere Handlungsspielräume politisch und wirtschaftlich deutlich einschränkt. Anders als in vielen Bereichen haben wir bei 5G noch zwei führende Unternehmen in Europa. Sie besitzen einen standortbedingten Vertrauensvorteil und sollten nicht durch Dumpingpreise vom Markt verdrängt werden können. Hierzu sind erhebliche Investitionen auf europäischer Ebene zwingend notwendig.

Schnelles Entscheiden und konsequentes Handeln sind erforderlich:

Hundertprozentige Sicherheit kann es nie geben. Trotzdem haben wir die gemeinsame Verantwortung, das maximal Mögliche an Sicherheit für die Bürgerinnen und Bürger, den Staat, die Wissenschaft und Wirtschaft sowie die kritische Infrastruktur wie Krankenhäuser, Kraftwerke und Verkehr zu gewährleisten. Wenn Sicherheit nicht garantiert und die Gefährdungen nicht ausgeschlossen werden können, wird die Frage des Vertrauens in die Integrität des Herstellers und in das Rechtssystem des Herstellerlandes zentral. Die Überprüfung der Vertrauenswürdigkeit muss daher wesentlicher Bestandteil der Sicherheitsstrategie sein. Diese Überprüfung der Vertrauenswürdigkeit muss gesetzlich festgeschrieben sowie mit entsprechenden Auflagen versehen werden, sodass Anbieter nur dann zum Zuge kommen, wenn sie diese Vorgaben vollumfänglich erfüllen.

Konkret bedeutet dies aus unserer Sicht:

- Die Entscheidung, wer am Aufbau kritischer Infrastruktur beteiligt werden darf, ist eine politische Frage, die von politisch legitimierten Entscheidungsträgern zu treffen ist. Kurzfristig muss diese Entscheidung auf nationaler Ebene getroffen werden. Die konkrete Verantwortung dafür ist spätestens auf der Grundlage reformierter Gesetze (TKG, IT-Sicherheitsgesetz) zu entscheiden. Außerdem ist eine Entscheidung in Bezug auf die digitale Souveränität auf europäischer Ebene nötig. Auch gegen unzulässige Wettbewerbspraktiken muss auf europäischer Ebene vorgegangen werden, um die digitale Souveränität sicherzustellen.

- Unabhängigkeit und Sicherheit müssen bei der Entscheidung über die Zulassung von 5G Netzwerkanbietern absolute Priorität haben.
- Beim Ausbau des 5G-Netzes sollten nicht-vertrauenswürdige Hersteller – insbesondere dann, wenn nicht-rechtstaatlich kontrollierte Einflussnahme, Manipulation oder Spionage nicht auszuschließen sind – grundsätzlich ausgeschlossen werden (sowohl im Kern- wie im peripheren Netz).
- Für das bestehende Netz ist kein sofortiger Austausch von Hardware nicht-vertrauenswürdiger Hersteller notwendig. Spätestens beim Umstieg auf den neuen Mobilfunkstandard müssen allerdings die Sicherheitsvorgaben zur Anwendung kommen.
- Beim Infrastrukturausbau ist auf eine Diversifizierung im Gesamtnetz sicherzustellen sowie darauf, dass die Hard- & Software verschiedener Hersteller auf offenen Standards basiert, Interoperabilität gewährleistet und Komponenten verschiedener Hersteller miteinander kompatibel sind. In besonders kritischen Bereichen und für entsprechende Anwendungsfälle ist eine Redundanz der Infrastruktur sicherzustellen.
- Die Sicherheitsanforderungen gelten für alle Anbieter gleichermaßen.

Diese Maßnahmen sind erste wichtige Schritte bei der Absicherung des Netzes. Alleine ausreichend und Ersatz für weitere Sicherheitsmaßnahmen wie Zertifizierung, Open-Hardware und fortlaufenden Code-Review, Verschlüsselung und Tätigkeiten der Sicherheitsbehörden sind sie nicht.

Anhang - weitere Informationen zum Hintergrund:

Diskutiert wird derzeit innerhalb der Bundesregierung, dass es zwar keine „Lex Huawei“ und keinen expliziten Ausschluss von einzelnen Unternehmen geben soll, wohl aber eine deutliche Überarbeitung und Anhebung der Sicherheitsvorgaben. Diese sollen für alle Netzwerkausrüster gleichermaßen gelten und wurden noch vor der Versteigerung der 5G-Frequenzen angekündigt. Konkret sollen in § 109 TKG höhere technische Schutzmaßnahmen (fortlaufendes Code Review, Zertifizierung der Hard- und Software und Festschreibung von Mindeststandards) festgeschrieben werden. Zudem sollen die Anbieter in einer Art No-Spy-Abkommen rechtlich verbindliche Garantien abgeben, dass ausländische Staaten oder Stellen keinen Zugriff auf Daten oder Netze in Deutschland haben.

Um die Sicherheit und Vertrauenswürdigkeit unserer Kommunikationsnetze sicherzustellen, bedarf es aus unserer Sicht einer umfassenden Sicherheitsstrategie. Eine Fokussierung auf die Sicherheit primär durch technische Zertifizierungen von Soft- und Hardware der 5G-Technologieanbieter und die Offenlegung des Quellcodes wird dem allein nicht gerecht. Selbst das Bundesinnenministerium hat in 2012 noch attestiert, dass auch in ausführlichen Tests nicht alle Fehler oder Schadfunktionen zu finden seien. Von dieser Einschätzung ist das Bundesinnenministerium noch heute überzeugt. Die Erfahrung in Großbritannien zeigt, dass in überprüfter Hard- und Software Backdoors und Schwachstellen eingebaut waren. Zusätzlich war das „Verhalten“ in Laborbedingungen nicht im Feld reproduzierbar. Auch entsprechend der Aussagen in der öffentlichen Anhörung des Deutschen Bundestages vom 11. November 2019 stellen darüber hinaus Softwareupdates – und insbesondere sogenannte „Emergency Patches“ (also kurzfristige Sicherheitsupdates) einen nicht zu bewältigenden Kontrollaufwand dar, da die dafür benötigte Zeit teils Monate beträgt. Softwareupdates müssen aber in kürzester Zeit auf- und ggf. auch wieder überspielt werden.

Durch die Verschmelzung des Kern- und des peripheren Netzes ist auch eine unterschiedliche Bewertung dieser beiden Netzabschnitte nicht zielführend. Denn beispielsweise eine bloße Absicherung des Kernnetzes würde Angriffe auf und über das RAN nicht bzw. nicht ausreichend verhindern. Geringe Latenz und mobiles Edge Computing verlangen z.B. Rechenkapazitäten nah an der Peripherie, wodurch auch Kernnetz und RAN verschwimmen. Auch bei 5G findet eine Ende-zu-Ende-Verschlüsselung nur in der Form statt, dass in der Basisstation entschlüsselt und vor Weitergabe ins Kernnetz wieder verschlüsselt wird. Jedwede Daten liegen also unverschlüsselt in der Basisstation vor.

Die derzeit in der Bundesregierung diskutieren Vorgaben könnten zwar einen Beitrag für etwas mehr Sicherheit leisten, es ist aber höchst fraglich, ob das ausreicht. Untersucht und zertifiziert werden Typenmuster und Momentaufnahmen des Quellcodes, die nicht den tatsächlichen Einbau entsprechen müssen und die durch Updates (Firmware) und Fernwartung schnell verändert werden können. Auf der Ebene der Hardware sind mögliche Hintertüren auch nur noch begrenzt erkennbar. Angesichts der Bedeutung von 5G als die zentrale digitale Infrastruktur und der auf ihr zukünftig basierenden Anwendungen sowie angesichts der besonderen Angriffsmöglichkeiten der neuen Netzarchitektur werden diese Sicherungen aber nicht ausreichen.

Wenn Sicherheit nicht garantiert und die o.g. Gefährdungen nicht ausgeschlossen werden können, wird die Frage des Vertrauens in die Integrität des Herstellers und in das Rechtssystem des Herstellerlandes zentral. Die Überprüfung der Vertrauenswürdigkeit der Anbieter muss daher wesentlicher Bestandteil der Sicherheitsstrategie sein. Diese Überprüfung der Vertrauenswürdigkeit muss gesetzlich festgeschrieben sowie mit entsprechenden Auflagen versehen werden, sodass Anbieter nur dann zum Zuge kommen, wenn sie diese Vorgaben vollumfänglich

erfüllen. Zudem muss die Reziprozität sichergestellt sein: Länder, die europäische Anbieter ausschließen oder begrenzen, sollten auch in Europa nicht oder nur in Grenzen zum Zuge kommen.

Die EU-Kommission hat im Auftrag der Mitgliedstaaten am 9.10.2019 einen Risikobericht zum 5G Ausbau vorgelegt. Darin kommt sie zum Ergebnis, dass das Risikoprofil der einzelnen Lieferanten eine entscheidende Rolle spielt. Dieses Risiko muss politisch bewertet werden. Die entscheidenden Kriterien sind dabei: Eine starke Abhängigkeit des Lieferanten von der Regierung eines Drittstaates, die rechtsstaatliche Lage des Drittstaates, in dem der Lieferant seinen Sitz hat (speziell demokratische Checks and Balances), die Möglichkeit des Drittstaates auf den Lieferanten Druck auszuüben und die Eigentümerstruktur. Diese Risikoeinschätzung der EU sollte auch Grundlage der Debatte in Deutschland sein.