UNTERNEHMERVERBÄNDE
NIEDERSACHSEN E.V.

POSITIONSPAPIER

Mobilfunkstandard 5G

Forderungen zur Daten-, Dienste- und Netzsicherheit

Stand: 13. Februar 2019

Mobilfunkstandard 5G - Forderungen zur Daten-, Dienste- und Netzsicherheit

Die UVN begrüßen die aktuelle Diskussion über die Sicherheit von digitalen Netzen, Anwendungen und Daten. Niedersachsens Wirtschaft benötigt in Zeiten der Digitalisierung eine leistungsfähige und sichere Netzwerkinfrastruktur.

Wir sind bei der digitalen Transformation auf technische Lösungen sowohl nationaler als auch internationaler Unternehmen angewiesen. Eine systematische Ausgrenzung von internationalen Anbietern beim Aufbau digitaler Infrastrukturen oder bei Endgeräten wäre daher weder technologisch, wirtschaftlich noch zeitlich zielführend. Digitale Souveränität darf nicht mit digitaler Autarkie verwechselt werden.

Um langfristig die Sicherheit von digitalen Daten, Diensten und Netzen gewährleisten zu können, sprechen sich die UVN für die Umsetzung folgender Handlungsempfehlungen aus:

Gleiche Kriterien für alle Anbieter ermöglichen

Für alle Hersteller müssen idealerweise europaweit die gleichen produkt- und angebotsspezifischen Prüfkriterien, Regeln und Verfahren gelten. Falls ein Verdacht auf Spionage, Manipulation, o.ä. besteht, müssen die Vorwürfe eingehend geprüft werden. Fakt ist: Rechtstaatliche Verfahren bedürfen „harter Fakten". Dies umfasst technologische, wirtschaftliche und juristische Erkenntnisse.

Unberechtigte politische Einflussnahme durch Drittstaaten verhindern

Falls der Verdacht einer Einflussnahme auf Hersteller durch Drittstaaten besteht, erfordert dies eine eingehende Prüfung durch die Bundesregierung beziehungsweise die zuständigen EU-Institutionen/Agenturen. In diese Prüfung müssen auch gesetzliche Rahmenbedingungen und gängige Praktiken einbezogen werden, denen die Anbieter auf ihrem Heimatmarkt oder mit Tochtergesellschaften in einem Drittstaat ausgesetzt sind, aber für ihre Tätigkeit in der EU relevant sind (bspw. verpflichtende Weitergabe von Daten an staatliche Stellen). Die Zulassung oder der Ausschluss von Unternehmen und ihrer Angebote muss in jedem Fall nach transparenten nachvollziehbaren Kriterien erfolgen (z. Bsp. eine Kombination aus technischen, wirtschaftlichen, politischen und juristischen Erwägungen).

Einsichtnahme in Quellcodes und Entwicklungsprozesse ermöglichen

Mit Blick auf digitale Infrastrukturen wäre für die Stärkung von Vertrauen in Anbieter neben einer Überprüfung der Hardwarekomponenten, zum Beispiel die Einsichtnahme in Quellcodes und Entwicklungsprozesse durch Behördenvertreter in Unternehmen

sinnvoll. Anschließend wäre eine Zertifizierung von Technologien, die in besonders sensiblen kritischen Infrastrukturen (wie 5G-Netzen) verwendet werden, durch akkreditierte Zertifizierungsstellen und/oder Aufsichtsbehörden wie das BSI denkbar. Auch hier müsste das Prinzip „gleiche Pflichten für Gleiche" gelten. Zudem muss sichergestellt werden, (1) dass das BSI ausreichend Ressourcen zur Überprüfung der Quellcodes und Entwicklungsprozesse von Soft- und Hardware hat, (2) welche Konsequenzen sich aus einer Prüfung ohne Fund von Sicherheitsschwachstellen ergeben und (3) dass unbefugte Dritte keinen Zugang zu diesen Quellcodes sowie Informationen über Entwicklungsprozesse bekommen können.

Europaweit einheitliche Sicherheitsstandards zügig entwickeln

Um den europäischen Digitalen Binnenmarkt zu stärken und unberechtigte Datenzugriffe effektiv zu verhindern, bedarf es zudem europaweit einheitlicher Sicherheitsstandards. Im Rahmen des EU Cybersecurity Acts sollte schnellstmöglich ein Zertifizierungsschema für 5G- Technologien erarbeitet werden. Bei Schemata, die konkrete Produkte betreffen, sollten diese sowohl das Wechselspiel von Hard- und Software als auch Prozesse, wie das Updatemanagement und die Nachvollziehbarkeit von Softwareentwicklungen, abdecken. Regionale Sicherheitszertifizierungen müssen auf internationalen Normen basieren und mit internationalen Regelungen zur gegenseitigen Anerkennung kompatibel sein. Um zu raschen Ergebnissen zu kommen, sollte die Expertise der deutschen Industrie in die Erarbeitung der Cybersicherheitszertifizierungsschemata einbezogen werden.

Effektive Prüfverfahren, ausreichend Ressourcen und Sanktionsmechanismen gewährleisten

Zertifizierungsverfahren sollten stets in enger Abstimmung zwischen den nationalen Aufsichtsbehörden (in Deutschland das BSI), Netzausrüstern und -betreibern, (Anwender-) Industrien, und akkreditierten unabhängigen Prüflaboren erfolgen. Das BSI benötigt sowohl die personellen als auch finanziellen Ressourcen, um vor allem als kritisch eingestufte Technologien nicht nur einmalig vor dem Roll-out zu zertifizieren, sondern auch kontinuierlich über den gesamten Produktlebenszyklus zu überprüfen. Falls Anbieter festgeschriebene Standards nicht einhalten, bedarf es konsequenter Sanktionen.

Engen Dialog mit Betreibern kritischer IKT-Infrastrukturen etablieren

Zudem muss sowohl die Landes- als auch die Bundesregierung in einen engen Dialog mit Betreibern kritischer IKT-Infrastrukturen treten. Deren Erfahrungen und technische

Expertise sollten als Grundlage für Entscheidungsprozesse herangezogen werden. Die deutsche Industrie steht für einen vertrauensvollen und sachorientierten Austausch gern zur Verfügung.

Innovationsfreundliche Forschungs- und Industriepolitik heute für Morgen implementieren

Damit Europa bei zukünftigen technologischen Entwicklungen ein Höchstmaß an technologischer Souveränität besitzt, sollten europäische Förderprogramme wie Horizon Europe schon jetzt zielgerichtet genutzt werden. Eine intelligente, zukunftsgerichtete und innovationsfreundliche Forschungs- und Industriepolitik muss jetzt implementiert werden, um in Zukunft digital souverän zu sein.

Nutzerinnen und Nutzern sensibilisieren

Die Landes- aber auch die Bundesregierung sollte Bürgerinnen und Bürgern sowie Unternehmen stärker dafür sensibilisieren, dass sich unberechtigte Datenzugriffe kaum vollständig verhindern lassen. Auch die Nutzerinnen und Nutzer sind gefordert, ihren Beitrag für Sicherheit, Integrität und Verfügbarkeit von Daten zu leisten. Sichere Netze und Datenübertragung helfen wenig, wenn an Endgeräten sorglos mit Daten umgegangen wird. Zum Beispiel sollte bei sensiblen Daten eine konsequente Ende-zu-Ende-Verschlüsselung eingesetzt werden — dies gilt für 5G genauso wie für 4G, 3G und 2G. Gleichzeitig müssen Anbieter von Technologien und Dienstleistungen durch geeignete Maßnahmen die Sicherheit und Integrität von Daten, Diensten und Netzen gegenüber Anwenderinnen und Anwendern gewährleisten.

5G-Frequenzversteigerung umsetzen

Wichtig ist jetzt, das Augenmerk auf die nun bevorstehende 5G-Frequenzversteigerung zu richten. Die Netzbetreiber brauchen Rechtssicherheit, um den Ausbau leistungsfähiger 5G-Netze voranbringen zu können.