**Deutscher Bundestag**

Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)751

DIE FAMILIEN UNTERNEHMER

DIE FAMILIENUNTERNEHMER | Charlottenstraße 24 | 10117 Berlin

An die Mitglieder des Innenausschusses
des Deutschen Bundestages
(CDU/CSU, SPD, Bündnis 90/Die Grünen, FDP)
Platz der Republik 1
11011 Berlin

→ Übermittlung per E-Mail

Berlin,
26. Februar 2021

Nachbesserung des IT-Sicherheitsgesetzes 2.0
Stellungnahme von DIE FAMILIENUNTERNEHMER

Sehr geehrte Damen und Herren,

Sie sind im Begriff, mit dem „zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ wesentliche Weichenstellungen für die Sicherheit und Vertrauenswürdigkeit unserer 5G-Mobilfunkinfrastruktur vorzunehmen. Mit diesem Schreiben übermitteln wir die Stellungnahme von DIE FAMILIENUNTERNEHMER dazu.

Das 5G-Netz wird das Zentralnervensystem unseres auf Wissen gestützten Hochtechnologie-Standortes sein. Unternehmen und Bürger müssen sich auf ein sicheres 5G-Netz ohne Spionage- und Sabotagehintertüren verlassen können. Nur so kann die internationale Wettbewerbsfähigkeit unserer Wirtschaft erhalten und damit die Zukunftsfähigkeit unseres Landes gesichert werden. Unternehmen und Bürger vertrauen aus diesem Grund auf ein Sicherheitsgesetz, das diesen Schutz verlässlich leistet.

In seiner derzeitigen Form ist das nicht gegeben. Der Gesetzentwurf leidet im Gegenteil an einem fundamentalen Konstruktionsfehler, indem gemäß § 9b Komponenten zweifelhafter Anbieter automatisch verbaut werden dürfen, solange nicht alle beteiligten Ministerien geschlossen für einen Ausschluss dieses Anbieters stimmen.

Mögliche Sicherheitsbedenken nur eines Ressorts - und seien sie auch noch so begründet! - würden nicht ausreichen. Mit derartigen hohen Verbotshürden würde faktisch der gesamte Prüfprozess entwertet.
DIE FAMILIENUNTERNEHMER appellieren daher an Sie, diese Regelung zu verbessern.

Albrecht von der Hagen
Hauptgeschäftsführer und
Mitglied des Bundesvorstands
Charlottenstraße 24
10117 Berlin

Tel. 030 300 65-310
Fax 030 300 65-390

vdhagen@familienunternehmer.eu

DIE FAMILIEN UNTERNEHMER



Es sollte stattdessen entweder das Parlament bei der Überprüfung der politischen Vertrauenswürdigkeit beteiligt oder hilfsweise ein Genehmigungsvorbehalt vorgesehen werden. Entscheidend aber ist, nur solche Hersteller für den 5-G-Netzausbau zuzulassen, gegen die keine Sicherheitsbedenken erhoben werden.

Denn nur eine sichere Technologie bietet die Gewähr, im Zuge der Transformation zur Industrie 4.0, dem „Internet der Dinge“ und der Nutzung künstlicher Intelligenz nicht ins Hintertreffen zu geraten oder uns gar abhängig zu machen, sondern verloren gegangenes Terrain zurückzugewinnen. Bitte sorgen Sie mit dafür, dass wir beim Zukunftsthema 5G auf diese Weise unsere beiden verbliebenen europäischen Anbieter von 5G-Komponenten unterstützen.

Mit freundlichen Grüßen

[redacted]

Albrecht von der Hagen
Hauptgeschäftsführer und Mitglied des Bundesvorstands

Anlage

# STELLUNGNAHME

DIE FAMILIEN UNTERNEHMER

DIE JUNGEN UNTERNEHMER

## Letzter Weckruf für die Sicherheit

## Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)

Angesichts zunehmender Cyberattacken auf Krankenhäuser, Behörden und Mittelständler rückt die Frage der Datensicherheit und der digitalen Souveränität immer mehr in das Bewusstsein. Beim Schutz der betrieblichen IT gewinnt auch die Abwehr von Wirtschaftsspionage und Sabotage an Bedeutung: Denn mit relativ geringen Aufwand könnten sensible Geschäftsgeheimnisse abgefischt und sogar zentrale Infrastrukturen wie die Daseinsvorsorge aus der Ferne abgeschaltet werden.

Mit dem derzeit laufenden Aufbau der 5G-Mobilfunkinfrastruktur wird das Fundament für die Zukunftsfähigkeit Deutschlands gelegt. Gerade im Zuge der Transformation zur Industrie 4.0, dem „Internet der Dinge“ und der Nutzung künstlicher Intelligenz kommt dem künftigen 5G-Netzen große Bedeutung zu. Das 5G-Netz wird das Zentralnervensystem unseres auf Wissen gestützten Hochtechnologie-Standortes. Unternehmen und Bürger müssen sich aus diesem Grund auf ein sicheres 5G-Netz ohne Spionage- und Sabotagehintertüren verlassen können. Nur auf diese Weise kann auch der Wunsch nach digitaler Souveränität erreicht werden.

## Unsicherheitsgesetz? Kompromisse bei der Sicherheit

Deshalb muss der Sicherheit kritischer Infrastrukturen besondere Aufmerksamkeit geschenkt werden. Mit dem „zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ (kurz IT-Sicherheitsgesetz 2.0) hat die Bundesregierung kurz vor Weihnachten dazu einen Entwurf vorgelegt.

Neben der Erfüllung technischer Sicherheitskriterien soll laut Gesetzesentwurf auch die politische Vertrauenswürdigkeit der Hersteller von Ausrüstung für das 5G-Netz geprüft werden: Nimmt ein fremder Staat Einfluss auf das Privatunternehmen? Handelt es sich beim Herkunftsland des Herstellers um eine Demokratie mit rechtsstaatlichen Strukturen? Gibt es dort Regelungen, die das Unternehmen zur Datenherausgabe an das Regime verpflichtet?

Was erst einmal gut klingt, entpuppt sich in der Gesetzesausgestaltung allerdings als Mogelpackung. Zwar ist es positiv, dass mit dem Gesetz versucht wird die Cybersicherheit zu stärken, aber in Bezug auf den vertrauenswürdigen 5G-Netzaufbau handelt es sich um ein „Unsicherheitsgesetz“. Anstatt die Chance zu nutzen, Deutschland wirklich sicher und damit zukunftsfähig zu machen, ist das Design der Entscheidungsprozesse über die Frage, ob ein

DIE FAMILIENUNTERNEHMER e.V.
DIE JUNGEN UNTERNEHMER
Dr. Julian Dörr
Charlottenstraße 24 | 10117 Berlin

Tel. 030 300 65-443
Fax 030 300 65-390
doerr@familienunternehmer.eu
www.familienunternehmer.eu

Anbieter „vertrauenswürdig“ ist, so angelegt, dass es in der Praxis kaum je final zu einem Ausschuss kommen werden dürfte.

Denn leider ist für den Prüfprozess lediglich der so genannte Untersagungsvorbehalt vorgesehen: Sollten nicht alle beteiligten Ministerien geschlossen für einen Ausschluss zweifelhafter Hardware stimmen, darf sie automatisch verbaut werden. Mögliche Sicherheitsbedenken nur eines Ressorts würden nicht ausreichen. Aufgrund solcher hohen Verbotshürden würden faktisch alle Komponenten durchgewinkt und der gesamte Prüfprozess entwertet. Damit öffnen wir das 5G-Netz bereitwillig Anbieter aus Staatswirtschaften und Diktaturen, die auch mit staatlich verschleierten Dumpingpreisen versuchen Marktmacht zu gewinnen.

Vernünftiger wäre es aus Sicht deutscher Hochtechnologie-Anbieter, wenn die Entscheidung über die politische Vertrauenswürdigkeit der Anbieter von 5G-Komponenten einem Gremium des Bundestages übertragen werden würde. Hilfsweise sollte im IT-Sicherheitsgesetz zumindest die aktive Zustimmung aller beteiligter Ministerien festgeschrieben werden (Genehmigungsvorbehalt): Nur falls sämtliche Beteiligte keine Sicherheitsbedenken haben, sollten Hersteller für den 5G-Netzausbau zugelassen werden.

Deutschland würde mit dem derzeit vorliegenden Entwurf eines Sicherheitsgesetzes einen Sonderweg gehen und sich in Europa isolieren. Vorbilder sollten uns Großbritannien, Frankreich und Schweden sein, die die potentielle Einflussnahme durch einen fremden Staat nicht akzeptieren und durch strikte Prüfungen sichere 5G-Netze aufbauen.

DIE FAMILIENUNTERNEHMER haben wiederholt deutlich gemacht, dass für uns auf Dauer angelegte, nachhaltige Datensouveränität schwerer wiegt als mögliche Benachteiligungen für deutsche Akteure auf z. B. asiatischen Teilmärkten, falls die politische Führung von nicht-europäischen Anbietern deutsche Unternehmen im Kontext einer 5G-Regulierung abstrafen sollte. Datensicherheit, Schutz vor Manipulation sowie Erpressbarkeit und technologische Unabhängigkeit sind gerade für unsere deutschen Technologie-Champions überlebenswichtig.

## Nachbesserungen und Änderungen im Einzelnen

- Sämtliche nachfolgende Änderungsvorschläge beziehen sich auf Absätze des § 9b „Untersagung des Einsatzes kritischer Komponenten“ des IT-Sicherheitsgesetz-Entwurfes (aufgeführt unter dem Abschnitt „19. Nach §9 werden die folgenden §§ 9a bis 9c eingefügt“).

- 5G-Netze sind in ihrer Gesamtheit kritische Infrastrukturen und als solche insgesamt zu prüfen, eine Differenzierung des Vorbehaltes einer Vertrauenswürdigkeitsprüfung anhand einer anderweitig geregelten Zertifizierungspflicht ist nicht sinnvoll. Entsprechender Nebensatz sollte gestrichen werden:

**§ 9b Absatz 1**

(1) Der Einsatz kritischer Komponenten gemäß § 2 Absatz 13~~, für die eine gesetzliche Zertifizierungspflicht besteht,~~ ist durch den Betreiber der Kritischen Infrastruktur dem Bundesministerium des Innern, für Bau und Heimat vor Einsatz anzuzeigen. In der Anzeige ist die kritische Komponente und die Art ihres Einsatzes anzugeben. ~~Die Pflicht aus Satz 1 besteht bereits dann, wenn für die Pflicht zur Vorlage von Zertifikaten eine Übergangsfrist gewährt wird.~~

- Die Selbsterklärung (Garantieerklärung) eines Herstellers ist keine hinreichende Bedingung für die Vertrauenswürdigkeit des jeweiligen Herstellers. Stattdessen sollte vielmehr durch die beteiligten Ressorts eine grundlegende Überprüfung der Vertrauenswürdigkeit im Sinne einer Bewertung des Risikoprofils von Herstellern erfolgen. Entsprechend sollte § 9b (2) umformuliert werden:

**§ 9b Absatz 2**

(2) Kritische Komponenten gemäß § 2 Absatz 13 dürfen nur eingesetzt werden, wenn **das Bundesministerium des Innern, für Bau und Heimat im Einvernehmen mit dem Auswärtigen Amt, dem Bundeskanzleramt und dem Bundesministerium der Verteidigung** ~~der Hersteller eine Erklärung über seine~~ **die Vertrauenswürdigkeit** ~~gegenüber dem Betreiber der Kritischen Infrastruktur (Garantieerklärung) abgeben~~ **des Herstellers der kritischen Komponenten festgestellt hat.**

~~Diese Erklärung erstreckt sich auf die gesamte Lieferkette des Herstellers. Die Garantieerklärung des Herstellers der kritischen Komponente ist der Anzeige nach Absatz 1 beizufügen. Aus der Garantieerklärung muss unter anderem hervorgehen, ob und wie der Hersteller hinreichend sicherstellen kann, dass die kritische Komponente über keine technischen Eigenschaften verfügt, die geeignet sind, missbräuchlich, insbesondere zum Zwecke von Sabotage, Spionage oder Terrorismus auf die Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können. Das Bundesministerium des Innern, für Bau und Heimat legt die Mindestanforderungen für die Garantieerklärung im Einvernehmen mit den betroffenen Ressorts unter Berücksichtigung überwiegender öffentlicher Interessen, insbesondere sicherheitspolitischer Belange, durch Allgemeinverfügung fest, die im Bundesanzeiger bekannt zu machen ist. Das Verbot in Satz 1 gilt erst ab der Bekanntmachung der Allgemeinverfügung nach Satz 5. Soweit Änderungen der Allgemeinverfügung erfolgen, sind diese für bereits nach Absatz 2 abgegebene Garantieerklärungen unbeachtlich.~~

- Entsprechend der eingangs ausgeführten Ablehnung lediglich eines Untersagungsvorbehaltes sollte stattdessen ein Genehmigungsvorbehalt verankert werden:

**§ 9b Absatz 3, 4**

(3) Das Bundesministerium des Innern, für Bau und Heimat ~~kann~~ **muss** den Einsatz ~~einer~~ **aller** kritischen Komponenten **eines Herstellers** gegenüber dem Betreiber der Kritischen Infrastruktur im Einvernehmen mit ~~den betroffenen Ressorts~~ **dem Auswärtigen Amt, dem Bundeskanzleramt und dem Bundesministerium der Verteidigung** bis zum Ablauf von ~~einem Monat~~ **drei Monaten** nach Eingang der Anzeige nach Absatz 1 ~~untersagen~~ **erlauben** oder Anordnungen erlassen, wenn überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland **oder mangelnde Vertrauenswürdigkeit des Herstellers**, dem Einsatz entgegenstehen. Vor Ablauf der Frist von ~~einem~~ **drei** Monaten **nach** Anzeige nach Absatz 1 ist der Einsatz nicht gestattet.

(4) Das Bundesministerium des Innern, für Bau und Heimat **muss** ~~kann~~ den weiteren Betrieb **aller kritischen Komponenten eines Herstellers** ~~einer kritischen Komponente gegenüber dem Betreiber der Kritischen Infrastruktur~~ im Einvernehmen **mit dem Auswärtigen Amt, dem Bundeskanzleramt und dem Bundesministerium der Verteidigung** ~~den betroffenen Ressorts~~ **untersagen** ~~oder Anordnungen erlassen~~, wenn der Hersteller der kritischen Komponente sich als nicht vertrauenswürdig erwiesen hat.

- Vertrauenswürdigkeit kann nicht durch technische Kriterien überprüft werden, da sie nicht-technische Risiken ausklammert. Entsprechend sollte das Gesetz bei der Definition der Vertrauenswürdigkeit eines Herstellers weder allein technische Kriterien heranziehen noch die strategischen, nicht-technischen Kriterien in nachgelagerte Verordnungen verschieben.

**§ 9b Absatz 5**

(5) Ein Hersteller einer kritischen Komponente ist nicht vertrauenswürdig, wenn
~~1. er gegen die in der Garantieerklärung eingegangen Verpflichtungen und Versicherungen verstoßen hat,~~
~~2. die in der Garantieerklärung angegebenen Tatsachen unwahr sind,~~
~~3. er Sicherheitsüberprüfungen und Penetrationsanalysen nicht im erforderlichen Umfang an seinem Produkt und in der Produktionsumgebung in angemessener Weise unterstützt,~~
~~4. er bekannte oder bekannt gewordene Schwachstellen oder Manipulationen nicht unverzüglich dem Betreiber der Kritischen Infrastruktur meldet und beseitigt oder~~
~~5. die kritische Komponente über technische Eigenschaften verfügt oder verfügt hat, die geeignet sind oder waren, missbräuchlich auf die Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können. Ein Verstoß nach Nummer 5 liegt nicht vor, wenn der Hersteller nachweisen kann, dass er die technische Eigenschaft im Sinne von Nummer 5 nicht implementiert hat und er diese jeweils ordnungsgemäß beseitigt hat.~~

DIE FAMILIENUNTERNEHMER e.V.
DIE JUNGEN UNTERNEHMER
Dr. Julian Dörr
Charlottenstraße 24 | 10117 Berlin

Tel. 030 300 65-443
Fax 030 300 65-390
doerr@familienunternehmer.eu
www.familienunternehmer.eu

**1. eine hohe Wahrscheinlichkeit einer Einwirkung von Regierungsorganisationen eines Drittstaates auf den Hersteller besteht.**

**2. die Möglichkeit der Einflussnahme auf den Hersteller durch gesetzgeberische Akte eines Drittstaates besteht, falls der Hersteller in diesem Drittstaat seinen Sitz hat.**

**3. Sicherheits- oder Datenschutzübereinkommen zwischen der Europäischen Union und dem Sitzstaat des Lieferanten fehlen, sofern es sich dabei um einen Drittstaat handelt.**

**4. die Fähigkeit eines Drittstaates, Druck auf den Hersteller auszuüben, vorhanden ist, insbesondere hinsichtlich des Produktionsstandorts.**

**5. bestimmte Charakteristika in der Eigentümerstruktur des Herstellers vorhanden sind, die eine Einflussnahme eines Drittstaates ermöglichen.**

- Die Konsequenz eines Ausschlusses nicht-vertrauenswürdiger Hersteller greift nicht weit genug, da sie lediglich auf die Untersagung des Einsatzes einzelner Komponenten abstellt und damit rein technischen Erwägungen folgt. Deutschland sollte sich an der EU 5G Toolbox (Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures) orientieren: Länder wie Großbritannien (de jure) und Frankreich (de facto) verfahren nach einem Phase-Out-Modus für bereits verbaute Komponenten nicht-vertrauenswürdiger Hersteller.

**§ 9b Absatz 6, 7**

~~(6) Wurde nach Absatz 4 der Einsatz einer kritischen Komponente untersagt, kann das Bundesministerium des Innern, für Bau und Heimat im Einvernehmen mit den betroffenen Ressorts~~
~~1. den angezeigten Einsatz weiterer kritischer Komponenten desselben Typs und desselben Herstellers untersagen und~~
~~2. nach Ablauf einer angemessenen Frist die Nutzung bereits im Einsatz befindlicher kritischer Komponenten desselben Typs und desselben Herstellers untersagen.~~

~~(7) Bei wiederholter Feststellung nicht vorliegender Vertrauenswürdigkeit nach Absatz 5 Nummer 1 bis 3 kann das Bundesministerium des Innern, für Bau und Heimat im Einvernehmen mit den betroffenen Ressorts den Einsatz aller kritischen Komponenten des Herstellers untersagen.~~

**(6) Bereits verbaute Komponenten eines Herstellers, der sich im Nachhinein als nicht-vertrauenswürdig erwiesen hat, dürfen nach einer Frist von 5 Jahren nach Inkrafttreten dieses Gesetzes nicht mehr eingesetzt werden.**