Positionen | Sicherheit und Trustworthiness

NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

Trust should be based on facts, facts should be verifiable, and verification should be based on harmonized standards

Festhalten am Konzept des Einsatzes kritischer Komponenten – §41: Huawei unterstützt, dass die Bundesregierung in ihrem Kabinettsentwurf an ihrem Prinzip festgehalten hat, Unternehmen nicht wegen ihres Herkunftsortes zu diskriminieren. Es braucht weiterhin klare Risikoassessments verbunden mit technischen Standards und Zertifizierungen, im Dreiklang derer die Cybersicherheit gewährleistet wird. Die Änderungen im §41 in den bekanntgewordenen Formulierungshilfen verabschieden sich von den bisher bekannten Prinzipien und führen zu einer weiteren Politisierung von unternehmerischen Entscheidungen und einer Machtkonzentration in einem einzelnen Bundesministerium.

Einige Vorbemerkungen:

- **Unternehmerische Freiheiten nicht beeinträchtigen**: Der Bund sollte per se davon absehen, die Nutzung bestimmter Technologieanbieter zu verbieten. Nutzer und Betreiber können am besten beurteilen, welche Technologien für ihre Geschäftsmodelle und -systeme am besten geeignet sind, und im eigenen Interesse Risikoanalysen durchführen.

- **IT- und Cybersicherheit ist kein Zustand, sondern ein Prozess**: Viele bekannte IT- und Cybersicherheitsrisiken sowie neue Szenarien können bereits heute durch geeignete Maßnahmen von Nutzern und Betreibern mitigiert werden. Wir stimmen daher der Notwendigkeit technisch fundierter Sicherheitsstandards für die Akzeptanz und den Betrieb von Systemen in kritischen Infrastrukturen zu.

- **Eine Geopolitisierung der IT-Sicherheit gefährdet diese**: Die Diskussion um IT-Sicherheit ist stark geopolitisch geprägt. Unter IT-Sicherheitsexperten herrscht ein überwältigender Konsens darüber, dass die Herkunft einer Technologie kein aussagekräftiges Kriterium für deren Sicherheit ist. Zumal der überwiegende weltweite Anteil bspw. von Computern, Routern und anderer Hardware herstellerübergreifend bereits jetzt in China gefertigt wird und dann auch all jene Produkte unter Generalverdacht stünden. Es ist daher aus Sicht der IT-Sicherheit nicht sinnvoll, Anbieter die alle anerkannten Zertifizierungsprozesse und objektiven Sicherheitsstandards erfüllen und alle unabhängigen Audits bestehen sowie weltweit zuverlässig genutzt werden, in Deutschland nur aufgrund ihrer Herkunft per se auszuschließen. Dieser Ansatz wird zu massiven Sicherheitsproblemen führen, da Schwachstellen von jedem böswilligen Akteur überall auf der Welt ausgenutzt werden können, wenn er sie kennt. Die Sicherheit für die Installation und den Betrieb von Systemen muss anhand objektiver Kriterien nachgewiesen werden, unabhängig von der Herkunft eines potenziellen Herstellers. Und die Vertrauenswürdigkeit eines Herstellers muss kontinuierlich allein auf der Grundlage der Einhaltung von Prozess- und Produktstandards überprüft werden.

HUAWEI TECHNOLOGIES Deutschland GmbH
Hansaallee 205

40549 Düsseldorf, Germany

Sitz der Gesellschaft: Düsseldorf
Amtsgericht Düsseldorf, HRB 72992
Geschäftsführer: Zuo Defeng, Wei Zhou, Xin Wang, Hebin Yang

Ust-IdNr. DE221 644 379
Tel: +49 (0)211 88254-8000
Fax: +49 (0)211 88254-8932

www.huawei.com/de

- **Die Vermischung von IT- und Cybersicherheit mit anderen politischen Zielen ist nicht zielführend**: Wir stellen auch fest, dass in der Debatte nicht mehr klar zwischen IT- und Cybersicherheit und anderen Risiken wie wirtschaftlichem Schutz und Resilienzbemühungen unterschieden wird. Wir plädieren für eine klare Trennung dieser Themen in der Debatte. Klar ist aber auch, dass Unternehmen nicht von einem einzigen Unternehmen abhängig werden wollen, weshalb sie in der Regel auf eine Multi-Vendor-Strategie setzen und Produkte von verschiedenen Technologieanbietern beziehen. Wir plädieren deshalb für einen wettbewerbsorientierten Ansatz, unter Berücksichtigung der unternehmerischen Freiheit.

Mit Blick auf die Änderungen in §41:

- **Fehlen eines ganzheitlichen Ansatzes – Teil I**: Die alleinige Entscheidungsbefugnis des BMI bei der Untersagung von kritischen Komponenten ohne verbindliche Einbindung anderer Ressorts, verhindert eine ausgewogene Interessenabwägung. Bei solch weitreichenden Entscheidungen – auch mit Blick auf die Investitionen und den Betrieb von Kritischen Anlagen – scheint es wenig sinnvoll, hier mit dem Argument des Bürokratieabbaus Änderungen herbeizuführen. Zwar sind das AA sowie das betroffene Fachministerium formal in den Prozess eingebunden, aber bei Untersagung kritischer Komponenten nur noch ins Benehmen zu setzen. Dies führt aber gerade beim ressortübergreifenden Querschnittthema Digitalisierung zwangsläufig zu einer massiven Einseitigkeit in der Entscheidungsfindung und einer starken Machtverschiebung zugunsten eines möglichen „Superministeriums“. Je nach politischer Ausrichtung eines Ministeriums kann dies im Zweifelsfall sogar eine Gefährdung für demokratische Entscheidungsfindungen bedeuten. Ferner regen wir auch dazu an, das Bundeskanzleramt formell in den Entscheidungsprozess zu integrieren und eine Entscheidung für die Untersagung von kritischen Komponenten im Einvernehmen zu erzielen.

- **Fehlen eines ganzheitlichen Ansatzes – Teil II**: Das BMI wird durch §56 (7) künftig in die Lage versetzt, per Rechtsverordnung im Einvernehmen mit dem betroffenen Fachministerium kritische Komponenten für neue Bereiche zu bestimmen. Es ist begrüßenswert, dass hier weiterhin auf das Einvernehmen gesetzt. Es erschließt sich jedoch fachlich-technisch nicht, weshalb zukünftig die Rolle der Zuschreibung von kritischen Komponenten *voraussichtlich* ausschließlich im BMI mittels Erlass einer Rechtsverordnung nach § 56 liegen soll. Die Änderungen in § 5c EnWg und § 167 TKG heben dadurch alle Anstrengungen der Industrie auf und sorgen für weitere Unsicherheiten. Es wäre notwendig, wenn der etablierte Prozess in der Zusammenarbeit zwischen Bundesnetzagentur und Bundesamt für Sicherheit in der Informationstechnik weiter Bestand hat und kritische Funktionen und Komponenten im Einvernehmen festgeschrieben und technisch bestimmt werden. Ferner sollte sichergestellt sein, dass weiterhin auch die betroffenen Verbände, Betreiber kritischer Anlagen und Anbieter in den Prozess der Festlegung eingebunden sind.

➔ ***Wir empfehlen dringend, den Begriff „im Benehmen“ in §41 (1) in „im Einvernehmen“ zu ändern. Ferner, regen wir dazu an, auch das Bundeskanzleramt formell in den Entscheidungsprozess zu integrieren.***

➔ ***Wir empfehlen, dass festgeschrieben wird, dass weiterhin die Bundesnetzagentur im Einvernehmen mit dem Bundesamt für Informationstechnik und unter Berücksichtigung betroffener Verbänden, Betreiber Kritischer Anlagen und Anbieter kritische Funktionen und Komponenten festlegt.***

HUAWEI TECHNOLOGIES Deutschland GmbH
Hansaallee 205

40549 Düsseldorf, Germany

Sitz der Gesellschaft: Düsseldorf
Amtsgericht Düsseldorf, HRB 72992
Geschäftsführer: Zuo Defeng, Wei Zhou, Xin Wang, Hebin Yang

Ust-IdNr. DE221 644 379
Tel: +49 (0)211 88254-8000
Fax: +49 (0)211 88254-8932

www.huawei.com/de

- **Massive Rechtsunsicherheit der Wirtschaft – I**: § 41 (3) bedeutet in der neuen Fassung, dass ein Widerspruch oder eine Klage (des Betreibers der kritischen Anlage) gegen die Entscheidung des BMI deren Vollzug nicht automatisch aufhält. Mit anderen Worten: Die Entscheidung des BMI bleibt trotz eines eingelegten Widerspruchs oder einer eingereichten Klage wirksam und muss befolgt werden, bis ein Gericht anders entscheidet. Wenn sich also ein Verfahren über zwei bis drei Jahre hinzieht, sind bereits alle kritischen Komponenten u.U. mit erheblichen Mehrkosten verbunden aus dem Einsatz entfernt und ein anderslautendes Urteil läuft ins Leere. Neben der Ungewissheit, ob so ein Verfahren gewonnen werden kann, weil Beweise z. B. der Geheimhaltung unterliegen, würden auf Betreiber der kritischen Anlagen und Hersteller von kritischen Komponenten ein potenzielles wirtschaftliches Risiko in Milliardenhöhe zukommen.

- **Massive Rechtsunsicherheit der Wirtschaft – II**: Nach dem neu formuliertem § 41 (4) Nr. 3 können die bisherigen politischen Kriterien (Nr. 1, 2 und 4) berücksichtigt werden, müssen sie aber nicht (*Zitat aus der Begründung: „Der Begriff „insbesondere“ verdeutlicht, dass die in Absatz 4 genannten Aspekte nicht abschließend aufgeführt werden.“*). Es können auch andere Gründe sein. Nach Nr. 3 sind sogar „*hinreichende Anhaltspunkte*" ausreichend.

  „Hinreichende Anhaltspunkte“ sind Tatsachen oder Umstände, die eine gewisse Wahrscheinlichkeit dafür begründen, dass ein bestimmtes Ereignis eingetreten ist oder eintreten könnte. Im deutschen Recht bedeutet dies, dass es konkrete und objektive Anzeichen gibt, die eine weitere Untersuchung oder ein weiteres Vorgehen rechtfertigen.

  Zum Beispiel könnten hinreichende Anhaltspunkte im Strafrecht bedeuten, dass es genügend Indizien gibt, die den Verdacht auf eine Straftat begründen und somit eine Ermittlung rechtfertigen. Diese Anhaltspunkte müssen allerdings über vage Vermutungen hinausgehen und auf konkreten Beobachtungen oder Beweisen basieren.

  Es besteht also ein Anfangsverdacht und dieser soll ausreichen, um eine komplette Untersagung der kritischen Komponenten zu rechtfertigen? Wir halten dies für verfassungsrechtlich äußerst bedenklich.

➔ ***Wir empfehlen daher, den § 41 (3) und § 41 (4) Nr. 3 ersatzlos zu streichen.***

- **Gefährdung von Investitionen und Innovation**: Im schlimmsten Falle könnte die Entscheidung eines einzelnen Ministeriums Milliardenbelastungen für deutsche Unternehmen darstellen und das in einer Zeit, in der die Wettbewerbsfähigkeit vieler deutscher Industriezweige gestärkt und nicht geschwächt werden sollte. Entscheidungen mit potenziell erheblichen Eingriffen in Grundrechte, die schwere wirtschaftliche Schäden verursachen könnten, sollten in einem großen Konsens innerhalb einer Bundesregierung getroffen werden. Ist dieser Konsens nicht erzielbar, dann dürfte die Sachlage auch nicht eindeutig genug sein für solch weitreichenden Entscheidungen.

  Schon die bloße Möglichkeit einer niedrigschwelligen Untersagung kann dazu führen, dass deutsche Unternehmen ohne wirklichen Sicherheitsgewinn auf Lieferanten setzen, die nicht das beste Preis-Leistungs-Verhältnis bieten, im schlimmsten Falle sogar geringere Sicherheitsstandards implementieren, nur weil sie aus einem Herkunftsland kommen, das

nicht in geopolitischen Diskussionen präsent ist. Hier droht bereits durch die bloße Existenz einiger Bestimmungen im Gesetz die Wettbewerbsfähigkeit deutscher Unternehmen Schaden zu nehmen, denn nur wer die maximale Auswahl an Zulieferern zur Verfügung hat, kann unter Qualitäts- und Kostengesichtspunkten optimal entscheiden. Wer auf Lieferanten setzen muss, die geringere Qualität bei höheren Kosten liefern, nur weil ein Gesetz Rechtsunsicherheit erzeugt, wird im globalen Wettbewerb einen schwereren Stand haben.

Eine erste kursorische juristische Prüfung unserseits hat verfassungsrechtliche Bedenken bzgl. der vergleichsweise niedrigen Schwelle ("hinreichende Anhaltspunkte" und „sonstigen Gründen nicht vertrauenswürdig“) ergeben, die das BMI zu nehmen hat, um schwerwiegende Eingriffe in privates Eigentum und Investitionen in Form von Untersagungen von kritischen Komponenten zu rechtfertigen.

Die sehr niedrigen Anforderungen für Untersagungen, über deren Erfüllung auch nur ein Ministerium am Ende entscheiden würde, in Kombination mit keinerlei aufschiebenden Wirkung der Rechtsmittel, stellen eine erhebliche Einschränkung wirtschaftlicher Freiheiten von investierenden Unternehmen dar, die je nach Branche bei einer nicht unerheblichen Anzahl potenzieller Lieferanten keine hinreichende Rechtssicherheit mehr hätten, wenn sie auf diese Lieferanten auch nur teilweise setzen wollen.

Vor diesem Hintergrund fragen wir uns, ob es seitens des Parlaments bereits eigene Prüfungen durch den Wissenschaftlichen Dienst gibt, ob die Anforderungen für diese angedachten potenziell massiven Einschränkungen von Eigentums- und Freiheitsrechten verfassungsrechtlich hinreichend bestimmt formuliert wurden. Daher hoffen wir insgesamt, dass sich mehr Zeit für die Anpassungen des Mechanismus für kritische Komponenten genommen wird und diese nicht vorschnell im Parlament verabschiedet werden.

➔ ***Wir empfehlen daher generell, dass die Anpassungen des kritischen Komponenten Konzepts mit der gesamten Industrie und betroffenen Unternehmen in bewährten Beteiligungsverfahren durchgeführt werden. Insbesondere, da dies nie Thema in den Abstimmungsrunden mit dem BMI in der vorherigen Phase zur NIS2-Umsetzung war.***

HUAWEI TECHNOLOGIES Deutschland GmbH
Hansaallee 205

40549 Düsseldorf, Germany

Sitz der Gesellschaft: Düsseldorf
Amtsgericht Düsseldorf, HRB 72992
Geschäftsführer: Zuo Defeng, Wei Zhou, Xin Wang, Hebin Yang

Ust-IdNr. DE221 644 379
Tel: +49 (0)211 88254-8000
Fax: +49 (0)211 88254-8932

www.huawei.com/de