



Der Präsident

Bundesnetzagentur | Postfach 80 01 | 53105 Bonn

Per Mail: adi@bundestag.de

Mitglied des Deutschen Bundestages
Tabea Rößner
Vorsitzende des Ausschusses für Digitales
Platz der Republik 1
11011 Berlin

23.01.23

Digitalausschuss am 25.01.2023; SB20(23)14 **Strategiepapier zur Resilienz der Telekommunikationsnetze**

Sehr geehrte Frau Abgeordnete,

über das Interesse, das den Fragen für den Digitalausschuss „Cybersicherheit – Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland“ zugrunde liegt, freue ich mich sehr. Das Thema Resilienz ist auch in Zusammenhang mit Cybersicherheit bereits seit längerem ein wichtiges Thema in der Bundesnetzagentur.

Die Telekommunikationsnetze müssen ein hohes Schutzniveau und größtmögliche Stabilität aufweisen. Ereignisse wie die Flutkatastrophe an der Ahr, die Corona-Pandemie und die aktuelle Lage in der Ukraine haben verdeutlicht, dass sich die äußere Bedrohungslage in der Telekommunikation verschärft hat. Daher spielt das Thema Cybersicherheit ebenfalls eine entscheidende Rolle in diesem Bereich.

Bundesnetzagentur für
Elektrizität, Gas, Telekommunikation,
Post und Eisenbahnen

Telefax Bonn
0228 14-8872

E-Mail
poststelle@bnetza.de
Internet
<http://www.bundesnetzagentur.de>

Bitte neue Bankverbindung beachten!
Bundeskasse Weiden
Dt. Bundesbank – Filiale Regensburg
BIC: MARKDEF1750
IBAN: DE08 7500 0000 0075 0010 07

Behördensitz: Bonn
Tulpenfeld 4
53113 Bonn
☎ 0228 14-0

Datenschutzhinweis:

Der Schutz Ihrer Daten ist uns wichtig. Nähere Informationen zum Umgang mit personenbezogenen Daten in der BNetzA können Sie der Datenschutzerklärung auf <https://www.bundesnetzagentur.de/Datenschutz> entnehmen. Sollte Ihnen ein Abruf der Datenschutzerklärung nicht möglich sein, kann Ihnen diese auch in Textform übermittelt werden.

Die Bundesnetzagentur möchte gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und in Zusammenarbeit mit den Vertretern der Telekommunikationsbranche die Widerstandsfähigkeit der öffentlichen Telekommunikationsnetze und öffentlich zugänglichen Telekommunikationsdienste steigern. Hierzu wurde bereits am 6. September 2022 ein Strategiepapier zur Resilienz der Telekommunikationsnetze veröffentlicht (<http://www.bundesnetzagentur.de/tkresilienz>). Darin werden erste Handlungsempfehlungen für eine weitere Stärkung der sowohl physischen als auch digitalen Widerstandsfähigkeit der Telekommunikationsnetze aufgezeigt.

Die Bundesnetzagentur setzt aktuell den Branchendialog zwischen den beteiligten Unternehmen, Verbänden und Behörden weiter fort. Ziel ist es, in einem ersten Schritt gemeinsam konkrete Maßnahmen in Form einer „Best Practice“ zu beschreiben und mit der Branche zu vereinbaren und damit langfristig die Widerstandsfähigkeit der Netze zu stärken. Dabei gilt es auch entsprechende bereits in anderen Ländern festgelegte Best Practices in die Überlegungen einzubeziehen. Hiermit kann erreicht werden, dass bereits bewährte Verfahren und Prozesse sowie technische Systeme schnellstmöglich in der gesamten Branche eingesetzt werden. Ein zusätzlich wichtiges Instrument zum Erreichen des Zieles stellt sicherlich die Erarbeitung und Festlegung von „Best Practice-Maßnahmen“ in Bezug auf die Cybersicherheit in Telekommunikationsnetzen dar. Hierbei gilt es nicht nur, entsprechende Maßnahmen für die Unternehmen festzulegen, sondern auch die Zusammenarbeit der zuständigen Behörden untereinander zu stärken und damit auch schnelle und abgestimmte Verfahren zu entwickeln, die in Sicherheitsfällen ein schnelles Handeln ermöglichen.

In einem weiteren Schritt gilt es zu eruieren, ob und inwieweit Anreize für die Unternehmen in weitere Investitionen in gesicherte Infrastrukturen und die Sicherheit der Telekommunikationsdienste gesetzt werden können.

Aber auch organisatorische Ansatzpunkte in Bezug auf ein gemeinsames Vorgehen der Unternehmen und der Behörden stellen einen wichtigen Punkt dar. So wurden seitens der Unternehmen im Rahmen des Strategiepapiers gemeinsame Lagezentren und Übungen als wirksame Maßnahmen identifiziert, um in Zusammenarbeit mit der Branche und der öffentlichen Hand schnell und wirkungsvoll in Krisenfällen und Sicherheitsfällen agieren zu können.

Auch die Herausforderungen einer wirkungsvollen Zusammenarbeit innerhalb Europas in Bezug auf innere und äußere Sicherheitsaspekte sowie deren Kompetenzen und Grenzen gilt es in den Blick zu nehmen, da gerade die Fragen der Cybersicherheit nicht an Ländergrenzen Halt machen darf.

Ebenso ist auch in den Blick zu nehmen, ob die Konkretisierung von bestehenden gesetzlichen Regelungen oder auch deren Weiterentwicklung für die Verbesserung der Sicherheit der Infrastrukturen und der Cybersicherheit notwendig oder sinnvoll sein könnte. Die Bundesnetzagentur wird sich insofern auch im Gesetzgebungsverfahren zum KRITIS-Dachgesetz aktiv einbringen.

Die Weiterentwicklung von Überlegungen und gegebenenfalls Regelungen zur Stärkung der Sicherheit der Telekommunikationsnetze und der Cybersicherheit sind von großer Bedeutung für die nationale und internationale Sicherheit. Hierzu bedarf es einer konstruktiven Zusammenarbeit mit den Marktteilnehmern und den zuständigen Behörden, aber auch der Wissenschaft und Forschung. Hierfür gilt es angesichts der jüngsten Bedrohungslagen schnellstmöglich Lücken und mögliche Regelungsbedarfe zu erkennen und zu beseitigen.

Mit freundlichen Grüßen
Klaus Müller