ANTWORTEN DER EUROPÄISCHEN KOMMISSION AUF DEN SONDERBERICHT DES EUROPÄISCHEN RECHNUNGSHOFES: „5G-AUSBAU IN DER EU: VERZÖGERUNGEN BEI DER EINFÜHRUNG DER NETZE UND UNGELÖSTE SICHERHEITSPROBLEME“

ZUSAMMENFASSUNG

Einführende Bemerkungen der Kommission

I. Eine zügige und sichere Einführung der 5G-Netze hat für die Europäische Kommission (im Folgenden „Kommission“) hohe Priorität. Beim Schutz der 5G-Netze gegen Bedrohungen durch Cyberkriminalität geht es um die Bewertung und Minderung von Bedrohungen und Risiken. Die Mitgliedstaaten haben diese Bedrohungen und Risiken mit Unterstützung der Kommission und der Agentur der Europäischen Union für Cybersicherheit (im Folgenden „ENISA“) gemeinsam ermittelt und bewertet; darauf aufbauend wurde eine Reihe umfassender Maßnahmen zur Begrenzung dieser Risiken erarbeitet. Während die entsprechenden Arbeiten in einigen Mitgliedstaaten noch laufen, haben die meisten Mitgliedstaaten die Sicherheitsanforderungen für 5G-Netze bereits auf der Grundlage des EU-Instrumentariums gestärkt oder sind zurzeit dabei, sie zu stärken.

Das EU-Instrumentarium wurde als umfassender Rahmen für den Umgang mit Sicherheitsrisiken von 5G-Netzen anerkannt.

Die auf EU-Ebene koordinierte Maßnahme zur 5G-Cybersicherheit und das EU-Instrumentarium sind Teil eines umfassenderen europäischen Rahmens für den Schutz elektronischer Kommunikationsnetze und anderer kritischer Infrastrukturen und ergänzen bestehende Maßnahmen, wie den Europäischen Kodex für die elektronische Kommunikation, den Rechtsrahmen für die Telekommunikation, den Rechtsakt zur Cybersicherheit sowie die Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie) und, je nach Sachverhalt, die im Vertrag und in der Charta der Grundrechte der Europäischen Union verankerten Freizügigkeitsbestimmungen.

III. In den kommenden Jahren wird 5G in unserer digitalen Wirtschaft und Gesellschaft eine zentrale Rolle spielen. Wir müssen die Cybersicherheit der 5G-Netze gewährleisten und dafür sorgen, dass sie widerstandsfähig gegen zunehmende Cyberbedrohungen und -vorfälle sind. Deshalb haben die Kommission und die Mitgliedstaaten einen Koordinierungsprozess zur Festlegung und Umsetzung eines umfassenden 5G-Sicherheitsrahmens eingeführt und sich im Januar 2020 auf ein Instrumentarium an Risikominderungsmaßnahmen verständigt, um die größten Risiken für 5G-Netze, wie kriminelle Hackerangriffe, Spionage und Sabotage, in koordinierter Weise wirksam zu bekämpfen. Während die entsprechenden Arbeiten in einigen Mitgliedstaaten noch laufen, haben die meisten Mitgliedstaaten die Sicherheitsanforderungen für 5G-Netze bereits auf der Grundlage des EU-Instrumentariums gestärkt oder sind zurzeit dabei, sie zu stärken.

VII. Das EU-Instrumentarium bildet einen Rahmen zur Förderung einheitlicher Regelungen im Binnenmarkt bei gleichzeitiger Achtung der Zuständigkeiten im Bereich der nationalen Sicherheit.

In Bezug auf die Vorgehensweise der Mitgliedstaaten gegenüber mit hohem Risiko behafteten Anbietern wird nach Ansicht der Kommission eine abschließende Bewertung erst möglich sein, wenn mehr Informationen vorliegen.

Parallel zur Umsetzung arbeitet die Kommission in der NIS-Kooperationsgruppe mit den Mitgliedstaaten daran, die Angleichung und Konvergenz der nationalen Herangehensweisen zu fördern.

IX. Erster Aufzählungspunkt – Die Kommission akzeptiert die Empfehlung.

Zweiter Aufzählungspunkt – Die Kommission akzeptiert die Empfehlung.

Dritter Aufzählungspunkt – Die Kommission akzeptiert die Empfehlung.

Die Kommission wird die nationalen Zuständigkeiten bei der Bewertung berücksichtigen.

EINLEITUNG

04. Die Kommission erkennt an, dass Sicherheitsrisiken für 5G-Netze bestehen, weist jedoch darauf hin, dass die 5G-Netztechnologien und -standards auch Verbesserungen der Sicherheit gegenüber früheren Generationen von Netzen mit sich bringen können.

BEMERKUNGEN

30. Obwohl 4G bereits eine Vielzahl von Diensten unterstützen kann, dürfte 5G einen deutlichen Sprung und damit eine große Veränderung gegenüber 4G darstellen; die größte Herausforderung wird also darin liegen, den Wechsel von 4G auf 5G mit Einführung von 5G in der gesamten EU zu vollziehen. Es besteht immer das Risiko einer digitalen Kluft; es ist jedoch geplant, dieses Risiko im Politikprogramm „Weg in die digitale Dekade“ im Zusammenhang mit den Zielpfaden auf dem Weg zur 100%igen 5G-Abdeckung in allen besiedelten Gebieten bis 2030 als politische Priorität zu behandeln, sodass die Mitgliedstaaten dabei unterstützt werden, diesbezüglich – insbesondere mit Blick auf den Zugang im ländlichen Raum – tätig zu werden.

32. Die 5G-Beobachtungsstelle war eine zuverlässige Quelle für die Überwachung der 5G-Einführung in- und außerhalb der EU, auch wenn einige Mängel zu verzeichnen waren. Die Dienststellen der Kommission gehen davon aus, dass mit dem neuen Auftragnehmer aktuellere Informationen verfügbar sein werden.

Gemeinsame Antwort der Kommission zu den Ziffern 48 und 49:

Nach Auffassung der Kommission waren die Wahl des Instruments (Empfehlung) und der kooperative Ansatz, bei der Ermittlung der Risiken und der Festlegung der Minderungsmaßnahmen mit den Mitgliedstaaten zusammenzuarbeiten, der geeignetste Weg, um den Sicherheitsrisiken von 5G-Netzen zügig, wirksam und in abgestimmter Weise zu begegnen.

Die Kommission entschied sich angesichts der Komplexität und des Querschnittscharakters des Themas, das Zuständigkeiten sowohl auf nationaler als auch auf EU-Ebene berührt, und aufgrund seiner hohen Relevanz für nationale Sicherheitsinteressen für das Instrument der Empfehlung und für die Zusammenarbeit mit den Mitgliedstaaten. Zudem hat die Kommission berücksichtigt, dass die nationalen Rahmenbedingungen (im Hinblick auf Marktstruktur, Fähigkeiten im Bereich der Cybersicherheit, nachrichtendienstliche Bedrohungsdaten usw.) in den Mitgliedstaaten stark voneinander abweichen.

Das EU-Instrumentarium ist ein flexibles, risikobasiertes Werkzeug für den Umgang mit Herausforderungen für die Sicherheit, das es ermöglicht, Aspekte der 5G-Cybersicherheit zügig und wirksam zu handhaben.

In ihrer Mitteilung „Sichere 5G-Einführung in der EU – Umsetzung des EU-Instrumentariums“ vom Januar 2020 kündigte die Kommission an, dass sie die Umsetzung von Maßnahmen des Instrumentariums in Bezug auf Sicherheitsanforderungen, insbesondere im Hinblick auf die einschlägigen Bestimmungen im Rahmen der europäischen Vorschriften für die elektronische Kommunikation, unterstützen und den Mehrwert möglicher Durchführungsrechtsakte, in denen die technischen und organisatorischen Sicherheitsmaßnahmen im Einzelnen festgelegt werden, prüfen wird, um die nationalen Vorschriften zu ergänzen und die den Betreibern auferlegten Sicherheitsmaßnahmen wirksamer und kohärenter zu gestalten.

Gemeinsame Antwort der Kommission zu den Ziffern 51 und 52:

Im Rahmen der im Dezember 2020 durchgeführten Überprüfung der Empfehlung der Kommission hat die Kommission die zuständigen Behörden aller Mitgliedstaaten befragt. Sie beurteilten das

koordinierte Handeln Europas im Bereich der 5G-Cybersicherheit als zügig, wirksam und verhältnismäßig. Die Zusammenarbeit zwischen den nationalen Behörden, der Kommission, der ENISA und anderen relevanten Akteuren wurde als geeigneter Weg für den Umgang mit diesem komplexen Thema angesehen. Der Ansatz ermöglichte eine zügige Festlegung gemeinsamer Ziele und Methoden und erlaubte es den Mitgliedstaaten gleichzeitig, die Maßnahmen an ihre nationalen Rahmenbedingungen anzupassen.

Im EU-Instrumentarium und in dem von der NIS-Kooperationsgruppe im Juli 2020 veröffentlichten Fortschrittsbericht wird empfohlen, Umsetzungspläne und/oder Übergangsfristen für diejenigen Betreiber festzulegen, die Ausrüstung von mit hohem Risiko behafteten Anbietern verwenden oder die vor der Annahme des EU-Instrumentariums bereits Verträge mit solchen Anbietern geschlossen hatten (indem z. B. die Aktualisierungszyklen der Ausrüstung berücksichtigt werden, insbesondere der Übergang von „nicht eigenständigen“ hin zu „eigenständigen“ 5G-Netzen).

55. Die Kommission nimmt die Bemerkungen des Europäischen Rechnungshofes zur Kenntnis.

Zur weiteren Unterstützung ihrer Umsetzung wurden die im Instrumentarium vorgesehenen Kriterien für die Bewertung von mit hohem Risiko behafteten Anbietern seit Verabschiedung des EU-Instrumentariums im Rahmen der NIS-Kooperationsgruppe mehrfach zwischen den zuständigen nationalen Behörden erörtert.

56. Im EU-Instrumentarium wird empfohlen, bei der Bewertung des Risikoprofils von Anbietern den in der EU-weit koordinierten Risikobewertung genannten Risikofaktoren ebenso wie den länderspezifischen Informationen (z. B. Bedrohungsanalysen der nationalen Sicherheitsdienste usw.) Rechnung zu tragen.

61. Die Gewährleistung der Versorgungssicherheit durch den Anbieter ist eines der Kriterien, die im EU-Instrumentarium für die Bewertung des Risikoprofils eines Anbieters empfohlen werden. Die Fähigkeit zur Gewährleistung der Versorgungssicherheit könnte, wie in der EU-weit koordinierten Risikobewertung im Risikoszenario zur „Abhängigkeit“ erwähnt, auch durch etwaige Handelssanktionen gegen einen bestimmten Anbieter beeinträchtigt werden.

Gemeinsame Antwort der Kommission zu den Ziffern 70 und 73:

Die Kommission und die Mitgliedstaaten tauschen im Rahmen der NIS-Kooperationsgruppe detaillierte Informationen über die Umsetzung des Instrumentariums auf nationaler Ebene aus. Die Frage der Offenlegung nicht öffentlicher Informationen ist Sache der Mitgliedstaaten.

Gemeinsame Antwort der Kommission zu den Ziffern 74 bis 76 und Kasten 5:

Das EU-Instrumentarium bildet einen Rahmen zur Förderung einheitlicher Regelungen im Binnenmarkt bei gleichzeitiger Achtung der Zuständigkeiten im Bereich der nationalen Sicherheit.

In Bezug auf die Vorgehensweise der Mitgliedstaaten gegenüber mit hohem Risiko behafteten Anbietern wird nach Ansicht der Kommission eine abschließende Bewertung erst möglich sein, wenn mehr Informationen vorliegen.

Parallel zur Umsetzung arbeitet die Kommission in der NIS-Kooperationsgruppe mit den Mitgliedstaaten daran, die Angleichung und Konvergenz der nationalen Herangehensweisen zu fördern.

SCHLUSSFOLGERUNGEN UND EMPFEHLUNGEN

81. Eine zügige und sichere Einführung der 5G-Netze hat für die Kommission hohe Priorität. Beim Schutz der 5G-Netze gegen Bedrohungen durch Cyberkriminalität geht es um die Bewertung und Minderung von Bedrohungen und Risiken. Die Mitgliedstaaten haben diese Bedrohungen und Risiken mit Unterstützung der Kommission und der ENISA gemeinsam ermittelt und bewertet; darauf aufbauend wurde eine Reihe umfassender Maßnahmen zur Begrenzung dieser Risiken erarbeitet. Während die entsprechenden Arbeiten in einigen Mitgliedstaaten noch laufen, haben die meisten

Mitgliedstaaten die Sicherheitsanforderungen für 5G-Netze bereits auf der Grundlage des EU-Instrumentariums gestärkt oder sind zurzeit dabei, sie zu stärken.

Das EU-Instrumentarium bietet einen umfassenden Rahmen für den Umgang mit Sicherheitsrisiken von 5G-Netzen.

83. 5G stellt einen deutlichen Sprung gegenüber der 4G-Technologie dar, sodass die größte Herausforderung bei der Vermeidung der digitalen Kluft darin liegen wird, den Wechsel von 4G auf 5G in der gesamten EU zu vollziehen.

Die 5G-Spezifikationen umfassen eine ganze Reihe an Leistungsindikatoren, die insbesondere mit Fällen der vertikalen Nutzung verbunden sind. Dies kann unter anderem Anforderungen in Bezug auf die Zuverlässigkeit, die Geschwindigkeit der Dienstinstanziierung, die Flexibilität der Umsetzung und das Sicherheitsniveau betreffen.

Empfehlung 1 − Fördern einer gleichmäßigen und zügigen Einführung von 5G-Netzen in der EU

a) Die Kommission akzeptiert die Empfehlung.

Die Kommission arbeitet gemeinsam mit den Mitgliedstaaten daran, eine gemeinsame Definition der erwarteten Dienstqualität von 5G-Netzen zu entwickeln. Die Kommission beabsichtigt, im Zusammenhang mit der Digitalen Dekade und dem Vorschlag für einen Beschluss über ein Programm für die Digitalpolitik 2030 mit den Mitgliedstaaten einen gemeinsamen Ansatz in Bezug auf die Dienstqualität von 5G-Netzen in der EU zu erarbeiten, der auch die Vergleichbarkeit von Messgrößen und Überwachungsdaten umfasst.

Die Dienstqualität betrifft nicht nur Geschwindigkeit und Latenz, sondern eine ganze Reihe von Leistungsindikatoren, insbesondere im Zusammenhang mit Fällen der vertikalen Nutzung.

Die Kommission beabsichtigt, gemeinsam mit den Mitgliedstaaten eine Definition solcher Messgrößen zu erarbeiten, jährliche Überprüfungen durchzuführen und Strategien, Maßnahmen und Aktionen zu empfehlen, um bis 2030 eine vollständige 5G-Abdeckung zu erreichen.

Mit dem Programm für die Digitalpolitik wird eine robuste Governance in Form eines Überwachungs- und Kooperationsmechanismus eingeführt, um zu gewährleisten, dass Fortschritte in Bezug auf die Ziele des Politikprogramms – einschließlich der 5G-Einführung – erzielt werden, und es sollen den Mitgliedstaaten entsprechende Abhilfemaßnahmen empfohlen werden.

b) Die Kommission akzeptiert die Empfehlung.

c) Die Kommission akzeptiert die Empfehlung.

Empfehlung 2 − Unterstützung eines abgestimmten Vorgehens im Hinblick auf die 5G-Sicherheit in den Mitgliedstaaten

a) Die Kommission akzeptiert die Empfehlung.

Die Kommission wird gemeinsam mit den Mitgliedstaaten prüfen, inwieweit weitere Maßnahmen oder Unterstützung benötigt werden, beispielsweise in Form von Leitlinien zu bestimmten Aspekten des EU-Instrumentariums.

b) Die Kommission akzeptiert die Empfehlung.

Die Überwachung und Berichterstattung wird von der Kommission in enger Zusammenarbeit mit den Mitgliedstaaten und der ENISA durchgeführt.

c) Die Kommission akzeptiert die Empfehlung.

Empfehlung 3 – Befassung mit den Auswirkungen der unterschiedlichen Ansätze der Mitgliedstaaten im Bereich der 5G-Sicherheit auf das wirksame Funktionieren des Binnenmarkts

a) Die Kommission akzeptiert die Empfehlung.

b) Die Kommission akzeptiert die Empfehlung.

Die Kommission wird die nationalen Zuständigkeiten bei der Bewertung berücksichtigen.

Im EU-Instrumentarium ist vorgesehen, dass die Mitgliedstaaten über den genauen Umfang der geeigneten bzw. notwendigen Ausschlüsse bei wichtigen Anlagen und Einrichtungen entscheiden, die in der EU-weit koordinierten Risikobewertung als kritisch und anfällig eingestuft wurden (z. B. Kernnetzfunktionen, Netzverwaltungs- und -koordinierungsfunktionen sowie Zugangsnetzfunktionen), um die – auch unter Berücksichtigung der Bedrohungsanalysen der nationalen Nachrichtendienste – festgestellten Risiken wirksam zu mindern. Die Mitgliedstaaten haben das Recht, Maßnahmen im Zusammenhang mit der nationalen Sicherheit zu treffen, einschließlich etwaiger Beschränkungen oder Ausschlüsse im Falle von mit hohem Risiko behafteten Anbietern.