Sichere 5G-Netze: Fragen und Antworten zum EU-Instrumentarium

Brüssel, 29. Januar 2020

Warum ist die Cybersicherheit von 5G-Netzen so wichtig?

Als wichtige Voraussetzung für künftige digitale Dienste werden 5G-Netze in den kommenden Jahren eine wesentliche Rolle bei der Entwicklung unserer digitalen Wirtschaft und Gesellschaft spielen. Von der personalisierten Medizin bis hin zur Präzisionslandwirtschaft, von intelligenten Energienetzen bis hin zu vernetzter Mobilität wird sich 5G potenziell auf fast alle Lebensbereiche der Bürgerinnen und Bürger der EU auswirken. Gleichzeitig bieten 5G-Netze unter anderem wegen der weniger zentralisierten Architektur, modernster intelligenter Rechenkapazitäten, des Bedarfs an mehr Antennen und der zunehmenden Abhängigkeit von Software mehr potenzielle Angriffspunkte. Daher ist es von größter Bedeutung, die Sicherheit der künftigen 5G-Netze der EU zu gewährleisten.

Die sichere Einführung von 5G ist zwar weitgehend Sache der Betreiber, und die Mitgliedstaaten sind für die nationale Sicherheit zuständig, aber die Sicherheit der Netze ist von strategischer Bedeutung für die gesamte EU. Ein koordinierter Ansatz auf der Grundlage robuster Sicherheitsmaßnahmen, die auf nationaler und auf EU-Ebene getroffen werden, wird Europa dabei helfen, eine der führenden Regionen beim 5G-Ausbau zu bleiben.

Worum geht es beim EU-Instrumentarium für die 5G-Cybersicherheit?

Mithilfe dieses EU-Instrumentariums für die 5G-Cybersicherheit soll ein koordinierter Ansatz auf der Grundlage einer Reihe gemeinsamer Maßnahmen verfolgt werden, mit denen die größten Risiken für die Cybersicherheit von 5G-Netzen, auf die in dem EU-weit koordinierten Risikobewertungsbericht hingewiesen wurden, gemindert werden sollen. Außerdem soll es als Orientierungshilfe bei der Auswahl und Priorisierung von Maßnahmen dienen, die Teil der nationalen und EU-Risikominderungspläne sein sollten. Das Ziel besteht letztlich darin, einen soliden und objektiven Rahmen für Sicherheitsmaßnahmen zu schaffen, der ein angemessenes Cybersicherheitsniveau von 5G-Netzen in der gesamten EU gewährleistet. Dazu werden Empfehlungen für ein koordiniertes Vorgehen unter den Mitgliedstaaten gegeben. Dieser Ansatz wahrt in vollem Umfang die Offenheit des EU-Binnenmarkts, ist risikobasiert und beruht ausschließlich auf Sicherheitserwägungen.

Welche Hauptschlussfolgerungen enthält das Instrumentarium?

Das Instrumentarium enthält Empfehlungen für eine Reihe von Schlüsselmaßnahmen, die von den Mitgliedstaaten und/oder der Kommission ergriffen werden sollen.

Die Mitgliedstaaten haben sich geeinigt, dafür zu sorgen, dass sie über Maßnahmen verfügen (einschließlich entsprechender Befugnisse der nationalen Behörden), um angemessen und verhältnismäßig auf die bereits ermittelten Risiken und auf mögliche künftige Risiken reagieren zu können. Sie haben insbesondere vereinbart, dafür zu sorgen, dass sie in der Lage sind, auf der Grundlage eines risikobasierten Ansatzes bestimmte Anforderungen und Bedingungen für die Bereitstellung, den Ausbau und den Betrieb von 5G-Netzausrüstungen zu beschränken, zu verbieten und/oder vorzuschreiben. Insbesondere sollten sie:

- die **Sicherheitsanforderungen an Mobilfunknetzbetreiber verschärfen** (z. B. strenge Zugangskontrollen, Vorschriften für sicheren Betrieb und sichere Überwachung, Beschränkungen für die Auslagerung bestimmter Funktionen usw.);
- die Risikoprofile der Anbieter bewerten die Risikoprofile der Anbieter bewerten und in der Folge **auf Anbieter, die als mit einem hohen Risiko behaftet gelten, einschlägige Beschränkungen anwenden, darunter den Ausschluss von Anbietern zur wirksamen Minderung der Risiken für wichtige Anlagen und Einrichtungen**, die in der EU-weit koordinierten Risikobewertung als kritisch und anfällig eingestuft wurden (z. B. Kernnetzfunktionen, Netzverwaltungs- und Koordinierungsfunktionen sowie

Zugangsnetzfunktionen);

- sicherstellen, dass jeder Betreiber über eine angemessene herstellerneutrale Strategie verfügt, um **eine größere Abhängigkeit** von einem einzigen Anbieter (oder Anbietern mit ähnlichem Risikoprofil) **zu vermeiden oder zu begrenzen**, für ein angemessenes Gleichgewicht zwischen den Anbietern auf nationaler Ebene sorgen und eine **Abhängigkeit von Anbietern vermeiden, die als mit einem hohen Risiko behaftet gelten**; dazu muss auch jede feste Bindung *(„lock-in")* an einen einzigen Anbieter vermieden werden, unter anderem durch die Förderung einer größeren Interoperabilität der Anlagen und Ausrüstungen.

In dem Instrumentarium wird empfohlen, dass die Kommission gemeinsam mit den Mitgliedstaaten zu Folgendem beitragen sollte:

- Aufrechterhaltung einer **diversifizierten und zukunftsträchtigen 5G-Lieferkette**, um eine langfristige Abhängigkeit zu vermeiden, unter anderem durch

o die umfassende Nutzung der bestehenden Werkzeuge und Instrumente der EU, insbesondere durch die Überprüfung ausländischer Direktinvestitionen mit Auswirkungen auf wichtige 5G-Anlagen und Einrichtungen und durch die Vermeidung von Verzerrungen auf dem 5G-Zuliefermarkt aufgrund von potenziellem Dumping oder möglichen Subventionen und

o die weitere Stärkung der **Kapazitäten der EU im Bereich der 5G-Technik und deren Folgetechnik** durch Nutzung der einschlägigen EU-Programme und Fördermittel.

- Erleichterung der Koordinierung zwischen den Mitgliedstaaten im Bereich der **Normung**, um spezifische Sicherheitsziele zu erreichen, und Entwicklung **einschlägiger EU-weiter Zertifizierungssysteme**, um sicherere Produkte und Verfahren zu fördern.

Wie ist der Stand der Umsetzung des Instrumentariums für die 5G-Cybersicherheit in den Mitgliedstaaten?*

- Am 24. Juli 2020 veröffentlichten die EU-Mitgliedstaaten mit Unterstützung der Kommission und der EU-Cybersicherheitsagentur ENISA einen Bericht über die erzielten Fortschritte bei der Umsetzung des gemeinsamen EU-Instrumentariums der Risikominderungsmaßnahmen, das von den Mitgliedstaaten vereinbart und im Januar 2020 mit einer Mitteilung der Kommission gebilligt wurde.
- Dem Bericht zufolge wurden bei einigen der Maßnahmen des Instrumentariums bereits gute Fortschritte erzielt, insbesondere in folgenden Bereichen:

o Die **Befugnisse der nationalen Regulierungsbehörden zur Regulierung der 5G-Sicherheit** wurden oder werden derzeit in einer großen Mehrheit der Mitgliedstaaten gestärkt, einschließlich der Befugnisse zur Regulierung der Beschaffung von Netzausrüstungen und Idiensten durch die Betreiber.

o In einigen Mitgliedstaaten bestehen bereits Maßnahmen, mit denen die **Beteiligung von Anbietern auf der Grundlage ihres Risikoprofils beschränkt** werden soll. In vielen anderen Mitgliedstaaten befinden sich die Vorbereitungen für solche Maßnahmen bereits in einem fortgeschrittenen Stadium. In dem Bericht werden die anderen Mitgliedstaaten aufgefordert, diesen Prozess in den kommenden Monaten weiter voranzubringen und abzuschließen. Hinsichtlich des genauen Umfangs dieser Beschränkungen wird im Bericht unterstrichen, wie wichtig es ist, das Netz in seiner Gesamtheit zu betrachten und neben dem Kernnetz auch andere kritische und hochsensible Elemente wie z. B. die Verwaltungsfunktionen und das Funkzugangsnetz zu berücksichtigten sowie Beschränkungen auch für andere maßgebliche Elemente wie festgelegte geografische Gebiete, Regierungs- und andere kritische Stellen Beschränkungen einzuführen.

o Die **Anforderungen an Mobilfunkbetreiber in Bezug auf die Netzsicherheit und -widerstandsfähigkeit** werden derzeit in den meisten Mitgliedstaaten überprüft. In dem Bericht wird hervorgehoben, dass unbedingt für eine Verschärfung dieser Anforderungen gesorgt werden muss, dass diese dem neuesten Stand entsprechen müssen und dass ihre Umsetzung durch die Betreiber wirksam geprüft und durchgesetzt werden muss.

- Bei anderen Maßnahmen ist die Umsetzung noch nicht so weit gediehen. So wird in dem Bericht insbesondere Folgendes festgestellt:

o Es sind dringend Fortschritte erforderlich, um die **Gefahr der Abhängigkeit von Hochrisikoanbietern** zu mindern, auch im Hinblick auf die Verringerung der Abhängigkeiten auf Unionsebene. Dies sollte auf einer gründlichen Bestandsaufnahme der Lieferkette der Netze beruhen und erfordert auch eine fortlaufende Überwachung der Lage.

o Bei der **Konzipierung und Einführung angemessener herstellerneutraler Strategien für einzelne Betreiber oder auf nationaler Ebene** wurden Probleme festgestellt, die durch technische oder operative Schwierigkeiten (z. B. mangelnde Interoperabilität, Größe des Landes usw.) bedingt sind.

o Hinsichtlich der **Überprüfung ausländischer Direktinvestitionen** sollten Schritte unternommen werden, um in 13 Mitgliedstaaten, in denen dieser Mechanismus noch nicht besteht, unverzüglich einen nationalen Überprüfungsmechanismus für ausländische Direktinvestitionen einzuführen, auch im Hinblick auf die bevorstehende Anwendung des EU-Rahmens für die Überprüfung von Investitionen ab Oktober 2020. Diese Überprüfungsmechanismen sollten bei investitionsbezogenen Entwicklungen greifen, die die 5G-Wertschöpfungskette beeinträchtigen könnten, wobei die Ziele des Instrumentariums zu berücksichtigen sind.

Was sollten die nationalen Behörden tun, um die Umsetzung des Instrumentariums voranzutreiben?*

- **Vollendung des Umsetzungsprozesses** auf nationaler Ebene **unter besonderer Berücksichtigung der Elemente**, die im Fortschrittsbericht hervorgehoben wurden;
- **verstärkter Austausch von Informationen über Herausforderungen, bewährte Verfahren und Lösungen** für die Umsetzung der Maßnahmen des Instrumentariums;
- Fortsetzung der **Überwachung und Bewertung der Umsetzung des Instrumentariums**;
- Fortsetzung der Zusammenarbeit mit der Kommission zur Umsetzung der im Instrumentarium aufgeführten Maßnahmen auf EU-Ebene, unter anderem in den Bereichen **Normung und Zertifizierung**, handelspolitische Schutzinstrumente und Wettbewerbsregeln, um Verzerrungen auf dem 5G-Zuliefermarkt zu vermeiden;
- darüber hinaus **Investitionen in die Kapazitäten der EU** in den Bereichen 5G-Technik und deren Folgetechnik und Sicherstellung, dass mit öffentlichen Mitteln geförderte 5G-Projekte den Cybersicherheitsrisiken Rechnung tragen.

Welche verschiedenen Arten von Maßnahmen sind in dem EU-Instrumentarium vorgesehen?

Für jeden der neun Risikobereiche, die im Bericht über die EU-weit koordinierte Risikobewertung genannt wurden, sieht das Instrumentarium Risikominderungspläne vor. Sie bestehen aus möglichen Kombinationen strategischer und technischer Maßnahmen.

- Die **strategischen Maßnahmen** des Instrumentariums reichen von erweiterten Regulierungsbefugnissen der Behörden zur Kontrolle der Beschaffung und des Ausbaus der Netze über besondere Maßnahmen zur Bewältigung von Risiken im Zusammenhang mit nichttechnischen Schwachstellen (z. B. Risiko von Eingriffen durch Drittstaaten oder von Drittstaaten unterstützte Akteure) bis hin zur Bewertung des Risikoprofils der Anbieter und zur Förderung von Initiativen, mit denen die Entwicklung zukunftsfähiger und diversifizierter 5G-Anbieter unterstützt wird.
- Die **technischen Maßnahmen** des Instrumentariums reichen von einer strengen Zugangskontrolle und einem sicheren Netzmanagement und -betrieb und deren Überwachung bis hin zur Zertifizierung von 5G-Netzkomponenten und -prozessen.
- Die **Unterstützungsmaßnahmen** betreffen Bereiche wie 5G-Normen, den Ausbau der Test- und Prüfkapazitäten, die Verbesserung der Koordinierung bei Sicherheitsvorfällen oder die volle Berücksichtigung von Cybersicherheitsrisiken in den von der EU geförderten 5G-Projekten. Diese Unterstützungsmaßnahmen sollen die strategischen und technischen Maßnahmen überhaupt erst ermöglichen, ihre Durchführung unterstützen und ihre Wirksamkeit erhöhen.

Was ist ein Risikominderungsplan?

Für jeden der neun Risikobereiche, die im Bericht über die EU-weit koordinierte Risikobewertung genannt wurden, sieht das Instrumentarium Risikominderungspläne vor. Sie bestehen aus möglichen Kombinationen strategischer und/oder technischer Maßnahmen (zusammen mit geeigneten Unterstützungsmaßnahmen) zur Minderung eines Sicherheitsrisikos.

Sind die Maßnahmen des Instrumentariums verbindlich?

Beim EU-Instrumentarium für die 5G-Cybersicherheit handelt es sich um ein Dokument, das von der NIS-Kooperationsgruppe einvernehmlich ausgearbeitet wurde. Die Gruppe besteht aus Vertretern der Behörden aller Mitgliedstaaten, der Kommission und der EU-Cybersicherheitsagentur. Die Entwicklung eines koordinierten EU-Ansatzes für die 5G-Cybersicherheit ist davon abhängig, dass sich sowohl die Mitgliedstaaten als auch die Kommission nachdrücklich dazu verpflichten, empfohlene Schlüsselmaßnahmen anzuwenden und vollständig umzusetzen. Das Instrumentarium legt eine genaue und objektive Methodik für den Umgang mit den Risiken fest, die in der im Oktober 2019 veröffentlichten europäischen Risikobewertung aufgeführt sind, wobei die nationalen Zuständigkeiten in diesem Bereich zu beachten sind.

Ausbau und Betrieb der 5G-Netze sind gleichzeitig eine Frage der nationalen Sicherheit. Die Mitgliedstaaten können über die im Instrumentarium vorgeschlagenen Maßnahmen hinausgehen, wenn sie dies für notwendig erachten.

Wie wird das EU-Instrumentarium umgesetzt werden?

Um die festgestellten Risiken wirksam zu mindern, wird eine geeignete Kombination verschiedener Arten von Maßnahmen benötigt. So werden die Mitgliedstaaten eine ganze Reihe von Risikominderungsmaßnahmen ergreifen müssen, um den Sicherheitsrisiken im Zusammenhang mit 5G-Netzen wirksam begegnen zu können. Je nach Art der spezifischen Maßnahmen und Aktionen kann auf nationaler und/oder EU-Ebene vorgegangen werden. Einige Maßnahmen können direkt auf nationaler Ebene eingeführt oder verstärkt werden, während in anderen Fällen weitere oder gemeinsame Maßnahmen auf EU-Ebene – unter Wahrung der jeweiligen Zuständigkeiten der Mitgliedstaaten und der EU – erforderlich werden können.

Geht das Instrumentarium auf das Risiko von Eingriffen aus Drittländern ein?

Das Instrumentarium erstreckt sich auf alle Risiken, die im Zuge der EU-weit koordinierten Bewertung ermittelt wurden, einschließlich solcher in Verbindung mit Eingriffen durch Drittstaaten über die 5G-Lieferkette. Es zielt nicht auf bestimmte Anbieter oder Länder ab. Um dieses Risiko zu mindern, werden allen Mitgliedstaaten im Instrumentarium die folgenden Schritte empfohlen:

1) Bewertung des Risikoprofils der Anbieter unter Berücksichtigung der in der EU-weit koordinierten Risikobewertung festgelegten Kriterien;

2) in der Folge die Anwendung einschlägiger Beschränkungen auf Anbieter, die als mit einem hohen Risiko behaftet gelten, darunter den Ausschluss von Anbietern zur wirksamen Minderung der Risiken für wichtige Anlagen und Einrichtungen, die als kritisch und anfällig eingestuft wurden (z. B. Kernnetzfunktionen, Netzverwaltungs- und Koordinierungsfunktionen sowie Zugangsnetzfunktionen).

Wie ergänzt die Mitteilung der Kommission das EU-Instrumentarium?

In der Mitteilung der Kommission wird das EU-Instrumentarium unterstützt und ein weiteres Vorgehen für seine Umsetzung vorgeschlagen.Die Kommission wird darüber hinaus den Vorgaben aus dem Instrumentarium folgen und, wo angemessen, alle ihr zur Verfügung stehenden Instrumente nutzen, um die Sicherheit der 5G-Infrastruktur und -Lieferkette zu gewährleisten, darunter:

- Telekommunikations- und Cybersicherheitsvorschriften, z. B. Unterstützung im Rahmen der Vorschriften für die elektronische Kommunikation, einschließlich der Prüfung von Durchführungsrechtsakten über technische und organisatorische Sicherheitsmaßnahmen;
- Koordinierung der Normung, z. B. im Hinblick auf die Beteiligung an Normungsgremien, und Förderung der Interoperabilität durch offene Schnittstellen;
- EU-weite Zertifizierung gemäß dem EU-Rechtsakt zur Cybersicherheit;
- Überprüfung ausländischer Direktinvestitionen zum Schutz der europäischen 5G-Lieferkette;
- handelspolitische Schutzinstrumente: Marktüberwachung und Maßnahmen zum Schutz der EU-Akteure auf dem 5G-Markt vor potenziell handelsverzerrenden Praktiken (Dumping oder Subventionierung);
- Wettbewerbsregeln: Marktüberwachung zur Gewährleistung wettbewerbsorientierter Ergebnisse, auch in Bezug auf eine potenzielle Anbieterbindung („lock-in");
- Vergabe öffentlicher Aufträge, wobei sicherzustellen ist, dass Sicherheitsaspekte dabei gebührend berücksichtigt werden, EU-Förderprogramme und Gewährleistung, dass die

Begünstigten die einschlägigen Sicherheitsanforderungen einhalten;

- umfassende Nutzung der Rahmen für die Reaktion auf Sicherheitsvorfälle und Krisenmanagement auf EU-Ebene, um auf große Cybersicherheitsvorfälle zu reagieren;
- Erhöhung der Investitionen in Forschung, Innovation und Ausbautechnik.

Welche Instrumente stehen auf EU-Ebene zum Schutz der 5G-Netze zur Verfügung?

Die EU verfügt bereits über eine Reihe von Instrumenten zum Schutz elektronischer Kommunikationsnetze:

Nach dem **EU-Telekommunikationsrahmen** können Telekommunikationsbetreibern Verpflichtungen auferlegt werden. Die Mitgliedstaaten müssen die Integrität und Sicherheit der öffentlichen Kommunikationsnetze gewährleisten und dafür sorgen, dass öffentliche Kommunikationsnetze und Idiensten Maßnahmen ergreifen, um Sicherheitsrisiken zu beherrschen. In dem Rahmen ist ferner vorgesehen, dass die zuständigen nationalen Regulierungsbehörden befugt sind, verbindliche Anweisungen zu erteilen, um die Einhaltung der Verpflichtungen sicherzustellen.

Im **europäischen Kodex für die elektronische Kommunikation** (EKEK), der ab dem 21. Dezember 2020 an die Stelle des derzeitigen Rechtsrahmens treten wird, werden die Sicherheitsbestimmungen des derzeitigen Rahmens beibehalten und Vorgaben für die Sicherheit von Netzen und Diensten sowie für Sicherheitsvorfälle gemacht. Darüber hinaus sieht der EKEK vor, dass bei den Sicherheitsmaßnahmen allen relevanten Aspekten bestimmter Elemente in Bereichen wie der Sicherheit von Netzen und Einrichtungen, der Bewältigung von Sicherheitsvorfällen, dem Betriebskontinuitätsmanagement, der Überwachung, Überprüfung und Erprobung sowie der Einhaltung internationaler Standards Rechnung getragen werden sollte.

Die **NIS-Richtlinie** verpflichtet Betreiber wesentlicher Dienste in anderen Bereichen (Energie, Finanzen, Gesundheitswesen, Verkehr, Anbieter digitaler Dienste usw.) geeignete Sicherheitsmaßnahmen zu ergreifen und schwerwiegende Vorfälle der zuständigen nationalen Behörde zu melden. Die NIS-Richtlinie sieht auch eine Koordinierung zwischen den Mitgliedstaaten bei grenzüberschreitenden Sicherheitsvorfällen vor, die Betreiber in ihrem Anwendungsbereich betreffen. In dem heute angenommenen Arbeitsprogramm der Kommission wird die Überarbeitung der Richtlinie noch vor Ende 2020 angekündigt.

Mit dem im Juni 2019 in Kraft getretenen **Rechtsakt zur Cybersicherheit** wird ein Rahmen für die europäische Cybersicherheitszertifizierung von Produkten, Prozessen und Diensten geschaffen. Sobald Zertifizierungssysteme eingeführt sind, können die Hersteller auch nachweisen, dass sie in den frühen Phasen der Produktgestaltung spezifische Sicherheitsmerkmale aufgenommen haben, und die Nutzer können sich EU-weit über das Sicherheitsniveau vergewissern. Der Rahmen stellt ein wichtiges Instrument dar, um ein einheitliches Sicherheitsniveau zu fördern. Dies ermöglicht die Entwicklung von Systemen für die Cybersicherheitszertifizierung, die den Bedürfnissen der Nutzer von 5G-Geräten und -Software entsprechen.

Des Weiteren wird die Kommission die Umsetzung des EU-Instrumentariums unterstützen und, wie von den Mitgliedstaaten gefordert, wo angemessen alle ihr zur Verfügung stehenden Instrumente nutzen, um die Sicherheit der 5G-Infrastruktur und -Lieferkette zu gewährleisten (siehe vorangegangene Frage).

Was sind die nächsten Schritte?

Wie von der NIS-Kooperationsgruppe empfohlen und in der Mitteilung der Kommission unterstützt, werden die Arbeiten in der NIS-Kooperationsgruppe, um die Umsetzung des Instrumentariums zu überwachen und seine wirksame und einheitliche Anwendung sicherzustellen, fortgesetzt.

Die Gruppe wird auch die Abstimmung der nationalen Konzepte fördern, und zwar durch einen weiteren Erfahrungsaustausch und durch die Zusammenarbeit mit dem Gremium europäischer Regulierungsstellen für elektronische Kommunikation (GEREK).

Im Rahmen der Umsetzung der im vergangenen Jahr angenommenen Empfehlung der Kommission sollten die Mitgliedstaaten – in Zusammenarbeit mit der Kommission – bis zum **1. Oktober 2020** die Auswirkungen der Empfehlung bewerten, um festzustellen, ob weitere Maßnahmen erforderlich sind.

Bei dieser Bewertung sollten die Ergebnisse der EU-weit koordinierten Risikobewertung, die im Oktober 2019 veröffentlicht wurde, und die Wirksamkeit der Maßnahmen des Instrumentariums berücksichtigt werden.

* Aktualisiert am 24.7.2020

QANDA/20/127

Kontakt für die Medien:

Johannes BAHRKE (+32 2 295 86 15)
Marietta GRAMMENOU (+32 2 298 35 83)

Kontakt für die Öffentlichkeit: Europe Direct – telefonisch unter 00 800 67 89 10 11 oder per E-Mail