Europäische Kommission - Pressemitteilung

Mitgliedstaaten veröffentlichen Bericht über EU-weit koordinierte Risikobewertung von 5G-Netzen

Brüssel, 9. Oktober 2019

Pressemitteilung der Europäischen Kommission und des finnischen EU-Ratsvorsitzes

Mit Unterstützung der Kommission und der EU-Cybersicherheitsagentur haben die Mitgliedstaaten heute einen Bericht über die EU-weit koordinierte Risikobewertung in Bezug auf die Cybersicherheit in den Netzen der 5. Generation (5G) veröffentlicht.Dieser wichtige Schritt ist Teil der Umsetzung der im März 2019 abgegebenen Empfehlung der Europäischen Kommission zur Gewährleistung eines hohen Cybersicherheitsniveaus der 5G-Netze in der gesamten EU.

5G-Netze sind das künftige Rückgrat unserer zunehmend digitalisierten Volkswirtschaften und Gesellschaften. Sie werden Milliarden von Objekten und Systemen mit einander verbinden, auch in kritischen Sektoren wie Energie, Verkehr, Bank- und Gesundheitswesen, aber auch in industriellen Steuerungssystemen, die sensible Informationen verarbeiten und Sicherheitssysteme unterstützen. Die Gewährleistung der Sicherheit und Widerstandsfähigkeit der 5G-Netze ist daher von größter Bedeutung.

Der Bericht beruht auf den Ergebnissen der nationalen Risikobewertungen, die alle EU-Mitgliedstaaten in Bezug auf ihre Cybersicherheit durchgeführt haben. Darin werden die Hauptbedrohungen und deren Verursacher, die anfälligsten Anlagen und Einrichtungen, die wichtigsten Schwachstellen (technischer und anderer Art) und eine Reihe strategischer Risiken aufgezeigt.

Diese Bewertung bildet die Grundlage für die Ermittlung von Risikominderungsmaßnahmen, die auf nationaler und europäischer Ebene ergriffen werden können.

Wichtigste Erkenntnisse aus der EU-weit koordinierten Risikobewertung

In dem Bericht werden mehrere große **Sicherheitsprobleme** genannt, die in 5G-Netzen auftreten oder – im Vergleich zu den bestehenden Netzen – dort stärker ins Gewicht fallen dürften.

Diese Sicherheitsprobleme stehen hauptsächlich im Zusammenhang mit

- großen *Innovationen* der 5G-Technik (die zugleich eine Reihe spezifischer Sicherheitsverbesserungen mit sich bringen), insbesondere im wichtigen Softwarebereich und im breiten Spektrum der Dienste und Anwendungen, die durch 5G-Technik ermöglicht werden;
- der Rolle der *Lieferanten* beim Aufbau und Betrieb von 5G-Netzen und dem Grad der Abhängigkeit von einzelnen Lieferanten.

Konkret ist davon auszugehen, dass der Aufbau der 5G-Netze folgende Auswirkungen haben wird:

- Eine **erhöhte Angriffsgefahr und mehr potenzielle Ansatzpunkte für Angreifer**: Da 5G-Netze zunehmend auf Software basieren, steigen die Risiken im Zusammenhang mit größeren Sicherheitslücken, z. B. wegen mangelhafter Softwareentwicklungsprozesse bei Lieferanten. Dadurch könnte es auch für Angreifer leichter werden, Hintertüren in die Produkte einzubauen und deren Erkennung zu erschweren.
- Aufgrund der neuen Merkmale der 5G-Netzarchitektur und neuer 5G-Funktionen **werden bestimmte Netzausrüstungen oder Netzfunktionen leichter verwundbar**, z. B. Basisstationen oder wichtige technische Verwaltungsfunktionen der Netze.
- Erhöhte Risiken durch die **Abhängigkeit der Mobilfunknetzbetreiber von ihren Lieferanten**. Dadurch wird sich auch die **Zahl der Angriffspunkte, die von Angreifern ausgenutzt werden könnten**, und die potenzielle Schwere der Folgen solcher Angriffe erhöhen. Unter den verschiedenen potenziellen Akteuren gehen die größten Gefahren von Nicht-EU-Staaten oder von staatlich unterstützten Organisationen aus, die zudem höchstwahrscheinlich 5G-Netze ins Visier nehmen werden.
- Vor diesem Hintergrund einer erhöhten, von Lieferanten begünstigten Angriffsgefahr wird das **Risikoprofil der einzelnen Lieferanten** eine besondere Bedeutung haben, denn es besagt, wie wahrscheinlich ist es, dass der Lieferant dem Einfluss eines Nicht-EU-Landes erliegt.

- **Erhöhte Risiken durch größere Abhängigkeiten von Lieferanten**: Eine große Abhängigkeit von einem einzigen Lieferanten erhöht die Gefahr möglicher Lieferunterbrechungen, was beispielsweise zu geschäftlichen Ausfällen mit allen ihren Folgen führen kann. So verschärft sie auch die möglichen Folgen von Schwachstellen und Anfälligkeiten und deren möglicher Ausnutzung durch Angreifer, insbesondere bei einer Abhängigkeit von einem Lieferanten, der ein hohes Risiko aufweist.
- **Bedrohungen der Verfügbarkeit und Integrität der Netze werden große Sicherheitsbedenken hervorrufen**: Da 5G-Netze voraussichtlich das Rückgrat vieler unverzichtbarer IT-Anwendungen bilden werden, wird neben der Vertraulichkeit und dem Schutz der Privatsphäre auch die Integrität und Verfügbarkeit dieser Netze zu einer wichtigen Frage nationaler Sicherheitsinteressen und zu einer großen sicherheitspolitischen Herausforderung für die EU.

Zusammengenommen entsteht durch alle diese Herausforderungen **ein neues Sicherheitsparadigma**, das es erforderlich macht, den derzeit für diesen Sektor und sein Ökosystem geltenden politischen und sicherheitspolitischen Rahmen zu überprüfen, damit die Mitgliedstaaten die erforderlichen Risikominderungsmaßnahmen ergreifen können.

Die Bedrohungslage aus Sicht der EU-Cybersicherheitsagentur: Ergänzend zu dem Bericht der Mitgliedstaaten stellt die EU-Cybersicherheitsagentur gerade ihren Überblick über die spezifische Bedrohungslage im Zusammenhang mit 5G-Netzen fertig, in dem sie ausführlicher auf bestimmte technische Aspekte des Berichts eingeht.

Nächste Schritte

Bis zum 31. Dezember 2019 sollte sich die Kooperationsgruppe auf ein Instrumentarium von Risikominderungsmaßnahmen einigen, mit dem auf die festgestellten Cybersicherheitsrisiken auf nationaler und Unionsebene reagiert werden soll.

Bis zum 1. Oktober 2020 sollten die Mitgliedstaaten – in Zusammenarbeit mit der Kommission – die Auswirkungen der Empfehlung bewerten, um zu ermitteln, ob weitere Maßnahmen erforderlich sind. Bei dieser Bewertung sollten die Ergebnisse der koordinierten europäischen Risikobewertung und die Wirksamkeit der Maßnahmen berücksichtigt werden.

Hintergrund

Nachdem sie die Unterstützung des Europäischen Rates erhalten hatte, nahm die Kommission am 26. März 2019 eine Empfehlung zur Cybersicherheit von 5G-Netzen an, in der sie die Mitgliedstaaten aufrief, ihre nationalen Risikobewertungen abzuschließen, ihre nationalen Maßnahmen zu überprüfen und auf EU-Ebene zusammenzuarbeiten, um eine EU-weit koordinierte Risikobewertung durchzuführen und ein gemeinsames Instrumentarium von Risikominderungsmaßnahmen zu schaffen.

Auf nationaler Ebene haben alle Mitgliedstaaten nun eine nationale Risikobewertung der 5G-Netzinfrastrukturen abgeschlossen und der Kommission und der EU-Cybersicherheitsagentur (ENISA) die Ergebnisse übermittelt. Im Einklang mit der Empfehlung der Kommission wurde in den nationalen Risikobewertungen insbesondere auf die hauptsächlichen Bedrohungen in Bezug auf 5G-Netze und deren Verursacher, auf verwundbare 5G-Anlagen und Einrichtungen sowie auf einschlägige Anfälligkeiten sowohl technischer als auch anderer Art eingegangen, darunter auch auf die potenziell aus der 5G-Lieferkette erwachsenden Schwachstellen.

IP/19/6049

Kontakt für die Medien:

Nathalie VANDYSTADT (+32 2 296 70 83)
Tove ERNST (+32 2 298 67 64)
Marietta GRAMMENOU (+32 2 298 35 83)
Kasia KOLANKO (+ 32 2 296 34 44)

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