European Commission - Press release

Member States publish a report on EU coordinated risk assessment of 5G networks security

Brussels, 9 October 2019

Press release by the European Commission and the Finnish Presidency of the Council of the EU

Today, Member States, with the support of the Commission and the European Agency for Cybersecurity published a report on the EU coordinated risk assessment on cybersecurity in Fifth Generation (5G) networks. This major step is part of the implementation of the European Commission Recommendation adopted in March 2019 to ensure a high level of cybersecurity of 5G networks across the EU.

5G networks is the future backbone of our increasingly digitised economies and societies. Billions of connected objects and systems are concerned, including in critical sectors such as energy, transport, banking, and health, as well as industrial control systems carrying sensitive information and supporting safety systems. Ensuring the security and resilience of 5G networks is therefore essential.

The report is based on the results of the national cybersecurity risk assessments by all EU Member States. It identifies the main threats and threats actors, the most sensitive assets, the main vulnerabilities (including technical ones and other types of vulnerabilities) and a number of strategic risks.

This assessment provides the basis to identify mitigation measures that can be applied at national and European level.

Main insights of the EU coordinated risk assessment

The report identifies a number of important **security challenges**, which are likely to appear or become more prominent in 5G networks, compared with the situation in existing networks:

These security challenges are mainly linked to:

- key *innovations* in the 5G technology (which will also bring a number of specific security improvements), in particular the important part of software and the wide range of services and applications enabled by 5G;
- the role of *suppliers* in building and operating 5G networks and the degree of dependency on individual suppliers.

Specifically, the roll-out of 5G networks is expected to have the following effects:

- An **increased exposure to attacks and more potential entry points for attackers**: With 5G networks increasingly based on software, risks related to major security flaws, such as those deriving from poor software development processes within suppliers are gaining in importance. They could also make it easier for threat actors to maliciously insert backdoors into products and make them harder to detect.
- Due to new characteristics of the 5G network architecture and new functionalities, **certain pieces of network equipment or functions are becoming more sensitive**, such as base stations or key technical management functions of the networks.
- An increased exposure to risks related to the **reliance of mobile network operators on suppliers**. This will also lead to a higher **number of attacks paths that might be exploited by threat actors** and increase the potential severity of the impact of such attacks. Among the various potential actors, non-EU States or State-backed are considered as the most serious ones and the most likely to target 5G networks.
- In this context of increased exposure to attacks facilitated by suppliers, the **risk profile of individual suppliers** will become particularly important, including the likelihood of the supplier being subject to interference from a non-EU country.
- **Increased risks from major dependencies on suppliers**: a major dependency on a single supplier increases the exposure to a potential supply interruption, resulting for instance from a commercial failure, and its consequences. It also aggravates the potential impact of weaknesses or vulnerabilities, and of their possible exploitation by threat actors, in particular where the

dependency concerns a supplier presenting a high degree of risk.

- **Threats to availability and integrity of networks will become major security concerns**: in addition to confidentiality and privacy threats, with 5G networks expected to become the backbone of many critical IT applications, the integrity and availability of those networks will become major national security concerns and a major security challenge from an EU perspective.

Together, these challenges create a **new security paradigm**, making it necessary to reassess the current policy and security framework applicable to the sector and its ecosystem and essential for Member states to take the necessary mitigating measures.

European Agency for Cybersecurity threat landscape: To complement the Member States' report, the European Agency for Cybersecurity is finalising a specific threat landscape mapping related to 5G networks, which considers in more detail certain technical aspects covered in the report.

Next Steps

By 31 December 2019, the Cooperation Group should agree on a toolbox of mitigating measures to address the identified cybersecurity risks at national and Union level.

By 1 October 2020, Member States – in cooperation with the Commission – should assess the effects of the Recommendation in order to determine whether there is a need for further action. This assessment should take into account the outcome of the coordinated European risk assessment and of the effectiveness of the measures.

Background

On 26 March 2019, after receiving the support from the European Council, the Commission adopted a Recommendation on Cybersecurity of 5G networks calling on Member States to complete national risk assessments and review national measures and to work together at EU level on a coordinated risk assessment and a common toolbox of mitigating measures.

At national level, each Member State has completed a national risk assessment of 5G network infrastructures and transmitted the results to the Commission and ENISA, the EU Agency for cybersecurity. The national risk assessments reviewed in particular main threats and threat actors affecting 5G networks, sensitive 5G assets as well as relevant vulnerabilities, including both technical ones and other types of vulnerabilities, such as those potentially arising from the 5G supply chain, in line with the EC Recommendation.

IP/19/6049

Press contacts:

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)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email