FORSVARSMINISTERIET

NOTITS TIL FOLKETINGETS EUROPAUDVALG

EU's risikovurdering af cybersikkerheden i 5G netværk

25. november 2019

Baggrund
Europa-Kommissionen har udsendt en rapport om risikovurdering af cybersikkerheden i 5G-netværk ("EU coordinated risk assessment of the cybersecurity of 5G networks") den 9. oktober 2019. Rapporten bygger på medlemsstaternes, herunder Danmarks, risikovurdering af 5G-infrastrukturen, som blev fremsendt til Europa-Kommissionen i juli 2019. Risikovurderingen er udarbejdet i henhold til Kommissionens henstilling fra marts 2019 vedr. cybersikkerhed ifm. 5G-teknologi.

Folketingets Europaudvalg blev orienteret skriftligt om henstillingen den 2. maj 2019 (Europaudvalget 2018-19, EUU Alm. del – Bilag 663). Risikovurderingen har ikke i sig selv økonomiske, juridiske eller politiske konsekvenser. Risikovurderingen vil dog danne baggrund for arbejdet med en fælles værktøjskasse med tiltag, der muliggør en effektiv risikohåndtering af 5G-netværk, som beskrevet i henstillingen.

Indhold
Rapporten om risikovurdering af cybersikkerheden i 5G-netværk peger på, at 5G-nettet bliver rygraden i Europas højt digitaliserede og tæt forbundne samfund. Derfor er et højt sikkerhedsniveau essentielt. Risikovurderingens formål er at skabe grundlaget for afbødende foranstaltninger nationalt og på EU-niveau.

Helt overordnet peges der på, at risikoen hænger sammen med 5G-teknologiens grundlæggende innovation, der indebærer visse sikkerhedsforbedringer, men også indebærer en række sikkerhedsudfordringer. Udfordringerne kan henføres til den radikalt ændrede opbygning af nettet sammenlignet med det nuværende mobilnetværk, og at de enkelte leverandører kommer til at spille en større rolle for sikkerheden end i dag.

Hovedelementerne i risikovurderingen er:

- Med 5G forøges angrebsfladen og antallet af mulige angrebspunkter på mellemlangt sigt, idet funktionaliteten i nettet gradvist decentraliseres sammenlignet med de nuværende mobilnetværk, hvor kernefunktionaliteten i vid udstrækning er centraliseret.
- 5G består i større grad af mange forskellige softwarepakker, hvorfor udviklings- og opdateringsprocesser giver anledning til forøget risiko for konfigurationsfejl.
- De nye teknologiske egenskaber i 5G vil forøge mobiloperatørernes afhængighed af underleverandører og øge den sikkerhedsmæssige betydning af forsyningskæden.
- Markedet for teleudstyr udgøres hovedsageligt af en håndfuld globale leverandører. Det øger samlet set sårbarhederne.
- Forsyningskæden kan være særligt sårbar, når der er tale om leverandører under påvirkning af ikke-EU-stater.

5G har i forhold til 2G, 3G og 4G en øget afhængighed af, at den enkelte leverandør ikke fejler. Det giver større muligheder for at udnytte leverandørers svagheder og angribe EU medlemsstaters telekommunikationsnetværk, især kan aktører fra ikke-EU stater eller statssponserede aktører udnytte det, da de har den nødvendige evne, hensigt og kapacitet.

Fordi 5G netværk vil blive en vigtig del af forsyningskæden for mange kritiske IT-tjenester, vil det ikke kun være hensyn til fortrolighed, men også integritet og tilgængelighed, der bliver vigtige nationale sikkerhedsudfordringer og store sikkerhedsudfordringer fra et EU perspektiv.

Videre proces
Senest 31. december 2019 skal NIS-samarbejdsgruppen (nedsat i henhold til NIS Direktivet, Center for Cybersikkerhed er dansk repræsentant) fremlægge en værktøjskasse, der skal indeholde en række anbefalinger til at reducere risici.