FORSVARSMINISTERIET

NOTITS TIL FOLKETINGETS EUROPAUDVALG

Kommissionens henstilling om cybersikkerheden i forbindelse med 5G-net

1. maj 2019

Baggrund
Kommissionen fremlagde d. 26. marts 2019 en henstilling vedr. cybersikkerheden i forbindelse med 5G-teknologi (Dokument: C(2019) 2335 – Kommissionens henstilling af 26.3.2019 om cybersikkerheden i forbindelse med 5G-net). Tiltaget er også omtalt som ét af ti handlingspunkter i Kommissionens nylige Kina-meddelelse.

Henstillingens indhold
Kommissionen slår indledningsvis fast, at 5G vil give store muligheder for den fortsatte digitalisering på tværs af EU. I fremtiden vil 5G, i højere grad end 4G, udgøre rygraden i vitale samfundsfunktioner som f.eks. energi, transport, bankvæsen og sundhed. 5G vil således blive en katalysator for Europas økonomi, men 5G-teknologien vil også gøre samfundet mere sårbart, og der vil være store konsekvenser forbundet med et 5G-nedbrud.

Samtidig peger Kommissionen på andre sikkerhedsmæssige udfordringer, der forudses ifm. 5G. Det omfatter cyberspionage og sårbarhed for cyberangreb, men også risikoen for, at visse leverandører af teknologien kan være underlagt tredjelandes lovgivning og forvaltningsmodel.

Henstillingen indeholder ikke konkrete anbefalinger, men opstiller en plan for at kunne komme frem til et fælles, koordineret modsvar til sikring af cybersikkerheden. Ifølge Kommissionen bør der foretages en koordinering for effektivt at kunne håndtere disse cybertrusler, hvilket har afgørende betydning for et velfungerende indre marked og for beskyttelse af personoplysninger og privatlivets fred.

Visse tiltag i planen forudses implementeret af medlemsstaterne, mens Kommissionen skal have en koordinerende rolle. Det understreges, at henstillingen ikke bør berøre medlemsstaternes beføjelser med hensyn til offentlig sikkerhed, forsvar, statens sikkerhed og statens aktiviteter på det strafferetlige område.

Henstillingen anbefaler konkret, at der skal arbejdes frem mod en fælles værktøjskasse, der skal muliggøre, at risici effektivt kan håndteres. Der lægges op til et hurtigtgående arbejde. Hver medlemsstat bør således inden juli foretage en risikovurdering af 5G-infrastrukturen og herunder fastlægge de mest følsomme elementer, hvor sikkerhedsbrud ville have betydelige negative konsekvenser. Arbejdet drøftes undervejs i en sam-

arbejdsgruppe etableret i regi af NIS-direktivet. Parallelt hermed foretager medlemsstaterne med støtte fra Kommissionen og EU's cyberagentur ENISA en fælles evaluering af eksponeringen på EU-plan i forhold til de identificerede risici.

Efter planen vil ENISA frem mod oktober 2019 med støtte af medlemsstaterne udarbejde en samlet kortlægning af trusselsbillede ift. 5G. På den baggrund bygges værktøjskassen op med foranstaltninger til at håndtere 5G-risici på både EU- og nationalt plan. Værktøjskassen skal udover et overblik over de identificerede risici indeholde konkrete tiltag til at håndtere risiciene. Arbejdet skal være færdigt inden udgangen af 2019. Der lægges op til, at værktøjskassen herefter kan danne grundlag for, at Kommissionen kan udvikle fælles minimumskrav. Denne proces er dog ikke beskrevet nærmere.

Der lægges desuden op til, at den fælles EU-certificeringsordning for IKT-produkter, som blev vedtaget med den såkaldte cybersikkerhedsforordning i 2018, skal bringes i anvendelse i forhold til 5G. Kommissionen lægger således op til, at medlemsstaterne bør indføre national regulering om obligatorisk certificering af 5G-relevante produkter, tjenester og systemer, når de relevante certificeringsordninger er udviklet.

Vejen frem

Forsvarsministeriet koordinerer arbejdet som national myndighed for informationssikkerhed og beredskab i telesektoren. Energi- Forsynings-, og Klimaministeriet er som ansvarlig for teleområdet også inddraget i arbejdet. Det samme gælder Erhvervsministeriet i forhold til de omtalte IKT-certificeringsordninger.

Fra dansk side er Kommissionens henstilling hilst velkommen. Telesektoren er kritisk infrastruktur, og introduktionen af 5G rejser vigtige sikkerhedsmæssige spørgsmål. Der vurderes at være tale om udfordringer, som bedst kan håndteres gennem fælleseuropæisk koordination. Det gælder også hensynet til bedre at kunne modvirke tredjelandes pres på individuelle medlemslande. Fra dansk side er der fokus på at holde en balance mellem 1) den teknologiske udvikling til gavn for virksomheder og borgere, 2) et velfungerende marked og de rigtige priser, og 3) det nødvendige fokus på sikkerhed.

Det kan bemærkes, at henstillingen er blevet positivt modtaget hos medlemsstaterne, og at arbejdet er gået i gang henset til den ambitiøse tidsplan frem mod årsskiftet.