Ministeriet for Samfundssikkerhed og Beredskab

Dato: 13-03-2025
Sagsnr.: 2025 - 508
Akt-id.: 2951

Besvarelse af spørgsmål nr. 149 (Alm. del) fra Forsvars-, Samfundssikkerheds- og Beredskabsudvalget

Hermed sendes besvarelse af spørgsmål nr. 149 (Alm. del), som Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg har stillet til ministeren for samfundssikkerhed og beredskab den 18. februar 2025. Spørgsmålet er stillet efter ønske fra Alexander Ryle (LA).

Torsten Schack Pedersen

Spørgsmål nr. 149 (Alm. del) fra Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg:

> ”Flere danske kommuner, Vejdirektoratet, Forsvaret og senest Københavns Universitet har købt og opsat overvågningskameraer fra de stærkt udskældte kinesiske producenter Hikvision og Dahua – kameraer, der ikke opfylder kravene i Center for Cybersikkerheds vejledning om cybersikkerhed i overvågningsudstyr, og som Politiets Efterretningstjeneste, Rigspolitiet og flere IT-sikkerhedseksperter gentagne gange har advaret imod at anvende. Hvad vil ministeren gøre for at sikre, at offentlige myndigheder ikke gentager disse problematiske indkøb? Og vil ministeren tage initiativ til, at blackliste de pågældende virksomheder, ligesom en række andre lande – herunder USA og Storbritannien – allerede har gjort?”

Svar:

Det er en problemstilling, der optager mig meget. Trusselsbilledet på cyberområdet i Danmark er kompleks og alvorligt. Derfor er det vigtigt, at myndigheder, virksomheder og offentlige institutioner har øget fokus på cybersikkerhed. Og at både myndigheder og virksomheder tænker sig grundigt om.

Det er klart, at hvis man køber udstyr fra lande, som vi ikke har et sikkerhedspolitisk samarbejde med, så skal man være ekstra opmærksom.

Derudover har Ministeriet for Samfundssikkerhed og Beredskab til brug for besvarelsen af spørgsmålet indhentet en udtalelse fra Styrelsen for Samfundssikkerhed, der har oplyst følgende:

> ”Brugen af overvågningskameraer indebærer, ligesom andre digitale enheder, en sikkerhedsrisiko i forhold til beskyttelsen af enhederne og den data, enhederne indsamler. Set fra en cybersikkerhedsvinkel vil der f.eks. altid være risiko for, at digitale enheder kan indeholde sårbarheder, som hackere kan udnytte til at få adgang til enheden eller netværket.

Selvom risikoen som udgangspunkt gælder alle teknologier, uagtet producent, kan der imidlertid være en skærpet risiko forbundet med brugen af teknologier, som er produceret af og lagrer data i stater, som Danmark ikke har et sikkerhedspolitisk samarbejde med. Dette omfatter f.eks. overvågningsudstyr fra Kina. Det skyldes bl.a., at Kinas efterretningslov fra 2017 gør det muligt for efterretningstjenesterne at kræve, at kinesiske virksomheder overdrager den data, som virksomheden måtte indsamle via deres enheder Det kan også indebære at virksomhederne stiller systemadgange og viden om enhederne til rådighed for efterretningstjenesterne, hvilket f.eks. kan bruges i forbindelse med cyberangreb.

Styrelsen for Samfundssikkerhed anbefaler, at der altid foretages en konkret risikovurdering, hvori det bl.a. overvejes, hvad enheden skal bruges til, hvor den skal anvendes og i hvilken kontekst. Styrelsen tilbyder sparring både ift. eventuelle sektorspecifikke trusselsvurderinger og ift. de risikovurderinger, som myndigheder foretager inden for deres ressort og respektive sektorer. Selve risikovurderingen og den endelige accept af en eventuel risiko er forankret i den enkelte myndighed. Styrelsen for Samfundssikkerhed yder ligeledes rådgivning om god cybersikkerhedspraksis, og der er tidligere udgivet en vejledning om "Cybersikkerhed i overvågningsudstyr", som har været en del af den løbende rådgivningsindsats på området.

Styrelsen for Samfundssikkerhed følger udviklingen på området og vil løbende vurdere, hvorvidt eksisterende vejledning og anbefalinger på området er dækkende, herunder behovet for fornyet fokus på oplysning herom."

Vedrørende gældende udbudsregler har Ministeriet for Samfundssikkerhed og Beredskab til brug for besvarelsen af spørgsmålet indhentet en udtalelse fra Erhvervsministeriet, der har oplyst følgende:

"De gældende udbudsregler giver gode muligheder for, at den enkelte ordregiver kan varetage væsentlige sikkerhedshensyn i forbindelse med en udbudsprocedure. Offentlige ordregivere kan uden nogen nærmere begrundelse afvise tilbud fra virksomheder, som er etableret i et land uden for EU, som ikke har forpligtende handelsaftaler med EU. Dette gælder bl.a. virksomheder, som er etableret i Kina. Det er derimod ikke muligt at afvise tilbud om fx kinesiske kameraer, når virksomheden, som afgiver tilbuddet, er etableret i EU eller i et land, som EU har en forpligtende handelsaftale med.

Den enkelte offentlige ordregiver har dog fri mulighed for at stille relevante tekniske krav til produkterne eller kontraktuelle krav til gennemførelsen af den pågældende kontrakt for at sikre, at produkterne som anskaffes, lever op til nødvendige sikkerhedskrav. I forbindelse med anskaffelse af kameraer kan ordregiver fx udarbejde kravene ud fra de anbefalinger, som findes i Styrelsen for Samfundssikkerheds vejledning om cybersikkerhed i overvågningsudstyr.

I forhold til indkøb af kameraer er det derfor som udgangspunkt op til den enkelte ordregiver at stille passende sikkerhedskrav inden for rammerne af udbudsreglerne. Hvis den enkelte ordregiver vurderer ikke at kunne håndtere sikkerhedsudfordringerne inden for rammerne af udbudsreglerne, kan der være mulighed for at indføre særlige yderligere foranstaltninger, når dette vurderes nødvendigt for at sikre et konkret hensyn til national sikkerhed og offentlig orden. Det er den enkelte ordregivers vurdering, om hensynet til national sikkerhed kan varetages inden for udbudsreglerne, eller om der er et nødvendigt og konkret behov for at indføre yderligere sikkerhedsforanstaltninger."