FORSVARSMINISTERIET

22. juni 2023
Dok.nr.: 557886

SAMRÅD VEDR. HIKVISION D. 22/6 2023

Hovedbudskaber

- Produkter koblet til internettet udgør altid en trussel for cyberspionage. Det gælder også overvågningskameraer tilkoblet en netværksforbindelse – uanset producent.
- Regeringen tager truslen alvorligt.
- Center for Cybersikkerhed har ikke hjemmel til at forbyde kinesiske kameraer, men står til rådighed for myndigheder ift. rådgivning om cybersikkerheden i overvågningskameraer.
- Offentlige myndigheder er forpligtiget til at efterleve udbudsreglerne.

Jeg er sammen med min kollega, justitsministeren, blevet bedt om at besvare tre spørgsmål vedrørende kinesisk-producerede overvågningskameraer. Jeg vil besvare spørgsmålene i den rækkefølge, de er stillet. Jeg vil tillige afslutte min besvarelse med at forholde mig til, hvordan problematikken må adresseres.

Indledningsvis vil jeg dog gerne knytte et par generelle kommentarer til cyberspionage og cybersikkerheden i overvågningsudstyr.

***

Center for Cybersikkerhed vurderer, at truslen fra cyberspionage mod Danmark er meget høj.

Den trussel skal vi tage meget alvorligt. Ikke mindst i den nuværende sikkerhedspolitiske situation.

Overvågningsudstyr, der tilkobles et netværk, kan indeholde sårbarheder, der kan udnyttes. I overvågningsudstyr forbundet til internettet er der en risiko for, at andre kan se med.

Overvågningskameraer kan derfor udgøre en sikkerhedstrussel.

Den trussel kræver, at man er opmærksom på en lang række sikkerhedsaspekter. Ikke mindst i forhold til om udstyret indsamler sensitiv data eller eksempelvis er placeret på et netværk med adgang til andre systemer.

Grundlæggende er det afgørende, at man tænker cybersikkerhed ind i sine indkøb.

***

Jeg er i samrådsspørgsmål N blevet bedt om at forholde mig til indkøb af overvågningskameraer fra firmaet Hikvision. Jeg besvarer spørgsmålet for så vidt angår indkøb foretaget af Forsvarsministeriets koncern.

Offentlige myndigheder er forpligtiget til at efterleve udbudsreglerne, der skal sikre en lige og gennemsigtig konkurrence. Dette indebærer et helt generelt princip om, at offentlige indkøbere ikke må diskriminere på baggrund af nationalitet.

I forbindelse med FMI's anskaffelser foretages der løbende vurderinger af produkter og deres sikkerhed i forhold til understøttelse af Forsvarets helt særlige behov og vilkår.

I forbindelse med modernisering, renovering og udskiftning af Forsvarets kapaciteter vil der kunne blive fortaget en vurdering af risikoen for bl.a. cyberspionage, og på den baggrund

taget stilling til om produkter fra specifikke leverandører kan udelukkes.

Jeg kan oplyse, at HIKVISION-kameraer ikke længere anvendes på Søværnets fartøjer af IVER HUITFELDT-klassen og er under udfasning fra fartøjer af ABSALON-klassen og KNUD RASMUSSEN-klassen.

Et stort antal [samtlige på Søværnets sejlende enheder] af de HIKVISION-kameraer, der anvendes i Forsvaret, er ikke direkte forbundet til internettet.

***

I samrådsspørgsmål O er jeg blevet spurgt til, om jeg er enig i, at brugen af kinesisk-producerede kameraer involverer en risiko for spionage.

Jeg kan besvare spørgsmålet for så vidt angår cyberspionage forbundet med kinesiske overvågningskameraer.

Som jeg nævnte indledningsvist, kan de fleste overvågningssystemer indeholde sårbarheder, der potentielt kan udnyttes. Det kan samtidig ikke afvises, at kameraer fra bestemte producenter indeholder såkaldte bagdøre.

Forsvarets Efterretningstjeneste har oplyst mig, at i disse overvågningskameraer vil det generelt være vanskeligt at afsløre eventuelle skjulte funktionaliteter, herunder om sådanne vil kunne implementeres på et senere tidspunkt ved en såkaldt firmware-opdatering.

Ifølge Forsvarets Efterretningstjeneste kan anvendelse af overvågningsudstyr fra lande uden for Danmarks normale sikkerhedspolitiske kreds øge risikoen for cyberspionage, hvis f.eks. udstyret opsættes i nærheden af sensitive lokaliteter.

Derfor opfordrer Forsvarets Efterretningstjeneste til omtanke ved indkøb og anvendelse af overvågningsudstyr fra lande, der står uden for Danmarks normale sikkerhedspolitiske kreds.

I den forbindelse kan det, ifølge Forsvarets Efterretningstjeneste, blandt andet være relevant at tage i betragtning, om leverandøren er hjemmehørende i eller varetager produktionen eller driften fra et land, hvor det efter det pågældende lands lovgivning er muligt at pålægge leverandører eller deres underleverandører at udføre eller deltage i forhold, som vil udgøre spionage eller sabotage.

I Kina er alle kinesiske borgere og virksomheder underlagt Kinas nationale efterretningslov, som giver de kinesiske efterretningstjenester vide beføjelser til at indsamle oplysninger fra kinesiske selskaber, organisationer og individer, uanset hvor i verden de befinder sig.

Det er den enkelte myndigheds ansvar at udarbejde risikovurderinger og retningslinjer for det udstyr, som myndigheden anvender.

Som Danmarks nationale it-sikkerhedsmyndighed og nationalt kompetencecenter på cybersikkerhedsområdet oplyser, rådgiver og vejleder Forsvarets Efterretningstjenestes Center for Cybersikkerhed myndigheder og virksomheder for at styrke cybersikkerheden.

Center for Cybersikkerhed står til rådighed og kan vejlede og rådgive myndigheder med blandt andet "best practice" for cyber- og informationssikkerhed i systemer til videoovervågning.

I februar 2023 udgav Center for Cybersikkerhed en vejledning, som netop handler om sikkerhed i overvågningsudstyr. I vejledningen fremgår konkrete anbefalinger vedrørende indkøb, opsætning, drift og bortskaffelse af overvågningsudstyr.

***

I spørgsmål P er jeg blevet bedt om, at fremlægge begrundelser for, hvorfor det med Udbudsloven og Udbudsdirektivet ikke er muligt at udelukke indkøb, som kan være en trussel mod Danmarks sikkerhed.

Lad mig slå fast, at erhvervsrettet lovgivning, herunder Udbudsloven, hører under Erhvervsministeriets ressort. Jeg kan således alene oplyse, hvorledes Forsvarsministeriets Materiel- og Indkøbsstyrelse (FMI) tolker lovgivningen.

Lad mig for god ordens skyld starte med at præcisere, at FMI i den omtalte redegørelse fra 2020 ikke skriver, at udbudslo-

ven forhindrer udelukkelse, men at FMI's muligheder for at udelukke en virksomhed er begrænsede.

FMI har oplyst mig, at muligheden for at kunne afvise kameraer fra Hikvision, når FMI foretager anskaffelser, altid skal bero på en konkret vurdering af bl.a. anskaffelsens karakter, Hikvisions rolle i leverancen samt kameraernes egenskaber og deres påtænkte anvendelse.

Der findes i udbudsreglerne en række mulige udelukkelsesgrunde. Overordnet gælder, at en virksomhed enten skal være dømt, eller have begået alvorlige forsømmelser i forbindelse med sit erhverv for at kunne udelukkes. Hikvision fremgår ikke af gældende FN eller EU sanktionslister, som kan danne grundlag for udelukkelse.

***

Er der således mulighed for at gennemføre tiltag, der kan forhindre indkøb af kinesisk produceret materiel?

Først og fremmest skal jeg igen gøre opmærksom på, at erhvervsrettet lovgivning hører under Erhvervsministeriets ressort, det gælder både Udbudsloven samt Investeringsscreeningsloven, der har til formål at forhindre, at udenlandske direkte investeringer og særlige økonomiske aftaler kan udgøre en trussel mod den nationale sikkerhed.

For så vidt angår de juridiske muligheder for at forhindre indkøb af kinesisk produceret materiel, må jeg derfor henvise til erhvervsministeren.

Når det er sagt, vil jeg gerne understrege, at vi i regeringen er meget opmærksomme på de sikkerhedsudfordringer, der desværre også kommer med den øgede digitalisering.

I den her sag er der to ting, der er vigtige at være opmærksom på: Cybersikkerhed ved indkøb generelt, og indkøb af produkter fra lande, der står uden for Danmarks normale sikkerhedspolitiske kreds.

***

Som jeg allerede har nævnt, kan der være sårbarheder i al internetforbundet overvågningsudstyr. Og de sårbarheder kan udnyttes.

Her kan jeg eksempelvis nævne, at man med den Nationale Strategi for Cyber- og Informationssikkerhed for 2022-2024 igangsatte en analyse, der skal afdække, hvordan man i endnu højere grad kan tage højde for it-sikkerhed i offentlige it-indkøb.

Herudover kan jeg nævne, at der også i EU er fokus på cybersikkerheden i produkter. Europa-Kommissionen har blandt andet offentliggjort et udkast til en ny forordning, der har til formål at styrke cybersikkerheden i produkter med digitale elementer tilgængelig på det indre marked.

***

Samtidig må vi ikke være blinde over for de særlige forhold, der gør sig gældende ved kinesiske virksomheder, der er underlagt den kinesiske efterretningslov.

Jeg er derfor rigtig glad for, at vi i dag kan drøfte udfordringerne ved indkøb af kinesiskproduceret overvågningsudstyr.

FMI har tydeliggjort, at der er begrænsninger i mulighederne for at udelukke en virksomhed, som Hikvision, fra udbudsprocesser.

Jeg finder det derfor nødvendigt, at vi får undersøgt, hvordan vi konkret kan håndtere den generelle udfordring, der er. jeg vil tage initiativ til at drøfte muligheder i regeringen.

***

Jeg vil nu give ordet videre til justitsministeren.