FORSVARSMINISTEREN

Folketingets Forsvarsudvalg
Christiansborg

Dato:

Enhed: CNI
Sagsnr.: 2022/001159
Dok.nr.: 345903
Bilag: Ingen

Forsvarsministeriet
Holmens Kanal 9
1060 København K

Tlf.: +45 7281 0000
Fax: +45 7281 0300
E-mail: fmn@fmn.dk
www.fmn.dk

EAN: 5798000201200
CVR: 25 77 56 35

Medlem af Folketinget Christoffer Aagaard Melson (V) har den 11. februar 2022 stillet følgende spørgsmål nr. 159, som hermed besvares.

Spørgsmål nr. 159:
I aftale om et styrket cyberforsvar findes et initiativ om et cyberhjemmeværn. Vil ministeren redegøre for, hvordan dette tænkes ind i Danmarks beredskab og har NOS'en *[sic]* mulighed for med kort varsel at aktivere ressourcer i den private sektor?

Svar:
Der var med *Aftale om et Styrket Cyberforsvar* (24. juni 2021) enstemmig opbakning i forsvarsforligskredsen til etableringen af et cyberhjemmeværn. Med cyberhjemmeværnet styrkes mulighederne for at mobilisere civile cyberkompetencer, når der er et samfundsmæssigt behov herfor.

Oprettelsen af cyberhjemmeværnet er i sin tidlige fase. Det er forventningen, at cyberhjemmeværnet – når fuldt etableret – vil styrke den fælles cyberrobusthed i hele Danmark på tværs af Hjemmeværnet og i samfundskritiske virksomheder. Desuden skal cyberhjemmeværnet kunne fungere som beredskabsstøtte for Forsvarets samlede cyber- og informationssikkerhed.

Det vil samtidig give Hjemmeværnet mulighed for at bruge civile kompetencer i en militær kontekst og dermed understøtte rekruttering og fastholdelse i Hjemmeværnet.

For så vidt angår NOST'ens mulighed for med kort varsel af aktivere ressourcer i den private sektor har jeg anmodet Justitsministeriet om bidrag til besvarelsen. Justitsministeriet oplyser følgende:

"Justitsministeriet skal indledningsvis henvise til det samtidige bidrag til besvarelse af spørgsmål nr. 158 (alm. del) fra Folketingets Forsvarsudvalg. Ministeriet har til brug for besvarelsen indhentet en udtalelse fra Rigspolitiet, der har oplyst følgende:

I forbindelse med cyberhændelser indebærer sektoransvarsprincippet, at det er de sektoransvarlige myndigheders ansvar at håndtere hændelsen og dens følger. De sektoransvarlige myndigheder skal desuden

sikre et overblik over hændelsens omfang og rapportere dette til relevante myndigheder, herunder Center for Cybersikkerhed samt National Operativ Stab (NOST), hvis denne er etableret, ligesom det er de berørte virksomheder og organisationers ansvar at håndtere hændelsen og dens følger.

I december 2021 udsendte regeringen en national strategi for cyber- og informationssikkerhed (NCIS 2022-2024).

Strategien ændrer ikke på sektoransvarsprincippet. Det fremgår således af strategien, at den enhed (myndighed, virksomhed og organisation), der har ansvaret for en opgave til daglig, fortsat har ansvaret, når der opstår en cyberhændelse. Enheden skal sikre, at den i den forbindelse får den aftalte bistand fra eventuelle driftsleverandører. Derudover kan enheden få bistand fra de decentrale cybersikkerhedsenheder. Det er enhedens ansvar at aktivere denne bistand, forestå den indledende hændelseshåndtering og – afhængigt af hændelsens omfang – at anmelde til politiet samt indberette til kompetente myndigheder og Center for Cybersikkerhed. Det er ligeledes den ansvarlige myndighed, virksomhed eller organisation, der som udgangspunkt varetager eventuel ekstern kommunikation om hændelsen.

Det fremgår endvidere af strategien, at NOST kan aktiveres ved større cyberhændelser, der påvirker flere sektorer.

Det følger af selve rammen for NOST, at staben kan sammensættes fleksibelt med deltagelse af såvel de faste medlemmer som de ad hoc-aktører, der skønnes at være relevante i forhold til en given hændelse. Der vil i den forbindelse også kunne ske indkaldelse af private aktører, hvilket der også er fortilfælde for i forbindelse med tidligere NOST-indsatser."

Med venlig hilsen

Morten Bødskov