FORSVARSMINISTEREN

Folketingets Udvalg for Digitalisering og It
Christiansborg

Dato: 15. december 2023

Enhed: CNI
Sagsnr.: 2023/009324
Dok.nr.: 667976
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

Udvalget for Digitalisering og It har den 2. november 2023 stillet følgende spørgsmål nr. 19 (alm. del), som hermed besvares.

Spørgsmål nr. 19:
Er ministeren tryg ved, at ansatte ved det danske forsvar, ansatte i staten med ansvar for samfundskritisk infrastruktur, medlemmer af Folketinget eller ministre i regeringen af de danske mobilselskaber får udleveret en kinesisk 4G- eller 5Groutere til brug i privaten, som samtidig også bruges til hjemmearbejde?

Svar:
Der er til brug for besvarelsen indhentet bidrag fra Forsvarets Efterretningstjeneste, der oplyser følgende:

"Fremmede stater, herunder Kina, spionerer aktivt mod Danmark. Hensigten er blandt andet at få indsigt i Danmarks udenrigs- og sikkerhedspolitik, men også i dansk viden og teknologi.

Fremmede staters hackergrupper, herunder kinesiske med tilknytning til landets efterretningstjenester, har betydelige cyberkapaciteter, som de bruger til at kompromittere mål i andre lande – også i Danmark. De vil forsøge at udnytte de sårbarheder, der er til stede, også private enheder. Den form for trussel er ikke isoleret til kinesisk udstyr, men er til stede uafhængigt af udstyrets oprindelsesland. Dog er kinesiske borgere og virksomheder underlagt Kinas nationale efterretningslov, som giver efterretningstjenesterne vide beføjelser til at indsamle oplysninger fra kinesiske selskaber, organisationer og individer, uanset hvor i verden de befinder sig.

Center for Cybersikkerhed fastsatte i 2022 sammen med Digitaliseringsstyrelsen, Statens IT og Politiets Efterretningstjeneste 20 tekniske minimumskrav for statslige myndigheder. Minimumskravene skal bidrage til at sikre et højt it-sikkerhedsniveau i staten. Et af kravene er, at der anvendes VPN-forbindelse, når medarbejdere er koblet på netværk uden for myndighedens egen it-infrastruktur. Kravet gælder for alle stationære og bærbare computere, der administreres af myndigheden.

Anvendelse af VPN sikrer, at kommunikationen mellem den mobile enhed og arbejdspladsen er krypteret, således at uvedkommende ikke

kan få indsigt i det, der overføres. Dette mindsker betydningen af routeres eventuelle sårbarheder."

Med venlig hilsen

Troels Lund Poulsen