



Folketingets Forsvarsudvalg

ERHVERVSMINISTEREN

28. februar 2023

Besvarelse af spørgsmål 5 alm. del stillet af udvalget den 11. januar efter ønske fra Lisbeth Bech-Nielsen (SF).

ERHVERVSMINISTERIET

Slotsholmsgade 10-12
1216 København K

Spørgsmål 5:

Kan ministeren garantere, at kinesiske trådløse routere hos private danske husstande ikke udgør en national sikkerhedsrisiko.

Tlf. 33 92 33 50

Fax 33 12 37 78

CVR-nr. 10 09 24 85

EAN nr. 5798000026001

em@em.dk

www.em.dk

Svar:

På Erhvervsministeriets område er lov om produkter og markedsovervågning med til at styrke beskyttelsen af danske forbrugere mod farlige og ulovlige produkter mhp. at danske forbrugere ikke udsættes for fare. Loven har ikke til formål at sikre national sikkerhed, men Sikkerhedsstyrelsen foretager generel overvågning af markedet for en række produkter, herunder trådløse routere. Jeg har indhentet bidrag fra Sikkerhedsstyrelsen, som oplyser følgende:

”Sikkerhedsstyrelsens markedsovervågning er risikobaseret. Det betyder, at styrelsen som udgangspunkt fokuserer sine kontrolindsatser på områder og produktkategorier, hvor risikoen for lovovertrædelser vurderes at være størst jf. lov om produkter og markedsovervågning. Vurderingerne er baseret på bl.a. anmeldelser, advarsler fra myndigheder i andre lande, statistikker og anden type data”

Jeg har derudover indhentet bidrag ved Forsvarsministeriet, som oplyser følgende:

”Center for Cybersikkerhed (CFCS) opfordrer til omtanke ved indkøb og brug af teknologi fra lande, som Danmark ikke har et sikkerhedsmæssigt samarbejde med, og som har en anden sikkerhedskultur og lovgivning end Danmark. CFCS opfordrer således offentlige og private organisationer til i deres informationssikkerhedspolitik at tage stilling til anvendelse af teknologi fra andre lande på baggrund af en risikovurdering. Det er vanskeligt at undersøge, om teknologi fra en bestemt producent indeholder skjulte sårbarheder, som giver mulighed for bl.a. spionage. Ved anskaffelse af internetopkoblede produkter skal forbrugere derfor bl.a. være

opmærksomme på vigtigheden af, at hard- og software opdateres og opgraderes for at imødegå kendte sårbarheder.”

Med venlig hilsen

Morten Bødskov