ERHVERVSMINISTERIET

Folketingets Erhvervsudvalg

ERHVERVSMINISTEREN

19. marts 2021

ERHVERVSMINISTERIET

Slotsholmsgade 10-12
1216 København K

Tlf. 33 92 33 50
Fax. 33 12 37 78
CVR-nr. 10092485
EAN nr. 5798000026001
em@em.dk
www.em.dk

Besvarelse af spørgsmål 2 ad L 174 stillet af udvalget den 12. marts efter ønske fra Christoffer Aagaard Melson (V).

Spørgsmål:
Ministeren bedes redegøre udførligt for, hvordan administrationen af cybersikkerhedscertificeringsordningen vil foregå, og hvordan det sikres, at også de små virksomheder får mulighed for at kunne opnå certificering på en måde, så det sikres at de små virksomheder ikke får sværere ved at konkurrere end de større virksomheder. Herunder bedes ministeren redegøre for, hvilke – og hvor store - omkostninger, der er forbundet for virksomhederne med at søge og opnå cybersikkerhedscertificering, specificeret på forskellige virksomhedsstørrelser

Svar:
Med forordningen om cybersikkerhed skabes den europæiske ramme for, at det bliver muligt for virksomheder at opnå certificering af cybersikkerhed. Med andre ord er forordningen ikke i sig selv en europæisk cybersikkerhedscertificeringsordning. Forordningen definerer, hvordan certificeringsordningerne fastlægges.

Lovforslaget sikrer den danske gennemførelse af forordningen, bl.a. ved at Sikkerhedsstyrelsen udpeges som national cybersikkerhedscertificeringsmyndighed. Denne udpegning indebærer, at Sikkerhedsstyrelsen tillægges opgaver af overordnet karakter, f.eks. at føre tilsyn med reglerne i de europæiske cybersikkerhedscertificeringsordninger, at behandle klager og at samarbejde med andre myndigheder.

Lovforslaget supplerer forordningen og fastlægger ikke administrationen af de enkelte certificeringsordninger. Der er endnu ikke godkendt konkrete certificeringsordninger, da arbejdet, som foregår på EU-niveau, er forsinket på grund af COVID-19. Det er derfor ikke på nuværende tidspunkt muligt at redegøre udførligt for administrationen af hver enkelt certificeringsordning. Således vil det afhænge af den enkelte certificeringsordning, hvilke krav der gælder og dermed der tilkoblede administrationen.

Grundlæggende gælder dog, at virksomheder kan opnå certificering af deres produkt, tjeneste eller proces, hvis de lever op til kravene i relevante

standarder eller et tilsvarende sikkerhedsniveau. Disse krav fastsættes i de enkelte certificeringsordninger.

I praksis vil certificering oftest fungere ved, at virksomheden bestiller en certificering ved et såkaldt overensstemmelsesvurderingsorgan, dvs. en virksomhed, som er akkrediteret (godkendt) af DANAK til, at de må udstede certifikater inden for cybersikkerhed. Forudsætningen for dette er dog, at der er vedtaget konkrete certificeringsordninger på europæisk niveau.

På nuværende tidspunkt er flere europæiske cybersikkerhedscertificeringsordninger på vej. Længst er arbejdet med den såkaldte EUCC-ordning (Common Criteria based European candidate cybersecurity certification scheme). Det er en ordning, som fastsætter nogle generelle krav, som kan bruges på tværs af relevante IKT-produkter, tjenester eller processer. Undervejs er også arbejdet med ordninger inden for hhv. cloud-tjenester og 5G. Endelig er det forventningen, at arbejdet med IoT (Internet of Things) og IACS (Industrial Automation Control Systems) påbegyndes snarest. Arbejdet med nye certificeringsordninger vil løbende blive offentliggjort af Kommissionen.

Forordningens artikel 54 opstiller en lang række elementer, der som minimum skal omfattes af alle certificeringsordningerne. Det gælder f.eks. en ordnings eventuelle tillidsniveau (”grundlæggende”, ”betydeligt” eller ”højt”), reglerne for overvågning af produkter mv., og om det er muligt at foretage såkaldt selvvurdering af overensstemmelse.

Små og store virksomheder vil på lige vilkår kunne opnå certificering i henhold til en certificeringsordning, alt efter hvilke krav, der stilles i ordningen. Nogle certificeringsordninger vil dog forventeligt være mere relevante for store virksomheder, end mindre virksomheder, ligesom der kan være forskelle i relevansen på tværs af brancher.

Omkostningerne ved certificering vil også variere afhængigt af produktet, tjenesten eller processen samt evaluerings- og sikringsniveauet. Idet der endnu ikke findes nogle endeligt vedtagne certificeringsordninger, og fordi der er mange variabler, der kan have indflydelse, er det ikke muligt at redegøre for omkostningerne, heller ikke efter virksomhedsstørrelse.

En certificeringsordning med grundlæggende tillidsniveau vil som udgangspunkt være mindre omkostningstung end ordninger med betydeligt eller højt tillidsniveau. Det skyldes bl.a., at der som udgangspunkt vil være færre og mindre komplekse komponenter, som skal evalueres for at opnå certificering.

Af samme grund vil det også være muligt at fastsætte i en certificeringsordning med grundlæggende tillidsniveau, at en producent eller udbyder selv kan vurdere overensstemmelsen (selvvurdering). Dermed kan producenten eller udbyderen selv udstede en EU-overensstemmelseserklæring i stedet for at søge og opnå certificeret hos en tredjepart (overensstemmelsesvurderingsorgan). I disse tilfælde kan udgiften til en tredjepart altså undgås.

En certificeringsordning med højt tillidsniveau vil i udgangspunktet være relativt omkostningstung, fordi den krævede evaluering omhandler avancerede risici. Af samme grund vil det i udgangspunktet formentlig være virksomheder med flere ressourcer der har kapaciteten, til at udbyde mere komplekse IKT-produkter, tjenester og processer, som vil overveje en certificering, hvor tillidsniveauet er højt.

Generelt forventes det, at certificering vil være en relativt stor udgift for virksomhederne. I forslaget til forordningen om cybersikkerhed[1] angives som det eneste eksempel, at et certifikat til et såkaldt smart meter der attesterer, at produktet og dets omkringliggende struktur overholder de højeste tekniske og sikkerhedsmæssige standarder (BSI »Smart Meter Gateway« certificate), beløber sig til mere end en million euro. Det antages dog, at udgiften vil være væsentligt mindre på andre og mindre omfattende certificeringer.

Det er igen vigtigt at fremhæve, at certificering – medmindre andet fastsættes nationalt eller i EU – er frivillig. Det vil derfor være op til den enkelte virksomhed at afveje de positive effekter, som en certificering vil have, over for de omkostninger, som er forbundet hermed.

Med venlig hilsen

Simon Kollerup

[1] Proposal for a regulation of the European Parliament and of The Council on ENISA, the »EU Cybersecurity Agency«, and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (»Cybersecurity Act«), The European Commission, Brussels 13.9.2017