Til
- Forsvarsministeriet
ner@fmn.dk, thr@fmn.dk, nhj@fmn.dk, aso@fmn.dk
- Energistyrelsen
sihr@ens.dk, mabi@ens.dk, mmo@ens.dk

29.1.2021

Specialudvalgshøring over Europa-Kommissionens forslag til direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen og om ophævelse af direktiv (EU) 2016/1148

TI har noteret sig, at Europa-Kommissionen den 18. januar 2020 har fremsat forslag til Europa-Kommissionens direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen. TI takker endvidere Forsvarsministeriet, Erhvervsministeriet såvel som Energistyrelsen for denne indledende specialudvalgshøring over forslaget.

TI finder det positivt, at regeringen såvel som Europa-Kommissionen fastholder fokus på den digitale infrastrukturs samfundskritiske funktion. TI deler i øvrigt regeringens og Europa-Kommissionens vurdering af, at økonomisk genopretning som følge af COVID-19-krisen, som skal værne om velfærd og velstand i det danske samfund, i høj grad afhænger af en velfungerende og sikker teleinfrastruktur.

En velfungerende og sikker teleinfrastruktur er afgørende for det danske og europæiske samfund, teleselskabernes kunder og naturligvis også for branchen selv. Med det afsæt har den danske telebranchen over de seneste 10 år investeret 70 mia. kr. i at udbygge den digitale infrastruktur i Danmark med fokus på både kapacitet og sikkerhed. Udbygningen er sket i tæt dialog med danske myndigheder, herunder særligt Center for Cybersikkerhed (CFCS).

TI's specifikke bemærkninger til forslaget
Med henvisning til det forslåede anvendelsesområde (artikel 1 og 2), herunder forpligtelser om, at medlemsstaterne skal vedtage en national cybersikkerhedsstrategi, om risikostyring og rapportering vedrørende cybersikkerhed samt vedrørende udveksling af cybersikkerhedsoplysninger, forudser TI ikke væsentlige ændringer i forhold til dansk praksis på teleområdet. Det hilser vi velkommen.

TI finder desuden flere af bestemmelserne om de nationale rammer for cybersikkerhed (artikel 5-11) særligt interessante. Det gælder fx om at udpege CSIRT'er. Da begrebet nævnes i flertal, forestiller TI sig flere CSIRT'er i Danmark, men hvor samlingspunktet naturligt vil være CFCS, som i dag har en 24/7 enhed. Alternativt kan det give mening, at de sektorspecifikke DCIS'er bliver samlingspunkt, da disse i dag er en "information hub", men som ville kunne udvikles til CSIRT-opgaver, såfremt dette påkrævedes, hvilket dog ville kræve en væsentlig anden bemanding.

Hvis samlingspunktet for CSIRT-arbejdet i stedet for skulle blive CFCS, ser TI gerne, at der grundlæggende sker en opdeling således, at den/de myndighed(er) eller enhed(er), som skal facilitere videndeling, udveksling af oplysninger, risikostyring og rapportering om fx cybersikkerhedshændelser ikke er den/de samme myndighed(er), som også skal føre tilsyn, audits m.m., og som kan udstede sanktioner.

Udviklingen og vedligehold af et europæisk sårbarhedsregister i regi af ENISA i medfør af artikel 6 finder TI umiddelbart positivt.

For så vidt angår de forslåede bestemmelser om samarbejde, herunder om et europæisk netværk af cybersikkerhedsorganisationer (artikel 12-16), syntes disse at være et naturligt næste skridt og noget, som er naturligt koordineret af de nationale CSIRT'er.

Kravet om et konkret arbejdsprogram i medfør af artikel 12, stk. 5, for de foranstaltninger, der skal iværksættes for at nå mål og opgaver, finder TI afgørende for fremdrift af en sådan tværnational samarbejdsgruppe.

TI finder i medfør af de forslåede forpligtelser vedrørende risikostyring og rapportering i forbindelse med cybersikkerhed (artikel 17-23), at de forslåede bestemmelser om, at ledelsesorganer i alle enheder, der er omfattet af anvendelsesområdet, skal godkende de risikohåndteringsforanstaltninger vedrørende cybersikkerhed, der træffes af de respektive enheder, og følge specifik cybersikkerhedsrelateret uddannelse, er proportionale og naturlige.

Med henvisning til artikel 21 omkring IKT-certificering finder TI det såvel positivt som proportionalt, at det er leverandøren, der skal sikre, at sikkerheden er på plads gennem en certificeringsordning. Andre udenlandske aktører i telebranchen vil muligvis have en størrelse og tyngde, der muliggør en selvstændig vurdering, men det vil være en disproportional afvejning, hvis samme vurdering blev pålagt mindre spillere i en europæisk eller international sammenhæng. Dertil kommer spørgsmålet om, hvilken certificeringsordning der vil blive tale om. Her anbefaler TI, at der arbejdes for fælles standarder på tværs af EU's medlemslande.

TI hilser i øvrigt bestemmelserne om udveksling af oplysninger (artikel 26 og 27) velkommen, men skal samtidig påpege, at der er behov

for klart at definere, hvad der karakteriseres som en "væsentlig hændelse" på europæisk niveau. Der ses dog en udfordring i at sikre denne vidensdeling, hvis samme myndighed eller enhed samtidig skal føre tilsynet.

TI ønsker i denne sammenhæng fokus på, at videndelingen skal foregå i begge retninger, således at myndigheder pålægges at dele viden med aktørerne på samme måde, som disse skal dele med myndighederne.

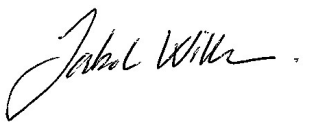
Henvisningen til fælles standarder på sårbarhedshåndteringsområdet i medfør af artikel 28, herunder håndhævelse af artikel 18, 20 og 22, finder TI væsentlige for at sikre samordnet praksis. Hvis dette tilstræbes, bør disse, når de er kendt og vedtaget, ligeledes implementeres i dansk retstilling i form af udmøntning i bekendtgørelsen.

I direktivet er der meget eksplicit krav om, at der skal føres tilsyn, og at der skal være stærke muligheder for anvendelse af sanktioner fra den kompetente myndighed. Der nævnes bl.a., at den kompetente myndighed skal have mulighed for: onsite/offsite audit med stikprøver, regelmæssige tilsyn, tilsyn baseret på risikovurderinger eller risikorelateret tilgængelig information, sikkerhedsscanninger m.m. Vi appellerer til, at disse beføjelser anvendes med omtanke, samt at der vil være et fokus på, at der ikke sker en konkurrenceforvirring. Historisk har myndighederne på teleområdet ikke anvendt de sanktionsmuligheder, de har haft, men i stedet fokuseret på dialog og samarbejde, hvilket vi anbefaler, lovgivningen fortsat vil give plads til.

TI undres umiddelbart over skellet mellem "væsentlige enheder" og "vigtige enheder" i medfør af tilsyn og håndhævelse af sådanne (artikel 29-30).

TI står naturligvis til rådighed måtte ovenstående give anledning til kommentarer eller opfølgende spørgsmål.

Med venlig hilsen



Jakob Willer
Direktør