

Forsvarets Efterretningstjeneste,
Center for Cybersikkerhed
Att.: Anette Arnsted
Kastellet 30
2100 København Ø

Sendt til:
fe@fe-mail.dk
fe-4418@fe-ddis.dk

Sagsnr.: 2020/001583.

Den 4. februar 2021

Høring over udkast til bekendtgørelser om sikkerhed i net og tjenester

Nærværende høringssvar drejer sig om *Udkast til bekendtgørelse om oplysnings- og underretningsspligter vedrørende sikkerhed i net og tjenester*.

Dansk Erhverv sætter pris på at få mulighed for at indgive høringssvar på dette område, som efter vores mening er af stor vigtighed.

Generelle bemærkninger

Sikkerheden i teleinfrastrukturen er af højeste betydning for et velfungerende informationssamfund. Derfor støtter Dansk Erhverv generelt tiltag, som har til formål at styrke teleselskabernes mulighed for at øge sikkerheden i telenet og -tjenester.

Overordnet finder Dansk Erhverv det vigtigt at skabe størst mulig gennemskuelse og juridisk klarhed for udbydere af net- og kommunikationstjenester. Det vil derfor være hensigtsmæssigt, at Center for Cybersikkerhed (evt. i samspil med andre relevante myndigheder) laver tydelige definitioner og afgrænsninger til denne bekendtgørelse. F.eks. er definitionen af "kritiske netværkskomponenter" uhensigtsmæssig bred, ligesom "business support systemer" ikke er et begreb, hvorom der findes en ensartet branchemæssig forståelse.

Dansk Erhverv er endvidere af den holdning, at regulering bør være proportionel ift. den risiko, der adresseres og væres fokuseret på den reelle mulighed for håndhævelse. Dvs. reguleringen bør adressere netop de net- og kommunikationstjenester, hvor en sikkerhedshændelse vil have størst negativ konsekvens, og bør vurderes ud fra, om Center for Cybersikkerhed har en de facto mulighed for at håndhæve reglerne.

For de tjenester, der kendetegnes ved ofte eller altid at have grænseoverskridende karakter, opfordrer Dansk Erhverv til, at danske myndigheder i højere grad arbejder for, at den tilsvarende regulering ligeledes er international, så en udbyder undgår at skulle melde ind til en flæthed af nationale myndigheder, men fx kan melde ind til én EU-myndighed.

Specifikke bemærkninger

§1

En række begreber (fx kritiske netkomponenter) er ikke klart defineret, ligesom der mangler afgrænsninger (fx for centrale versus ikke-centrale routere). Dansk Erhverv foreslår, at bekendtgørelsen i højere grad bør gøre brug af klare definitioner og afgrænsninger, som bl.a. kan baseres på en konkret risikovurdering el. lign.

§3-6

I overensstemmelse med artikel 40 samt præambel 94-95 i det europæiske kodeks for elektronisk kommunikation (EU direktiv 2018/1972), finder Dansk Erhverv det væsentligt at få sikkerhed for, om forpligtelserne i disse paragraffer i bekendtgørelsen gælder for den bredere gruppe af nummeruafhængige interpersonelle kommunikationstjenester (NUIK-tjenester) og/eller netværksuafhængige nummerbaserede interpersonelle kommunikationstjenester¹.

Dansk Erhverv mener, det vil være uhensigtsmæssigt at omfatte denne type kommunikationstjenester uden en forudgående evidensbaseret vurdering af, hvorvidt disse forpligtelser er nødvendige. Vi beder derfor de danske myndigheder om at bekræfte, om dette er tilfældet.

Samtidig understreges det, at såfremt danske myndigheder ikke vil undtage de ovennævnte typer af kommunikationstjenester, bør nye informationsforpligtelser ikke træde i kraft uden en høring blandt de relevante udbydere, ligesom forpligtelserne bør baseres på evidens og være passende, proportionale og tage hensyn til den kontekst, udbyderne opererer i.

Derudover mener vi, det er vigtigt, at udbydere har klarhed om, hvor hurtigt de kan forvente en reaktion fra Center for Cybersikkerhed, når der foretages en underretning. Dansk Erhverv foreslår derfor, at der i §5 indsættes en frist på max. 20 arbejdsdage dage for, hvornår Center for Cybersikkerhed skal træffe afgørelse om, hvorvidt der er behov for et påbud om indsendelse af endeligt aftaleudkast til centeret.

§7-8

Den skærpede frist for underretning i §7 stk. 3 kan reducere udbyderes mulighed for at analysere en hændelse forud for indberetning, hvilket kan medføre unødvendige indberetninger af hændelser, som ved nærmere eftersyn ikke er væsentlige ud fra de opstillede kriterier.

Dansk Erhverv arbejder med udgangspunkt om, at der skal være fair og lige konkurrence mellem udbydere – herunder de forpligtelser, udbyderne underlægges. Vi finder det ikke klart, hvorfor der i § er gjort forskel på grænseværdier for hhv. NUIK-tjenester og mobilabonnementer. Vi foreslår derfor, at grænseværdierne ensrettes, så de for brugertimer og slutbrugere også er 50.000 for mobilabonnementer.

¹ Et eksempel på netværksuafhængige nummerbaserede interpersonelle kommunikationstjenester er "Skype til telefon"-planer

Vi ønsker, at forpligtelserne for NUIK-tjenester også skal gælde de netværksuafhængige nummer-baserede interpersonelle kommunikationstjenester, som på nuværende tidspunkt ikke falder under nogen af de andre kategorier, da disse minder mest om NUIK-tjenester.

For disse typer tjenester vil det være særdeles uhensigtsmæssigt at bliver underlagt krav om at anmelde hændelser til nationale myndigheder. For disse tjenester vil et nedbrud aldrig eller yderst sjældent skyldes en fejl på en lokal netværkskomponent, og et nedbrud vil med større sandsynlighed være grænseoverskridende og gælde i flere lande og/eller regioner. Disse udbydere bør ikke underlægges krav om at skulle vurdere et enkelt nedbrud på tværs af 27 (EU) eller 31 (EØS) landes forskellige kriterier.

Dansk Erhverv understreger behovet for, at der på sigt bør etableres et (1) sæt af harmoniserede kriterier for hændelsesrapportering indenfor EU, ligesom det i størst mulig grad bør tilstræbes at strømline hændelsesrapporteringsproceduren på tværs af grænser. Hvor det er muligt bør hændelsesrapportering ske til en tværeuropæisk enhed, så virksomhedernes forpligtelser ikke giver unødvendige administrative byrder, samtidig med slutbrugerne ydes tilstrækkelig beskyttelse på tværs af Europa.

Dansk Erhverv opfordrer de danske myndigheder til at være opmærksomme på ENISA-rapporten af 10. januar 2020 '*Security Supervision under the EECC*', som anerkender, at det eksisterende regime på tværs af Europa bør opdateres, og at der ideelt bør udvikles en fælles grænseværdi og rapporteringsmodel, så et konsistent system for hændelsesrapportering kan implementeres, der samtidig tager højde for de særlige karakteristika ved OTT-kommunikationstjenester.

Vi anmoder de danske myndigheder om at bakke op om etableringen af en sådan fælleseuropæisk løsning, så én hændelse også kun skal anmeldes et sted.

Dansk Erhverv står gerne til rådighed for uddybning af ovenstående.

Med venlig hilsen,

Christian von Stamm Jonasson

Erhvervspolitisk konsulent