Forsvarsministeriet
Holmens Kanal 9
1060 København K

Sendt pr. mail til fmn@fmn.dk,
nmc@fmn.dk, nls@fmn.dk,
nbb@fmn.dk, eba@fmn.dk

Sagsnummer 2020/004886 &
Sagsnummer 2020/005122

København, 26. august 2020

Høring over forslag til lov om ændring af lov om net- og informationssikkerhed (implementering af direktivet om oprettelse af en europæisk kodeks for elektronisk kommunikation for så vidt angår sikkerhed i net og tjenester) samt høring over udkast til forslag til lov om ændring af lov om elektroniske kommunikationsnet og -tjenester (etablering af mobilbaseret varslingssystem)

Generelle bemærkninger

Teleindustrien og IT-Branchen (herefter høringsparterne) har noteret sig Forsvarsministeriets offentlige høring over lovforslaget om ændring af lov om net- og informationssikkerhed (NIS-loven) samt høringen over udkast til forslag til lov om ændring af lov om elektroniske kommunikationsnet og -tjenester (Teleloven) fsva. etablering af mobilbaseret varslingssystem) og fremsender herunder sine bemærkninger.

Da begge lovforslag, som er sendt i høring, omfatter delelementer af etableringen af mobilbaseret varslingssystem, fremkommer høringsparterne med ét samlet høringssvar på begge disse høringer.

Lovforslagene implementerer dele af direktiv 2018/1972/EU om oprettelse af en europæisk kodeks for elektronisk kommunikation (herefter direktivet). Indledningsvist vil høringsparterne gerne kvittere positivt for den relativt tekstnære direktivimplementering.

Høringsparterne kvitterer positivt for, at udbydere af nummeruafhængige interpersonelle kommunikationstjenester til forskel fra tidligere nu bliver genstand for en række forpligtelser i relation til sikkerheden i sådanne tjenester. Samlet er der dog behov for en ensretning af definitioner med de tilsvarende definitioner i Teleloven.

Høringsparterne sætter pris på Forsvarsministeriets udkast til ændring af Teleloven fsva. etablering af mobilbaseret varslingssystem. Det gælder særligt beslutningen om, at et mobilt varslingssystem baseres på cell broadcast-teknologi, samt at Forsvarsministeriet dækker udgifterne til etableringen og driften af et sådant system.

Høringsparterne sætter desuden spørgsmålstegn ved den nye foreslåede forpligtelse om, at udbydere skal informere brugere om mulige beskyttelsesforanstaltninger i tilfælde af en særlig og betydelig trussel om sikkerhedshændelse. Høringsparterne har svært ved at gennemskue, hvorledes teleudbydere skal kunne informere en specifik (gruppe af) forbrugere, der fx anvender sikkerhedsmæssigt kompromitterbart brugerudstyr, og mener, at det bør præciseres, hvordan der tages beslutning om eventuel informering af brugere om potentielle trusler eller sikkerhedshændelser og mulige beskyttelsesforanstaltninger konkret udmøntes i praksis. Den konkrete udmøntning vil være afgørende for den faktiske mulighed for efterlevelse og for de reelle omkostninger af løsningen. Løsning bør være omkostningseffektiv og proportional i forhold til den ønskede effekt.

Høringsparterne fremsender herunder sine specifikke bemærkninger til lovforslagene, hvor talmarkeringen følger nummerering af foreslåede lovændringer i NIS-loven henholdsvis Teleloven.

Specifikke bemærkninger til ændring af NIS-loven

Nr. 1-3 om ændring af lovens titel

Høringsparterne har forståelse for den foreslåede ændring af lovens titel, da denne er som konsekvens af tilsvarende begrebsændring i teledirektivet. I lyset af ændring af lovens definitioner bør anvendelsen af begreberne "*net og tjenester*" imidlertid ikke anvendes i overskriften, da de rejser tvivl om lovens anvendelsesområde. Høringsparterne opfordrer til, at telelovens begreber "elektroniske kommunikationsnet og -tjenester" anvendes i stedet, jf. også nedenfor. Høringsparterne undres dog over ændringen til det meget generelle begreb "sikkerhed", da der ikke synes at være en konkret begrundelse herfor. Høringsparterne finder, at "informationssikkerhed" er et bredere begreb.

Nr. 4 om ensretning af definitioner med telelovens definitioner

Høringsparterne kvitterer for, at der med ændringen søges en ensretning af definitionerne med de tilsvarende definitioner i Teleloven. Der er dog i enkelte af definitionerne, hvor Forsvarsministeriet lægger op til visse nuanceforskelle i ordvalget. Høringsparterne opfodrer generelt til, at definitionerne affattes fuldstændigt ordret med tilsvarende definitioner i Teleloven, således at der ikke opstår fortolkningstvivl om definitionerne i de to love skal forstås forskelligt.

Høringsparterne skal i øvrigt opfordre til, at definitionerne "*elektroniske kommunikations net og -tjenester*" anvendes konsekvent gennem hele loven i stedet for "net- og tjenester". Eksempelvis fremgår "*net og -tjenester*" fortsat af ændringen til § 2 stk. 1, nr. 8.

Nr. 4 om ny definition af udbyder af nummeruafhængig interpersonel kommunikationstjeneste jf. § 2, nr. 6

Høringsparterne kvitterer umiddelbart positivt for den foreslåede definition i medfør af § 2, nr. 6, af udbyder af nummeruafhængig interpersonel kommunikationstjeneste (i lovforslaget udbydere af NUIK-tjenester). Høringsparterne mener, at denne definition bør være identisk med samme definition som foreslået i § 2, nr. 20 i Lov om Elektroniske kommunikations net og -tjenester (Teleloven), hvilket tillige fremgår som hensigten i lovbemærkningernes side 8 g 23, således at der til enhver tid sikres en ensartet forståelse af begreberne. Dette kan bør gøres ved henvisning til definitionen i Teleloven.

Høringsparterne gør desuden opmærksom på, at begrebet "en nummeruafhængig interpersonel kommunikationstjeneste" ikke forkortes i Teleloven. Således kunne der med fordel skabes mere ensartethed og juridisk klarhed ved at behandle samme begreb på samme måde. Høringsparterne anbefaler at skrive begrebet fuldt ud gennemgående i loven.

Endvidere mener høringsparterne, at udbydere af nummeruafhængige interpersonelle kommunikationstjenester, der opretter forbindelse til offentligt tildelte nummerressourcer, tillige bør være omfattet af definitionen. Sådanne tjenester er allerede omfattet af definitionen om en "*elektronisk kommunikationstjeneste*", jf. Teleloven, da der er tale om en tjeneste, der helt eller delvis består i elektronisk overføring af kommunikation i form af lyd, billeder, tekst eller kombinationer heraf ved hjælp af radio- eller telekommunikationsteknik mellem nettermineringspunkter. Høringsparterne ønsker derfor dette entydigt afklaret i lovens bemærkninger.

Høringsparterne finder det desuden uklart, hvorledes flere af branchens value-added-tjenester vil blive omfattet af definitionen. Det være sig fremtidens interaktive TV-produkter, hvor kommunikation mellem TV-brugere eller kundeservice muliggøres som en støttefunktion. Der kunne også være tale om e-mail-tjenester tilknyttet slutbrugeres bredbåndsabonnement. Såfremt sådanne value-added tjenester menes omfattet, bør det fremgå tydeligt af lovens bemærkninger. Høringsparterne gør tillige opmærksom på, at det er væsentligt at sikre et 'level playing field' i forhold til andre udbydere af fx e-mail-konti, der – såfremt ovenstående bør være omfattet – tillige underlægges samme krav og forpligtelser.

Høringsparterne mener desuden, at det i lovens bemærkninger bør specificeres, hvad der menes med "*som der normalt ydes mod betaling*", som både fremgår direkte af bestemmelsen og af lovbemærkningerne på side 24. Det bør i lovens bemærkninger afklares, hvorvidt der alene er tale om en tjeneste, der normalt ydes mod monetær betaling, eller om betalingen også kan udgøre adgang til brugerens data. Ovenfornævnte tjenester, interaktive tv-pakker og e-mail-tjenester, er eksempelvis ikke tjenester, som kunden betaler monetært for, men er en value-added tjeneste i fx bredbåndsabonnementet.

Nr. 4 om ny definition af sikkerhed i net og tjenester jf. § 2, nr. 7

Høringsparterne noterer sig, at "autenticiteten" nu også er indbefattet i definitionen af "*sikkerhed i net og tjenester*" jf. § 2, nr. 7, som teledirektivets artikel 2, nr. 21, foreskriver, værende i tillæg til tilgængeligheden, integriteten og fortroligheden af elektroniske kommunikations net og -tjenester. Høringsparterne henfører til, at "autenticiteten" i lovbemærkningernes side 24 nærmere defineres som, *"at data og informationssystemer mv. er, hvad de foregiver at være. Begrebet anses således at handle om ægthed og originalitet"*.

Høringsparterne vurderer, at ændringen vil medføre, at teleoperatører i fremtiden fx skal rapportere til myndighederne, hvis data og informationssystemer mv. således ikke er, hvad de foregiver at være.

Et eksempel herpå kunne i praksis være, hvis en ondsindet aktør implementerede et delelement i en operatørs netværk, som operatøren ikke umiddelbart havde kendskab til. Derved ville en given kunde tilgå operatørens systemer, som ikke nødvendigvis er, hvad de foregiver at være, nemlig operatørens fuldt kontrollerede udstyr og systemer. Dette ville i så fald skulle rapporteres til myndighederne, når hændelsen bliver kendt af operatøren.

Hvis ovenstående eksempel er korrekt forstået, finder høringsparterne det rimeligt, at teleoperatørerne bliver genstand for en sådan forpligtelse.

Nr. 4 om ny definition af sikkerhedshændelse jf. § 2, nr. 8

Høringsparterne støtter den foreslåede definition af en sikkerhedshændelse og støtter desuden, at der ikke fokuseres på en potentiel, men en faktisk, indvirkning på sikkerheden. Høringsparterne gør dog opmærksom

på, at graden af den "faktiske negative påvirkning" ikke kendes umiddelbart ved sikkerhedshændelsens begyndelse.

Nr. 6-9 om minimumskrav til informationssikkerhed for udbydere jf. § 3

Høringsparterne støtter den foreslåede ændring af § 3, stk. 1 og 3, om inkludering af nummeruafhængige interpersonelle kommunikationstjenester med samme forbehold som anført ovenfor ved punkt 4. Det er her væsentligt at sikre en level playing field blandt elektroniske kommunikationstjenester, der i stigende grad konkurrerer med hinanden.

I den nye foreslåede § 3, stk. 3, anvendes begrebet "betydelig trussel" om en sikkerhedshændelse, der kan lede til påbud fra myndighederne om at træffe nødvendige foranstaltninger, hvis en sådan identificeres. Høringsparterne finder det hensigtsmæssigt, at begrebet specificeres i lovens bemærkningerne. Høringsparterne finder det ligeledes hensigtsmæssigt, at det specificeres, hvilke typer påbud man påtænker at anvende, samt hvilke konsekvenser disse påbud kan have for operatøren.

Som nævnt ovenfor kendes graden af den faktiske negative påvirkning af en sikkerhedshændelse, og dermed tillige den faktiske negative påvirkning af en betydelig trussel om en sikkerhedshændelse, først senere i forløbet. Derfor kan det være vanskeligt konkret af vurdere den faktiske påvirkning af en betydelig trussel. Høringsparterne finder i øvrigt, at Domstolene bør afsige kendelse om påbuddet, hvis disse foranstaltninger indebærer begrænsninger i de grundlæggende rettigheder.

Selvom vi forstår og anerkender hensynet med og baggrunden for den foreslåede bestemmelse, herunder dens ophav i artikel 41 i teledirektivet, er vi bekymrede over det upræcise omfang af bestemmelsens rækkevidde i forhold til den kompetence, der tillægges CFCS. Omfanget af de konkrete foranstaltninger, CFCS kan pålægge de enkelte udbydere at foretage, er kun i meget begrænset omfang specificeret i lovforslaget og kan med den foreslåede ordlyd af bemærkningerne potentielt tolkes meget bredt.

Det fremgår således af bemærkningerne, at "*det vil afhænge af sikkerhedshændelsens karakter, hvilke foranstaltninger der er nødvendige for at afhjælpe denne", og at en udbyder kan blive pålagt at sikre, "at leverancer af hardware, firmware eller software, der kan udgøre en sårbarhed i den pågældende udbyders net eller tjeneste, skal undersøges for sårbarheder, samt at foretage logisk og fysisk adgangskontrol til nærmere angivne systemer eller udstyr og sikre sporbarhed heraf*."

Dermed tillægges CFCS en i praksis næsten ubegrænset mulighed for at kræve, at konkrete udbydere foretager potentielt særdeles indgribende og omkostningstunge foranstaltninger. Høringsparterne skal kraftigt opfordre til, at denne bestemmelse indsnævres, og at det i langt højere grad præciseres, hvor vidtrækkende kompetencer CFCS får med denne bestemmelse.

Høringsparterne har forståelse for og støtter, at den foreslåede § 3, stk. 4, om at traditionelle teleudbydere kan pålægges forpligtelser ved hensyn af væsentlig samfundsmæssig betydning, fortsætter som hidtil med de mindre, foreslåede sproglige præciseringer.

I lovens bemærkninger på side 10 fremgår et ønske, med henvisning til teledirektivet, om at fremme kryptering, som ikke umiddelbart er en del af det eksisterende lovgrundlag i dag, med mindre det anskues som en del af den interne risikostyringsproces i medfør af lovens § 3, stk. 1. Høringsparterne anerkender dog også, at denne bestemmelse stammer fra teledirektivets artikel 40, stk. 1.

For danske teleudbydere er kryptering i risikostyringen, fx af management styring af infrastrukturen, allerede fuldt implementeret, hvorfor høringsparterne ikke umiddelbart kan se, hvorledes yderligere fremhævelse af kryptering kan/bør ske i Danmark. Høringsparterne har dog ikke kendskab til, hvorledes kryptering anvendes

for udbydere af nummeruafhængige interpersonelle kommunikationstjenester. På den baggrund finder høringsparterne det rimeligt, at der stilles krav til kryptering både på teleoperatørniveau og blandt nye typer af tjenesteudbydere. Endelig anmoder høringsparterne om særlig forsigtighed og proportionalitet i overvejelserne herom, da vidtgående (system-)krav herom kan udgøre væsentlige ekstraomkostninger for udbyderne. Endelig ønsker høringsparterne at gøre opmærksom på, at fremtidens mobile teknologier, herunder 5G, har kryptering af data mellem mobilnetværkets radio access netværk og mobil core-systemet indbygget som standard.

I lovens bemærkninger på side 10, fremgår det desuden af udbydere af nummeruafhængige interpersonelle kommunikationstjenester kan have egen teknisk infrastruktur. Høringsparterne gør i den anledning opmærksom på, at denne type infrastruktur ikke alene omhandler "*forbindelser til internetudbydernes net, som kan blive omfattet sikkerhedskrav*" jf. lovbemærkningernes side 10, men også andre typer af infrastrukturejerskab og drift af fx store datacentre, som bør tages højde for i lovforslaget og dets bemærkninger.

Nr. 11-14 om oplysnings- og underretningspligter for udbydere jf. § 4

Høringsparterne finder det relevant, at udbydere på det danske marked pålægges at informere CfCS om sikkerhedshændelser og anerkender, at den foreslåede ændring i § 4, nr. 3, om såvel tilføjelsen af udbydere af nummeruafhængige interpersonelle kommunikationstjenester samt tilføjelsen af "*uden unødigt ophold*" er en implementering af teledirektivets artikel 40, stk. 2. TI finder dog, at tilføjelsen af "*uden unødigt ophold*" er en signifikant stramning af bestemmelsen i forhold til i dag, hvor fristen er 14 dage. TI skal opfordre til, at denne frist fastholdes i den konkrete udmøntning i bekendtgørelsen.

Høringsparterne finder tilføjelsen af ny nr. 4 i § 4 særligt bekymrende, om at udbydere generelt i alle tilfælde skal underrette offentligheden ved sikkerhedshændelser, der har haft væsentlig indvirkning på driften af net eller tjenester.

Høringsparterne er bekymret over udsigten til i medfør af den foreslåede § 4, stk. 4, at skulle informere offentligheden som sådan om sikkerhedshændelser, der i øvrigt måtte være forsvarligt håndteret. Der vil være stor risiko for, at en generel udmelding til offentligheden om en afsluttet trussel kunne skabe unødig utryghed.

Samtidig bør det overvejes nøje, hvilke risici der løbes, ved at der kommer information om sikkerhedstrusler ud i offentligheden. Høringsparterne er bekymret for, at hvis der er offentlighed om en trussel (uanset om denne anses for at være afsluttet), kan anspore hackere til at gå målrettet mod en udbyder eller en sektor, der har været ramt.

Høringsparterne skal i stedet foreslå, at bestemmelsen ændres således, at udbyderne i stedet forpligtes til at informere konkrete berørte kunder om sikkerhedshændelsen og eventuelt om, hvilke forholdsregler de konkret berørte kunder kan tage i den forbindelse, eller alternativt blødgøres med tilføjelse af "*hvor det findes relevant*".

Høringsparterne sætter imidlertid spørgsmålstegn ved den nye foreslåede bestemmelse i § 4, stk. 5, om at udbydere skal informere brugere om mulige beskyttelsesforanstaltninger i tilfælde af en særlig og betydelig trussel om sikkerhedshændelse. Høringsparterne har således svært ved at gennemskue, hvorledes teleudbydere skal kunne informere en specifik (gruppe af) forbrugere, der fx anvender sikkerhedsmæssigt kompromitterbart brugerudstyr (CPE), fx en ukurant WiFi-router, når denne type information ikke er kendt af teleudbyderen. Høringsparterne anerkender dog også, at teleudbyderne har en interesse i at sikre et så sikkert netværk, som muligt, hvorfor intentionen med forslaget giver god mening.

Usikkerheden omkring udmøntningen af kravene i medfør af § 4, nr. 4, indebærer, at det for visse udbydere i branchen er usikkert, om der skal etableres nye funktioner i virksomheden til at håndtere sådanne nye krav. Det er således nærliggende, at det vil have yderligere omkostningsmæssige konsekvenser for sådanne udbydere at opfylde kravene.

Af bemærkningerne til lovforslaget fremgår det derudover, at "*Som i dag indebærer dette, at udbyderne efter påbud skal underrette offentligheden, eller at CFCS kan foretage underretning af offentligheden, hvis det godtgøres, at dette er i offentlighedens interesse*". Det kan have stor skadegørende effekt på en udbyder, hvis det påbydes en udbyder at melde ud til brugere og offentligheden om mulige trusler eller hvis der af CFCS meldes offentligt ud om mulige trusler. Dette gør sig særligt gældende, når selve hjemmelsgrundlaget for at udstede påbud vedrørende sikkerhedstrusler er uklart. Derfor bør det i loven og bemærkningerne fastlægges under hvilke omstændigheder denne ret til at meddele påbud og egen offentliggørelse kan udnyttes, herunder at udbyderen får mulighed for at blive partshørt, medmindre det af tidsmæssige grunde er umuligt.

Endelig bør det derfor præciseres, hvordan der tages beslutning om eventuel informering af brugere om potentielle trusler eller sikkerhedshændelser og mulige beskyttelsesforanstaltninger konkret udmøntes i praksis.

Høringsparterne finder, at den konkrete udmøntning af bestemmelsen i en bekendtgørelse vil være afgørende for den faktiske mulighed for efterlevelse og for de reelle omkostninger af løsningen. Høringsparterne mener, at den løsning, som tænkes implementeret i Danmark, bør være omkostningseffektiv og proportional i forhold til den ønskede effekt. Som eksempel kunne en samlet informationsportal om kompromitterbart brugerudstyr, som bliver bekendt for teleudbyderen, gøres tilgængeligt for offentligheden og udbyderens kunder på en samlet internetside. Der er mange eksempler på, at dette ikke i praksis er muligt, da udbyderne ikke har de nødvendige processer og data til at sikre effektiv, praksis udmøntning af en sådan løsning. Høringsparterne finder således, at det som minimum tydeliggøres i lovbemærkningerne, hvorledes myndighederne forventer, at udbydere kan designe et system, som kan håndtere dette, og samtidig beskrive de væsentlige omkostninger, der eventuelt vil være forbundet med et sådant system.

Andre bemærkninger

Høringsparterne har ingen indholdsmæssige bemærkninger til lovforslagets punkter 17-27.

Høringsparterne anser desuden, at de i lovbemærkningerne anførte økonomiske konsekvenser for erhvervslivet virker særdeles underestimerede særligt henset til lovforslagets mange usikkerheder. Lovforslaget lægger op til, både direkte og indirekte gennem efterfølgende udmøntning i bekendtgørelser, at flere nye systemer skal designes, indkøbes og implementeres hos udbyderne. Derudover bidrager usikkerheden om kravene til beskyttelsesforanstaltninger og kryptering tillige til øget usikkerhed om omkostningerne. Når det endnu ikke er fuldt ud belyst, hvilke foranstaltninger og lignende loven og efterfølgende bekendtgørelser vil medføre, er det ikke muligt for høringsparterne at vurdere omfanget af de økonomiske konsekvenser for de enkelte selskaber. Samtidig må det forventes, at når udbydere af nummeruafhængige interpersonelle kommunikationstjenester indbefattes en række nye krav, vil det medføre øgede omkostninger for erhvervslivet.

Specifikke bemærkninger til etablering af mobilbaseret varslingssystem jf. NIS-lovens § 5 a og Telelovens §§ 61 a og 81

Generelt

Høringsparterne støtter Forsvarsministeriets forslag til etablering af mobilbaseret varslingssystem jf. NIS-lovens § 5 a og Telelovens §§ 61 a og 81. I særdeleshed beslutningen om, at et mobilt varslingssystem baseres på cell broadcast-teknologi, samt at Forsvarsministeriet afholder omkostningerne ved etablering og drift af et sådant system.

Nr. 1 om etablering af mobilbaseret varslingssystem jf. Teleloven § 61 a

Høringsparterne ser positivt på implementeringen af teledirektivets artikel 108, 2. pkt., om et offentligt mobilbaseret varslingssystem, der kan udsende offentlige advarsler om overhængende eller truede nødsituationer og katastrofer. En forpligtelse til at indføre et sådant system er dog ikke uproblematisk, da mobilselskaberne ikke på nuværende tidspunkt råder over et sådant, og ikke selv har incitament til at indføre systemer, der ikke understøtter driften af selskabernes netværk og forretning. Høringsparterne deler Forsvarsministeriets vurdering af etableringsomkostninger på ca. 140 mio. kr. og årlige driftsomkostningerne på 10 mio. kr. For at undgå unødige tunge økonomiske byrder på erhvervslivet, sætter høringsparterne stor pris på, som det indgår i lovforslaget om ændring af Teleloven, at staten afholder udgifterne forbundet med etablering og drift af det mobilbaserede offentlige varslingssystem. Høringsparterne støtter tillige, at staten også vil afholde dokumenterede udgifter forbundet med krav i medfør af den foreslåede bestemmelse, som ikke allerede følger af de gældende §§ 3 og 5 i NIS-loven. I forlængelse heraf sætter høringsparterne pris på lovbemærkningerne til nr. 1 om, at mobiloperatørerne forud for større økonomiske dispositioner kan have en dialog med de relevante beredskabsmyndigheder med henblik på at afklare, om dispositioner har en karakter, hvor der kan ydes refusion.

Desuden støtter høringsparterne op om Forsvarsministeriets overvejelser og vurdering af, at et mobilbaseret varslingssystem bør baseres på cell broadcast-system. Høringsparterne er enige i, at den foreslåede løsning baseret på cell broadcast-teknologien er den bedste løsning til formålet, blandt andet på grund af de fordele, der nævnt i høringsmaterialet, herunder særligt det forhold, at alle nyere mobiltelefoner kan modtage sådanne beskeder, og at der ikke sker registrering af personoplysninger i forbindelse med brug af systemet.

Der kan synes at være en begrebsforvirring til, hvem pligtsubjektet i medfør af forpligtelsen i den foreslåede bestemmelse i Telelovens § 61 a, hvor begrebet "*Udbydere af elektroniske kommunikationstjenester i mobilnet og udbydere af mobilnet*" anvendes. Dette begreb er imidlertid ikke nærmere defineret i Teleloven. Høringsparterne anbefaler således, at det gøres klart for hvem denne forpligtelse konkret påhviler såvel i Telelovens § 61 a og NIS-lovens § 5a med korrekt anvendelse af klart definerede begreber jf. Telelovens § 2 og NIS-lovens § 2. Således anbefaler TI, at Telelovens § 61 a, stk. 1, affattes:

> "***§ 61 a.*** *Udbydere af* ***offentlige*** *elektroniske kommunikations****net og -****tjenester ~~i mobilnet og udbydere af mobilnet~~ skal på vegne af beredskabsaktører udsende offentlige advarsler om overhængende eller truende alvorlige nødsituationer og katastrofer til berørte slutbrugere. Udbyderne skal udsende offentlige advarsler til de slutbrugere, der i varslingsperioden opholder sig i nærmere angivne geografiske områder, straks efter modtagelse af anmodning herom."*

Samt at NIS-lovens § 5a affattes:

> ***"§ 5 a.*** *Center for Cybersikkerhed fastsætter regler om, at udbydere, som i medfør af telelovens* ***§ 61 a*** *skal udsende offentlige advarsler om overhængende eller truende alvorlige nødsituationer og katastrofer, skal træffe alle nødvendige foranstaltninger til at sikre uafbrudt transmission af advarslerne."*

Nr. 16 om uafbrudt transmission af offentlige advarsler jf. NIS-lovens § 5 a

Høringsparterne ser frem til at bidrage konstruktivt i forbindelse med den konkrete udmøntning af bestemmelsen i bekendtgørelsen, herunder hvorledes *"alle nødvendige foranstaltninger til at sikre uafbrudt transmission af advarslerne"* konkret skal forstås, da dette synes noget uklart. Heriblandt hvad der menes med "uafbrudt", som ikke indgår i ændringen af Telelovens § 61 a. Høringsparterne anbefaler, at den konkrete løsning er fleksibel samt at krav hertil er proportionelle.

I forlængelse heraf vil høringsparterne sætte pris på en bekræftelse af, at opfyldelse af kravet om "uafbrudt transmission" er dækket af Forordning om foranstaltninger vedrørende adgang til det åbne internet artikel 3, stk. 3, 3. afsnit, hvori det fremgår, at udbyderen af internetadgangstjenester kan foretage mere vidtgående trafikstyringsforanstaltninger, hvis det er nødvendigt for at overholde lovgivning, for at opretholde integriteten og sikkerheden i nettet eller for at forebygge truende overbelastning af nettet og afbøde virkningerne af ekstraordinære eller midlertidige overbelastning af nettet.

Da systemet skal kunne tages i brug senest den 22. juni 2022, og da der vi være tale om et teknisk kompliceret setup med høje driftssikkerhedskrav, sætter høringsparterne pris på, at der med lovforslaget er lagt op til et tæt samarbejde mellem mobilselskaberne og Forsvarsministeriet om indførelsen af systemet, herunder udvikling, test, etablering og drift, samt ikke mindst en løbende dialog om de nødvendige økonomiske dispositioner med henblik på at sikre, at mobiloperatørerne kun disponerer således, at der kan ydes refusion af de afholdte udgifter.

Afsluttende bemærkninger

Høringsparterne står naturligvis til rådighed måtte Forsvarsministeriet, Klima-, Energi- og Forsyningsministeriet, Center for Cybersikkerhed, Energistyrelsen eller andre relevante myndigheder have opklarende spørgsmål til ovenstående.

Med venlig hilsen

Mette Lundberg, direktør, IT-Branchen

Jakob Willer, direktør, Teleindustrien