EUROPA-
KOMMISSIONEN

Bruxelles, den 4.10.2017
COM(2017) 476 final

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET

Fuld udnyttelse af NIS – mod en effektiv gennemførelse af direktiv (EU) 2016/1148 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen

DA

Indledning

Direktiv (EU) 2016/1148 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen[1] (i det følgende benævnt "NIS-direktivet" eller "direktivet"), som blev vedtaget den 6. juli 2016, er EU's første horisontale lovgivning om håndtering af cybersikkerhedsudfordringer og et sandt vendepunkt, når det drejer sig om modstandsdygtighed over for cyberangreb og samarbejdet inden for cybersikkerhed i Europa.

De tre primære målsætninger med direktivet er, at:

- forbedre de nationale cybersikkerhedskapaciteter
- styrke samarbejdet på EU-niveau og
- fremme en risikostyringskultur og underretningen om hændelser blandt de vigtigste økonomiske aktører, navnlig de operatører, der leverer tjenester, som er væsentlige for opretholdelsen af samfundsmæssige og økonomiske aktiviteter (operatører af væsentlige tjenester) og udbydere af digitale tjenester.

NIS-direktivet er en milepæl i EU's indsats mod de voksende cybertrusler og -udfordringer, som følger i kølvandet på digitaliseringen af vores økonomiske og samfundsmæssige liv, og direktivets gennemførelse er derfor en vigtig del af den cybersikkerhedspakke, der blev fremlagt den 13. september 2017. Effektiviteten af EU's indsats vil være begrænset, så længe NIS-direktivet ikke er gennemført fuldt ud i alle EU's medlemsstater. Dette blev også fremhævet som en væsentlig pointe i Kommissionens meddelelse fra 2016 om styrkelse af Europas system for modstandsdygtighed over for cyberangreb[2].

NIS-direktivets nyhedsværdi og det akutte behov for at håndtere den hastigt voksende cybertrussel gør, at der er særlig fokus på de udfordringer, som alle aktører står over for, når det handler om at sikre en rettidig og succesfuld gennemførelse af direktivet. Eftersom fristen for gennemførelse er den 9. maj 2018, og fristen for identificering af operatører af væsentlige tjenester er den 9. november 2018, støtter Kommissionen medlemsstaternes gennemførelsesproces og det arbejde, de yder i samarbejdsgruppen med dette mål for øje.

Nærværende meddelelse med bilag er baseret på Kommissionens forberedende arbejde og analyse vedrørende den hidtidige gennemførelse af NIS-direktivet, input fra Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA) og på de drøftelser, der er ført med medlemsstaterne i direktivets gennemførelsesfase, navnlig inden for rammerne af samarbejdsgruppen[3]. Meddelelsen er et supplement til den betydelige indsats, der allerede er gjort, især gennem:

- Det intensive arbejde i samarbejdsgruppen, som er nået til enighed om en arbejdsplan, der overvejende fokuserer på gennemførelsen af NIS-direktivet, herunder særligt på

[1] Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen. Direktivet trådte i kraft den 8. august 2016.
[2] COM(2016) 410 final.
[3] En mekanisme for strategisk samarbejde mellem medlemsstaterne i henhold til NIS-direktivets artikel 11.

spørgsmålet vedrørende identificering af operatører af væsentlige tjenester og deres forpligtelser med hensyn til sikkerhedskrav og pligt til at underrette om hændelser. Selv om direktivet giver skønsbeføjelser med hensyn til gennemførelsen af bestemmelserne vedrørende operatører af væsentlige tjenester, anerkender medlemsstaterne vigtigheden af en harmoniseret tilgang[4].

- Oprettelsen og den hurtige iværksættelse af netværket af enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er), jf. direktivets artikel 12, stk. 1. Efterfølgende er netværket begyndt at lægge fundamentet for et struktureret operationelt samarbejde på europæisk niveau.

Både hvad angår den politiske og det operationelle dimension af disse strukturer er alle medlemsstaters fulde engagement afgørende for at nå målet om et højt fælles sikkerhedsniveau for net- og informationssystemer i Unionen.

Nærværende meddelelse med bilag vil styrke denne indsats ved at samle og sammenligne medlemsstaternes bedste praksis, som er relevant for direktivets gennemførelse, ved at give yderligere vejledning i, hvordan direktivet bør gennemføres, og ved at give mere detaljerede forklaringer af specifikke bestemmelser. Det overordnede mål er at støtte medlemsstaterne med henblik på en effektiv og harmoniseret gennemførelse af NIS-direktivet i hele EU.

Meddelelsen vil endvidere blive suppleret af Kommissionens kommende gennemførelsesforordning om en yderligere specifikation af elementer og parametre i forbindelse med kravene om sikkerhed og underretning om hændelser for udbydere af digitale tjenester, jf. NIS-direktivets artikel 16, stk. 8. Gennemførelsesforordningen vil fremme direktivets gennemførelse med hensyn til de forpligtelser, der påhviler udbydere af digitale tjenester[5].

Meddelelsen indeholder de vigtigste konklusioner af analysen af de områder, der ses som vigtige referencepunkter og potentiel inspiration, når det drejer sig om gennemførelse i national ret. Her er det primære fokus på de bestemmelser, der vedrører medlemsstaternes kapaciteter og forpligtelser med hensyn til de enheder, der er omfattet af direktivets anvendelsesområde. Bilaget indeholder en mere udførlig undersøgelse af de områder, hvor Kommissionen ser den største værdi i at give praktisk vejledning i gennemførelsen. Det sker via forklaringer og fortolkninger af visse af direktivets bestemmelser og via fremlæggelse af bedste praksis samt den akkumulerede erfaring med direktivet indtil videre.

Mod en effektiv gennemførelse af NIS-direktivet

[4] Samarbejdsgruppen arbejder p.t. på retningslinjer for bl.a. kriterierne for identificering af operatører af væsentlige tjenester, jf. direktivets artikel 5, stk. 2, de omstændigheder, hvorunder operatører af væsentlige tjenester har pligt til at underrette om hændelser, jf. direktivets artikel 14, stk. 7, og sikkerhedskravene for operatører af væsentlige tjenester, jf. artikel 14, stk. 1 og 2.

[5] Udkastet til gennemførelsesforordning er tilgængeligt for offentligheden på https://ec.europa.eu/info/law/better-regulation/have-your-say_da.

Målsætningen med NIS-direktivet er at sikre et højt sikkerhedsniveau for net- og informationssystemer i Unionen. Det indebærer forbedring af sikkerheden i internettet og private net- og informationssystemer, der er grundstenen i vores samfund og økonomier. Det første vigtige element i den henseende er medlemsstaternes beredskab, som skal sikres gennem nationale cybersikkerhedsstrategier som beskrevet i direktivet, CSIRT'ernes arbejde og de kompetente nationale myndigheders arbejde.

De nationale strategiers udstrækning

Det er vigtigt, at medlemsstaterne griber den mulighed, der er i forbindelse med gennemførelsen af NIS-direktivet, til at revidere deres nationale cybersikkerhedsstrategier ud fra de mangler, den bedste praksis og de nye udfordringer, der behandles i bilaget.

Selv om direktivet forståeligt nok fokuserer på de virksomheder og tjenester, som er af særligt afgørende betydning, er det cybersikkerheden for økonomien og samfundet som helhed, der skal tages hånd om på helhedsorienteret og sammenhængende vis, den stadig voksende afhængighed af IKT taget i betragtning. Derfor vil vedtagelsen af omfattende nationale strategier, som går ud over minimumskravene i NIS-direktivet (f.eks. at flere sektorer og tjenester end dem, der er opført i henholdsvis bilag II og III til direktivet, skal omfattes), øge den overordnede sikkerhed i net- og informationssystemerne.

Eftersom cybersikkerhed er et relativt nyt og hurtigt voksende område for offentlig politik, er der i de fleste tilfælde brug for nye investeringer, også selv om de offentlige finansers generelle situation kræver nedskæringer og besparelser. Det er følgelig elementært for opnåelsen af direktivets målsætninger, at der træffes ambitiøse beslutninger, som sikrer tilstrækkelige finansielle og menneskelige ressourcer, hvilket er afgørende for en effektiv gennemførelse af nationale strategier, herunder tilstrækkelige ressourcer til nationale kompetente myndigheder og CSIRT'er.

Gennemførelsens og håndhævelsens effektivitet

Behovet for at udpege henholdsvis nationale kompetente myndigheder og centrale kontaktpunkter er fastsat i direktivets artikel 8 og er afgørende for at sikre en effektiv gennemførelse af NIS-direktivet og grænseoverskridende samarbejde. Her har medlemsstaterne både centraliserede og decentraliserede tilgange. Når medlemsstaterne har en mere decentraliseret tilgang med hensyn til udpegning af nationale kompetente myndigheder, har det afgørende betydning, at der sørges for et stærkt samarbejde mellem forskellige myndigheder og kontaktpunkter (*se tabel 1 i bilagets afsnit 3.2*). Dette øger gennemførelsens og håndhævelsens effektivitet.

Tidligere erfaringer med beskyttelsen af kritisk informationsinfrastruktur kan være nyttige, når det drejer sig om at udforme en optimal forvaltningsmodel for medlemsstaterne, der sikrer sektoropdelt gennemførelse af NIS-direktivet såvel som en sammenhængende horisontal tilgang (*se afsnit 3.1 i bilaget*).

Øget kapacitet for de nationale CSIRT'er

Hvis de nationale CSIRT'er i EU ikke er effektive eller har tilstrækkelige ressourcer, jf. NIS-direktivets artikel 9, vil EU fortsat være alt for sårbar over for grænseoverskridende cybertrusler. Medlemsstaterne bør derfor overveje at udvide anvendelsesområdet for CSIRT'erne til også at omfatte andre sektorer og tjenester end dem, der er omfattet af direktivets anvendelsesområde (*se bilagets afsnit 3.3*). Dette vil gøre det muligt for de nationale CSIRT'er at yde operationel støtte ved cyberhændelser i virksomheder og organisationer, som ikke er omfattet af direktivets anvendelsesområde, men som også er vigtige for samfundet og økonomien. Derudover vil medlemsstaterne kunne gøre fuld brug af de supplerende finansieringsmuligheder, der findes under Connecting Europe-facilitetens (CEF) program om digitaltjenesteinfrastrukturer, som har til formål at styrke de nationale CSIRT'ers kapaciteter og indbyrdes samarbejde (*se afsnit 3.5 i bilaget*).

Sammenhæng i identificeringen af operatører af væsentlige tjenester

Ifølge artikel 5 i NIS-direktivet skal medlemsstaterne senest den 9. november 2018 identificere de enheder, der vil blive betragtet som operatører af væsentlige tjenester. I forbindelse med denne opgave kunne medlemsstaterne overveje konsekvent at anvende definitionerne og vejledningen i nærværende meddelelse med henblik på at sikre, at lignende typer enheder, som spiller lignende roller på det indre marked, konsekvent bliver identificeret som operatører af væsentlige tjenester i andre medlemsstater. Medlemsstaterne kunne ligeledes overveje at udvide anvendelsesområdet for NIS-direktivet til også at omfatte offentlige forvaltninger, pga. den rolle de spiller for samfundet og økonomien som helhed (*se afsnit 2.1 og 4.1.3 i bilaget*).

Det vil være meget nyttigt at tilpasse de forskellige nationale tilgange til identificering af operatører af væsentlige tjenester til hinanden i videst muligt omfang, navnlig ved at følge de retningslinjer, der er udarbejdet af samarbejdsgruppen (*se afsnit 4.1.2 i bilaget*), da det vil føre til en mere harmoniseret anvendelse af direktivets bestemmelser og mindske risikoen for markedsfragmentering. I tilfælde hvor operatører af væsentlige tjenester leverer væsentlige tjenester i to eller flere medlemsstater, er det afgørende at stræbe efter at nå en aftale mellem medlemsstaterne (inden for rammerne af høringsprocessen under artikel 5, stk. 4) om en ensartet identificering af enheder (*se afsnit 4.1.7 i bilaget*) for således at undgå forskellig regulering af samme enhed under forskellige medlemsstaters jurisdiktioner.

Forelæggelse af oplysninger for Kommissionen om identificering af operatører af væsentlige tjenester

Ifølge artikel 5, stk. 7, skal medlemsstaterne meddele Kommissionen de nationale foranstaltninger, som gør det muligt at identificere operatører af væsentlige tjenester, listen over tjenester, antallet af operatører af væsentlige tjenester samt deres betydning i forhold til den pågældende sektor. Derudover skal medlemsstaterne angive tærskler, hvis sådanne findes,

til fastlæggelse af det relevante forsyningsniveau eller vigtigheden af den pågældende operatør af væsentlige tjenester. Medlemsstaterne kunne også overveje at dele listerne over identificerede operatører af væsentlige tjenester med Kommissionen, om nødvendigt fortroligt, da dette kunne bidrage til at øge nøjagtigheden og kvaliteten af Kommissionens vurdering (*se afsnit 4.1.5 og 4.1.6 i bilaget*).

Tilpassede tilgange vedrørende sikkerhedskrav og underretning om hændelser for operatører af væsentlige tjenester

Hvad angår sikkerhedskrav og underretningspligt for operatører af væsentlige tjenester (artikel 14, stk. 1-3), vil en tilpasset tilgang med henblik på at gøre det lettere for operatører af væsentlige tjenester at overholde bestemmelserne på tværs af EU-medlemsstaternes grænser i høj grad få en indre marked-effekt. Der henvises her til det arbejde, der pågår med hensyn til samarbejdsgruppens udarbejdelse af en vejledning (*se afsnit 4.2 og 4.3 i bilaget*).

I tilfælde af en væsentlig cyberhændelse, som påvirker adskillige medlemsstater, er det meget sandsynligt, at en operatør af væsentlige tjenester eller en udbyder af digitale tjenester foretager en obligatorisk underretning om hændelsen i henhold til artikel 14, stk. 3, og artikel 16, stk. 3, eller at en anden enhed, som ikke er omfattet af anvendelsesområdet for direktivet, foretager underretningen på frivillig basis, jf. artikel 20, stk. 1. Medlemsstaterne kan i overensstemmelse med Kommissionens henstilling om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser overveje at tilpasse deres nationale tilgange, så de så hurtigt som muligt kan forelægge relevante oplysninger baseret på disse underretninger for de kompetente myndigheder eller CSIRT'erne i andre berørte medlemsstater. Nøjagtige og handlingsrettede oplysninger vil være afgørende for at reducere påvirkningerne eller afhjælpe svagheder, før de bliver udnyttet.

Kommissionen har – i en ånd af partnerskab, der søger at få mest muligt ud af NIS-direktivet – til hensigt at udvide støtten under Connecting Europe-faciliteten til alle relevante interessenter, der er omfattet af denne lovgivning. Om end fokus har været på at opbygge CSIRT'ernes kapacitet og etablere en platform for hurtigt og effektivt operationelt samarbejde med henblik på at styrke CSIRT-netværket, vil Kommissionen nu undersøge, hvordan finansiering under Connecting Europe-faciliteten også kan gavne nationale kompetente myndigheder såvel som operatører af væsentlige tjenester og udbydere af digitale tjenester.

Konklusion

I lyset af, at fristen for indarbejdelse af NIS-direktivet i national lovgivning, som er den 9. maj 2018, nærmer sig, og under hensyntagen til at fristen for identificering af operatører af væsentlige tjenester er den 9. november 2018, bør medlemsstaterne træffe passende foranstaltninger for at sikre, at bestemmelserne og samarbejdsmodellerne i NIS-direktivet kan give de bedst mulige værktøjer på EU-niveau til at nå et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen. Kommissionen opfordrer medlemsstaterne til i processen at medtage alle relevante oplysninger, vejledninger og henstillinger indeholdt i denne meddelelse.

Meddelelsen kan blive fulgt op at yderligere tiltag, herunder tiltag affødt af det igangværende arbejde i samarbejdsgruppen.