SUNDHEDS- OG ÆLDREMINISTERIET

Holbergsgade 6
DK-1057 København K

T +45 7226 9000
F +45 7226 9001
M sum@sum.dk
W sum.dk

Folketingets Sundheds- og Ældreudvalg

Dato: 3. april 2018
Enhed: SUNDOK
Sagsbeh.: DEPMAHA
Sagsnr.: 1706260
Dok. nr.: 572566

Folketingets Sundheds- og Ældreudvalg har den 1. marts 2018 stillet følgende spørgsmål nr. 6 (L 143 – Forslag til lov om krav til sikkerhed for net- og informationssystemer inden for sundhedssektoren) til sundhedsministeren, som hermed besvares. Spørgsmålet er stillet efter ønske fra Stine Brix (EL) og Kirsten Normann Andersen (SF).

Spørgsmål nr. 6:
"Ministeren bedes oplyse, hvilke konkrete oplysninger det forventes, at ministeren og Center for Cybersikkerhed vil kunne eller skulle udveksle med andre myndigheder, både nationalt og i EU."

Svar:
Det fremgår af den foreslåede § 5, stk. 1, i forslag til lov om krav til sikkerhed for net- og informationssystemer inden for sundhedssektoren, at operatører af væsentlige tjenester hurtigst muligt skal underrette sundhedsministeren og Center for Cybersikkerhed om hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, der leveres.

Det skal bemærkes, at det fremgår af lovforslagets afsnit 4.6, at Sundhedsdatastyrelsen vil skulle varetage de opgaver, der i lovforslaget er tillagt ministeren, hvorfor underretningen vil skulle ske til Sundhedsdatastyrelsen.

Det fremgår endvidere af lovforslagets § 5, stk. 5, at sundhedsministeren vil fastsætte nærmere regler om underretning, herunder hvilke oplysninger der skal underrettes om.

Et udkast til bekendtgørelse om operatører af væsentlige tjenester forventes sendt i høring ultimo marts 2018. Bekendtgørelsen vil skulle træde i kraft samtidig med lovforslaget, det vil sige den 10. maj 2018.

Det forventes, at bekendtgørelsen bl.a. vil angive følgende kategorier af oplysninger, som en operatør af en væsentlig tjeneste vil skulle oplyse i tilfælde af en hændelse, der har væsentlige konsekvenser for kontinuiteten af den væsentlige tjeneste, der leveres: Navn og kontaktoplysninger på operatøren, oplysninger om hændelsens årsag, karakter, varighed, forløb og konsekvenser, oplysninger om foranstaltninger, som operatøren har truffet, eller foreslår truffet, for at håndtere hændelsen, oplysninger om omfanget af hændelsen og oplysninger om eventuelle grænseoverskridende konsekvenser af hændelsen.

Oplysningerne, som Sundhedsdatastyrelsen og Center for Cybersikkerhed vil kunne komme i besiddelse af, er således som udgangspunkt oplysninger om en hændelses karakter.

Det vil dermed også være disse kategorier af oplysninger, som Sundhedsdatastyrelsen og Center for Cybersikkerhed vil kunne udveksle med andre myndigheder.

Lovforslaget regulerer ikke området for behandling af personoplysninger. Men som det fremgår af lovforslagets afsnit 2, vil videregivelse af personoplysninger skulle ske i overensstemmelse med gældende ret, herunder bl.a. databeskyttelsesdirektivet, som ophæves den 25. maj 2018, jf. Europa-Parlamentets og Rådets forordning 2016/679/EU af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (herefter databeskyttelsesforordningen), som finder anvendelse fra den 25. maj 2018.

Da spørgsmålet tilmed omhandler, hvilke oplysninger det forventes, at Center for Cybersikkerhed vil kunne eller skulle udveksle med andre myndigheder, både nationalt og i EU, har mit ministerium bedt Forsvarsministeriet om bidrag til besvarelsen heraf. Forsvarsministeriet oplyser følgende:

"FE/Center for Cybersikkerhed er anmodet om en udtalelse til brug for Forsvarsministeriets besvarelse. FE/Center for Cybersikkerhed har i den anledning oplyst følgende:

"Det følger af NIS-direktivets artikel 14, stk. 3, at medlemsstaterne skal sikre, at operatører af væsentlige tjenester hurtigst muligt foretager underretning til tilsynsmyndighederne eller CSIRT'en af hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som de leverer. Underretningerne skal indeholde oplysninger, der gør det muligt at fastslå eventuelle grænseoverskridende konsekvenser af hændelsen. Der gælder en lignende underretningsforpligtelse for udbydere af digitale tjenester, jf. artikel 16, stk. 3. Derudover følger det af direktivet, at enheder, som ikke er blevet identificeret som operatører af væsentlige tjenester eller udbydere af digitale tjenester, kan foretage frivillige underretninger om hændelser, der har væsentlige konsekvenser for kontinuiteten af de tjenester, som de leverer, og at frivillige underretninger skal behandles efter samme regler som pligtmæssige underretninger, jf. artikel 20.

Det følger af direktivets artikel 14, stk. 4, at der ved fastlæggelsen af, om en hændelses konsekvenser er betydelige, navnlig skal lægges vægt på følgende forhold: Antallet af brugere, der berøres af hændelsen, hændelsens varighed og den geografiske udbredelse med hensyn til det område, der berøres af hændelsen. Der gælder nogenlunde tilsvarende kriterier i forhold til udbydere af digitale tjenester, jf. artikel 16, stk. 4.

Bortset fra kravet om, at underretninger skal indeholde oplysninger, der gør det muligt at fastslå eventuelle grænseoverskridende konsekvenser af hændelsen, indeholder NIS-direktivet ikke krav om, hvilke oplysninger en underretning i øvrigt skal indeholde. Det vil derfor være op til ressortmyndighederne inden for de enkelte sektorer at fastsætte nærmere regler om underretning inden for deres respektive sektorer.

Det vil i almindelighed være tilstrækkeligt for at kunne varetage de opgaver, som følger af direktivet, jf. nedenfor, at underretningerne indeholder overordnede oplysninger om hændelsen, herunder om den berørte virksomhed, tidspunktet for og varigheden af hændelsen, beskrivelse af hændelsen og dens konsekvenser samt en vurdering af mulige grænseoverskridende konsekvenser af hændelsen. Underretningerne vil som det helt klare udgangspunkt ikke indeholde personoplysninger, bortset fra eventuelle oplysninger om den medarbejder, som har forestået selve underretningen. Hvis hændelsen er forårsaget af et egentligt angreb, vil det desuden kunne være relevant at anføre IP-adresser, mailadresser mv., som anvendes af den ondsindede aktør. Det vil eksempelvis også kunne være relevant at medtage såkaldte phishing-mails, der har forårsaget en hændelse.

Underretningerne er en forudsætning for, at tilsynsmyndighederne, CSIRT'en og det centrale kontaktpunkt kan varetage en række opgaver efter NIS-direktivet. Visse af opgaverne forudsætter, at der videregives oplysninger til andre myndigheder, herunder udenlandske. Det kan i den forbindelse nævnes, at underretningerne bl.a. skal danne grundlag for, at det nationale centrale kontaktpunkt årligt kan forelægge en sammenfattende rapport om modtagne underretninger for EU's Samarbejdsgruppe, jf. artikel 10, stk. 3. Det fremgår endvidere af bestemmelsen, at den sammenfattende rapport bør indeholde oplysninger om antallet af modtagne underretninger og arten af de underrettede hændelser. Det fremgår udtrykkeligt af betragtning nr. 33 til direktivet, at den sammenfattende rapport bør anonymiseres for at sikre, at underretningerne og identiteten på den underrettende operatør eller tjeneste forbliver fortrolige, eftersom oplysninger om de underrettende enheders identitet ikke er påkrævet for udveksling af bedste praksis i Samarbejdsgruppen.

Underretningerne er også en forudsætning for, at tilsynsmyndigheden eller CSIRT'en kan orientere andre medlemsstater om hændelser af relevans for dem, jf. artikel 14, stk. 5, og artikel 16, stk. 6. I den forbindelse sikrer tilsynsmyndigheden eller CSIRT'en i overensstemmelse med EU-retten eller national lovgivning, der er i overensstemmelse med EU-retten, sikkerheden og de kommercielle interesser for operatøren eller udbyderen samt fortrolig behandling af de oplysninger, der er givet i dennes underretning.

Underretningerne er derudover en forudsætning for, at tilsynsmyndigheden eller CSIRT'en kan orientere offentligheden om konkrete hændelser, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse, jf. artikel 14, stk. 6, og artikel 16, stk. 7. Det følger af direktivet, at offentliggørelsen skal ske under hensyntagen til bl.a. operatørens sikkerhed, operatørens kommercielle interesser og fortrolig behandling af de af operatøren angivne oplysninger i forbindelse med dennes underretning. For så vidt angår udbydere af digitale tjenester kan offentliggørelse endvidere ske, hvis det i øvrigt er i offentlighedens interesse.

Der er ved implementeringen af NIS-direktivet i dansk ret lagt op til, at opgaverne som CSIRT og centralt kontaktpunkt skal varetages af Center for Cybersikkerhed. Der er endvidere lagt op til, at centeret skal varetage opgaverne med at underrette andre medlemsstater om hændelser med grænseoverskridende konsekvenser og at orientere offentligheden om konkrete hændelser i de tilfælde, hvor hændelsen berører

flere sektorer. Forsvarsministeriet har den 7. februar 2018 fremsat lovforslag nr. L 139 om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter mv., som regulerer Center for Cybersikkerheds opgavevaretagelse på området. Der er med lovforslaget bl.a. lagt op til at give centeret en udtrykkelig hjemmel til at videregive de modtagne underretninger om hændelser af grænseoverskridende karakter til nationale tilsynsmyndigheder, CSIRT'er og nationale centrale kontaktpunkter i andre EU-medlemslande samt til CSIRT-netværket (operationelt samarbejdsforum i EU). Der lægges i den forbindelse op til, at der bør ske orientering af den underrettende operatør eller udbyder af digitale tjenester i forbindelse med videregivelsen. Operatøren eller udbyderen vil ligeledes modtage kopi af de videregivne oplysninger.

For så vidt angår orientering af offentligheden om en konkret hændelse, er der lagt op til, at orienteringen som udgangspunkt varetages af de enkelte tilsynsmyndigheder, idet orienteringen dog foretages af Center for Cybersikkerhed i de tilfælde, hvor en hændelse berører flere sektorer. Det fremgår udtrykkeligt af lovudkastet, at centerets orientering ikke må indeholde oplysninger om enkeltpersoners forhold. Videregivelsen af oplysninger fra Center for Cybersikkerhed til andre myndigheder, herunder udenlandske, vil basere sig på de modtagne underretninger, og der vil således i almindelighed være tale om at videregive overordnede oplysninger om en hændelse.

Der vil som det helt klare udgangspunkt ikke blive tale om at videregive personoplysninger. Dog vil det efter omstændighederne kunne være relevant at videregive oplysninger om IP-adresser, mailadresser mv., som anvendes af en formodet ondsindet aktør, der måtte have forårsaget den pågældende hændelse, med henblik på, at andre kan beskytte sig mod tilsvarende angreb. Af samme grund vil det f.eks. også kunne være relevant at medtage såkaldte phishing-mails, der har forårsaget en hændelse. Hvis der måtte være behov for at videregive personoplysninger, vil det skulle ske i overensstemmelse med reglerne i lov om Center for Cybersikkerhed (CFCS-loven). Reglerne om behandling, herunder videregivelse, af personoplysninger er fastsat i CFCS-lovens kapitel 6, som indeholder størstedelen af de centrale principper fra persondataloven."

Forsvarsministeriet kan henholde sig til Center for Cybersikkerheds udtalelse."

Jeg kan henholde mig til Forsvarsministeriets bidrag.

Med venlig hilsen

Ellen Trane Nørby / Maja Holm Andreasen