FORSVARSMINISTERIET
DANISH MINISTRY OF DEFENCE

Folketingets Forsvarsudvalg
Christiansborg

FORSVARSMINISTEREN
23. maj 2014

Folketingets Forsvarsudvalg har den 13. maj 2014 stillet følgende spørgsmål 3 vedrørende L 192 til forsvarsministeren, som hermed besvares. Spørgsmålet er stillet efter ønske fra Nikolaj Villumsen (EL).

Spørgsmål 3:
"Ministeren bedes yde teknisk bistand til udarbejdelse af ændringsforslag, der løser følgende:
a) Hvordan kan definitionen af "sikkerhedshændelser" ændres, så den i stedet svarer til Beredskabsstyrelsens definition?
b) Hvordan kan det sikres, at offentligheden får indsigt i hvilke firmaer og institutioner, som bliver tilkoblet?
c) Hvordan kan der strammes op på definitionen af "nødvendigt", som anvendes mange steder i lovforslaget?
d) Hvordan kan der sikres lognings- og notatpligt af personfølsomme oplysninger?
e) Hvordan sikres det, at der udelukkende er mulighed for opbevaring af pakkedata i 14 dage?
f) Hvordan sikres det, at der udelukkende er mulighed for opbevaring af trafikdata i 12 måneder?
g) Hvordan sikres der vandtætte skodder mellem FE og Center for Cybersikkerhed?
h) Hvordan sikres det, at Center for Cybersikkerhed får forbud mod at udlevere oplysninger til andre efterretningstjenester?
i) Hvordan sikres der forbud mod at bryde kryptering uden dommerkendelse i tråd med brevhemmeligheden?"

HOLMENS KANAL 42
1060 KØBENHAVN K
TELEFON: 33 92 33 20
TELEFAX: 33 32 06 55
MAIL: FMN@FMN.DK
WEB: www.FMN.DK
CVR: 25-77-56-35
EAN: 5798000201200

Svar:
ad a) Et forslag til ændring af definitionen af sikkerhedshændelse som anført i spørgsmålet vil f.eks. kunne affattes således:

Til § 2

1) Nr. 1 affattes således:

»1) *Sikkerhedshændelse:* Elektroniske angreb rettet mod informations- og kommunikationsteknologi, herunder computere, servere, netværk og tjenester, som er forbundet direkte eller indirekte til internettet, med det formål at skade eller ødelægge informations- og kommunikationsteknologi, tilegne sig kontrol over styringen af informations- og kommunikationsteknologi eller uretmæssigt at få adgang til data lagret på informations- og kommunikationsteknologi.«

Indledningsvist bemærkes det, at Beredskabsstyrelsen ikke opererer med en egentlig definition af begrebet sikkerhedshændelse. Beredskabsstyrelsen har imidlertid i Nationalt Risikobillede af 9. april 2013 beskrevet en række karakteristika ved cyberangreb, og disse er anvendt ved affattelsen af ændringsforslaget.

Ændringsforslaget indebærer, at begrebet sikkerhedshændelser defineres mere snævert, således at begrebet alene omfatter angreb på informations- og kommunikationssystemer, men ikke trusler om sådanne angreb. Dette vil have som konsekvens, at Center for Cybersikkerhed i medfør af lovforslagets § 3, stk. 1, alene vil have til opgave at opdage, analysere og bidrage til at imødegå deciderede angreb. Centeret vil dermed i mindre grad få mulighed for at foretage forebyggende arbejde ved at opdage, analysere og bidrage til at imødegå trusler med henblik på at hindre angreb. Det kan endvidere være vanskeligt at fastslå, hvornår en hændelse kan karakteriseres som et angreb.

Herudover indebærer ændringsforslaget, at en sikkerhedshændelse defineres som angreb på informations- og kommunikationsteknologi, som er forbundet direkte eller indirekte til internettet. Dette vil f.eks. have som konsekvens, at en hændelse, hvor et netværk, der ikke er forbundet til internettet, ødelægges af en virus introduceret via en USB-nøgle, ikke kan karakteriseres som en sikkerhedshændelse. Som eksempel på netværk, der ikke er forbundet til internettet, kan nævnes netværk, der anvendes til klassificeret kommunikation.

Den foreslåede definition vurderes endvidere at være vanskelig at benytte i praksis. Det vil således som udgangspunkt være vanskeligt at påvise det subjektive element, som følger af den foreslåede bestemmelse. En typisk sag i det nuværende GovCERT starter i dag ved, at

der opstår en computergenereret alarm i sensornetværket. Det kan eksempelvis ske, hvis der i en tilsluttet myndigheds internetkommunikation ses indikatorer på kommunikation fra en ip-adresse, som er kendt for at sende malware. Grundlaget for at analysere data er således, at der er en formodning for, at der i den pågældende internetkommunikation findes malware, og at det udgør en trussel. Det kan dog ikke uden en nærmere analyse af internetkommunikationen konstateres, om der rent faktisk er tale om malware og endnu mindre, om en eventuel malware har til formål at skade eller ødelægge informations- og kommunikationsteknologi, tilegne sig kontrol over styringen af informations- og kommunikationsteknologi eller uretmæssigt at få adgang til data lagret på informations- og kommunikationsteknologi.

På denne baggrund kan jeg ikke støtte et sådant ændringsforslag.

ad b) Det følger allerede af lovforslaget (bemærkningerne til § 3), at Center for Cybersikkerhed regelmæssigt vil offentliggøre, hvilke myndigheder og virksomheder der efter § 3, stk. 2 og 3, er tilsluttet netsikkerhedstjenesten.

Det følger endvidere af bemærkningerne til lovforslagets § 24, at oversigten også vil omfatte statistiske oplysninger om antallet af myndigheder og virksomheder, der midlertidigt er tilsluttet netsikkerhedstjenesten.

Såfremt det også skal være en pligt at offentliggøre navnene på de midlertidigt tilsluttede myndigheder eller virksomheder efter § 6, vil dette kunne fastsættes i Forsvarsudvalgets betænkning over lovforslaget af et flertal i udvalget.

Det bemærkes, at jeg ikke kan støtte et sådant forslag, da den midlertidige tilslutning forudsætter, at der er tale om en begrundet mistanke om en sikkerhedshændelse. En midlertidig tilslutning vil således primært være relevant i de tilfælde, hvor myndigheder eller virksomheder er udsat for et cyberangreb eller trusler herom. En liste over de midlertidigt tilsluttede myndigheder og virksomheder vil derfor kunne anvendes som en liste over interessante angrebsmål. En liste med navnene på midlertidigt tilsluttede myndigheder og virksomheder vil endvidere kunne føre til, at myndigheder og virksomheder af denne grund vil være tilbageholdende med at anmode om midlertidig tilslutning.

ad c) Et krav om, at behandlingen af personoplysninger skal være nødvendig, anføres i lovforslagets § 10, nr. 2-6, § 11, stk. 2, nr. 3 og 4, § 12, stk. 1 og stk. 2, nr. 3 og 4, § 14, § 15 og § 16, nr. 2.

En skærpelse af kravet til f.eks. ”strengt nødvendigt” skal således foretages i disse bestemmelser (eller en del af disse).

Nødvendighedskravet i lovforslagets §§ 10, 11, 12 og 14 svarer til det tilsvarende nødvendighedskrav i persondataloven.

Nødvendighedskravet i lovforslagets §§ 15 og 16 svarer til nødvendighedskravet efter den gældende GovCERT-lov, jf. dennes § 4, stk. 1, og § 6, nr. 3.

Bl.a. på den baggrund kan jeg ikke støtte en skærpelse af kravet til f.eks. strengt nødvendigt.

Udtrykket strengt nødvendigt anvendes i øvrigt heller ikke i danske lovbestemmelser, så vidt det er Forsvarsministeriet bekendt. Hertil kommer, at et krav om nødvendighed er et restriktivt kriterium.

ad d) Et ændringsforslag om lognings- og notatpligt vil f.eks. kunne affattes således:

Til § 15

1) Efter stk. 1 indsættes som nyt stykke:

»*Stk. 2.* Center for Cybersikkerhed skal foretage logning i forbindelse med analyse af data efter stk. 1.«

Forsvarsministeriet er enig i, at Center for Cybersikkerhed skal foretage logning i de tilfælde, hvor en analytiker fra Center for Cybersikkerhed på baggrund af indgreb i meddelelseshemmeligheden foretager en analyse af data.

Det fremgår imidlertid allerede af bemærkningerne til lovforslagets § 24, at Tilsynet med Efterretningstjenesterne i den årlige redegørelse skal medtage en statistik over antallet af tilfælde, hvor en analytiker fra Center for Cybersikkerhed på baggrund af indgreb i meddelelseshemmeligheden har foretaget en analyse af data. Denne statistik skal desuden indeholde en overordnet kategorisering af, hvor alvorlige disse tilfælde har været. En sådan statistik forudsætter, at Center for Cybersikkerhed foretager logning af samtlige tilfælde, hvor der i medfør af lovforslagets § 15, stk. 1, foretages analyse af data, ligesom centeret forudsættes at notere alvorligheden af de pågældende tilfælde. Det fremgår således allerede i dag af lovforslaget, at Center for Cybersikkerhed skal foretage logning, og der er derfor ikke behov for ændringsforslaget, jf. også besvarelsen af spørgsmål 8, sidste afsnit.

ad e og f) Det forudsættes, at de i spørgsmålene anførte begrænsninger af opbevaringsperioden kun skal gælde for data, der ikke knytter sig til en sikkerhedshændelse, og at æn-

dringsforslaget således går ud på at opretholde den gældende retstilstand. I så fald kan et sådant ændringsforslag affattes således:

Til § 17

1) Stk. 2 affattes således:
»*Stk. 2.* Uanset at formålet med behandlingen ikke er opfyldt, jf. stk. 1, må
1) data, der knytter sig til en sikkerhedshændelse, højst opbevares i tre år, og
2) data, der ikke knytter sig til en sikkerhedshændelse, højst opbevares i 12 måneder for så vidt angår trafikdata og højst 14 dage for så vidt angår pakkedata.«

For god ordens skyld bemærkes, at jeg ikke kan støtte et sådant ændringsforslag. Om begrundelsen herfor henvises til besvarelsen af spørgsmål 10 c.

ad g) Et ændringsforslag om, at der skal være vandtætte skodder mellem Forsvarets Efterretningstjeneste og Center for Cybersikkerhed vil f.eks. kunne affattes således:

Til § 16

1) Efter stk. 1 indsættes som nyt stykke:

»*Stk. 2.* Data, der er omfattet af §§ 4, 6 og 7, må ikke gøres tilgængelige for den øvrige del af Forsvarets Efterretningstjeneste.«

Jeg kan ikke støtte et sådant ændringsforslag.

Baggrunden herfor er, at Center for Cybersikkerhed ikke i forbindelse med et cyberangreb vil kunne trække på de relevante ressourcer i den øvrige del af Forsvarets Efterretningstjeneste, f.eks. i forbindelse med undersøgelser af den meget store andel af cyberangrebene mod Danmark, som hidrører fra udlandet, og hvor Forsvarets Efterretningstjeneste som udenrigsefterretningstjeneste vil kunne bidrage med en række værdifulde oplysninger, såfremt Center for Cybersikkerhed kan stille data til rådighed for tjenesten. Der henvises i øvrigt til besvarelsen af spørgsmål 7.

ad h) Center for Cybersikkerheds netsikkerhedstjeneste kan efter lovforslaget (§ 16, nr. 2) ikke videregive data, der stammer fra civile danske myndigheder eller virksomheder, til udenlandske efterretningstjenester. Tekniske data (trafikdata) kan dog videregives til udenlandske netsikkerhedstjenester, fordi samarbejdet med disse netsikkerhedstjenester er af afgørende betydning for beskyttelsen mod cyberangreb fra udlandet. Dette gælder også,

selv om en udenlandsk netsikkerhedstjeneste måtte være placeret i en efterretningstjeneste.

Videregivelse af tekniske oplysninger til udenlandske netsikkerhedstjenester må dog kun ske, når der er begrundet mistanke om en sikkerhedshændelse, og hvis det er nødvendigt for udførelsen af netsikkerhedstjenestens opgaver.

Netsikkerhedstjenesten må ikke videregive indholdet af internetkommunikation (pakkedata) – f.eks. indholdet af e-mails – til udlandet, heller ikke til en udenlandsk netsikkerhedstjeneste.

I øvrigt gælder, at videregivelse af data vil være underlagt tilsyn af Tilsynet med Efterretningstjenesterne.

På den anførte baggrund følger det således allerede af lovforslagets § 16, nr. 2, at Center for Cybersikkerhed har forbud mod udlevering af oplysninger til andre efterretningstjenester.

ad i) Et ændringsforslag om et forbud mod afkryptering vil f.eks. kunne affattes således:

Til § 15

1) Efter stk. 1 indsættes som nyt stykke:

»*Stk. 2.* Center for Cybersikkerhed må ikke uden forudgående retskendelse foretage afkryptering i forbindelse med analyse af data efter stk. 1.«

Det fremgår af bemærkningerne til GovCERT-lovens § 4 (L 197, 1. samling 2010-11), at GovCERT som udgangspunkt ikke vil afkryptere en krypteret e-mail eller andet indhold af en internetkommunikation. Den eneste undtagelse hertil er, hvis ikke-krypteret kommunikation, som GovCERT har indsamlet via sensornetværket, indeholder en skadelig fil, f.eks. en virus med et krypteret indhold. I dette tilfælde kan GovCERT afkryptere indholdet af filen for nærmere at analysere virussen. GovCERT kan ikke foretage denne delvise afkryptering, hvis hele kommunikationen er krypteret.

Ændringsforslaget indebærer således en skærpelse af den gældende ordning, idet Center for Cybersikkerhed ikke uden retskendelse vil kunne afkryptere data i forbindelse med analyse af pakkedata, der er omfattet af lovforslagets §§ 4, 6 og 7 – heller ikke, hvor der alene er tale om en krypteret fil vedhæftet en ikke-krypteret kommunikation.

Hvis Center for Cybersikkerhed ikke kan få adgang til at opdage skadelige filer i en krypteret kommunikation, indebærer dette en meget væsentlig og meget uhensigtsmæssig begrænsning for Center for Cybersikkerheds netsikkerhedstjeneste, særligt set i lyset af, at angribere ofte anvender krypteret kommunikation for at søge at skjule cyberangreb.

Det kan i øvrigt oplyses, at hvis Center for Cybersikkerhed, som det foreslås i lovforslaget, får mulighed for at foretage afkryptering, vil det alene være i situationer, der knytter sig til en konkret sikkerhedshændelse.

Endvidere vil Center for Cybersikkerhed i sin årlige beretning om sin virksomhed beskrive de omstændigheder, hvor det har været nødvendigt at foretage afkryptering.

Endelig kan det nævnes, at der efter lovforslaget ikke er adgang til at kræve de tilsluttede myndigheders og virksomheders krypteringsnøgler udleveret. Der henvises herom til bemærkningerne til lovforslagets § 4.

Det er Forsvarsministeriets opfattelse, at spørgsmålet om, hvorvidt der må foretages kryptering, ikke er egnet til domstolsprøvelse. Det skyldes, at den krypterede internetkommunikation i sagens natur ikke vil være læselig forud for en afkryptering, og idet det ofte ikke vil være muligt at identificere en mistænkt, ligesom det ikke vil være muligt nærmere at fastslå omfanget af og eventuelt formålet med det mulige angreb. Domstolene vil således reelt ikke kunne foretage en nærmere prøvelse i denne type sager.

På den baggrund kan jeg ikke støtte et sådant ændringsforslag.

Det bemærkes i øvrigt, at et krav om retskendelse, før der må foretages afkryptering, vil forudsætte, at der i bemærkningerne til lovbestemmelsen/lovteksten på en lang række punkter vil skulle tages stilling til procesretlige spørgsmål i forbindelse med domstolsbehandlingen af en anmodning om afkryptering.

Med venlig hilsen

Nicolai Wammen