FORSVARSMINISTERIET
DANISH MINISTRY OF DEFENCE

Folketingets Forsvarsudvalg
Christiansborg

FORSVARSMINISTEREN
23. maj 2014

Folketingets Forsvarsudvalg har den 14. maj 2014 stillet følgende spørgsmål 10 vedrørende L 192 til forsvarsministeren, som hermed besvares. Spørgsmålet er stillet efter ønske fra ikkemedlem af udvalget (MFU) Simon Emil Ammitzbøll (LA).

Spørgsmål 10:
"Ministeren bedes kommentere de synspunkter og bekymringer angående:
a) definitionen på sikkerhedshændelser og hvilke beføjelser myndighederne præcis har til at undersøge sikkerhedshændelser,
b) lovindgrebets proportionalitet og
c) opbevaringstider,
som blev fremført af oplægsholderne under høringen i Retsudvalget den 8. maj 2014 om lovforslaget, jf. høringsoplæggene omdelt på L 192 – bilag 2."

Svar:
ad a) Lovforslagets definition af en sikkerhedshændelse er en videreførelse af definitionen i den gældende GovCERT-lov (lov nr. 596 af 14. juni 2011), der blev enstemmigt vedtaget af Folketinget.

Definitionen er dog sprogligt præciseret, således at det udtrykkeligt fremgår af bestemmelsens ordlyd, at sikkerhedshændelser er hændelser med en negativ påvirkning af tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale tjenester. Det præciseres endvidere, at begrebet sikkerhedshændelse omfatter hændelser, der vurderes at ville kunne have den beskrevne påvirkning.

Undersøgelser af sikkerhedshændelser foretages af Center for Cybersikkerheds særlige netsikkerhedstjeneste. Lovforslagets § 15 regulerer rammerne for netsikkerhedstjenestens analyser af pakkedata (indholdet af elektronisk kommunikation) på baggrund af indgreb i med-

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

delelseshemmeligheden. Efter bestemmelsen må netsikkerhedstjenestens sikkerhedsanalytikere kun analysere indholdet af kommunikationen, hvis der er en begrundet mistanke om en sikkerhedshændelse – og da kun i det omfang, det er nødvendigt for afklaring af forhold vedrørende hændelsen.

Lovforslagets § 15 er, som de øvrige behandlingsregler i lovforslagets kapitel 6 og 7, underlagt tilsyn af Tilsynet med Efterretningstjenesterne.

ad b) For så vidt angår proportionaliteten af indgreb i meddelelseshemmeligheden fremgår det af afsnit 3.2.3 i de almindelige bemærkninger til lovforslaget, at Center for Cybersikkerheds netsikkerhedstjeneste altid ud fra et proportionalitetshensyn i videst muligt omfang vil søge at løse opgaverne ved hjælp af data, som ikke vil kræve et indgreb i meddelelseshemmeligheden.

I den forbindelse skal det endvidere understreges, at lovforslaget er baseret på den ordning, der blev indført med GovCERT-loven i 2011. Der henvises i den forbindelse til afsnit 3.7 i de almindelige bemærkninger til GovCERT-loven (L 197), hvoraf det fremgår, at der i forbindelse med udarbejdelsen af GovCERT-loven blev foretaget en vurdering af forholdet til Den Europæiske Menneskerettighedskonventions artikel 8. Konklusionen var i den forbindelse, at GovCERT's behandling af data på baggrund af indgreb i meddelelseshemmeligheden ville opfylde betingelserne i artikel 8, stk. 2, i Den Europæiske Menneskerettighedskonvention om, at indgreb i retten til privatliv skal være i overensstemmelse med loven og være nødvendigt, sagligt og proportionalt. Der henvises i den forbindelse til det notat, der er vedlagt besvarelsen af spørgsmål 2.

En tilsvarende vurdering er foretaget i forhold til lovforslaget, der på samme vis som GovCERT-loven vurderes at opfylde betingelserne i artikel 8, stk. 2, i Den Europæiske Menneskerettighedskonvention.

ad c) Lovforslaget sikrer, at Center for Cybersikkerhed fortsat er underlagt restriktive opbevarings- og sletningsregler, der gælder for alle typer af data.

Da de mest avancerede cyberangreb ofte først opdages et stykke tid efter, at de er påbegyndt, er det af væsentlig betydning for centerets evne til at opdage og imødegå cyberangreb, at data kan opbevares i en længere periode end i dag. Det vil give bedre muligheder for at rekonstruere et angreb, når det opdages – og f.eks. finde ud af, hvilke data hackerne er sluppet afsted med.

I den forbindelse er det vigtigt at kunne foretage år-til-år-sammenligning af internetaktiviteten for at opdage cyberangreb. Ved vurdering af det, der f.eks. umiddelbart vil kunne ligne

en afvigelse fra normalbilledet i januar, vil der således kunne foretages en langt mere kvalificeret vurdering, hvis der er mulighed for at sammenligne med aktiviteterne i januar året før. Derfor foreslås det, at data, der knytter sig til en sikkerhedshændelse, højst kan opbevares i tre år ligesom i dag, og at data, der ikke knytter sig til en sikkerhedshændelse, højst kan opbevares i 13 måneder. For så vidt angår pakke- og trafikdata, der ikke knytter sig til en sikkerhedshændelse, er det i dag sådan, at pakkedata højst kan opbevares i 14 dage, og at trafikdata højst kan opbevares i 12 måneder.

Det skal understreges, at danske myndigheder og virksomheder, der modtager sikkerhedsvarslinger fra netsikkerhedstjenesten, efter omstændighederne vil være underlagt persondatalovens behandlingsregler, såfremt en sikkerhedsvarsling indeholder personoplysninger.

Det indebærer, at modtagerne skal sikre, at der ikke er mulighed for at identificere fysiske personer i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil personoplysningerne behandles.

Som efter gældende ret fastsætter lovforslaget (§ 17) som nævnt maksimale opbevaringsperioder for data. Center for Cybersikkerheds netsikkerhedstjeneste vil imidlertid efter lovforslaget fortsat være forpligtet til at slette data, når formålet med behandlingen er opfyldt, hvis dette sker før den maksimale opbevaringsperiodes udløb.

Samtidig vil lovforslagets generelle princip om, at indsamlede personoplysninger ikke må opbevares på en måde, der giver mulighed for at identificere den pågældende person i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles, også finde anvendelse på personoplysninger, der behandles af netsikkerhedstjenesten (§ 14).

De foreslåede opbevaringsperioder repræsenterer således en rimelig balance mellem hensynet til beskyttelsen mod cyberangreb og hensynet til retssikkerheden og den personlige frihed.

Med venlig hilsen

Nicolai Wammen