FOLKETINGSTIDENDE B

FOLKETINGET

Til lovforslag nr. **L 192** Folketinget 2013-14

Betænkning afgivet af Forsvarsudvalget den 2. juni 2014

Betænkning

over

Forslag til lov om Center for Cybersikkerhed

[af forsvarsministeren (Nicolai Wammen)]

1. Ændringsforslag med bemærkninger

Enhedslistens medlemmer af udvalget har stillet 11 ændringsforslag til lovforslaget.

2. Udvalgsarbejdet

Lovforslaget blev fremsat den 2. maj 2014 og var til 1. behandling den 9. maj 2014. Lovforslaget blev efter 1. behandling henvist til behandling i Forsvarsudvalget.

Møder

Udvalget har behandlet lovforslaget i 3 møder.

Høring

Et udkast til lovforslaget har inden fremsættelsen været sendt i høring, og forsvarsministeren sendte den 4. februar 2014 dette udkast til udvalget, jf. FOU alm. del – bilag 61. Den 2. maj 2014 sendte forsvarsministeren de indkomne høringssvar og et notat herom til udvalget.

Retsudvalget afholdt den 8. maj 2014 en offentlig høring om lovforslaget, hvor Forsvarsudvalget deltog.

Samråd

Udvalget har stillet 1 spørgsmål til forsvarsministeren til mundtlig besvarelse, som denne har besvaret i et åbent samråd med udvalget den 23. maj 2014. Ministeren har efterfølgende sendt udvalget det talepapir, der dannede grundlag for ministerens besvarelse af spørgsmålet.

Spørgsmål

Udvalget har stillet 13 spørgsmål til forsvarsministeren til skriftlig besvarelse, som denne har besvaret. 2 af udvalgets spørgsmål og ministerens svar herpå er optrykt som bilag 2 til betænkningen.

3. Udtalelse fra forsvarsministeren

Forsvarsministeren har over for udvalget oplyst følgende:

»1. Begrebet »sikkerhedshændelse« er et centralt element i forslaget til lov om Center for Cybersikkerhed. Det følger således af lovforslaget, at Center for Cybersikkerhed kun må foretage analyse af data, der stammer fra de tilsluttede civile myndigheder og virksomheder, hvis der er tale om en sikkerhedshændelse. Endvidere må alene data, der er knyttet til en sikkerhedshændelse, videregives efter lovens særlige videregivelsesbestemmelse, ligesom der gælder særlige regler for sletning af data, der er knyttet til en sikkerhedshændelse.

Når ordet »cyberangreb« anvendes i bemærkningerne til lovforslaget, sker dette i samme betydning som det mere tekniske begreb »sikkerhedshændelse«, der anvendes i lovteksten. Sagt med andre ord er en sikkerhedshændelse et cyberangreb eller en trussel herom.

Center for Cybersikkerhed indsamler i dag primært data ved hjælp af elektroniske alarmenheder, som er opsat hos de frivilligt tilsluttede myndigheder og virksomheder, hvor de monitorerer ind- og udgående internetkommunikation.

Monitoreringen giver et normalbillede af internetkommunikationen og dermed også det overblik, der er nødvendigt for at opdage afvigelser. Cyberangreb (sikkerhedshændelser) vil typisk optræde som afvigelser fra normalbilledet og udløse en alarm hos centerets netsikkerhedstjeneste.

Netsikkerhedstjenesten foretager således allerede i dag en automatiseret (altså maskinel) løbende monitorering af internettrafikken for at se, om den indeholder trusler mod itsikkerheden. Det sker faktisk mange, mange tusinde gange om dagen, at der udløses en alarm. Det er imidlertid i gennemsnit ganske få gange i døgnet, at en alarm har en så alvorlig karakter, at den fører til, at en analytiker i centeret foretager en nærmere analyse, fordi der er en begrundet mistanke om en sikkerhedshændelse, og fordi analysen er nødvendig for afklaring af forhold vedrørende hændelsen. Der skal således foreligge konkrete indikationer på et cyberangreb eller en trussel herom, før der kan foretages en analyse af data.

Analysen har alene til formål at klarlægge konkrete sikkerhedshændelsers karakter, og netsikkerhedstjenestens interesse er derfor kun rettet mod tekniske oplysninger om sikkerhedshændelserne, f.eks. analyse af en virus i en fil, der

er vedhæftet en e-mail, og ikke mod selve indholdet af kommunikationen, herunder personoplysninger.

Når en analyse er gennemført, logges den, og Tilsynet med Efterretningstjenesterne vil kunne kontrollere, at betingelserne for analysen i det enkelte tilfælde har været opfyldt. Derudover fører centerets ledelse og centerets jurister løbende kontrol med, at analyserne foretages i overensstemmelse med reglerne.

Tilsynets årlige redegørelse skal indeholde oplysninger om antallet af sager med relation til sikkerhedshændelser, der er behandlet i centeret. Den årlige redegørelse skal herudover indeholde en anonymiseret beskrivelse af et eller flere konkrete cyberangreb, og der skal være en statistik over, hvor mange gange analytikere fra centeret har foretaget analyse af data.

Hvad der skal forstås ved en sikkerhedshændelse, er nærmere uddybet og illustreret nedenfor i pkt. 2-5.

2. I lovforslaget er en sikkerhedshændelse defineret således:

§ 2. I denne lov forstås ved:

1) Sikkerhedshændelse: En hændelse, der negativt påvirker eller vurderes at ville kunne påvirke tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale tjenester.

Denne definition svarer til definitionen i den gældende GovCERT-lov (lov nr. 596 af 14. juni 2011), der blev enstemmigt vedtaget af Folketinget, og denne afgrænsning af begrebet sikkerhedshændelse har dermed dannet grundlag for netsikkerhedstjenestens arbejde i knap 3 år.

Det fremgår således af bemærkningerne til lovforslagets § 2, stk. nr. 1, at definitionen af sikkerhedshændelse er en videreførsel af definitionen fra GovCERT-lovens § 3, nr. 3, med en sproglig præcisering af, 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.

Definitionen indebærer, at enhver unormal situation, der potentielt kan kompromittere informationssystemer, digitale netværk, digitale tjenester eller andre elektroniske systemer eller data, der lagres, processeres eller transmitteres af disse systemer, vil være at betragte som en sikkerhedshændelse.

Desuden præciseres det, at begrebet omfatter data, informationssystemer, digitale netværk og digitale tjenester, således at det udtrykkeligt fremgår, at også hændelser, som rammer lukkede netværk (netværk, der ikke er forbundet til internettet), kan have karakter af sikkerhedshændelser.

Et eksempel på en sikkerhedshændelse, der negativt påvirker tilgængeligheden af en digital tjeneste, er et overbelastningsangreb (denial-of-service angreb), hvor f.eks. en hjemmeside rammes af et stort antal forespørgsler, så brugere ikke kan få adgang til hjemmesiden. En sikkerhedshændelse, der negativt påvirker integriteten af såvel data som et informationssystem, kan eksempelvis være indtrængen i en database, hvor oplysninger ændres uden databaseejerens vidende. En sikkerhedshændelse, der negativt påvirker fortroligheden af et informationssystem, kan være en såkaldt »trojansk hest«, hvor der installeres et program på en myndigheds informationssystem, som muliggør uautoriseret kopiering af data fra myndigheden.

3. I et spørgsmål fra Forsvarsudvalget blev forsvarsministeren anmodet om at yde teknisk bistand til et ændringsforslag, således at definitionen af sikkerhedshændelser svarer til Beredskabsstyrelsens definition.

Besvarelsen af spørgsmålet lyder således:

»Et forslag til ændring af definitionen af sikkerhedshændelse som anført i spørgsmålet vil f.eks. kunne affattes således:

»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 Risiko-billede 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 Cyber-sikkerhed 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 mal-

ware, 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.«

4. På Retsudvalgets høring den 8. maj 2014 om lovforslaget foreslog DANSK IT følgende definition af en sikkerhedshændelse:

»Cyberangreb (sikkerhedshændelsen) er elektroniske angreb rettet mod informations- og kommunikationsteknologi (IKT) herunder computere, servere, netværk, tjenester, som er forbundet direkte eller indirekte til Internettet, med den hensigt at skade eller ødelægge IKT, tilegne sig kontrol over styringen af IKT eller uretmæssigt at få adgang til data lagret på IKT, med det formål at underminere tilgængeligheden, integriteten og tilliden til det ramte eller tilsigtet IKT og/eller at tilegne/forvanske/ødelægge sensitive data.«

Som det fremgår, svarer første del af DANSK IT's forslag, dvs. indtil ordene »… med det formål at underminere …«, til ovennævnte ændringsforslag, og denne del af definitionen er dermed kommenteret ovenfor under pkt. 3.

Med hensyn til anden del af Dansk-It's definition, dvs. »… med det formål at underminere tilgængeligheden, integriteten og tilliden til det ramte eller tilsigtet IKT og/eller at tilegne/forvanske/ødelægge sensitive data«, svarer denne del af definitionen reelt (med elementer fra lovforslaget) til første del af definitionen, og dermed er første og anden del sammenfaldende. Sagt med andre ord, så siges det samme to gange.

5. Om antallet af sikkerhedshændelser kan oplyses, at netsikkerhedstjenesten (GovCERT) siden 2010 har registreret godt 1.100 sikkerhedshændelser. Heraf vurderes en fjerdedel at være alvorlige. Det er således – som nævnt ovenfor i pkt. 1 – i gennemsnit kun ganske få gange om dagen, at en alarm fører til en nærmere analyse af data.

De registrerede hændelser omfatter overbelastningsangreb og spor efter APT-angreb, fund af sårbarheder, tegn på infektion med vira og fund af forskellige typer malware (crimeware, botnet-malware mv.).

I perioden september 2011 til udgangen af marts 2014 har netsikkerhedstjenesten (Gov-CERT) udsendt godt 100 varslinger til GovCERT's kundekreds. Tallet omfatter generelle varslinger til en bredere kreds og specifikke varslinger til enkeltkunder på baggrund af en alarm.«

4. Indstillinger og politiske bemærkninger

Et *flertal* i udvalget (udvalget med undtagelse af EL og LA) indstiller lovforslaget til *vedtagelse uændret.* Flertallet stemmer imod de stillede ændringsforslag.

Socialistisk Folkepartis medlemmer af udvalget bemærker, at forsvar imod cyberangreb vil være et væsentligt element i fremtidens forsvarspolitik. SF støtter derfor lovforslaget. Placeringen af Center for Cybersikkerhed under Forsvarets Efterretningstjeneste vil give et mere effektivt system, men SF er helt opmærksom på, at der opstår nogle retssikkerhedsmæssige udfordringer, som må tages alvorligt. SF finder det tilfredsstillende, at der med loven etableres et mere effektivt tilsyn og øget transparens i forhold til centerets virksomhed. Det har været fremført, at begrebet »sikkerhedshændelse« er defineret for løst, men SF skal her henvise til det notat, som er optrykt som en udtalelse fra forsvarsministeren i betænkningen, og som præciserer betydningen. SF vil nøje følge centerets aktiviteter og lægger vægt på den evaluering, der skal gennemføres efter 3 år.

Et *mindretal* i udvalget (EL) indstiller lovforslaget til *vedtagelse* med de stillede ændringsforslag. Såfremt de stillede ændringsforslag ikke vedtages, indstiller mindretallet lovforslaget til *forkastelse* ved 3. behandling.

Enhedslisten kan ikke støtte lovforslaget, som regeringen har fremsat det. Til gengæld er Enhedslisten enig i behovet for et center for cybersikkerhed og en effektiv beskyttelse mod hackerangreb. Datainfrastruktur er ekstremt vigtig for vores samfund, så der skal være en beskyttelse. Men måden, hvorpå vi beskytter os mod cyberangreb, skal tage hensyn til de grundlæggende rettigheder, vi har som borgere i et demokrati. Regeringens lovforslag udsætter danske borgeres personfølsomme data for risiko for misbrug, sådan som det er fremgået på Retsudvalgets høring om lovforslaget i maj 2014.

Et stort problem udgør centerets placering under Forsvarets Efterretningstjeneste, som betyder, at man blander civile og militære opgaver sammen. Regeringen ønsker at placere centeret under den myndighed i Danmark, som vi har allermindst indsigt i og kontrol med, og som samtidig har de videste beføjelser til at undlade at overholde den basale lovgivning, som alle andre myndigheder skal. Det udvider FE's mulighed for at behandle oplysninger om danskere. De må bruges i FE's øvrige arbejde og også i et vist omfang udveksles med samarbejdspartnere i andre lande.

Lovforslaget rummer desuden problemer i forhold til centerets adgang til at bryde kryptering uden retskendelse, meget lange opbevaringstider, videregivelse af oplysninger til tredjepart og en for løs definition af, hvad der udgør en sikkerhedshændelse.

Lovforslaget kan dog justeres, så disse problemer afhjælpes. Enhedslisten ønsker som sagt et center for cybersikkerhed og et effektivt værn mod cyberangreb – et værn, der vel at mærke ikke krænker grundlæggende rettigheder og kompromitterer retssikkerheden. På den baggrund har Enhedslisten stillet en række ændringsforslag til lovforslaget. Såfremt ændringsforslagene vedtages, vil Enhedslisten kunne støtte det samlede lovforslag.

Et *andet mindretal* i udvalget (LA) vil redegøre for sin indstilling til lovforslaget og de stillede ændringsforslag ved 2. behandling.

Sambandsflokkurin og Javnaðarflokkurin var på tidspunktet for betænkningens afgivelse ikke repræsenteret med medlemmer i udvalget og havde dermed ikke adgang til at komme med indstillinger eller politiske udtalelser i betænkningen.

En oversigt over Folketingets sammensætning er optrykt i betænkningen.

5. Ændringsforslag med bemærkninger

Ændringsforslag

Af et *mindretal* (EL):

Til § 2

1) *Nr. 1* affattes således:

»1) *Sikkerhedshændelse:* Elektroniske angreb rettet mod informations- og kommunikationsteknologi, herunder computere, servere, netværk og tjenester, 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.«

[Ændret definition af sikkerhedshændelse]

Til § 10

2) I *nr. 2-6* ændres ordet »nødvendig« til: »strengt nødvendig«.

[Skærpelse af nødvendighedsbegrebet]

Til § 11

3) I *stk. 2, nr. 3* og *4,* ændres ordet »nødvendig« til: »strengt nødvendig«.

[Skærpelse af nødvendighedsbegrebet]

Til § 12

4) I *stk. 1* ændres ordet »nødvendigt«, til: »strengt nødvendigt« og i *stk. 2, nr. 3* og *4,* ændres ordet »nødvendig« til: »strengt nødvendig«.

[Skærpelse af nødvendighedsbegrebet]

Til § 14

5) Ordet »nødvendigt« ændres til: »strengt nødvendigt«.

[Skærpelse af nødvendighedsbegrebet]

Til § 15

6) Ordet »nødvendigt« ændres til: »strengt nødvendigt«.

[Skærpelse af nødvendighedsbegrebet]

7) Efter stk. 1 indsættes som nye stykker:

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

Stk. 3. Center for Cybersikkerhed må ikke uden forudgående retskendelse foretage afkryptering i forbindelse med analyse af data efter stk. 1.«

[Logningspligt og forbud mod afkryptering]

Til § 16

8) I *nr. 2* ændres ordet »nødvendigt« til: »strengt nødvendigt«.

[Skærpelse af nødvendighedsbegrebet]

9) I *nr. 2* indsættes efter 1. pkt. som nyt punktum:

»Trafikdata må ikke videregives til andre efterretningstjenester.«

[Forbud mod udlevering af trafikdata til andre efterretningstjenester]

10) 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.«

[Forbud mod, at data kan tilgå andre dele af Forsvarets Efterretningstjeneste]

Til § 17

11) *Stk. 2, nr. 2,* affattes således:

»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.«

[Krav til opbevaringstid for pakkedata og trafikdata]

Bemærkninger

Til nr. 1

Ændringsforslaget indebærer, at begrebet sikkerhedshændelse 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.

Til nr. 2-6 og 8

Ændringsforslagene betyder, at det nødvendighedsbegreb, der anvendes i loven, skærpes til, at der skal være tale om en streng nødvendighed.

Til nr. 7

Ændringsforslaget betyder, at Center for Cybersikkerhed vil blive pålagt logningspligt i selve lovteksten, og samtidig skærpes bestemmelsen om afkryptering, således at Center for Cybersikkerhed ikke uden forudgående retskendelse må foretage afkryptering i forbindelse med analyse af data.

Til nr. 9

Ændringsforslaget betyder, at Center for Cybersikkerhed får forbud mod at udlevere data til andre efterretningstjenester.

Til nr. 10

Ændringsforslaget betyder, at Center for Cybersikkerhed får forbud mod at udlevere data til andre dele af Forsvarets Efterretningstjeneste.

Til nr. 11

Ændringsforslaget skærper reglerne om opbevaringstid for data, der ikke knytter sig til en sikkerhedshændelse, således at trafikdata højst må opbevares i 12 måneder og pakkedata højst må opbevares i 14 dage.

Annette Lind (S) nfmd. *Bjarne Laustsen (S) Morten Bødskov (S) John Dyrby Paulsen (S) Ole Hækkerup (S)*

Trine Bramsen (S) Zenia Stampe (RV) Nadeem Farooq (RV) Lone Loklindt (RV) Holger K. Nielsen (SF) Trine Mach (SF)

Nikolaj Villumsen (EL) Jørgen Arbo-Bæhr (EL) Sara Olsvig (IA) Doris Jakobsen (SIU) Jakob Engel-Schmidt (V)

Jakob Ellemann-Jensen (V) Peter Juel Jensen (V) Karsten Lauritzen (V) Kristian Pihl Lorentzen (V)

Karsten Nonbo (V) fmd. *Troels Lund Poulsen (V) Hans Christian Thoning (V) Marie Krarup (DF) Martin Henriksen (DF)*

Søren Espersen (DF) Hans Kristian Skibby (DF) Leif Mikkelsen (LA) Lene Espersen (KF)

Sambandsflokkurin og Javnaðarflokkurin havde ikke medlemmer i udvalget.

Venstre, Danmarks Liberale Parti (V)	47	Det Konservative Folkeparti (KF)	8
Socialdemokratiet (S)	47	Inuit Ataqatigiit (IA)	1
Dansk Folkeparti (DF)	22	Siumut (SIU)	1
Radikale Venstre (RV)	17	Sambandsflokkurin (SP)	1
Socialistisk Folkeparti (SF)	12	Javnaðarflokkurin (JF)	1
Enhedslisten (EL)	12	Uden for folketingsgrupperne (UFG)	1
Liberal Alliance (LA)	9		

Bilag 1

Oversigt over bilag vedrørende L 192

Bilagsnr.	Titel
1	Høringssvar og høringsnotat, fra forsvarsministeren
2	Præsentationer vist under Retsudvalgets ekspertmøde 8/4-14 om lovforslaget
3	Tidsplan for udvalgets behandling af lovforslaget
4	1. udkast til betænkning
5	Ændret tidspunkt for betænkningsafgivelse
6	Udtalelse fra forsvarsministeren

Oversigt over spørgsmål og svar vedrørende L 192

Spm.nr.	Titel
1	Spm. om, i hvilke situationer ministeren kunne forestille sig, at Center for Cybersikkerhed vil benytte sig af lovens § 21, stk. 3, til forsvarsministeren, og ministerens svar herpå
2	Spm. om, hvordan den seneste dom fra EU-Domstolen med hensyn til logningsdirektivet påvirker lovforslaget, til forsvarsministeren, og ministerens svar herpå
3	Spm. om teknisk bistand til udarbejdelse af ændringsforslag m.v., til forsvarsministeren, og ministerens svar herpå
4	Spm., om danske virksomheder ikke er i fare for industrispionage på baggrund af udlevering af oplysninger fra Center for Cybersikkerhed m.v., til forsvarsministeren, og ministerens svar herpå
5	Spm. om, hvilke foranstaltninger ministeren har taget for at undgå misbrug af indsamlede oplysninger m.v., til forsvarsministeren, og ministerens svar herpå
6	Spm. om ministerens kommentar til oplæggene fra høringen i Retsudvalget 8/5-14, til forsvarsministeren, og ministerens svar herpå
7	Spm. om, hvorfor opgaven med beskyttelse mod cyberangreb i den militære efterretningstjeneste er placeret som en civil opgave, til forsvarsministeren, og ministerens svar herpå
8	Spm. om ministerens kommentar til de synspunkter om tilsynet og om, hvorvidt tilsynet er stærkt nok, som blev fremført af oplægsholderne under høringen i Retsudvalget 8/5-14, til forsvarsministeren, og ministerens svar herpå
9	MFU spm., om ministeren er indstillet på, at loven revideres efter en periode på f.eks. 2 eller 3 år, til forsvarsministeren, og ministerens svar herpå
10	MFU spm. om kommentar til oplæggene fra Retsudvalgets høring 8/5-14, til forsvarsministeren, og ministerens svar herpå
11	MFU spm. om, hvordan det sikres, at der er den nødvendige fagspecifikke ekspertise hos tilsynet til at kunne arbejde med cybersikkerhed, til forsvarsministeren, og ministerens svar herpå
12	Spm. om oversendelse af talepapir fra samrådet den 23/5-14 om samrådsspørgsmål A, til forsvarsministeren, og ministerens svar herpå

13 Spm. om teknisk bidrag til udarbejdelse af et ændringsforslag, der sikrer, at Center for Cybersikkerhed får udtrykkeligt forbud mod at udlevere trafikdata til andre efterretningstjenester, til forsvarsministeren, og ministerens svar herpå

Oversigt over samrådsspørgsmål vedrørende L 192

Samrådsspm.nr.	**Titel**
A	Samrådsspm., om statsrevisorernes beretning nr. 3/2013 fra den 9. oktober 2013 om forebyggelse af hackerangreb giver ministeren anledning til at iværksætte nye politiske tiltag i forhold til de arbejdsopgaver, som Center for Cybersikkerhed har ansvaret for, til forsvarsministeren

Bilag 2

To af udvalgets spørgsmål og forsvarsministerens svar herpå

Spørgsmålene og svarene er optrykt efter ønske fra V og KF.

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?

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 kommunikations-teknologi, 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 Risiko-billede 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 Cyber-sikkerhed 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 tilbage-holdende 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 meddelelses-hemmeligheden 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 ændringsforslaget 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 efterretningstje-

nester. 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.

Spørgsmål 11:

Hvordan sikres det, at der er den nødvendige fagspecifikke ekspertise hos tilsynet til at kunne arbejde med cybersikkerhed?

Svar:

Som led i, at Tilsynet med Efterretningstjenesterne efter lovforslaget tillige skal føre tilsyn med Center for Cybersikkerheds behandling af personoplysninger, er det aftalt med tilsynet, at tilsynet for at styrke dets kompetencer på det it-faglige område tilføres yderligere 600.000 kr. årligt til ansættelse af en it-specialist. Jeg er endvidere indstillet på at drøfte med tilsynet, om der er behov for at tilføre tilsynet yderligere ressourcer.