

Forsvarsministeriet

Sendt e-mail til fmn@fmn.dk
c.c. tbl@fmn.dk og sbu@fmn.dk

**Forsikring
& Pension**

Lov om ændring af lov om Center for Cybersikkerhed - hørings- svar - deres sagsnummer 2018/006599

Forsikring & Pension (F&P) værdsætter muligheden for at komme med bemærkninger til lovforslaget om ændring af lov om Center for Cybersikkerhed.

Der er stor opbakning fra F&P til en mere fokuseret indsats, der bidrager til at understøtte et højt informationssikkerhedsniveau i samfundet og til de overordnede tanker om, at Center for Cybersikkerhed (CFCS) får et bedre datagrundlag til forebyggelse og bekæmpelse af cyberangreb i Danmark. Særligt forslaget om mulighed for at kunne foretage forebyggende sikkerhedstekniske undersøgelser og at kunne foretage anvendelse og påvirkning af angrebsmål og angrebsinfrastruktur vil få stor betydning i det forebyggende arbejde. Det arbejde deltager forsikrings- og pensionsbranchen gerne i og støtter den ambitiøse nationale dagsorden om at beskytte samfundsvigtige funktioner og kritisk digital infrastruktur.

Forsikrings- og pensionsbranchen bruger i dag mange ressourcer på at følge cyber-risikobilledet og beskytte borgernes personoplysninger. Derfor hilser branchen det også velkomment, at det offentlige styrker Danmarks samlede robusthed i forhold til cybersikkerhed gennem aktivt og frivilligt samarbejde mellem offentlige virksomheder og private samfundsvigtige virksomheder. Det vil styrke Danmarks samlede robusthed.

F&P finder dog, at lovforslaget i sin nuværende form er alt for vidtgående. Lovforslaget giver meget vidtgående rammer for CFCS' adgang til virksomheders data uden retskendelse. Samtidig med at der åbnes for adgang til, at CFCS kan påbyde virksomheder at blive tilsluttet CFCS - hvis det har samfundsvigtig karakter - uden at der foreligger en nærmere definition af samfundsvigtig. Videre skal det bemærkes, at branchen finder det problematisk, at CFCS vil have mulighed for at tilgå ikke alene danske data uden en retskendelse men også udenlandske data. I de tilfælde, det er en finansiel koncern, vil CFCS derved få en videre adgang end tiltænkt i lovforslaget. Det er problematisk, at der ikke er taget stilling til denne udfordring, herunder om der vil være en udfordring i relation til persondataforordningen, at CFCS vil kunne tilgå andre EU borgeres persondata.

30.01.2019

Forsikring & Pension
Philip Heymans Allé 1
2900 Hellerup
Tlf.: 41 91 91 91
Fax: 41 91 91 92
fp@forsikringogpension.dk
www.forsikringogpension.dk

Henriette Günther Sørensen
Chefkonsulent
Dir. 41 91 91 74
hgs@forsikringogpension.dk

Sagsnr. GES-2019-00024
DokID 376113

Brancheorganisation
for forsikringsselskaber
og pensionskasser

Forslaget er bekymrende i forhold til borgernes grundlæggende rettigheder og frihedsrettigheder. Indgreb i borgernes grundlovsikrede rettigheder bør kun forekomme, hvis der er en væsentlig trussel, og det sker under iagttagelse af proportionalitetsprincippet. Det er F&P's vurdering, at lovforslaget i sin nuværende form ikke imødekommer ovenstående.

Sektorstrategierne

Der er allerede med de seks sektorstrategier taget hul på at igangsætte initiativer, der sikrer, understøtter og ruster samfundet mod cyberangreb. Initiativerne i sektorstrategierne igangsætter målrettede indsatser for de enkelte sektorer, ligesom CFCS har en central rolle i forhold til at sikre de rette tværgående indsatser for de seks kritiske sektorer. I delstrategien for den finansielle sektor lægges der op til, at Finansielt Sektorforum for Operationel Robusthed (FSOR) fortsat bliver et vigtig fora til at skabe overblik over operationelle risici på tværs af sektoren, sikre gennemførelse af fælles tiltag ift., at skabe robusthed overfor cyberangreb og endelig skabe rammer for samarbejde og vidensdeling. Der er også lagt op til at udvide samarbejdet med den Nordiske finansielle CERT (NFCERT), så alle større finansielle virksomheder, herunder forsikrings- og pensionselskaber bliver en del af disse fora. Det er derfor vigtigt, at disse eksisterende og velfungerende fora ikke undermineres af den nye lovgivning, men i stedet indtænkes. CFCS deltager på lige fod med de finansielle virksomheder allerede i disse fora.

Det er F&P's anbefaling, at Forsvarsministeriet bør afvente og vurdere effekten af de initiativer, der netop er igangsat, førend der gribes til en grundlæggende og vidtrækkende ændring af lovgivningen, der giver CFCS ubegrænset adgang til data fra regioner, kommuner og virksomheder, hvis dette tilbydes eller påbydes.

En indsats i den finansielle sektorstrategi går på, at viden skal udnyttes til at bekæmpe it-sikkerhedstrusler effektivt. Her vil man styrke indberetning af hændelser for at forbedre vidensgrundlaget. Det kan være en anden måde at dele data med CFCS og herigennem se på, hvordan der kan ske en hurtigere, bedre og om muligt realtime deling af data om cyberhændelser.

Retssikkerhed og proportionalitetsprincippet

Det er et grundlæggende princip i et retssamfund som Danmark, at indgreb i grundlovsikrede rettigheder – her meddelelseshemmeligheden – både er 1; nødvendigt, 2; at der er særligt tungtvejende hensyn til fx statens sikkerhed, som kan begrunde indgrebet, og 3; at der er proportionalitet mellem mål og middel (proportionalitetsprincippet).

En anden konsekvens af lovforslaget er, at indgrebet i meddelelseshemmeligheden medfører videregivelse og behandling af store mængder personoplysninger. Her bør der også foretages en afvejning af, om målet kan nås med mindre indgribende metoder end totalovervågning af alle en virksomheds data.

Der lægges op til, at CFCS kan behandle en virksomheds data uden retskendelse men efter frivillig "aftale". I særlige tilfælde kan en virksomhed også blive pålagt tilslutning, hvorefter CFCS kan få adgang til alle virksomhedens data uden retskendelse.

Det grundlæggende kriterium om, at indgrebet skal kunne bruges til at understøtte "et højt informationssikkerhedsniveau" i samfundet er for upræcist defineret i lovforslagets bemærkninger og efterlader et meget vidt skøn hos CFCS. Det bør defineres fuldstændigt klart og præcist i lovforslaget, hvad der skal til for at udløse CFCS' beføjelser.

Det er særligt vigtigt, at man overholder de grundlæggende retsprincipper i de situationer, hvor centeret har beføjelse til i § 3, stk. 4, at udpege virksomheder af særlig samfundsvigtig karakter, der skal tilsluttes netsikkerhedstjenesten. F&P opfordrer til, at det præciseres i bemærkningerne, hvad definitionen "samfundsvigtig" indebærer, og at det tydeliggøres, at proportionalitetsprincippet skal indgå i vurderingen af, hvornår det er nødvendigt at udstede påbud om tilslutning.

Lovforslaget indeholder heller ikke nogen nærmere ramme for indgrebets omfang, som sikrer, at CFCS anvender mindre indgribende midler end en totalovervågning af virksomhedens data. F&P opfordrer derfor til, at der i lovforslaget pålægges CFCS en forpligtelse til at undersøge, om målet kan nås på en mindre indgribende måde end ved at overvåge alle virksomhedens data.

F&P finder endvidere, at de rammer, der opsættes i den foreslåede § 15 for behandling af data erhvervet ved indgreb i meddelelseshemmeligheden, er alt for vide og upræcist definerede. P.t. står der blot, at manuel analyse kan foretages, når det vurderes at være "nødvendigt". Det bør klart beskrives i bemærkningerne, hvornår det er nødvendigt at foretage manuelle analyser af data.

Retsikkerheden og behandling af personoplysninger

Selvom det primære formål er overvågning af datatrafikken og ikke overvågning af enkeltpersoner, finder F&P det særdeles vidtgående, at der som led i overvågningen vil ske behandling af store mængder personoplysninger uden forudgående retskendelse og uden, at de almindelige retssikkerhedsmæssige garantier i fx retssikkerhedsloven overholdes.

Forsikrings- og pensionsbranchen er i sagens natur en branche, der lever af at behandle personoplysninger herunder mange følsomme oplysninger. En generel overvågning, som inkluderer alle data om en forsikringsvirksomheds kunder, er derfor meget vidtgående. For eksempel kan det nævnes, at et selskab som PFA har 1,2 mio. kunder.

F&P mener derfor, at CFCS ikke bør få mulighed for at kunne påbyde forsikrings- og pensionselskaber at blive tilsluttet netsikkerhedstjenesten.

Specifikke bemærkninger

Nedenfor listes en række særlige opmærksomhedspunkter og specifikke bemærkninger.

1. Frivillighed

Al anvendelse i den private sektor af netsikkerhedstjenesten bør i øvrigt ske frivilligt og med fuld gennemsigtighed for de deltagende virksomheder. Således bør den enkelte virksomhed have underretning og rapportering i alle tilfælde, hvor der foreligger mistanke om, eller er sket fuldblydet cyberangreb, mod virksomheden. Virksomheden skal ligeledes have mulighed for at tilkoble netsikkerhedstjenesten til sit eget SIEM-system, for bl.a. selv at kunne kontrollere, hvilke data

der oversendes til netsikkerhedstjenesten. Endelig skal den enkelte virksomhed kunne frakoble netsikkerhedstjenesten umiddelbart, hvis den finder tjenesten uhensigtsmæssig.

Forsikring & Pension

Sagsnr. GES-2019-00024

DokID 376113

2. Formål

Det bør være et ultimativt krav, at hverken Forsvarets Efterretningstjeneste eller Politiets Efterretningstjeneste skal kunne gøre brug af netsikkerhedstjenesten i deres efterretningsmæssige virke således forstået, at ingen af de to tjenester kan benytte netsikkerhedstjenesten til at overvåge eller på anden vis indhente oplysninger om en af dem i anden sammenhæng mistænkt virksomhed.

3. De finansielle videregivelsesregler

Hvor der sker videregivelse af data fra finansielle virksomheder, vil disse endvidere være underlagt Lov om Finansiell virksomhed kap. 9.

F&P opfordrer Forsvarsministeriet til at indhente en udtalelse fra Finanstilsynet om, hvorvidt tilsynet anser en videregivelse af oplysninger fra forsikrings- og pensionselskaber for berettiget – både i situationen, hvor tilslutning til netsikkerhedstjenesten sker på frivillig basis og i situationen, hvor tilslutning sker efter konkret påbud.

4. Reguleringen bør præciseres – i særdeleshed på nedenstående punkter:

- 4.1. Jf. § 3 stk. 5 kan Forsvarsministeren fastsætte reglerne om påbud, uden at disse er nærmere defineret
- 4.2 Jf. § 5 kan netsikkerhedstjenesten uden retskendelse behandle data fra en virksomhed, som ikke er tilsluttet (hvis det vurderes at kunne bidrage til at understøtte et højt informationsikkerhedsniveau i samfundet), uden at dette er nærmere præciseret

5. Tilsyn

Den tilhørende kontrolmyndighed bør føre periodiske tilsyn med, at sikkerhedsniveauet hos Center for Cybersikkerhed, og herunder netsikkerhedstjenesten, er på et absolut højt niveau. Et brud på sikkerheden hos Center for Cybersikkerhed vil kunne få katastrofale følger for hele samfundet, såfremt bruddet medførte uvedkommendes adgang til netsikkerhedstjenestens funktionalitet og de indhentede data.

6. Opfølgning

Ifølge kommentarerne til lovændringen skal Center for Cybersikkerhed efter tre år udarbejde en rapport om erfaringerne med den nye lovgivning til Folketinget. Henset til den alvorlige og hastige ændring i cybertruslerne, bør denne rapportering ske allerede efter første år og følges op med rapportering efter andet og tredje år. Rapporten bør være offentlig tilgængelig.

7. Det tekniske setup og performance

Der udtrykkes bekymring vedrørende CFCS' anvendte tekniske løsninger i forhold til opretholdelse eller ændring af virksomhedens sikkerhedsniveau og eventuelle påvirkning af systemernes og infrastrukturens ydeevne.

Afslutningsvist bemærkes, at F&P ikke har været på Forsvarsministeriets høringsliste. Fremadrettet bedes I være opmærksomme på dette og sørge for, at F&P er på høringslisten og modtager orienteringerne. I bedes sende til Forsikring & Pension på fp@forsikringogpension.dk.

Forsikring & Pension

Sagsnr. GES-2019-00024

DokID 376113

Med venlig hilsen

Henriette Günther Sørensen