Forsvarsministeriet
fmn@fmn.dk
tbl@fmn.dk
sbu@fmn.dk

Henvisning til sagsnummer 2018/006599.

FINANS DANMARK

Styrkelse af Center for Cybersikkerheds mulighed for at forsvare Danmark samtidig med, at virksomhedernes retssikkerhed sikres

Høringssvar

4. februar 2019

Dok. nr. FIDA-151247800-646019-v1
Kontakt Mette Stürup

Resumé

Danmark er et af verdens mest digitaliserede lande. Det gør os så mere sårbare over for digitale angreb. Det er væsentligt at sikre, at der er adgang til samfundskritiske tjenester som strøm, internet og finansielle tjenester. Finans Danmark mener, at der er behov for at styrke Danmarks cybersikkerhed. Der er en reel risiko for cyberangreb og for at blive hacket.

Et led i dette er, at Center for Cybersikkerhed har de rette værktøjer til at bekæmpe det stigende antal cyberangreb med. Vi støtter derfor lovforslagets intentioner. Men vi finder de brede og uprøcise hjemmeler betænkelige. Herunder giver det især anledning til bekymring, at er mulighed for at der skal gives adgang til alle virksomheders trafik uden retskendelse. Når dette så kombineres med muligheden for at pålægge en virksomhed at tilslutte sig centerets sensornetværk, kan det blive problematisk. Vi foreslår, at tilslutning sker ad frivillighedens vej og i fælles dialog.

Endelig finder vi det væsentligt, at der sker en øget videndeling, og vi opfordrer til, at der sker en endnu tættere dialog på operativ dialog med især de samfundskritiske sektorer. Vi ser gerne denne videndelingsforpligtigelse stærkere understreget i lovforslaget.

Finans Danmarks bemærkninger til lovforslag om ændring af Lov om Center for Cybersikkerhed

Høringssvar

4. februar 2019
Dok. nr. FIDA-151247800-646019-v1

Generelle bemærkninger

Danmark er et af verdens mest digitaliserede lande. Det gør os så mere sårbare over for digitale angreb. Det er væsentligt at sikre, at der er adgang til samfundskritiske tjenester som strøm, internet og finansielle tjenester. Finans Danmark mener, at der er behov for at styrke Danmarks cybersikkerhed. Der er en reel risiko for cyberangreb og for at blive hacket.

Et led i dette er, at Center for Cybersikkerhed har et tilstrækkeligt overblik i forhold til aktuelle trusler og de rette værktøjer til at bekæmpe det stigende antal cyberangreb med. Vi støtter derfor generelt set lovforslagets intentioner. Imidlertid finder vi det betænkeligt, at der påtænkes udstukket vide rammer i forhold til at kunne kræve bestemte sikkerhedskomponenter installeret hos bestemte myndigheder/virksomheder.

Finans Danmark og Cybersikkerhed

Finans Danmarks og vores medlemmer er særdeles optaget af cyber- og informationssikkerhed. Det er en topprioritet for sektoren, og vi har i de seneste år taget en lang række initiativer for at forbedre cyber- og informationssikkerheden i sektoren, blandt andet med etablering af NFCERT (Nordic Financial CERT) og FSOR (Finansielt Sektorforum for Operationel Robusthed). I sidstnævnte gennemfører sektoren bl.a. en meget omfattende red team test i de kommende år baseret på TIBER-DK rammeværket.

Derudover deltager Finans Danmark og Finans Danmarks medlemmer i en række offentlige aktiviteter og samarbejder om netop cybersikkerhed. Det drejer sig om fx Det Strategiske Samarbejdsforum i regi af Center for Cybersikkerhed og regeringens advisory board for den Nationale Cyber- og informationssikkerhedsstrategi. Vi deltager også i følgende samarbejder i regi af Erhvervsministeriet: Virksomhedsrådet for IT-sikkerhed og Erhvervspartnerskabet for øget it-sikkerhed i dansk erhvervsliv.

Finans Danmark har bidraget til og er positive over for de nye sektorstrategier for styrkelse af cyberrobustheden i energi-, tele-, søfart-, finans-, transport- og sundhedssektoren, der alle blev præsenteret primo januar 2019. Vi forventer, at disse strategier vil bidrage til at skabe et robust fundament for et øget og nødvendigt

samarbejde mellem offentlige og private parter, så vi i fællesskab kan styrke cyberrobustheden i Danmark i de kommende år. Det er vigtigt, at Center for Cybersikkerhed har de fornødne beføjelser for derved at kunne løfte sit ansvar i denne forbindelse.

Specifikke kommentarer til lovforslaget:

Pålæg om tilslutning til sensornetværket

Finans Danmark finder det betænkeligt, at der påtænkes udstukket vide rammer i forhold til at kunne kræve bestemte sikkerhedskomponenter installeret hos udvalgte myndigheder/virksomheder. Dette kan i sig selv udgøre en ny sikkerhedsmæssig risiko.

Herunder kan der være grund til at bekymre sig over den brede hjemmel, der giver adgang til virksomhedernes data uden retskendelse. Når dette så kombineres med muligheden for at pålægge en virksomhed at tilslutte sig centerets sensornetværk, kan det blive problematisk. Vi foreslår, at tilslutning sker ad frivillighedens vej og i fælles dialog.

Det er ikke helt klart, hvem denne bestemmelse i loven retter sig imod, da den ikke indeholder en nærmere definition af, hvem som kan blive pålagt et påbud om tilslutning.

Lovforslaget forholder sig ikke til de komplikationer, der kan opstå, såfremt sensornetværk påvirker eksempelvis den tilsluttede virksomheds it-driftsstabilitet. Leverer Center for Cybersikkerhed 24x7x365 support, hvis problemer opstår? Hvis er skylden, hvis virksomheden pga. sensornetværket får en forhøjet nedetid af virksomhedens it-systemer?

Endvidere skal det bemærkes, at der i disse år finder en hård konkurrence sted i forhold til, hvor nye tech-virksomheder etablerer sig. Dette gælder også inden for finansiel teknologi, hvor Danmark har oplevet en positiv og markant vækst inden for fintechvirksomheder. Der er en risiko for, at lovforslagets mulighed for at pålægge virksomheder at implementere sensornettet kan få en negativ indvirkning på Danmarks muligheder for fortsat at tiltrække investorer og virksomheder.

Karakteren og placeringen af sensorerne kan også have stor betydning for virksomhederne, og derfor bør installation være med passive elementer og udelukkende ske på ydersiden hos virksomhederne. Hvis tilslutningen skal have værdi for virksomheden. Er det er væsentligt, at der altid sker notificering hos dem, der er

tilsluttet sensornetværket, når Center for Cybersikkerhed identificerer en kritisk hændelse.

Virksomhederne bør derfor selv have læseadgang og adgang til at oprette regler. Virksomhederne bør også have adgang til de logs, som dannes på Center for Cybersikkerhed's enheder. Center for Cybersikkerhed må gerne begrænse adgang til specifikke regler på sensorerne, hvis denne visen ikke kan deles af hensyn til samarbejde med andre efterretningstjenester.

Selve tilslutningen til sensornetværket gøres fremadrettet gratis, men lovforslaget forholder sig ikke til, at en tilslutning kan medføre omkostninger vedr. fx dekryptering af data, væsentlig kompleks systemarkitektur etc. Dette kan også medføre udgifter for de tilsluttede virksomheder, hvis der ikke direkte kan gives adgang til ukrypteret netværkstrafik

Samlet set mener Finans Danmark derfor, at påbud ikke bør være en del af lovforslaget.

Aktivt Cyberforsvar

Indgriben/behandling ved begrundet mistanke bør altid foretages proportionalt med risikoen, herunder skal den indgribende handling vurderes i forhold til virksomhedens samlede aktiviteter og samfundsmæssige funktion. Vi henstiller til agtpågivenhed og særligt at oplyse om alle handlinger med evt. indgriben, der indebærer eks. nedlukning af systemer/services, blokeringer af datastrømme eller sletning af data.

Vi kan ikke acceptere ændringer, der kan have en negativ forretningsmæssig konsekvens i forhold til vores services uden at have mulighed for indsigelse eller selv foretage en risikovurdering forud for sådanne handlinger. Derudover kommer, at der er en risiko for "falske positiver".

Vi finder, at berørte virksomheder har et krav på at modtage rettidig information om alvorligheden og det potentielle omfang af en vurderet sikkerhedshændelse, herunder eventuel behandling af netværket. Dels for at kunne etablere egne forsvarsforanstaltninger på det præventive, opdagende og korrigerende plan, dels for at være oplyst om eventuelle direkte og afledte forretningsmæssige risici, som virksomheden skal tage højde for i den fortsatte daglige drift.

Ved konstaterede sikkerhedshændelser, hvor netsikkerhedstjenesten beslutter at forhindre levering af disse data til virksomheden, skal sådanne beslutninger ligele-

des ske under hensyntagen/overvejelser af konsekvenser for virksomhedens fortsatte drift. Vi mener, at netsikkerhedstjenesten kan have disse beføjelser i de situationer, hvor den nationale sikkerhed er truet eller er påvirket særlig negativt, men henstiller til, at det skal foregå under ordnede forhold og i høj kvalitet i udførelsen, hvor hensynet til konsekvensen for de berørte virksomheder er i højsædet.

Behov for øget videndeling mellem offentlige myndigheder og private virksomheder

I forbindelse med lovforslaget finder vi det væsentligt, at der er fokus på en øget videndeling, og vi opfordrer til, at der sker en endnu tættere dialog på et operationelt niveau mellem de samfundskritiske sektorer, herunder mellem de kommende sektor-"CERT'er". I forbindelse med lovforslaget finder vi det væsentligt, at der er fokus på øget videndeling, og vi opfordrer til, at der sker en endnu tættere dialog på et operationelt niveau mellem de samfundskritiske sektorer, herunder mellem de kommende sektor-CERT'er. Vi ser gerne denne videndelingsforpligtigelse stærkere understreget i lovforslaget.

Pakkedata

Bestemmelsen i forhold til Center for Cybersikkerheds adgang til at videregive data, jf. § 16, stk. 2, synes at være meget bred. Det bør præciseres under hvilke forhold og til hvem?

Forholdet til lov om finansiel virksomhed

Bankerne er underlagt regler om bankhemmelighed både i Danmark men også i udlandet. Der savnes en nærmere redegørelse for, hvordan disse regler spiller sammen med, at Forsvarets Efterretningstjeneste ønsker adgang til al kommunikation i finanssektoren. Der savnes en beskrivelse (eller en lempelse) af forholdet til særlovgivningens (FIL's) fortroligheds- eller tavshedspligtsbestemmelser.

En række finansielle institutter og virksomheder behandler også data for ikke-danske kunder. Her skal man også overholde udenlandske regler og kan være underlagt udenlandske tilsynsmyndigheder. Vi efterlyser, at lovforslaget forholder sig til denne problemstillling, der formentlig også gælder for andre sektorer.

Tilslutning til Center for Cybersikkerhed kan ske ved, at man tilslutter sig ordningen, og det kan ske ved, at Center for Cybersikkerhed påbyder en virksomhed at tilslutte sig. Hvis tilslutningen sker som følge af et påbud, kan det hævdes, at enhver efterfølgende videregivelse af oplysninger fra banken til Center for Cybersikkerhed er berettiget, da den følger af lov, jfr. FIL § 117. Hvis tilslutningen sker frivilligt, kan videregivelse af oplysninger næppe ske med henvisning til FIL § 117

(berettiget videregivelse), og det kunne være ønskværdigt, at lovforslaget forholder sig FIL § 117 og muligheden for at videregive oplysninger.

De finansielle outsourcingregler

Ad § 15: Hvilke kontroller er der etableret i forhold til at sikre Center for Cybersikkerhed's adgang til virksomhedens kommunikation og data, som centret opnår gennem sensornetværket ? Kan de tilsluttede virksomheder opnå en tilstrækkelig indsigt i Forsvarets Efterretningstjeneste's kontroller, fx gennem tilsynet med Center for Cybersikkerhed? Dette er et formelt krav i Outsourcingbekendtgørelsen, som gælder for finansielle institutioner i forhold til anvendte (kritiske) underleverandører.

Forholdet til de fire essentielle europæiske garantier i forhold til GPDR

De almindelige bemærkninger indeholder en analyse af forholdet til den Europæiske Menneskerettighedskonvention (EMRK), men ikke en specifik analyse af forholdet til de fire essentielle europæiske garantier.

Fra Finans Danmarks side ser vi gerne, at lovforslaget udbygges med en analyse af forholdet til de fire essentielle europæiske garantier, som de europæiske datatilsyn har beskrevet i *"Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (WP 237)"*.

De fire essentielle europæiske garantier har følgende indhold:

1. Myndigheder i tredjelandes adgang til og brug af personoplysninger hidrørende fra EU skal ske på grundlag af klare, præcise og tilgængelige regler.
2. Myndigheder i tredjelandes adgang til og brug af personoplysninger hidrørende fra EU skal være nødvendig og proportional, der skal være balance mellem formålet (national sikkerhed) og indgrebet i de registreredes ret til beskyttelse af deres privatliv.
3. Der skal være en uafhængig og effektiv tilsynsmyndighed i tredjelandet.
4. Der skal være tilgængelige og effektive retsmidler for de registrerede i tredjelandet.

I dag påkalder de fire essentielle europæiske garantier sig især opmærksomhed, når personoplysninger om europæiske registrerede overføres fra EU til tredjelande uden for EU.

På længere sigt har EU-kommissionen imidlertid bebudet, at man vil kigge nærmere på, hvorvidt EU's medlemslande også selv overholder de fire essentielle garantier, og hvordan – i det omfang dette ikke er tilfældet – det sikres, at garantierne overholdes inden for EU's grænser.

Lovforslaget indebærer, at Center for Cybersikkerhed fremadrettet vil få mulighed for i større omfang end hidtil at indsamle personoplysninger af hensyn til national sikkerhed. I dét lys henstiller Finans Danmark til, at lovgiver forholder sig til, om forslaget i sin nuværende udformning sikrer tilstrækkelige garantier for de registrerede, når deres personoplysninger overføres til Danmark.

Specifikke bemærkninger

Er § 8 a omfattet af offentlig aktindsigt?

Med venlig hilsen

Mette Stürup

Direkte: +4527152020
Mail: ms@fida.dk