Finanstilsynet

Sendt e-mail til:
jesu@ftnet.dk
jja@ftnet.dk
Kopi til:
eu.mail@ftnet.dk

Forsikring & Pension

Input til dansk høringssvar vedr. EU kommissionens høring angående modstandsdygtighed over for cyberangreb

Finanstilsynet anmoder om input til EU kommissionens høring angående modstandsdygtighed over for cyberangreb. Finanstilsynet udarbejder et samlet dansk høringssvar til EU-kommissionen. Forsikring & Pension (F&P) værdsætter muligheden for at komme med input til et samlet dansk høringssvar til EU-kommissionen.

EU-Kommissionen lancerede den 19. december 2019 en høring angående modstandsdygtighed over for cyberangreb. Høringen søger at kortlægge behovet for at ændre i de eksisterende regler, herunder særligt Network and Information Security (NIS) direktivet samt mulig ny lovgivning vedr. 'digital operational resilience for financial services'. Høringen er en del af en større indsats i EU-regi for at håndtere en stadig stigende brug af 'Information and Communication Technology' (ICT) i den finansielle sektor og de deraf affødte sikkerhedsudfordringer.

F&P's høringssvar fokuserer på den mulige ny lovgivning vedrørende 'digital operational resilience for financial services'. Høringssvaret forholder sig ikke til eventuelle ændringer i Network and Information Security (NIS) direktivet. F&P afventer, at der kommer noget mere konkret fra EU-kommissionen ift. eventuelle ændringer i NIS-direktivet. Dette skulle angiveligt komme i Q4 2020.

Der er generelt stor opbakning fra F&P til en mere fokuseret EU-indsats, der bidrager til at øge modstandsdygtigheden over for cyberangreb i både EU og Danmark. Det arbejde deltager forsikrings- og pensionsbranchen gerne i, og vi støtter EU's dagsorden om at håndtere en stadig stigende brug af ICT i den finansielle sektor og de deraf affødte sikkerhedsudfordringer.

Cybersikkerhedsdagsorden er højt prioriteret i den danske forsikrings- og pensionsbranche. Der er tæt koordinering og videndeling i branchen, og branchen arbejder for at sikre den samlede finansielle sektor i et tæt samarbejde med National banken (gennem Finansielt Sektorforum for Operationel Robusthed, FSOR), Finanstilsynet via Decentral enhed for Cyber- og Informationssektoren for finanssektoren (DCIS) og med Center for Cybersikkerhed (CFCS). De enkelte selskaber bruger store ressourcer på at forebygge cyberhændelser, værne om borgernes personoplysninger og klæde medarbejderne godt på. Cyber- og informationssikkerhed er af meget høj prioritet i branchen.

06.02.2020

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

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

Sagsnr. GES-2020-00042
DokID 396634

Brancheorganisation
for forsikringsselskaber
og pensionskasser

F&P finder, at rammeværket i sin nuværende udformning ikke i tilstrækkelig grad giver grundlag for at vurdere behovet for ny regulering, og den værdi det giver at besvare spørgsmålene i rammeværket. Den europæiske indsats bør fokusere på, hvordan vi samlet løfter robustheden gennem videndeling og samarbejde.

Cybertruslen er et grundvilkår, og det *er* vigtigt at beskytte den finansielle sektor nationalt og på EU-plan. F&P efterspørger, at der kommer mere fokus på EU og statens opgave med at nedbringe risikoen for sektoren ved fx at etablere værn til at stoppe den kriminelle aktivitet. I stedet bliver søgelyset oftest rettet mod virksomhederne, og bliver de ramt af cyberangreb, betragtes de mere som skyldige end som ofre og er derfor forfalden til straf.

F&P er oprigtigt bekymret for, at der bare i Danmark bliver oprettet så mange organer inden for både den offentlige og private sektor, der skal forholde sig til og håndtere cybertruslen, at det vandes ud pga. silotænkning og bureaukrati. Sektoren har allerede mange forskellige organer alene på nationalt niveau, jf. tidligere er der FSOR, DCIS, CFCS og også Nordic Finansiel CERT (NFCERT) samt Digitaliseringsstyrelsen.

Her følger en række mere konkrete kommentarer til Digital operationel resilience framework

De første punkter vedr. en vurdering af værdien ved 'Digital operationel resilience framework':

- Der er allerede på nuværende tidspunkt mange gode initiativer på cyber- og informationssikkerhed både lokalt i virksomhederne, men også gennem diverse konsulenthuse og revisionsselskaber. Der er eksempelvis mange modenhedsmodeller, der søger at vurdere en virksomheds modenhed inden for cyber- og informationssikkerhed. Det er svært at se, hvordan dette europæiske framework adskiller sig, og hvad det bidrager med af nyt og som noget, der ikke allerede eksisterer og findes i forvejen.
- Forsikrings og pensionsbranchen er langt med implementering af cyber- og informationssikkerhedsforanstaltninger. De nationale risikoanalyseanalyser af henholdsvis bank- og F&P-branchen viser, at effekten på samfundet er forskellig, hvis man bliver ramt af cyberangreb. Banksektoren er præget af at være mere tidskritiske, og det er F&P-branchen ikke på samme måde. Derfor er det anbefalelsesværdigt at tage en mere risikobaseret tilgang til de europæiske indsatser, da behovet også vil være forskelligt ift., om det er pengeinstitutter eller F&P-branchen.
- Hvis man ser rammeværket i et bredere perspektiv, kan det have en berettigelse ift., at EU ad den vej får et klarere billede af sikkerhedsniveauet i den finansielle sektor i de forskellige europæiske lande. Det vil give en bedre viden til at løfte det generelle sikkerhedsniveau på tværs af EU-landene.
- Et positivt outcome er, hvis opsamlinger på cyber- og informationssikkerhedshændelser kan blive anvendt til erfaringsudveksling imellem landene, med henblik på at styrke cyberrobustheden, sammen med anbefalinger til, hvordan man kan modvirke de aktuelle cyber- og sikkerhedshændelser. Der er allerede til en vis grad i dag en orientering om aktuelle cyber- og sikkerhedshændelser i et bredere perspektiv fra EC3 Europol Cybercrime Centre, der udsender et ugentligt dashboard med det, de har observeret.

De næste punkter vedr. en mulig regulering af rammeværket:

- F&P mener for nuværende, at det er vigtigt at understøtte videndeling og samarbejde i EU. Det er helt centralt, at ny lovgivning øger værdien i arbejdet med cybersikkerhed, hvorfor ny lovgivning ikke bør hastes igennem og slet ikke på baggrund af det bestående spørgeskema (rammeværket). Finanstilsynet har også nogle spørgeskemaer, som de benytter i forbindelse med inspektioner, og her kunne spørgeskemaet eventuelt anvendes som supplement, hvis spørgsmålene ikke allerede er dækket. Men der er en stor forskel fra at lade et rammeværk være en rettesnor, som fx ISO27001, til at man er underlagt et krav om at følge det.
- Rammeværket bør tage højde for forskellighederne i den finansielle sektor, jf. både forskelle i risici og i modenhedsniveauer. En ulempe kan være, at for de mindre modne virksomheder kan tilgangen være, at hvis de blot overholder reglerne, så er det sikkerhedsmæssigt godt nok. Det vil i givet fald kræve, at barren for rammeværket sættes relativt højt for, hvad der er minimumsniveauet.
- F&P forudser, at det bliver svært at efterprøve, om virksomhederne efterlever rammeværket i dets nuværende form, og derfor er vores holdning til rammeværket også meget afhængig af, hvad konsekvensen ved et brud på efterlevelse bliver.

De sidste punkter vedr. selve formen og opbygningen af rammeværket:

- Spørgsmålene i rammeværket skal ramme bredt, hvilket de også gør. Men det betyder også, at de vil have varierende relevans afhængig af modenhedsniveauet hos dem, der besvarer spørgsmålene.
- Rammeværket er kun i test i øjeblikket, og det er også F&P's vurdering, at rammeværket ikke er tilstrækkeligt gennemarbejdet. Der er en del fejl og mange af spørgsmålene, der afdækker modenhedsniveau, er vanskelige at svare på. Derudover bør svarmulighederne bliver ændret til mindre mulighed for fritekst og mere styrede svarmuligheder således, at den der svarer på spørgeskemaet kun får en besvarelse, der indikerer "sikkerhedsniveauet". Når man svarer med fritekst, betyder det, at 'modtageren' skal udtrække besvarelsen og give deres subjektive vurdering af besvarelsen. Hvis man i stedet skal vælge mellem allerede definerede svarmuligheder, kan resultatet automatiseres meget bedre, og man får derfor et resultat man reelt kan bruge.

Med venlig hilsen

Henriette Günther Sørensen