

Finansdepartementet

Fi2024/00073

Yttrande

Stockholm 2024-03-18

Promemorian Digital operativ motståndskraft för finanssektorn

Svensk Försäkring uppskattar möjligheten att yttra sig över promemorian *Digital operativ motståndskraft för finanssektorn*.

Svensk Försäkring har inget att erinra beträffande föreslagna ändringar av befintlig reglering av försäkrings- och tjänstepensionsverksamhet som följer av genomförandet av DORA-förordningen.

Beträffande det förslag till kompletterande bestämmelser i nationell rätt i form av en ny lag har Svensk Försäkring följande kommentarer:

Svensk Försäkring tillstyrker förslaget att Sverige inte bör utnyttja möjligheterna att bestämma att finansiella entiteter ska använda DORA-förordningens mallar när de överlämnar information om en IKT-relaterad incident till behörig myndighet.

I promemorian föreslås att Finansinspektionen ska bestämma vilka finansiella entiteter som ska genomföra hotbildsstyrda penetrationstester och hur ofta testerna ska ske. Svensk Försäkring tillstyrker förslaget samt den föreslagna ansvarsfördelning mellan Finansinspektionen och Riksbanken när det gäller genomförandet av hotbildsstyrda penetrationstester och därmed sammanhängande behov av informationsutbyte mellan myndigheterna.

Enligt promemorian bedöms högst ett 20-tal svenska företag omfattas av kravet att utföra hotbildsstyrda penetrationstester, däribland något eller några enstaka försäkrings- eller tjänstepensionsföretag. Svensk Försäkring vill understryka att denna form av resurskrävande och avancerade tester endast bör omfatta företag som bedriver en verksamhet som är av särskild betydelse för den finansiella stabiliteten.

Kriterier för beslut om vilka företag som bör omfattas av hotbildstyrda penetrationstester framgår av DORA-förordningen artikel 26.8 tredje stycket, men kommer att tydliggöras i en kompletterande genomförandereglering som fastställs under 2024¹. I förslaget till kompletterande genomförandereglering så föreslås att vissa försäkringsföretag kan omfattas bland annat utifrån premievolyms och förvaltad kapital. I förslaget finns emellertid även en möjlighet för den behöriga myndigheten att besluta att företag som kan omfattas utifrån dessa kriterier undantas från kravet att genomföra hotbildsstyrda penetrationstester, om störningar i verksamheten inte kan anses utgöra en systematisk risk för det finansiella systemet.

Svensk Försäkring menar att utifrån vad som anges i DORA-förordningen artikel 26.8 tredje stycket, förslagen i kompletterande genomförandereglering samt med beaktande av DORA-förordningens proportionalitetsprincip i artikel 4, så bör Finansinspektionen besluta att försäkringsföretag eller tjänstepensionsföretag **inte** omfattas av krav på att utföra hotbildsstyrd penetrationstestning. De företag som inte utför hotbildsstyrd penetrationstestning kommer fortfarande att omfattas av kraven på testverksamhet i enlighet med DORA-förordningen artikel 24 och 25.

Svensk Försäkring



Mats Galvenius



Pär Karlsson

¹ JC 2023 72 - Draft Regulatory Technical Standards specifying elements related to threat led penetration tests