Svensk Försäkring

finansinspektionen@fi.se
malin.alpen@fi.se
linda.lofgren@fi.se

YTTRANDE
2024-11-12

TLPT-tester enligt DORA-förordningen

Enligt DORA-förordningen ska vissa företag omfattas av så kallade hotbildstyrda penetrationstester (TLPT-tester). Finansinspektionen ska fatta beslut om vilka företag som ska genomföra denna typ av test.

I samband med genomförandet av FI forum om DORA den 6 november meddelades att Fi har inlett en process för att bedöma vilka företag som omfattas. Beslut ska meddelas berörda företag under första halvåret 2025.

I samband med remissen av promemorian om Digital operativ motståndskraft för finanssektorn (Fi2024/00073) har Svensk Försäkring framhållit att endast företag som bedriver en verksamhet som är av särskild betydelse för den finansiella stabiliteteten bör omfattas av denna form av tester. Företag som inte utför TLPT-tester omfattas alltjämt av kraven på testverksamhet i enlighet med DORA-förordningen artikel 24 och 25.

Kriterier för beslut om vilka företag som bör omfattas av hotbildstyrda penetrationstester framgår av DORA-förordningen artikel 26.8 tredje stycket och den kompletterande genomföranderegleringen som nu är föreslagen[1]. I förslaget till genomföranderegleringen så framgår att försäkrings- eller tjänstepensionsföretag kan omfattas utifrån vissa kriterier såsom premievolym och förvaltat kapital. Det finns emellertid en möjlighet för den behöriga myndigheten att både undanta och inkludera företag för TLPT-tester oavsett om verksamheten uppfyller vissa kriterier. En anledning till att undanta ett företag är om störningar i verksamheten inte kan anses utgöra en systematisk risk för det finansiella systemet.

Vid beslut om vilka företag som omfattas av krav på TLPT-tester bör särskilt angivna skäl i DORA-förordningen samt i den kompletterande genomföranderegleringen beaktas.

---

[1] Draft Regulatory Technical Standards specifying elements related to threat led penetration tests under Article 26(11) of Regulation (EU) 2022/2554

Av DORA-förordningen skäl 56 framgår:

" […] hotbildsstyrd penetrationstestning. Sådana avancerade tester bör krävas endast av finansiella entiteter som är tillräckligt mogna ur ett IKT-perspektiv för att utföra dem på ett rimligt sätt. Den testning av den digitala operativa motståndskraften som krävs enligt denna förordning bör därför vara mer krävande för de finansiella entiteterna som uppfyller de krav som fastställs i denna förordning (t.ex. stora, systematiska och IKT-mogna kreditinstitut, fondbörser, värdepapperscentraler och centrala motparter) än för andra finansiella entiteter. Samtidigt bör testning av digital operativ motståndskraft genom hotbildsstyrd penetrationstestning vara mer relevant för finansiella entiteter som är verksamma inom delsektorer för *centrala finansiella tjänster och som har en central betydelse för systemet* (t.ex. betalningar, bankverksamhet, och clearing och avveckling) och mindre relevant för andra delsektorer (t.ex. kapitalförvaltare och kreditvärderingsinstitut)."

Det bör särskilt noteras att försäkrings- och tjänstepensionsföretag inte nämns bland de exempel på verksamhetsutövare som är relevanta vid hotbildsstyrd penetrationstestning.

Enligt skäl 3 i förslaget till kompletterande genomföranderegler ska myndigheten beakta följande vid beslut om vilka företag som omfattas:

" Considering the complexity of the TLPT and the risks relating to it, the test should be performed only by financial entities for which it is justified. Hence, authorities responsible for TLPT matters (TLPT authorities, either at national or Union level) should exclude from the scope of TLPT those financial entities operating in core financial services subsectors for which a TLPT is not justified. It means that credit institutions, payment and electronic money institutions, central security depositories, central counterparties, trading venues, insurance and reinsurance undertakings, *even though when meeting the quantitative criteria identified in this Regulation, could be opted out of the TLPT scope in light of an overall assessment of their ICT risk profile and maturity, impact on the financial sector and related financial stability concerns*."

Erfarenheter från företag som har genomfört TIBER-SE visar att ett TLPT-test är mycket komplext, resurskrävande och att kostnader för upphandlade tjänster, avgifter och egen personal uppgår till i storleksordningen 5–10 miljoner SEK.

Svensk Försäkring

Utifrån vad som anges i skälen enligt ovan, DORA-förordningen artikel 26.8 tredje stycket, förslaget till kompletterande genomföranderegelering samt med beaktande av DORA-förordningens proportionalitetsprincip, så är det Svensk Försäkrings uppfattning att försäkrings- och tjänstepensionsföretag inte bör omfattas av krav på att genomföra TLPT-tester.

SVENSK FÖRSÄKRING

Mats Galvenius
Vice VD

Pär Karlsson
Senior rådgivare