Datum för beslut: 2024-04-10

Diarienummer: V-2024-0043

Till: Regeringskansliet (Finansdepartementet)

Kungl. Tekniska högskolans synpunkter på remiss av promemorian Digital operativ motståndskraft för finanssektorn (Fi2024/00073)

Sammanfattning

Rekommendationer:

Tydliggör vad som gäller för digital infrastruktur kopplat till kontanter.

Förtydliga definitionen av ledningsorgan för att undvika feltolkningar.

Synkronisera DORA med befintliga regelverk, med en övergångsperiod där det behövs.

Det bör övervägas om krav på hotbildsstyrda penetrationstester vart tredje år (om inte den behöriga myndigheten begär något annat) är tillräckligt med hänsyn till snabbt skiftande hotbilder och hastigheten med vilken moderna tekniklösningar (IKT-tjänster) utvecklas och omsätts.

Synpunkter

Förslagen i promemorian bedöms stärka den digitala operativa motståndskraften för finanssektorn, men detaljsynpunkterna nedan bör beaktas för att uppnå syftet utan oavsiktliga konsekvenser eller orimliga bördor för finanssektorn.

Förtydligande av begreppet betaltjänster

Förslaget visar otydlighet vad gäller vad som omfattas av betaltjänster (kapitel 2, del 10; samt kapitel 20, del 10) då det inte finns några skrivningar om reglering av kontanter som betaltjänst trots att infrastrukturen för kontanter bygger på digitala system kopplat till hantering (som t ex kassasystem, uttagsautomater, transportsystem, konton, mm.). Detta är en brist som bör förtydligas.

Förtydligande av begreppet ledningsorgan

DORA-förordningen använder begreppet *ledningsorgan* för finansiella entiteter. Det har i den svenska finansbranschen tidigare uttryckts oro över att definitionen i förordningen (nr 30) inte är otvetydig, framförallt med hänsyn till skrivningen om ”eller motsvarande personer som i praktiken leder entiteten eller har nyckelfunktioner i enlighet med relevant unionsrätt eller nationell rätt”.

Utredningen är tydligare än förordningen när den skriver att ”Ingripanden bör därför kunna ske mot den som ingår i styrelsen för en finansiell entitet eller är dess verkställande direktör, eller ersättare för någon av dem” (s. 89).

Här kvarstår dock en viss osäkerhet kring begreppet *ersättare*. Det går att göra olika tolkningar av detta. En tolkning är att exempelvis att det bara omfattar den som vid en given tidpunkt faktiskt fungerar som vd; alltså antingen är ordinarie eller är tillförordnad/tjänsteförrättande vd i ordinarie vd:s frånvaro. En annan tolkning är att det även omfattar den som under normala omständigheter biträder eller under särskilda omständigheter är beredd att ersätta vd; exempelvis en vice/biträdande/ställföreträdande vd.

Det vore önskvärt om propositionen ännu tydligare kunde uttrycka exakt vem som kan omfattas av begreppet ledningsorgan och under vilka omständigheter.

Avveckling av överlappande regelverk

Det finns många regelverk som på olika sätt styr informations- och cybersäkerhet i den finansiella sektorn. DORA är *lex specialis* i förhållande till NIS2 (förordningens skäl 16); DORA har företräde (ss. 56–57 i utredningen). Utredningen gör också bedömningen att DORA-förordningen inte föranleder några ändringar i nationell lagstiftning inom områdena allmän säkerhet, försvar eller nationell säkerhet (s. 65).

Detta är dock knappast en uttömmande analys av alla beröringspunkter med befintliga regelverk. Det är troligt att det finns andra överlapp, kanske inte med lag eller förordning, men definitivt med myndighetsföreskrifter som exempelvis Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker (FFFS 2014:4) eller Riksbankens föreskrifter och allmänna råd om företag av särskild betydelse för genomförandet av betalningar under fredstida krissituationer och vid höjd beredskap (RBFS 2023:3).

För att göra regelverket tydligt, överskådligt och lätt att följa bör myndigheterna skyndsamt se över och när DORA träder i kraft avveckla sådana föreskrifter som har överlapp med DORA. Annars löper Sverige risken att få otydliga regler och onödigt höga implementationskostnader.

Hotbildsstyrda penetrationstester

Att planera och genomföra hotbildsstyrda penetrationstester är resurskrävande och tar tid. Ur det perspektivet är treårscyklerna i DORA rimliga. Samtidigt förändras moderna IKT-miljöer löpande och i snabb takt. Ur det perspektivet framstår tre år som mycket lång tid och resultaten riskerar att snabbt bli föråldrade.

Mot bakgrund av dessa två perspektiv bör kraven på hotbildsstyrda penetrationstester möjligen kompletteras med krav som skapar incitament för finansiella entiteter att nyttja IKT-lösningar (-tjänster) som löpande (vidare-) utvecklas, drifthålls och förvaltas med hänsyn till snabbt förändrade hotbilder och med hjälp av kunskap från forskningens framkant om hur moderna säkra IKT-lösningar (-tjänster) tas fram och vidmakthålls.

Remissvaret har utarbetats inom skolan för industriell teknik och management och därutöver beretts med Cybercampus Sverige. I den slutliga beredningen har föreståndare David Olgart och adjungerad professor Ulrik Franke deltagit.

Stockholm 2024-04-10

Anders Söderholm
Rektor