Informationssäkerhet

Svar på regeringsuppdrag

PENSIONS
MYNDIGHETEN

Innehåll

Sammanfattning

Det övergripande målet för Pensionsmyndighetens säkerhetsarbete är att ha en väl avvägd och riskbaserad säkerhetsnivå, och att värna om pensionärernas förmåner och integritet, medarbetarnas trygghet samt skydda myndighetens tillgångar.

Pensionsmyndighetens säkerhetsarbete styrs genom ett ledningssystem som baseras på de internationella standarderna ISO/IEC 27001 Ledningssystem för informationssäkerhet – krav och ISO/IEC 27002 Riktlinjer för informationssäkerhetsåtgärder. Pensionsmyndigheten följer Myndigheten för samhällsskydd och beredskaps (MSB:s) föreskrifter (MSBFS 2020:6) och allmänna råd om statliga myndigheters informationssäkerhet. Ledningssystemet ger myndigheten en sammanhållen bild av säkerhetsarbetet och de processer och rutiner inom säkerhetsarbetet som ingår i en större helhet.

Pensionsmyndigheten arbetar aktivt med styrning och uppföljning inom informationssäkerhet, och anpassar processerna för att fungera i det agila arbetssätt som myndigheten infört.

Pensionsmyndigheten använder sig regelbundet av MSB:s analysverktyg Infosäkkollen för att undersöka vilken nivå myndighetens systematiska informations- och cybersäkerhetsarbete befinner sig på samt hur den kan utvecklas.

Årets resultat är en förbättring jämfört med tidigare mätning som genomfördes 2021. Pensionsmyndigheten har prioriterat ett par områden med förbättringsmöjligheter för att stärka upp förmågan inom informationssäkerhetsområdet. Dessa områden kommer att inkluderas i en handlingsplan som är under framtagande.

Inledning

En god informationssäkerhet är en förutsättning för att Pensionsmyndigheten ska kunna utföra sitt uppdrag, vilket i huvudsak är att administrera och betala ut den allmänna pensionen, att ge pensionssparare en samlad bild av och korrekt information om hela pensionen samt att stärka pensionssparares ställning som konsumenter. Myndigheten värnar om pensionärernas förmåner och integritet, medarbetarnas trygghet samt skyddet av interna tillgångar.

Uppdraget

Enligt regleringsbrevet ska Pensionsmyndigheten redogöra för hur myndigheten har arbetat för att förvalta och utveckla sin informationssäkerhet och för hur myndigheten planerar för att möta framtida behov.

Pensionsmyndigheten ska även särskilt redogöra för huruvida myndigheten gjort en utvärdering av det egna informationssäkerhetsarbetet genom något analysverktyg, t.ex. Myndigheten för samhällsskydd och beredskaps verktyg Infosäkkollen, samt redogöra för de åtgärder som vidtagits med anledning av resultatet.

Förvaltning och utveckling

Det övergripande målet för Pensionsmyndighetens säkerhetsarbete är att ha en väl avvägd och riskbaserad säkerhetsnivå, och att värna om pensionärernas förmåner och integritet, medarbetarnas trygghet samt skydda myndighetens tillgångar. Säkerhetstänkande ska genomsyra all verksamhet inom Pensionsmyndigheten. Målet uppnås genom att förebygga och minimera risken för skador, störningar och oegentligheter inom verksamheten.

Pensionsmyndigheten tillämpar ett systematiskt och riskbaserat informationssäkerhetsarbete. Roller och ansvar är definierade och har anpassats för det agila arbetssättet, vilket är en förutsättning för att lyckas med myndighetens informationssäkerhetsarbete.

Säkerhetsarbetet vid Pensionsmyndigheten är riskbaserat och utgår från verksamhetens behov, författningskrav, styrande dokument, avtal och rådande hotbild. Dessa utgör alla en viktig del i Pensionsmyndighetens övergripande arbete med intern styrning och kontroll.

Säkerhetsledningssystemet

Ledningssystemet baseras på de internationella standarderna ISO/IEC 27001 Ledningssystem för informationssäkerhet – krav och ISO/IEC 27002 Riktlinjer för informationssäkerhetsåtgärder. Pensionsmyndigheten följer MSB:s föreskrifter (MSBFS 2020:6) och allmänna råd om statliga

myndigheters informationssäkerhet. Detta ger myndigheten en sammanhållen bild av informationssäkerhetsarbetet och de processer och rutiner som ingår i en större helhet. Det omfattar alla organisatoriska delar vid alla myndighetens verksamhetsorter och är en del av myndighetens totala ledningssystem.

Som en grundläggande del i ledningssystemet ingår att systematiskt analysera och hantera interna och externa intressenters krav och förväntningar. I detta arbete ingår löpande omvärldsanalys där framtida behov fångas, analyseras, värderas och senare införs i styrdokument, processer eller rutiner i ledningssystemet. Policyn, riktlinjer och anvisningar inom informationssäkerhetsområdet och angränsande områden uppdateras kontinuerligt utifrån både externa krav och interna processer och arbetssätt.

Ett annat fundament i säkerhetsledningssystemet är informationsklassning. Myndigheten har en beslutad metod för informationsklassning, som syftar till att säkerställa att information har ett korrekt skydd i förhållande till dess värde och att upprätthålla myndighetens beslutade säkerhetsnivå. Informationsklassning genomförs för befintliga informationstillgångar såväl som vid förändrade eller nya informationsmängder. Myndighetens metod innehåller värdering av information, avvikelseanalys, riskanalys och åtgärdsanalys, och det finns en framtagen mall som verktygsstöd för samtliga steg. Informationsägaren ansvarar för att informationsklassning sker, med stöd av informations- och it-säkerhetsfunktionerna.

Samverkan

Pensionsmyndigheten medverkar i en bredare samverkan inom informationssäkerhetsområdet, som kan skapa långsiktiga förutsättningar för att höja nivån av informationssäkerhet inom statsförvaltningen. Här kan särskilt nämnas samarbeten i säkerhetsforum med Försäkringskassan avseende IT-tjänster och samverkan med Statens servicecenter avseende informationssäkerhetsfrågor vid servicekontoren. Pensionsmyndigheten är också medlem i eSam. Myndigheten arbetar dessutom kontinuerligt med att stärka den interna samverkan, bland annat mellan funktionerna för informationssäkerhet, IT-säkerhet, risk och dataskydd i syfte att ytterligare förbättra förmågan att fånga upp samtliga aspekter av informationssäkerhetsarbetet.

Hantering av säkerhetsrisker

Den väl avvägda och riskbaserade säkerhetsnivån appliceras genom myndighetens ramverk för riskhantering, vilket ger ett enhetligt förhållningssätt till risk, och skapar en struktur för ett systematiskt riskarbete. Ramverket stödjer verksamheten med att identifiera möjliga risker, analysera dessa, besluta om hur de ska hanteras samt utforma, planera och genomföra åtgärder för att hantera dem. Detta för att med rimlig säkerhet uppfylla myndighetens uppdrag och mål och därmed skapa värde för pensionärer och pensionssparare. Riskhanteringen innebär också att följa upp risker och riskhanterande åtgärder, samt att sammanställa, analysera och

rapportera dessa. Riskhanteringsprocessens tillämpning konkretiseras genom stödjande mallar med tydligt definierade konsekvenskategorier och konsekvensnivåer för att säkerställa uppfyllnad av lagkrav och styrande dokument. Myndigheten har också en grundutbildning för alla medarbetare i det interna ramverket för riskhantering. Riskanalyser utförs generellt av riskägaren, men med stöd av exempelvis informationssäkerhetsfunktionen.

Myndigheten utför varje år ett stort antal riskanalyser inom många olika områden, och specifikt inom informationssäkerhet när det gäller exempelvis upphandlingar, informationsklassningar och konsekvensbedömningar. Myndighetens inköpsprocess inleds exempelvis med en grundlig verksamhetsanalys, där säkerhetsmässiga förutsättningar analyseras. Dessa tas sedan vidare till nästa steg, där kravställning baserad på riskanalyser genomförs. Specialister inom inköp lotsar beställaren genom hela inköpsprocessen, men resurser från informationssäkerhet och it-säkerhet deltar också aktivt i arbetet.

Pensionsmyndighetens riskhantering är anpassad till en modell med tre ansvarslinjer, som formaliseras i arbetsordningen. Första ansvarslinjen utgörs av den operativa verksamheten, där riskägaren ansvarar för det systematiska säkerhetsarbetet. Andra linjen utgörs av en riskfunktion, som stödjer, övervakar och följer upp första ansvarslinjens arbete. Den tredje ansvarslinjen utgörs av internrevisionsfunktionen. Detta skapar struktur kring riskägarskap genom att tydliggöra vem som ansvarar för vad rörande riskhantering och intern styrning och kontroll.

Riktlinjen för riskhantering tydliggör också roller och ansvar i övrigt i riskhanteringsarbetet, och definierar också struktur för eskalering av risker. Identifierade risker ska kommuniceras till närmaste verksamhetsansvarig och eskaleras till behörig riskägare för beslut. Risker som uppnår ett visst riskvärde ska alltid eskaleras till avdelningschef. Om risken bedöms som väsentlig ska den rapporteras till generaldirektören. Generellt för säkerhetsrisker gäller att säkerhetschefen har ett särskilt ansvar för att följa upp och rapportera säkerhetsrelaterade risker till generaldirektören.

Minst en gång per år genomförs en genomgång av säkerhetsläget och säkerhetsledningssystemet med myndighetens ledningsgrupp. Vid genomgången ges ledningen en möjlighet att informera sig om säkerhetsåtgärder och allvarliga risker, eller andra hinder för att uppnå ledningens målsättning och inriktning med säkerhetsarbetet.

Säkerhetsmedvetande

Utöver att samtliga medarbetare har ansvar att följa myndighetens säkerhetspolicy, riktlinjer och anvisningar ingår det också att samtliga medarbetare årligen ska genomgå en obligatorisk säkerhetsutbildning i syfte att säkerställa att alla medarbetare har kännedom om vad som krävs ur ett säkerhetsperspektiv för sin roll inom Pensionsmyndigheten. Utbildningen redogör, bland mycket annat, för informationsklasser, skyddsåtgärder, hantering och lagring av information utifrån hur den är klassad, samt vilken konkret roll och ansvar medarbetarna har för att kunna säkerställa

informationssäkerheten. I dagsläget har 83 % av myndighetens medarbetare genomgått denna utbildning.

Vissa utpekade roller, såsom handläggare av ärenden för personer med skyddade personuppgifter, informationsägare och chefer genomgår fördjupade utbildningar inom informationssäkerhetsområdet, som innehåller fördjupningar kring ansvar i den specifika rollen. Chefer har exempelvis ett fördjupat säkerhetsansvar när det gäller hantering av säkerhetsrisker, behörigheter, personalsäkerhet och uppföljning. Samtliga utbildningar genomförs återkommande utifrån fastställda tidpunkter.

Hantering av incidenter

En annan viktig del av informationssäkerhetsarbetet utgörs av rapportering och hantering av informationssäkerhetsincidenter. Tillbud eller händelser som påverkar eller riskerar att negativt påverka myndighetens verksamhet rapporteras av myndighetens samtliga medarbetare, och tas omhand enligt myndighetens incidenthanteringsprocess. Samtliga anmälningar gås igenom och beslut kring uppföljning och eventuella åtgärder säkerställs.

Krisberedskap och civilt försvar

Pensionsmyndigheten är en beredskapsmyndighet och ska i verksamheten verka för att minska sårbarheten i samhället genom att utveckla en god förmåga att utföra sitt uppdrag under fredstida krissituationer samt inför och vid höjd beredskap. Myndigheten arbetar därför med processer och rutiner för hantering av allvarliga kriser och incidenter, och planerar för att kunna anpassa verksamheten inför en förändrad säkerhetspolitisk situation.

Kontinuitets-/beredskapsplaner uppdateras fortlöpande, och kontinuitetsförmågan följs upp genom bland annat förmågebedömningar och risk- och sårbarhetsanalyser. Myndigheten arbetar också med totalförsvarsspecifika uppgifter och utveckling av praktisk förmåga vid krishantering, som till exempel krisledningsgrupp, lägesbild och robusta kommunikationsmedel. Utbildning, övning och uppföljning är viktiga verktyg. Samarbetet inom beredskapssektor Ekonomisk säkerhet är ett forum för samverkan med andra myndigheter inom området.

Framtida behov

Grunden i Pensionsmyndighetens systematiska säkerhetsarbete är att sträva efter ständig förbättring. Det sker genom att årligen följa upp och mäta effekterna av säkerhetsledningssystemet och rapportera till ledningen. Det sker också genom att föreslå och implementera förbättringar.

Myndighetens informationshantering behöver stärkas ytterligare utifrån det försämrade säkerhetsläget i omvärlden. Under 2024 kommer därför informationsklassningsmodellen att uppdateras. Syftet är att tydliggöra roller och ansvar, och att förenkla för informations- och riskägare att

framför allt säkerställa att identifierade risker kan omhändertas på ett bra sätt.

Utvärdering av det egna informationssäkerhetsarbetet

För att Pensionsmyndigheten ska kunna upprätthålla en hög säkerhet, och därmed minska riskerna för incidenter samtidigt som myndigheten strävar mot ständiga förbättringar, har säkerhetsenheten bland annat ansvar för att regelbundet följa upp och utvärdera det systematiska säkerhetsarbetet.

Pensionsmyndigheten har använt sig av MSB:s analysverktyg Infosäkkollen för att undersöka vilken nivå myndighetens systematiska informations- och cybersäkerhetsarbete befinner sig på samt hur den kan utvecklas.

Årets resultat av Infosäkkollen är en förbättring jämfört med tidigare mätning som genomfördes 2021. Det är främst inom områdena analys och hantering av informationssäkerhetsrisker samt medarbetarnas kunskaper och myndighetens utbildningsverksamhet som det har skett förbättringar.

Efter senaste mätningen som genomfördes 2023 har myndigheten identifierat ett par områden med förbättringsmöjligheter för att stärka upp förmågan inom informationssäkerhetsområdet. Dessa områden kommer att inkluderas i den handlingsplan som är under framtagande, som efter beslut kommer att införlivas i myndighetens riskbaserade och systematiska informationssäkerhetsarbete.

www.pensionsmyndigheten.se