Informationssäkerhet

Svar på regeringsuppdrag

PENSIONS
MYNDIGHETEN

Innehåll

Sammanfattning

Informationssäkerhet är en uppsättning säkerhetsåtgärder för att bevara egenskaperna konfidentialitet, riktighet och tillgänglighet hos information. Med konfidentialitet avses att inga obehöriga får tillgång till informationen. Riktighet innebär att informationen inte är manipulerad eller förstörd och med tillgänglighet avses att informationen ska finnas tillgänglig när den behövs.

Pensionsmyndighetens verksamhet är både samhällsviktig och har betydelse för Sveriges säkerhet. Vårt mål för säkerhetsarbetet är att Pensionsmyndigheten ska ha en väl avvägd och riskbaserad säkerhetsnivå. Vi värnar om kundernas förmåner och integritet, medarbetarnas trygghet samt skyddar våra tillgångar.

Vi styr och leder säkerhetsarbetet genom ett säkerhetsledningssystem som består av ett antal processer och rutiner, organisation och ett säkerhetsregelverk. Ledningssystemet är baserat på internationella standarder för ledningssystem för informationssäkerhet, ISO/IEC 27001 och ISO/IEC 27002.

Vår bedömning är att vi har ett väl fungerande systematiskt arbetssätt för informationssäkerhet och säkerhetsskydd. Vi har tydliga regelverk som beskriver organisation, ansvar och vilka säkerhetsbestämmelser som gäller inom myndigheten. Alla medarbetare har en viktig roll i säkerhetsarbetet och vi strävar efter ett högt säkerhetsmedvetande inom myndigheten.

1. Inledning

Säkerhet är viktigt för det offentliga Sverige och en förutsättning för att vi fullt ut ska kunna tillvarata de effekter som digitaliseringen kan ge vårt samhälle. Vi stödjer en bredare samverkan inom säkerhetsområdet som kan skapa långsiktiga förutsättningar för att höja nivån på säkerhet inom statsförvaltningen. Vi ser positivt på den ökade medvetenhet och fokus inom området som regeringen visar och välkomnar uppdrag inom säkerhetsområdet.

Pensionsmyndighetens verksamhet berör merparten av alla medborgare och är både samhällsviktig och har betydelse för Sveriges säkerhet. Ett systematiskt säkerhetsarbete är en förutsättning för att Pensionsmyndighetens ska kunna utföra sitt uppdrag effektivt och rättssäkert. Säkerhetsarbetet är en integrerad del i Pensionsmyndighetens verksamhet och säkerhetsaspekter ska vägas in i de beslut som fattas.

1.1. Uppdraget

Regleringsbrevsuppdrag 2022

Informationssäkerhet

Pensionsmyndigheten ska övergripande redogöra för hur myndigheten arbetat för att stärka sin informationssäkerhet och hur myndigheten planerar att möta framtida behov, bl.a. utifrån aktuella digitaliseringsinitiativ.

1.2. Avgränsningar

I dokumentet redovisas övergripande åtgärder inom informationssäkerhet samt hur såväl vidtagna som planerade åtgärder möter framtida behov.

Utifrån uppdragets syfte och begränsade tidsram har vi valt ut ett antal informationssäkerhetsåtgärder tillsammans med ett antal framtida behov. Det är ingen fullständig sammanställning.

2. Informationssäkerhet

Pensionsmyndigheten har funnits i tolv år och bildandet av myndigheten föregicks av Pensionsmyndighetsutredningen (S 2008:05). Sedan myndighetens bildande har det funnits ett systematiskt arbetssätt för säkerhet innefattandes informationssäkerhet.

Från myndighetens start har det funnits ett beslutat säkerhetsledningssystem, bestående av internt styrande dokument för säkerhet, och en genomförd säkerhetsskyddsanalys.

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 och pensionärer en samlad bild av och korrekt information om hela pensionen samt att stärka pensionssparares och pensionärers ställning som konsumenter.

Vår verksamhet är helt beroende av it-lösningar och våra verksamhetssystem lagrar och behandlar information om ca 7,8 miljoner personer. Att administrera och betala ut pensioner berör alla aspekter (konfidentialitet, riktighet, tillgänglighet och spårbarhet) av informationssäkerhet.

Vårt mål för säkerhetsarbetet är att Pensionsmyndigheten ska ha en väl avvägd och riskbaserad säkerhetsnivå. Vi värnar om kundernas förmåner och integritet, medarbetarnas trygghet samt skyddar våra tillgångar.

2.1. Säkerhetsledningssystemet

Säkerhetsarbetet vid Pensionsmyndigheten är riskbaserat och utgår från verksamhetens behov, författningskrav, avtal, interna regler och rådande hotbilder. Säkerhetsarbetet är en viktig del i Pensionsmyndighetens övergripande arbete med intern styrning och kontroll samt riskhantering och säkerhetsaspekter ska vägas in i de beslut som fattas.

Vi styr och leder säkerhetsarbetet genom ett säkerhetsledningssystem som omfattar alla aspekter av säkerhet inklusive informationssäkerhet. Vi anser att det är det mest effektiva och systematiska sättet att leda arbetet. Det ger oss en sammanhållen bild av säkerhetsarbetet och våra processer och rutiner inom säkerhetsarbetet ingår i en större helhet. Säkerhetsledningssystemet omfattar alla organisatoriska delar vid alla myndighetens verksamhetsorter.

Vi följer Myndigheten för samhällsskydd och beredskap - MSB:s föreskrifter (MSBFS 2020:6) och allmänna råd om statliga myndigheters informationssäkerhet.

Säkerhetsledningssystemet baseras på standarderna ISO/IEC 27001 Ledningssystem för informationssäkerhet - krav och ISO/IEC 27002 Riktlinjer för informationssäkerhetsåtgärder.

2.2. Ansvar inom säkerhet

Alla medarbetare har ett ansvar för säkerheten i Pensionsmyndigheten. För att nå målen för säkerhet är engagemang från myndighetens ledningsgrupp, chefer och medarbetare en förutsättning.

- Generaldirektören har det yttersta ansvaret för säkerheten inom Pensionsmyndigheten. I övrigt följer ansvaret för säkerheten det ordinarie verksamhetsansvaret.
- Chefer på alla nivåer har ett ansvar för att medarbetare (avser både anställda och uppdragstagare) har tillräcklig kunskap om Pensionsmyndighetens säkerhetsregelverk bestående av policy, riktlinjer, anvisningar och stöddokument.
- Medarbetare på alla nivåer har ett ansvar för att följa regler, genomgå läraktiviteter i säkerhet samt att vara uppmärksamma på och rapportera säkerhetsbrister och säkerhetsincidenter till närmaste chef eller säkerhetsenheten.
- Arbete pågår med en översyn av hur säkerhetsansvaret ska fördelas i myndighetens agila it-utveckling.

2.2.1. Organisation av säkerhetsarbetet

Myndigheten har en säkerhets- och säkerhetsskyddschef som i säkerhetsskyddsfrågor rapporterar direkt till generaldirektören. Det finns två enheter inom myndigheten, säkerhetsenheten och it-säkerhets- och tjänsteleveransenheten, som har bestämmande ansvar (i förhållande till övriga avdelningar) inom säkerhet.

Säkerhetsenheten tillhör avdelningen för myndighetsstyrning och stöd och ansvarar för informationssäkerhet, personsäkerhet, fysisk säkerhet, internutredningar, kontinuitetsplanering samt krisberedskap och civilt försvar på Pensionsmyndigheten.

It-säkerhets- och tjänsteleveransenheten tillhör it-avdelningen och ansvarar för att ta fram, etablera och underhålla det interna regelverket inom it-säkerhet. Enheten ansvarar även för att säkerställa att it-säkerhetskraven beaktas och upprätthålls inom ramen för Pensionsmyndighetens säkerhetsledningssystem, till exempel inom utvecklingsprojekt, förvaltning och servicenivåavtal. Utöver detta samordnar enheten även frågor som rör identitets- och åtkomsthantering (IAM).

Även om det bestämmande ansvaret är tydligt uppdelat mellan de två enheterna finns ett tätt samarbete.

Samarbetet sker på strategisk nivå i frågor som rör styrning av säkerhet, samverkan och ansvarsfördelning, på taktisk nivå exempelvis vid utformning av styrande dokument, processer och rutiner samt även på operativ nivå där representanter från båda enheterna deltar i projekt, upphandlingar, utvecklingsinsatser m.m.

2.2.2. Internt samarbete

Säkerhetsledningssystemet är en del av myndighetens totala ledningssystem. I Pensionsmyndighetens strategiska plan beskrivs vårt uppdrag och hur vi ska genomföra det. Myndigheten har delat in uppdraget i fem områden där ”god myndighetsförvaltning” är ett. Inom det området definieras att ”vår verksamhet har en väl avvägd och riskbaserad säkerhetsnivå”. Säkerhet ska vara en del av verksamheten och säkerhetsaspekter ska vägas in i de beslut som fattas.

För att kunna bedriva ett systematiskt säkerhetsarbete är ett väl fungerande internt samarbete med alla delar av verksamheten en förutsättning. Detta är särskilt viktigt när det gäller stödfunktioner som exempelvis juridik, dataskydd, risk, arkiv- och registratur samt inköp.

2.3. Säkerhetsregelverk och säkerhetsmedvetande

Pensionsmyndighetens beslutade säkerhetsnivå och säkerhetsregler framgår i vårt interna säkerhetsreglerverk. Regelverket består av internt styrande dokument på tre nivåer policy, riktlinjer och anvisningar indelade efter syfte och målgrupp. I dagsläget finns ca 30 styrande dokument som utgör regelverket, inom områdena informationssäkerhet, it-säkerhet, personsäkerhet och fysisk säkerhet. De styrande dokumenten är utgivna av antingen säkerhetsenheten eller it-säkerhets- och tjänsteleveransenheten.

Genom att ha ett internt strukturerat regelverk kan vi arbeta mer effektivt med säkerhet. Det är transparant för organisationen vilken nivå av säkerhet som gäller vid myndigheten och återkommande frågor inom säkerhetsområdet kan ofta besvaras genom att beskriva säkerhetsnivån i regelverket.

Regelverket uppdateras och anpassas löpande för att hantera myndighetens säkerhetsrisker och för att säkerställa att vi har en väl avvägd säkerhetsnivå. Ett exempel på det är att vi nu inom kort kommer att fastställa en ny riktlinje som ska ersätta nuvarande riktlinjer ”Säkerhet för chefer” och ”Styrning och ledning av säkerhet”. Detta är ett led i vårt arbete med att regelbundet se över styrande dokument och att roller och ansvar stämmer med förändrade arbetssätt etc. Ett exempel på detta är att myndigheten nu succesivt går över till agil it-utveckling enligt Safe-ramverket, vilket innebär nya roller och ny fördelning av ansvar.

2.3.1. Säkerhetsmedvetande

Säkerhetsarbetet är inriktat mot att skapa ett högt allmänt säkerhetsmedvetande inom hela Pensionsmyndigheten. Vi genomför olika aktiviteter som syftar till att öka medarbetarnas säkerhetsmedvetande för att skapa en god säkerhetskultur. Med säkerhetskultur menas ett gemensamt tanke-, beteende och värderingsmönster som kan påverka myndighetens säkerhet. Säkerhetsmedvetande i sig är en ständigt pågående lärandeprocess.

Pensionsmyndigheten har ett övergripande program för ökat säkerhetsmedvetande som knyter ihop aktiviteterna och som syftar till att säkerställa att alla väsentliga områden täcks. Genom programmet kan vi också mäta och få en samlad bild av medarbetarnas nivå av säkerhetsmedvetande. Några exempel på aktiviteter vi genomför är säkerhetsutbildningar, föreläsningar, artiklar på intranätet, tertialrapporter, krisberedskapsveckan (infaller i maj) och informationssäkerhetsmånaden (oktober). Vi har identifierat prioriterade målgrupper där vi genomför målgruppsanpassade insatser. Några av de prioriterade målgrupperna är medarbetare med SID[1]-behörighet, medarbetare med höga behörigheter eller som är lokala administratörer, chefer, lokala krisledare, utvecklare, programmerare och arkitekter inom it-avdelningen.

Som en bas i programmet har vi en webbaserad läraktivitet inom säkerhet som består av fem delar, där den första grundläggande läraktiviteten ”säkerhet för alla” är obligatorisk för samtliga medarbetare på Pensionsmyndigheten. Läraktiviteten är återkommande och medarbetare ska genomföra den minst vartannat år.

Utöver den här basutbildningen finns även rollspecifika påbyggnadsdelar för dessa roller:

- SID-handläggare
- Projektägare och projektledare
- Objektägare och förvaltningsledare
- Chefer

Vi genomför också anpassade utbildningar för särskilda målgrupper exempelvis inom it-avdelningen. Bland annat:

- En återkommande mognadsmätning som omfattar förmågor inom it-säkerhetsarkitektur. Detta är tänkt som stöd kring framtida investeringar och riskminimeringar.
- Fortsätta höja säkerheten i vår utvecklingsprocess (DevSecOps).

Just nu pågår även ett framtagande av en helt ny utbildning inom it-säkerhet, en mer teknisk informationssäkerhetsutbildning, som ska rikta sig till alla medarbetare. Utbildningen kommer vara återkommande och syftar till att höja säkerhetsmedvetandet för att minska risker och att det ska vara lätt att göra rätt.

[1] SID (Skyddad identitet)

2.4. Hantering av incidenter

Incidenthantering handlar om att identifiera svagheter och brister i vår verksamhet och ge oss underlag till förbättringar. Hanteringen innefattar att rapportera, åtgärda och följa upp incidenter. Att förebygga att incidenter inträffar och mildra de potentiella konsekvenserna utgör en viktig del av Pensionsmyndighetens riskhantering och säkerhetsarbete.

Vi har väl fungerande verktygsstöd och process för att hantera incidenter inom ramen för informationssäkerhet på myndigheten.

En incident kan beröra flera områden i verksamheten och förutsätter intern samverkan vid hanteringen. Säkerhetsenheten har bestämmande ansvar för incidenthantering, men alla myndighetens avdelningar är delaktiga i hanteringen av incidenterna. Vi har ett bra samarbete med andra funktioner internt inom myndigheten.

Vi har även väl fungerande rutiner för hur vi rapporterar it-incidenter till MSB och följer MSB:s föreskrifter om statliga myndigheters rapportering av it-incidenter (MSBFS 2020:8).

2.5. Informationsägarskap, informationsklassning och hanteringsregler

De största informationsmängderna inom Pensionsmyndigheten lagras och behandlas i it-system. För att den information vi hanterar ska ha ett korrekt skydd behövs övergripande säkerhetsåtgärder inom flera områden:

1. Att våra it-lösningar har rätt nivå av säkerhet
2. Att våra lokaler där informationen finns har rätt nivå av säkerhet
3. Att våra medarbetare hanterar informationen korrekt.

En viktig del i det systematiska arbetssättet med informationssäkerhet är att säkerställa att det finns tydliga ägare av informationen internt inom myndigheten, vilket också är tydliga krav i MSBFS 2020:6 och MSBFS 2020:7.

Pensionsmyndigheten använder sig av förvaltningsmodellen PM3[2] för förvaltningsstyrning av verksamheten där detta är tydliggjort, men Pensionsmyndigheten fasar nu ut PM3 och inför successivt ett agilt arbetssätt inom vår it-utveckling, där arbetet organiseras i värdeströmmar. Arbetssättet utformas med stöd av ramverket Scaled Agile Framework (SAFe). Genom ett agilt arbetssätt bedrivs både förvaltnings- och utvecklingsarbete utifrån tvärfunktionella samarbeten över avdelningsgränserna. Detta arbetssätt har lett till att roller som exv.

[2] PM3 förvaltningsmodell utvecklad av företaget PÅ AB, se www.pm3.se

informationsägare och riskägare behöver anpassas, vilket är ett arbete som pågår.

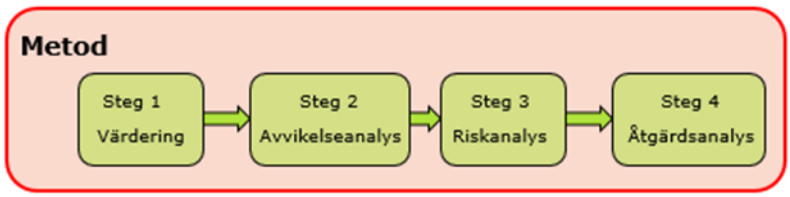
Vad gäller dataskydd har Pensionsmyndigheten en dataskyddsorganisation med bland annat ett Dataskyddsombud och dataskyddsteam som utifrån regleringen i dataskyddsförordningen (GDPR) arbetat med att ta fram styrande dokument samt metod, mallar och stöd för personuppgiftshanteringen. Skyddet av personuppgifter är en del av informationssäkerheten och är integrerat i myndighetens säkerhetsregelverk.

2.5.1. Informationsklassning

Informationsklassning är en metod som myndigheten använder för att säkerställa att information har ett korrekt skydd i våra it-system i förhållande till dess värde. Om skyddet är fel dimensionerat kan det t.ex. leda till onödigt höga kostnader eller att information utsätts för en för hög risk.

Informationsklassning är en viktig del i att upprätthålla myndighetens beslutade säkerhetsnivå och vi har arbetat systematiskt med informationsklassning sedan 2012. Säkerhetsenheten ansvarar för metoden, modellen och verktygsstöd för informationsklassning och specialister från it-säkerhetsenheten deltar som stöd vid genomförandet av informationsklassning.

Metoden för informationsklassning består av fyra steg som genomförs i workshopform.



Genom metoden kontrollerar vi att ett enskilt it-system har rätt nivå av säkerhet i förhållande till värdet hos informationen som behandlas i systemet. I metoden följer vi upp att de säkerhetsåtgärder som är tillämpbara är införda och fungerar. Att upprätthålla rätt nivå av säkerhet över lång tid är en utmaning och det finns nästan alltid en eller flera avvikelser som behöver åtgärdas. Genom metoden för informationsklassning identifieras dessa avvikelser med tillhörande risker och en åtgärdsplan upprättas för att korrigera avvikelserna och hantera riskerna.

2.5.2. Hanteringsregler för information och utrustning

Ett viktigt kompletterande skydd för informationen, utöver det skydd som finns i it-miljön och våra lokaler, är hanteringsregler som beskriver hur medarbetarna får hantera information och arbetsutrustning.

Hanteringsreglerna beskriver vilka säkerhetsbestämmelser som gäller för exempelvis användning av e-post, Skype, mobila enheter m.m. Vi har även särskilda bestämmelser för hur utrustning och information ska hanteras vid distansarbete, eller när medarbetare är på tjänsteresa.

Vi ser löpande över de här hanteringsreglerna då det ständigt sker förändringar som exempelvis nu de senaste åren med en förflyttning mot distansarbete, men även teknikskiften som påverkar informationssäkerheten.

2.6. Säkerhet i it-miljön

Som vi beskrivit tidigare är Pensionsmyndigheten helt beroende av it-lösningar för att kunna utföra vårt uppdrag. Ett systematiskt arbetssätt med säkerhet och it-säkerhet för it-miljön är en förutsättning för detta. Vi följer också MSB:s föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7).

I Pensionsmyndighetens strategi för it[3] identifieras nio strategiska inriktningar för arbetet med it inom myndigheten. Inriktningarna utgör ett fundament för hur vi arbetar med it för att maximera nyttan för pensionärer och pensionssparare och är i linje med myndighetens övergripande inriktning för kundcentrerad digitalisering.

Den första av de nio inriktningarna är ”Säker leverans”. Där framgår bland annat att it-säkerhet och driftstabilitet ska vara i fokus och prägla vår it-leverans i alla avseenden.

Eftersom Pensionsmyndigheten är en bevakningsansvarig myndighet[4] och bedriver samhällsviktig verksamhet har vi höga krav på tillgänglighet och god it- och informationssäkerhet. Detta innebär att:

- It-leveransen ska bedrivas utan störningar och i de fall sådana inträffar ska vi kunna hantera dem på ett kontrollerat och effektivt sätt.
- Då tillgängligheten för våra informationssystem är central för vår verksamhet prioriterar it-avdelningen arbetet med robusthet och redundans, samt ett fungerande kontinuitetsarbete.
- Myndighetens säkerhetsarbete ska följa lagar och förordningar och vara riskbaserat, med säkerhetsåtgärder som anpassas till risknivå och kostnadseffektivitet i lösningarna.
- Vi ska ha ett högt kvalitets- och säkerhetsmedvetande inom hela myndigheten.

Vi har en väl fungerande styrning och systematiskt arbetssätt och det finns ett antal processer och rutiner inom it-säkerhet. Vi redovisar inte dessa processer och rutiner här, då vi anser att de faller utanför vår tolkning av uppdraget.

---

[3] Strategi för it 3.0, dnr VER 2018-133

[4] https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-20151052-om-krisberedskap-och_sfs-2015-1052

Vi har ett tydligt och strukturerat regelverk för it-säkerhet, som består av 12 anvisningar inom området. I regelverket anges vilka säkerhetsåtgärder som är beslutade inom it-säkerhet, hur ansvar fördelas inom området samt beskrivningar av processer och rutiner.

It-säkerhetsenheten arbetar aktivt med olika former av uppföljning och sammanställer bland annat tertialrapporter över it-säkerhetsläget. Det finns också ett väl fungerande samarbete inom it-avdelningen där it-säkerhetsspecialister deltar i olika beslutsfora för att säkerställa att it-säkerheten upprätthålls.

2.7. Leverantörsrelationer och myndighetssamverkan

Delar av Pensionsmyndighetens verksamhet utförs av eller hos andra aktörer, såväl offentliga och privata. Vår verksamhet ska ha rätt nivå av säkerhet oavsett om utförandet sker inom Pensionsmyndigheten eller för vår räkning hos en extern part. Det är viktigt att säkerhet beaktas tidigt i processen vad gäller inköp eller användande av tjänster hos extern part. Krav på säkerhet ska specificeras i avtal eller överenskommelser. Vi har etablerade processer och rutiner för inköp där säkerhet ingår som en viktig del. Vi har fungerande leverantörsrelationer där vi bland annat följer upp säkerhetskraven, hantering av incidenter m.m.

Några exempel på delar av vår verksamhet som utförs av eller hos andra myndigheter är

- Statens Servicecenter som ansvarar för servicekontorsverksamheten, där Pensionsmyndigheten ingår. Inom ramen för servicekontoren samverkar alla myndigheter som deltar och diskuterar/beslutar om vilken nivå av säkerhet som ska gälla inom servicekontorsverksamheten.

- Försäkringskassan levererar datahallstjänster och förvaltning av vissa verksamhetssystem till Pensionsmyndigheten. Vi har löpande samverkan där vi bland annat följer upp säkerheten och diskuterar olika säkerhetslösningar i leveranserna.

2.8. Bedömning av informationssäkerhet

Vår bedömning är att vi har ett väl fungerande systematiskt arbetssätt för informationssäkerhet. Våra processer och arbetssätt är väl etablerade sen många år och vi arbetar löpande med att förbättra säkerhetsarbetet.

Pensionsmyndighetens ledningsgrupp har ett stort engagemang för säkerhetsfrågor och förutom ledningens genomgång föredras säkerhetsrelaterade ärenden för ledningsgruppen ett flertal gånger varje år.

Vi följer MSB:s föreskrifter (MSBFS 2020:6) och allmänna råd om statliga myndigheters informationssäkerhet. Vårt säkerhetsledningssystem är baserat på och följer internationella standarder (ISO/IEC 27001 och 27002) på en

godtagbar nivå. Vår bedömning är att systemet är lämpligt, tillräckligt och effektivt. Vi genomför regelbundna kontroller och uppföljningar enligt beslutade kontrollplaner och analyserar inträffade incidenter för att identifiera brister och avvikelser inom säkerhet. Vi har ett tydligt säkerhetsregelverk med tillhörande säkerhetsutbildningar och våra medarbetare har ett gott säkerhetsmedvetande.

Den interna samverkan mellan olika funktioner inom myndigheten är väl fungerande och har stor betydelse för det systematiska arbetssättet med säkerhet.

Vi deltar också i olika former av extern samverkan inom säkerhetsområdet för att utbyta erfarenheter med exempelvis andra myndigheter. I samverkan får vi en möjlighet att kvalitetssäkra vårt säkerhetsarbete genom att utbyta erfarenheter med andra och jämföra metoder och arbetssätt. Att dela med sig av kunskap och erfarenheter ser vi som en framgångsfaktor i det totala arbetet med säkerhet inom det offentliga Sverige.

3. Hur Pensionsmyndigheten möter framtida behov

Pensionsmyndigheten har, som tidigare beskrivits, sedan en längre tid ett väl fungerande systematiskt arbetssätt för informationssäkerhet. Processer är på plats med definierade roller och ansvar samt tydliga rapporteringsvägar som nu också är på gång att anpassas för att även svara mot den agila utvecklingsformen, vilket är en förutsättning för att lyckas med informationssäkerheten då det agila ramverket leder till nya och förändrade roller och arbetssätt.

Ett systematiskt informationssäkerhetsarbete innebär att uppnå ständiga förbättringar och att följa med i utvecklingen. Vi har under 2021 utfört ett uppföljningsarbete genom MSB:s verktyg ”Infosäkkollen” och påbörjat ett större arbete inom tre stycken delar av informationssäkerhetsområdet som ska fortsätta under 2022.

1. Ta fram en ny informationsklassningsmetod som blir både bredare och djupare än nuvarande metod.
2. Ta fram en ny metod för uppföljning, samt genomföra en mer grundlig revision av det systematiska informationssäkerhetsarbetet.
3. Utveckla arbetssätt med säkerhetsrisker som tydligare kopplar till Pensionsmyndighetens övriga riskhantering.

Systematiskt informationssäkerhetsarbete är viktigt för såväl myndigheter som för företag och andra organisationer. Ofta väger dock andra intressen tyngre, exempelvis för ett företag är det själva affären som till stor del går före säkerhet och för en myndighet är det ofta tidspress, nya uppdrag och tillkommande initiativ som är utmaningar för en god informationssäkerhet.

Digitalisering är ett begrepp som används frekvent och lyfts ofta fram som att den skapar nya möjligheter för innovation och öppnar upp för nya samarbeten och arbetssätt där privatpersoner, företag och andra aktörer kan spela en aktiv och samskapande roll i utformandet av bl.a. offentliga tjänster.

Säkerhet nämns sällan i samhällsdebatten i samband med digitalisering. Vi anser att det finns behov av att i stället prata om säker digitalisering i alla sammanhang som digitalisering lyfts upp i. I detta anser vi att såväl dataskydd och integritet som hanteringen av allmänna handlingar ingår och i förlängningen ett korrekt och lagligt myndighetsutövande.

Delar av de här resonemangen har också uppmärksammats av ett projekt - Cybersäkerhet för ökad konkurrenskraft - inom Kungl. Ingenjörsvetenskapsakademien (IVA)[5].

Pensionsmyndigheten får, likt andra myndigheter, ett flertal nya uppdrag med snäva tidsramar som tillsammans med övrig utveckling ställer krav på snabb digitalisering, vilket medför att myndigheten allokerar stora resurser till detta. I praktiken innebär det att resurser omfördelas från förvaltningsarbetet till it- och verksamhetsutveckling, vilket bland annat leder till att införandet av säkerhetsåtgärder inte sker i samma takt.

Utöver de nya uppdrag och initiativ som tillkommer från nationellt håll finns det på EU-nivå en rad gränsöverskridande digitaliseringsinitiativ som syftar till att förenkla och möjliggöra för privatpersoner och företagare att utföra ärenden digitalt. Dessa initiativ medför vissa utmaningar i olika avseenden för Pensionsmyndigheten, men även för andra myndigheter och EU:s medlemsstater i stort. SDG-förordningen[6] kräver exempelvis att medlemsstaterna ska ge användare tillgång till information och e-tjänster inom utpekade områden, däribland pensionsområdet. Från ett informationssäkerhetsperspektiv finns i dagsläget utmaningar med att säkerställa att utfärdade e-legitimationer från andra medlemsstater kan kopplas till den person som legitimationen är utfärdad för. Felaktiga kopplingar kan innebära risker, sett till kraven på bl.a. konfidentialitet och riktighet. Andra pågående EU-initiativ är arbetet med att införa certifierade europeiska e-identitetsplånböcker (European Digital Identity Wallets).

De ökade digitaliseringsinitiativen inom ramen för EU-samarbetet medför nya krav på digitala lösningar med hög säkerhet och acceptans inom hela EU. Förutom utmaningar vad gäller teknikutvecklingen kan även här omprioriteringar av den egna verksamheten och personella resurser behöva göras. Inom ramen för de pågående initiativen görs såväl enskilda som myndighetsgemensamma insatser för att möta de krav som ställs. Sannolikt kommer fler och fördjupade initiativ från EU framöver och ytterligare utmaningar kopplat till informationssäkerhetsaspekter.

---

[5] https://www.iva.se/globalassets/bilder/projekt/cybersakerhet/202111-iva-cybersakerhet-a5-e.pdf

[6] Europaparlamentets och rådets förordning (EU) 2018/1724 av den 2 oktober 2018 om inrättandet av en gemensam digital ingång för tillhandahållande av information, förfaranden samt hjälp- och problemlösningstjänster och om ändring av förordningen (EU) nr 1024/2012

Som nämnts tidigare har vi på Pensionsmyndigheten till stora delar grunden för en väl fungerande informationssäkerhet på plats och vi anpassar också vårt informationssäkerhetsarbete allteftersom för att på bästa sätt kunna möta förändringar.

Genom medlemskapet i eSam verkar Pensionsmyndigheten för att bättre ta tillvara digitaliseringens möjligheter, för att underlätta för privatpersoner och företag och för att använda våra gemensamma resurser på ett effektivt sätt. Pensionsmyndigheten deltar i olika arbetsgrupper inom eSam, t. ex. Moln, Juridik och Säkerhet. Genom att verka i dessa grupper arbetar vi för digitala tjänster som är tekniskt ändamålsenliga, säkra och lagenliga.

I myndighetens strategiska plan definieras fyra fokusområden med tillhörande önskade tillstånd. Två av dessa önskade tillstånd har tydlig koppling till digitalisering och eSam:

• Vi tänker ”digitalt först” och har alternativ för dem som behöver

• Vi är innovativa och använder ny teknik för att effektivisera vår verksamhet.

I sammanhanget är det svårt att bortse ifrån de stora händelser i vår omvärld som påverkar vårt informationssäkerhetsarbete. Dels är det den pandemi som drabbat världen, vilket medfört att vi snabbt behövt göra förflyttningar och organisera säkerhetsarbetet efter hand. Ett exempel är att det i ett tidigt skede av pandemin inordnades en redovisningspunkt hos myndighetens ledningsgrupp där Pensionsmyndighetens säkerhetschef varje vecka redogjorde för det aktuella läget och olika åtgärder vidtogs.

Sedan har vi det krig som nu pågår i Ukraina vilket har medfört att cyberhoten mot oss som myndighet har ökat. Det rör sig om olika typer av hot som ex. informationspåverkan och angrepp mot våra it-system. Med anledning av det har vi vidtagit en rad åtgärder, både tekniska och organisatoriska och vi har en ständig omvärldsbevakning.

www.pensionsmyndigheten.se