Datum
2025-04-07

Vår beteckning
FK 2025/000552

Svar på regeringsuppdrag

Informations- och cybersäkerhet

Försäkringskassan

Informations- och cybersäkerhet på Försäkringskassan

Försäkringskassan har fått i uppdrag att redovisa hur myndigheten arbetat för att säkerställa en hög nivå av informations- och cybersäkerhet i sin verksamhet. Försäkringskassan ska också redovisa hur myndigheten planerar att möta framtida behov inom informations- och cybersäkerhetsområdet. Försäkringskassan ska även särskilt redogöra för huruvida myndigheten utvärderat det egna informations- och cybersäkerhetsarbetet genom användning av Myndigheten för samhällsskydd och beredskaps verktyg Cybersäkerhetskollen, samt huruvida åtgärder vidtagits med anledning av resultatet.

Inledning

Försäkringskassan har ett ledningssystem för säkerhet anpassat till standarden ISO/IEC 27001. Försäkringskassans Riktlinjer *Säkerhetsregler* fungerar som ramverk till ledningssystemet. Säkerhetsreglerna är baserade på krav utifrån ISO 27001, lagar, förordningar och föreskrifter.

Myndigheten bedriver en samhällsviktig-, och till viss del säkerhetskänslig verksamhet. Potentiella angrepp från främmande makt samt hot från kriminella nätverk ligger därför bland annat till grund för Försäkringskassans skyddsåtgärder. Försäkringskassan är som en del i välfärdssystemet en måltavla för välfärdsbrott. Hot ställer krav på skydd för samtliga av Försäkringskassans tillgångar och resurser.

Försäkringskassan arbetar proaktivt med att göra en lägesbild över säkerhetsområdet. Lägesbilden ska påvisa risker och händelser på kort sikt och agerar bland annat som komplement till säkerhetsskyddsanalysen. Den fortlöpande lägesbilden går helt i linje med den nya nationella säkerhetsstrategin om att till egen ledningsgrupp och samtliga chefer meddela vilka hot och risker verksamheten står inför i syfte att göra vår del för att stärka samhällets motståndskraft. Lägesbilden är en proaktiv produkt som syftar till att ge ledningen underlag för prioriteringar och beslut ur ett säkerhetsperspektiv. Lägesbilden bidrar till att stärka myndighetens säkerhetskultur.

Utbildning och informationsinsatser

Säkerhet ska vara en del av Försäkringskassans kultur. Varje medarbetare ska ha ett högt säkerhetsmedvetande och inse betydelsen av sin egen medverkan i ett effektivt skydd. Utbildning och informationsinsatser är viktiga verktyg för att stärka säkerhetsmedvetenheten hos medarbetarna.

Försäkringskassan har en säkerhetsutbildning med tillhörande obligatoriskt kunskapstest som medarbetarna ska genomföra minst vartannat år. Dessutom ställs krav på kompletterande utbildningar för medarbetare som ska arbeta inom särskilda områden. Exempel på särskilda områden är skyddade personuppgifter, säkerhetsskydd, signalskydd och säkerhet vid it-utveckling. Myndighetens säkerhetsrådgivare har därtill genomfört utbildningsinsatser inom informationssäkerhet för Försäkringskassans medarbetare under hela det gångna året.

Försäkringskassans cybersäkerhetsorganisation inledde i början av året ett arbete för att öka kunskaper och medvetenhet om cybersäkerhet hos it-avdelningens medarbetare och för att långsiktigt stärka säkerhetskulturen. Med den enade kraften i ett stort antal medarbetare som har motivation och förmåga att utveckla och förvalta it-miljön med säkerhet i fokus kan it-avdelningen uppnå bättre resultat med högre effektivitet än när avdelningen enbart genomför reaktivt säkerhetsarbete av en mindre grupp experter. Initiativet inleddes med besök hos alla områdesledningar och följdes sedan av en stor mängd informationsträffar med medarbetare på områdes- och enhetsnivå.
Två utbildningar har även tagits fram. En webbutbildning för att utveckla grundläggande kunskaper – *Cybersäkerhet på jobbet och i vardagen*, som nu är tillgänglig för alla

Försäkringskassans medarbetare. Vid slutet av 2024 hade ca 3500 medarbetare genomfört utbildningen. Den andra utbildningen genomfördes som seminarier som riktade sig till chefer på IT-avdelningen.

Flera kommunikationsinsatser har även genomförts i syfte att stärka bland annat informationssäkerhetsarbetet. Exempel på kommunikativa initiativ är beredskapsveckan och informationssäkerhetsmånaden.

Försäkringskassan arbetar även aktivt med att stävja dataintrång. Det görs bland annat genom kommunikationsinsatser och information till medarbetarna.
För att höja kunskapen om korruption och oegentligheter och öka samarbetet mellan Försäkringskassans stödfunktioner har informationsinsatser utförts inom bland annat områdena ekonomi, Intern försäkringskontroll, inköp, upphandling och internrevision.
Flera artiklar har publicerats på Försäkringskassans intranät med olika teman såsom; dataintrång, antikorruptionsdagen och Visselblåsarfunktionen.
Som ytterligare ett led i att stärka Försäkringskassans arbete mot korruption behöver myndigheten försäkra sig om att chefer har den kunskap som krävs.
Därför har webbutbildningen *Korruption* tagits fram som riktar sig till chefer på Försäkringskassan men även till riskanalysledare som stöttar chefer i arbetet mot korruption.

Genomförda och planerade insatser för att stärka informations- och cybersäkerhetsarbetet
Försäkringskassan arbetar systematiskt med att stärka informations- och cybersäkerhetarbetet. Arbete planeras för att visualisera och beskriva Försäkringskassans ledningssystem för säkerhet på ett bättre och tydligare sätt. Aktiviteten förväntas bidra till att det går att få ut ännu mer effekt av ledningssystemet och bidra till målet om tillgångar skyddas på rätt sätt.

Arbete pågår löpande för att skapa bättre förutsättningar för medarbetarna att hantera information på ett säkert sätt. I början av 2024 publicerades bland annat en ny version av *Säkerhet på Försäkringskassan* som är en anvisning med hanteringsregler för information. Anvisning för informationsklassning har uppdaterats utifrån anpassningar av informationsklassningsmodellen.

Försäkringskassan har under året arbetat vidare med ett tvärfunktionellt uppdrag avseende livscykelhantering av verksamhetsinformation. Initiativet ger stöd till informationsägare så att de metodiskt och utifrån ett helhetsperspektiv kan omhänderta krav inom bland annat informationssäkerhet, dataskydd och arkivrätt. Stödet kommer till exempel bestå av ett antal verktyg för att lättare kunna tillämpa myndighetens styrning inom informationshantering. I initiativet ingår även stöd i att identifiera brister vad gäller skydd och förslag till åtgärder som säkerställer systematiska förbättringar. Att arbeta med förbättringar av myndighetens informationshantering är en viktig förutsättning för att upprätthålla ett gott informationssäkerhetsarbete, vilket i sin tur är en viktig utgångspunkt i arbetet med att möta framtida digitaliseringsbehov.

Arbete har inletts för att se över hur riskarbetet på Försäkringskassan kan förbättras och vilka förutsättningar som finns för verksamheten att tillämpa myndighetens styrning inom området. Arbetet kommer fortsätta, inte minst genom att utveckla metodstöd för riskhanteringen och se över möjligheten att höja förmågan ytterligare att analysera risker som har identifierats på alla nivåer inom Försäkringskassan.

Vid årets uppdatering av Försäkringskassans säkerhetsregler har särskilt fokus lagts på att förtydliga regelverket. Syftet är att det ska bli tydligare vilka krav och ansvar som finns och vad som krävs för att efterleva reglerna.

Genomlysning av säkerhetsreglerna har skett för att studera styrningen av säkerhet inom it-området. Genomlysningen utmynnade i förtydligande och förstärkt styrning, samt justering av begrepp. I den nya versionen av säkerhetsreglerna finns även en begreppslista som ska bidra till ökad tydlighet.

Försäkringskassans behörighetshantering syftar bland annat till att förhindra obehörig åtkomst till information och säkerställa minsta möjliga åtkomst för att utföra arbetsuppgifterna. Myndighetens behörighetsadministration har arbetat med att ta fram en förvaltningsmodell för myndighetens behörighetspaket. Förvaltningsmodellen syftar till att behörighetspaketen regelbundet anpassas efter aktuell process eller arbetsuppgift för att minimera risken för dataintrång och andra överträdelser. Ett omfattande arbete har även genomförts för att ge behörigheter tydligare namn och bättre beskrivningar. Detta i syfte att underlätta för cheferna att beställa rätt behörigheter och genomföra obligatoriska behörighetsuppföljningar. Arbete pågår även fortsatt för att stärka förmågan att följa upp och kvalitetssäkra priviligierade åtkomsträttigheter ur ett ägarperspektiv.

Inom cybersäkerhetsområdet har en analys av it-avdelningens säkerhetsmognad genomförts. Utifrån analysen har en lista på rekommenderade förbättringsåtgärder inom åtta olika områden tagits fram. Såväl analysen som de rekommenderade förbättringsåtgärderna för att åstadkomma en strategisk förflyttning mot förbättrad it-säkerhet presenterades för avdelningens ledningsgrupp i augusti 2024. En uppföljning av åtgärder och effekter genomförs under början av 2025 med målet att presentera en uppdaterad säkerhetsmognadsrapport under våren. Arbetet med säkerhetsmognadsanalys som ett verktyg för långsiktig förbättring ska därefter vara en årligen återkommande aktivitet.

Vid översyn av it-säkerhetsanvisningarna under 2024 lades särskild fokus på anpassning utifrån den nya struktur som infördes i säkerhetsreglerna 2023 och som följer standarden ISO 27001:2022.

Försäkringskassan har sedan tidigare initierat ett pilotprojekt som handlar om att inrätta verksamhetsnära säkerhetsrådgivare på ett mindre antal avdelningar för att säkerställa att det finns en utpekad samarbetspartner inom säkerhetsfrågor. Syftet är att utveckla stödet inom säkerhet och att stärka avdelningarnas förmåga att analysera, utveckla och hantera uppkomna säkerhetsutmaningar för att kunna lösa sitt uppdrag. Det verksamhetsnära stödet på avdelningsnivå är i en etableringsfas och några avdelningar har nu ett strukturerat stöd ifrån verksamhetsnära säkerhetsrådgivare i säkerhetsfrågor. Arbetet kommer fortskrida tills att samtliga avdelningar har ett upparbetat verksamhetsnära stöd.

Under 2024 har ett fortsatt fokus varit att vidareutveckla delar inom medarbetarskydd och implementera vissa säkerhetsåtgärder kopplat till avdelningarnas arbete med att identifiera våra mest utsatta roller för otillåten påverkan. Samtidigt har projektet ”motverka hotet från insidan” pågått men avslutades i juni 2024, och resultatet av projektet har sammanfattats i en rapport (A136.339-2023). Projektet syftade till att stärka skyddet på myndigheterna som samverkar i satsningen mot organiserad brottslighet. Projektet fokuserade på tre områden:

- att öka medvetenheten om insiderproblematik
- att förbättra myndigheternas enhetlighet kring hantering av insiderproblematik
- att verka för anpassad reglering i syfte att stärka skyddet mot insiderproblematik inom myndigheterna

Projektet ”motverka hotet från insidan” samt projekt medarbetarskydd har bidragit till arbetet med att ta fram en ny rutin, ”medarbetarskyddssamtal”. Detta för att hantera de situationer när risker för otillåten påverkan från relationsperson har uppmärksammats

och som bland annat skulle kunna bidra till röjande av information. Medarbetarskyddsamtalet är en förebyggande åtgärd där arbetsgivaren intar en aktiv roll i att medvetandegöra risker för otillåten och otillbörlig påverkan hos våra medarbetare och samtidigt tydliggöra vilket stöd som finns att få i det fall en sådan situation ändå skulle uppstå.

Vidare har även en ny webbutbildning tagits fram i syfte att ge ökad förståelse och kunskap om otillåten påverkan, otillbörlig påverkan och infiltration. Målsättningen är att skapa högre medvetande om riskerna för att därmed stärka säkerhetskulturen och motståndskraften för hela Försäkringskassan. Utbildningen inspireras av en utbildning som Skatteverket, Tullverket och Kronofogdemyndighetens har tagit fram på uppdrag av Finansdepartementet. Innehållet i webbutbildningen bygger på projekt inom den myndighetsgemensamma satsningen mot organiserad brottslighet samt rapporter och information från bland annat Brottsförebygganderådet, Polismyndigheten och Säkerhetspolisen.

Försäkringskassan stod i slutet av 2024 värd för en utbildning i medarbetarskydd där cirka 40 medarbetare från tolv myndigheter deltog. Utbildningen var en pilot och genomfördes inom ramen för den myndighetsgemensamma satsningen mot organiserad brottslighet som bland annat bygger på arbetet från ”projekt medarbetarskydd”, som genomfördes på uppdrag av operativa rådet 2022.
Vidare, bland annat för att stärka skyddet för informationstillgångarna, har Försäkringskassan infört integrerade säkerhetsrelaterade frågor i intervjuguider för rekrytering och via hemställan till regeringen lyft behovet och föreslagit utredning om utökade möjligheter till bakgrundskontroller.

Försäkringskassan har en etablerad process för incidenthantering med tillhörande incidenthanteringsverktyg för rapportering, hantering och uppföljning av incidenter. Inom området incidenthantering planeras utvecklingsinitiativ i form av ett gemensamt forum för lärande av incidenter med hjälp av det verksamhetsnära säkerhetsstödet. Det är vanligt förekommande att orsaker till incidenter är likartade över avdelnings- och förmånsgränser. Avsikten med initiativet är att identifiera gemensamma lösningar som kan skapa värde inom flera avdelningar men även att skapa ett lärande mellan avdelningar vad gäller förbättringsåtgärder för uppkomna incidenter. Förutom ökad säkerhetsnivå skulle det kunna bidra till minskade kostnader.

Med syfte att förenkla förbättringsarbete inom informationssäkerhets- och incidentområdet har förfinade incidentkategorier tagits fram. Kategorierna ska, tillsammans med orsaksanalyser användas för att samla olika typer av informationssäkerhetsincidenter och utifrån det bedöma vilka korrigerande- och förebyggande åtgärder som kan sättas in.

Externa samarbeten som bidrar till förbättrad informations- och cybersäkerhet
Digitala bedrägerier ökar i takt med att samhället blir mer uppkopplat där bedragare utnyttjar tekniska och mänskliga sårbarheter. Nätfiskeförsöken är mer avancerade och det är svårare än någonsin att skilja falskt från äkta. Försäkringskassan har därför publicerat en permanent sida på myndighetens webbplats med råd och hänvisningar till utbildningar som syftar till att stärka motståndskraften. Försäkringskassan har även anslutit sig till Digitala varningsgruppen som är en neutral privat-offentlig samverkansgrupp som främjar insamling och delning av varningar kring pågående digitala brott och brottsförsök. Syftet är att snabbt kunna varna allmänheten och mindre företag om pågående bedrägeriförsök.

Försäkringskassan deltar fortsatt i samverkan på operativ nivå inom it-säkerhetsarbetet mellan svenska myndigheter genom att SOC-funktionen deltar i GovSec samverkansforum som drivs av MSB/CERT-SE. Syftet med GovSec är att på ett

operativt plan inom cybersäkerhetsområdet utveckla ett effektivt samarbete för bättre incidenthantering, erfarenhetsutbyte, informationsdelning samt stärkt förtroende mellan forumets medlemmar.

Försäkringskassan arbetar även vidare i eSamverkansprogrammet, vars olika initiativ bland annat syftar till att stärka informationssäkerheten.

Utvärdering av informations- och cybersäkerhetsarbetet
Försäkringskassan har en etablerad mätmetod för att studera efterlevnad av myndighetens säkerhetsregler. Mätmetoden används i kombination med andra mätningar för att undersöka efterlevnaden av säkerhet inom ramen för Försäkringskassans ledningssystem för säkerhet.
Under det första halvåret 2024 genomfördes en mätning som omfattade alla Försäkringskassans avdelningar. Mätningen omhändertog de flesta områdena i säkerhetsreglerna där urvalet av regler gjordes utifrån Försäkringskassans myndighetsövergripande risker och att ansvar finns utpekat på verksamhetsansvarig chef eller avdelningschef. Respektive avdelning genomförde självskattning av hur väl kraven i säkerhetsreglerna efterlevs.
Resultatet av mätningen kommer att användas på flera olika sätt för att bidra till att utveckla ledningssystemet och informationssäkerhetsarbetet. Mätningen skapar även förutsättningar för att bättre säkerhetsstöd ska kunna ges till avdelningarna.

Under 2024 har även Försäkringskassans tillsynsfunktion i samarbete med säkerhetsorganisationen genomfört en tillsyn av säkerhetsarbetet på vissa utvalda kontor. Tillsyn på enskilda kontor ger ett lokalt perspektiv på hur Försäkringskassans verksamhet upplever arbetet med säkerhet. Arbetet kommer att fortsätta under våren 2025 för att möjliggöra fördjupningar inom vissa sakområden.

Försäkringskassan har precis som tidigare år använt sig av MSB:s cybersäkerhetskollen som stöd för att utvärdera informations- och cybersäkerhetsarbetet. Cybersäkerhetskollen består av två olika delar; infosäkkollen som innehåller utvärderingsunderlag avseende informationssäkerhet samt it-säkerhetskollen som innehåller utvärderingsunderlag avseende cybersäkerhet. Utvärderingsunderlagen har bidragit till att identifiera förbättringsområden inom informations- och cybersäkerhetsområdet men har även fungerat som ett bra verktyg för det interna samarbetet och dialogen kopplat till dessa områden.
För att göra cybersäkerhetskollen ännu mer användbar så finns en möjlighet till förbättring av resultat- och analysmodulen. Även utveckling av it-säkkollen i verktyget för att motsvara utformningen i infosäkkollen skulle skapa ytterligare värde i arbetet med uppföljning av informations- och cybersäkerhetsområdet.
Försäkringskassan kommer att arbeta vidare med resultatet och identifierade förbättringsområden inom ramen för det systematiska informationssäkerhetsarbetet, tillsammans med resultatet från övriga genomförda mätningar och uppföljningsresultat.

Beslut i detta ärende har fattats av generaldirektör Nils Öberg i närvaro av avdelningschef Stefan Blom och verksamhetsutvecklare Stefan Hultemar, den senare som föredragande.

Nils Öberg

Stefan Hultemar