Försäkringskassan

Datum
2023-03-20

Vår beteckning
FK 2023/001741

Svar på regeringsuppdrag

Informationssäkerhet

Försäkringskassan

Informationssäkerhet på Försäkringskassan

Ledningssystem för systematiskt informationssäkerhetsarbete

Försäkringskassan har fått i uppdrag att redogöra för hur myndigheten arbetat för att förvalta och utveckla sin informationssäkerhet och för hur myndigheten planerar för att möta framtida behov.

Försäkringskassans mål med rätt säkerhet innebär balans mellan att: kostnad och arbetsinsats för att efterleva säkerhetsreglerna är acceptabla, och att; incidenter inträffar med en allvarlighetsgrad och i en omfattning som kan tolereras. Balansen motsvarar Försäkringskassans riskaptit. Informationssäkerhet är en del av Försäkringskassans säkerhetsarbete.

Försäkringskassan har ett ledningssystem för säkerhet anpassat till standarden ISO/IEC 27001. Lämpligheten, tillräckligheten och verkan av ledningssystemet säkerställs genom arbete med ständiga förbättringar. Det görs bland annat genom mätningar, riskbedömningar och incidenthantering. Ledningssystemet utvecklas även genom anpassningar baserat på krav från anslutna myndigheter inom ramen för uppdraget med samordnad och säker statlig it-drift.

Försäkringskassan har inlett arbete med att ta fram nyckeltal för att kunna följa riskexponeringen inom cybersäkerhetsområdet och hur den motsvarar Försäkringskassans riskaptit.

Försäkringskassan har en process för riskhantering som omfattar kriterier för riskacceptans och bedömning av risker inom säkerhetsområdet. Riskanalyser genomförs regelbundet där risker med avseende på informationssäkerhet ingår som en del av verksamhetens samlade risker. Uppföljning och sammanställning av risker sker med hjälp av systemstöd.

Försäkringskassan har en process för hanteringen av incidenter. Försäkringskassan har under 2022 uppdaterat processen för incidenthantering med tillhörande anvisningar för att utveckla incidenthanteringen ytterligare.

Säkerhetskultur och säkerhetsmedvetande hos medarbetare

Säkerhet är en del av Försäkringskassans kultur. Varje medarbetare ska ha ett högt säkerhetsmedvetande och inse betydelsen av sin egen medverkan i ett effektivt skydd. Försäkringskassans medarbetare genomför en obligatorisk säkerhetsutbildning vartannat år som kompletteras med lärarledda utbildningar. Ytterligare krav på genomförda utbildningar finns inom särskilda områden, till exempel säkerhetsskydd eller hantering av skyddade personuppgifter.

Arbetet med att klassificera information som behandlas inom myndigheten fortsätter. Anvisningar för informationsklassning har uppdaterats med anpassningar utifrån verksamhetens behov och för att ge ökat stöd till hela verksamheten. Arbetet med att anpassa skyddet av information utifrån resultatet av genomförda informationsklassningar genomförs kontinuerligt för att nå målet om rätt säkerhet. Försäkringskassan arbetar kontinuerligt med att utveckla informationsklassningsmodellen tillsammans med säkerhetsåtgärderna för de olika nivåerna i modellen.

Den rättsliga styrningen och stödet har stärkts med ett ökat antal jurister som arbetar med dataskyddsfrågor där personalresurserna kommer att utökas ytterligare. Stöd och

styrning har tagits fram för att utföra konsekvensbedömningar enligt 35 artikeln i EU:s dataskyddsförordning.
Utbildningsinsatser har skett med lärarledda utbildningar avseende integritet och dataskydd.
En webbutbildning har skapats för att öka säkerhetsmedvetenheten hos systemutvecklare vid it-utveckling.

Under år 2023 kommer en digitaliseringsvägledning tas fram för att ge stöd för medarbetare inom Försäkringskassan som arbetar med verksamhetsutveckling. Vägledningen lägger fokus på digitalisering och de rättsfrågor som kan uppkomma i samband med utvecklingsinitiativ.

Genomförda och planerade insatser för att stärka informationssäkerhetsarbetet

Inom myndigheten pågår ett arbete för att utveckla det administrativa stödet för åtkomststyrning. Det innebär bland annat att hanteringen och uppföljning av åtkomsträttigheter till medarbetare har digitaliserats vilket medför bättre spårbarhet. Försäkringskassan kommer att utreda möjligheter till attributbaserad åtkomststyrning för att möta framtida krav och behov av Informationscentrisk åtkomststyrning.

Sedan maj 2022 finns möjligheten att använda BankID för att legitimera sig när man ringer till Försäkringskassans kundcenter. Legitimering via BankID sker i cirka 70% av samtalen.

En lösning för uppgiftsminimering har tagits fram som innebär att brev som skickas digitalt inte innehåller mottagarens adressuppgift. Syftet är att minimera konsekvensen om meddelandet kommit på avvägar. Cirka 18 miljoner digitala brev beräknas skickas utan adressuppgifter under 2023.

Försäkringskassan utvecklar kontinuerligt sitt arbetssätt för att möta informationspåverkan. En ny metod har tagits fram med stöd av bland annat Myndigheten för psykologiskt försvar.

Försäkringskassan fortsätter stärka sin operativa förmåga avseende robust och säker kommunikation i kris. I det arbetet ingår att säkerställa tillgång till kritisk information och på så sätt upprätthålla verksamheten.

Externa samarbeten som bidrar till förbättrad informationssäkerhet

Försäkringskassan deltar i flera myndighetsgemensamma samarbeten, bland annat eSam-programmet där flera initiativ syftar till att stärka informationssäkerheten. Försäkringskassan finns även representerad i arbetet med förvaltningsgemensam infrastruktur (ENA) och säkert utbyte av information. Uppdraget med säker statlig it-drift har förlängts. Även där kommer Försäkringskassans initiativ och säkerhetsarbete till nytta för andra myndigheter.

Försäkringskassan är sedan oktober 2022 sektorsansvarig myndighet för sektorn ekonomisk säkerhet. Sektorsansvaret innebär att Försäkringskassan leder arbetet med att samordna åtgärder både inför och vid fredstida krissituationer och höjd beredskap. I uppdraget ingår även att driva på arbetet inom beredskapssektorn, stödja beredskaps-myndigheterna och verka för att samordning sker med andra aktörer.

Försäkringskassan har tagit ett initiativ till samarbete inom cybersäkerhetsområdet där ett tiotal myndigheter ingår. Syftet är att stärka informationsdelning och arbetsmetodik i säkerhetsarbetet.

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

Nils Öberg

Stefan Hultemar