Datum
2018-01-29

Vår beteckning
042731-2017

Svar på regeringsuppdrag

Rapport – Försäkringskassans analys och bedömning av informationssäkerheten i den egna verksamheten

Försäkringskassans analys och bedömning av informationssäkerheten i den egna verksamheten

Försäkringskassan har, som bevakningsansvarig myndighet, av regeringen ålagts att analysera och bedöma informationssäkerheten i de delar av den egna verksamheten som är nödvändiga för att myndigheten ska kunna utföra sitt arbete. Vid genomförandet av uppdraget ska också krisberedskapsperspektivet samt planeringen för det civila försvaret beaktas.

Av redovisningen av uppdraget ska framgå hur myndigheten bedömer informationssäkerheten, vilka hot, sårbarheter och risker som har identifierats samt vilka åtgärder som har vidtagits, respektive kommer att vidtas, i syfte att reducera dessa.

Försäkringskassan redovisar härmed svaret på uppdraget.

Beslut i detta ärende har fattats av generaldirektör Ann-Marie Begler i närvaro av avdelningschef Sture Hjalmarsson, Eva Nordqvist, Gabriella Bremberg, Stefan Olowsson, Helena Östman, Marie Axelsson, Per-Arne Dahlberg, Alexandra Wallin, Ulrika Havossar, Per Eleblad, Lena Sandh, XXX, XXX, säkerhetschef Birgitta Målsäter och biträdande säkerhetsskyddschef Ola Sten, den senare som föredragande.

Ann-Marie Begler

Ola Sten

Innehåll

Bakgrund

Försäkringskassan har, som bevakningsansvarig myndighet, av regeringen ålagts att analysera och bedöma informationssäkerheten i de delar av den egna verksamheten som är nödvändiga för att myndigheten ska kunna utföra sitt arbete. Vid genomförandet av uppdraget ska också krisberedskapsperspektivet samt planeringen för det civila försvaret beaktas.

Av redovisningen av uppdraget ska framgå hur myndigheten bedömer informationssäkerheten, vilka hot, sårbarheter och risker som har identifierats samt vilka åtgärder som har vidtagits, respektive kommer att vidtas, i syfte att reducera dessa.

Uppdraget ska redovisas av de bevakningsansvariga myndigheterna var och en för sig till Regeringskansliet (respektive ansvarigt departement) samt till Myndigheten för samhällsskydd och beredskap senast den 1 mars 2018.

Disposition

Redovisningen följer det dispositionsstöd[1] som utfärdats av MSB.

[1] Dnr 2017-7116

Generellt om informationssäkerhet på Försäkringskassan

Försäkringskassan bedriver en verksamhet som har stor betydelse för medborgare och samhällsekonomi. Uppdraget är att administrera den svenska socialförsäkringen vilket medför att Försäkringskassans register innehåller en stor mängd personuppgifter samt att det dagligen betalas ut stora summor. Det innebär ett stort ansvar att trygga de försäkrades personliga integritet och ekonomiska trygghet med avseende på socialförsäkringssystemet.

Information som hämtas in och behandlas inom Försäkringskassan ska med stöd av lagar och förordningar samt med hjälp av särskilda åtgärder hanteras så att informationen:

- är skyddad mot obehörig åtkomst (Konfidentialitet)
- är korrekt, fullständig och aktuell (Riktighet)
- finns tillgänglig vid behov för den som behöver den (Tillgänglighet)
- och att dess användning kan härledas (Spårbarhet).

Hög informationssäkerhet är nödvändig för att allmänhet, företag och myndigheter ska ha förtroende för den information som Försäkringskassan hanterar.

Ledningssystem och ramverk för säkerhet

Försäkringskassan har ett ledningssystem för säkerhet anpassat till standarden ISO/IEC 27001.

Riskbaserat angreppssätt

Försäkringskassans mål är att minimera risker på ett kostnadseffektivt sätt. Beslut om säkerhetsnivåer och skyddsåtgärder ska alltid baseras på en formell riskanalys. För informationstillgångar ska risker identifieras och hanteras med avseende på konfidentialitet, riktighet, tillgänglighet och spårbarhet.

Kontinuitetsplaner finns eller ska tas fram för samtliga verksamhetskritiska produktions- och stödprocesser. En plan ska också finnas för att hantera allvarliga kriser och incidenter.

Försäkringskassans informationstillgångar

Försäkringskassan har informationstillgångar som är skyddsvärda och som är samhällsviktiga. Bland annat hanterar Försäkringskassan uppgifter kring personer med skyddade identiteter.

Det finns även information vid Försäkringskassan som har bedömts som hemlig uppgift enligt säkerhetsskyddslagen (1996:627) och offentlighets- och sekretesslagen (2009:400).

Pågående aktiviteter

Försäkringskassan har identifierat ett behov av att tydligare integrera standarden ISO/IEC 27 000 samt underliggande standarder i det befintliga ramverket för säkerhet. Ett projekt genomförs för att enligt nämnd standard klassificera Försäkringskassans informationstillgångar. Förändringarna förväntas leda till ökad

tydlighet, förbättrad uppföljning samt bättre möjlighet att samverka med andra myndigheter som följer samma standard.

Hotbild i ett normalläge

I hotbildsanalyser vid Försäkringskassan ska samtliga hot som deklareras i ISO/IEC 27005:2013 beaktas. Följande hot har identifierats som de mest aktuella och/eller de mest allvarliga gentemot Försäkringskassans informationstillgångar. Hänsyn har tagits till de fyra skyddsbehoven, sekretess, riktighet, tillgänglighet och spårbarhet.

Ett hot har definierats som en möjlig, oönskad händelse med negativa konsekvenser för verksamheten[2]. Hoten ska klassificeras enligt MSB:s dispositionsförslag[3]:

- Ingen eller försumbar
- Måttlig
- Betydande
- Allvarlig

Samtliga hot som presenteras nedan har klassificerats som allvarliga.

Hotkällor

De hot/hotaktörer som definieras nedan återfinns i ISO/IEC 27005:2013.

- Naturfenomen
- Hacker
- Terrorist
- Brottslingar inkl. organiserad brottslighet
- Främmande makt
- Interna hot

Det finns olika tillvägagångssätt och drivkrafter bakom hot och hotaktörernas agerade som kräver särskild bevakning för att kunna se förändringar i hotbilden. Bevakning av dessa sker genom omvärldsbevakning.

Hot

Rubrik	Förlust av viktiga tjänster som berör IT-drift
Beskrivning	• Funktionsfel i luftkonditionering vatten etc. • Strömförsörjning • Funktionsfel kommunikationstjänster
Relation till hotet	IT-drift är centralt för att Försäkringskassan skall kunna utföra sitt myndighetsuppdrag. Förlust av viktiga tjänster är hot som är högst aktuellt för Försäkringskassan. Hoten hanteras förebyggande och med omfattande skyddsåtgärder.
Förändrad bedömning Vid kris och höjd beredskap	Hoten kvarstår med hög prioritet.

[2] Terminologi för informationssäkerhet, SIS-TR 50:2015
[3] Redovisning av regeringsuppdrag att analysera och bedöma informationssäkerhet i den egna verksamheten, MSB 2017-7116

Rubrik	Fysisk skada
Beskrivning	• Brand • Omfattande vattenskada • Sabotage och Terrorism
Relation till hotet	Hoten hanteras förebyggande och med omfattande skyddsåtgärder.
Förändrad bedömning Vid kris och höjd beredskap	Vid en ökad hotbild från främmande makt ökar sannolikheten för fysisk skada gentemot verksamheten.

Rubrik	Obehörig åtkomst till system
Beskrivning	• Olaga intrång i IT-system • Otillåten påverkan gentemot personal • Medveten överträdelse av interna rutiner • Omedveten överträdelse av interna rutiner
Relation till hotet	Försäkringskassan utsätts frekvent av hot av denna karaktär. Hoten hanteras förebyggande och med omfattande skyddsåtgärder.
Förändrad bedömning vid kris och höjd beredskap	Vid en ökad hotbild från främmande makt ökar sannolikheten för försök till obehörig åtkomst.

Rubrik	Tekniska fel
Beskrivning	• Utrustningsfel • Icke fungerande utrustning • Överbelastning i informationssystemet • Icke fungerande programvara • Brist i ett informationssystem
Relation till hotet	I en komplex verksamhet krävs ett ständigt underhåll och övervakningsarbete för att bibehålla en säker drift.
Förändrad bedömning vid kris och höjd beredskap	Hoten kvarstår med hög prioritet

Risker i ett normalläge

Följande hot har identifierats som de mest aktuella och/eller de mest allvarliga gentemot Försäkringskassans informationstillgångar. Hänsyn har tagits till de fyra skyddsbehoven, konfidentialitet, riktighet, tillgänglighet och spårbarhet.

Samtliga risker bedöms som allvarliga.

Titel	Brand eller annan ödeläggelse av driftcentral
Beskrivning	En omfattande brand eller annan ödeläggelse som leder till total förstörelse av infrastruktur, system och data.
Konsekvens	Minskar Försäkringskassans redundans och möjlighet att hantera störningar i övriga IT-infrastrukturen.
Vidtagna åtgärder	• Systematiskt brandskyddsarbete • Brandlarm och släckningssystem i driftcentraler • Redundanta system på olika geografiska platser
Planerade åtgärder	
Förändrad bedömning Vid kris och höjd beredskap	Antal hot som kan leda till brand ökar vid kris och höjd beredskap vilket gör att sannolikheten ökar.

Titel	Omfattande strömavbrott för större kontor
Beskrivning	Ett strömavbrott som påverkar ett eller flera av Försäkringskassans större kontor där handläggning bedrivs under en längre tid.
Konsekvens	Handläggningskapaciteten kan komma att påverkas i större omfattning.
Vidtagna åtgärder	• Handläggning är nationellt spridd för ett flertal förmåner • Reservkraft finns på ett fåtal platser.
Planerade åtgärder	Anpassning av möjligheten till reservkraft på större handläggningskontor. Översyn av vissa förmåner för att skapa större nationell spridning och redundant kompetens.
Förändrad bedömning vid kris och höjd beredskap	Sannolikheten för längre strömavbrott ökar med den ökade hotbilden.

Titel	Omfattande strömavbrott, driftcentral
Beskrivning	Ett strömavbrott som påverkar samtliga driftcentraler.
Konsekvens	IT-drift är inte möjlig utan strömförsörjning vilket leder till att Försäkringskassans interna och externa system inte längre kommer vara tillgängliga.
Vidtagna åtgärder	• Reservkraft i driftcentraler • Avtal om drivmedelsförsörjning • Regelbundna tester av reservkraftsystem
Planerade åtgärder	Anpassning av planeringen för reservkraft utifrån totalförsvarets krav.
Förändrad bedömning vid kris och höjd beredskap	Sannolikheten för längre strömavbrott ökar med den ökade hotbilden. Uthållighetskraven ökar.

Titel	Missbruk av höga IT-behörigheter
Beskrivning	Medarbetare med administratörsrättigheter orsakar skada i system, gentemot infrastruktur eller otillbörligt tar del av information.
Konsekvens	Kan leda till driftavbrott eller till att känslig information sprids, används för kriminella ändamål eller delges främmande makt.
Vidtagna åtgärder	• Behörighetsstyrning • Begränsa fysisk åtkomst till viktiga system • Uppdaterade riktlinjer för behörighet, styrning och ansvar • Mönstersökning för att upptäcka avvikelser • Riktlinjer om hantering av misstänkta överträdelser
Planerade åtgärder	Tydligare informationsklassning möjliggör mer restriktiv åtkomst till känslig data. Löpande utvärdering och korrigering av behörighetsstyrning.
Förändrad bedömning vid kris och höjd beredskap	Vid höjd beredskap blir främmande makt en tydlig antagonist som sannolikt kommer försöka använda personal vid Försäkringskassan för att kunna påverka socialförsäkringen.

Titel	Otillåten påverkan mot medarbetare med omfattande behörighet
Beskrivning	Medarbetare används som brottsverktyg för att påverka infrastruktur, system eller data.
Konsekvens	Stöld av känslig information samt påverkan på socialförsäkringen kan vara systemhotande verksamhet. Brottslighet i syfte att ge ekonomiska fördelar kan hota förtroendet för Försäkringskassans hantering av socialförsäkringen.
Vidtagna åtgärder	• Information och särskild säkerhetsutbildning för chefer • Sekretess kring handläggare med åtkomst till skyddsvärda uppgifter • Övning av krisledning vid otillåten påverkan • Särskilda krav för priviligierade behörigheter • Dygnet runt bemannad stödtelefon • Obligatorisk webbaserad säkerhetsutbildning med krav på repetition vart annat år • Särskilda krav för priviligierade behörigheter gentemot avdelning, chef och medarbetare.
Planerade åtgärder	Kontinuerlig utbildning i säkerhetsskydd för IT-avdelningen
Förändrad bedömning vid kris och höjd beredskap	Vid höjd beredskap blir främmande makt en tydlig antagonist som sannolikt kommer att försöka använda personal vid Försäkringskassan för att kunna påverka socialförsäkringen.

Titel	Intrång i IT-miljö
Beskrivning	Externt IT-intrång i Försäkringskassans IT-infrastruktur.
Konsekvens	Vid ett IT-intrång kan en person med brottsligt uppsåt eventuellt få tillgång till information som är känslig för Försäkringskassans verksamhet eller enskilda medborgares socialförsäkringsdata. Vidare skulle en angripare med djupare kunskaper kunna påverka drift och tillgänglighet för system som är kritiska för Försäkringskassans drift.
Vidtagna åtgärder	Försäkringskassan har ett omfattande IT-säkerhetsarbete och en löpande bevakning och hantering av säkerhetsrelaterade incidenter.
Planerade åtgärder	IT-säkerhetsarbetet omfattas av en kontinuerlig förbättringsprocess med mål att minska antalet inträffade incidenter samt dess konsekvenser.
Förändrad bedömning vid kris och höjd beredskap	Cyberangrepp förväntas öka vid en ökad antagonistisk hotbild.

Titel	Otillåten åtkomst av hemliga uppgifter i IT-miljö
Beskrivning	En obehörig kommer åt uppgifter som är hemliga.
Konsekvens	För att en uppgift ska bedömas som hemlig måste rikets säkerhet vara hotad om den röjs.
Vidtagna åtgärder	Försäkringskassan följer säkerhetsskyddslagen och har vidtagit signalskyddsåtgärder för att skydda data som bedömts hemlig.
Planerade åtgärder	Löpande utvärdera vilken data som kan hota rikets säkerhet samt pröva tidigare bedömningar.
Förändrad bedömning vid kris och höjd beredskap	Vid höjd beredskap blir främmande makt en tydlig antagonist som sannolikt kommer att försöka använda personal vid Försäkringskassan för att kunna påverka socialförsäkringen.

Tillkommande hot och risker vid ett krisläge

Ingen generell hot eller riskbildsförändring utifrån ett krisläge. Vid specifika samhällskriser kommer delar av de identifierade riskerna bli mer aktuella och skyddsåtgärderna kommer behöva förstärkas.

Tillkommande hot och risker i höjd beredskap

Hot

Rubrik	Störning på grund av strålning
Beskrivning	Elektromagnetisk puls som kan skada elektronisk utrustning. Radioaktiv strålning som följd av ett kärnvapenangrepp.
Relation till hotet	Hotbilden beaktas inom ramen för långsiktiga satsningar kopplat till totalförsvaret. Tillgång till skyddsutrustning bedöms hanteras enligt en prioritering som görs myndighetsgemensamt om behovet aktualiseras.

Risker

Titel	Sabotage
Beskrivning	Förstör eller skadar egendom som har betydelse för rikets försvar, folkförsörjning, rättsskipning eller förvaltning eller för upprätthållande av allmän ordning och säkerhet.
Konsekvens	Kan påverka Försäkringskassans förmåga att administrera socialförsäkringen.
Vidtagna åtgärder	Sabotage kan inträffa i fredstid men risken förväntas öka vid höjd beredskap. Ett proportionerligt skydd finns men bygger på att det inte finns en hotbild från främmande makt. Idag pågår en utredning över vilka åtgärder som behöver vidtas för att bygga ett skydd som svarar upp mot den nya hotbilden.
Planerade åtgärder	Löpande utvärderas vilka åtgärder som behöver vidtas för att skydda Försäkringskassans, och andra myndigheters, samhällsviktiga verksamhet. Inkluderar totalförsvarets krav i utvecklingsuppdrag och infrastruktursatsningar.

Titel	Spionage och olovlig underrättelseverksamhet mot Sverige
Beskrivning	Inhämtar information i syfte att överlämna till främmande makt,
Konsekvens	Påverkan på rikets säkerhet
Vidtagna åtgärder	Spionage kan inträffa i fredstid men risken förväntas öka vid höjd beredskap. Ett proportionerligt skydd finns men bygger på att det inte finns en hotbild från främmande makt. Försäkringskassan följer säkerhetsskyddslagen och har vidtagit signalskyddsåtgärder för att skydda data som bedömts hemlig.
Planerade åtgärder	Löpande utvärdera vilken data som kan hota rikets säkerhet samt pröva tidigare bedömningar.