ARBETSFÖRMEDLINGEN
SWEDISH PUBLIC EMPLOYMENT SERVICE

Informations- och cybersäkerhet

Återrapport 2024

Arbetsförmedlingen
Författare: Per-Anders Ode, Lisa Karlsson, Gabor Sebastiani, Kim Nilsson, Jan Jonasson
Datum: 2024-10-01
Diarienummer: Af-2024/0050 5456

Förord

Rapporten har tagits fram med anledning av följande uppdrag i Arbetsförmedlingens regleringsbrev för 2024:

Uppdrag 3.5 Informations- och cybersäkerhet
Arbetsförmedlingen ska senast den 1 oktober 2024 till Regeringskansliet (Arbetsmarknadsdepartementet) övergripande redogöra för hur myndigheten arbetat för att förvalta och utveckla sin informationssäkerhet och för hur den planerar för att möta framtida behov. Arbetsförmedlingen ska särskilt:

- *Genomföra en utvärdering av det egna informationssäkerhetsarbetet genom exempelvis Myndigheten för samhällsskydd och beredskaps verktyg Infosäkkollen, samt redovisa vilka åtgärder som vidtagits eller planerats med anledning av resultatet.*
- *Redogöra för vilka åtgärder som har vidtagits för att öka förmågan att identifiera och rapportera it-incidenter, samt för att skyndsamt kunna vidta nödvändiga åtgärder.*
- *Genomföra en analys av om hot och sårbarheter för myndigheten förändrats i och med det rådande omvärldsläget, samt redogöra för om åtgärder vidtagits eller planerats för att minska eventuella identifierade risker med anledning av detta.*

Beslut i ärendet har fattats av vikarierande överdirektör Thomas Hagman. Ärendet har föredragits av Per-Anders Ode, VO It. Övriga som deltagit i den slutliga handläggningen är Krister Dackland, verksamhetsområdeschef VO It, samt Per Gauffin, VO It. Beslutet är fastställt digitalt i Diariet och saknar därför namnunderskrifter.

Thomas Hagman

Vikarierande överdirektör

Per-Anders Ode

Verksamhetscontroller

Innehåll

1 Sammanfattning

För att upprätthålla och förstärka informationssäkerhetsskyddet arbetar Arbetsförmedlingen kontinuerligt med sitt systematiska informationssäkerhetsarbete. Sedan flera år finns en organisatorisk funktion på myndigheten med specialister inom informations- och cybersäkerhet som arbetar med att förvalta och utveckla myndighetens informationssäkerhet.

Myndigheten har sedan tidigare identifierat behovet av att förtydliga informationsägarens roll och ansvar. Det är en grundförutsättning för att stärka systematiken i informationssäkerhetsarbetet. Ett arbete pågår med att utveckla och förtydliga verksamhetens informationsägarskap och säkerställa gemensamma sätt att hantera information på ett informations- och rättssäkert sätt. Myndigheten planerar att flytta informationsägarskapet från it-verksamheten till chefer med verksamhets- och riskansvar. Åtgärden planeras vara genomförd 1 januari 2026.

Två nya EU-direktiv, NIS2 och CER, syftar till att uppnå en hög gemensam cybersäkerhetsnivå i hela Europeiska unionen. Myndighetens informationssäkerhetsarbete utgår från ISO-standarder samt MSB:s föreskrifter och går väl i linje med direktivens intentioner men kommer behöva kompletteras.

För utvärderingen av informationssäkerhetsarbetet har vi använt MSB:s verktyg Infosäkkollen. Inom flera arbetsområden har vi sedan tidigare identifierat ett antal brister och har pågående aktiviteter. Vi har också identifierat ett antal nya förbättringsområden: ledningens styrning och kontroll, uppföljning och utvärdering av arbetssätt, undersökning av kunskap och tillämpning av kunskapen, kontinuitetshantering samt inventering av informationsmängder och informationssystem.

Myndigheten har en tydlig process för hantering av it-incidenter. Vår bedömning är att benägenheten att anmäla incidenter är hög. Incidenthanteringen är en del av arbetet med kontinuerliga förbättringar. Vi förbättrar ständigt förmågan att förebygga och upptäcka incidenter. Det handlar dels om att anmäla incidenter, dels om att söka efter felaktigheter och att bevaka it-driften.

Omvärldsbevakning inom informationssäkerhetsområdet sker löpande och tillgängliggörs internt för myndighetens anställda. Fokus i kommunikationen ligger på vilka förändringar myndigheten bör driva med anledning av omvärldsförändringarna. Vi ser primärt tre områden som påverkas i hög grad till följd av det förändrade omvärldsläget: cyberangrepp, insiderbrott och påverkanskampanjer.

Insiderproblematik, med efterföljande personalsäkerhetsfrågor, är alltmer relevant och kommer behöva omfatta även områden utanför säkerhetsskydd. Här ser vi ett behov hos myndigheten att förstärka kunskap, rutiner och processer.

2 Metod och genomförande

2.1 Disposition

Rapporten har strukturerats utifrån de frågeställningar som ingår i redovisningen av uppdraget.

I kapitel tre redovisar vi arbetet med att förvalta och utveckla informationssäkerhet.

I kapitel fyra redovisas resultat från utvärderingen av informationssäkerhetsarbetet.

I kapitel fem redovisar vi hanteringen av it-incidenter.

I kapitel sex redovisar vi hur myndigheten påverkas av och agerar på omvärldsförändringar.

2.2 Metod

Avseende förvaltning och utveckling av informationssäkerhet har kartläggningar genomförts av pågående initiativ och stämts av med berörda verksamheter. För utvärderingen av informationssäkerhetsarbetet har vi använt MSB:s verktyg Infosäkkollen som är en del av Cybersäkerhetskollen.[1] Svar har samlats in genom intervjuer och workshops med representanter från olika delar av myndigheten.

I beskrivningen av hantering av it-incidenter har vi utgått från myndighetens incidenthanteringsprocess. Avseende analys av hot och sårbarhetsläget har vi utgått från och kompletterat den analys som genomfördes och beskrevs i återrapporten om informationssäkerhet 2023.[2] Daglig omvärldsbevakning genomförs också för att hålla myndigheten uppdaterad inför nya risker och hot samt för ökad intern säkerhetsmedvetenhet.

2.3 Koppling till tidigare återrapport

I återrapporten om informationssäkerhet 2023 redogjorde myndigheten för åtgärder som vidtagits respektive planerades att vidtas med anledning av uppdraget i regleringsbrevet 2023. I denna återrapport redogör vi för hur vi har fortsatt att förvalta och utveckla informationssäkerhetsarbetet (se kapitel 3). Vi redogör också för hur den analys av omvärldsförändringar som gjordes 2023 har utvecklats under 2024 (se kapitel 6).

[1] Cybersäkerhetskollen (msb.se)
[2] Informationssäkerhet - Arbetsförmedlingen (arbetsformedlingen.se)

3 Förvaltning och utveckling av informationssäkerhet

3.1 Inledning

I en omvärld där hotbilden mot samhällsviktiga verksamheter fortsätter att öka och säkerhetskraven är höga, är arbetet med informationssäkerhet särskilt viktigt. För att upprätthålla och förstärka skyddet arbetar myndigheten kontinuerligt med sitt systematiska informationssäkerhetsarbete.

Sedan flera år finns en organisatorisk funktion på myndigheten med specialister inom informations- och cybersäkerhet som arbetar med att förvalta och utveckla myndighetens informationssäkerhet. Säkerhetsplattformar för centrala och specialiserade säkerhetsförmågor såsom övervakning, loggning, behörighetshantering och incidenthantering är implementerade sedan tidigare.

3.2 Pågående initiativ

Omvärldsbevakning inom informationssäkerhetsområdet sker löpande och tillgängliggörs internt för myndighetens anställda. En sammanställning tas fram kvartalsvis och omfattar det rådande omvärldsläget och förändringar i hot och attackvektorer allmänt, såväl som specifikt mot Arbetsförmedlingen. Sammanställningen innehåller även analys av den närmaste framtiden där fokus i kommunikationen ligger på vilka förändringar myndigheten bör driva med anledning av omvärldsförändringarna.

Arbetsförmedlingen har sedan tidigare identifierat behovet av att förtydliga informationsägarens roll och ansvar. Det är en grundförutsättning för att stärka systematiken i informationssäkerhetsarbetet. Myndigheten arbetar med att utveckla och förtydliga verksamhetens informationsägarskap och säkerställa gemensamma sätt att hantera information på ett informations- och rättssäkert sätt. Myndigheten planerar att flytta informationsägarskapet från it-verksamheten till chefer med verksamhets- och riskansvar. Åtgärden planeras vara genomförd 1 januari 2026.

Arbetet med handlingsplan för ledningssystem för informationssäkerhet (LIS) fortlöper. Myndighetens arbete utgår från krav i enlighet med MSB:s föreskrifter om informationssäkerhet för statliga myndigheter[3] samt med stöd av ISO 27000-serien. Förtydligande av krav och implementering av säkerhetsprocesser bygger på tvärfunktionellt samarbete i organisationen. Arbete pågår bland annat med att förtydliga stöd och styrning för roller och ansvar inom informationssäkerhet samt fastställande av stöd och styrning rörande fysisk säkerhet och personalsäkerhet. Vi arbetar också med att ta fram krav för säker it-utveckling samt tydliggörande av informationssäkerhetskrav i leverantörsstyrning. Ledningens genomgång[4] har avrapporterats till Generaldirektörens ledningsgrupp. Syftet är att informera

[3] MSBFS 2020:6
[4] ISO/IEC 27001:2022, Avsnitt 9.3

myndighetsledningen om informationssäkerhetsarbetet, i enlighet med föreskriftskrav.[5]

Myndighetens process för it-utveckling och inköp av tjänster och produkter består av flera delprocesser med syfte att stötta olika initiativs informationssäkerhetsarbete. Processen har tillämpats och utvecklas kontinuerligt sedan 2019 och omfattar bland annat informationsklassning, hot- och riskanalys och laglighetsbedömning samt uppföljning av utestående säkerhetsåtgärder. Processen sker tvärfunktionellt mellan it-verksamheten, förmedlingsverksamheten, rättsavdelningen och inköpsavdelningen.

Myndigheten har flera interna utbildningar inom informationssäkerhet och säkerhetsmedvetenhet, en av dessa är MSB:s grundutbildning DISA.[6] Sedan 2023 genomförs även mikroutbildningar[7] i syfte att höja medvetenheten om hur man hanterar information i vardagen på ett säkert sätt. Mikroutbildningarna innehåller förberedda och oförberedda tester för att kontinuerligt utbilda och höja medarbetarnas säkerhetsmedvetenhet.

Antalet arbetssökande med skyddade personuppgifter (SPU) ökar kontinuerligt. Myndigheten arbetar löpande med att skydda dessa personer och deras information samtidigt som vi tillgängliggör digitala tjänster för medborgare som har eller får skyddade personuppgifter. Genom införandet av en nationell geografisk funktion och ett utpekat helhetsansvar har myndigheten under året påbörjat skapandet av en sammanhållen och enhetlig styrning, ledning och kontroll av hanteringen av denna kundkategori. I ansvaret ingår bland annat att säkra verksamhetsprocesser samt kommunikationsvägar mellan arbetssökande, myndigheten och samverkanspartners.

Arbetsförmedlingen är sedan 2022 en beredskapsmyndighet och har två uppdrag: att betala ut ersättningar till enskilda och att stå för personalförsörjning till totalförsvaret. Arbetet med uppdragen bidrar till förstärkning av informations-säkerheten särskilt avseende robusthet och kontinuitetshantering, till exempel genom tekniska förbättringar.

3.3 Planering för att möta framtida behov

Två nya EU-direktiv, NIS2 och CER, syftar till att uppnå en hög gemensam cybersäkerhetsnivå i hela Europeiska unionen. NIS2 införlivas i en ny lag, cybersäkerhetslagen från 1 januari 2025. I september 2024 lämnas förslag om införlivning av CER-direktivet. Myndighetens informationssäkerhetsarbete utgår från ISO-standarder samt MSB:s föreskrifter och går väl i linje med direktivens intentioner men kommer behöva kompletteras efter mer utförlig analys.

Vi ser att ökningen av informationssäkerhetshot kräver samverkan mellan myndigheter och leverantörer. Vilket är en förutsättning för att kunna hushålla med offentliga medel och dra nytta av och dela på den gemensamma kompetens som finns

[5] MSBFS 2020:6, §15
[6] Digital informationssäkerhetsutbildning för alla (Disa) (msb.se)
[7] Mikroutbildning är en utbildningsmetod som handlar om att lära sig ny information i små korta enheter.

inom myndighetssverige. Några exempel på områden där samordningsvinster bör vara möjliga: synen på artificiell intelligens juridiskt och säkerhetsmässigt, möjligheterna att kunna använda molntjänster från globala marknadsledande leverantörer samt kontroll och uppföljning för att motverka välfärdsbrott.

Myndighetens utmaningar kring de legala möjligheterna för utkontraktering av it-tjänster kvarstår från föregående år. EU:s adekvansbeslut och den sekretessbrytande bestämmelsen[8] från 2023 är möjliggörande i viss mån. Utmaningen ligger i att identifiera lösningar för utkontraktering som är lagliga och samtidigt ekonomiskt fördelaktiga jämfört med drift i egen regi. Myndigheten arbetar med att utreda möjligheter att ur ett rättsligt och informationssäkert perspektiv kunna nyttja utkontraktering till utländska leverantörer.

Utbetalningsmyndighetens övergripande uppdrag är att förebygga, förhindra och upptäcka felaktiga utbetalningar från välfärdssystemet. Från och med april 2024 förser Arbetsförmedlingen Utbetalningsmyndigheten med data i en första leverans. Arbetsförmedlingens samverkan med Utbetalningsmyndigheten bedrivs i spåren dataanalys, granskning och återkoppling (underrättelser) samt transaktionskonto.

Insiderproblematik, med efterföljande personalsäkerhetsfrågor, är alltmer relevant och kommer behöva omfatta även områden utanför säkerhetsskydd. Här ser vi ett behov hos myndigheten att förstärka kunskap, rutiner och processer.

[8] Offentlighets- och sekretesslag, Kap 10 §2a

4 Utvärdering genom Infosäkkollen

4.1 Metod

För utvärderingen av informationssäkerhetsarbetet har vi använt MSB:s verktyg Infosäkkollen som är en del av Cybersäkerhetskollen[9]. Svar har samlats in genom intervjuer och workshops med representanter från olika delar av myndigheten. Vi har också granskat styrande och vägledande dokument. Resultatet ger oss en indikation om vad myndigheten behöver förstärka inom informationssäkerhets-arbetet. Mätperioden är september 2022 – augusti 2024.

4.2 Analys

Myndigheten arbetar löpande med att förbättra och förstärka förmågan inom informationssäkerhet, exempel på områden som vi arbetar med tas upp i kapitel 3. Infosäkkollen visar dock på ytterligare förbättringsområden som till exempel:

- Ledningens styrning och kontroll
- Undersökning av kunskap och tillämpning av kunskapen inom informationssäkerhet
- Uppföljning och utvärdering av arbetssätt inom informationssäkerhet
- Kontinuitetshantering
- Inventering av informationsmängder, informationssystem och nätverk

Avseende ledningens styrning och kontroll så har vi styrande och vägledande dokument på plats. Ledningen informerar sig löpande om området. Det framkommer i intervjuer att det är viktigt att styrningen kommuniceras bättre ut i organisationen för att vi ska få en utveckling inom området. Det kan till exempel handla om målbild för informationssäkerhetsarbetet. Området handlar även om att förtydliga roller och ansvar samt stöd och styrning inom informationshantering. Här har vi redan ett pågående arbete avseende förtydligande av informationsägarskap (se avsnitt 3.2 Pågående initiativ).

Som beskrivs i kapitel 3 så finns det utbildningar och kunskapshöjande initiativ inom informationssäkerhet. Ett utvecklingsområde är mätning och uppföljning av insatserna med syfte att undersöka om medarbetarna använder sina kunskaper efter genomförd utbildning i informationssäkerhet. En planerad åtgärd är att göra vissa utbildningar obligatoriska för samtliga anställda.

Myndigheten behöver förstärka den systematiska uppföljningen och utvärderingen av arbetssätt inom informationssäkerhet. Resultatet visar att vi i de flesta fall inte följer upp och utvärderar våra arbetssätt. Ett undantag är arbetssättet för incident-hantering där det finns en rutin för uppföljning och utvärdering (se kapitel 5).

[9] Cybersäkerhetskollen (msb.se)

Arbetet med kontinuitetshantering behöver utvecklas för att nå en högre nivå. Kontinuitetsplaner finns framtagna inom vissa delar av verksamheten, exempelvis är det en del av arbetet med beredskapsmyndighet, men det saknas en organisationsgemensam modell.

Resultatet från Infosäkkollen visar att vi kan förbättra arbetssättet avseende inventering. Det finns olika initiativ men vi kan inte med säkerhet säga i vilken omfattning det har gjorts en inventering av samtliga delar det vill säga informationsmängder och informationssystem inklusive nätverk.

4.3 Planerade åtgärder

Nedan beskrivs övergripande åtgärder med anledning av resultatet:

- Myndigheten planerar att flytta informationsägarskapet från it-verksamheten till chefer med verksamhets- och riskansvar. Åtgärden planeras vara genomförd 1 januari 2026.
- Myndigheten planerar att tillsätta en oberoende roll som har förmåga att leda och samordna informationssäkerhetsarbetet, samt kan vara såväl kravställande som granskande.
- Tydligare involvering från ledningen till exempel genom beslut om målbild och åtgärdsplan.
- För att öka medvetenheten inom informationssäkerhet kommer MSB:s DISA-utbildning samt myndighetens interna mikroutbildningar att bli obligatoriska för myndighetens chefer och medarbetare.
- Utveckling av process för uppföljning och utvärdering av arbetssätt inom informationssäkerhet.
- Utveckling och etablering av myndighetens modell för kontinuitetshantering.
- Utveckling av arbetssätt för inventering av informationsmängder, informationssystem och nätverk.

5 Hantering av it-incidenter

5.1 Inledning

Myndigheten har en tydlig process för it-incidenter i enlighet med ITIL[10]. Incidenter ska anmälas av medarbetare så snart en incident upptäcks. It-stöd finns för anmälan och hantering av incidenter. Medarbetarna får regelbundet och har kontinuerligt tillgång till utbildning för incidentanmälan. Utifrån jämförelse med andra myndigheter, inom ramen för eSam[11], är vår bedömning att benägenheten att anmäla incidenter är hög.

Förutom en process för it-incidenter har vi även processer för kritiska it-incidenter och för krishantering (aktiverad samordningsstab). En incident kan under ärendets gång eskaleras och de-eskaleras mellan dessa processer. Det finns en tydlig styrnings- och ansvarsstruktur för varje process och för övergången mellan processerna.

Incidentprocessen består i huvudsak av stegen: upptäckt incident rapporteras, kompletterande information samlas in, felkälla identifieras, felkälla åtgärdas och åtgärdens effekt verifieras.

5.2 Proaktivt lärande

Incidenthanteringen ingår i en större helhet som utgör myndighetens arbete med kontinuerliga förbättringar. Vi förbättrar ständigt förmågan att upptäcka incidenter. Förutom att medarbetare, arbetssökande och leverantörer kan upptäcka incidenter, arbetar vi proaktivt med att söka efter felaktigheter och bevaka it-driften med förmågor som: logganalys, Security operation center (SOC), Operation center (driftövervakning) och sårbarhetsscanning.

Incidentärendet i sig kan eskaleras och de-eskaleras mellan nivåerna Incident, Kritisk incident och Krisledning. I incidentprocessen hanteras även myndighetens rapporteringsskyldighet till andra myndigheter och anmälan om misstanke om brott till brottsutredande myndigheter.

För återkommande incidenter som riskerar att ge större konsekvenser för medborgare, leverantörer, myndigheten eller som riskerar myndighetens efterlevnad, genomförs en djupare grundorsaksanalys. Analysen genererar åtgärder som syftar till att minska sannolikheten för återkommande incidenter, alternativt minska konsekvenserna av dem. Utöver felkällor och grundorsaker följs även incidenthanteringen upp efter större incidenter. Syftet är att utveckla hanteringen samt att vi ska bli skickligare och mer effektiva utifrån de egna lärdomarna. Arbetssättet ledde exempelvis till att myndigheten kunde identifiera hanteringen av skyddade personuppgifter som ett förbättringsområde.

Incidentprocessen – från att upptäcka incidenter till att lösa ut dem, analysera och förebygga framtida incidenter – kan ses som repetitiv då varje incident leder till att

[10] Information Technology Infrastructure Library (ITIL) är en samling principer för hantering av it-tjänster.
[11] Offentlig samverkan för ökad digitalisering

sannolikheten för att samma incident ska inträffa igen minskar. Därmed agerar myndigheten proaktivt med hjälp av kunskap från egna lärdomar.

5.3 Genomförda åtgärder

Medarbetarna genomför utbildningar om incidentprocessen och it-stödet för incidentanmälan. Myndigheten upplever generellt en hög benägenhet att rapportera incidenter. Det finns enstaka exempel på att incidenter inte har rapporterats tillräckligt fort, men endast i undantagsfall har anmälningsplikten till Integritetsskyddsmyndigheten (IMY) inte kunnat hållas inom 72 timmar[12].

Myndigheten har, med målet att minimera risker vid förändringar i it-system, infört en Change Advisory Board (CAB) och satt gemensamma krav som måste uppfyllas innan en förändring får genomföras i it-miljön. Det bidrar också till dokumentation om vilka ändringar som införs och vid vilken tidpunkt. Med hjälp av detta kan vi spåra oväntade negativa effekter av en release och vilken förändring som föranlett problemet.

It-stödens servicenivå (SLA)[13] följs upp löpande. Om tillgänglighetskraven inte uppfylls, genomförs en djupare utredning av bakomliggande orsaker.

Vi har en driftövervakning (Operation Center). Med hjälp av övervakning upptäcks om någon tjänst inte fungerar och incidentprocessen kopplas in.

Vi har byggt en förmåga att utföra sårbarhetsskanning. Myndigheten prenumererar på kända sårbarheter och utför även egen omvärldsbevakning.

Vår förmåga att proaktivt upptäcka incidenter har förstärkts genom logganalys och Security Operation Center (SOC). Genom realtidsnära analys av loggar kan felaktigt beteende fångas och incidentprocessen kopplas in.

[12] Personuppgiftsincidenter | IMY
[13] Service Level Agreement (SLA) är en överenskommelse för en produkts servicenivå.

6 Analys av hot och sårbarhetsläget

6.1 Inledning

Ett alltmer försämrat säkerhetsmässigt omvärldsläge, Sveriges medlemskap i NATO samt kriminella nätverks framflyttade positioner, ställer högre krav på myndighetens informationssäkerhet. Myndigheten ser, som beskrivet i tidigare återrapport[14], primärt tre områden som påverkas i hög grad till följd av det förändrade omvärldsläget: cyberangrepp, insiderbrott samt påverkanskampanjer. Insiderproblematik, med efterföljande personalsäkerhetsfrågor, är alltmer relevant och kommer behöva omfatta även områden utanför säkerhetsskydd.

Vidtagna och planerade åtgärder är av säkerhetsskäl beskrivna på en övergripande nivå för att inte motverka åtgärdernas syften.

6.2 Analys och åtgärder

6.2.1 Cyberangrepp

Vi ser en ökad hotbild i form av cyberangrepp. Informationssäkerhetshoten som riktas mot myndigheten är mångfacetterade och kan kopplas till flera olika typer av hotaktörer.

Antalet upptäckta intrångsförsök mot myndighetens it-infrastruktur har också ökat. Ett sätt att göra intrång är att via nätfiske och social manipulation få tillgång till information i syfte att exempelvis stjäla eller offentliggöra den. Sårbarheter i myndighetens infrastruktur kan utnyttjas för att införa skadlig kod, som till exempel ransomware (gisslantagande av data) vilket kan påverka förtroendet för myndigheten.

Den tekniska utvecklingen, inom bland annat AI-området, genererar också nya hot och sårbarheter då den nya tekniken används av aktörer i skadliga syften. Det kan till exempel handla om AI-baserat nätfiske där man utger sig för att vara en känd eller betrodd person.

Åtgärder

- Vi arbetar kontinuerligt och systematiskt med att förebygga och upptäcka cyberangrepp genom tekniska, administrativa och fysiska åtgärder.
- Myndighetens Security Operation Center (SOC) övervakar it-system och nätverk samt utför olika cybersäkerhetsövningar för att ta fram förslag på förbättringar och säkerhetsåtgärder.
- Utbildning för samtliga medarbetare samt initiativ om att agera informationssäkert, är viktiga verktyg för att kontinuerligt förbättra medvetenhet och kunskap om informationssäkerhet i myndigheten.

[14] Informationssäkerhet - Arbetsförmedlingen (arbetsformedlingen.se)

6.2.2 Insiderbrott

Personalsäkerhetsfrågor, med efterföljande insiderproblematik, är alltmer relevant. Samhällsviktiga organisationer är särskilt exponerade för korruptionsförsök, infiltration och otillåten påverkan. Med syftet att skaffa information, påverka ett beslut eller tillgodogöra sig pengar från brott. Risken för att redan anställda medarbetare kan vara föremål för värvningsförsök från fientliga krafter, utländska såväl som nationella, är högre än tidigare. Syftet är ofta att utnyttja Sveriges välfärdssystem eller ta del av och sprida information till orätta händer.

Upptäcktsrisken är låg och det är inte ovanligt att en anställd som blir föremål för intern utredning väljer att på egen hand avsluta sin anställning och därmed undgå en rättslig utredning. Vi vet att det har funnits, och sannolikheten är stor att det finns anställda på myndigheten som samarbetar med kriminella aktörer.

Här ser myndigheten ett behov att förstärka rutiner och processer. Åtgärderna kan till exempel handla om att ställa rätt säkerhetskrav vid inköp, upphandling och utkontraktering samt medvetenhet om vilken historik konsulter och medarbetare har som söker jobb på myndigheten.

Åtgärder

- Ett arbete är uppstartat med att se över rekryteringsprocessen och bakgrundskontroller i samband med anställning.

6.2.3 Påverkanskampanjer, otillåten påverkan och desinformation

I takt med ett alltmer försämrat säkerhetsläge i omvärlden behöver ett högt säkerhetsmedvetande och en betryggande säkerhetskultur vara en naturlig del i det dagliga arbetet.

Desinformation är ett sätt att undergräva förtroendet för Sverige och det demokratiska samhället. Utvecklingen inom AI-området har en stor påverkan inom området desinformation. Möjligheterna att genom manipulerad digital media utge sig för att vara någon annan ställer högre krav på myndigheten och allmänheten att verifiera källor och information som sprids.

Åtgärder

- Vi arbetar kontinuerligt med att öka kunskapen och medvetenheten hos myndighetens medarbetare gällande desinformation och behovet av källkritiskt tänkande för att öka säkerhetskulturen på myndigheten.

- Vi har en daglig omvärldsbevakning som är tillgänglig för alla anställda.

- Tekniska säkerhetsåtgärder som blockning av olika webbtjänster, behörighetsstyrning och spårbarhet är en viktig del i att upptäcka och stoppa spridande av desinformation.