ARBETSFÖRMEDLINGEN
SWEDISH PUBLIC EMPLOYMENT SERVICE

Informationssäkerhet

Återrapport uppdrag 3.7 i regleringsbrevet 2023

Arbetsförmedlingen
Författare: Per Gauffin, Per-Ola Persson, Kim Nilsson, Stefan Adeen, Gabor Sebastiani
Datum: 2023-11-01
Diarienummer: Af-2023/0048 2823

Förord

Rapporten har tagits fram med anledning av följande uppdrag i Arbetsförmedlingens regleringsbrev för 2023:

Uppdrag 3.7 Informationssäkerhet
Arbetsförmedlingen ska senast 1 november 2023 till Regeringskansliet (Arbetsmarknadsdepartementet) övergripande redogöra för hur myndigheten arbetat för att förvalta och utveckla sin informationssäkerhet och hur Arbetsförmedlingen planerar för att möta framtida behov.

Arbetsförmedlingen ska särskilt:

- *Redogöra för åtgärder för att fortsatt utveckla den interna styrningen och uppföljningen av informationssäkerhetsarbetet inklusive myndighetsledningens roll i detta.*
- *För myndighetens verksamhetskritiska system genomföra en analys av kopplingar till och beroenden av externa parter, exempelvis it-tjänsteleverantörer och andra myndigheter.*
- *Genomföra en analys av hur arbete på distans påverkar informationssäkerheten och vidta åtgärder för att hantera identifierade risker.*
- *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 generaldirektör Lars Lööw. Ärendet har föredragits av Per Gauffin, enhetschef VO It. Övriga som deltagit i den slutliga handläggningen är Krister Dackland, verksamhetsområdeschef VO It, Robert Hansson, säkerhetschef samt Per-Anders Ode, VO It och Per-Ola Persson, enheten Strategisk säkerhet. Beslutet är fastställt digitalt i Diariet och saknar därför namnunderskrifter.

Lars Lööw

Vikarierande generaldirektör

Per Gauffin

Enhetschef

Innehåll

1 Sammanfattning

Utvecklingen av Arbetsförmedlingens ledningssystem för informationssäkerhet (LIS) är en förutsättning för att myndigheten ska kunna genomföra sin förflyttning mot en digitaliserad verksamhet. Myndighetens LIS utvecklas med stöd av ISO 27000-serien[1] och ska beskriva interna regler, arbetssätt och stöd samt roller och ansvar. Arbetet bedrivs genom tvärfunktionella grupper med sakkunskap från olika delar av verksamheten, som tillsammans utformar de krav och processer som behövs.

Myndighetsledningens roll i informationssäkerhetsarbetet har fått ett större fokus. Ledningens genomgång[2] har genomförts i enlighet med MSB:s föreskrifter. Myndighetsledningen har i och med det informerat sig om risker och hinder i informationssäkerhetsarbetet.

”Agera informationssäkert” är ett särskilt initiativ med syfte att öka medvetenhet och kunskap inom informationssäkerhet för hela myndigheten. Inom it-verksamheten drivs mer specifika kompetens- och processutvecklingsinitiativ som till exempel utbildning i och vidareutveckling av Säkerhetsresan[3] som är en stödprocess för informationssäkerhetsarbetet.

Genom tekniska förebyggande skyddsåtgärder samt utveckling av tekniska övervakningsverktyg stärker vi kontinuerligt vår motståndskraft och resiliens mot cyberangrepp. Myndigheten blev 2022 en beredskapsmyndighet. Detta understryker ytterligare vikten av god informationssäkerhet, främst avseende robusthet.

En del i den digitala förflyttningen är att uppnå en ökad extern samverkan för både tekniska förmågor och informationsutbyten. Myndigheten har många olika centrala kopplingar till externa parter som vi beskriver i fyra huvudgrupper: leverantörer av arbetsmarknadspolitiska tjänster, andra myndigheter, it-tjänsteleverantörer och övriga externa parter.

I och med pandemin införde myndigheten ett mer tillåtande förhållningssätt till distansarbete. Vi har utifrån ett informationssäkerhetsperspektiv arbetat med identifierade risker och implementerat åtgärder.

Omvärldsläget har förändrats negativt ur ett informationssäkerhetsperspektiv. Snabb teknisk utveckling och omvärldsförändringar ställer stora krav på informationssäkerhet. Vi ser utmaningar inom AI-området såväl rörande den egna användningen av ny teknik som hotaktörers nyttjande av tekniken.

Ett högt säkerhetstänk behöver i högre utsträckning än tidigare vara en naturlig del i det dagliga arbetet. Cyberangrepp syftande till att påverka myndighetens digitala tillgänglighet eller att stjäla eller förstöra information ökar. Vi ser även ökade risker i form av externa påverkanskampanjer och desinformation.

[1] I enlighet med MSBFS 2020:6, 4 §
[2] Diarienummer Af-2023/0050 6088, Ledningens genomgång
[3] Diarienummer Af-2021/0011 2967, Säkerhetsresan

2 Metod och genomförande

2.1 Metod

Kartläggningar och analyser har genomförts i tvärfunktionella arbetsgrupper. Vissa av analyserna har genomförts under året, andra analyser som exempelvis riskanalys för distansarbete är genomförd sedan tidigare. Källmaterial har inhämtats från ett antal myndigheter och andra externa nätverk såsom via myndighetssamverkan, traditionell media, privata säkerhetsföretag och it-relaterad media. Prioritering av hot och sårbarheter har skett via intervjuer med representanter från olika delar av myndigheten.

2.2 Disposition

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

I kapitel tre redovisas arbetet med att förvalta och utveckla informationssäkerhet.

I kapitel fyra redovisas den fortsatta utvecklingen av den interna styrningen och uppföljningen av informationssäkerhet.

I kapitel fem redovisar vi kopplingar till och beroenden av externa parter.

I kapitel sex redovisar vi hur myndighetens regelverk för distansarbete har förtydligats.

I kapitel sju redovisar vi hur myndigheten påverkas av omvärldsförändringar.

2.3 Koppling till återrapport 2022

I en första återrapport i oktober 2022[4] redogjorde myndigheten för åtgärder som vidtagits respektive planerades att vidtas med anledning av uppdraget i regleringsbrevet 2022. I denna återrapport redogör Arbetsförmedlingen för hur införandet av Ledningssystemet för informationssäkerhet och myndighetsledningens involvering har fortlöpt (se särskilt kapitel 4).

[4] Diarienummer Af-2022/0075 2570, Informationssäkerhet

3 Arbetet med att förvalta och utveckla informationssäkerhet

Arbetsförmedlingens verksamhet och information och därmed också informationssäkerhet flyttas alltmer mot en digital hantering. Myndigheten har under flera års tid utvecklat och förbättrat arbetet med informationssäkerhet men det finns en eftersläpning i befintliga processer och system. Vi ser också att behovet av bättre säkerhetsförmågor ökar kontinuerligt.

Myndigheten är sedan hösten 2022 en beredskapsmyndighet. Uppdraget som beredskapsmyndighet ställer krav på både helt nya verksamhetsförmågor och på informationssäkerheten i befintlig verksamhet. Ett större initiativ för att säkerställa dessa förmågor är uppstartat och drivs samordnat på myndigheten.

3.1 Pågående initiativ

Arbetet med myndighetens ledningssystem för informationssäkerhet (LIS) har en tydlig handlingsplan[5] och är en central del i myndighetens informationssäkerhetsarbete vilket beskrevs i 2022 års återrapport[6]. Handlingsplanen beskriver informationssäkerhetsåtgärder, struktur och integration av LIS i myndighetens övriga styrmodeller. Den visar även på utveckling av processer, ansvar och informationsklassning som utvecklas och anpassas efter verksamhetens behov. Arbete pågår med att systematiskt gå igenom ISO 27002:2022 och dess 93 åtgärder. Exempel på åtgärder som genomarbetats i LIS-arbetet är loggning och behörigheter. Andra områden som utvecklas i linje med handlingsplanen är till exempel processer för kontinuitetshantering och hantering av informationssäkerhetsincidenter.

Myndigheten har i Säkerhetsresan[7] samlat flera processer och arbetssätt för att stötta verksamheten i sitt informationssäkerhetsarbete. Säkerhetsresan är en samverkande arbetsmodell mellan it-verksamheten, rättsavdelningen, och inköpsavdelningen. Arbetsmodellen har, inom dessa funktioner, lett till en högre medvetenhet, kunskap och förmåga inom informationssäkerhet.

”Agera informationssäkert” är ett särskilt initiativ med syfte att öka medvetenhet och kunskap inom informationssäkerhet för hela myndigheten. Initiativet är riktat till alla medarbetare och innehåller bland annat nanoutbildningar, filmer på intranätet och quizmaterial för arbetsplatsträffar.

Tekniska specifika skyddsförmågor har förstärkts, till exempel med ett internt Security Operation Center (SOC) som övervakar myndighetens system ur ett säkerhetsperspektiv för att skydda mot externa angrepp. Förmågan består av en serie tekniska övervakningsverktyg som hanteras av interna specialister.

[5] Diarienummer Af-2023/0007 3546, LIS, Handlingsplan
[6] Diarienummer Af-2022/0075 2570, Informationssäkerhet
[7] Diarienummer Af-2021/0011 2967, Säkerhetsresan

3.2 Framtida behov och utmaningar

Den digitala transformationen fortsätter, vilket leder till att myndighetens hotbild förskjuts och ökade krav på digital säkerhetsförmåga. Nedan lyfts några exempel på framtida behov samt utmaningar som vi ser.

Behov av intern kompetens och medvetenhet inom informationssäkerhet
Kompetens och förmåga rörande informationssäkerhet behöver förbättras både för specialister inom säkerhet och teknik och för övriga medarbetare. I takt med att mängden information som hanteras ökar och att hotbilden ständigt förändras behöver medarbetarna utbilda sig kontinuerligt.

Utmaningar med informationsklassning och informationsägarskap
Att förtydliga informationsägarens roll och ansvar är en central fråga för att utveckla myndighetens systematiska informationssäkerhetsarbete. Vi har idag utmaningar med att definiera vilka befattningar som ansvarar för informationsklassning, när och i vilka situationer informationsklassning ska genomföras samt vilka kriterier som ska användas för bedömning av konsekvens (se även kapitel 4).

Behov av extern samverkan kommer att öka på flera sätt
Leverantörer av arbetsmarknadspolitiska tjänster utgör en central del av myndighetens verksamhetslogik. Att integrera dessa leverantörers informations-hantering i myndighetens processer för att säkerställa att detta kan ske med bibehållen säkerhet är en central fråga. Effektiv hantering av information och data kommer alltmer att bygga på delning av gemensam information mellan externa organisationer och interna funktioner. För att uppnå en högre effektivitet, både ur ett kostnads- och funktionsperspektiv kommer myndigheten att nyttja externa leverantörer i en allt större omfattning.

Hinder att nyttja molnbaserade it-tjänster
Det har funnits starka hinder för svenska myndigheter att nyttja flertalet molnbaserade it-tjänster på grund av begränsningar inom GDPR:s lagstiftning som begränsar tredjelandsöverföringar. EU:s adekvansbeslut under sommaren 2023 kan öppna upp detta hinder. Myndigheten utreder för tillfället vilka följder som adekvansbeslutet leder till vilket skulle kunna leda till utökad tillgänglighet för it-tjänster med högre funktionalitet och bättre säkerhet till en lägre kostnad.

3.3 Planering för att möta framtida behov

I takt med att omvärlden kontinuerligt och snabbt förändras behöver myndigheten hela tiden förändra och förbättra arbetet med informationssäkerhet. Det kommer att omfatta både tekniska förflyttningar och strukturella processförändringar i myndighetens verksamhet.

Den verksamhetsförändring och digitala transformation som har genomförts inom myndigheten under de senaste åren har lett till omfattande processförändringar. Dessa förändringar är komplexa och kräver anpassningar för att nå fullgod informationssäkerhet. Ett exempel på förbättringsarbete är hanteringen av

information för personer med skyddade personuppgifter. Förbättringsarbetet beskrivs i återrapport för uppdrag 3.6 i regleringsbrevet.

Myndigheten har gjort stora investeringar i tekniska skydd för informationssäkerhet. Området har varit eftersatt och det finns kvarstående brister i det tekniska skyddet. Arbetet med LIS, anpassning till beredskapsmyndighet samt kommande krav från till exempel NIS2-direktivet[8], hjälper till att driva arbetet med att förbättra det tekniska skyddet.

4 Fortsatt utveckling av den interna styrningen och uppföljningen av informationssäkerhet

Myndigheten har vidtagit flera åtgärder för att utveckla den interna styrningen och uppföljningen av informationssäkerhetsarbetet.

4.1 Ledningssystem för informationssäkerhet (LIS)

Utvecklingen av Arbetsförmedlingens ledningssystem för informationssäkerhet (LIS) är en förutsättning för att myndigheten ska kunna fortsätta sin förflyttning mot en digitaliserad verksamhet. Myndighetens roll som beredskapsmyndighet med ansvar för flera viktiga samhällsfunktioner understryker ytterligare behovet av ett LIS som en integrerad del av myndighetens ordinarie sätt att styra och leda verksamheten.

Myndighetens LIS utvecklas med stöd av ISO 27000-serien[9] och ska beskriva interna regler, arbetssätt och stöd samt roller och ansvar. Arbetet bedrivs genom tvärfunktionella grupper med sakkunskap från olika delar av verksamheten som till exempel juridik, HR och lokalförsörjning, som tillsammans utformar de krav och processer som behövs.

En prioriterad aktivitet i myndighetens verksamhetsplan för 2023[10] är att ”etablera en tydlig struktur för samordning och styrning av myndighetens informations-säkerhetsarbete”. Myndigheten har fastställt interna styrande och stödjande dokument[11][12] för hur den organisatoriska förmågan ska stärkas. Detta innefattar förtydliganden kring såväl den samordnande förmågan som utpekade ansvar och roller inom cybersäkerhet, dataskydd, personalsäkerhet och fysisk säkerhet.

[8] EU-direktivet om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen.
[9] I enlighet med MSBFS 2020:6, 4 §
[10] Diarienummer Af-2022/0029 2963
[11] Diarienummer Af-2023/0054 2633, Arbetsförmedlingens interna instruktioner, Ledningssystem för informationssäkerhet
[12] Diarienummer Af-2023/0054 2613, Arbetsförmedlingens handbok, Ledningssystem för informationssäkerhet

4.2 Myndighetsledningens roll inom informationssäkerhet

Arbetsförmedlingen har vidtagit flera åtgärder för att stärka myndighetsledningens roll i att utveckla den interna styrningen och uppföljningen av informationssäkerhetsarbetet.

De övergripande målen för säkerhetsarbetet har reviderats i samband med den senaste översynen av myndighetens säkerhetspolicy[13]. Målen visar på en riktning även för arbetet med informationssäkerhet. Arbetssätt som långsiktighet och systematik stödjer att informationssäkerheten utgör en naturlig och integrerad del av verksamhetens ordinarie ledning och styrning.

Myndigheten har under 2023 sammanställt *ledningens genomgång*[14] som är en intern uppföljning baserad på krav i MSB:s föreskrifter om informationssäkerhet för statliga myndigheter[15]. Fokus har legat på risker och hinder i informationssäkerhetsarbetet som myndighetsledningen ska informera sig om. Bland de frågor som lyfts kan särskilt nämnas behovet att

- förtydliga informationsägarens roll och ansvar
- stärka ledningens åtagande på alla nivåer och organisatoriska delar.

Båda dessa frågor är centrala för att utveckla myndighetens systematiska informationssäkerhetsarbete och kan, om de inte hanteras, utgöra hinder i arbetet framåt.

Ledningens genomgång har även omfattat förbättringsförslag med förtydliganden kring

- hur informationsägare och verksamhetsansvariga genom informationssäkerhetsklassning ska involveras i arbetet med ett systematiskt och riskbaserat arbetssätt
- organisation för hur informationssäkerhetsarbetet ska bedrivas, med beskrivningar kring ansvar och roller.

Myndigheten arbetar med att ta fram en uppdaterad struktur för informationsansvar och informationsägarskap. Syftet är att förtydliga roller och ansvar för informationshantering med koppling till verksamhetsansvar.

5 Kopplingar till och beroenden av externa parter

Arbetsförmedlingen har en stor mängd informationsutbyten med och beroenden till olika typer av externa parter. Många av dessa är kritiska för myndighetens förmåga att fullfölja sitt uppdrag. Vissa av dem är politiskt beslutade medan andra är mer teknik- eller förmågerelaterade.

[13] Diarienummer Af-2023/00892636, Säkerhetspolicy för Arbetsförmedlingen
[14] Diarienummer Af-2023/0050 6088, Ledningens genomgång
[15] MSBFS 2020:6 Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter, särskilt 14–15 §§

I vår analys har vi delat in externa parter i följande huvudgrupper:

- Leverantörer av arbetsmarknadspolitiska tjänster
- Andra myndigheter
- It-tjänsteleverantörer
- Övriga externa parter

Vid beroenden av inhämtning av information från externa parter är det i första hand tillgängligheten till den extern källan som är kritisk och behöver stå i paritet med våra behov av information från källan. Vid utlämnande behöver vi i första hand säkerställa konfidentialitet och riktigheten hos informationen.

Extern exponering av information kan medföra potentiella informationssäkerhets-risker och måste därför ske med beaktande av behov av skyddsåtgärder baserat på informationsklassning av berörd information samt genomförda riskanalyser. Det är viktigt att exponeringen sker i enlighet med relevanta juridiska krav genom exempelvis GDPR, Offentlighets- och sekretesslagen (OSL) eller säkerhetsskydds-lagen.

Nedan ges en utförligare beskrivning av de olika huvudgrupperna av externa parter samt vilka åtgärder vi har implementerat.

5.1 Leverantörer av arbetsmarknadspolitiska tjänster

Myndigheten nyttjar sedan länge externa parter som komplement till egna interna resurser för utförande av myndighetens uppdrag. Dessa benämns här *leverantörer av arbetsmarknadspolitiska tjänster*. I och med förordningsförändringar[16] under 2022 om att i högre grad nyttja kommersiella aktörer för myndighetens uppdrag att rusta och matcha arbetssökanden till arbete, ökade nyttjandet av sådana leverantörer. Dessa utgör nu en central del av myndighetens verksamhetslogik. Vid nyttjande av leverantörer av arbetsmarknadspolitiska tjänster delar myndigheten information rörande arbetssökande och arbetsgivare med leverantörerna. Informationen innehåller en stor andel personuppgifter och sedan 2023 har personuppgiftsansvaret genom nya och förändrade författningar[17] och föreskrifter[18], helt överförts till leverantören av den arbetsmarknadspolitiska tjänsten.

Åtgärder
Vid avtalsgenomgång med nya leverantörer av arbetsmarknadspolitiska tjänster görs alltid en genomgång av vad god personuppgiftshantering innebär. Uppföljning av avtalsefterlevnaden sker löpande i form av dels proaktiva åtgärder som exempelvis ekonomiska analyser, spårning av anomalier och oanmälda kontrollbesök, dels reaktiva åtgärder baserade på klagomål och avvikelserapporteringar från exempelvis deltagare, allmänheten eller medarbetare. En visselblåsarfunktion finns etablerad.

[16] Förordning (2022:812) om förmedlingsinsatser samt Förordning om ändring i förordningen (2000:628) om den arbetsmarknadspolitiska verksamheten
[17] Offentlighets- och sekretesslag (2009:400) samt Förordning (2022:812) om förmedlingsinsatser Sveriges kommuner
[18] AFFS 2023:1 - Uppgiftsskyldighet för leverantörer

Olika typer av sanktioner som exempelvis vite eller ytterst hävande av avtal kan i förekommande fall komma i fråga.

5.2 Andra myndigheter

För utförande av sitt myndighetsuppdrag är Arbetsförmedlingen beroende av informationssamverkan med andra myndigheter. Arbetsförmedlingen utväxlar stora mängder information med till exempel Skatteverket, Försäkringskassan och MSB.

Åtgärder
Kompenserande tekniska och administrativa åtgärder finns etablerade för informationssamverkan med Skatteverket och Försäkringskassan där så är möjligt och det bedöms motiverat.

5.2.1 Skatteverket

Personuppgifter om såväl arbetssökande som egna medarbetare (anställda och konsulter) hämtas från Skatteverket via tjänsten Navet. För nyregistrering av arbetssökande och medarbetare är den tekniska åtkomsten till Navet därför kritisk. I uppgifterna från Navet återfinns bland annat uppgift om huruvida berörd person har skyddade personuppgifter. För att säkerställa att personer med skyddade person-uppgifter inte får sina uppgifter röjda är det viktigt att uppgifterna är korrekta och uppdaterade.

5.2.2 Försäkringskassan

Myndigheten har även verksamhetskritiska systemsamband med Försäkringskassan bland annat rörande utbetalning av olika typer av ersättningar för arbetsmarknads-politiska program och insatser.

5.2.3 MSB

Arbetsförmedlingen nyttjar i ökande omfattning den av MSB tillhandahållna kommunikationstjänsten SGSI (Swedish government secure intranet) för elektronisk kommunikation med andra anslutna myndigheter. Nyttjande av SGSI bidrar till ökad robusthet i kommunikationen med andra myndigheter och skapar förutsättningar för bibehållen kommunikationsförmåga även då tillgång till Internet saknas, exempelvis vid överbelastningsattacker.

5.3 It-tjänsteleverantörer

5.3.1 Utkontrakterade tjänster

Arbetsförmedlingen nyttjar utkontrakterade it-tjänster för vissa syften. Ett exempel är personalsystemet som driftas av Statens servicecenter som även utför all ärendehandläggning i systemet för Arbetsförmedlingens medarbetare. Ett annat exempel är system för hantering av psykologiska utredningar av arbetssökande som driftas av extern part. Andra typer av mindre verksamhetskritiska utkontrakterade tjänster är till exempel enkätverktyg med mera.

Det finns även system som driftas i myndighetens interna it-miljö men där den tekniska förvaltningen helt eller delvis utkontrakterats till extern part. Ett exempel är myndighetens redovisningssystem där ägandeskapet och den tekniska förvaltningen åligger extern part. Även ägande och logistisk hantering av personliga enheter i form av såväl arbetsdatorer som mobiltelefoner för myndighetens medarbetare är utkontrakterade.

Åtgärder
Vid utkontrakteringar görs myndighetens information tillgänglig för extern part, vilket potentiellt medför en ökad risk för i första hand röjande av information. För utkontrakterade it-tjänster genomförs, på samma sätt som för interna tjänster, alltid en analys där risker identifieras och skyddsvärdet för den information som ska hanteras i tjänsten fastställs till grund för krav på kompenserande skyddsåtgärder samt att relevanta lagrum identifieras. I detta ingår att avgöra huruvida GDPR, OSL eller säkerhetsskyddslagen behöver beaktas vid tecknandet av affärsavtal för tjänsten. Exempel på skyddsåtgärder som kan vara relevanta är upprättande av personuppgiftsbiträdesavtal och/eller säkerhetsskyddsavtal. Dessutom görs tekniska åtgärder i syfte att minimera den exponerade informationen.

5.3.2 Infrastrukturella komponenter

Arbetsförmedlingen nyttjar en stor mängd kommersiella standardprodukter i den tekniska infrastrukturen, till exempel nätverkskomponenter, plattformar för databaser, servervirtualisering, datalagring, olika typer av säkerhets- och utvecklingsplattformar med mera. För dessa finns oftast ett beroende till extern part (oftast leverantören) för nödvändig support, vilken kan vara kritisk vid till exempel driftstörningar.

Även delar av myndighetens it-infrastruktur är utkontrakterade till externa parter. Dessa är till sin natur kritiska för myndighetens förmåga att tillhandahålla såväl interna it-stöd som externa it-tjänster.

Åtgärder
Vid utkontraktering samt nyttjande av support från externa leverantörer görs myndighetens information tillgänglig för extern part, vilket potentiellt medför en ökad risk för i första hand röjande av information. För dessa typer av avtal med externa parter görs alltid en bedömning huruvida personuppgiftsbiträdesavtal och eventuellt säkerhetsskyddsavtal ska tecknas som bilaga till affärsavtalet. Dessutom görs tekniska åtgärder i syfte att minimera den exponerade informationen.

5.3.3 Kompetens- och resurskonsulter

Arbetsförmedlingen anlitar olika typer av externa konsulttjänster för olika delar av verksamheten, främst rörande it-leveranser. Sådana konsulter ges ofta åtkomst till potentiellt skyddsvärd information i myndighetens it-system.

Åtgärder
Det tecknas alltid individuella sekretessavtal och säkerhetsprövning (inklusive säkerhetsskyddsavtal) övervägs och genomförs då det bedöms som relevant. I syfte

att minimera exponeringen av skyddsvärd information tillämpas ”principen om lägsta behörighet” för konsulter. Detta gäller även för myndighetens anställda.

5.4 Övriga externa parter

5.4.1 A-kassorna

A-kassorna är beroende av information från Arbetsförmedlingen. För beslut om utbetalning av arbetslöshetsersättning är a-kassorna beroende av information från Arbetsförmedlingen rörande om arbetssökande är inskriven som arbetssökande på myndigheten, samt om de i övrigt uppfyller de allmänna villkoren för rätten till ersättning. Arbetsförmedlingen ska även skicka underrättelser till a-kassan om Arbetsförmedlingen har anledning att anta att arbetssökande har misskött sitt arbetssökande, förlängt tiden i arbetslöshet eller orsakat sin arbetslöshet. Informationsutbytet sker genom organisationen Sveriges a-kassor. Arbetsförmedlingen utväxlar även information med banker rörande utbetalning av a-kasseersättning till arbetssökande. Om uppgifterna från Arbetsförmedlingen inte överensstämmer med de uppgifter som banken får från a-kassorna, stoppas utbetalningen. Det är därför viktigt med riktighet i uppgifterna.

Åtgärder
Kompenserande tekniska och administrativa åtgärder finns etablerade för det fall tekniska lösningar inte är tillgängliga och ordinarie rutiner inte kan tillämpas.

5.4.2 Sveriges kommuner

Via en digital tjänst tillhandahåller Arbetsförmedlingen information om arbetssökande till Sveriges kommuner som kommunerna behöver för att hantera ekonomiskt bistånd.

Åtgärder
Tjänsten har strikt behörighetskontroll och endast av Arbetsförmedlingen godkända nyttjare kan ta del av dess informationsinnehåll.

5.4.3 Plattform för digitala matchningstjänster

Arbetsförmedlingen tillhandahåller en gemensam infrastruktur för digitala matchningstjänster i Sverige. Genom plattformen[19] ges tillgång till öppna data och öppen källkod som är tillgängligt för alla. Plattformen nyttjas av en stor mängd företag och organisationer från privat och offentlig sektor som aktivt delar data, kunskap och kod. All information som delas via plattformen är publik och delas utan behörighetskontroll. Dock är kraven på tillgänglighet för informationen ofta höga, vilket har beaktats i den tekniska arkitekturen för tjänsterna.

[19] Om JobTech Development | Jobtech

6 Distansarbete

I och med pandemin införde Arbetsförmedlingen ett mer tillåtande förhållningssätt till distansarbete. I samband med detta har regelverket för distansarbete förtydligats.

Med distansarbete avses ordinarie arbete som regelbundet utförs från en annan plats än Arbetsförmedlingens lokaler (huvudarbetsplatsen).[20] Distansarbete sker normalt i medarbetarens hem (distansarbetsplatsen). Arbete som utförs hos kund, på tjänsteresa eller vid konferenser är inte distansarbete. Distansarbetsplatsen kan tillfälligt, i överenskommelse med närmaste chef, vara på annan plats. I enlighet med Arbetsgivarverkets rekommendation får distansarbete endast förekomma inom Sverige.

Minst 51 procent av arbetet ska utföras på huvudarbetsplatsen sett över ett år. Medarbetare ska vara anträffbara på telefon, mejl, videomöten etcetera och hålla kontakt med chef, kollegor och andra intressenter utifrån verksamhetens behov. I arbetstiden inräknas tid ute hos kund, tjänsteresa eller exempelvis konferenser. Möjligheten till distansarbete varierar mellan olika medarbetare utifrån till exempel verksamhetens behov, arbetsuppgifternas karaktär och medarbetarnas individuella förutsättningar till distansarbete.

6.1 Risker och åtgärder

Här följer en övergripande lista med risker och åtgärder som myndigheten arbetat med under perioden 2020–2023. Riskanalysen beaktade Arbetsförmedlingens ambition att erbjuda möjlighet till distansarbete 49 procent av medarbetarnas arbetstid. Skulle andelen distansarbete öka behöver en ny riskanalys genomföras.

Risk att annan än svensk lagstiftning gäller
Under 2020 uppstod många frågor kring vilka platser och länder medarbetare och konsulter kan arbeta ifrån och vilka risker detta kan medföra.

Åtgärder
Arbetsförmedlingen följer Arbetsgivarverkets rekommendation om att bara tillåta distansarbete inom Sverige. Denna avgränsning säkerställer att myndighetens medarbetare omfattas av svensk lagstiftning och att annat lands lagstiftning inte kan bli aktuell. Detta infördes främst med tanke på arbetsrätt, men avgränsningen undanröjer även frågeställningar kring sekretess och andra aspekter som har bäring på informationssäkerhet.

Risk att medarbetare har en osäker huvudarbetsplats
En hypotetisk frågeställning var om medarbetare kunde arbeta 100 procent från hemmet och vilket ansvar arbetsgivaren då har för att kontrollera efterlevnaden av myndighetens informationssäkerhet i hemmet.

[20] Diarienummer Af-2022/0041 2343, Arbetsförmedlingens handbok, Distansarbete

Åtgärder
Begränsningen att förlägga minst 51 procent av arbetstiden till Arbetsförmedlingen lokaler säkerställer en tydlighet avseende medarbetarens huvudarbetsplats. Huvudarbetsplatsen ska vara i Arbetsförmedlingens lokaler och det ska vara platsen där men oftast arbetar. I myndighetens egna lokaler kan Arbetsförmedlingen säkerställa att det finns förutsättningar för god informationssäkerhet. Där kan även efterlevnaden följas upp. Åtgärden motiveras inte främst av informationssäkerhetsskäl, men det skapar en möjlighet att styra vissa arbetsuppgifter till myndighetens lokaler. Exempelvis säkra utskrifter saknar idag stöd utanför myndighetens egna lokaler liksom arbete som rör säkerhetsskydd.

Risk att distansarbete sker med osäker utrustning
Medarbetare har inkommit med önskemål om att få utföra distansarbete med egen teknisk utrustning, där Arbetsförmedlingen inte kan kontrollera om det finns virusskydd och annan programvara för säkerhet.

Åtgärder
Distansarbete sker med bärbar dator som myndigheten tillhandahåller. Egen utrustning får inte användas. Det finns även tekniska skydd som hindrar egna datorer eller telefoner från åtkomst till Arbetsförmedlingens nät.

Risk för osäker datakommunikation
Myndigheten hade tidigare fler lösningar för säker anslutning på distans, men medarbetaren behövde själv aktivera någon av dessa lösningar.

Åtgärder
Arbetsförmedlingen tillhandahåller krypterad kommunikation (VPN) mellan tjänstedatorn och myndighetens nätverk som aktiveras när datorn är på distans. Arbetsförmedlingen har under pandemin utökat kapaciteten för att fler medarbetare ska kunna arbeta på distans samtidigt. Det finns även tekniska skydd som övervakar tjänstedatorns säkerhet.

Risk för osäker fysisk miljö med obehöriga som ser eller hör
Myndigheten såg över sina föreskrifter för distansarbete då fler medarbetare utnyttjade möjligheten. Risken identifierades att medarbetare efter pandemin skulle vilja arbeta från caféer eller anläggningar för co-working där medarbetare från andra arbetsgivare finns i samma lokal.

Åtgärder
Arbetsförmedlingen har förtydligat att distansarbete kan ske från en lokal som motsvarar avskildheten i en bostad. Allmänna platser, som caféer, är inte godkända för arbete på distans. Det görs en bedömning av medarbetarens arbetsuppgifter innan det skrivs en överenskommelse om distansarbete.

Arbetsförmedlingen tillhandahåller hörlurar med mikrofon för att minska risken för överhörning i samband med videomöten.

Risk för osäker hantering av sekretessbelagda och känsliga uppgifter
Då en stor informationsmängd inom myndigheten utgörs av ärenden som omfattas av sekretess gjordes en större analys av vilka arbetsuppgifter som kan utföras på distans med tillräckliga skyddsåtgärder.

Åtgärder
Samma grad av informationssäkerhet som vid huvudarbetsplatsen ska kunna garanteras vid distansarbete. Samtliga rutiner som gäller avseende säkerhet och sekretess vid huvudarbetsplatsen gäller också distansarbetsplatsen och det är medarbetarens skyldighet att se till att utrustning och känslig information inte hamnar i orätta händer.

Allt distansarbete sker efter överenskommelse mellan medarbetare och närmaste chef. Arbetsuppgifternas känslighet vägs in i överenskommelsen och det finns arbetsuppgifter som inte bedöms kunna utföras på distans på grund av informationens känslighet.

Risk för osäkra skrivare
Arbetsförmedlingens handläggning förutsätter att brev och dokument med känslig information kan skrivas ut utan att sekretess röjs på väg till skrivaren eller vid skrivaren.

Åtgärder
Arbetsförmedlingen erbjuder inte skrivare för distansarbete och tillåter inte utskrifter via andra skrivare än myndighetens. Utskrift måste ske i Arbetsförmedlingens lokaler. Detta är inte något problem idag, men krävde en bemanning under pandemin för att kuvertera och posta utskrivna brev.

6.2 Implementering av åtgärder

Samtliga åtgärder är implementerade. Arbetsförmedlingen tillhandahåller verktyg för distansarbete och tekniska skydd finns på plats. Regler och arbetssätt finns dokumenterade i instruktioner och handböcker. Det har även tagits fram stödjande material som lathundar, checklistor och utbildningar.

7 Omvärldsförändringar

Under de senaste åren har ett flertal större förändringar skett i Sverige och i vår omvärld som påverkar myndigheten ur ett informationssäkerhetsperspektiv. Krig råder i vårt absoluta närområde i och med Rysslands fullskaliga militära invasion i Ukraina, och Sverige är på väg att bli fullvärdig medlem i försvarsalliansen NATO.

Inom Sveriges gränser har kriminella nätverk flyttat fram sina positioner. Infiltration på myndigheter och kommuner förekommer i syfte att utnyttja välfärdssystemen. Stora tekniska framsteg sker inom AI-området, inte minst i och med att ChatGPT tillgängliggjordes för allmänheten i slutet av 2022. En följdeffekt av pandemin är också att distansarbete blivit mycket mer förekommande (se föregående kapitel).

Arbetsförmedlingen ser att primärt tre områden påverkas i hög grad till följd av det förändrade omvärldsläget. Vidtagna och planerade åtgärder är av säkerhetsskäl beskrivna på en begränsad detaljeringsnivå för att inte motverka åtgärdernas syften.

7.1 Cyberangrepp

De informationssäkerhetshot som riktas mot myndigheten är mångfacetterade och kan kopplas till flera olika typer av hotaktörer. Myndigheten ser en ökad hotbild i form av statsunderstödda cyberangrepp, i synnerhet från Ryssland. Ryssland bedriver underrättelseinhämtning metodiskt och långsiktigt och det ligger också i landets intresse att sprida misstro mot svenska myndigheter och det svenska totalförsvaret.

Ett sätt att göra detta är att via nätfiske och social manipulation få tillgång till information i syfte att exempelvis stjäla eller tillgängliggöra den. Sårbarheter i myndighetens infrastruktur kan utnyttjas för att implementera skadlig kod, som till exempel ransomware som kan påverka förtroendet för myndigheten men också finansiera hotaktörer. Antalet upptäckta intrångsförsök mot myndighetens it-infrastruktur har också tydligt ökat på senare tid.

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 handla om till exempel AI-baserat nätfiske där man utger sig för att vara en känd eller bekant person.

Åtgärder
Arbetsförmedlingen arbetar systematiskt och kontinuerligt med att förebygga och upptäcka cyberangrepp genom tekniska, administrativa och fysiska åtgärder. Arbetet innefattar såväl egen utveckling och förvaltning som inköp av externa verktyg och tjänster.

Initiativet ”agera informationssäkert” är ett viktigt verktyg för att successivt hålla en hög medvetenhet och kunskap om informationssäkerhet hos myndighetens medarbetare (se även kapitel 3).

7.2 Ökat behov av säkerhetsmedvetande

I takt med ett alltmer försämrat säkerhetsläge i världen och att stater som Ryssland, Kina och Iran agerar mer aggressivt (i form av till exempel sabotage, desinformation och destabiliserande aktiviteter) än tidigare, blir hög kunskap och medvetenhet inom informations- och cybersäkerhetsfrågor hos myndighetens medarbetare än mer viktig. Ett högt säkerhetstänk behöver i högre utsträckning än tidigare vara en naturlig del i det dagliga arbetet och kan röra vitt skilda områden (se nedan åtgärder).

Åtgärder
Arbetsförmedlingen genomför löpande insatser för att öka medvetenhet och kunskap inom informationssäkerhetsområdet. Det kan till exempel handla om

- att kunna ställa rätt säkerhetskrav vid inköp, upphandling och utkontraktering
- att iaktta försiktighet i sin dagliga e-posthantering samt i andra kanaler
- medvetenhet om vilken historik konsulter och medarbetare har som söker jobb på myndigheten.

Omvärldsbevakning sker också löpande för att hålla myndigheten uppdaterad inför nya risker och hot. Kunskapen tillgängliggörs till hela myndigheten via interna kommunikationskanaler.

7.3 Påverkanskampanjer och desinformation

Ytterligare sätt att undergräva förtroendet för Sverige och det demokratiska samhället är att sprida falsk information via olika kanaler, främst via sociala medier. Infiltration av olika delar av samhället är också ett sätt att långsiktigt påverka beslut och inriktningar. Under 2021 genomfördes den största påverkanskampanjen någonsin i Sverige där målet var Socialtjänsten. Kampanjen hade kopplingar till radikalislamistiska miljöer och fenomenet har tidigare förekommit internationellt mot ett flertal länder. Ett annat exempel är koranbränningar i samband med Sveriges ansökan till NATO. Påverkanskampanjer av denna typ ökar, med syfte att destabilisera och undergräva förtroendet för samhället.

Utvecklingen inom AI-området har stor påverkan inom området desinformation. Möjligheterna att genom både manipulerad text, bild och video utge sig för att vara någon annan ställer högre krav på myndigheten och allmänheten att verifiera källor och information som sprids.

Åtgärder
Arbetsförmedlingen arbetar kontinuerligt med att öka kunskapen och medvetenheten hos myndighetens medarbetare gällande desinformation och behovet av källkritiskt tänkande.

Tekniska säkerhetsåtgärder som exempelvis blockning av olika webbtjänster, behörighetsstyrning och spårbarhet är också en viktig del i att upptäcka och stoppa spridandet av desinformation och otillbörlig åtkomst till information.