ARBETSFÖRMEDLINGEN
SWEDISH PUBLIC EMPLOYMENT SERVICE

Öppen källkod

Riskanalys av Arbetsförmedlingens hantering av öppen källkod

Författare: Peter Nilsson
Datum: 2021-10-25
Diarienummer: Af-2021/0082 2220

Innehåll

1 Bakgrund

Arbetsförmedlingen använder idag, som många andra organisationer, öppen källkod i verksamhetssystem och i olika delar av den tekniska infrastrukturen. Exempel på lösningar med öppen källkod inom Arbetsförmedlingen är Open Shift, Mulesoft, Linux, Maria db mm. Vidare använder Arbetsförmedlingen Matomo för webbanalys, samt Elasticsearch för bl.a. Platsbankens sökmotor. Vi går över till eArkiv open source och har anskaffat ett CRM-system som öppen källkod. Arbetsförmedlingen licensierar också Jobtechs kod som öppen källkod.

Inom myndigheten pågår det en diskussion om vilka fördelar och risker detta beroende medför. Vi bör dock utgå från att öppen källkod är och kommer att vara en allt viktigare del i myndighetens IT-lösningar.

I fackpress tas det upp risker med öppen källkod. Exempel man nämner är att utvecklingsprojekt använder sig av i allt högre utsträckning, kodbibliotek som innehåller sårbarheter. Bland annat så har andelen utvecklingsprojekt med beroenden till sårbara kodbibliotek tredubblats på bara ett år[1].

Github skriver i sin årliga rapport om säkerhetsläget inom öppen källkod, att det tar i snitt fyra år innan sårbarheter i öppen källkod upptäcks. 94 procent av alla kodprojekt har i snitt 700 beroenden till öppen källkod[2].

Paketsystemet npm varnar för tre kodbibliotek som öppnar terminal-skal så fort de installeras. npm har nu tagit bort paketen efter en genomsökning, men de som installerat paketen måste se sina system som komprometterade[3].

Över hälften av alla analyserade JavaScriptkomponenter innehåller minst en känd sårbarhet.[4]

Sårbarheter fortsätter att öka. 17000 CVE (Common Vulnerabilities and Exposures) publicerades 2019. Nästan 9000 CVE publicerades första halvåret 2020. Av dessa 26000 var över 4000 (15%) klassificerade som kritiska.[5] David Wheeler, direktör vid ”Open Source Supply Chain Security” vid Linux Foundation säger "I want to emphasize that software is under attack."[6] Denna utredning har inte sökt eller hittat någon analys av i vilken grad sårbarheter finns i proprietär kod.

Det finns risker med att använda öppen källkod. Det är dock viktigt att påpeka att dessa risker också gäller proprietär kod. I diskussionen om ifall öppen eller proprietär kod är mest osäker är svaret inte självklart. Rätt hanterat argumenteras

1 Sex av tio utvecklingsprojekt använder farliga kodbibliotek. De här ska du undvika - TechWorld (idg.se) 2020-10-18
2 Github-rapport – fyra år innan sårbar öppen källkod upptäcks - TechWorld (idg.se) 2020-12-03
3 NPM: Om du kör dessa kodbibliotek är du hackad - TechWorld (idg.se) 2020-10-19
4 Threats, Risks, and Mitigations in the Open Source Ecosystem Michael Scovetta, Microsoft in collaboration with the Open Source Security Coalition.
5 Threats, Risks, and Mitigations in the Open Source Ecosystem Michael Scovetta, Microsoft in collaboration with the Open Source Security Coalition.
6. What to do about open source vulnerabilities? Move fast, says Linux Foundation expert • The Register

det att öppen källkod är säkrare än proprietär. Detta bygger på principen att det är många kvalificerade personer som granskar koden. Men det förutsätter då att det verkligen är många granskare i det specifika projektet. Med proprietär källkod måste du lita på leverantören, du kan inte själv granska koden. Leverantören kan ansvara för att granska och rätta sin kod men friskriver sig i avtalet från ansvar för och konsekvenser av brister i levererad kod.

Vi kan heller inte säga i vilken grad dessa sårbarheter är relevanta för Arbetsförmedlingen. Det beror på vilka källor som använd. Detta är en fråga att ta upp när ett initiativ gör en riskanalys för ett projekt.

2 Mål, syfte och metod

Målet med detta PM är att ta fram ett underlag till en policy för hur öppen källkod ska hanteras ur ett risk och säkerhetsperspektiv. Därefter ska en handbok eller motsvarande stöd tas fram med rekommendationer om hur dessa risker bör hanteras.

Detta PM tar inte upp frågan om en övergripande policy för hur Arbetsförmedlingen ska förhålla sig till öppen källkod eller nyttan med öppen källkod. Inte heller att i detalj analysera olika varianter av t ex licenser eller communitys (den ”grupp” där koden utvecklas) eller rekommendera specifika licenser som ska användas. Denna typ av frågor kan tas upp principiellt i syfte att analysera vilka typer av risker som kan förekomma och hur de kan hanteras.

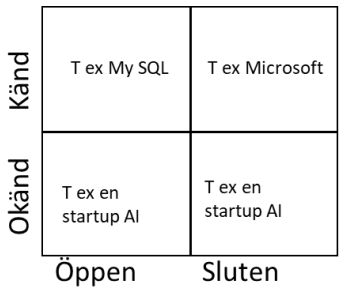
Perspektivet är i första hand kod som hämtas till och konsumeras av Arbetsförmedlingen i utvecklingen av myndighetens produkter och byggstenar. Det Arbetsförmedlingen utvecklar och bidrar med i olika communitys ingår inte i denna analys. Arbetsförmedlingen driver t ex inom Jobtech https://gitlab.com/arbetsformedlingen/. I vilken mån det finns andra bidrag har inte utretts här.

I intervjuerna och diskussionerna i denna analys har ett flertal personer framfört att Arbetsförmedlingen inte har någon policy för hur projekt ska hantera öppen källkod. Det är upp till varje initiativ och projektledare att ansvara för laglighet och kodkvalitet. Enligt vad som framkommit i intervjuer varierar det om, hur och i vilken omfattning hämtad kod kvalitets- och licenskontrolleras.

Underlaget baserar sig på intervjuer och rapporter (se referenslista) under 2021. Det har inte gjorts egna analyser av t ex hur specifika initiativ på Arbetsförmedlingen kvalitetskontrollerar öppen källkod.

3 Vad är öppen källkod

Kod är kod. Den principiella skillnaden mellan öppen och proprietär kod är licensieringen. Figuren nedan illustrerar öppen och sluten kod där koden kan vara känd eller okänd.



Öppen källkod innebär att vem som helst, av vilken anledning som helst, fritt får använda källkoden, samt inspektera, ändra och dela vidare källkoden. Detta innebär att öppen programvara inte kan upphandlas. Däremot kan man upphandla, eller ha egna resurser för anpassningar, drift, support och underhåll av programvara byggd med öppen källkod. Proprietära system kan också använda sig av öppen källkod. Motsvarande risker kan även finnas i sådana system.

Vid öppen källkod har upphovspersonen copyright © för sin kod. Upphovspersonens namn, datum och licensvillkor är tillagda i koden.

Det finns ett stort antal licensmodeller för öppen källkod. En programutvecklare kan vidareutveckla och anpassa kod som andra har utvecklat utan att betala någon avgift till den som har copyright på koden. Normalt erbjuder utvecklaren sina modifikationer tillbaka till upphovspersonen. Detta regleras i licensen för just den koden. I den community som har copyright kan det finnas kommittéer som beslutar om vilka bidrag eller förändringar som ska föras in i projektet.

I ett öppen källkodsprojekt utvecklas, testas och underhålls koden av oberoende personer, organisationer och företag som koordinerar sitt samarbete via en s.k. community. För proprietär källkod är det vanligen ett företag som utvecklar och tillhandahåller koden, men som också hemlighåller källkoden. Företaget som äger och utvecklar koden tar normalt ett avtalsmässigt ansvar för förvaltning och kontroll av kvaliteten i sin kod. I avtalet ingår dock normalt en friskrivning från ansvar för fel och konsekvenser av fel.

I öppen källkod finns oftast inte detta ansvar. Det finns ingen garanti för att koden förvaltas och uppdateras och det finns inget avtal där upphovspersonen tar ansvar för förvaltning. Det finns exempel[7] på när kritisk kod har utvecklats av ett fåtal personer och där de inte kunnat förvalta den fullt ut.

[7] Hämtat från ”Introduktion till öppen programvara”. PPT. Johan Linåker PHD. Lunds Universitet

Ett Företag kan basera hela sin produkt på öppen källkod och ingå i en community. Företaget kan ta samma ansvar för denna kod som om den vore proprietär mot sina kunder. Att systemet, eller delar av den är öppen källkod är en licensfråga. Att ett företag kan, och borde, ta ansvar fullt ut är inte samma sak som att det sker. Det finns exempel på proprietär kod som innehåller fel och sårbarheter. Att ta ansvar för att koden kvalitetsgranskas innebär inte att företaget tar ansvar för att koden är felfri, konsekvenserna eller kostnaderna för sårbarheterna. Ingen kod är felfri. Det man kan ta ansvar för är att kvalitetsgranskningen är god.

3.1 Communitys

Öppen källkod utvecklas i projektform av ”nätverk”, communitys, som kan vara mer eller mindre löst sammansatta. Medlemmarna kan vara såväl utvecklare som användare. En community kan bestå av en enskild individ, en stor global grupp individer som utvecklar av eget intresse men också numera att stora företag som IBM, Google etc deltar i communityn.

Hur ett projekt utvecklas och vilken licensmodell man använder är beroende av medlemmarnas intentioner, inte nödvändigtvis av andra användares eller kunders behov. Detta innebär att det inte är självklart att man kan få snabb och professionell support eller att man kan få sitt funktionsbehov implementerat. Det går heller inte att beordra individer inom community att arbeta enligt den egna agendan. Vad man kan få beror på vilket inflytande man har på en community. Att bidra till en community innebär inflytande.

Öppen källkod görs tillgänglig i en värdtjänst för lagring av öppen källkod som t ex Github. Github, som ägs av Microsoft, är en webbaserad och centraliserad lagring av versionshistorik för programvaruutvecklingsprojekt som använder versionshanteringssystemet Git. Github erbjuder gratis lagring men även abonnemang för extra funktionalitet.

Att kod görs tillgänglig via en tjänst som Github är dock ingen garanti för kvalitet. I analyser som gjorts (se referenslista nedan) pekas det på många brister i kod. Orsaken till brister kan vara att en community inte förvaltar sin kod tillräckligt aktivt om alls. Detta kan bero på bristande intresse men också för att väldigt få personer i communityn är aktiva och bidrar till underhållet.

En användare kan vara beroende av öppen källkod från ett flertal källor i sitt system. Det kan också finnas system som använder moduler från andra källor som i sin tur använder moduler från andra källor. En rapport indikerar exempelvis att 85% av all granskad kodbas som innehöll öppen källkod var föråldrad med mer än 4 år[8]. Det fanns nya versioner som inte användes pga bristande förvaltning.

[8] 2021 Open Source Security and Risk Analysis Report. Synopsys Inc. 2021. (sid 22)

3.2 Öppen källkod-licenser

I grunden finns det två typer av licenser för öppen källkod:

- Tillåtande licenser
- Stränga licenser, sk copyleft licenser

Inom respektive områden finns en mängd varianter. Vi kommer här inte gå in på dessa delar.

Tillåtande licenser (permissive licenses), exempelvis public domain, innebär att den som modifierar, säljer eller annars sprider programvaran inte är skyldig att göra källkoden tillgänglig. Flertalet tillåtande licenser förutsätter att upphovspersonen attribueras och att licensvillkoren nämns. Kända exempel är ursprunglig och modifierad BSD-licens och Apache License.

Copyleft delas upp i svag respektive stark copyleft. Licenser av typen copyleft syftar till att säkerställa att bidragsgivare delar med sig av sin vidareutveckling av koden. Den som säljer eller sprider koden till andra (men inte den som kör sin egen kod) måste därför distribuera den öppna källkoden med den kompilerade programvaran, åtminstone om koden har ändrats. Licenser för svag copyleft tillåter att koden kombineras med proprietär programvara genom länkning och anrop mellan programkomponenter, medan stark copyleft förhindrar detta[9].

Den mest spridda copyleft-licensen torde vara GNU Public License, GPL (med stark copyleft). Free Software Foundation (FSF) har också publicerat GNU LGPL (med svag copyleft), och den ändå mer restriktiva GNU AGPL.

Problem som kan uppstå är när man försöker kombinera programkomponenter med olika licensformer. Dessa kan vara inkompatibla och det kallas för licensspridning.

4 IT-rättsliga aspekter på öppen källkod *(Detta avsnitt är skrivet av Erik Stavegren, Rättsavdelningen – Enheten för Avtal, IT- och Förvaltningsrätt)*

4.1 Avtal, firmateckning och licenser

Varje nedladdning av öppen källkod innebär att Arbetsförmedlingen accepterar och lovar att efterleva de licensvillkor som den öppna källkoden är förknippad med.

[9] https://sv.wikipedia.org/wiki/%C3%96ppen_k%C3%A4llkod

Befogenhet att teckna avtal för myndighetens räkning tillkommer styrelsen, vartefter den delegeras till Generaldirektören och vidare ner i myndigheten. Det nämns inte i någon av Arbetsförmedlingens arbetsordningar vilka befogenheter rörande tecknande av licensavtal som delegeras. Det nämns inte heller något specifikt om avtal. Det som däremot nämns är att alla chefer har mandat att ”Fastställa behov av anskaffning av varor och tjänster inom ramen för sitt verksamhetsområde.”[10] Ur detta kan uttolkas att det finns ett mandat att teckna avtal för att anskaffa varor och tjänster för alla chefer på nivå 2, inklusive IT-chefen.

Det är alltså i dagsläget generaldirektör och IT-chef som har rätt att teckna licensavtal för öppen källkod för Arbetsförmedlingens räkning. Mandatet får delegeras till chef, enligt arbetsordningen.

4.2 Avsaknad av licens eller brott mot licenser

Utgångspunkten när det kommer till källkod är att den är skyddad av upphovsrätten som litterärt verk. Öppen källkod kännetecknas av att den upphovsrättsligt skyddade koden görs tillgänglig för allmänheten under vissa villkor. Villkoren varierar mellan olika licenstyper.

Om källkod finns tillgänglig utan att det finns information rörande på vilket sätt den får användas kan detta betyda två saker. Det ena är att källkoden har gjorts tillgänglig för allmänheten utan villkor över huvud taget. Det andra är att källkoden har gjorts tillgänglig av någon annan än upphovsrättsinnehavaren. I det första fallet har Arbetsförmedlingen rätt att använda källkoden utan begränsning annat än att respektera den ideella delen av upphovsrätten, nämligen att bli namngiven som upphovsperson och att ens verk inte blir använt i ett kränkande sammanhang. Det är dock mycket svårt att veta vad som faktiskt gäller för en mängd kod där villkoren inte är kända.

I det andra fallet, eller för de fall Arbetsförmedlingen använder källkod i strid med den licens som källkoden omfattas av, kan det röra sig om ett upphovsrättsbrott. Konsekvenserna av det kan vara straffrättsliga (straff för enskild person) eller civilrättsliga (myndigheten blir stämd på skadestånd).

Med hänsyn till dessa risker bör Arbetsförmedlingen bara använda sig av öppen källkod där villkoren är kända och acceptabla för myndigheten.

[10] S. 3 i bilaga 8.1 till Generaldirektörens arbetsordning för Arbetsförmedlingen, Af-2021/0009 5175.

4.3 Licensvillkor

De vanligast förekommande licensformaten bland öppen källkod är varianter av Creative Commons-licenser[11], GPL[12], Apache[13] och BSD 2-clause[14]. De innebär alla att mottagaren av koden får använda, inspektera, ändra och vidaredistribuera källkoden och programvaran. Licenserna i övrigt har vissa olikheter. DIGG rekommenderar i sin policy för öppen källkod[15] att använda sig av Apache eller BSD 2-clause i första hand. I undantagsfall där öppen spridning inte är målet ska GPL-licenser väljas. Av dessa innehåller GPL copyleft-villkor.

Copyleft-villkor kräver i de flesta fall att den bearbetade versionen av programmet distribueras under samma villkor som den kod myndigheten har hämtat, om programmet ska distribueras utanför myndigheten. Det innebär att kan vara utmanande att kombinera två olika koddelar till ett nytt program om de är publicerade under olika licenser som båda innehåller Copyleft. Det är därför viktigt att kontrollera vilka villkor som gäller för öppen källkod som hämtas till myndigheten, särskilt om olika delmängder källkod ska kombineras. Det är särskilt viktigt om programmet som skapas är produkten av samverkan och flera aktörer ska dra nytta av slutprodukten.

4.4 Övrigt om avtalsperspektivet

I övrigt vad gäller avtalsrättsliga perspektiv på öppen källkod hänvisas till texten ”Avtalsgruppen om open source” skriven av Mylaine Hedreul[16].

Det är särskilt viktigt att påpeka att det i princip inte finns några möjligheter att få ersättning från någon annan part om det finns fel i programvaran – vare sig rättsliga eller faktiska fel i programvaran.

På grund av det ovan sagda uppmanar Rättsavdelningen till försiktighet och noggrannhet när det gäller val av vilken källkod som ska användas inom verksamhet som omfattas av säkerhetsskyddslagen. Det måste säkerställas att utomstående inte kan dra slutsatser om verksamheten med hjälp av källkod som finns tillgänglig på ett öppet sätt.

4.5 Lämplig teknisk säkerhet

Det finns anledning att kort beröra att EU:s dataskyddsförordning ställer krav på lämplig säkerhet för personuppgiftsbehandling i artikel 32. Kravet innebär att säkerhetsnivån på system som används för att behandla personuppgifter ska

11 Creatice Commons: Så funkar cc-licenser - Internetstiftelsen
12 GNU General Public License v3 (GPL-3) Explained in Plain English - TLDRLegal
13 Apache License 2.0 (Apache-2.0) Explained in Plain English - TLDRLegal
14 BSD 2-Clause License (FreeBSD/Simplified) Explained in Plain English - TLDRLegal
15 DIGG tar policybeslut kring öppen källkod | DIGG
16 Avtalsgruppen om open source. Arbetsförmedlingen, Rättsavdelningen Sektionen Informationsstrategi, 2021-05-06. Mylaine Hedreul. Dnr: Af-2021/0082 0598.

anpassas till den känslighet hos de uppgifter som behandlas. Eftersom öppen källkod kan ändras av vem som helst finns det därför indirekt ett krav på att granska kvaliteten på den kod som laddas ned för att användas i myndighetens verksamhet, så att den inte påverkar den tekniska säkerheten på ett negativt sätt.

4.6 Förvaltningslagens krav på serviceskyldighet

Det går även att säga att förvaltningslagen innehåller ett indirekt krav på kvalitet på de system som en myndighet använder i sin verksamhet, vilket har framhållits i ett antal yttranden från Justitieombudsmannen.[17] En myndighet är enligt förvaltningslagens 6§ skyldig att se till att en enskilds kontakt med myndigheten blir smidig och enkel. När myndigheten har som strategi att möta enskilda digitalt först blir det därför avgörande för myndighetens möjligheter att leva upp till 6§ förvaltningslagen att den kod som används har en säkerställd kvalitetsnivå. Detta blir särskilt viktigt när det kommer till människor med skyddad identitet, där myndigheten behöver säkerställa att de system som används ger lika goda möjligheter till service för dessa enskilda som för alla andra, eller åtminstone så goda möjligheter som alls är möjligt.

5 Risker

De områden vi kan se risker i för Arbetsförmedlingens hantering av öppen källkod är:

- Kodkvalitet
- Licensbrott
- Ansvar internt

5.1 Kvalitet i kod, komponenter

Slutsatsen från de diskussioner som förekommer i litteraturen är att det inte går att säga om proprietär eller öppen källkod är säkrast. Ett vanligt argumentet för öppen källkod är att om tillräckligt många granskar koden så upptäcks (kanske) ”alla” buggar. Detta förutsätter då att många granskar koden. Det finns också exempel på att kända program från stora leverantörer (som exempelvis Microsoft[18]) har haft allvarliga brister.

De risker vi kan se för kod är:

- Misstag eller bristande kompetens i projektet som leder till dålig kvalitet.
- Medvetna ”fel” för att t ex plantera trojaner eller bakdörrar i en kod[19].

[17] Nu senast till exempel efter en inspektion av Arbetsförmedlingens kontor, särskilt det som sägs om bristande motivering i beslut på grund av begränsningar i antalet tecken i systemet. Inspektion av Arbetsförmedlingens kontor i Solna den 29–30 mars och i Malmö den 26–27 april 2021, hämtat från https://www.jo.se/sv/Inspektioner1/Inspektionsprotokoll/.
18 https://techworld.idg.se/2.2524/1.741108/microsoft-patch-buggar?queryText=Outlook%20trojan
19 https://computersweden.idg.se/2.2683/1.752236/microsoft-varnar-for-cyberattacker-via-kubernetes-kluster

- Fel pga bristande uppdateringar och källans felhantering. Användaren använder en gammal version som innehåller (ofta) kända brister. Att ett fel eller brist inte uppdateras kan t ex bero på att ägaren eller utvecklaren har slutat förvalta just den koden och ingen annan tagit över.
- Man är beroende av ett program som innehåller öppen källkod som i sin tur är beroende av annan öppen källkod. Det blir då en kedja av beroenden. Säkerheten är då beroende av att god förvaltning sker i alla delar av flera andra parter. Det finns analyser[20] som visar att system som beroende av flera kodprojekt kan fortsätta att vara i drift i flera år innan en upptäckt brist har blivit rättad.

En kritisk fråga här är då de projekt man är beroende av och hur kompetenta och seriösa de är. För att bedöma detta bör man ha tillräcklig insyn i hur projektet fungerar och utvecklas. Chaoss[21] (Community Health Analytics Open Source Software) jobbar med att skapa mått på communitys ”hälsa”.

Exempel på frågor här är:

- hur projekten styrs
- hur många experter och utvecklare som aktivt deltar
- hur mycket aktivitet det är i projektet
- hur väl fel- och förändringshanteringen fungerar
- dokumentation, testprocesser och kvalitetskontroll.

Eftersom man inte alltid kan veta hur en community kommer att utvecklas eller om de funktioner man själv behöver kommer att tas om hand bör egen kompetens för utveckling, förvaltning och kvalitetskontroll finnas. I detta ingår då användning av olika analysverktyg.

En andra kritisk fråga är hur vi säkerställer att kod inte innehåller säkerhets- (eller andra) brister. Krav som ska ställas är att koden granskas av en annan person än utvecklaren. Det kan ske med hjälp av program som går igenom källkoden och hittar alla relationer till annan öppen källkod. Ett förslag är att sådana program körs regelbundet i Arbetsförmedlingens drift och utvecklingsmiljöer. Andra förslag är att förslagsvis två personer granskar koden. Att koden testas i en utvecklarmaskin. Att penetrationstest av koden sker innan lansering. Med tanke på att penetrationsteser är en begränsad resurs bör prioritering baseras på risk och hur känslig produkten eller byggstenen är.

Ansvaret för kvalitetskontroll kan naturligtvis läggas på en extern part. Ur Arbetsförmedlingens eller kundens perspektiv skiljer sig detta inte principiellt från en leverantör av proprietär programvara. Ur kundens perspektiv blir det en avtalsfråga. Två exempel på sådana leverantörer som Arbetsförmedlingen använder är Red Hat (För Linux) respektive Vertel (för Ubuntu Linux och Odoo, för CRM).

20 Se t ex 2021 Open Source Security and Risk Analysis Report. Synopsys Inc. 2021. Sid 22
21 https://chaoss.community

En särskild fråga är vilka krav på kontroll som ska ställas på system som på något vis berörs av säkerhetsskyddslagen eller av andra skäl är särskilt skyddsvärda. Det bör innebära att Arbetsförmedlingen har än större krav på att ha kontroll på den kod som ingår och att skadlig kod inte kan planteras.

5.2 Licensrisker

Som nämnts ovan finns det en stor mängd olika licenser för öppen källkod. Att koden är öppen innebär inte fullständig frihet. Vid användande av öppen källkod har man accepterat den licens som utvecklaren har skrivit.

Risker vi kan se med licenser för öppen källkod:

- Att vi använder licenser som är olämpliga. Ett exempel kan vara stränga copyleft-licenser. Vid distribution ska vi dela tillbaka eventuella ändringar och anslutande källkod. Detta är då ett åtagande som myndigheten gjort, inte det enskilda projektet. Vill vi inte dela med oss av koden, kan vi sluta och använda aktuellt projekt. Den reella konsekvensen vid vägran är bara att rätten till licensen upplöses. För att veta vad som är olämpligt bör en analys göras av vilka licenser som är lämpliga och olämpliga. Det finns också exempel på licenser som är otydliga, exempelvis (JSON) att koden enbart får användas till att göra gott, inte ont (shall be used for good, not evil)[22].
- Att vi har flera olika licensmodeller i ett och samma system och att dessa konfliktar. Det kan också vara en konflikt mellan öppen och proprietär kod. Om detta förekommer inom Arbetsförmedlingen utreds inte här.
- Att vi använder kod som inte har någon licens. Detta kan innebära upphovsrättsbrott.
- En konsekvens av detta är att Arbetsförmedlingen (eller den som hämtade hem koden) kan bli stämda för upphovsrättsintrång.

Risken att bli stämd för upphovsrättsbrott i Sverige måste betraktas som minimal idag. Vi kan inte hitta något svenskt exempel även om det kan ändras i framtiden. I amerikansk rätt finns fall där det mest kända borde vara SCO mot IBM[23]. Ett annat fall, Jacobsen v. Katzer[24], innebär att det är möjligt att stämma ett brott mot en Open Source-licens som ett upphovsrättsbrott och inte bara som ett avtalsbrott. De juridiska riskerna diskuteras[25, 26].

I analyser som gjorts[27] visas det att över hälften av alla kodbaser som analyserats för år 2020 innehöll licenskonflikter. 26 % innehöll öppen källkod utan licens. Trenden är sjunkande (enligt denna redovisning) men risken är fortfarande ganska hög. Det

[22] Se t ex Sid 16 “2021 Open Source Security and Risk Analysis Report. Synopsys Inc. 2021”
[23] https://en.wikipedia.org/wiki/SCO%E2%80%93Linux_disputes
[24] https://macworld.idg.se/2.1038/1.174694/amerikansk-domstol-slar-ett-slag-for-oppen-kallkod
[25] https://www.lindahl.se/aktuellt/insikter/2020/hur-och-nar-open-source-riskerar-att-smitta-och-vad-du-kan-gora-for-att-undvika-det/
[26] https://www.dentons.com/en/insights/articles/2020/august/25/open-source-software-litigation-windfall-or-landmine
[27] Se t ex: 2021 Open Source Security and Risk Analysis Report. Synopsys Inc. 2021

finns verktyg för att göra sådana analyser. Enligt uppgift ska sådana finnas inom Arbetsförmedlingen.

5.3 Ansvar internt

Ett tredje riskområde är hur organisationen hanterar dessa risker. Dessa områden kan delas in i:

- Vem har rätt att ingå licensavtal med upphovsrättsinnehavaren/havarna till öppen källkod.
- Vem är ansvarig för att vi inte hamnar i en licenskonflikt. T ex om flera produkter ingår i en plattform och de olika ägarna har olika licensavtal.
- Vad innebär det juridiskt om vi inte uppfyller (enligt lag) rimliga kvalitetskontroller av kod.
- Vilka krav på kvalitetskontroll av kod och kontroll av projektet ska vi ha i avtal med en extern leverantör.

När vi använder öppen källkod ingår vi i ett licensavtal med upphovsrättsinnehavaren till koden. Det är då myndigheten som ingår detta avtal, inte den enskilde utvecklaren eller projektledaren. Att inte uppfylla ett licensavtal innebär att myndigheten kan förlora rätten att använda aktuell licens, dvs. kan ej distribuera projektet vidare enskilt eller i bearbetad form. Stämning kan vara en möjlig konsekvens i vissa fall. En följdfråga är då vad som blir konsekvensen om en icke behörig (anställd eller konsult) använder otillåten kod.

Sannolikt blir det Arbetsförmedlingens ansvar om detta inte är reglerat. Detta medför ett par konsekvenser som kan behöva utredas:

- Är det tillräckligt illa för att inleda ett ärende i Personalansvarsnämnden för den anställde? Kan vara en fråga för IT och HR.

- Arbetsförmedlingen är bundet av licensavtalet om inte ägaren till koden hade anledning att misstänka att vår anställde inte hade rätt att ingå avtal, s.k. ond tro. Det borde så gott som aldrig varit möjligt vad gäller öppen källkod. Det bör även utredas kring AFs inställning till sk Community License Agreements (CLAs) och den enklare formen DCOer (Developer Certificate of Origin), där man frånskriver sig upphovsrätt, förtydligar att man är skapare till verket och accepterar att den får spridas under aktuell licens.

- Copyleft-smitta på kod som AF har utvecklat. Även om öppen källkod inte nödvändigtvis är mindre säkert än proprietär kod, så kan det finnas kod vi inte ska sprida av säkerhetsskäl.

Kritiska frågor är vilka licensformer som är acceptabla och vilka som inte är det och vem som beslutar vilka licenser (kod) som får användas för att undvika licensbrott och licenskonflikt.

Arbetsförmedlingen hanterar en stor mängd personuppgifter som är under stark sekretess. Om Arbetsförmedlingen inte kvalitetssäkrar kod som används tillräckligt

väl kan det innebära brott mot Dataskyddsförordningen och Förvaltningslagen (se avsnitt ovan om IT-rättsliga aspekter).

I de fall en extern leverantör utvecklar och förvaltar kod åt Arbetsförmedlingen ska motsvarande krav ställas på denne. Detta regleras i ett avtal.

6 Övergripande förslag

För att olika projekt ska kunna uppfylla sitt ansvar bör vissa övergripande stöd tas fram.

Det bör det tydliggöras vem som är ansvarig för att ett projekt hanterar öppen källkod i enlighet med Arbetsförmedlingens policy, dvs krav på kontroll av kodkvalitet och licenser, i bred mening krav på projektets hälsa.

- **Förslag**: Produkt och byggstensansvarig ansvarar för hanteringen av sin kodkvalitet och projekts hälsa.

Verktyg för och bevakning av projekts hälsa bör på sikt kunna hanteras centralt. Denna fråga bör förslagsvis utredas vidare.

Rättsavdelningen bör ta fram riktlinjer för vilka licenser för öppen källkod som är lämplig och acceptabla för Arbetsförmedlingen och vilka som är oacceptabla. I detta ingår att utveckla kompetens att allmänt kunna bedöma licenser för öppen källkod för att kunna ge råd samt göra en konsekvensbedömning om ett projekt anser sig behöva kod under andra licenser.

- **Förslag**: Rättsavdelningen ansvarar för att bedöma och rekommendera lämpliga licensformer.

Eventuellt kan ansvaret för rekommendation av lämpliga licenser flyttas över till ett framtida OSPO. På sikt bör Arbetsförmedlingen på myndighetsnivå kunna redovisa vilka licenser, licenskonflikter etc som Arbetsförmedlingen hanterar. Var detta ansvar ska ligga finns i nuläget inget förslag på.

IT avdelningen bör utreda och rekommendera lämpliga verktyg för analys av licens och kodkvalitet samt föreslå en process för hur dessa ska tillämpas och följas upp. I detta ingår ansvar för de olika delarna. En lista på verktyg (ej komplett) finns slutet av denna PM.

- Förslag: VO IT ansvarar för verktyg för licensefterlevnad och kodkvalitet.

Förslag: Övergripande stöd till Arbetsförmedlingens utvecklingsprojekt:

- Starta upp ett OSPO[28] (Open Source Program Office). En grupp med olika experter som kan stödja initiativ att uppfylla kraven. En början är att en grupp utvecklar vad som kan bli Arbetsförmedlingens OSPO beroende på vilka frågor som visar sig vara relevanta. En OSPO kan på sikt ta centrala

[28] A guide to setting up your Open Source Program Office (OSPO) for success | Opensource.com

ansvaret för koordinering, utbildning, facilitering och uppföljning. Detta är en viktig aspekt för att hålla samman alla delar rörande konsumtion, bidrag, communitysamverkan, licensuppfyllnad, utbildning och kulturfrämjande.

- Frågan om öppen källkod tas upp i säkerhetsresan i en egen flik. Den ska redovisas som övriga delar i säkerhetsresan. Om öppen källkod inte används ska denna flik inte användas. Därmed tydliggörs ansvaret att hantera frågan enligt Arbetsförmedlingens policy.

7 Om policy för öppen källkod

Utifrån denna analys är slutsatsen att Arbetsförmedlingen behöver en policy som reglerar intag/konsumtion av öppen källkod i myndighetens olika produkter, plattformar och byggstenar. Resonemanget utgår från egen utveckling inom myndigheten men motsvarande krav bör gälla när utvecklingen hanteras av en extern part.

En policy bör innehålla följande områden.

- Organisation och ansvar
- Communitysamverkan
- Licenser
- Kodkvalitet och rutiner

7.1 Om organisation och ansvar.

En nyckelfråga är att tydliggöra var ansvaret för att ett Arbetsförmedlingsprojekt eller initiativ hanterar öppen källkod på ett korrekt sätt. I detta ligger att hantera licensfrågor och kodkvalitetsfrågor. Förslagsvis bör det operativa ansvaret ligga på produkt- och byggstensansvarig.

I ansvaret bör då ligga att följa Arbetsförmedlingen policy för hantering av öppen källkod. Viktiga områden här är:

- Att kunna redovisa vilka communitys projektet är beroende av, på vilket sätt bedömning av projektet har gjorts och vilka risker beroendet innebär.
- Att kunna redovisa vilka licenser och avtal projektet ingått och om avvikelser från rekommenderade licensformer finns. Om så är fallet, varför har så skett och hur hanteras konsekvenserna. Avvikelser bör förslagsvis rapporteras till Rättsavdelningen.
- Vilka åtaganden mot community har man ingått.
- Att baserat på riskanalys och informationsklassificering granska mottagen kod.
- Att om koden ingår i en lösning som faller under säkerhetsskyddslagen eller har andra särskilda skyddsvärden kunna redovisa hur kraven på säkerhet hanteras. Denna kod bör normalt inte göras tillgänglig. Om så sker (av

licensskäl eller andra skäl) bör det förslagsvis rapporteras till Rättsavdelningen och Riskmanager.
- Att kunna redovisa hur kvalitetskontroll av kod sker. I detta ingår vilka verktyg som används och om penetrationstest genomförs och vilka resultat analysen visat.

7.2 Om communitys

Ansvarig ska göra bedömning av, men även vid behov uppföljning, av de communitys Arbetsförmedlingen är beroende av. Grundfrågan är i vilken grad Arbetsförmedlingen kan lita på ett projekt och den kod projektet levererar. Vinnova har påbörjat ett projekt för att motarbeta sårbarhetsrisker i användning av öppen källkod[29]. En annan aspekt är vilka communitys som Arbetsförmedlingen vill medverka i utifrån ett varumärkesperspektiv.

Exempel på frågor som ingår vid kvalitetsbedömning av communitys och projekt:
- Kommer projektet att finnas kvar och vara aktivt om två år?
- Sker det en aktiv utveckling och underhåll av projektet?
- Kan projektets källkod laddas ner, användas, spridas och förändras utan motprestation. Är motprestationen acceptabel?
- Sker utvecklingen öppet och utspritt på flera individer? Kommer deltagarna från flera organisationer.
- Har deltagande organisationer eller personer därifrån en policy för hur de arbetar med öppen källkod?
- Kan användare påverka utvecklingen av projektet?
- Hur distribueras projektets källkod? Den bör distribueras under en licens som är godkänd av Open Source Initiative. https://opensource.org/licenses.
- Kommer det att finnas support tillgänglig?
- Finns det kvalitetskontroll av kod. Finns det förvaltnings och förändringsprocesser? Har projektet en kommitté eller motsvarande som granskar och godkänner kodbidrag för att säkerställa kvaliteten på källkoden innan den accepteras av projektet?
- Är Projektet publikt tillgängligt på internet där källkod, felrapporter och förbättringsförslag kan läsas av vem som helst?
- Hur analyseras koden för att upptäcka säkerhetsbrister? Verktyg? Penetrationstest?
- Finns det system för skadeersättning?

En bedömning bör göras hur förvaltning av kod ska hanteras om aktuellt projekt av något skäl slutar att förvalta kod Arbetsförmedlingen är beroende av.

[29] https://www.vinnova.se/p/metodstod-for-svensk-industri-att-mota-sarbarhetsrisker-i-anvandningen-av-oppen-programvara

7.3 Om licenser

Målsättningen bör vara att programvaruprojekt som ska tillhandahålla öppen programvara väljer en välanvänd licens för öppen programvara som innehåller av Rättsavdelningen godkända licenser. Licensen ska företrädesvis följa ”Open Source Definition” och vara godkänd av Open Source Initiative (http://opensource.org). Programvaran ska utvecklas öppet på GitHub eller motsvarande värdtjänst.

Det är dock viktigt att vi inte skapar onödig friktion. Målet är att utvecklare och projektledare enkelt ska kunna fatta rätt beslut. Ett OSPO skulle kunna vara ett sådant stöd.

Licenser med sträng licens (copyleft) som tvingar användare att licensiera anslutande kod med samma licens bör undvikas. Det kan dock finnas skäl att använda kod med sträng licens.

Produkt- eller byggstensansvarig ska kunna redovisa orsaken till valet av licens och vilka konsekvenser det medför. En riskbedömning för valet av licens ska göras och redogöra för licenskonflikter. Allvarliga risker som val av licens medför ska rapporteras till Riskmanager eller annan utsedd part t ex OSPO.

I de fall kod ingår i en produkt eller byggsten som faller under säkerhetsskyddslagen eller är extra skyddsvärt av andra orsaker får licensvalet inte leda till ökad risk. Risk och konsekvensbedömningen ska redovisas.

Vilket verktyg för licenskontroll som använts ska redovisas.

7.4 Om kod

Den kod som används i Arbetsförmedlingens byggstenar och produkter ska vara säker och inte medföra onödiga risker. I detta ingår t ex att uppdatera bibliotek till senaste versionen för att minimera risken för sårbarheter. Innan en sådan uppdatering måste det självklart analyseras om den nya versionen är säker och inte orsakar andra problem.

Produkt eller byggstensansvarig ska säkerställa att använd kod och dokumentation, egenutvecklad eller hämtad, kvalitetssäkras. En motsvarande process kan behövas för kod och dokumentation som Arbetsförmedlingen ska bidra tillbaka med till det öppna programvaruprojektet. Utan externa bidrag försvinner många av de fördelar och värde som öppen programvara kan bidra till.

- En riskbedömning av kod ska göras:
    - Om den innehåller information (t ex personuppgifter) som är extra känsliga och som därmed ställer högre krav än Arbetsförmedlingen bassäkerhet.
    - Om kod används inom ett område som faller under säkerhetsskyddslagen eller som i säkerhetsresan bedöms som extra skyddsvärd.
- Kod ska kvalitetsgranskas förslagsvis av två personer. Riktlinjer för sådan granskning bör tas fram av VO IT.

- Kod testas i verktyg[30] för att identifiera säkerhetsrisker. Vilket verktyg som används och resultat av analys ska kunna redovisas.
- Inför varje nylansering av större funktion bör penetrationstest göras för att identifiera IT säkerhetsluckor enligt deras rutin. Behovet (prioriteringen, se ovan) beror på hur kritiskt eller känslig funktionen är. Dessa test utförs av andra personer än de som utvecklat och testat.

30 T ex: guides/tools-for-managing-open-source-programs.md at master · todogroup/guides · GitHub

Intervjuade

- Bengt Bäverman
- Maria Dalhage
- Jonas Södergren
- Lotta Råberg
- Malin Åkerlund
- Erik Stavegren
- Fredrik Arvas
- Johan Linåker, PhD Postdoctoral Researcher. Software Engineering Research Group | Dept. of Computer Science | Faculty of Engineering | Lund University
- Mark Driver. Gartner Interaction. Videointervju 25 maj 2021.

Samtliga intervjuade utom Mark Driver, Gartner, har också varit referensgrupp.

Referenser

Hur vill Arbetsförmedlingen arbeta med open source. Arbetsförmedlingen Jobtech PPT. Maria Dalhage 2021-02-08.

Introduktion till öppen programvara. PPT. Johan Linåker PHD. Lunds Universitet

10 myter om öppen källkod (digitalist.se)

The DIY Guide to Open Source Vulnerability Management. Synopsis Inc 2020

Securing Open Source Libraries. *Managing Vulnerabilities in Open Source Code Packages*. Guy Podjarny. O'Reilly Media, Inc. 2019

Ensure Safe and Successful Usage of Open-Source Software with a Comprehensive Governance Policy. Published 20 November 2020 - ID G00732588. By Analysts Anne Thomas, Arun Batchu. Gartner

2020 Open Source Security and Risk Analysis Report. Synopsys Inc. 2020.

2021 Open Source Security and Risk Analysis Report. Synopsys Inc. 2021.

State of Open Source Security Report 2020. snyk. Report author: Alyssa Miller. Report editor: Eirini Eleni Papadopoulou.

Förslag till: Inriktningsdokument för hantering av öppen källkod. Ver 0.06. 2021-03-26. Underlag under framtagande av CRM-projektet, Odoo (Fredrik Arvas, Jason Andersson)

Linux Foundation låter utvecklare signera öppen källkod – techworld 2021-03-11. https://techworld.idg.se/2.2524/1.748108/sigstore-signera-oppen-kallkod

Community Health Analytics Open Source Software https://chaoss.community/

Threats, Risks, and Mitigations in the Open Source Ecosystem Michael Scovetta, Microsoft in collaboration with the Open Source Security Coalition. wg-identifying-security-threats/Threats, Risks, and Mitigations in the Open Source Ecosystem - v1.1.pdf at main · ossf/wg-identifying-security-threats · GitHub

Red Hat Product Security. Risk Report: 2019. rh-2019-risk-report-overview-f21332wg-202003-en_0.pdf (redhat.com)

Defense in depth with Red Hat Insights. February 24, 2021Mary Roark. Defense in depth with Red Hat Insights

Red Hat Risk Report: A tour of 2020's branded security flaws. March 1, 2021 Christopher Robinson. Red Hat Risk Report: A tour of 2020's branded security flaws

What to do about open source vulnerabilities? Move fast, says Linux Foundation expert. The Register, Tim Anderson wed 26 May 2021. What to do about open source vulnerabilities? Move fast, says Linux Foundation expert • The Register

Linux Foundation Compliance Program: Generic FOSS Policy (Free and open-source software) policies/lf_compliance_generic_policy.pdf at master · todogroup/policies · GitHub

Tools for Managing Open Source Programs. guides/tools-for-managing-open-source-programs.md at master · todogroup/guides · GitHub

Avtalsgruppen om open source. Arbetsförmedlingen, Rättsavdelningen Sektionen Informationsstrategi, 2021-05-06. Mylaine Hedreul. Dnr: Af-2021/0082 0598.

Analys av DIGG:s policy för utveckling av programvara. University of Skövde, Professor Björn Lundell (Ph.D.) 2020-05-20.

Öppen programvara i offentlig förvaltning – En juridisk inblick, Erik Woodcock, Markus Holm. Ett PM från det IT-rättsliga observatoriet, ITObservatoriePM 17:2003

Upphandling av IT – inlåsningseffekter och möjligheter. Uppdragsforskningsrapport 2013:2. Richard Wessman. Konkurrensverkets uppdragsforskningrapport 2013:2.

DIGG (Myndigheten för Digital Förvaltning) Policy för utveckling av programvara, Ärendenummer: 2019–136. 2019-05-08.

https://www.lindahl.se/aktuellt/insikter/2020/hur-och-nar-open-source-riskerar-att-smitta-och-vad-du-kan-gora-for-att-undvika-det/

https://www.dentons.com/en/insights/articles/2020/august/25/open-source-software-litigation-windfall-or-landmine

Länkar till verktyg

https://github.com/todogroup/guides/blob/master/tools-for-managing-open-source-programs.md

https://www.blackducksoftware.com/

https://www.whitesourcesoftware.com/

https://www.flexera.com/solutions/challenge/application-security/open-source-license-compliance.html

https://www.sonatype.com/

https://jfrog.com/

https://www.roguewave.com

https://tidelift.com/