Granskning av behörigheter
Laxå kommun

Martin Bernhardtz, projektledare
Linnéa Holm

Februari 2019

LAXÅ KOMMUN

pwc

Innehåll

1 Inledning

Om uppdraget

Bakgrund

Verksamheternas utveckling i en kommun har med åren blivit alltmer IT-beroende, vilket medför nya risker och hot. Behörighetsstyrning och åtkomstkontroll blir då i sammanhanget en viktig och central komponent i kommunens arbete med informationssäkerheten. Detta arbete innebär bland annat upprättande av rättigheter för användare så att dessa enbart får åtkomst till den information och de applikationer som de behöver i sitt dagliga arbete.

Syfte och revisionsfråga

Syftet med granskningen är att bedöma om den interna kontrollen är tillräcklig när det gäller **tilldelning**, **ändring**, **uppföljning** och **borttag** av behörigheter i kommunens datasystem.

Granskningen ska besvara följande revisionsfrågor:

- *Är kommunstyrelsens och nämndernas interna kontroll avseende behörigheter i kommunens datasystem tillräcklig?*

Revisionskriterier

Behörigheter, interna styrdokument och policys samt respektive nämnds regelverk.

Kontrollmål

- Det finns rutiner på plats för att säkerställa att befintliga riktlinjer och policys följs.
- Det finns ett systemstöd för att säkerställa god intern kontroll.
- Behörighetstilldelning, ändring och borttag sker på ett säkert och ändamålsenligt sätt.
- Det finns en ansvarsfördelning mellan olika roller/behörigheter i systemen som kontinuerligt säkerställs.
- Logglistor över förändringar i fasta data hanteras på ett säkert och ändamålsenligt sätt.

Metod och avgränsning

Metod

Granskningen har genomförts genom intervjuer med ansvariga tjänstemän.

Genomgång och analys av relevanta dokument och dokumentation av eventuella kontroller. Viss verifiering av genomförda kontroller sker genom urval.

Avgränsning

Granskningen avgränsas till kommunstyrelsen, barn- och utbildningsnämnden, omsorgs- och socialnämnden samt Sydnärkes miljönämnd.

Intervjupersoner

- Kommunchef tillika säkerhetschef
- Ekonomichef
- Personalchef
- IT-support
- IT-chef

2

Kontrollmål
lakttagelser och bedömningar

Kontrollmål

Det finns rutiner på plats för att säkerställa att befintliga riktlinjer och policys följs.

Iakttagelser

I Laxå kommun finns i dagsläget inga styrande dokument eller riktlinjer som reglerar behörighetshantering.

Riktlinjer för behörighetstilldelning, ändring eller borttagning av behörigheter saknas. Ansvarsfördelningen är ej reglerad varken i riktlinjer eller genom internkontroll, det finns heller inte någon reglering kring uppföljning eller revidering. Enligt intervjusvar finns vissa rutiner på plats som är kända och tillämpade. Exempelvis finns en känd praxis kring behörighetstilldelning, ändring och borttag där närmsta chef är ansvarig för beställning av behörigheter. Dessa rutiner är dock inte formaliserade och följs inte upp på ett systematiskt sätt.

Informationssäkerhetspolicyn som är framtagen i kommunen har viss bäring mot behörighetshantering men saknar explicit reglering kring behörigheter.

Bedömning

En viktig del i behörighetsstyrningen gäller uppföljning och kontroll av befintliga behörigheter samt eventuella avvikelser. Då Laxå kommun saknar formaliserade processer för uppföljning, finns det en stor risk inom kommunen att behörigheter hanteras felaktigt utan att det åtgärdas.

Vidare leder frånvaron av styrning till "Ad Hoc" förfaranden som präglas av osäkerhet då tillämpning av rutiner riskerar att skilja sig från situation och person.

Laxå kommun bör beakta hur nyttjande och uppföljning av behörigheter ska kontrolleras för att kunna säkerställa spårbarhet. Vidare lever kommunen inte upp till tredje stycket i informationssäkerhetspolicyn som stipulerar krav på både riktighet och spårbarhet. Då formaliserade rutiner inte finns på plats riskerar information att otillbörligt ändras. Då det saknas rutin för logghantering blir även kravet på spårbarhet svårt att uppfylla.

Kontrollmålet bedöms vara:

ej uppfyllt

Kontrollmål

Det finns ett systemstöd för att säkerställa god intern kontroll.

Iakttagelser

I dagsläget finns det inte ett systemstöd för att säkerställa god intern kontroll. Intervjuerna uppmärksammar att det pågår ett arbete för att upprätta en plan för intern kontroll men den saknas i nuläget. Det pågår även ett arbete med att optimera kommunens IT-miljö. I det ingår en plan på att sammanföra kommunens Active Directory, (AD) med ett gemensamt AD för Sydnärkes IT-nämnd. Enligt intervjusvar kan ett systemstöd komma att införas i och med optimeringen.

Bedömning

Risken som är förknippad med avsaknaden av systemstöd innebär att kontroll är avhängig manuella processer. Manuella processer är i hög grad präglade av personberoende och underminerar systematik och uppföljning. Med särskild hänsyn till att Laxå kommun i nuläget saknar en plan för intern kontroll blir behörighetshantering en osäker process från början till slut.

Laxå kommun bör fortsätta utveckla och optimera systemkontroll genom att införa automatiserade processer som stödjer kommunen i arbetet att uppnå och säkerställa god intern kontroll.

Kontrollmålet bedöms vara:

ej uppfyllt

Kontrollmål

Behörighetstilldelning, ändring och borttag sker på ett säkert och ändamålsenligt sätt.

Iakttagelser

Processen för behörighetsstyrning (tilldelning, ändring och borttag) är till viss del känd i kommunen, den är dock inte formaliserad eller vidare fastställd. Det finns en osäkerhet gällande personberoende i hanteringen av ändringar då rutiner förlitar sig på personliga relationer mellan beställare och utförare. Processen är genomgående baserad på tillfälliga ändamål.

Vidare sker ingen kommunikation kring vad behörigheter innebär i vidare mening samt ur ett ansvarsperspektiv.

Det finns för närvarande inga rutiner kopplade till längre frånvaro vid exempelvis föräldraledighet/tjänstledighet.

Enligt intervjusvar är det respektive chef som är ansvariga för att göra en beställning av behörigheter för sina anställda hos IT-supporten. Detsamma gäller om behörigheter ska ändras eller avslutas. Detta är dock inte formellt fastställt. I de system som ej är kopplade till AD sker en liknande process där utpekad ansvarig sköter behörigheter.

Vidare uppges vid intervjuer att användare uppger sitt personnummer som legitimering hos IT-supporten då den vill ändra exempelvis lösenord.

Bedömning

Det är av yttersta vikt att skapa strukturerade processer och kontroll av behörighetshantering genom samtliga faser som hör identitets- och behörighetsstyrning till. Dessa faser innefattar hur behörigheter tilldelas, ändras och hur de tas bort.

Rutinen för legitimering hos IT-supporten bedöms vara godtycklig. Personnummer ska enligt informell rutin uppges men personliga förhållanden möjliggör förbiseende för denna kontroll. Laxå kommun bör således formalisera processen för legitimering genom exempelvis ökad autentisering. Det bör i sammanhanget även noteras att personnummer är en extra skyddsvärd personuppgift.

Laxå kommun bör upprätta ett tydligt ägarskap av kontomodellen och behörigheter. Personalavdelningen kan vara en lämplig hamn för detta ansvar då de redan har ett övergripande ansvar för samtliga anställda och upprättande av grundbehörigheter.

Kontrollmålet bedöms vara:

ej uppfyllt

Kontrollmål

Det finns en ansvarsfördelning mellan olika roller/behörigheter i systemen som kontinuerligt säkerställs.

Iakttagelser

Enligt intervjusvar finns det ingen formell nivåindelning av användare och dess behörigheter. Behörigheter baseras på förutvarande person på samma tjänst. Enligt intervjusvar är det upp till varje chef att bedöma vilken typ av behörighet en användare ska ha.

Det görs inte någon analys över behörighetstilldelning ur en säkerhetssynpunkt, istället baseras behörigheter på tillgänglighet och funktionalitet. Användarvänligheten är prioriterad över säkerhet.

Av intervjuer framkommer att det inte genomförs någon uppföljning för att säkerställa ansvarsfördelningen, att rätt person eller roll har rätt behörighet.

Bedömning

Identitets- och behörighetsstyrning har som syfte att möjliggöra att rätt person får tillgång till rätt information. Dessutom ska det finnas en skälig grund till varför en person ska ha en viss behörighet. Därför bör kommunen definiera ett tydligt ägarskap för processen för att processägaren i sin tur ska kunna ställa krav och kontrollera efterlevnad på ett adekvat sätt.

Området behörighetsstyrning lägger stor vikt vid hantering av höga behörigheter, vilka i Laxå kommun kallas chefsbehörigheter. Dessa behörigheter innefattar ofta fullständig behörigheter till kritiska IT-system och är särskilt viktiga att kontrollera. Laxå kommun kan med fördel genomföra en behovs- och riskanalys för att på så sätt uppnå en väl avvägd behörighetstilldelning. Vidare bör kommunen strukturera ansvarsfördelningen mellan olika behörighetsnivåer samt säkerställa att dessa användare är medvetna om ansvaret kopplat till en viss behörighet.

Kontrollmålet bedöms vara:

ej uppfyllt

Kontrollmål

Logglistor över förändringar i data hanteras på ett säkert och ändamålsenligt sätt.

Iakttagelser

Enligt intervjusvar finns ingen kontroll över logghantering och vidare saknas tydligt ägarskap i hantering och kontroll av logglistor. Ändringar i behörigheter loggas men omhändertagandet av loggarna är inte säkerställt på ett kontrollerat sätt.

Bedömning

Det finns i Laxå kommun ingen kontroll av logghantering. En process för logghantering bör inrättas för att säkerställa korrekt hantering och kontroll. Vidare bör ägarskapet av logghantering ses över, ett tydligt ägarskap bör upprättas där det finns en uppdelning mellan logghantering och kontroll av densamma. Laxå kommun bör vidare överväga att lägga ansvar för logglistor hos en funktion som är frånställd IT. Detta för att undvika att samma funktion har möjlighet att ändra behörigheter och samtidigt kunna göra ändringar i loggar för behörighetsändring.

Kontrollmålet bedöms vara:

ej uppfyllt

3

Sammanfattning & rekommendationer

Sammanfattning

Identitets- och behörighetsstyrning i Laxå kommun.

Laxå kommuns behörighetsstyrning är präglad av informella rutiner och situationsanpassat förfarande. Detta leder till ett antal risker då behörigheter lätt kan utnyttjas i felaktigt syfte. Uppföljning på området saknas vilket ytterligare stärker ovan nämnda risk. Laxå kommun är en förhållandevis liten kommun där personliga förhållanden mellan medarbetare kan vara en fördel i det dagliga arbetet, startsträckorna blir kortare och kommunikation mellan olika delar i kommunen förenklas. Å andra sidan skapar personberoenden ett mått av osäkerhet då rutiner lätt blir grundade i person snarare än i regelverk.

Vidare saknar Laxå kommun ett tydligt ägarskap av behörighetsstyrningens samtliga delar. Ansvaret för uppföljning och kontroll bör tydliggöras då det i nuläget präglas av osäkerhet. Exempelvis bör ansvaret för kontroll i form av logghantering ligga på funktion frånställd IT. För att minimera risker kopplade till behörigheter bör en tydligare separation göras mellan den som har möjlighet att ändra behörigheter och den som har möjlighet att ändra i loggarna.

Rekommendationer

- Upprätta riktlinjer och policys för behörighetsstyrning och formalisera processen för uppföljning av dessa.
- Säkerställ tydligt ägarskap och ansvar för behörigheter, både för beställare och för utförare.
- Formalisera anställningsprocessen och med den behörighetstilldelning samt information angående behörigheter och ansvaret kopplat till dessa.
- Formalisera förändringsprocessen då användare byter roller eller ansvarsområden. Vid tilldelning eller ändring av behörigheter bör formella rutiner följas.
- Formalisera processen vid anställningens upphörande. Vid borttag av behörigheter bör rutiner finnas på plats för att öka säkerheten och minska risken för att inaktiva konton ligger kvar.
- Säkerställ adekvat uppföljning av behörigheter samt rutiner som möjliggör kontroll.
- Överväg att införa automatiserade processer kopplade till Active Directory. Detta underlättar kontrollen av behörigheter som varit inaktiva under längre tid.

Rekommendationer (forts.)

- Överväg insatser för att medvetandegöra ansvaret som är kopplat till olika behörighetsnivåer. Information kan med fördel ges vid nyanställning angående vikten av korrekt hantering av behörigheter.

- Överväg att nivåindela och standardisera behörigheter för att underlätta korrekt ansvarsfördelning. Detta fungerar som ett stöd och en kontroll både för beställare och för utförare av behörighetstilldelning och ändring.

- Överväg att genomföra en teknisk kontroll av samtliga kontoinställningar i Active Directory för att få klarhet i rådande status.

2019-02-27

Martin Bernhardtz
Projektledare

Lars Dahlin
Uppdragsledare