ÄLVSBYNS KOMMUN
Kommunrevisionen

SLUTDOKUMENT
2017-12-06

För kännedom:
Kommunfullmäktige
Partiernas gruppledare
Kommunchef
Socialchef
IT-chef

Till:
Kommunstyrelsen

Granskning av behörigheter och loggkontroller

Vi har granskat hanteringen av behörigheter och åtkomstkontroll i kommunens datoriserade verksamhetsstöd Viva. Behörighetshantering och åtkomstkontroll bedömer vi är en viktig och central komponent i kommunens arbete med informationssäkerheten.

Vi har granskat styrdokument, intervjuat samt analyserat data för första halvåret 2017 från Viva (användarinformation och loggar), anställningsdata från PA-systemet samt utdrag ur kommunens katalogsystem (AD: et). Granskningen har varit inriktad mot att avgöra om tilldelningen av behörigheter följer de styrande dokumenten och via analysen göra bedömningar hur man lyckas efterleva dem i praktiken.

Från granskningen vill vi särskilt framhålla följande:

- Kontroll av den så kallade händelseloggen har utförts under januari 2017. Enligt uppgift lika mycket som ett test av instruktionerna som en regelbundet åter-kommande kontroll. Den instruktion som använts är en lovande början men den saknar delar som kan kompletteras genom att ansluta till de instruktioner som socialstyrelsen så sent som i mars 2017 uppdaterade.

- Det är otillfredsställande att det inte finns en formaliserad och dokumenterad hantering av behörigheter i Viva som även de efterlever socialstyrelsens föreskrifter.

- Både kommunens och granskad verksamhets styrande dokument vad gäller in-formationssäkerhet har stora brister och förehåller sig inte till varandra på ett sätt som underlättar förståelse och efterlevnad. Kommunen är i stort behov av att snarast upprätta ett nytt modern riskanalyserad ledningssystem för att åt¬gärda detta. Regelbundet måste det sedan ske en organiserad kontroll så att alla känner till styrningen, vad den innebär samt att de förstås och efterlevs.

- Våra jämförande analyser av data från olika källor redovisar risk för brister som bör undersökas likaväl som åtgärdas. Vi anser att analysresultaten och kommunens egen uppföljning av dessa ska ligga till grund för de metoder som behöver införas för loggkontrollen.

Yttrande från kommunstyrelsen önskas senast den 28 februari 2018.

För Älvsbyns kommuns revisorer

Bo Johansson
Ordförande

Älvsbyns kommun
Behörigheter och loggkontroll
Revisionsrapport
2017-11-13

Behörigheter och loggkontroll

Revisionsrapport

Älvsbyns kommun

KPMG AB

2017-11-13

Antal sidor 13

Innehållsförteckning

Älvsbyns kommun
Behörigheter och loggkontroll
Revisionsrapport
2017-11-13

1 Sammanfattning

Vi har av revisorerna i Älvsbyns kommun haft i uppdrag att granska hanteringen av behörigheter och åtkomstkontroll i kommunens datoriserade verksamhetsstöd Viva. Behörighetshantering och åtkomstkontroll bedömer vi är en viktig och central komponent i kommunens arbete med informationssäkerheten.

Vi har granskat styrdokument, intervjuat samt analyserat data för första halvåret 2017 från Viva (användarinformation och loggar), anställningsdata från PA-systemet samt utdrag ur kommunens katalogsystem (AD: et). Granskningen har varit inriktad mot att avgöra om tilldelningen av behörigheter följer de styrande dokumenten och via analysen göra bedömningar hur man lyckas efterleva dem i praktiken. Hur kontroll av loggad information utförs har här särskilt analyserats.

Från granskningen vill vi särskilt framhålla följande:

- Kontroll av den så kallade händelseloggen har utförts under januari 2017. Enligt uppgift lika mycket som ett test av instruktionerna som en regelbundet återkommande kontroll. Den instruktion som använts är en lovande början men den saknar delar som kan kompletteras genom att ansluta till de instruktioner som socialstyrelsen så sent som i mars 2017 uppdaterade.
- Det är otillfredsställande att det inte finns en formaliserad och dokumenterad hantering av behörigheter i Viva som även de efterlever socialstyrelsens föreskrifter.
- Både kommunens och granskad verksamhets styrande dokument vad gäller informationssäkerhet har stora brister och förehåller sig inte till varandra på ett sätt som underlättar förståelse och efterlevnad. Kommunen är i stort behov av att snarast upprätta ett nytt modern riskanalyserad ledningssystem för att åtgärda detta. Regelbundet måste det sedan ske en organiserad kontroll så att alla känner till styrningen, vad den innebär samt att de förstås och efterlevs.
- Våra jämförande analyser av data från olika källor redovisar risk för brister som bör undersökas likaväl som åtgärdas. Vi anser att analysresultaten och kommunens egen uppföljning av dessa ska ligga till grund för de metoder som behöver införas för loggkontrollen.

2 Inledning

2.1 Bakgrund

Vi har av revisorerna i Älvsbyns kommun haft som uppdrag att granska hanteringen av behörigheter och loggkontroll i kommunens datoriserade verksamhetsstöd.

Verksamheternas utveckling i en kommun har med åren blivit alltmer IT-beroende vilket innebär nya former av hot och risker. Behörighetsstyrning och loggkontroll blir då i sammanhanget en viktig och central komponent i kommunens arbete med informationssäkerheten. Detta arbete innebär bland annat upprättande och upprätthållande av

rättigheter för användare så att dessa enbart får och har åtkomst till den information som de behöver i sitt dagliga arbete.

2.2 Risk och väsentlighet

Revisionen utesluter inte att det finns risk för att behörighetstilldelning och kontroll av loggar inte följer det som anges i kommunens övergripande styrdokument för informationssäkerhet Riskbedömningen är densamma avseende de verksamhetsspecifika dokumenten.

2.3 Syfte och revisionsfråga

Syftet med granskningen har varit att besvara följande frågekomplex:

- Vilka styrdokument (policy med tillhörande riktlinjer, anvisningar och instruktioner) finns som kommunövergripande hanterar behörighetstilldelning? Finns det verksamhetsspecifika dokument som ställer ytterligare och mer detaljerade krav för det system granskningen avgränsats till?

- Finns det särskilda anvisningar och instruktioner för:

  - Personer som *inte* är tillsvidareanställda eller uppdragstagare?

  - Systemleverantörer, implementeringskonsulter, extern supportpersonal etc?

- Hur säkerställs kunskapen om och efterlevnaden av styrdokumenten i den verksamhet som granskningen avgränsats till?

- I vilken omfattning, när, hur och efter vilka anvisningar utförs så kallade loggkontroller?

- På vilken analysgrund, på vems verksamhetsansvar har det dokumenterats och tilldelats behörigheter för personal:

  - Som vid granskningstillfället använder det verksamhetsstöd som granskningen är avgränsad till?

  - Knuten till IT-avdelningen?

- I vilken omfattning och på vilket sätt berörs behörighetshantering och loggkontroller i internkontrollplanerna?

- Vad framkommer när vi jämför personförekomst i PA-systemet, med vad som framgår av den centrala katalogtjänsten (AD: et) och data från granskat verksamhetssystem?

2.4 Avgränsning

Granskningen är i princip avgränsad till resultatenheter omfattande den sociala verksamheten, förutom barn- och familjeenheten, och som hanteras med stöd av verksamhetssystemet Viva. Vivas uppbyggnad gör det inte lätt att identifiera vilka användare som omfattas av granskningen. Systemförvaltaren har varit till hjälp med att identifiera vilka dessa är och de har sedan fått bilda grund för våra analyser. I och med detta uppges det att vi granskat HSV, Hemtjänst och SÄBO.

2.5 Revisionskriterier

Kommunallagen 6 kap 7 § om nämndens ansvar.

Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården SOSFS 2008:14. Från 2017-03-01 HSLF-FS 2016:40 Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården.

De kriterier som legat till grund för bedömning och rekommendationer är hämtade från kommunallagens 6 kap kommunallagen samt reglemente för intern kontroll och tillämpningsanvisningar.

Tillämpbara interna regelverk, policys och beslut

2.6 Ansvarig nämnd

Granskningen avser kommunstyrelsen.

2.7 Projektorganisation/granskningsansvariga

Granskningen har utförts av Lars Anteskog. Kristian Damlin har medverkat i sin roll som kundansvarig.

2.8 Metod

Granskningen har genomförts genom dokumentstudier och intervjuer med berörda tjänstemän. Utöver detta har BKS[1]-data och loggdata från Viva inhämtats. Vi har även inhämtat ett anställningsregister från kommunens PA-system samt data från kommunens centrala katalogtjänst (AD[2]). Data har använts i jämförande analyser för redovisning i rapporten. Analysperiod har varit 2017 års sex första månader.

I en kombinerad gruppintervju, översiktlig faktagranskning och information deltog 2017-11-01: Tre av kommunens förtroendevalda revisorer, MAS, socialchef, systemadministratör för Viva och därtill en ersättare, en assistent till enhetschefer Omsorgen

[1] BKS en förkortning av behörighetskontrollsystem
[2] Active Directory, AD, är en katalogtjänst från Microsoft som innehåller information om olika resurser i en domän (nätverk) till exempel, datorer, skrivare och användare. Dessa klassificeras som objekt och kan hanteras samt skyddas i den egna domänen.

om funktionshindrade, enhetschef för bemanningsenheten, Enhetschef för HSV-teamet, chef samt två handläggare från lönekontoret, Informationssäkerhetsansvarig och en IT-tekniker. Rapporten är faktagranskad av systemförvaltaren och MAS.

3 Resultat av granskningen

3.1 Styrande dokument

3.1.1 Informationssäkerhetspolicy och riktlinje

Kommunen har en formellt beslutad policy avseende säkerhet. Av dokumentets innehåll framgår att även informationssäkerhet omfattas. Dokumentet är fastställt av kommunstyrelsen 2013-11-12, förlängd (49/16-002) 2016-03-27 med giltighetstid till 2019-12-31. Av dokumentet framgår att syftet är att *"skapa trygghet och säkerhet för kommunens medarbetare, medborgarna och de som vistas i kommunen"*. Vidare framgår att *"personsäkerheten alltid ska prioriteras högst"*. Under rubriken ansvar står att läsa: *"Kommunstyrelsen fastställer kommunens säkerhetspolicy och de ekonomiska ramarna för säkerhetsarbetet. Kommunstyrelsen har det övergripande ansvaret för ledning, styrning, genomförande och att fastställa säkerhetsarbetets övergripande riktlinjer. Respektive enhet och styrelse ansvarar för att säkerhetspolicyn med tillhörande riktlinjer efterlevs och utarbetar vid behov egna handlingsplaner för respektive verksamhet."*

Under rubriken tillämpning står att läsa: *"Tillämpningen av säkerhetspolicyn inom enheterna sker med stöd av konkreta riktlinjer. I dessa riktlinjer regleras de instruktioner och rutiner som ska tillämpas för säkerhetsarbetet inom kommunen."* Slutligen under rubriken uppföljning sägs bland annat att: *"Kommunstyrelsen ska aktivt följa upp effekterna av vidtagna åtgärder enligt de övergripande riktlinjerna och att dessa utvärderas."*

Det finns ett styrdokument i form av en riktlinje upprättad 2013-11-12 benämnd "Riktlinjer för säkerhetsarbetet". Förlängd av kommunstyrelsen samma datum som policydokumentet och med samma giltighetstid. Riktlinjen redovisar bland annat kommunövergripande styrning av informationssäkerheten. I ett särskilt avsnitt i det sjusidiga dokumentet ges en allmän förklaring av begreppet, inriktningen och ansvaret. Vidare hänvisas det till tre konkretiserande instruktioner. En för vardera förvaltning, drift- och kontinuitet samt användare. Inget av dessa har per granskningstillfället upprättats.

Under rubriken *"Roller och ansvar"* i riktlinjen framgår följande: *"Informationssystem med alla dess delar är en resurs i en verksamhet på samma sätt som personal, lokaler, kontorsmaterial mm. Informationssäkerhetssamordnaren är i dessa frågor direkt underställd kommunchef samt har det operativa ansvaret att samordna informationssäkerhetsarbetet. Kommunchef har det övergripande ansvaret för kommunens informationssäkerhet och utser systemägare för respektive informationssystem. Systemägare är den som har ansvaret för den verksamhet som aktuellt informationssystem stödjer. Systemansvarig utses av systemägare och ansvarar för den dagliga användningen av kommunens informationssystem."*

Vad gäller avgränsningen för denna granskning noterar vi att det inte finns några kommunövergripande anvisningar eller instruktioner om krav och villkor för vare sig behörighetshantering eller loggkontroll.

3.1.2 Styrande verksamhetsspecifika informationssäkerhetsdokument

3.1.2.1 Behörighetshantering

Vi har erhållit två ensidiga och odaterade dokument omfattande behörighetshantering. Enligt uppgift är det MAS som upprättat och beslutat om båda. "Dokumentation av behörighetstilldelning" beskriver i punktform hur beställning av behörighet i Viva ska behandlas av en systemadministratör. Beställningen kan enligt dokumentet nå administratören på olika sätt och det är hen som i systemet ska notera vem som beställt och när.

Dokumentet "Behörighetstilldelning" har underrubriken "Checklista anmälan om användare i Viva". Instruktionerna är här mer detaljerade än i föregående dokument och samstämmigt i vissa delar. Här framgår vilka funktioner som har rätt att beställa och förändra behörigheter. Det finns även instruktioner om hur en nödvändig så kallad Windowsinloggning görs för användare av Viva som anmäls utan att de finns registrerade i kommunens PA-system. De uppgifter som beställningen ska innehålla redovisas i punktform och dokumentet avslutas med texten: *"Det är också av vikt att nya användare informeras om sitt ansvar angående sekretess/inre sekretess/tystnadsplikt samt att de får utbildning i att använda systemet."*

Dokumenten saknar hänvisning till kommunövergripande dokument och refererar inte till de lagar och förordningar som gäller för den verksamhet som bedrivs.

3.1.2.2 Loggkontroll

Det finns ett elvasidigt styrande dokument för loggkontroll benämnt "Rutin för logg kontroll". Det är upprättat 2015-05-05 (reviderat 2015-09-28) av MAS och systemansvarig för Viva och giltigt till och med 2017-05-30. Dokumentet saknar hänvisning till kommunövergripande styrdokument.

Dokumentet inleds med ett utdrag ur SOSFS 2008:14 (Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården) och fortsätter med att ange *"Vårdgivare behöver ha en systematisk logguppföljning är dels för att kunna kontrollera om någon som inte är behörig har kommit åt patientuppgifter, dels att avhålla personal från att läsa patientuppgifter som de inte behöver i sitt arbete."* I avslutande stycke står *"Hösten 2015 körs en kontroll för att verksamheten ska testa hur det fungerar. Utifrån de erfarenheter som görs utarbetas en tydlig rutin för kontroll."*

Dokumentet innehåller anvisningar om hur urval sker, när kontroll ska utföras, av vem samt vad som ska kontrolleras och hur det ska dokumenteras. Till stöd finns två blanketter *"Uppföljning av loggkontroll i Viva"* och *"Checklista – Genomgång av loggkontroll – Viva"*. Vad som händer vid sekretessbrott och hur kontrollerna ska redovisas för socialtjänstens ledning samt till arbete och omsorgsutskottet avslutar dokumentet.

Kommentarer till avsnittet 3.1

Det framgår otillfredsställande lite om hur den kommunövergripande informationssäkerhet konkret och praktiskt ska hanteras och uppnås. Riktlinjen hanterar informationssäkerhet mer ur ett krishanteringsperspektiv än som en styrning av det operativa arbetet i vardagen. Vi rekommenderar kommunledningen att tydliggöra vad som gäller för säker informationshantering i vardagen. Baserat på en sådan riktlinje behöver sedan ansvariga på resultatsenhetsnivå upprätta anvisningar och instruktioner som följer riktlinjen och i detalj beskriver vem/vilka som dokumenterat gör hur, när och varför i förhållande till den verksamhet som bedrivs. Ett sätt att genomföra detta är att besluta om att införa ett ledningsstöd för informationssäkerhet (LIS) i kommunen. Myndigheten för samhällsskydd och beredskap (MSB) tillhandahåller vägledningar och annat stöd för ett införande i någon omfattning.

I avgränsningen för vår granskning hade vi förväntat oss att de verksamhetsspecifika anvisningarna anslutet till föreskriften HSLF-FS 2016:40 som 2017-03-01 ersatte SOSFS 2008:14 (Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården). Notera i sammanhanget att den nya föreskriften innehåller allmänna råd vilka ersätter innehållet i den tidigare publicerade handboken kopplad till SOSFS 2008:14. Instruktioner och anvisningar behöver utvecklas inte minst med hur hantering av behörigheter ska gå till. Dokument avhandlande loggkontroll är en lovande början på något som måste anpassas till ny föreskrift, göras giltigt och känt och sättas i kontinuerlig drift. Sist men inte minst måste dokumenten kompletteras med kontrollåtgärder som innebär att efterlevnaden säkerställs. Vi påminner i sammanhanget om att dessa åtgärder även är viktiga att årligen redovisa i patientsäkerhetsberättelsen.

När vi rekommenderar att HSLF-FS 2016:40 allmänna råd får bilda stöd och underlag för åtgärdsarbetet så är det även en påminnelse om nödvändigheten att anpassa sig till Dataskyddsförordningen (GDPR). Den börjar gälla som svensk lag från 2018-05-25. Kommande dataskyddslag (SOU 2017:39) och sektorspecifika författningar[3], vilka förändras i och med GDPR, kommer rimligtvis även de att påverka åtgärderna.

Avslutningsvis: Vi noterar särskilt att den grundläggande och viktiga åtgärden informationsklassning saknas i alla de styrdokument vi erhållit. Vi rekommenderar att SKL: s gratisverktyg KLASSA[4] används för detta ändamål. Om värdet av den information som ska hanteras inte är fastställd och känd finns risk för att åtgärderna inte blir ändamålsenliga och kostnadseffektiva.

[3] Vi exemplifierar sektorspecifika författningar med Lagen (2001:454) om behandling av personuppgifter inom socialtjänsten och Patientdatalagen (2008:355).
[4] Informationsklassning är en metod som hjälper verksamheten att välja rätt åtgärder som skyddar informationen. För att förenkla kommuners, landstings och regioners genomförande av informationsklassningen har Sveriges Kommuner och landsting (SKL) tagit fram verktyget KLASSA.

3.2 Hur säkerställs kunskapen om och efterlevnaden av styrdokumenten?

Vi får inga uppgifter som redovisar att någon form av riktad aktivitet genomförts under granskningsperioden för att säkerställa efterlevnaden av de verksamhetsspecifika styrdokumenten. Det uppges att det informeras om dokumenten vid introduktion av nyanställda och återkommande vid arbetsplatsträffar.

3.3 I vilken omfattning, när och hur utförs kontroll av händelseloggen?

Vi kan notera att det utförts loggkontroller under januari 2017. Vid dessa har använts de anvisningar och instruktioner som vi redovisar och kommenterar ovan. Kontrollerna är utförda, som vi uppfattar det, för att testa introducerad rutin. Kontrollerna efterlämnar en dokumentation av varierande kvalitet. Dokumentationen av kontrollerna sparas enligt uppgift endast pappersburet och vi kan notera att det görs på ett sätt och i ett utrymme som vid granskningstillfället uppfyller kriterierna för ett arkiv.

Kommentarer

Systematisk logguppföljning skall utföras för att den enskilde ska känna sig trygg med att ingen obehörig personal tar del av information som denne inte är behörig till. Vårdgivare av hälso- och sjukvård är skyldig att kontrollera att inga obehöriga tar del av patient-/brukaruppgifter och att personal inte tar del av information som de inte behöver ha tillgång till för att utföra sitt arbete. Den som bedriver verksamhet inom socialtjänst är skyldig att tillse att inga obehöriga tar del av information som de inte behöver ha tillgång till för att utföra sitt arbete.

Vi anser, och som redovisats ovan, att de instruktioner och metoder som beskrivs i de dokument vi erhållit inte är fullständiga och tydliga i en utsträckning som gör att kontrollarbetet är så ändamålsenligt och effektivt att det upptäcker och förhindrar att journaluppgifter eventuellt hanteras obehörigt. Nuvarande anvisningar och instruktioner behöver som tidigare sagts kompletteras och förtydligas.

Vi exemplifierar detta med att:

- Urvalmetodiken är sådan att analyserbara indikationer används så att även riskbeteenden ligger till grund för urvalet.
- Om stickprov och slump skall användas som urvalsmetod ska den vara statistiskt säkerställd och representativ för populationen av loggade personer. Hänsyn skall även tas till beslutade kontrollmål i internkontrollplaner.
- Beakta vad Datainspektionen skriver på sin hemsida. *”Bestäm med vilken omfattning (antal och tidsintervall) logguppföljningen ska ske. Eftersom det inte enbart är antalet loggposter vid logguppföljningen som avgör om kontrollen blir verkningsfull, finns det inget generellt svar på hur många loggposter som bör granskas vid varje tillfälle. Varje vårdgivare måste ta hänsyn till verksamhetens omfattning (antalet patienter och personal med behörighet) samt vilket urval och vilken systematik som används vid uppföljningen.”*

- Bedömning över tid av loggdata ska göras på samma sätt och på samma grunder oavsett vem som utför den. Här skall även ingå hur en kontroll kan överlämnas för överprövning[5].

- Hanteringen av dokumentationen från loggkontrollen skall vara enhetlig och hanteras på ett sätt så att informationen som uppdaterar personalakter beaktar vad som idag framgår av Personuppgiftslagen och i GDPR från 2018-05-25.

- Dokumentationen av loggkontroller är allmän handling, därför måste den sparas på ett sätt så att den hålls fullständig och oförändrad. Det ska även vara enkelt att identifiera och återfinna enskilda dokument. Detta innebär inte att förvaringen av dokumenten skall vara tillgänglig för alla. Verksamhetsansvariga måste över tid kunna säkerställa att endast de som ska hantera dokumenten har tillgång till dem.

- Av all dokumentation skall framgå vem/vilka som upprättat respektive beslutat, när det skett samt tidsomfattningen av loggdata.

I avsnittet 3.6 nedan redovisar vi ett antal iakttagelser av genomgången av sex månaders loggrader. Vi utesluter inte att flera av de iakttagelser som redovisas där kan bidra till att öka tillförlitlighet likaväl som kvalitet i arbetet med att kontrollera händelseloggen.

3.4 På vilken analysgrund, på vems verksamhetsansvar har det dokumenterats och tilldelats behörigheter för personal?

Det saknas ett enhetligt sätt att hantera behörigheter. Det finns heller inget stöd att söka i kommunövergripande styrdokument. Över tid har e-post och telefonsamtal varit de vanligaste metoder för chefer att anmäla användare av systemet. Inte sällan saknas det då uppgift om roll, organisatorisk avgränsning och varaktighet.

Vi har bett att få ta del av underlagen till ett antal användares behörigheter. Från vår granskning av dessa gör vi följande iakttagelser:

- Analysgrunden för behörighetshanteringen enligt SOSFS 2008:14 eller ersättande föreskrift (HSLF-FS 2016:40) finns inte.
- Det saknas underlag för användare som fick sina behörigheter för flera år sedan.
- Information om att anställda avslutar sin anställning når inte alltid systemförvaltaren så att behörigheterna kan avvecklas i rätt tid.
- Det finns anledning att stärka kontrollen av behörigheters giltighet när användaren byter befattning och/eller samtidigt utför arbete inom annan resultatenhet.
- Vi noterar ett användande av kortnamn vid registreringen som inte är fullständigt genomfört och vars syfte vi inte finner klarlagt.

[5] Den kontrollerade skall kunna få utförd kontroll gjord på nytt av person i linjen överordnad den som utförde den initiala kontrollen.

- Vi finner användare (har inte använt systemet under granskningsperioden) som inte går att härleda till en enskild identifierbar person.
- Vi finner användare av systemet som inte har en anställning enligt det underlag vi fått. Anledningen till detta bör undersökas för att säkerställa att registrerad anställning krävs för tillgång till systemet.
- Vi finner användare som avvecklats ur systemet och inte finns som anställd men ändå finns som aktiva i AD: et. Anledningen till detta bör undersökas för att säkerställa att registrerad anställning krävs för att få förekomma i AD: et.
- Vi finner exempel på användare med dubbla användaridentiteter. En är använd inom granskningsperioden den andra inte. Ändring av civilstånd eller namn av annan anledning verkar vara en vanlig orsak till detta. Metoder/Rutiner för att undvika att detta kan uppkomma bör rimligtvis ingå när styrdokumenten för behörighetshanteringen utvecklas.
- Vi finner nio (9) användare från systemleverantören registrerade som användare. Ingen av dessa finner vi loggen för granskningsperioden.

Kommentarer

Det är inte tillfredsställande att det inte finns en formaliserad och dokumenterad tilldelning av behörigheter. Det är därmed otillfredsställande att det inte på ett enkelt och effektivt sätt går att utgå från identiteter systemet och **alltid** hitta en handling som kan knytas till en beställning från en ansvarig chef. Oavsett om användaren är anställd av kommunen eller ej så behövs en dokumentation om vem och varför som behörigheter tilldelats.

Sekretess är en grundpelare i den verksamhet systemet stödjer. De förbindelser som upprättas med för externa parter ska rimligen kontrolleras med en periodicitet som överensstämmer med bedömd risk för att den kan missbrukas. Ansvariga ska inte tveka i att från externa användare begära dokumenterade bevis på att de efterlever de krav kommun ställer på en användare.

3.5 I vilken omfattning och på vilket sätt berörs behörighetshantering och loggkontroller i internkontrollplanerna?

Internkontrollplanen för 2017 innehåller inga kontrollmål vad gäller rubricerat. Informationssäkerhet ur ett kommunövergripande och/eller verksamhetsspecifikt perspektiv fanns inte heller med som någon identifierad riskidentitet.

Kommentarer

Informationssäkerhet bedöms generellt vara ett eftersatt område i kommunen. Ska ansvariga lyckas med att säkerställa effektivitet i allt från digitalisering av verksamheter till att ändamålsmässigt skydda alla involverades integritet krävs att alla förstår och lever efter samma enkelt tillgängliga och lättfattliga regelverk. Det torde ur det perspektivet vara svårt att kommande år *inte* ta med ett eller flera kontrollmål som för kommunledningen redovisar med vilken kvalitet på informationssäkerheten verksamheterna bedrivs.

3.6 Vad framkommer när vi jämför personförekomst i PA-systemet, med vad som framgår av den centrala katalogtjänsten (AD: et) och data från granskat verksamhetssystem?

Vi har jämfört data ifrån de källor som nämns i rubriken.

- 636 392 rader från Vivas händelselogg.
- Användardata (behörigheter och roller i Viva) för 813[6] identiteter.
- 1 342 personers anställningsdata[7] registrerade i kommunens PA-system
- 2 156 registrerade identiteter i AD: et

Beroende på system kan en identitet vara en person eller en funktion. En person kan beroende på system även vara knuten till fler än en identitet. Nedanstående exempel tillsammans med iakttagelser under avsnitt ovan anser vi kan användas som urvalsunderlag när kontroll och inventering skall utföras. Enstaka exempel motiverar kanske inte ett urval för kontroll. En kombination av exempel och iakttagelser som omfattar samma person gör hen rimligtvis betydligt mer aktuell för en kontroll. Från jämförelserna och andra analyser noterar vi följande:

1. Det finns användare i Viva som *inte* återfinns i det utdrag av anställningsregistret vi erhållit. Bland dessa finner vi personer som har en brukbar användaridentitet[8] vilken har eller inte har använts[9] enligt händelseloggen. Är utdraget korrekt utfört innebär det rimligen att ansvariga har gett sin tillåtelse att personer *utan* anställning eller uppdrag (uppdragstagare enligt anställningsregistret) i kommunen använder systemet. Om en utredning kan bekräfta iakttagelsen så går det uppenbarligen att kringgå för kommunen elementära och grundläggande informationssäkerhetskrav.
2. Några av personerna i punkt 1 ovan återfinns *inte* i erhållet utdrag av AD: et vilket rimligtvis kan innebära att dessa personer använt någon annan persons identitet och lösen för att ha haft tillgång till Viva. Om en utredning kan bekräfta iakttagelsen så behöver det säkerställas att så inte skett.
3. Vi finner exempel på att samma användare har lagts upp med fler än en identitet. Det finns inga motiv för att en och samma person skall kunna använda systemet iklädande sig fler än en identitet. Blotta förekomsten likaväl som möjlig-

[6] För att identifiera denna numerär har vi tagit hjälp av systemadministratören. Antalet identiteter blir detta eftersom det tagits hänsyn till att det finns personer som både helt och delvis är sysselsatta inom avgränsningen för granskningen.
[7] Enbart under granskningsperioden 2017-01-01 till 2017-06-30
[8] Med brukbar identitet i Viva menar vi en användaridentitet som *inte* har ett till och med datum angivet. Ett sådant datum förhindrar tillgång till systemet efter det angivna datumet.
[9] Med använts menar vi att händelseloggen visar att personen bakom identiteten utfört en eller flera åtgärder (som var och en genererar en loggrad) för en eller flera patienter/brukare.

heten visar på brister i kontrollen över att enbart av ansvariga godkända användare har tillträde till systemet. Vi rekommenderar att kontroller som upptäcker det som beskrivits här införs så snart tillfälle ges.

4. Vi identifierar flera personer i utdraget från PA-systemets anställningsregister som med ledning av hur de där kategoriseras (undersköterska, vårdare och vårdbiträden) borde ha en identitet registrerad i Viva men *inte* har det. Förhållandet innebär risk för att dessa personer inte tar del av information som de ska. Alternativt använder de någon annans identitet, uppdaterar inte systemet eller låter någon annan göra det. Därmed kan inte uteslutas att personer gör journalanteckningar sidoordnat som hanteras oskyddat under kortare eller längre tid. Om sidoordnade anteckningar inte tillförs systemet eller förs in felaktigt och/eller ofullständigt innebär det risk för att journaler blir missvisande. Missvisande eller saknade journalanteckningar innebär bristande patient-/brukarsäkerhet. I den omfattning detta sker upptäcks inte om kontroller enbart baseras på vad som framgår av händelseloggen. Vi rekommenderar att kontroller som upptäcker det som beskrivits här införs så snart tillfälle ges.
5. Med risk för samma effekter som beskrivs i punkt 4 finner vi en stor mängd registrerade användare med ett konto i AD: et som inte gör något avtryck i loggen. Flera av dem är registrerade som vikarier men inte alla. Med andra ord det finns användare som vare sig läser eller skriver journalanteckningar.
6. Vi noterar att utöver legitimerad personal så tillför undersköterskor, vårdare och vårdbiträden information till systemet. I förhållande till punkt 5 så noterar vi att alla i de kategorierna inte gör det.
7. Vår analysperiod innebär att händelseloggen omfattar ett halvår. Heltidsengagerade som har loggats (läst och/eller skrivit) på ett mycket stort respektive ett mycket litet antal datum inom den perioden torde vara kandidater för kontroll.
8. Vi finner sammanlagt 813 användare med behörighet under hela eller delar av granskningsperioden. I händelseloggen har under samma tid sammanlagt 380 av dessa genererat en eller flera loggrader. Det innebär att ca 53 % av alla registrerade användare inte använt sin behörighet i sådan omfattning att det gjort något avtryck i händelseloggen. Vilka är de anledningar som finns för att så många behöriga *inte* lämnar något spår av sin verksamhet i loggen? Ingenting läst, ingenting tillfört?
9. Vi noterar att det är 38 av 380 (10 %) användare som under halvåret sammanlagt genererat 38 % av alla loggrader. Om en användares befattning och ansvar *inte* motiverar att en så omfattande mängd loggrader genererats torde de vara aktuella för kontroll.
10. Vi noterar att det är 170 av 380 (45 %) användare som under halvåret sammanlagt genererat 10 % av alla loggrader. Nio (9) av de 170 har loggats för färre än tio (10) rader. Vilken typ av befattning och ansvar motiverar en så liten mängd av aktivitet i systemet?

11. 21 användare har mellan 200 och 404 loggrader registrerade på *ett enskilt datum*. 25 användare har i genomsnitt mellan 50 och 196 loggrader räknat på de dagar de har loggade rader registrerade. Dessa två "fåtal" användare i en stor mängd sticker ut i jämförelse med övriga. Detta är inte sällan ett motiv för en kontroll som klargör varför och avslöjar eventuellt felaktig användning av systemet.
12. Att det är legitimerad personal tillsammans med handläggare och chefer som skriver och läser journalanteckningar för flest antal patienter/brukare under ett år bedöms som rimligt. Enligt händelseloggen är de sammanlagt 46 stycken under ett halvår. De 10 av 46 som har hanterat flest journaler har gjort det för mellan 201 och 275 patienter/brukare. De 10 av 46 som hanterat minst antal journaler har gjort det för mellan 14 och 59 patienter/brukare. I genomsnitt hanterar de 46 dokumentation för 133 patienter/brukare. Detta är variationer som kanske inte alltid kan förklaras av sysselsättningsgrad, ansvar och hur många dagar man var i tjänst under halvåret. För urval till kontroller anser vi att det ska tas hänsyn till denna typ av indikation.
13. Bland de som inte tillhör gruppen legitimerad personal med flera hittar vi under året 331 användare i händelseloggen. De har hanterat dokumentation för mellan 1 och 970 patienter/brukare. I genomsnitt hanterar de journaler för 36 patienter/ brukare. De som i huvudsak läser/tittar i journalen gör de det av en legitim anledning? För urval till kontroller anser vi att det även ska tas hänsyn till denna typ av indikation.
14. Vi finner att det enligt händelseloggen för halvåret 2017 dokumenteras i någon omfattning för 1 377 patienter/brukare. För de tio (10) patienter/brukare vars dokumentation hanterats av flest användare är det mellan 86 och 102 stycken som läst och/ eller skrivit. Vi noterar i sammanhanget att det finns 672 (49 %) patienter/brukare vars dokumentation *endast hanterats av en (1) användare* under halvåret. Att undersöka rimligheten i de två redovisade förhållandena kan även det resultera i ett behov av kontroll.
15. Om man inte jobbar natt enligt PA-systemets anställningsuppgifter och ändå loggar merparten av raderna före 07:00 och efter 21:00 borde det vara en anledning till kontroll. Vi anger inget antal här då vi inte känner oss säkra på att PA-systemet är fullständigt uppdaterat med de som faktiskt någon gång har sin arbetstid förlagd till natt.

16. Även de som av någon anledning inte registreras som anställda i kommunens PA-system skall rimligen omfattas av loggkontroll.

KPMG, dag som ovan

Kristian Damlin

Kundansvarig

Lars Anteskog

Projektansvarig

Detta dokument med bilagor har upprättats enbart för i dokumentet angiven uppdragsgivare och är baserat på det särskilda uppdrag som är avtalat mellan KPMG AB och uppdragsgivaren. KPMG AB tar inte ansvar för om andra än uppdragsgivaren använder dokumentet och informationen i dokumentet. Informationen i dokumentet kan bara garanteras vara aktuell vid tidpunkten för publicerandet av detta dokument. Huruvida detta dokument ska anses vara allmän handling hos mottagaren regleras i offentlighets- och sekretesslagen samt i tryckfrihetsförordningen.