Kumla kommun

Behörigheter
Revisionsrapport

KPMG AB
1 december 2014
Antal sidor: 15

Innehåll

1. Sammanfattning med kommentarer

Vi har av revisorerna i Kumla kommun haft i uppdrag att granska hanteringen av behörigheter och åtkomstkontroll i kommunens datoriserade verksamhetsstöd. Behörighetsstyrning och åtkomstkontroll blir då i sammanhanget en viktig och central komponent i kommunens arbete med informationssäkerheten.

Vi har granskat styrdokument, intervjuat samt analyserat data från Procapita (kontoinformation och loggar för Vård och Omsorg), Agresso (ekonomisystemet), 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:

De övergripande styrande dokumenten för informationssäkerhet finns formellt beslutade från 2006. En av tre tillämpningsföreskrifter saknas och inga vid tiden aktuella systemsäkerhetsplaner (eller motsvarande) finns upprättade för de system som omfattas av denna granskning. Det är i dessa som det föreskrivs vad som allmänt och särskilt gäller avseende behörighetshantering. Dokumenten i sin helhet är ålderstigna och behöver uppdateras. De är inte kända i ändamålsenlig omfattning och inte efterlevda av ansvariga för de i granskningen ingående systemen. Vi rekommenderar att dokumenten uppdateras och att de särskilda informationssäkerhetskrav systemägarna identifierar i analyser särskilt redovisas och kommuniceras till användarna. (8.1)

Kontroll av loggar görs vid granskningstillfället *inte* i Agresso. I Procapita kontrolleras loggarna en gång i månaden. Enligt IT-säkerhetsinstruktion förvaltning punkt 4.1.3 skall systemägarens krav på säkerhets- och transaktionsloggar framgå av de systemsäkerhetsplaner som respektive systemägare upprättat. Några sådana planer eller motsvarande finns inte upprättade.

Det finns inga definierade mål för loggkontrollen, vare sig kvalitativa eller kvantitativa. Det är tveksamt om externa regler annat än patientdatalagen efterlevs. Av de dokument som beskriver och stödjer kontrollen av loggar i Procapita framgår inte motivet till hur urval skall göras. Uttryck som stickprov och slump används utan att det säkerställs att urvalen på något sätt är statistiskt säkerställda. Endast *ett* datum varje månad tas i dag ut för granskning. Vilka personer som skall granskas lämnas helt till den chef som genomför den. Det finns inga styrmedel så att alla granskas över en viss period och chefer granskas inte alls. Inga gemensamma och genomtänkta kriterier för bedömning finns och det säkerställs inte att alla får samma bedömning. Det finns inga instruktioner för hur en överprövning skall gå till. Vi ställer oss tveksamma till om ansvariga kan leva upp till socialstyrelsens krav att loggdata skall sparas i tio år. Nedan i rapporten lämnar vi allmänt hållna rekommendationer för ett åtgärdsarbete. Dessa kan med fördel även användas analysfasen inför nästkommande års internkontrollplan. Behörigheter i synnerhet och informationssäkerhet i allmänhet kan vi notera inte har varit en kontrollåtgärd de senaste åren.

Vid granskningstillfället kunde noteras att möjligheten att radera delar av journaler (”HSL-texter”) tillförts roller i en omfattning som vi bedömer *inte* överensstämmer med en säker hantering utförd av personer med kunskaper om, varför och när detta får ske. Varför möjligheten getts till de som felaktigt har den skall utredas. I övrigt skall användningen av den begränsas till ett fåtal. (8.3)

Det är bra att det finns en formaliserad och dokumenterad tilldelning av behörigheter. Det är otillfredsställande att det inte på ett enkelt och effektivt sätt går att utgå från identiteter i respektive system och alltid hitta en handling underskriven av berättigad som verifierar riktigheten i en enskild persons behörighet. Vi finner oidentifierade användare (funktionsidentitet) med systemrättigheter i Agresso. De måste tas bort om de inte kan knytas till enskild person.(8.4)

Våra jämförelse av personförekomst i PA-systemet, i den centrala katalogtjänsten och data från respektive verksamhetssystem visar på oacceptabla diskrepanser. Det skall inte vara möjligt att få behörighet i ett verksamhetssystem utan att vara känd och identifierad i katalogtjänsten (AD: et) och i PA-systemets anställningsdata.

Vi redovisar ett större antal rekommendationer baserat på vår analys av loggdata från Procapita. Vi anser att dessa både kan och ska användas som urvalsunderlag när loggkontroller utförs. Enstaka exempel motiverar kanske inte ett urval. En kombination av rekommendationer som omfattar samma person gör dock rimligtvis hen betydligt mer aktuell för en kontroll. (8.5)

Slutligen, det är av stor vikt att inse att ansvaret för att åtgärder utförs och att förändringar sker ytterst vilar på ett *aktivt* deltagande av respektive systemägare och systemansvarig. Vi påminner om att det i informationssäkerhetspolicyn anges att ”under kommunstyrelsen är det kommundirektören eller motsvarande som har det övergripande ansvaret för säkerheten.”

2. Bakgrund

Vi har av revisorerna i Kumla kommun haft i uppdrag att granska hanteringen av behörigheter och åtkomstkontroll 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 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.

3. Syfte

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?

- Finns det särskilda anvisningar och instruktioner för hur:

    - Personer som *inte* är tillsvidareanställda och uppdragstagare skall hanteras?

    - Systemleverantörer, implementeringskonsulter, extern supportpersonal etc. skall hanteras?

- Hur säkerställs kunskapen om och efterlevnaden av styrdokumenten i respektive verksamhet? I vilken omfattning utförs så kallade loggkontroller? I vilken omfattning och på vilket sätt berörs behörigheter och behörighetstilldelning i internkontrollplanerna?

- Roller och därtill knutna behörigheter. På vilken analysgrund, på vems verksamhetsansvar och för vilka system har det dokumenterats och tilldelats för personal:

    - Knuten till den centrala IT-verksamheten?

    - Som vid granskningstillfälle har någon roll i kommunens ekonomisystem?

    - Som vid granskningstillfälle har någon roll i kommunens systemstöd för äldreomsorgen?

- Vad framkommer när vi jämför personförekomst i PA-systemet, med vad som framgår av den centrala katalogtjänsten och data från respektive verksamhetssystem?

4. Avgränsning

Granskningen har varit avgränsad att omfatta två delar av kommunledningskontoret, kommunens centrala IT-verksamhet (IT-Service hädanefter ITS) under serviceavdelningen och ekonomiavdelningen. Vidare omfattas vård och omsorg (V&O) inom socialförvaltningen. Granskning har inte omfattat val av autentiseringsmetoder.

5. Revisionskriterier

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

Den interna kontrollen är viktig att utgå från då den är ett medel för ledningens kontroll av att verksamheten efterlever lagar, förordningar, policys och riktlinjer. Intern kontroll är en process vilken styrelsen, ledningen och annan personal skaffar sig rimlig säkerhet för att målen uppnås och som påverkas av hur man agerar i vad man säger och utför.

6. Ansvarig styrelse

Granskningen avser kommunstyrelsen samt socialnämnden.

7. Metod

Granskningen har genomförts genom dokumentstudier och intervjuer med berörda tjänstepersoner. Utöver detta har BKS[1]-data från verksamhetssystem inhämtats för jämförelse med person- och anställningsregister samt vad som framgår av kommunens centrala katalogtjänst (AD[2]: et). Analysperiod har varit 2014-01-01 till 2014-08-31.

Rapporten är faktagranskad av systemförvaltare för Procapita (V&O) och för Agresso (ekonomisystemet) samt IT-chef.

8. Granskningsnoteringar

Noteringarna redovisas avsnittsvis med kommentarer i samma ordning revisionsfrågorna anges under avsnittet syfte ovan.

[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.

8.1 Vilka styrdokument finns som kommunövergripande hanterar behörighetstilldelning[3]?

I mars 2006 antog kommunfullmäktige (KF) en informationssäkerhetspolicy. Vid samma tidpunkt antog samma instans därtill hörande tillämpningsföreskrifter. Det är två av tre IT-säkerhetsinstruktioner som finns omnämnda i policyn som är antagna, förvaltning och användare. Den senare reviderad 2008-11-05. Den ej antagna, eventuellt inte upprättade, instruktionen är den för drift.

Ett komplement till policyn benämnd systemsäkerhetsplan[4] finns inte upprättad för något av de verksamhetssystem som omfattas av denna granskning.

Vad gäller behörigheter hänvisar policyn till IT-instruktion förvaltning. Av denna framgår bland annat att det är kommunens IT-grupp som skall beställa ”enskilda användares behörigheter till IT-system”. Vidare skall de anmäla till ”systemförvaltare och/eller IT-enheten när personal slutar eller av annat skäl ska ha ändrade behörigheter”. Vidare i dokumentet finns instruktioner om administration och kontroll av behörigheter samt vad som gäller för loggning och spårbarhet.

De kommunövergripande styrdokumenten baserar sig på rekommendationer från en myndighet som inte längre existerar, Krisberedskapsmyndigheten (KBM[5]). Den myndighet som nu hanterar frågor om informationssäkerhet är Myndigheten för samhällsskydd och beredskap (MSB). De tillsammans med SKL[6] tillhandhåller stöd och råd i informationssäkerhetsfrågor på siten www.informationssäkerhet.se

Kommunens övergripande styrning av informationssäkerheten baserar sig därmed på äldre rekommendationer och på stöd samt hjälpmedel som inte längre underhålls. Kommunen har dessutom gjort uppdatering och revidering av dokumenten till en omständlig procedur då de är antagna av KF. I nedanstående avsnitt redovisar vi att kunskapen om och efterlevnaden av styrdokumenten vad gäller behörigheter inte är nämnvärt stor. Vi har anledning att förmoda att så är fallet även för övriga informationssäkerhetsområden.

Kommunstyrelsen (KS) har enligt informationssäkerhetspolicyn det ”övergripande ansvaret för säkerheten i kommunens IT-verksamhet.” Vidare framgår det att ”under kommunstyrelsen är det kommundirektören eller motsvarande som har det övergripande ansvaret för säkerheten.”

[3] Med behörighetstilldelning menas här även förändring och avveckling av behörigheter.

[4] Systemsäkerhetsplan (senare ersatt av systemsäkerhetsanalys): Dokument avseende ett enskilt informationssystem eller internt IT-nätverk som redovisar de samlade kraven på detta avseende tillgänglighet, riktighet och sekretess (konfidentialitet). Av säkerhetsplanen ska framgå vilka säkerhetsåtgärder som är vidtagna samt de eventuella ytterligare säkerhetsåtgärder som behöver vidtas för att kraven på informationssystemet ska uppfyllas. Säkerhetsplanen ska vara avstämd mot informationssäkerhetspolicyn.

[5] KBM inrättades 2002 efter beslut av riksdagen. Samtidigt upphörde Överstyrelsen för civil beredskap (ÖCB). Riksdagen beslutade 20 maj 2008 att en ny myndighet skulle inrättas 1 januari 2009 och att KBM, Statens räddningsverk och Styrelsen för psykologiskt försvar skulle läggas ned. Den nya myndigheten, Myndigheten för samhällsskydd och beredskap (MSB), har en samordnande roll i krisberedskapsarbetet.

[6] Sveriges Kommuner och Landsting

Kommentar

Ansvariga skall inte tveka att så fort tillfälle ges starta ett arbete med att revidera, uppdatera modernisera och komplettera de för dagen gällande dokumenten till en policy som möter moderna verksamheters krav. Alternativt så inför man i tillämplig omfattning ett ledningssystem för informationssäkerhet (LIS[7]). Görs ett sådant val är det fullt möjligt att återanvända befintlig styrdokumentation förutsatt att den är aktuell och korrekt. Vad vi kan bedöma är det inte endast informationssäkerheten fokuserad på behörigheter som behöver en uppdatering utan hela arbetet med att integrera, prioritera, informera och utbilda i informationssäkerhet i all den verksamhet kommunen bedriver.

Uppdaterat, alternativt nytt, policydokument antas i KF. Vad gäller tillämpningsföreskrifterna tas riktlinjerna (vad göra i förhållande till de mål som framgår av policydokumentet) med fördel i den sammanslutning av tjänstemän som bildar kommunens ledningsgrupp. Anvisningar och instruktioner (vem, när, var och hur) baserade på riktlinjen tas med fördel på lämpliga nivåer i linjeorganisationen. Allt för att uppnå integration och god anpassning till de informationsrisker som identifieras i respektive verksamhet.

Kommentarer explicit om behörigheter lämnar vi under avsnitten nedan.

8.2 Särskilda anvisningar för behörighetstilldelning

De verksamheter där systemägande och systemansvar ligger för de två system som granskningen omfattar har inte dokumenterat och kommunicerat några särskilda anvisningar eller instruktioner som kompletterar de övergripande dokumenten. Med andra ord det finns inga speciella regler och förhållningsorder dokumenterade när det gäller tilldelning av behörigheter för uppdragstagare, systemleverantörer, implementeringskonsulter, extern supportpersonal och andra som saknar en anställning i kommunen. Hur behörigheterna administreras redovisas i avsnitt nedan.

ITS har en dokumentation som ger anvisning om vad som gäller för uppläggning av manuella konton. De som inte har en anställning faller inom den kategorin. Av dokumentationen framgår att en beställning skall finnas från ”behörig chef/systemägare/ systemförvaltare.” Beställning sker via blankett som anges finnas på intranätet eller via ITS ärendehanteringssystem.

Kommentar

En enhetlig, väl känd och efterlevande de informationssäkerhetskrav som antagits, anser vi skall bilda underlag för en kommungemensam process för att hantera icke anställdas behov av behörigheter. Det är lämpligt att så sker i samband med den övergripande förändring av behörighetstilldelning som ITS planerar göra under första kvartalet 2015.

[7] LIS ett modernt metodstöd som riktar sig till de som ska bedriva informationssäkerhetsarbete t ex i en kommun. Stödet utgår fram för allt från standarderna i ISO 27000-serien. Läs mer på www.informationssäkerhet.se.

8.3 Kontroll av loggar och internkontroll

8.3.1 Agresso

Loggkontroller utförs *inte* i Agresso. Möjligheten att logga finns och vad vi förstår så finns det på dagordningen att starta loggning och kontroll av loggar. Det som skall beslutas är när och exakt hur det skall utföras och följas upp.

Kommentar

Enligt IT-säkerhetsinstruktion förvaltning punkt 4.1.3 skall systemägarens krav på säkerhets- och transaktionsloggar framgå av de systemsäkerhetsplaner som respektive systemägare upprättat. Någon sådan plan eller motsvarande finns inte upprättad. Det finns inga motiv för systemägaren och systemansvarig att inte skyndsamt upprätta detta dokument. Vi förutsätter att när detta görs så kompletteras planen eller motsvarande med ytterligare konkretiserade krav för att möta övriga krav som framgår av informationssäkerhetspolicyn med vidhängande tillämpningsföreskrifter. Det förefaller nödvändigt att systemägaren för detta ändamål även så fort tillfälle ges startar en verksamhets- likväl som riskanalys för att få underlag till planen. Vi utesluter inte att en GAP[8]-analys även skulle tillföra ytterligare kunskap för det arbetet.

8.3.2 Procapita

I Procapita utförs loggning kontinuerligt. Den verksamhet systemet stöder regleras vad gäller loggning av framför allt Patientdatalagen. Sekretess och tystnadsplikt gäller enligt Offentlighets- och Sekretesslagen. Överträdelser som kan leda till åtal regleras i Brottsbalken. ”*Den som olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift döms för dataintrång …*”

Enligt av Socialförvaltningen 2012-02-07 upprättad ”Checklista för chefer vid kontroll av loggar i Procapita VoO och IFO” kommer logglistor en gång i månaden från systemförvaltaren. Enligt systemförvaltarens aktivitetsnoteringar framgår under rubriken månatligen ”Procapita loggning, kör enbart för VoO”. Logglistor kan även tas fram av personer som innehar systemadministratörsrollen.

Det finns inga gemensamma dokumenterade anvisningar om vad som skall ingå i en genomgång av loggdata. Enligt uppgift undersöks om och var vederbörande arbetat de aktuella dagarna genomgången omfattar. I ett PowerPoint-dokument från 2009-05-20 benämnt ”Manual för loggning i Procapita” visas på en bild att det används ett sökverktyg i programmet. Det är endast personal med rollen systemansvarig som kan utföra sökningen. Vi är av den uppfattningen att det är rollen systemadministratör som avses här. Vid granskningstillfället finns det sammanlagt sju personer som innehar denna roll. Av bilden drar vi slutsatsen att loggdata från *endast* ett datum varje månad tas ut för granskning. Detta bekräftas även av svaret på en direkt fråga till MAS och MAR[9]. I erhållen dokumentation framgår inte varför och hur endast ett datum skall väljas. Övervägande delen av manualen redovisar hur loggdata hanteras i kalkylmatrisprogrammet Excel. Av

[8] GAP-analysen identifierar skillnaden mellan nuvarande läge och ”best practise”. Detta för att ge insikt om inom vilka områden som det finns rum för förbättring.

[9] MAS = Medicinskt ansvarig sjuksköterska. MAR = Medicinskt ansvarig för rehabilitering.

dokumentets tre sista sidor framgår att ”*Gör nu ett slumpvist urval av användare och markera dessa. Det bör vara minst 10 användare som ska granskas. Hela listan ska omfattas. Markera de utvalda genom att färgmarkera texten.*” På inget sätt redovisas hur slumpen skall avgöra val av personer att granska. Det framgår inte om urvalet skall vara representativt för någon population. Övriga instruktioner berättar om hur man identifierar personernas befattning och organisatoriska tillhörighet. Vidare beskrivs hur loggdata skall distribueras och sparas. Vi saknar här svar på vår fråga: ”På vilket sätt har man kommit fram till att vald metod för urval är representativ för målsättningen och kravet på kontroll?” Vad vi förstår så är arbetssättet och manualen initierad och beskriven av en tidigare systemförvaltare.

På frågan om hur lång omloppstiden är mellan varje loggkontroll av enskild medarbetare får vi svaret att det kan bli så att vissa medarbetares loggade aktiviteter aldrig blir kontrollerade. Vi får svaret ”utförs inte” på frågan om den metod som används regelbundet kvalitetskontrolleras mot externa och/eller interna regler. Det är enhetschefer som utför kontroll av loggdata. Enligt uppgift görs ingen motsvarande kontroll av deras aktiviteter i systemet.

Av ”Checklista för chefer vid kontroll av loggar i Procapita VoO och IFO” kan läsas att genomgången med berörd personal skall innefatta eventuella oklarheter eller osäkerheter som framgår av loggdata. Definition och stöd vid tolkning av dessa uttryck finns inte. Enligt uppgift finns ingen vägledning för genomgången och det är ”oklart” om alla enhetschefer använder samma definitioner och bedömningsgrunder.

Resultatet av kontroll av loggdata meddelas den som kontrollerats på särskild blankett ”Loggning Procapita”. Kopia skickas till systemförvaltaren. Resulterar kontrollen i åtgärder så uppges detta leda till att vederbörandes personalakt uppdateras med information om vilka åtgärder som vidtagits. Av ”Checklista för chefer vid kontroll av loggar i Procapita VoO och IFO” framgår att ”Vid misstanke om obehörigt informationsinhämtande eller annan oegentlighet i systemet” skall enhetschef kontakta personalsekreterare för eventuella disciplinära åtgärder. Beslut om polisanmälan skall göras av förvaltningschef. Systemförvaltaren skall även här få återkoppling när ärendet är avslutat. Syftet med det framgår inte och innevarande systemförvaltare har ingen kunskap om vad som skall göras med den specifika informationen. Vi kan inte se att det dokumenteras att och hur man kan få en loggkontroll överprövad.

Loggkontrollerna (i princip Exceldokumenten) sparas enligt uppgift i en särskild mapp på en server. Det krävs särskilda behörigheter för tillgång till mappen. Personal inom socialförvaltningen har inte teknisk möjlighet att se vilka som har behörighet till mappen. Med stöd av ITS identifierar vi nio personer. Sju av dessa finns med som loggansvariga för V&O under 2014. Av de sju är en den före detta systemförvaltaren. Övriga två identifierar vi via PA-systemet som personer med administrativa uppgifter inom socialförvaltningen. I mappen finns bland annat årsmappar från 2010 till 2014. Av antalet Exceldokument i respektive årsmapp ställer vi oss frågande till om alla kontroller utförts varje månad respektive år. Alternativt lagras kontrollresultatet för fler än en månad i samma dokument eller så är resultat inte lagrat eller lagrat där det inte ska lagras.

Vi kan med stöd av systemets sökfunktion notera att den fullständiga loggen för de senaste tio åren eller från när systemet driftsatts inte är tillgänglig. Loggdata verkar endast finnas från 2012-01-01 och framåt. Jämför det med att loggkontroller finns från 2010. ITS meddelar att de inte separat lagrat någon loggdata från Procapita. Vad vi förstår har de heller inte erhållit något uppdrag att göra detta.

Vid granskningstillfället kunde noteras att möjlighet att radera delar av journaler (”HSL-texter”) tillförts roller i en omfattning som vi bedömer inte överensstämmer med en säker hantering utförd av personer med kunskaper om, varför och när detta får ske.

Kommentar

I princip gäller kommentarerna för Agresso även för Procapita. I övrigt vill vi kommentera våra iakttagelser enligt följande:

Systematisk logguppföljning görs 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 patientuppgifter 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 att de instruktioner och metoder som används för loggkontroll inom vård och omsorg inte är vare sig ändamålsenliga eller effektiva för att upptäcka och förhindra att journaluppgifter eventuellt hanteras av obehöriga. Patientdatalagen efterlevs men inte fullt ut övriga externa regler och intern policy. Det saknas tydliga och dokumenterade instruktioner som anger varför och hur loggkontroll skall utföras.

Vi exemplifierar detta med att:

- Alla som använder systemet över en given tidsperiod skall omfattas av kontroll.
- Urvalmetodiken är sådan att analyserbara indikationer används så att även riskbeteenden ligger till grund för urvalet.
- Om stickprov och slump skall användas som urvalsmetod skall den vara statistiskt säkerställda och representativ för populationen av loggade personer. Hänsyn skall även tas till beslutade kontrollmål.
- 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.
- Alla användare skall omfattas av loggkontroll, även chefer.
- Hanteringen av dokumentationen från loggkontrollen skall vara enhetlig och hanteras på ett sätt så att informationen som uppdaterar personalakter beaktar vad som framgår av Personuppgiftslagen.

- Dokumentationen av loggkontroller är allmän handling, därför måste den sparas på ett sätt så att den är 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 ”SOSFS[10] 2008:14. Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården” framgår att loggar skall sparas i 10 år. Det måste finnas processer/rutiner som säkerställer att så sker och att informationen under denna tid inte kan förändras eller förstöras.

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

Vi anser att det snarast möjligt sker en översyn av rollerna i Procapita så att inte journaldata raderas och/eller förvanskas så journaler får ett ofullständigt och därmed missvisande innehåll.

I avsnittet nedan redovisar vi ett antal iakttagelser av genomgången av 844 439 loggrader omfattande perioden januari till augusti 2014.

8.3.3 ITS

Enligt uppgift så utför ITS inga systematiska loggkontroller av något system. Anledningen till det uppges vara att några sådana uppdrag inte erhållits från någon systemägare.

8.3.4 Internkontroll

Vad vi förstår av intervjusvaren så har informationssäkerhet inte i någon omfattning identifierats som ett kontrollmål i de senaste årens internkontrollplaner. Följaktligen har inte behörighetshanteringen varit föremål för någon internkontrollåtgärd.

Kommentar

En korrekt hantering och användning av behörigheter är en central komponent för att ge kommunens information rätt skydd:

- Tillgänglighet: Att information är tillgänglig i förväntad utsträckning och inom önskad tid

- Riktighet: Att den skyddas mot oönskad och obehörig förändring eller förstörelse

- Konfidentialitet: Att den inte i strid med lagkrav eller lokala överenskommelser/riktlinjer tillgängliggörs eller delges obehörig

- Spårbarhet: Att i efterhand entydigt kunna härleda specifika aktiviteter eller händelser till ett identifierat objekt eller användare (vem, vad, när)

[10] Socialstyrelsens författningssamling

Vi anser att, inte minst med underlag av våra iakttagelser i denna granskning, behörighet kvalificerar sig som en egen kontrollåtgärd med vidhängande kontrollmoment i kommande internkontrollplaner.

8.4 På vems verksamhetsansvar tilldelas behörigheter

8.4.1 Agresso och Procapita

För att få behörighet till Agresso likväl som Procapita krävs en administrativ åtgärd som dokumenteras på en blankett.

För behörigheter till Agresso används blanketten ”Ny användare i Agresso”. Här skall anges namn, användar-ID (finns upplagd i kommunens katalogtjänst), förvaltning och e-postadress. Vidare skall anges om man skall granskningsattestera och/eller beslutsattestera för det senare krävs att ett delegationsbeslut bifogas. Kostnadsställe för beslutsattest skall även det anges samt vilken ersättare inom kostnadsstället man har för sin beslutsattest. Chef skall anges, under vilken tid behörigheten skall gälla och vem som är uppgiftslämnare. Underskrifter behövs inte på Agresso-blanketten.

Enligt uppgift så har en stor mängd användare manuellt matats in i Agresso med underlag av uppgifter från det avvecklade ekonomisystemet Aditro. Innan inmatning gjordes avstämning mot förteckning över godkända attestanter. Här har man med andra ord förlitat sig på att det finns äldre korrekt utförda beställningar. I Agresso tillåter man även att så kallade funktionsbehörigheter (kan användas av fler än en användare) läggs upp. När vi kombinerar dessa med de roller som definierats i systemet finner vi två stycken med mycket omfattande behörigheter. Rollerna beskrivs som ”Super roll för att bygga upp ekonomisystemet endast Agresso konsulter” och ”Systemansvarig”. Systemansvarig är även den roll som getts två personer anställda på Askersunds kommun. Vi förstår att motsvarande upplägg finns med anställda i Kumla som har systembehörigheter i Askersunds kommuns Agresso-system.

Vad gäller Procapita så skall närmaste chef ange namn, befattning, arbetsenhet, telefon, datum för anmälan samt det användar-ID man har tilldelats för att få tillgång till nät samt allmänna tjänster och program. Det skall kompletteras med typ av behörighet, för vilken organisatorisk enhet den skall gälla samt under vilken tid. Från 2014-04-01 är det obligatoriskt att ange användaridentiteten vilken erhålls från ITS.

Identiteter kan inte snabbt och enkelt verifieras mot beställd tillgång till systemet. Beställningarna är inte systematiskt arkiverade. För Procapita införs därför i omgångar en elektronisk variant där e-posten med kopior till berörda får ersätta den pappersburna metoden. Underskrifter från både användare och chef krävs för Procapita om blanketten används.

Kommentar

Det är bra att det finns en formaliserad och dokumenterad tilldelning av behörigheter. Det är otillfredsställande att det inte på ett enkelt och effektivt sätt går utgå från identiteter i respektive system och *alltid* hitta en handling underskriven av berättigad som verifierar riktigheten i en enskild persons behörighet. Blanketterna för detta oavsett om de är pappersburna eller ej måste till skillnad

från idag även omfatta förändring av förutsättning för behörighetstilldelningen samt avveckling av desamma. Under avsnitt 7.5 nedan redogörs för exempel på detta.

Även funktionsbehörigheter, behörigheter till konsulter, uppdragstagare och anställda i annan kommun måste omfattas av en formaliserad hantering där det finns en ansvarig som beställer. De två funktionsbehörigheter med omfattande tillgång till systemet skall tas bort om de inte kan knytas till enskilda individer. Kommunexterna behörigheter bör omgärdas av detaljerade föreskrifter om vad de får utföra inkluderande att de inte får överlåtas till annan utan godkännande från ansvarig beställare. Behörigheterna skall även vara tidsbegränsade. Under längre bortovaro skall de avaktiveras. Det faktum att ingen och bedömt bristfällig loggning sker innebär att det inte kan utföras kontroller i en omfattning som skulle kunna kompensera en bristfällig eller utebliven beställning.

8.4.2 ITS

Tilldelningen av behörigheter följer i princip samma ordning som redovisats för manuella konton under 7.2 ovan. I dokumentationen nämns kortfattat om hur behörigheter till databasåtkomst (åtkomst till data utan att använda det ordinarie användargränssnittet) skall hanteras i förhållande till andra typer av behörigheter. Ingenting sägs om vilka förutsättningar som gäller i förhållande till respektive systemägares behov och formellt uttryckta tillåtelse.

Kommentar

Inte minst för system som Agresso och Procapita är det utomordentligt viktigt att det finns instruktioner som innebär stor restriktivitet i tilldelning av databasåtkomst. Det skall klart och tydligt framgå vem som över tid har tillgång till vilka databaser och på vems skriftliga beställning.

8.5 Jämförelse av personförekomst i PA-systemet, i den centrala katalogtjänsten och data från respektive verksamhetssystem.

Vi har jämfört data ifrån de källor som nämns i rubriken. Nedan redovisar vi de iakttagelser inklusive kommentarer vi gjort baserat på:

- 844 439 loggrader från Procapita
- Kontodata för 659 användare av Procapita
- 471 registrerade identiteter i Agresso
- 3 367 personers anställningsdata i PersonecP (kommunens PA-system)
- 2 941 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. Iakttagelser och kommentarer redovisas under respektive punkt i avsnitten nedan.

8.5.1 Agresso

Från jämförelser med bäring på användare av Agresso noterar vi följande:

- Agressokonsulter förekommer inte i AD: et vilket innebär att dessa personer använder någon annan persons identitet. Mer troligt har de en gemensam identitet i AD: et eller kan ansluta sig till systemet utan att vara upplagd i AD: et. Detsamma gäller de två anställda med systembehörigheter från Askersunds kommun. Om man frångår det sätt som informationssäkerhetspolicyn anger ska det beskrivas och godkännas av ansvarig beställare.

- Det finns ingen rutinmässig och dokumenterad hantering av förändring och avveckling av identiteter. Detta får till följd att risk finns för att personer uppbär behörigheter efter det att anställning upphör eller att ny arbetsuppgift/anställning inom kommunen (annan förvaltning) inte motiverar tillgång till systemet.

8.5.2 Procapita

Från jämförelser med bäring på användare av Procapita noterar vi följande:

- Det finns flera användare i systemet som inte återfinns i AD: et vilket innebär att dessa personer använder någon annan persons identitet och lösen för att över huvud taget få tillgång till Procapita.

- Identiteter kan inte snabbt och enkelt verifieras mot beställd tillgång till systemet. Blanketterna är inte på något sätt systematiskt ordnade förrän 2014-04-01. Detta faktum gör det svårt och tidsödande att kvalitetssäkra att endast behöriga har tillgång till systemet.

- Det finns ingen rutinmässig och dokumenterad hantering av förändring och avveckling av identiteter. Detta får till följd att risk finns för att personer uppbär behörigheter efter det att anställning upphör eller att ny arbetsuppgift/anställning inom kommunen (annan förvaltning) inte motiverar tillgång till systemet.

- Vi identifierar personer i PA-systemet som med ledning av kategori (sjuksköterska, undersköterska, vårdare etc.) borde ha en identitet registrerad i Procapita 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 av en loggkontroll på det sätt den idag utförs. Vi rekommenderar att kontroller som upptäcker det beskrivna förhållandet införs som ett komplement till loggkontrollerna.

- Vi identifierar inhyrd personal som inte återfinns vare sig i AD eller som uppdragstagare i PA-systemet. Följaktligen så går det att runda de informationssäkerhetskrav man har att leva efter i kommunen. Risker och rekommenderade åtgärder är desamma som i punkten ovan.

- Vi finner identiteter i loggdata som inte verkar ha något konto i systemet (vara registrerad som användare). Undersökning av orsaken visar att kontoinformation kan registreras alternativt ändras så den är/blir inkomplett vad gäller från och till datum för behörighetens giltighet.

Ovanstående punkter anser vi kan användas som urvalsunderlag när loggkontroller skall utföras. När vi analyserar loggdata gör vi ytterligare iakttagelser som kan användas som urvalsunderlag. Nedan redovisas några exempel. Enstaka exempel motiverar kanske inte ett urval. En kombination av exempel som omfattar samma person gör hen rimligtvis betydligt mer aktuell för en kontroll.

- Vår analysperiod innebär att loggen omfattar 243 kalenderdagar. Heltidsengagerade som har loggats på ett mycket stort respektive ett mycket litet antal datum inom den perioden torde vara kandidater för kontroll.

- Vi noterar att det är 28 personer som sammanlagt genererat 33 % av alla loggrader under åtta månader. Om personens befattning inte motiverar att en stor mängd loggrader torde de vara aktuella för kontroll.

- 34 personer har 300 eller fler loggrader registrerade på ett enskilt datum. Dubbelt så många har i genomsnitt 50 loggrader eller fler räknat på de dagar de har loggade rader. Ett fåtal personer i en stor mängd sticker ut i jämförelse med varandra. Detta är inte sällan ett motiv för en kontroll som klargör varför och avslöjar eventuellt felaktig användning av systemet.

- 35 personer har tre fjärdedelar av alla sina loggrader på två enskilda datum. Ett sådant begränsat intresse kan ha flera olika förklaringar. Dessa framkommer vid en loggkontroll.

- Bedömt okontrollerat tilldelade möjligheter att ta bort journaldata redovisade i avsnitt ovan motiverar att kontrollera de med en befattning som rimligtvis inte har anledning att ta bort journaldata men enligt loggen gjort så.

- Finns det personer bland de som endast läst under åtta månader som rimligen även ska ha sparat data. Med andra ord personer som enligt befattningen ska göra journalanteckningar.

- Om man inte jobbar natt enligt PA-systemets anställningsuppgifter och ändå loggar merparten av raderna före 06:00 och efter 18:00 borde det vara en anledning till kontroll. Detta gäller rimligen även de som har loggrader för 16 eller fler timmar på ett och samma dygn.

- Personer som inte har någon benämning/kategori enligt PA-systemet och som kan knytas till Vård & Omsorg är rimligtvis intressanta kontrollobjekt. Personer som enligt AD: et tillhör en annan förvaltning/verksamhet än socialförvaltningen torde även de vara av intresse.

- Även de som registreras som uppdragstagare i PA-systemet skall rimligen omfattas av loggkontroll.

KPMG, dag som ovan

Lars Anteskog
Projektansvarig