Örebro kommun

Behörigheter och loggkontroll
Revisionsrapport

Lars Anteskog, KPMG
Offentlig sektor
KPMG AB
24 november 2015
Antal sidor: 15

Innehåll

1. Sammanfattning och kommentarer

Vi har av revisorerna i Örebro kommun haft i uppdrag att granska hanteringen av behörigheter och åtkomstkontroll i kommunens datoriserade verksamhetsstöd Treserva. Behörighetsstyrning och åtkomstkontroll är en viktig och central komponent i kommunens arbete med informationssäkerheten.

Vi har granskat styrdokument, intervjuat samt analyserat data från Treserva (kontoinformation och patientjournalens logg för verksamhetsområde; Hälso-, sjukvård och social omsorg), 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:

Kommunen har en modern och tydlig övergripande informationssäkerhetspolicy som till sin utformning även innehåller tydliga och praktiska riktlinjer. Socialtjänsten å sin sida har tydliga och riktiga ambitioner med sina dokument. De är dock i sin helhet inte enligt riktlinjerna och därtill inte fullständiga och ändamålsenliga som styrande dokument för det granskningen omfattat.

Kommentar
Vi bedömer att socialtjänsten har ett digert arbete framför sig för att nå efterlevnad av de kommungemensamma dokumenten avseende informationssäkerhet. Avgränsat till denna granskning skall arbetet enligt vårt synsätt övergripande inrikta sig mot att upprätta en systemsäkerhetsinstruktion för Treserva. Särskilt skall arbetet inrikta sig på att nå förståelse för och efterlevnad av Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården SOSFS 2008:14. (8.1)

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 en dokumenterad identitet och *alltid* hitta en handling underskriven av berättigad som verifierar riktigheten i en enskild persons behörighet.

Kommentar
I arbetet med att efterleva kommungemensam och verksamhetsspecifik tillämpning av informationssäkerhet anser vi att det finns anledning att prioritera utvecklingen av rutinerna för behörighetstilldelning. Rimligtvis finns det över ettusen användare som behöver avaktiveras samt ett stort och okänt antal som behöver verifieras som legitima användare med rätt behörigheter. Detta inventerings- och åtgärdsarbete förutsätter vi även leder fram till att framtida förändringar och avveckling av behörigheter kommer att ingå i den formaliserade behörighetshanteringen. (8.6)

Att vid loggkontroll endast använda ett urval styrt av slumpen anser vi inte ger ansvariga möjlighet att säkerställa att patientjournalen över tid hanteras på ett korrekt sätt.

Kommentar
Vi anser att förvaltningen skall genomföra en risk och väsentlighetsanalys som omfattar hela processen för loggkontroll oavsett om det är kommunen eller en extern aktör som är utförare. Resultatet av den utmynnar rimligtvis i en dokumentation som vägleder de ansvariga och informerar användarna. Erfarenheter från åtgärderna av de brister vi iakttagit i våra jämförande analyser förutsätter vi återanvänds som instruktioner i den nya dokumentationen (8.5) (8.7)

2. Bakgrund

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

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.

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 verksamhets-specifika dokument som ställer ytterligare och mer detaljerade krav för det system gran-skningen 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?

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

- 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-kontoret?

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

4. Avgränsning

Granskningen är avgränsad att omfatta det verksamhetssystem som används inom Vård- och omsorgsnämnd Öster och Vård- och omsorgsnämnd Västers verksamhetsområden. Granskning omfattar inte val av autentiseringsmetoder.

5. Revisionskriterier

De kriterier som legat till grund för bedömning och rekommendationer är hämtade från kommunallagens 6 kap kommunallagen 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 och riktlinjer. Intern kontroll är en process genom 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.

Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården SOSFS 2008:14.

6. Ansvarig styrelse

Granskningen avser Vård- och omsorgsnämnd Öster och Vård- och omsorgsnämnd Väster, Programnämnd Social välfärd men i och med sin uppsynsplikt även kommunstyrelsen.

7. Metod

Granskningen har genomförts genom dokumentstudier och intervjuer med berörda tjänstemän. Utöver detta har BKS[1]-data och patientjournalens logg från Treserva 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 januari till maj 2015.

En gruppintervju genomfördes 2015-10-06. Syftet med sammankomsten var även att delge alla de vars funktioner och ansvar som i någon del omfattas av granskningen en möjligt att ta del av vad som framkommit. Intervjun fick därmed även ett inslag av en bred och allmän sakgranskning. Intervjun resulterade i ett behov av att komplettera och förtydliga några av tidigare erhållna uppgifter. Efter dessa justeringar är rapporten sakgranskad av systemadministratörer för Treserva och förvaltningsledare för Vård- och Omsorg.

[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.

Nedanstående funktioner, samt en representant från revisionen, deltog 2015-10-06:

- Systemförvaltare PersonecP (kommunens PA-system).
- Systemadministratörer Treserva.
- Förvaltningsledare Vård- och Omsorg.
- Förvaltningsledare IT.
- Gruppchef IT Systemstöd.
- Enhetschef IT Systemstöd/IT Utveckling.
- MAS/MAR Vård- och Omsorg.
- Socialt ansvarig Samordnare Vård- och Omsorg.
- MAS/ Socialt ansvarig Samordnare, Förvaltningen för funktionshinder.
- Programchef Vård och Omsorg (Systemägare av Treserva).
- Planerare ansvarig för externa utförare.
- Gruppchef IT Kundtjänst.
- Databastekniker Treserva Drift.
- Kommunens informationssäkerhetsansvarig.
- Verksamhetschefer Förvaltningen för Funktionshinder.

8. Granskningsnoteringar

8.1 Styrande dokument

Kommunen som helhet har en formellt antagen informationssäkerhetspolicy och därtill ett dokument redovisande kommunövergripande riktlinjer. Socialtjänsten har inte formaliserat sig och sin verksamhet med motsvarande dokument. Den systemsäkerhetsinstruktion som enligt riktlinjerna formellt skall vara antagen för det system som nu granskas finns inte. I avsnitten nedan redovisas iakttagelser från de kommunövergripande dokumenten samt från de dokument som erhållits för att de i någon omfattning uppges styra hur informationssäkerheten hanteras och säkerställs på socialförvaltningen.

8.1.1 Kommunens informationssäkerhetspolicy

Rubricerade dokument inleds som följer. ”Informationssäkerhet är den del i kommunens lednings- och kvalitetsprocess som avser hantering av verksamhetens information. Policyn beskriver kommunens mål och inriktning för informationssäkerhetsarbetet. Informationssäkerhetspolicyn och riktlinjer styr kommunens informationssäkerhetsarbete.” Vidare framgår att information är en av kommunens viktigaste tillgångar. Utgångspunkt i arbetet med informationssäkerhet tas i lagar, förordningar, föreskrifter, avtal och kommunens egna krav.

Av policyn framgår att: ”Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat”. Informationssäkerheten omfattar kommunens informationstillgångar utan undantag.

Vad gäller roller och ansvar så har kommunstyrelsen det yttersta ansvaret. Av policyn framgår att: ”Kommundirektören har ansvar för att informationssäkerhetsarbetet bedrivs i linje med den av kommunstyrelsen fastställda informationssäkerhetspolicyn. Kommundirektören fastställer, på delegation av kommunstyrelsen, kommunövergripande riktlinjer och instruktioner. Kommundirektören ansvarar för att systemägare utses för respektive informationssystem. Systemägaren är ansvarig för säkerheten i sitt system. IT chefen ansvarar för att tillse att driftsäkerheten överensstämmer med systemägarens anvisningar. Informationssäkerhetsansvarige har det operativa ansvaret för samordning av informationssäkerhetsarbetet.”

8.1.2 Kommunens riktlinjer för informationssäkerhet

Rubricerade dokument är som informationssäkerhetspolicyn antagen av kommunstyrelsen och daterad 2013-10-30. Med bäring på syftet för denna granskning redovisas nedan några av de riktlinjer systemägaren har att efterleva.

I avsnitt 2.4.1 framgår att: ”Systemägaren är ansvarig för säkerheten för sitt system och ska därvid se till att systemet följer gällande informationssäkerhetspolicy, regler och riktlinjer. Vidare ska systemägaren säkerställa att nödvändiga säkerhetsanalyser och utbildning genomförs för att en godtagbar säkerhetsnivå ska kunna upprätthållas. En del av detta ansvar är att definiera systemets informationssäkerhetskrav.”

Riktlinjerna innehåller ett avsnitt 3 ”Riktlinjer för informationsklassning”. Här anges att: ”All information är känslig och kritisk i varierande grad. För att kunna bedöma om en viss informationsmängd har behov av ett utökat skydd eller särbehandling måste informationen bedömas ur känslighetssynpunkt. Denna process kallas informationsklassning.

Riktlinjerna innehåller ett avsnitt 5.6 ”Upphörande eller ändring av anställning”. Här anges bland annat att ”behörigheter till samtliga system och information tas bort alternativt ändras i enlighet med de behov som förändringen av anställningen medför.”

I avsnitt 8.1 sägs följande: ”Systemsäkerhetsinstruktionen är ett dokument i vilket krav på tillgänglighet, riktighet, sekretess, och spårbarhet för ett enskilt datasystem anges. Den ska innehålla de samlade krav på säkerhet som ställs på datasystemet. Det är viktigt att systemsäkerhetsinstruktionen *formellt fastställs av systemägaren* (vår kursivering) eftersom den ligger till grund för beslut om vilka säkerhetsåtgärder som ska vidtas. Av instruktionen skall bland mycket annat framgå hur behörighetstilldelningen skall hanteras. I avsnitt 8.6 kan läsas att ”Test- och utvecklingsmiljö ska

vara åtskild från driftmiljön eftersom icke testad program- och hårdvara kan orsaka allvarliga driftstörningar, t.ex. oönskad förändring av filer, dataförlust och systemfel. En liknande uppdelning bör också ske mellan utvecklings- och testfunktionerna för att testning ska kunna ske i känd och stabil miljö."

Under avsnitt 9.2 "Behörighetsadministration" framgår bland annat att: "Åtkomstskydd förutsätter en väl fungerande användarregistrering. Vid användarregistreringen ska alltid nedanstående *formella rutiner* (vår kursivering) användas:

- Verksamhetsansvarig ska skriftligen bevilja registrering av ny användare. Verksamhetsansvarig ska även skriftligen bevilja förändring i behörighet för enskilda användare.
- Varje användare skall tilldelas ett användar-ID som skall vara personligt och unikt.
- Alla användare ska vara registrerade i en förteckning.
- Ej giltiga behörigheter ska kontinuerligt ta bort för att undvika att personer som slutat sin anställning eller bytt arbetsuppgifter finns kvar i datorsystemen.
- Rutiner och ansvar för borttagning av användar-ID: n och behörigheter i samband med avslutande eller annan förändring av anställning ska finnas.

Under avsnitt 10 rubricerat "Riktlinjer för loggning av IT-resurser i Örebro kommun" framgår bland annat att:

- Loggning av kommunens datasystem, datanät och IT-baserade tjänster är enbart tillåten då den är nödvändig för att kunna säkerställa driften och säkerhetsnivåerna och för att kunna utföra felsökning. *All annan form av loggning är enbart tillåten då det i lagstiftning finns krav på att loggning av händelser ska ske* (vår kursivering) eller då det föreligger misstanke om brott.
- Vid all loggning av IT-resurser måste alltid skyddet av den personliga integriteten värderas högt.
- För all loggning som genomförs ska det finnas rutiner för hur loggningen ska följas upp.
- En viktig del av loggningen är att ge underlag för kontroll av att användare och systemadministratörer inte överträder sina tjänstemässiga befogenheter, därför ska behörigheten att ta del av säkerhetsloggar begränsas.
- Alla loggresultat ska skyddas mot obehörig förändring och borttagning. Skyddet ska omfatta både loggresultat och eventuella funktioner som kan förhindra loggning.

8.1.3 Styrande dokument för socialförvaltningen

Det hänvisas inte till eller nämns något om Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården SOSFS 2008:14 i de dokument vi tagit del av. Vi har erhållit tre dokument som i någon och olika omfattning uppges styra informationssäkerheten på förvaltningen. Vår iakttagelser håller sig inom avgränsningen för denna granskning.

8.1.3.1 Riktlinje för rapportering och informationsöverföring i Örebro kommun

Dokumentet daterat 2012-03-12. Det står även att läsa att dokumentet är: ”Upprättad och fastställd av Medicinskt ansvariga (MAS/MAR) i Örebro kommun 2010 reviderad 2012. Ansvariga för översyn och revidering av riktlinjerna är medicinskt ansvariga.” Med bäring på denna granskning finns instruktioner för läsbehörighet i journaler för omvårdnadspersonal. Instruktionerna underbyggs med en bakgrundsbeskrivning av de föreskrifter och lagar som styr läsbehörighet. Det finns även ett kortare stycke om loggning.

8.1.3.2 Informationshantering och journalföring i hälso- och sjukvård

Dokumentet är version 2 och giltigt från 2012-09-01, senast reviderad 2013-08-15 och beslutat av MAS/MAR-gruppen Regionförbundet Örebro. Det framgår även att dokumentet skall revideras under hösten 2015. Angående informationssäkerhet står bland annat följande att läsa:

- Vårdgivaren ska ge direktiv och säkerställa att det i verksamhetens ledningssystem för kvalitet och patientsäkerhet finns en dokumenterad informationssäkerhetspolicy.
- Vårdgivaren ska utse en eller flera personer som ska ansvara för informationssäkerhetsarbetet. Den eller de som har fått denna uppgift ska minst en gång om året till vårdgivaren rapportera vilka granskningar och skyddsåtgärder av större betydelse som har gjorts i enlighet med informationssäkerhetspolicyn, vilka riskanalyser som har utförts avseende informationssäkerheten och vilka förbättringsåtgärder som har vidtagits.
- Verksamhetschefen ska inom ramen för vårdgivarens ledningssystem för kvalitet och patientsäkerhet ansvara för att utdelade behörigheter för åtkomst till patientuppgifter är ändamålsenliga och förenliga med hälso- och sjukvårdspersonalens och andra befattningshavares aktuella arbetsuppgifter och att uppföljning av informationssystemens användning utförs genom regelbunden kontroll av loggarna.
- Vårdgivaren ska bestämma villkor för åtkomst till patientuppgifter samt upprätta rutiner för tilldelning, förändring, borttagning och regelbunden uppföljning av behörigheter.

8.1.3.3 Informationsöverföring och samtycke inom hälso- och sjukvård

Dokumentet är version 1 och giltigt från 2015-06-01, beslutat av MAS och MAR Örebro kommun. Tidigt i dokumentet framgår att: ”Det är endast vid en aktuell vårdrelation som hälso- och sjukvårdspersonal har rätt att ta del av uppgifter om den enskilde.” och ”Grunden vid all hantering av personuppgifter och uppgifter om den enskildes hälsotillstånd är sekretess. För att kunna bryta sekretessen krävs att en så kallad sekretessbrytande bestämmelse används.”

Loggning nämns på följande sätt: ”Vårdgivaren har ansvar för att det finns rutiner för att systematiskt kontrollera om någon obehörigen kommer åt dokumentation och personuppgifter. För att upptäcka eventuell felaktig eller obehörig åtkomst görs systematisk kontroll av loggar. Ett antal användare tas slumpvis ut varje månad av Treserva användarstöd och kontrolleras av respektive chef. Vid upptäckt av felaktigheter ska MAS/MAR, säkerhetsansvarig och områdeschef kontaktas för åtgärder. MAS/MAR och chef har också möjlighet att begära ut riktade loggar runt en speciell situation eller person.”

Kommentarer

Anledningarna till att vi valt att redovisa förhållandevis detaljerade iakttagelser i de styrande dokumenten är i grunden två. Kommunens har en modern och tydlig övergripande informationssäkerhetspolicy som till sin utformning även innehåller tydliga och praktiska riktlinjer. Socialtjänsten å sin sida har tydliga och riktiga ambitioner med sina dokument. De är dock i sin helhet inte enligt riktlinjerna och därtill inte fullständiga som styrande dokument. Dokumentet från regionförbundet Örebro torde inte ha någon formell betydelse. Det innehåller även instruktioner som inte överensstämmer med kommunens riktlinjer. Vi bedömer att socialtjänsten har ett digert arbete framför sig för att nå efterlevnad av de kommungemensamma dokumenten. Med bäring på avgränsningen för vår granskning saknar vi framför allt en systemsäkerhetsinstruktion för Treserva. Vi noterar att MAS/MAR avser revidera ett dokument under hösten 2015. Vi anser att det är mer ändamålsenligt att i en första fas snarast påbörja upprättandet av en systemsäkerhetsinstruktion. Med delanvisningar och -instruktioner som bygger på punktlistan i riktlinjens avsnitt 8.1 får förvaltning en användbar start på ett aktivt informationssäkerhetsarbete. SOSFS 2008:14 skall naturligtvis beaktas och efterlevas. Det som vi ovan och nedan framhåller från andra avsnitt i riktlinjerna är även de att beakta och hantera i ett sådant arbete. Utan tydlig och konkret styrning, information, utbildning och kontroll finns ingen möjlighet att uppfylla vare sig kommunens övergripande mål eller förvaltningens egna vad gäller tillförlitlig informationssäkerhet.

8.2 Särskilda instruktioner för tilldelning av behörigheter

8.2.1 Extern verksamhetspersonal och personer från annan verksamhet i kommunen

Extern part anmäler behörig person som skall fungera som beställare vad gäller AD-konton för sina anställda. Dessa konton identifieras av att de i sin benämning börjar med **temp** eller **ext**. Behörigheten till Treserva beställs efter detta av en intern bemanningsenhet på Örebro kommun. I detta fall den enhet som ansvarar för att köpt tjänsten av den externa parten. När bemanningssköterskorna jobbar i Örebro kommun loggar de in med sina konton på datorer tillhörande kommunen. Därefter loggar de in i Treserva. Detta är en beskrivning av vad som uppges göras. Ingen hänvisning finns till formellt beslutade rutiner med bäring på informationssäkerhet.

I de kommunövergripande dokumentet avsnittet 9.5 ”Riktlinjer för tredjepartsåtkomst” finns ett börkrav om att utföra en riskanalys för att identifiera vilka krav som ska ställas på åtkomstskyddet. Vi kan inte se att detta har anammats av socialförvaltningen. Vi kan heller inte iaktta att förvaltningen på ett formellt, enhetligt och dokumenterat sätt informerar tredje part om vilka säkerhetsåtgärder som krävs för att administrera tredjepartsåtkomst till kommunens informationsbehandlingsresurser. Hade det gjorts borde det finnas sekretessavtal enligt det skallkrav som framgår av 9.5.2 ”Principer”. I avsnittet nämns även att konsulters skyldigheter i övrigt skall regleras i avtal.

”LOV-företag” vilka ska utföra omsorg i Örebro kommun går först igenom en godkännandeprocess. Det görs en beställning företagsregistrering LOV, där anges vem som är behörig beställare på företaget. Efter godkännande registreras företag och beställare. Formulär finns på webben för ytterligare ansökningar av användarkonto till Treserva. Supportpersonal på kommunen skapar för LOV-företaget en organisatorisk enhet i Treserva och lägger upp en användare med behörighet som enhetschef på enheten. Den behöriga ”externa enhetschefen” kan nu beställa konton till AD: et för LOV-företagets medarbetare. Detta görs hos kommunens IT-kundtjänst via ett formulär på den

externa webben. IT-kundtjänsten kontrollerar att beställningen kommer från en behörig beställare och skapar ett AD-konto med prefixet **lov**. Efter detta skapar funktionen ”IT-Systemstöd, Vård och Omsorg” ett konto i Treserva. Med **lov**-kontot kan användaren externt nå en inloggningssida hos kommunen för att där sedan logga in i Treserva. Även detta är en beskrivning av vad som uppges göras. Ingen hänvisning finns till formellt beslutade rutiner med bäring på informationssäkerhet.

Det uppges inte finnas skriftliga rutiner för hur anställda databastekniker får behörighet till Treserva eller Treservas databas. Vi har dock fått en beskrivning av möjligheterna. Det finns en AD-grupp på sju personer för de som jobbar på enheten IT-System och datacenter. Dessa sju har alla behörighet till att komma åt data i Treservas databas. Det finns ytterligare en AD-grupp bestående av ca 20 personer vilka jobbar med driften av alla servrar i kommunen. Dessa har en teoretisk möjlighet att lägga till sig själva i AD-gruppen bestående av sju personer och därmed få tillgång till innehållet i Treservas databas.

”Sekretessförbindelse inom Vård och omsorg” som anställda inom socialförvaltningen undertecknar ser inte ut att användas för extern verksamhetspersonal och personer från annan verksamhet i kommunen.

8.2.2 Systemleverantörer, implementeringskonsulter, extern supportpersonal

Rubricerade externa användare kan vid vissa ärenden få ett tillfälligt s k VPN[3] konto med behörighet till databasen som när det till exempel behövs hjälp med felsökning. En instruktion daterad 2015-01-29 beskriver hanteringen enligt följande:

Reglerna gäller för samtliga systemleverantörer som vill ansluta till Örebro Kommuns nätverk via VPN. För varje användare skapas ett AD-konto vilket endast kan vara öppet under pågående ärende, dock längst tre månader. För varje AD-konto ska det finnas ansvarsförbindelse Denna ska skannas in och lagras som ett PDF-dokument. Beställningen kommuniceras via epost och lösenord via SMS. Alla behörigheter är grupptilldelade. Behörigheter får inte knytas direkt till AD-kontot. Driftansvarig håller koll på att varje grupp innehåller rätt medlemmar och att inte fler behörigheter än nödvändigt är kopplade till gruppen.

Väsentligt verksamhetsspecifikt innehåll i och därmed syftet med ”Sekretessförbindelse inom Vård och omsorg” som anställda inom socialförvaltningen undertecknar finns inte tydligt angivet i den ansvarsförbindelse som nu används för extern personal med VPN-anslutning mot kommunens nätverk. Det får anses osäkert om det är de senast antagna informationssäkerhetsdokumenten som nås från de länkar som redovisas i dokumentet. Exempel på ansvarsförbindelse, daterad 2012-08-16, vi tagit del av ger konsulten tillgång till kommunens nätverk och i förlängningen Treserva tills vidare. Detta trots att förbindelsen anger att ”samtliga VPN-konton har en bestämd tidsperiod”.

[3] En teknik som används för att skapa säkra förbindelser i ett datornätverk.

Kommentarer

Det finns ingen anledning till att extern verksamhetspersonal och personer från annan verksamhet i kommunen samt systemleverantörer, implementeringskonsulter och extern supportpersonal *inte* skall omfattas av samma tydligt redovisade sekretess som de som har sin anställning på socialförvaltningen. Verksamhetsansvariga skall inte tveka om att snarast identifiera alla dessa personer, informera de om vad sekretess innebär samt tillse att få en sekretessförbindelse undertecknad från var och en. Alternativet är att de ansvarsförbindelser som används inventeras och uppdateras till den sekretessnivå som är ändamålsenlig för socialtjänsten.

8.3 Hur säkerställs kunskapen om och efterlevnaden av styrdokumenten?

Inom förvaltningen finns inga formellt beslutade åtgärder som skall leda fram till att det finns kunskap om och efterlevnad av kommunens likaväl som förvaltningens styrdokument avseende informationssäkerhet.

Kommentarer

Förhållandet är otillfredsställande. Som framgår av ovan så saknas väsentliga styrdokument anpassade för den verksamhet socialtjänsten bedriver. När för verksamheten ändamålsenliga styrdokument finns plats är det nödvändigt att alla berörda över tid har en samlad tillgång till dessa. Regelbundet skall det ske kontroll av att alla känner till var de finns, vad de innebär, att de förstås och efterlevs. Det är särskilt viktigt att nyheter och förändringar når fram till berörda. Sker detta inte inom ramen för internkontrollplanen så behövs en alternativ lösning som säkerställer en regelbunden kontroll.

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

Det framkommer i våra intervjuer att behörighetshantering och loggkontroll *inte* varit föremål för några internkontrollmoment de senaste åren. Det är tveksamt om informationssäkerhet varit ett kontrollmål någon gång de senaste fem åren. I övrigt se kommentarerna i avsnittet ovan.

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

Treserva har en funktion som slumpvis kan välja kontrollobjekt datum/tid och på användare. Under vår granskningsperiod har det gjorts slumputtag på de olika roller som har behörighet att hantera patientjournalen. De användare som blir resultatet av ett slumpurval förtecknas och detta kommuniceras även till respektive enhetschef. Användaren får samtidigt ett meddelande om att den omfattas av en loggkontroll. Detta förfarande utförs en gång varje månad. Loggrapporten översänds till utsedda granskare som går igenom loggrapporten. Vad vi kan iaktta finns inga förvaltningsgemensamma instruktioner om hur detta skall gå till. Varje loggrapport finns även elektroniskt sparade i en särskild struktur på en server dit få har behörighet. Bland dessa finns två It-tekniker med

behörighet att ändra mappens innehåll. Undertecknade logglistor som visar att en rapport granskats arkiveras i kassaskåp.

Så kallade riktade kontroller kan utföras påkallat av att något särskilt har inträffat. Rutinen i övrigt överensstämmer med när slumpurval görs. En särskild beställning för denna typ av kontroll är vid granskningstillfället under framtagande.

Externa aktörer (som enligt uppgift utför 59 % av all tid inom service och 17 % inom omvårdnad) kan begära loggar från Treserva. Att och hur kommunen utför en kontroll gentemot de externa utförarna egna kontroller finns inte dokumenterat. Vi har tagit del av ett avtal med en extern aktör avseende omvårdnadstjänster. Av avtalet framgår att utföraren ska uppfylla dokumentationskrav enligt SOSFS 2008:14 och att det skall finnas en ”rutin för egenkontroll av dokumentation”.

Vi noterar att det inte finns någon beslutad strategi baserad på någon form av analys när ovan beskriven kontrollmetod valts. Det tycks vara så att det som erbjuds i Treservas användargränssnitt används utan att ha beaktat andra strategier och/eller metoder. Kommunens riktlinjer för informationssäkerhet anger inte exakt hur denna typ av loggning skall gå till.

Kommentarer

Att vid loggkontroll endast använda ett urval styrt av slumpen anser vi inte ger ansvariga möjlighet att säkerställa att patientjournalen över tid hanteras på ett korrekt sätt. Vi anser att förvaltningen skall genomföra en risk och väsentlighetsanalys som omfattar hela processen för loggkontroll oavsett om det är kommunen eller en extern aktör som är utförare. Resultatet av den utmynnar rimligtvis i en dokumentation som vägleder de ansvariga och informerar användarna. Vi vill i detta sammanhang särskilt uppmärksamma att dokumentationen skall innehålla instruktioner om hur urval sker, bedömningsgrunder, vad som skall dokumenteras, anställdas möjlighet att få utfallet av kontrollen överprövad och hur kontrollresultaten förvaras. Överväg i sammanhanget vilka möjligheter IT-tekniker skall ha vad gäller att kunna påverka fullständigheten och riktigheten i de lagrade loggrapporterna. Åtgärder måste även utföras för hur det skall kontrolleras att externa aktörer utför sin avtalsbundna kontroll samt var resultatet av denna skall förvaras. Vi anser även att de iakttagelser vi gör i avsnittet 8.7 nedan bör få påverka på vilket sätt kontrollerna utförs.

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

För att få behörighet till Treserva krävs en administrativ åtgärd som dokumenteras på en blankett vilken är åtkomlig på kommunens intranät. Det är chefen i linjen som beställer konton till underlydande personal. Kommunen tillämpar ”Windows verifierad användare” som inloggningsmetod. Metoden förutsätter att Windows katalogtjänst (AD) används i kommunens nätverk. Med denna metod måste användaren ange sitt nätverkslösenord vid inloggning i Treserva. Kontroll av användaren sker alltså mot katalogtjänsten och inte enbart mot att användaren finns upplagd i Treserva. I samband med att konto erhålls så måste användaren genomgå en interaktiv utbildning som utmynnar i att en ansvarsförbindelse skrivs under. Av ansvarsförbindelsen framgår vad som krävs av användaren. Bland annat framgår att det endast är tillåtet att använda sin behörighet i den utsträckning som krävs för att kunna utföra sina arbetsuppgifter. Användaren upplyses också om att dennes aktiviteter i Treserva loggas. Förbindelsen undertecknas av användaren och den chef

som beställt behörigheten. Det är funktionen IT-Systemstöd, Vård och Stöd som registrerar användaren med de behörigheter som krävs för dennes kombination av roll, organisation och uppdrag.

Vi noterar att det vid granskningstillfället saknas en effektiv och fullständig möjlighet att få överensstämmelse mellan alla i systemet registrerade användare och dokumentationerna beställning och ansvarsförbindelse. Anledningen till detta är bland annat att alla beställningar inte finns centralt och systematiskt förvarade. När Treserva infördes registrerades inte alla användare med underlag av beställningar. Listor med användare i avvecklade system användes istället som underlag. Listorna finns idag inte kvar. När det bedömts som akut att registrera användare har detta gjorts med löfte att en beställning skulle komma i efterhand. Alla sådana löften uppges inte ha uppfyllts. Vi noterar att blanketterna inte används för att förändra och avveckla behörigheter.

Det fanns vid granskningstillfället 6 776 användare, noterade som personer, i systemet. I våra jämförelser som redovisas under avsnitt 8.7 nedan noterar vi att av dessa så finns 5 531 även registrerade i AD: et. En skillnad på 1 245 användare. Det finns även vad vi benämner som funktionsbehörigheter till systemet. En grupp av individer som kan använda en och samma användaridentitet.

Kommentarer

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 en dokumenterad identitet och *alltid* hitta en handling underskriven av berättigad som verifierar riktigheten i en enskild persons behörighet. Vi anser att det finns anledning att utveckla rutiner för detta där förändringar och avveckling även kan hanteras. Rimligtvis finns det över ettusen användare som behöver avaktiveras samt ett stort och okänt antal som behöver verifieras som legitima användare med rätt behörigheter. Funktionsbehörigheter kan vara både praktiska och nödvändiga men det skall alltid gå att identifiera vilka som kan använda dem, på vems ansvar och under vilken tid. Funktionsbehörigheter med omfattande tillgång till och påverkan av 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 på kommunen. Behörigheterna skall även när så erfordras vara tidsbegränsade. Under längre bortovaro skall de avaktiveras. De iakttagelser vi gjort gör att vi rekommenderar att en inventering av befintlig behörighetstilldelningen utförs.

När organisatoriska förändringar inte återspeglas i vem som över tid skall ha behörighet ökar risken för att systemet inte används som det är avsett. Med organisatoriska förändringar avses personal som slutar eller övergår till annan verksamhet i kommunen. Även förändrat tjänsteinnehåll och/eller ansvar innebär att rolluppsättningen rimligen måste förändras.

8.7 Jämförelse av personförekomst i PA-systemet, i den centrala katalogtjänsten och data från Treserva.

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

- 1 043 292 rader från Treservas händelselogg.
- Användardata (behörigheter och roller i Treserva) för 6 776 noterade som personer. 5 331 av dessa återfinns i AD: et. Det är de 5 331 som nedan benämns användare.
- 19 825 personers anställningsdata registrerade i kommunens PA-system
- 16 975 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, ibland formulerad som en öppen fråga, tillsammans med iakttagelser och kommentarer under avsnitten 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. Under granskningsperioden finner vi användare i Treserva som *inte* återfinns i anställnings-registret. Detta även när hänsyn tas till de som har användaridentiteter som identifierar dem som kommunexterna användare. De är färre än tio men det låga antalet indikerar att det ändå finns en risk för att en person *utan* anställning i kommunen under en begränsad tid kan använda systemet.

2. Vi finner två identiteter för test. En kan knytas till en person. En finns upplagd i AD: et. Det är positivt att ingen av dem återfinns i händelseloggen. Anonyma testidentiteter *skall inte* finnas och användas där integritetskänslig data hanteras. Det skall aldrig under några förhållanden råda något tvivel om vem som använt systemet och varför. Alla tester skall ske i särskild testdatabas.

3. Det finns användare som är upplagda med fler än en identitet. Vi kan iaktta detta bland de som enbart har kommuninterna identiteter, de som har fler än en temporär (prefix temp) identitet och de som har en identitet knuten till ett LOV-företag. Eftersom händelseloggen, såsom den bristfälligt fungerar, inte redovisar användaridentiteter utan enbart användar-namn kan vi inte uttala oss om dubbletterna använts eller inte. Denna brist försvårar även exakt identifikation i loggen när flera användare har samma vanliga för- och efternamn. Oavsett det senare skall det finnas väl dokumenterade motiv för att en och samma person skall kunna använda systemet iklädande sig fler än en identitet.

4. Vi identifierar flera personer i PA-systemets anställningsregister som med ledning av hur de kategoriseras (sjuksköterska, undersköterska, vårdbiträde etc.) borde ha en identitet registrerad i Treserva 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 här beskrivits införs så snart tillfälle ges.

5. Vår analysperiod innebär att händelseloggen omfattar fem månader. Heltidsengagerade som har loggats på ett mycket stort respektive ett mycket litet antal datum inom den perioden torde vara kandidater för kontroll.

6. Under analysperioden på 5 månader fanns det sammanlagt 5 331 användare som under hela eller delar av den tiden hade behörighet till hela eller delar av systemet Treserva. Av dessa har 774 användare utifrån sin roll (sjuksköterska, arbetsterapeut) behörighet/skyldighet att läsa och skriva i patientjournalen. Av resterande är det många som i vissa fall har behörighet att läsa i patientjournal trots att deras ordinarie arbetsuppgifter i huvudsak rör andra delar i systemet. Totalt har 627 användare under denna period lämnat spår (tittat, läst, skrivit etc) efter sig i händelseloggen. Vilka anledningar kan finnas till att minst mellanskillnaden 774 minus 627 *inte* lämnar något spår av sin verksamhet i loggen?

7. Vi noterar att det är 54 av 627 (8,6 %) personer som sammanlagt genererat 25 % av alla loggrader under fem månader. Om en persons befattning och ansvar *inte* motiverar att en så stor mängd loggrader genererats torde de vara aktuella för kontroll.

8. Vi noterar att det är 320 av 627 (51 %) personer som sammanlagt genererat 11 % av alla loggrader under fem månader. 80 av de 320 har loggats för färre än 10 (tio) rader. Vilken typ av befattning och ansvar motiverar en så liten mängd av aktivitet i systemet?

9. 41 användare har mellan 200 och 533 loggrader registrerade på ett enskilt datum. Ett fåtal personer 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.

10. 21 användare har i genomsnitt 75 loggrader eller fler räknat på de dagar de har loggade rader (från 23 till 125 dagar) registrerade. Ett fåtal personer i en stor mängd sticker återigen ut i jämförelse med övriga. Detta är inte sällan ett motiv för en kontroll som klargör varför och avslöjar eventuellt felaktig användning av systemet.

11. Händelsetypen ”Ta bort” genererar alltid beskrivningen ”Avslutar” och används sällan. Endast 0,7 % av alla loggrader har händelsetypen ”Ta bort”. Den har använts av sammanlagt 316 användare för sammanlagt 2 773 brukare/patienter. Att ta bort någonting är en kraftfull åtgärd som inte sällan saknar en ångrafunktion. Har alla som tar bort sin egen

registrerade data ur systemet en befattning, en anledning och ett ansvar som korresponderar till detta?

12. Finns det användare bland de 121 (19 %) som *endast* läst under fem månader som rimligen även ska ha *tillfört* data? Med andra ord personer som enligt befattningen och ansvar ska göra journalanteckningar. Bland de 121 noterar vi 17 biståndshandläggare vilket vi vid intervjuerna får kännedom inte ska och därför inte kan tillföra journalanteckningar.

13. Om man *inte* jobbar ständig natt enligt PA-systemets anställningsuppgifter och ändå som drygt tio användare loggar merparten av sina rader före 07:00 och efter 21:00 borde det vara en anledning till kontroll.

14. Personer som har en benämning/kategori enligt PA-systemet och som inte kan knytas till Hälso-, sjukvård och social omsorg är rimligtvis intressanta kontrollobjekt. Personer som enligt AD: et och/eller PA-systemet helt eller delvis tillhör en annan förvaltning/verksamhet än socialförvaltningen torde även de vara av intresse. Vi är medveten om att bland dessa finns administrativ personal som är anställd på annan förvaltning men har arbetsuppgifter som knyter de till socialförvaltningen.

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

KPMG, dag som ovan

Lars Anteskog
Projektansvarig