

PM 2014:62 RI (Dnr 033-272/2014)

Paraplysystemets säkerhet och ändamålsenlighet, revisionsrapport nr 1/2014

Remiss från stadsrevisionen, revisorsgrupp 1

Svarstid den 9 maj 2014

Borgarrådsberedningen föreslår att kommunstyrelsen beslutar följande.

1. Som yttrande över stadsrevisionens rapport Paraplysystemets säkerhet och ändamålsenlighet, revisionsrapport nr 1/2014 hänvisas till vad som sägs i promemorian.
2. Stadsledningskontoret uppdras att i dialog med berörda förvaltningar se över behovet av ytterligare åtgärder med anledning av eventuella brister i Paraplysystemets säkerhet.

Föredragande borgarrådet Sten Nordin anför följande.

Ärendet

Revisionskontoret har genomfört en granskning avseende Paraplysystemets säkerhet och ändamålsenlighet. Paraplysystemet är ett verksamhetssystem för dokumentation av enskilda ärenden inom individ- och familjeomsorg, äldreomsorg och omsorg om funktionshindrade. Granskningen har inriktats på Paraplysystemets säkerhet gentemot andra system och skydd mot obehörig åtkomst. Vidare har tillgängligheten och organisationen kring systemet granskats samt systemets utveckling och fortlevnad.

Beredning

Ärendet har remitterats till stadsledningskontoret.

Stadsledningskontoret anser att det formella kunnandet vad gäller säkerhetsfrågor och den lagstiftning som reglerar den berörda verksamheten är mycket hög på stadsledningskontoret. Det finns heller inga indikatorer som tyder på att kunskapen är otillräcklig på lokal nivå.

Mina synpunkter

Informationssäkerhetsarbetet i staden är mycket viktigt, i synnerhet för it-system som hanterar känsliga uppgifter. Staden måste därför kontinuerligt arbeta med förbättringsåtgärder inom området.

I övrigt hänvisar jag till stadsledningskontorets synpunkter.

Jag föreslår att borgarrådsberedningen föreslår att kommunstyrelsen beslutar följande.

1. Som yttrande över stadsrevisionens rapport Paraplysystemets säkerhet och ändamålsenlighet, revisionsrapport nr 1/2014 hänvisas till vad som sägs i promemorian.
2. Stadsledningskontoret uppdras att i dialog med berörda förvaltningar se över behovet av ytterligare åtgärder med anledning av eventuella brister i Paraplysystemets säkerhet.

Stockholm den 7 april 2014

STEN NORDIN

Bilaga

Projektrapport från Stadsrevisionen ”Paraplysystemets säkerhet och ändamålsenlighet Nr 1, 2014”

Borgarrådsberedningen tillstyrker föredragande borgarrådets förslag.

Miljöpartiet avstår från att delta i beslutet.

Kommunstyrelsen

Miljöpartiet avstår från att delta i beslutet.

Remissammanställning

Ärendet

Revisionskontoret har genomfört en granskning avseende Paraplysystemets säkerhet och ändamålsenlighet. Granskningen har inriktats på Paraplysystemets säkerhet gentemot andra system och skydd mot obehörig åtkomst. Vidare har tillgängligheten och organisationen kring systemet granskats samt systemets utveckling och fortlevnad. Granskningen har genomförts med hjälp av konsult. Utifrån konsultens granskning vill revisionskontoret lyfta fram några områden som kommenteras nedan.

Den sammantagna bedömningen visar på brister beträffande säkerheten för Paraplysystemet och dess information. Detta gäller såväl sekretessen av känslig information, riktigheten av ekonomiska transaktioner samt hanteringen av tillgängligheten av systemet.

Granskningen visar att Paraplysystemet har sårbarheter som var för sig inte har allvarliga följder, men genom att utnyttja dem i kombination kan det inte uteslutas att det möjliggör intrång i systemet.

Vid tilldelning av behörighet till Paraplysystemet tillämpas ett roll-baserat behörighetssystem. Detta innebär att en användare tilldelas en i förväg definierad roll. Till varje roll har knutits vissa specifika behörigheter. Granskningen visar att det vid de granskande förvaltningarna finns ett stort antal användare som har högre behörighet än vad som kan vara nödvändigt för dess yrkesutövande. Detta har också påpekats vid tidigare genomförda revisioner av hantering av behörigheter.

I granskningen har man inte funnit att det genomförts någon riskanalys för hela Paraplysystemet. Granskningen har heller inte funnit att någon riskanalys har genomförts avseende systemets teknikval, uppbyggnad och framtida kostnader. Det har heller inte gått att finna en strategisk plan för systemets framtid och dess utveckling.

Det avtal som är tecknat mellan staden och leverantören avseende förvaltning av Paraplysystemet är tydligt vad gäller omfattning och kostnad. Granskningen har visat att det finns brister i uppföljningen av kraven på tjänsten SLA (Service Level Agreement). Detta kan medföra svårigheter i att stämma av levererad tillgänglighet med avtalad tillgänglighet. Det har också noterats brister i uppföljningen av avvikelser och incidenter.

Beredning

Ärendet har remitterats till stadsledningskontoret.

Stadsledningskontoret

Stadsledningskontorets tjänsteutlåtande daterat den 17 mars 2014 har i huvudsak följande lydelse.

På uppdrag av stadens revisionskontor har konsultföretaget Europoint genomfört en granskning av Paraplysystemet med avseende på dess säkerhet och ändamålsenlighet. Rapporten innehåller påpekanden om Paraplysystemets säkerhet som bör åtgärdas och i vissa delar pågår redan ett arbete i staden med att åtgärda de brister som nämns rapporten.

Rapporten pekar dock på ett antal brister som behöver åtgärdas och stadsledningskontorets IT-avdelning arbetar tillsammans med stadens verksamheter kring detta. Stadsledningskontoret delar helt uppfattningen om att informationssäkerhetsarbetet är viktigt, i synnerhet för IT-system som hanterar mycket känsliga uppgifter. I rapporten finns emellertid flera felaktiga uppgifter som sammantaget ger en missvisande och felaktig bild av att Paraplysystemet har allvarliga säkerhetsbrister. Trots påpekande från stadsledningskontorets IT-avdelning kvarstår dock fortfarande allvarliga sakfel som ligger till grund för felaktiga slutsatser om systemets säkerhet och spårbarhet. De största sakfelen sammanfattas och kommenteras i rapporten kommenterats nedan.

Behörighetshantering

I rapporten nämns att det inte kan uteslutas att ett stort antal personer ”på ett enkelt sätt” kan utföra olämpliga, otillåtna eller olagliga handlingar i systemet samt att sådana intrång inte behöver lämna tydliga spår. Vidare nämns i rapporten att konsulten vid granskning har identifierat ett antal tänkbara, enkla tillvägagångssätt för otillåten åtkomst av information eller styrning av ekonomiska transaktioner. Granskningen sägs också ha visat att det inte finns några skyddsåtgärder som förhindrar detta.

Det lyfts också fram att det förekommer att användare har högre behörighet än avsett, bland annat mot bakgrund av att man funnit att det finns fler användare i systemet som har antingen rollen ”Verksamhetschef” eller ”Sektionschef” än som innehar dessa funktioner i verkligheten.

Stadsledningskontoret menar att staden har såväl en väl strukturerad organisation för behörighetstilldelning som spårbarhet i systemet. I konsultrapporten har inte detta redovisats utan slutsatserna bygger på felaktiga uppgifter.

I behörighetssystemet ParaInn finns Stockholms stads organisation definierad. Till organisationen är roller knutna. Rollerna är utvecklade efter verksamhetsprocessen för att IT-stödet ska motsvara verksamhetens behov i handläggningen. Fördefinierade roller finns för alla kategorier av användare inom socialtjänsten. Rollernas beteckning motsvarar inte per automatik den befattning/titel som användaren har i organisationen. I ParaInn finns det också fördefinierade kontroller på kombinationer av roller som inte kan innehas av samma användare. Exempelvis kan en användare som har rollen ”Paraplysamordnare” inte samtidigt ha rollen ”Verksamhetschef” eller ”Sektionschef”. I rollen ”Paraplysamordnare” är användaren inte heller behörig beslutsfattare.

Den högsta behörighetsadministratören på förvaltningsnivå har den tilldelade rollen ”Lokal administratör”. En ”Lokal administratör” kan inte ge sig själv nya roller utan en elektronisk beställning måste skickas till central systemförvaltning på stadsledningskontorets IT-avdelning.

En ”Lokal administratör” kan inte heller ge andra på förvaltningen rollen ”Lokal administratör” utan en elektronisk beställning måste skickas till central systemförvaltning. Rollen ”Lokal administratör” ska inte innehas av någon som har en annan verksamhetsroll i Paraplysystemet. I samband med den elektroniska beställningen görs såväl manuella som maskinella kontroller att regelverket kring beställningen är uppfyllt. Om fel sker i den manuella hanteringen, finns spärrar i systemet som innebär att beställningen inte slutförs.

Rollen ”Sektionschef” och rollen ”Verksamhetschef” är tillika behörighetsadministratörer. De kan inte ge sig själva behörigheter utan har fått rollen tilldelad av ”Lokal administratör”. De kan inte själva tilldela sig andra roller. De kan inte heller ta bort sin egen behörighet utan beställning skett eller verkställts av högre administratörs nivå. De kan inte utan beställning till ”Lokal administratör” lägga in kollegor på samma nivå som sig själva. De kan enbart lägga in personal på sin egen organisatoriska enhet.

Stadsledningskontoret vill särskilt understryka att alla steg som görs i behörighetssystemet loggas både vad gäller organisationsförändringar och rolltilldelningar. I systemet ParaInn kan varje behörighetsadministratör ta fram en behörighetsrapport. Rapporten kan tas ut per användare, enhet, förvaltning och per roll och här redovisas vad

som ändrats och vem som registrerat detta.

Den bedömning som gjorts i rapporten är att det vid stadens nämnder förekommer användare som har högre behörighet än avsett tar enligt stadsledningskontoret inte hänsyn till de verksamhetsmässiga behoven och konsekvenserna av detta. Slutsatsen att det finns för många med hög behörighet eller felaktig behörighet kan inte bedömas med annat än att behörighetstilldelningen ställs i relation till de faktiska och verksamhetsmässiga behoven. En sådan genomgång och prövning måste regelbundet göras och det är först efter en sådan prövning en bedömning kan göras om antalet med hög behörighet är för stort eller inte.

Tilldelningen av behörigheter i Paraplyet ska motsvara det behov som finns i verksamheten och följer de roller som identifierats och följer inte automatiskt den organisatoriska titel man har på förvaltningen. Paraplysystemet har idag drygt 17 000 användare och för att verksamheten ska fungera är det stadsdelsförvaltningarnas uppgift att identifiera personer som ska tilldelas dessa olika roller. Att dra slutsatsen att staden har för många personer med för hög behörigheter måste ställas i relation till välfärdsuppdraget att få en fullt fungerande social verksamhet.

Åtkomstkontroll och inloggning

Påståenden i rapporten om att ett stort antal personer på ett enkelt sätt kan utföra olämpliga, otillåtna eller olagliga handlingar i systemet och inte behöver lämna tydliga spår är helt missvisande och felaktigt. Detta har beskrivits ovan i hur stadens behörighetssystem fungerar och att det finns tydlig spårbarhet.

När det gäller beslut och utbetalning av ekonomiskt bistånd finns dokumenterat vilka rutiner för utbetalning av ekonomiskt bistånd som ska följas och processen för detta beskrivs. Det finns även rutiner för avstämningar för ersättningar inom äldreomsorgen och omsorgen om funktionshindrade samt utbetalningar till kontaktpersoner och familjehem. Dokumentationen är tillgänglig för användarna under en länk i inloggningen till Paraplysystemet.

Beslutet om ekonomiskt bistånd är ett myndighetsbeslut och för att vara behörig beslutsfattare krävs att man som enskild handläggare har rätt delegation. Beslut om delegationsordningen fattas av nämnden inom respektive förvaltning. Processen med utbetalningar av bistånd inleds med att en handläggare, med rollen socialsekreterare eller biståndsbedömare, registrerar ett beslut. För att utbetalning ska kunna verkställas måste avstämning göras i Paraplysystemet. Avstämningar gör av en person med den tilldelade rollen avstämmare. Det finns en spärr i systemet så att en avstämmare inte kan stämma av beslut som de själva beslutat om i de fall avstämaren även innehar rollen socialsekreterare. För behörighet att få den tilldelade rollen avstämmare krävs underskrift av högsta behörig chef på förvaltningen, vanligtvis förvaltningschefen. Rollen avstämmare kan endast läggas in i systemet av den med högst behörighet på förvaltningen vilket är den lokala administratören.

I hela denna kedja av aktiviteter finns en spårbarhet i systemet.

I revisionsrapporten påstås vidare att det är möjligt att logga in i systemet med annans identitet utan att detta uppmärksammas. Detta påstående grundar sig på det faktum att inloggning i Paraplysystemet sker med användar-ID och lösenord och att den person som loggar in i systemet inte behöver vara samma person som samtidigt är inloggad på datorn.

Det stämmer att inloggning i Paraplysystemet sker med användar-ID och lösenord. Så är också fallet för majoriteten av de verksamhetssystem som finns i offentliga Sverige, olika typer av sociala system inräknat. På stadsledningskontoret pågår ett arbete med att övergå till enbart tjänstekortsinloggning även för Paraplysystemet men denna åtgärd kommer enbart att öka den redan idag höga säkerhetsnivån marginellt. Stadsledningskontoret vill tydliggöra följande: Inloggning i Paraplysystemet sker i tre steg. Det första steget är inloggning i arbetsplatsystemet, därefter inloggning i Citrix och slutligen i Paraplysystemet.

En användare i staden som inte använder tjänstekort behöver för att komma in i systemet först logga in på en dator med sitt användar-ID och lösenord till själva datorn. För att sen komma vidare till Paraplysystemet loggar användaren in i den så kallade Citrix-miljön där

ikonen till Paraplysystemet finns. I ett tredje steg loggar användaren, med helt andra inloggningsuppgifter (användaruppgifter och lösenord), sedan in i själva Paraplysystemet. För att nå Paraplysystemet måste användaren ha ett tilldelat konto och en tilldelad roll i Paraplysystemet och inloggning kan alltså inte ske om detta saknas. Har användaren endast ett konto men saknar roll kommer användaren inte vidare. Denna trestegsmodell gör att säkerheten avseende åtkomstkontroll är högre i Paraplysystemet än i de flesta andra verksamhetssystem i staden. Att logga in i systemet med annans identitet är endast möjligt om du dels har tillgång till en dator med åtkomst till Paraplysystemet, dels olovligen har tillförskaftat dig den personens inloggningsuppgifter.

Säkerhetsmedvetandet

I revisionsrapporten framhålls att säkerhetsmedvetandet vid såväl den centrala systemförvaltningen som de granskade förvaltningarna inte motsvarar den höga känsligheten hos informationen i systemet.

Stadsledningskontoret menar att rapporten inte grundar påståendet på några verifierbara fakta och är väl generella. Det finns inte heller några verifierbara fakta som detta påstående grundas på. Stadsledningskontoret anser vidare att det formella kunnandet vad gäller säkerhetsfrågor och den lagstiftning som reglerar den berörda verksamheten är mycket hög på stadsledningskontoret. Det finns heller inga indikatorer som tyder på att kunskapen är otillräcklig på lokal nivå.

Sådana fakta som skulle kunna ligga till grund för påståendet om brister i säkerhetsmedvetandet är till exempel sådant som anges i det följande. Inget av sådana fakta presenteras i rapporten.

- Om policys, riktlinjer och dokumentation finns och hur dessa efterlevs.
- Hur personal är motiverad att arbeta i enlighet med dessa policys med mera
- Tester om säkerhetsmedvetande och kunnande
- Antalet inträffade incidenter
- Logganalyser och uppmätta avvikelser

Stadsledningskontoret ansvarar för stadens gemensamma it-infrastruktur, leverantörsstyrning, större incidenthantering samt förvaltning och utveckling av stadsgemensamma system. När det gäller Paraplysystemet är just säkerhetskunnande och hantering av integritet och sekretesskyddad information en grundläggande del av allt förvaltnings- och utvecklingsarbete och den personal som arbetar med detta är anpassad för att klara dessa krav.