Stockholms stad

Paraplysystemets säkerhet och ändamålsenlighet

Nr 1, 2014

Projektrapport från Stadsrevisionen

Dnr 3.1.3-138/2013

Den kommunala revisionen är fullmäktiges kontrollinstrument för att granska den verksamhet som bedrivs i nämnder och bolagsstyrelser. Stadsrevisionen i Stockholm granskar nämnders och styrelsers ansvarstagande för att genomföra verksamheten enligt fullmäktiges uppdrag. Stadsrevisionen omfattar både de förtroendevalda revisorerna och revisionskontoret.

I ”årsrapporter” för nämnder och ”granskningspromemorior” för styrelser sammanfattar Stadsrevisionen det gångna årets synpunkter på verksamheten. Fördjupade granskningar som sker under året kan också publiceras som projektrapporter.

Publikationerna finns på Stadsrevisionens hemsida. De kan också beställas från revisionskontoret.

Paraplysystemets säkerhet och ändamålsenlighet
Nr 3, År 2014

Dnr 3.1.3-138/2013

Hemsida:
www.stockholm.se/revision

Till
Kommunstyrelsen
Socialnämnden
Äldrenämnden
Bromma stadsdelsnämnd
Hägersten-Liljeholmens
stadsdelsnämnd

Paraplysystemets säkerhet och ändamåls-enlighet

Revisorsgrupp 1 har den 4 februari 2014 behandlat bifogad revisionsrapport (nr 1/2014).

Granskningen visar bland annat att det finns brister i nämndernas behörighetshantering. Detta kan påverka säkerheten för Paraply-systemet och dess information. Detta gäller såväl sekretessen av känslig information, riktigheten av ekonomiska transaktioner samt hanteringen av tillgängligheten av systemet.

I granskningen har man inte funnit att det genomförts någon risk-analys 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.

Nämnderna bör snarast åtgärda de brister som noterats i behörighetshantering. Kommunstyrelsen, tillsammans med berörda nämnder, bör inom ramen för sitt ansvar se över behörighets-rollerna. Vidare bör kommunstyrelsen genomföra en riskanalys för hela Paraplysystemet. Kommunstyrelsen bör även genomföra en riskanalys med fokus på systemets teknikval, uppbyggnad och framtida kostnader.

Vi hänvisar i övrigt till rapporten och överlämnar den till kommun-styrelsen, socialnämnden, äldrenämnden samt stadsdelsnämnderna Bromma och Hägersten-Liljeholmen för yttrande. yttrandet ska ha inkommit till revisorsgrupp 1 senast den 9 maj 2014. Rapporten överlämnas också till övriga stadsdelsnämnder för kännedom.

På revisorernas vägnar

Bengt Akalla
Ordförande

Maria Lindgren Persson
Sekreterare

Stadsrevisionen
Revisionskontoret

Hantverkargatan 3 D, 1 tr
Postadress: 105 35 Stockholm
Telefon: 08-508 29 000
Fax: 08-508 29 399
www.stockholm.se/revision

Sammanfattning

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 rollbaserat 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 tecknats 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.

Granskningen visar att säkerhetsmedvetandet inte motsvarar den höga känsligheten hos den informationen som behandlas i Paraply-systemet. Nämnderna uppvisar bristande insikt om de sårbarheter som systemet uppvisar, liksom möjligheterna att utnyttja dessa.

Respektive nämnd har ansvar för att ta fram lokala kontinuitets-planer. Dessa ska beskriva vad som ska göras om och när de sociala systemen inte är tillgängliga. Vid de granskade nämnderna hade en sådan plan inte upprättats.

De synpunkter avseende systemets användbarhet som framkommit i granskningen visar att åsikterna skiljer sig åt mellan användarna. Vissa av användarna upplever att systemet är bra medan andra användare tycker det är ett otympligt och trögt system. Användarna har också haft synpunkter på att inloggningen till systemet är långsam.

Sammanfattningsvis bör ansvariga nämnderna snarast åtgärda de brister som noterats i behörighetshantering. Ansvariga nämnder bör också upprätta lokala kontinuitetsplaner. I samarbete med stadsdelsnämnderna, socialnämnden och äldrenämnden bör kommunstyrelsen inom ramen för sitt ansvar se över utformningen av behörighetsrollerna samt informera om it- och informationssäkerhet. Vidare bör kommunstyrelsen genomföra en riskanalys för hela Paraply-systemet.

I konsultens rapport beskrivs granskningen närmare. Där redovisas också iakttagelser, bedömningar och rekommendationer utifrån genomförd granskning.

europoint

Version: 1.3

Paraplysystemets säkerhet och ändamålsenlighet, Stockholm stad

Revisionsrapport

Datum: 2014-01-29

Författare: Lennart Beckman,
Martin Buczynski,
Ted Sinabian

Adress
Europoint Networking AB
Uppsala Science Park
751 83 Uppsala

Tel
018-18 30 30

Org.nr
556608-8810

E-post/Webb
info@europoint.se
www.europoint.se

Innehåll

1 Sammanfattning

Europoint har genomfört en granskning av Paraplysystemet med avseende på dess säkerhet och ändamålsenlighet. Tyngdpunkten för granskningen har varit säkerhet.

Kraven på säkerhet i Paraplysystemet är höga, då systemet hanterar känslig personinformation samt styr stora penningströmmar.

Granskningen har varit bred och avsedd att svara på ett antal olika revisionsfrågor, i syfte att belysa ett flertal aspekter av systemets säkerhet.

De viktigaste iakttagelserna är:

1. Det är inte uteslutet att användare enkelt och med liten risk för upptäckt kan utföra olämpliga åtgärder, även av ekonomisk art. En kombination av brister underlättar detta.
2. En långsiktig plan för systemet saknas.
3. Uppföljning av incidenter och leverantörens servicenivåer har brister.
4. Brister i riskhantering och riskanalyser.
5. Brister i säkerhetsmedvetande och säkerhetsarbete.

Vi rekommenderar att punkt 1 utreds noggrant och åtgärdas omgående. Vi rekommenderar att punkt 2 till 5 utreds och åtgärdas.

2 Uppdrag

Uppdraget omfattade revision av Paraplysystemets säkerhet och ändamålsenlighet.

Beställare av uppdraget var revisionskontoret, Stockholm stad. Uppdraget avsåg genomförande av ett projekt i revisionskontorets plan för år 2013[1], benämnt ”Paraplysystemets säkerhet och ändamålsenlighet”.

De revisionsfrågor som har ställts är:

1. Är roller och ansvar tydliga vad gäller systemägare, systemförvaltning, informationsansvar och drift?
2. Hur säkras att informationen i systemet är tillförlitlig?
3. Är systemet ändamålsenligt och effektivt, exempelvis vad gäller användarvänlighet, funktion, rätt information?
4. Hur säkras att systemet har en god tillgänglighet (driftstopp, informationsförlust, m.m.)?
5. Är informationen skyddad för obehörig åtkomst?
6. Finns en riskbedömning och planering (kostnader, säkerhet och funktionalitet) som underlag för ställningstagande vad gäller systemets framtida utveckling?
7. Finns rutiner för att garantera säkerheten i Paraplysystemets gränssnitt gentemot andra system?

Projektledare från revisionskontoret var Susanne Eriksson, kommunal revisor.

Uppdraget har utförts av Europoint Networking AB. Bemanningen var Lennart Beckman (projektledare), Björn Sjöholm (kvalitetsansvarig), Martin Buczynski och Ted Sinabian.

Vid projektets start framhölls att tyngdpunkten på revisionen är säkerhet. Revisionen har inriktats på att hantera hela omfattningen av revisionsfrågorna. Vissa frågeställningar bör utredas i ytterligare detalj.

3 Genomförande

Revisionen har genomförts genom intervjuer med nyckelpersoner samt dokumentgranskning.

Stockholms stad representerades av personer från Stadsledningskontoret, två stadsdelsförvaltningar samt två fackförvaltningar. Leverantören, Tieto, representerades av nyckelpersoner från förvaltningsledning, drift samt utveckling. Intervjuerna med Tieto har kompletterats med ett frågeformular omfattande cirka sextio frågor, vilka har besvarats skriftligen. Vissa intervjuer med Stadsledningskontoret och förvaltningarna har kompletterats med epost-frågor och i några fall telefonuppföljning.

[1] Se referens [17].

De personer som har intervjuats finns uppräknade i Bilaga 1. I Bilaga 2 anges de dokument som har granskats. I texten finns referenser till dessa dokument.

4 Bakgrund

4.1 Paraplysystemet

Paraplysystemet är ett verksamhetssystem för dokumentation av enskilda ärenden inom individ- och familjeomsorg, äldreomsorg och omsorg om funktionshindrade. Systemet är också stadens socialregister och innehåller enskilda ärenden inom dessa verksamhetsområden. Det finns cirka 17 000 aktiva användare av Paraplysystemet. Användarna består av handläggare på förvaltningar samt av interna respektive externa utförare av verksamheterna.

Detta innebär att systemet har ett omfattande innehåll, bestående bland annat av personakter, journalanteckningar, beslut, ekonomiska beslut, utförarrapportering, utförardokumentation samt fasta rapporter. Paraplysystemet är utvecklat speciellt för Stockholm stad, och utgör, tillsammans med ett antal standardsystem, en grupp system benämnd Sociala system[2].

4.2 Organisation

Kommunstyrelsen är systemägare till Paraplysystemet. Systemägaren genom sin förvaltning ansvarar för att driften, förvaltningen och utvecklingen av Paraplysystemet sker på ett säkert sätt i enlighet med lagar, förordningar och stadens riktlinjer samt att det finns rätt avtal, manualer, processer, supportfunktioner etc. Systemet förvaltas av IT-avdelningen på stadsledningskontoret.

Stadsdelsförvaltningarna, socialförvaltningen och äldreförvaltningen äger och ansvarar för den information som registreras i Paraplysystemet. Förvaltningarna ansvarar också för att regler kring behörigheter, lagar och förordningar följs.

4.3 Säkerhetsarbete

Stadsledningskontoret ansvarar under kommunstyrelsen för att leda och samordna stadens samlade trygghets- och säkerhetsarbete, inklusive krisberedskapen. Stadsdirektören fastställer programmets riktlinjer. Stockholms stads säkerhetschef (tillika säkerhetsskyddschef) är underställd stadsdirektören. Säkerhetschefen ansvarar för ledning och samordning av stadens säkerhetsarbete och krisberedskap. Stockholms stads informationssäkerhetschef är underställd säkerhetschefen och leder stadens arbete med informationssäkerhet.

[2] En utförlig beskrivning av systemets innehåll och utveckling ges i referens [8].

5 Tidigare revisioner

Paraplysystemet har granskats vid ett antal tillfällen tidigare. Systemet är kritiskt för verksamheten, och informationsinnehållet är känsligt och viktigt.

En övergripande granskning av IT-säkerheten i Paraplysystemet gjordes 2001. Granskningen påtalar brister i ansvarsfördelning, följsamhet mot lagar, regler och avtal, risk- och sårbarhetshantering, informationsklassificering och kontinuitetsplanering, referens [13].

En revision från december 2003 granskade användarnas syn på Paraplysystemet, och konstaterade ett utbrett missnöje med systemet avseende användarvänlighet och driftsäkerhet, referens [14].

Vid en revision från september 2008 konstaterades brister i hanteringen av behörigheter i systemet. Stadsrevisionen rekommenderade att gemensamma riktlinjer bör utarbetas samt att behörighet kontinuerligt följs upp, referens [15].

En revision från januari 2009 granskade hantering av personuppgifter i systemet, referens [16].

Stadsrevisionen gjorde en uppföljande revision av behörighetshanteringen 2012 och konstaterade brister i denna, referens [17].

Stadsrevisionen gjorde även en granskning av externa utförares åtkomst till Paraplysystemet, 2013. Granskningen fann brister i rutiner för uppföljning och avslut av behörigheter, referens [18].

6 Iakttagelser

Granskningen har resulterat i ett antal iakttagelser. Dessa är kategoriserade i tretton områden. För respektive område ges en kort bakgrund till området samt en beskrivning. För varje område ges också rekommendationer på åtgärder som bör vidtas.

6.1 Informationssäkerhet

Informationssäkerhet innebär att anpassa säkerheten för att skydda information avseende dess

- sekretess
- riktighet
- tillgänglighet

samt att ha

- spårbarhet

Information som är hemlig ska skyddas mot obehörig åtkomst. Informationen ska vara riktig, innehållet ska skyddas mot både avsiktlig och oavsiktlig manipulation. Till säkerhet hör också att informationen ska vara tillgänglig när den behövs. Dessa tre krav är delvis motstridiga. Starkt sekretesskydd minskar exempelvis ofta tillgänglighet. Det är därför lämpligt att göra en genomtänkt avvägning av skyddsbehovet för informationen, och även ställa detta mot kostnaden för skydd.

I informationssäkerhet ingår såväl administrativ som teknisk säkerhet. Teknisk säkerhet omfattar IT-säkerhet och fysisk säkerhet. Skydd av information kan bestå av såväl rutiner, processer, mjukvarulösningar, hårdvara och fysiskt skydd.

Paraplysystemet hanterar känslig information. Informationen är känslig av två anledningar.

1. Systemen rymmer enskilda ärenden för äldreomsorgen och handikappomsorgen samt individ- och familjeomsorgen. Det är ett heltäckande socialregister för Stockholm stad och innehåller personakter, journalanteckningar, beslut, utförarrapportering, utförardokumentation samt fasta rapporter. Denna information skyddas av Offentlighets- och sekretesslagen (2009:400) 26 kap.
2. Systemet styr dessutom utbetalning av ekonomiskt bistånd samt ersättningar och arvoden. Utbetalningarna för ekonomiskt bistånd, olika ersättningar (anhörigbidrag, habiliteringsersättning mm) och arvoden uppgår för perioden 201301–201311 till drygt 1 miljard kr. Ersättningar betalas inte ut via Paraplysystemet, men det är genom Paraplysystemet som beslut hanteras (genom beslut av insats).

Skydd av information bör utformas efter dess känslighet. Hoten mot den första typen av information är främst knutna till obehörig åtkomst till informationen. Hoten mot den andra typen är främst

försök att uppnå ekonomisk fördel genom att påverka utbetalningar, att ändra informationens riktighet. Dessa hotbilder är inte försumbara. Den förra på grund av att informationen är känslig för enskilda individer. Den senare på grund av att systemet styr stora penningflöden med många inblandade personer.

En modell för stadsövergripande risk- och sårbarhetsanalys finns. En organisation för informationssäkerhetsarbete i stadens förvaltningar finns. I förvaltningarna finns informationssäkerhetssamordnare som är kontaktperson mot stadens informationssäkerhetschef och har utöver detta ett stort eget ansvar. Även stadsledningskontoret har en informationssäkerhetssamordnare.

Staden har en framtagen informationssäkerhetshandbok[3], som följer standarden ISO/IEC 27001. ”Riktig information ska finnas tillgänglig för behörig personal på ett spårbart sätt när den behövs”.

6.1.1 Iakttagelser och bedömningar

1. Säkerhetsmedvetandet motsvarar inte den höga känsligheten hos informationen i systemet.

Vår samlade bedömning är att säkerhetsmedvetandet inte motsvarar den höga känsligheten hos den information som behandlas i Paraplysystemet. Detta gäller både känsligheten avseende sekretess och känsligheten avseende ekonomiska felaktigheter. Vi har noterat en bristande insikt om de sårbarheter som systemet uppvisar, liksom möjligheten att utnyttja dessa. Detta gäller såväl den centrala systemförvaltningen som de granskade förvaltningarna.

2. Säkerhetsorganisationen är ej känd.

Vi har noterat att informationssäkerhetsorganisationen inte är väl känd. Det är inte av alla väl känt vilka rapporteringsvägar för informationssäkerhetsrelaterade ärenden som finns, speciellt är informationssäkerhetssamordnarens roll mindre känd.

6.1.2 Rekommendation

Vi rekommenderar att åtgärder genomförs för att höja medvetenheten om säkerhet i de sociala systemen. Utbildning samt genomförda riskanalyser kan vara en del av detta, se avsnitt 6.6, ”Riskhantering”.

6.2 Förvaltning och avtal

För att säkerställa ett systems tillgänglighet är ett väl definierat förvaltningsarbete viktigt. Detta ska följa en väldefinierad och tydlig förvaltningsmodell. På så sätt kan förvaltningsåtgärder ske på ett planerat sätt. Avvikelser och incidenter kan uppmärksammas och åtgärdas. Tillgängligheten hos

[3] Se referens [22].

systemet kan följas upp, och stämmas av mot avtalade krav, SLA (Service Level Agreement). Brister i kravuppfyllnad kan uppmärksammas och leda till förbättringsåtgärder.

Förvaltningsmodellen bör bland annat innefatta roller hos beställare och leverantör, mötesstruktur och -innehåll samt modell för förvaltningsplaner. Förvaltning av en tjänst bör baseras på avtal med tydliga krav på tjänsten.

Förvaltning av de sociala systemen avropas mot ramavtal[4], vanligen benämnt KITT-avtalet. För den period denna granskning avser gäller avropsavtal för 2013[5]. KITT-avtalet kommer att ersättas 2014-08-01 med ett nytt ramavtal[6], vanligen benämnt SIKT-avtalet.

I ramavtalet (KITT) ges möjlighet att i avropsavtal avtala särskilda SLA, utöver de i ramavtalet givna (se paragraf 10 i avtalet). I denna paragraf sägs även ”Leverantörens uppdrag omfattar även mätning, uppföljning och rapportering av relevanta parametrar, resursslag och servicenivåer i enlighet med beskrivning i Bilaga 3”. Motsvarande skrivning finns även i det kommande ramavtalet (SIKT) i paragraf 11. Detta är en bra grund för förvaltningsmöten.

I det kommande ramavtalet (SIKT) specificeras servicenivåer i bilaga 6 till avtalet, ”SLA systemdrift och systemförvaltning”. Där anges bland annat en lista över servicenivåer med en inledande text ”Följande servicenivåer ska mätas och uppfyllas av leverantören” (kapitel 2). Arbete pågår med införande av det nya ramavtalet 2014-08-01.

I avtalet anges främst servicenivåer för tillgänglighet. Tillgänglighet definieras utgående från avtalad servicetid, avbrottstid samt tillåten avbrottstid. Med avbrottstid menas, för de sociala systemen, tid när systemen inte är fullt tillgängliga för samtliga användare.

6.2.1 Iakttagelser och bedömningar

3. Tydlighet gentemot Leverantören avseende leverans och kostnader.

Avropsavtal mellan staden och Leverantören angående förvaltning är tydliga vad avser omfattning och kostnad, med referens till ramavtalet. På förvaltningsmöten redovisas beställda uppdrag, och status på dessa.

4. Väldefinierad förvaltningsmodell och processer

Förvaltningen av de sociala systemen följer en väldefinierad förvaltningsmodell, Fguide[7]. Denna är Stockholm stads variant av pm3, som är en allmänt använd förvaltningsmodell. Denna förvaltningsmodell definierar bland annat roller, mötesstrukturer och framtagande av förvaltningsplaner. Förvaltningsmodellen är under utveckling, och avsikten är att den ska än bättre anpassas till stadens organisation och sourcing-strategi samt att den ska närma sig pm3 än mer.

[4] Se referens [22].
[5] Se referens [23].
[6] Se referens [24].
[7] Se referens [7].

Förvaltningsmöten hålls en gång i månaden, med deltagande av förvaltare och förvaltningssamordnare från staden, samt affärsansvarig, driftsansvarig, förvaltningsansvarig och utvecklingsansvarig hos leverantören. Dessa möten protokollförs av leverantören.

Leverantören har också tydliga och väldefinierade processer för förvaltningen av tjänsterna. Dessa processer är till stora delar gemensamma med övriga förvaltningsåtaganden hos leverantören, vilket är till fördel för staden.

5. Kända och tydliga roller hos beställare och leverantör.

Rollerna hos förvaltningsorganisationen hos både staden och leverantören är tydliga och väl kända hos båda parter.

6. Bristande uppföljning av servicenivåer

Vid granskning av protokoll från förvaltningsmöten har vi noterat en bristande uppföljning av kraven på tjänsten, SLA. Vi har inte kunnat finna att tjänstens tillgänglighet rapporteras och följs upp, varken månadsvis, kvartalsvis eller årsvis.

Detta innebär svårigheter att utläsa trender i tillgänglighet, följa upp problem samt stämma av levererad tillgänglighet med avtalad tillgänglighet.

6.2.2 Rekommendation

Vi rekommenderar en regelbunden uppföljning av levererade servicenivåer för Paraplysystemet, baserat på avtalade servicenivåer. Denna uppföljning bör redovisas på förvaltningsmöten, med en i förväg fastlagd regelbundenhet, exempelvis varje kvartal eller en gång per år. När det nya ramavtalet träder i kraft 2014-08-01 bör uppföljning av tjänstnivåer enligt bilaga 6, kapitel 2 redovisas.

Staden bör överväga att använda ramavtalets möjligheter att definiera fler parametrar för SLA, såsom maximal total avbrottstid, maximal avbrottslängd på enstaka avbrott samt maximalt antal avbrott. Staden kan även överväga att kravställa och mäta säkerhetsnivåer.

6.3 Behörighetshantering

Staden tillämpar ett rollbaserat behörighetssystem för de sociala systemen. Detta innebär att en användare tilldelas en (eller i några fall flera) i förväg definierade roller, t.ex. ”socialsekreterare” eller ”sektionschef”. Till varje roll har knutits vissa specifika behörigheter. Exempel på behörighet kan vara ”läsa journalanteckningar i systemet”, ”ändra eller återställa lösenord” eller ”aktivera gamla konton”. Avsikten är att det ska vara enkelt och säkert att dela ut rätt behörighet till rätt användare. En användare som fullgör en viss funktion ska tilldelas motsvarande roll.

Problem kan uppstå om användare tilldelas större behörighet i ett system än vad som är avsett eller nödvändigt för den funktion användaren har. Det kan finnas flera anledningar till att alltför höga

behörigheter ges till användare. En orsak kan vara att de givna rollerna inte passar exakt de behov en användare har. En lösning kan då bli att användare tilldelas en högre roll än avsett. Användarens behov blir tillgodosett, men i gengäld får användaren fler rättigheter än nödvändigt. En annan orsak kan vara slentrian. Detta kan bero på att kunskapen om behörigheter inte är spridd samtidigt som insikten om säkerhetsproblem är låg.

Det finns flera problem med alltför stora behörigheter. Om många användare har stora behörigheter, så ökar risken att det finns någon som gör något potentiellt olämpligt eller otillåtet i systemet.

Omvänt så innebär det en risk för den enskilda individen. Om något otillåtet uppdagas i systemet, så kan felaktigt misstankar falla på en användare som faktiskt hade möjlighet att genomföra den olämpliga åtgärden.

För att kunna ha spårbarhet i ett system, dvs. att i efterhand kunna fastställa vem som har gjort vad, så är det väsentligt att varje användare är knuten till en egen identitet (ett konto) i systemet. Detta är också avsikten i Paraplysystemet.

6.3.1 Iakttagelser och bedömningar

7. Höga behörigheter.

Vid granskningen har vi funnit att det vid olika förvaltningar förekommer att användare har högre behörighet än avsett. Bromma har 36 personer med rollen ”Verksamhetschef” och 34 med rollen ”Sektionschef”, och Hägersten-Liljeholmen har 28 personer med rollen ”Verksamhetschef” och 29 ”Sektionschef”. En stickprovskontroll av ytterligare en stadsdelsförvaltning utöver de som ingick i granskningen, visade att det inom denna förvaltning fanns 37 användare med rollen ”Verksamhetschef”. Totalt inom staden finns 636 personer som har antingen rollen ”Verksamhetschef” eller ”Sektionschef”. Detta antal är väsentligt högre än det antal personer som har dessa funktioner. Sammanlagt har dessa personer cirka 1700 roller. Tilldelning av roller med alltför höga behörigheter till ett stort antal personer ökar risken för missbruk.

Till dessa roller hör höga behörigheter i systemet. I ovan nämnda roller ingår per automatik rollen som ”Behörighetsadministratör”, vilket bland annat ger rätt att återställa lösenord och aktivera inaktiva konton. I staden finns således ett stort antal personer som kan hantera och få tillgång till andra personers inloggningsinformation.

Vi har även noterat att rensningar av konton och behörigheter inte genomförs på ett önskvärt sätt.

Tidigare revisioner har funnit brister i hanteringen av behörigheter, framför allt felaktig tilldelning av höga behörigheter[8]. Dessa påpekanden har inte åtgärdats fullt ut.

[8] Se referens [17, 18].

8. Delade konton hos externa aktörer.

Vid granskningen har vi fått indikationer att externa utförare hanterar rensning av oanvända identiteter (konton) på ett bra sätt, på grund av en prismodell där varje konto har en kostnad.

Prismodellen medför dock att konton delas mellan flera individer. Detta medför att spårbarheten försvinner. Det blir svårt att i efterhand utreda vem som gjort vad, om något oönskat har inträffat.

9. Tilldelning av roller styrs av regelverk, inte systemet.

Tilldelning av roller och därmed behörigheter styrs av regelverk. Regelverken anger vem som ska godkänna vad, och kräver bland annat dokument med underskrift av högre chef. Dessa dokument ska lagras, och i efterhand ska det vara möjligt att på så sätt spåra om rätt beslut har tagits.

Systemet har dock inga tekniska spärrar, som motsvarar regelverket, som förhindrar felaktig rolltilldelning. Enskilda individer har möjlighet att kringgå regelverket. Detta beskrivs mer i avsnitt 6.5 ”Intrångsmöjlighet”.

6.3.2 Rekommendation

Vi rekommenderar att systematiska, heltäckande genomgångar görs av samtliga innehavare av roller med högre behörighet, såsom ”lokal administratör”, ”enhetschef”, ”verksamhetschef” och ”sektionschef”, med syfte att identifiera användare som har felaktig rolltilldelning. En sådan genomgång behöver göras per förvaltning, under ledning av lokalt verksamhetsansvariga. Dessa genomgångar ska sedan genomföras regelbundet, exempelvis varje halvår eller år.

Vi rekommenderar att rutinerna och instruktionerna för rolltilldelning förbättras och efterlevnaden kontrolleras.

Vi rekommenderar att rollstrukturen granskas, för att säkerställa att de befintliga rollerna motsvarar verksamhetens krav.

Vi rekommenderar vidare att en granskning av hanteringen av identiteter (konton) görs hos externa utförare.

6.4 Åtkomstkontroll

När en användare vill ha åtkomst till ett IT-system görs normalt en kontroll av användarens identitet, för att säkerställa att endast behöriga användare kommer åt systemet. Denna autentisering av användaren kan göras på olika sätt och med olika säkerhet. Vanligt förekommande är autentisering med lösenord. Säkerheten styrs av lösenordets längd och komplexitet. En säkrare autentisering erhålls vid användning av digitala certifikat, elektronisk legitimation.

6.4.1 Iakttagelser och bedömningar

10. Inloggning utan kort är möjlig.

Stockholm stad har infört autentisering med digitala certifikat, ”Volvo-kort”, vid inloggning på klientdatorer. Detta är positivt, och medför både en ökad säkerhet att rätt person loggar in samtidigt som det är en enkel och praktisk inloggning för användare.

Vi har noterat att för många användare är det fortfarande möjligt att logga in enbart med tillgång till användarnamn och lösenord. Detta eliminerar den säkerhetshöjning som kort-användningen avser att ge. Inom staden pågår ett projekt med syfte att kunna ta bort möjligheten att logga in utan kort, OTIS (Obligatorisk TjänstekortsInloggning Stockholm stad).

11. Inloggning på Paraplysystemet med annans identitet är möjlig.

Inloggning på Paraplysystemet sker i tre steg. Först ska användaren logga in på sin dator, vilket normalt ska ske med kort innehållande ett certifikat. I steg två loggar användaren in i ett Citrix-system, som hanterar kontakten med bland annat Paraplysystemet. I steg tre loggar användaren slutligen in på Paraplysystemet. Steg två och tre sker med hjälp av användarnamn och lösenord.

Vid steg tre i förfarandet, inloggning på Paraplysystemet, kan någon annans användarnamn och lösenord användas. Paraplysystemet kräver således inte för denna inloggning att det är samma användarnamn som användes i steg ett och två. Detta öppnar för möjligheten för en användare att missbruka systemet genom att ta besittning av en annans persons inloggningsuppgifter. Konsekvenser av detta beskrivs i avsnitt 6.5, ”Intrångsmöjlighet”.

6.4.2 Rekommendation

Vi rekommenderar att dessa säkerhetsbrister åtgärdas på så sätt att inloggning med hårda certifikat, kort, blir obligatoriskt för alla. Vi rekommenderar också att åtgärder vidtas så att inloggning på Paraplysystemet inte kan göras med annans identitet, utan att detta uppmärksammas.

6.5 Intrångsmöjlighet

Ett system som hanterar eller styr stora ekonomiska belopp är utsatt för risken att en anställd eller en utomstående person missbrukar systemet. Risken ökar ju fler personer som har möjlighet till detta. System som hanterar känslig och potentiellt stöldbegärlig information är utsatt för risk för intrång. Se avsnitt 6.1, ”Informationssäkerhet”.

6.5.1 Iakttagelser och bedömningar

12. Möjlighet för intrång.

Vi har noterat att det inte kan uteslutas att ett stort antal personer[9] på ett enkelt sätt kan utföra olämpliga, otillåtna eller olagliga handlingar i systemet. Vi har noterat att sådana intrång inte behöver lämna tydliga spår. Sådana intrång kan utnyttja en kombination av de sårbarheter som nämns ovan, sårbarheter som var för sig inte har allvarligare följder. Konsekvensen av ett sammantaget agerande kan dock bli allvarligt. Det kan föra med sig såväl otillåtna utbetalningar som åtkomst till känslig personinformation.

Vid granskningen har identifierats ett antal tänkbara, enkla, tillvägagångsätt för otillåten åtkomst av information eller styrning av ekonomiska transaktioner. Tillvägagångssätten har inte provats i praktiken. Granskningen har dock inte visat några skyddsåtgärder som förhindrar dem.

6.5.2 Rekommendation

Vi rekommenderar att risken för intrång utreds noggrant.

Vi rekommenderar att de säkerhetsbrister som påtalas i avsnitt 6.3, ”Behörighetshantering” och 6.4 ”Åtkomstkontroll” åtgärdas.

Vi rekommenderar också att staden överväger att granska de loggar och den övervakning som finns spridd på flera platser, för att se om det finns spår efter redan utförda handlingar av ovan nämnt slag.

6.6 Riskhantering

Resultatet av en riskanalys används för att finna och prioritera skyddsåtgärder.

Riskhantering innebär ett systematiskt arbete med hot, sårbarheter och riskanalyser. Analys av hotbilden mot ett IT-system är komplex, och omfattar både kända hot såsom virus och DOS[10]-attacker liksom svåridentifierade hot såsom brist på utvecklare med specifik kompetens eller användning av nyutvecklad teknik för angrepp. Hotbilden ändras kontinuerligt när systemets omvärld ändras.

Sårbarheter kan finnas i ett system utan att vara kända av en tänkbar angripare, och kan komma att utgöra hot först när kunskapen om dem sprids. Nya sårbarheter i ett system kan uppstå när systemet vidareutvecklas. En riskanalys ger inte nödvändigtvis samma resultat vid olika tillfällen. En riskanalys för viktiga eller känsliga system bör därför genomföras regelbundet.

[9] Se avsnitt 7, ”Höga behörigheter.”
[10] DOS: Denial of Service, en attack där ett system överbelastas och därigenom slutar att fungera. Attacken är enkel att genomföra och är relativt vanlig.

6.6.1 Iakttagelser och bedömningar

13. Riskhantering på central nivå.

Vi har noterat att på en central nivå inom staden sköts riskhantering väl. Staden har en central säkerhetsorganisation, det finns en etablerad metod för riskanalys[11] vilken också följs.

14. Otydlig riskhantering.

Vid granskningen av Paraplysystemet har vi fått uppgift om att riskanalyser genomförs av ny funktionalitet.

Vi har däremot inte funnit att någon riskanalys genomförts för hela systemet. Vi har inte heller funnit någon genomförd analys av hotbilden mot systemet. Vi har inte funnit någon rutin eller process för regelbunden återkommande riskanalys.

Vi har inte heller funnit någon genomförd riskanalys avseende systemets framtid, vidareutveckling eller teknikuppbyggnad.

6.6.2 Rekommendation

Vi rekommenderar att en rutin införs för hot- och riskanalys för Paraplysystemet, samt att dessa genomförs regelbundet. Riskanalysen bör relateras till skyddsvärdet på den information som systemet hanterar.

Vi rekommenderar också att en riskanalys genomförs avseende systemets framtida fortlevnad.

6.7 Incident- och avvikelsehantering

Väl definierade rutiner för hantering av avvikelser och incidenter innefattar såväl den omedelbara hanteringen när något har inträffat som uppföljning efteråt för att dra lärdomar och genomföra långsiktiga motåtgärder. Till det förra hör både driftsrutiner hos driftsleverantören och kontinuitetsplaner i verksamheten. Den senare uppföljningen sker med fördel i samband med förvaltningsmöten.

Det är väsentligt att definiera kriterier för vad som ska bedömas som avvikelse, incident respektive allvarlig incident eller katastrof. Detta behövs för att tydliggöra för berörd personal när och hur de ska agera vid olika händelser.

Om och när allvarligare incidenter och katastrofer inträffar kommer i förväg framtagna kontinuitetsplaner att underlätta hanteringen av situationen. En viktig del av dessa är kriterier för när ärenden ska eskaleras till en högre nivå för åtgärd.

[11] Se referens [9].

Staden och leverantören har stående punkter på agendan på förvaltningsmöten för sociala system, ”Statusrapport drift” för Schemos, Vodok, ParaGå och Paraplysystemet.

6.7.1 Iakttagelser och bedömningar

15. Bristande uppföljning av avvikelser och incidenter

För sociala system har vi noterat brister i uppföljningen av avvikelser och incidenter. Vid stickprov av förvaltningsprotokoll och avvikelserapporter har vi funnit att inträffade avvikelser inte rapporteras och hanteras på förvaltningsmöten[12].

16. Lokala kontinuitetsplaner bristfälliga.

Varje förvaltning har ansvar för att ta fram lokala kontinuitetsplaner. Avsikten är att dessa planer ska beskriva vad som ska göras om och när de sociala systemen är otillgängliga[13]. Vid stickprovsgranskning har vi funnit att dessa planer inte alltid finns framtagna.

6.7.2 Rekommendation

Vi rekommenderar att rutiner för uppföljning av avvikelser och incidenter för Paraplysystemet tydliggörs.

Vi rekommenderar att förvaltningsorganisationen säkerställer att dessa rutiner följs och dokumenteras på förvaltningsmöten.

6.8 Ändamålsenlighet

Vid tidigare revision av Paraplysystemet har detaljerade synpunkter på dess användbarhet redovisats, se referens [14].

6.8.1 Iakttagelser och bedömningar

17. Varierande synpunkter på användbarhet.

Vi har vid stickprov noterat att många synpunkter på användbarheten av systemet kvarstår. Samtidigt har vi noterat att synpunkter och åsikter skiljer sig åt mellan olika användare. En åsikt är att systemet är bra att jobba med, för den som är väl förtrogen med verksamheten. En annan åsikt är att det är ett otympligt och trögt system.

[12] Förvaltningsmötet 2013-05-29 refererar till en avvikelse 2013-04-29 orsakad av inloggningsproblem hos Volvo IT. Andra avvikelser, inkluderande avbrottstid, har dock inträffat och rapporterats 2013-05-06, -07 och -08. Dessa tas inte upp vid något förvaltningsmöte, varken 2013-05-29 eller det nästkommande 2013-06-26.

[13] De ska exempelvis beskriva hur utbetalningar ska göras, om journaler och anteckningar ska föras med penna och papper och liknande.

18. Långsam inloggning.

En specifik notering är att inloggning till systemet är långsam, med variation över arbetsdagen. Detta faktum i sig kan vara orsak till ett generellt missnöje med systemets användbarhet.

6.9 Utvecklingsprocess och utvecklingsmiljö, säkerhet

Säkerheten för ett IT-system påverkas till en del av utvecklingsarbetet. Ett antal olika aktiviteter kan samverka för att höja säkerhetsnivån. Detta är speciellt viktigt för system som hanterar känslig information.

Granskning av design och programkod är en effektiv sådan åtgärd. Granskning kan genomföras av kollegor i utvecklingsgruppen, eller av utomstående part. Att utse en person i utvecklingsgruppen som ansvarig för säkerhet är ytterligare en åtgärd. Utbildning i säkerhetsfrågor är ännu en.

Utvecklingen beställs av staden och levereras av Tieto enligt fastställd kravspecifikation.

6.9.1 Iakttagelser och bedömningar

19. Bra utvecklingsmiljöer

    Ett flertal utvecklingsmiljöer används för olika faser och behov under utvecklingsprocessen. Dessa är kontrollerade med säkerhetsklassning och det data som används är i de flesta fall rensat från känslig information. I de fall då känslig information finns hanteras denna enligt de krav staden ställer på Tieto.

20. Bristande säkerhetsfokus vid utveckling

    Vi har noterat att kodgranskning eller annan säkerhetsgranskning av utvecklad kod saknas. Det som utförs är funktionell granskning av programkod och programfunktioner. Den testning som görs kring säkerhet sträcker sig till granskning av åtkomst och tar således inte upp andra aspekter av säkerhet.

    Vi har vid granskningen inte funnit att Leverantören använder en utvecklingsmodell där säkerhet hanteras på ett väldefinierat sätt.

21. Bristande hantering av risker och sårbarheter

    Den riskhantering och sårbarhetshantering som utförs är begränsad till riskhantering vid införande av ny funktionalitet och sårbarhetsanalys inom ramen för funktionell testning och integrationstestning. De upptäckta sårbarheterna prioriteras av Stockholm Stad.

    Ingen övergripande riskanalys är utförd för Paraplysystemets programkod. Den riskanalys som görs utförs vid införande av ny funktionalitet och är baserad på funktionella tester, integrationstester och åtkomstkontroll.

22. Åtkomst till programkod
    Programkoden skyddas i två olika verktyg vilka båda är behörighetsstyrda. Dock kan en programmerare arbeta via VPN-förbindelse från annan plats än Tietos lokaler.

6.9.2 Rekommendation

Vi rekommenderar att staden och Leverantören gemensamt tar fram riktlinjer för säkerhetsarbetet vid utveckling. Dessa bör innefatta utveckling, åtkomst och sårbarhetshantering.

6.10 Loggar

Loggning är att spara data om vilka händelser som ägt rum i en IT-miljö, vad som gjorts och vem som gjort dem. Spårbarhet är att genom loggning kunna identifiera och följa förloppet för olika händelser. Detta är nödvändigt för att kunna finna orsaker till problem eller den ansvarige vid säkerhetsrelaterade incidenter.

För Paraplysystemet sker loggning i flera nivåer. ParaInn lagrar egna loggar om användaraktivitet, Paraplysystemet lagrar felloggar, integrationssystemet lagrar integrationsloggar och åtkomstloggar för infrastruktur loggas.

6.10.1 Iakttagelser och bedömningar

23. Skydd av loggar

    Loggar lagras lokalt på de servrar där de skapas. I en del fall komprimeras de och lagras långsiktigt och i andra fall skrivs de över efter en viss tid. Någon kontrollerad central hantering och lagring av loggar sker inte. Den centrala hanteringen av loggar som finns sker som en bieffekt av backuptagning.

    Ingen ansvarsseparering finns mellan personal som hanterar loggar och personal som sköter drift av systemen som loggas hos Tieto. Det är samma personal i båda fall. Det finns därmed en möjlighet för en person att radera loggar över egna åtgärder.

24. Granskning av loggar

    Loggar granskas vid behov samt i samband med releaser. Ingen annan regelbunden granskning av loggar har noterats.

25. Innehåll i loggar

    De loggar som finns innehåller relevant information som exempelvis användare, tidpunkt och händelse.

6.10.2 Rekommendation

Vi rekommenderar att regelbunden granskning av loggar samt central lagring och hantering av loggar införs.

6.11 Infrastruktur

IT-infrastrukturen är grunden för säkerheten och ändamålsenligheten i ett system. Utan sund infrastruktur som är designad med både säkerhet och ändamålsenlighet i fokus blir det svårt att i efterhand skydda ett system och säkerställa god ändamålsenlighet.

Till infrastruktur räknas alla typer av hårdvara, nätverksutrustning samt även de virtuella miljöer som används i en modern IT-miljö.

6.11.1 Iakttagelser och bedömningar

26. Skalskydd

    Paraplysystemets yttre skydd består av brandväggar. Brandväggarna hanteras via särskilt utsedd och utbildad personal. Alla ändringar i brandväggarna sker enligt fastställd rutin där Stockholm Stad har del i ändringsbesluten.

27. Applikationsdistribution

    Paraplysystemet används via ett centralt system för applikationsdistribution. Detta innebär att systemet installeras och konfigureras på en central plats och därifrån skickas till brukarnas arbetsplatser när det ska användas. Någon installation av programvara hos användare behövs därmed inte. I den centrala platsen där systemet är installerat spåras användningen, men enbart i vissa fall.

    Paraplysystemet distribueras via en produkt för applikationsdistribution[14]. Denna applikation både lagrar information om sessioner och krypterar kommunikationen.

28. Interna skydd

    Internt är infrastrukturen uppbyggt som ett platt nätverk[15] där samtliga applikationer och system kan nå varandra. Det finns ingen separering mellan applikation och databas, vilket är brukligt. Inte heller finns kryptering av trafik mellan applikation och databas.

[14] Den produkt som används är Citrix, en välkänd och ofta använd produkt.
[15] Ett platt nätverk innebär att inga avgränsningar finns mellan de olika applikationerna och systemen.

29. Sårbarhetstester

    Sårbarhetstester genomförs i form av penetrationstester för de externt exponerade servrar som används gemensamt av staden. Inga andra övergripande sårbarhetstester har kunnat iakttas.

6.11.2 Rekommendation

Vi rekommenderar att staden och Tieto utföra en riskanalys för att klargöra om dagens skydd bestående av skalskydd och applikationsdistribution är starkt nog med tanke på informationen som skyddas. Dagens skydd hos Tieto bör dessutom granskas för att avgöra om det uppfyller de av staden ställda kraven.

Vi rekommenderar att en inre separering av databaser och applikationer samt återkommande sårbarhetstester, antingen automatiska eller manuella, införs.

Vi rekommenderar att kryptering av trafik innanför skalskyddet införs i syfte att minska risken för exponering av känslig information.

6.12 Gränssnitt mot andra system

Ett modernt system samlar information från olika källor och levererar oftast information till olika mottagare. Paraplysystemet kommunicerar med andra system hos staden, exempelvis ekonomisystemet Agresso. Paraplysystemet kommunicerar även med system utanför stadens kontroll, exempelvis Försäkringskassans system.

6.12.1 Iakttagelser och bedömningar

30. Integrationsmotor

    Integration sker idag genom TEIS (Tieto Enterprise Integration Server) vilken är en produkt utvecklad av Tieto som också sköter driften av den. Denna produkt är delad mellan olika kunder. Vi har inte noterat att detta leder till att information från Paraplysystemet exponeras mot andra kunder.

6.12.2 Rekommendation

Granskningen har inte gett upphov till någon rekommendation om förändring.

6.13 Systemets framtid

Paraplysystemet utvecklades med start 1995 och överlämning till förvaltning hösten 1999. Drift och förvaltning sköttes av WM-data fram till 2001-02-05 då denna övertogs av TietoEnator.

Under perioden efter 1999 har mycket ny funktionalitet tillkommit, och befintliga funktionalitet utvecklats.

Utvecklingen planeras och styrs vid förvaltningsmöten mellan staden och Leverantören. Vid dessa sammanställs innehåll i de releaser som görs två gånger årligen. Vid dessa planeras och rapporteras också de utvecklingsprojekt och –aktiviteter som bedrivs av Leverantören.

Inför projektstarten 1995 beslöts att utgående från standardprodukter utveckla ett eget system, då inga då befintliga standardprodukter uppfyllde ställda krav. Efter anbudsförfarande där projektgruppen tittade på de standardsystem som fanns på marknaden beslutades att utveckla ett eget system utifrån de standardprodukter som Cambridge Technology Partners (CTP) hade att erbjuda. Med anledning av detta började staden tillsammans med CTP bygga de första delarna av Paraplysystemet.[16]

PowerBuilder valdes som utvecklingsmiljö. PowerBuilder är ett utvecklingsverktyg och – språk som utvecklades 1991. PowerBuilder hade sin största användning omkring 1998, men har sedan fått ökad konkurrens från både Java-miljöer och Visual Studio (.NET). Kritik har riktats mot PowerBuilder för bristande skalbarhet[17].

Med version 12 av PowerBuilder, som lanserades 2010, avser man att närma sig .NET-miljön och underlätta integration med .NET- applikationer.

Tillgången på kunniga PowerBuilder-utvecklare är idag en trång sektor.

6.13.1 lakttagelser och bedömningar

31. Systemet är inte skrivet i något av de idag vanligaste språken.

Vi har noterat att Paraplysystemet är utvecklat i en miljö och språk som var mer använt när projektet startades än det är idag. Vi har noterat att en förstudie är startad avseende möjlig konvertering till .NET, vilket är en idag ofta använd miljö.

32. Gammalt system, ”lapptäcke”.

Vid granskningen har vi noterat att systemet upplevs som ett lapptäcke, efter många omgångar med tillägg och ändringar.

33. Ingen riskanalys gjord, ingen långsiktig plan.

Vid granskningen har vi inte kunnat återfinna att någon riskanalys genomförts avseende systemets teknikval, uppbyggnad eller framtida kostnader.

Vi har inte heller kunnat finna en strategisk plan för systemets framtid och dess utveckling.

[16] Se referens [8].
[17] God skalbarhet innebär att det är enkelt att t.ex. öka antalet användare av ett system.

6.13.2 Rekommendation

Vi rekommenderar att en förstudie genomförs avseende de sociala systemens framtid, speciellt Paraplysystemets. Denna förstudie skall baseras dels på riskanalyser avseende hot mot systemets informationsinnehåll, se avsnitt 6.1, dels på riskanalyser avseende systemets teknikval, arkitektur och kostnader.

Förstudien bör omfatta utredning av olika alternativa lösningar, inklusive vidareutveckling av befintligt system, konvertering till modernare miljö (t.ex. .NET), nyutveckling samt möjlighet att utnyttja andra standardsystem. Förstudien bör även omfatta hantering av risker. Kostnader för alla förslag bör vägas in.

Förstudien bör resultera i ett strategiförslag och en långsiktig plan för systemens framtid.

7 Slutsatser och sammanfattning

7.1 Svar på revisionsfrågorna

Granskningen ska besvara de ställda revisionsfrågorna. De slutsatser som kan dras från den genomförda granskningen är:

Paraplysystemets säkerhets och ändamålsenlighet.

Granskningen har påvisat brister beträffande säkerheten för systemet och dess information. Detta gäller såväl sekretessen av känslig information, riktigheten av ekonomiska transaktioner samt hanteringen av tillgängligheten av systemet.

Granskningen har inte visat några ytterligare väsentliga noteringar om ändamålsenligheten än de som tidigare granskningar visat.

Är roller och ansvar tydliga vad gäller systemägare, systemförvaltning, informationsansvar och drift?
Roller och ansvar är väldefinierade och följer en väldefinierad förvaltningsmodell. Behörighetsroller för användare följer inte fastställda regler och rutiner.

Hur säkras att informationen i systemet är tillförlitlig?
Hanteringen av systemets information hos driftsleverantören följer fastställda rutiner. Granskningen har inte kunnat utesluta att tillförlitligheten hos informationen kan påverkas negativt av relativt enkelt utförda intrång.

Är systemet ändamålsenligt och effektivt, exempelvis vad gäller användarvänlighet, funktion, rätt information?
Granskningen har inte visat några väsentliga noteringar om användarvänlighet utöver de som tidigare granskningar visat.

Hur säkras att systemet har en god tillgänglighet (driftstopp, informationsförlust, m.m.)?
Granskningen har påvisat bristande uppföljning av tillgänglighet och incidenter.

Är informationen skyddad för obehörig åtkomst?
Granskningen har inte kunnat utesluta att obehöriga relativt enkelt kan få åtkomst till information utan risk för upptäckt.

Finns en riskbedömning och planering (kostnader, säkerhet och funktionalitet) som underlag för ställningstagande vad gäller systemets framtida utveckling?
Granskningen har inte kunnat finna någon planering för systemets framtid och dess utveckling. Inte heller har granskningen funnit att någon riskanalys har genomförts. Systemet har utvecklats under ett större antal år, och är inte utvecklat med dagens teknik.

Finns rutiner för att garantera säkerheten i Paraplysystemets gränssnitt gentemot andra system?
Granskningen har inte visat på några avvikelser i säkerheten för gränssnitt mot andra system, och hanteringen av kommunikation med dessa.

7.2 Sammanfattning av iakttagelser och bedömningar

Granskningen har resulterat i trettiotre olika iakttagelser och bedömningar.

De viktigaste iakttagelserna kan sammanfattas i fem punkter:

1. Det kan inte uteslutas att många enskilda användare enkelt kan utföra olämpliga åtgärder i systemet, även av ekonomisk karaktär[18]. Kombinationen av flera sårbarheter kan medföra att detta går att utföra relativt enkelt och med liten risk för upptäckt. Brister i behörighetshantering inklusive rollhantering är en viktig orsak till detta[19].
2. En långsiktig plan avseende systemets framtid saknas[20]. Denna bör baseras på riskanalyser, och omfatta teknikval, arkitektur och kostnader.
3. Uppföljningen av servicenivåer, SLA, bör förbättras[21]. Uppföljningen av incidenter bör förbättras[22].
4. Riskhantering och riskanalyser bör förbättras[23].
5. Brister i säkerhetsmedvetande[24] och säkerhetsarbete.

[18] Se iakttagelse 12.
[19] Se iakttagelse 7, 9, 11.
[20] Se iakttagelse 33.
[21] Se iakttagelse 6.
[22] Se iakttagelse 15.
[23] Se iakttagelse 14.
[24] Se iakttagelse 1.

Bilaga 1, Intervjuade personer

Nedanstående personer har intervjuats:

1. IT-direktör, Stadsledningskontoret
2. Förvaltningssamordnare sociala system, Stadsledningskontoret
3. Informationssäkerhetschef, Stadsledningskontoret
4. IT-strateg, Stadsledningskontoret
5. IT-strateg, Stadsledningskontoret
6. Paraplysamordnare, Bromma
7. IT-samordnare, Bromma
8. Paraplysamordnare, Hägersten-Liljeholmen
9. IT-samordnare, Hägersten-Liljeholmen
10. Paraplysamordnare, Socialförvaltningen
11. Avdelningschef, Äldreförvaltningen
12. Strateg, Äldreförvaltningen
13. Strateg, Äldreförvaltningen
14. Affärschef, Tieto
15. Förvaltningsledare, Tieto
16. Projektportföljsledare, Tieto
17. Drift- och nätansvarig, Tieto

Bilaga 2, Granskade dokument

Följande dokument har ingått i granskningen eller utgjort underlag till den, och refereras till i texten:

1. ”Riktlinje Informationssäkerhet”, 2009-12-02, Dnr 307-2537/2009
2. ”Riktlinje säkerhetsskydd Stockholms stad”, 2013-02-25, Dnr 307-411/2013
3. ”Major Incidenthantering SLK IT”, 2013-06-07
4. ”Trygghets- och säkerhetsprogram för Stockholms stad 2013-2016”, april 2013
5. ”Stockholms stads IT-program 2013-2018”, 2013-04-29
6. ”Handbok Informationsklassificering”, 2008-03-18
7. ”Förvaltningsguide Fguide för Stockholms stad”, ver 2.0, 2006-10-06, Dnr 031/4117-2006
8. ”Övergripande beskrivning av Paraplysystemet”, ver 8.0, 2011-01-31
9. ”Riktlinje, Modell för Stockholms stads risk- och sårbarhetsanalys”, 2009-12-01
10. ”Rutiner vid avstämning, Ekonomiskt bistånd/Introduktionsersättning, Paraplysystemet”, november 2007
11. ”Lathund för lokal administratör, Paraplysystemet ParaInn”, januari 2011
12. ”Lathund för Behörighetsadministratör, Paraplysystemet ParaInn”, mars 2011
13. ”IT-säkerheten i Paraplysystemet”, mars 2001, Dnr 420/40-01
14. ”Användarnas syn på Paraplysystemet”, 2003-12-16, Dnr 420/153-03
15. ”Informationssäkerhetsgranskning av paraplysystemets applikation ParaSoL”, 2008-09-18, Dnr 420-117/08
16. ”Hantering av skyddade personuppgifter inom stadens individ- och familjeomsorg”, januari 2009, Dnr 420-01-2009
17. ”Granskning av Paraplybehörigheter vid tre stadsdelsnämnder”, 2012-09-13
18. ”Behörighetsadministration avseende externa utförares åtkomst till Paraplysystemet”, 2013-10-17
19. ”Revisionsplan 2013”, 2013-02-19, Dnr 301-62/2013
20. ”Stadsövergripande policy om skyddade personupp-gifter med riktlinjer till nämnder och bolag”, 2010-01-27
21. ”Systemförvaltning, Övergripande arbetssätt Paraplysystemet”, PM Samuel Rhodiner
22. ”Ramavtal, Helhetsåtagande avseende tjänster inom IT, telefoni och servicecentrum”, med bilagor, 2005-12-02, förlängt 2010-06-02, Dnr 033-4654/2005
23. ”Avropsavtal Systemförvaltning Paraplysystemet 2013” från 2012-11-22, Dnr 033-1688/2012
24. ”Avtal leverans av systemdrift och systemförvaltning av centrala system”, med bilagor, 2013-01-03, Dnr 125-1552/2012