Hägersten-Liljeholmens stadsdelsförvaltning
Administrativa avdelningen

Handläggare
Gunnela Börjes
Telefon: 08-508 22 052

Till
Hägersten-Liljeholmens stadsdelsnämnd
2014-04-10

Paraplysystemets säkerhet och ändamålsenlighet

Yttrande till revisorsgrupp 1

Förvaltningens förslag till beslut

Hägersten-Liljeholmens stadsdelsnämnd godkänner förvaltningens tjänsteutlåtande och översänder det som svar på remissen från revisorsgrupp 1.

Maria Mannerholm
stadsdelsdirektör

Lars Wennberg
avdelningschef

Sammanfattning

Revisionskontoret har genomfört en granskning av Paraplysystemets säkerhet och ändamålsenlighet. Granskningen har utförts med hjälp av konsult. Även tillgängligheten och organisationen av systemet har granskats samt systemets utveckling och fortlevnad.

Rapporten påpekar ett antal brister beträffande säkerheten i systemet samt i nämndernas behörighetshantering. Förvaltningen menar att rapporten innehåller ett flertal sakfel som sammantaget ger en missvisande bild. Detta medför att rapportens analys och förslag till åtgärder inte kan anses tillförlitliga. Säkerhetsmedvetandet på förvaltningen är högt. Behörighetshantering och behörighetskontroller fungerar utifrån de riktlinjer och anvisningar revisionskontoret och stadsledningskontoret fastställt.

Hägersten-Liljeholmens stadsdelsförvaltning
Administrativa avdelningen

Box 490
129 04 Hägersten
Telefon 08-508 22 000
www.hagersten-liljeholmen@stockholm.se

Ärendets beredning

Ärendet har beretts inom administrativa avdelningen. Ärendet behandlas i samverkansgrupp den 25 mars och i förvaltningsgrupp den 1 april 2014.

Ärendet

Revisionskontoret har genomfört en granskning avseende Paraplysystemets säkerhet och ändamålsenlighet. Granskningen har utförts med hjälp av konsult. Även tillgängligheten och organisationen kring systemet har granskats samt systemets utveckling och fortlevnad. Ett antal personer har intervjuats, däribland förvaltningens IT-samordnare och Paraplysamordnare.

Granskningen har resulterat i ett antal iakttagelser och rapporten framhåller de följande som viktigast:

- 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.
- En långsiktig plan för systemet saknas
- Uppföljning av incidenter och leverantörens servicenivåer har brister
- Brister i riskhantering och riskanalyser
- Brister i säkerhetsmedvetande och säkerhetsarbete

Detta remissvar inriktar sig på de synpunkter som framförts gentemot stadsdelsförvaltningarna.

Förvaltningens synpunkter och förslag

Säkerhetsmedvetande

Rapporten framhåller att säkerhetsmedvetandet vid såväl den centrala systemförvaltningen som de granskade förvaltningarna inte motsvarar den höga känsligheten hos informationen i systemet samt att säkerhetsorganisationen ej är känd.

Förvaltningen delar inte rapportens uppfattning i detta avseende. Vid intervjutillfället på Hägersten-Liljeholmens sdf redogjorde IT-samordnaren i detalj för informationssäkerhetsorganisationen . Förvaltningen har policies, riktlinjer och dokumentation som efterlevs väl. Det är dock viktigt att säkerhetsmedvetandet hålls aktuellt. Detta görs genom förvaltningens IT-samordnaren deltar i de centrala nätverksmöten som hålls av stadens IT-säkerhetschef

och sprider informationen på förvaltningen. Vid informationstillfällen och vid undervisning/introduktion av Paraplysystemet framhålls alltid känsligheten av de uppgifter som finns registrerade.

Behörighetshantering och -kontroll

Det lyfts fram att det förekommer att användare har högre behörighet än avsett.

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. Hägersten-Liljeholmen tas i rapporten upp som ett exempel på en förvaltning där anmärkningsvärt många (29 stycken) innehar rollen ”Sektionschef”. Av dessa 29 stycken är 20 stycken stadsdelens användare, varav alla förutom Paraplysamordnaren är chefer. Paraplysamordnaren innehar rollen för att kunna ge support till användarna. Återstående nio stycken är socialjourens arbetsledare vilka under icke kontorstid är chefer för det sociala arbetet i förvaltningen.

Konsulternas bedömning att det vid förvaltningar förekommer användare som har högre behörighet än avsett tar inte hänsyn till de verksamhetsmässiga behoven och konsekvenserna av dessa. 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. Behörighetsgenomgång och kontroll/rensning av behörigheter görs av paraplysamordnaren i stadsdelen i samarbete med sektionschefer. Detta görs halvårsvis utifrån de anvisningar revisionskontoret och central systemförvaltning skickat ut 2008.

Åtkomstkontroll och inloggning

Det uppges i rapporten 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.

Förvaltningen delar inte synpunkten att en person ”på ett enkelt sätt” kan utföra olagliga handlingar. För beslut och utbetalning av ekonomiskt bistånd finns dokumenterat vilka rutiner för utbetalning av ekonomiskt bistånd som ska följas och processen för detta beskrivs och följs av förvaltningen. 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. I hela denna kedja av aktiviteter finns en spårbarhet i systemet.

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. Konsulterna har dragit slutsatser om hur inloggning i Paraplysystemet går till och skulle kunna gå till som förvaltningen har svårt att följa. 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, oavsett om användaren har ett konto i arbetsplatssystemet eller inte. Har användaren endast ett konto men saknar roll kommer användaren inte vidare.

Om en person använder någon annans personnummer och lösenord (dvs. någon annans konto i paraplysystemet) kan detta, i likhet med de flesta system, enbart ske genom att användaren delat med sig informationen eller att man otillbörligt tillskansat sig informationen genom att i systemet ändra lösenordet på den användaren och sedan logga in. Det tillvägagångssättet loggas dock i systemet och är mycket lätt spårbart.

En behörighetsadministratör/chef har möjlighet att ändra en annan användares lösenord samt tilldela andra användare rollen ”avstämmare”. Om så sker åsidosätts redan här de rutiner som finns beskrivna - roll avstämmare ska godkännas av högre chef. Detta upptäcks dessutom tämligen omgående genom att användaren på det ”kapade” kontot inte kan logga in då lösenordet är okänt för honom/henne. Inloggning med annans identitet kan alltså inte göras utan att detta uppmärksammas.

I ett tänkt olovligt scenario registrerar chefen ett beslut om ekonomiskt bistånd, och loggar sedan in som den andre personen med roll avstämmare och stämmer av beslutet. För att begå denna olagliga (och i systemet spårbara) handling behövs att man handlar i samförstånd med en person boende i området att den personen ska uppbära ekonomiskt bistånd, alt. förfalskar en persons ansökan. Det

krävs också att man förfalskar de handlingar som krävs i en akt, hyreskontrakt, hyresavi, senaste beslut om slutlig skatt, kontoöversikt från bank, inkomstuppgifter för de tre senaste månaderna mm. Detta förfarande kräver en stor arbetsinsats och risken för upptäckt är stor. Förvaltningen delar inte bedömningen att detta är ett enkelt förfarande. För samtliga beslut om utbetalning av ekonomiskt bistånd skickas automatiskt ett brev till personen som får biståndet för att garantera att sökande får information om vilket belopp som utbetalts. Detta är ytterligare ett skydd för att olovliga utbetalningar inte sker.

En person kan ha flera roller i systemet om personens arbetsuppgifter är sådana att detta krävs. En vanlig kombination är till exempel att de som är avstämmare även är kravhandläggare och kassaförvaltare. Rapporten påpekar att ett flertal personer i staden har rollkombinationen sektionschef – avstämmare. Endast en användare/chef på förvaltningen har denna rollkombination som backup för oväntad frånvaro och har direktiv att använda detta enbart i akuta lägen. Denna användare har inte gjort några avstämningar 2013. Viktigt att påpeka är att en avstämmare aldrig kan stämma av beslut där han/hon uppgivits som beslutsfattare eller varit den som registrerat beslutet.

Sammanfattningsvis anser förvaltningen att de brister och slutsatser som rapporten framhåller rörande säkerhetsmedvetande och behörighetshantering härrör sig från felaktiga analyser och missuppfattningar. Behörighetshanteringen följer gällande riktlinjer och säkerhetsmedvetandet på förvaltningen är högt. Vi delar dock uppfattningen att det i enlighet med gällande anvisningar är av största vikt att regelbundet göra behörighetsgenomgångar och rensa inaktuella konton. Det är av också största vikt att kunskap om säkerheten och betydelsen av hantering känslig information förs vidare och hålls levande i förvaltningen.

Bilaga

Revisionskontorets rapport finns att läsa finns att läsa under sammanträdesdatum 10 april 2014 på www.insynsverige.se/stockholm.