PM 2008:227 RI (Dnr 033-2224/2008)

Informationssäkerhetsgranskning av Paraplysystemets applikation ParaSoL

Remiss från Stadsrevisionen, revisorsgrupp 1

Borgarrådsberedningen föreslår kommunstyrelsen besluta följande

Som svar på remissen Informationssäkerhetsgranskning av Paraplysystemets applikation ParaSoL överlämnas och åberopas denna promemoria.

Föredragande borgarrådet Sten Nordin anför följande.

Ärendet

Stadsrevisionen har genomfört en informationssäkerhetsgranskning av applikationen ParaSoL i Paraplysystemet. ParaSoL hanterar utförardokumentation inom äldreomsorg och inom omsorgen om funktionshindrade. I ParaSoL dokumenterar personal och enhetschefer som arbetar på de olika utförarenheterna inom hemtjänsten, vård- och omsorgsboenden, daglig verksamhet, dagverksamhet och servicehus. I rapporten framgår att ParaSoL uppfyller kraven på god spårbarhet, vilket innebär att det går att följa vad användarna gjort i systemet. I rapporten framgår vidare att stadsdelsnämndernas tilldelning av behörigheter sker enligt kommunfullmäktiges informationssäkerhetsregler. Det finns dock brister i rutinerna för uppföljning och avslut av behörigheter. Med anledning av den revision som utförts lämnas i denna promemoria förslag till åtgärder.

Beredning

Ärendet har beretts av stadsledningskontoret.

Mina synpunkter

Stadsrevisionen har genomfört en informationssäkerhetsgranskning av applikationen ParaSoL i Paraplysystemet. I rapporten framkommer att stadsdelsnämndernas rutiner för tilldelning av behörigheter sker i enlighet med kommunfullmäktiges policy. Det brister dock i rutinerna för behörighetsuppföljning och borttagning av användare. Jag instämmer i stadsledningskontorets förslag till åtgärder för att komma tillrätta med de brister som revisorerna pekat på. Det är viktigt att föreslagna åtgärder genomförs.

Jag föreslår att borgarrådsberedningen föreslår kommunstyrelsen besluta följande
Som svar på remissen Informationssäkerhetsgranskning av Paraplysystemets applikation ParaSoL överlämnas och åberopas denna promemoria.

Stockholm den 6 november 2008

STEN NORDIN

Bilaga

Revisionsrapport *Informationssäkerhetsgranskning av paraplysystemets applikation ParaSoL*

Borgarrådsberedningen tillstyrker föredragande borgarrådets förslag.

ÄRENDET

Stadsrevisionen har genomfört en informationssäkerhetsgranskning av applikationen ParaSoL i Paraplysystemet. ParaSoL hanterar utförardokumentation inom äldreomsorg och inom omsorgen om funktionshindrade. I ParaSoL dokumenterar personal och enhetschefer som arbetar på de olika utförarenheterna inom hemtjänsten, vård- och omsorgsboenden, daglig verksamhet, dagverksamhet och servicehus. I rapporten framgår att ParaSoL uppfyller kraven på god spårbarhet, vilket innebär att det går att följa vad användarna gjort i systemet. I rapporten framgår vidare att stadsdelsnämndernas tilldelning av behörigheter sker enligt kommunfullmäktiges informationssäkerhetsregler. Det finns dock brister i rutiner för uppföljning och avslut av behörigheter. Med anledning av den revision som utförts lämnas i denna promemoria förslag till åtgärder.

BEREDNING

Ärendet har beretts av stadsledningskontoret.

Stadsledningskontoret

Stadsledningskontorets tjänsteutlåtande daterat den 1 oktober 2008 har i huvudsak följande lydelse.

Stadsrevisionen har genomfört en informationssäkerhetsgranskning av applikationen ParaSoL i Paraplysystemet. ParaSoL hanterar utförardokumentation inom äldreomsorg och inom omsorgen om funktionshindrade. I ParaSoL dokumenterar personal och enhetschefer som arbetar på de olika utförarenheterna inom hemtjänsten, vård- och omsorgsboenden, daglig verksamhet, dagverksamhet och servicehus. I rapporten framgår att ParaSoL uppfyller kraven på god spårbarhet, vilket innebär att det går att följa vad användarna gjort i systemet. I rapporten framgår vidare att stadsdelsnämndernas tilldelning av behörigheter sker enligt kommunfullmäktiges informationssäkerhetsregler. Det finns dock brister i rutiner för uppföljning och avslut av behörigheter. De brister som framkommit och som bedöms som risker i Revisionsrapporten är numrerade 1 – 7. Förslag på åtgärder följer denna numrering.

Ärendets beredning

Ärendet har beretts av stadsledningskontorets IT-avdelning i samarbete med informationssäkerhetschefen vid administrativa avdelningen och finansavdelningen.

Stadsledningskontorets synpunkter och förslag

Stadsrevisionen har genomfört en informationssäkerhetsgranskning av applikationen ParaSoL i Paraplysystemet. I rapporten framkommer att stadsdelsnämndernas rutiner för tilldelning av behörigheter sker i enlighet med kommunfullmäktiges policy. Det brister dock i rutinerna för behörighetsuppföljning och borttag (inaktivering) av användare. Med anledning av den revision som utförts lämnas följande synpunkter och förslag till åtgärder.

1. Frekvens för byte av lösenord

Vi delar uppfattningen att frekvensen för lösenordsbyte är för hög. I nästa version av ”Stockholms stads policy och riktlinjer för informationssäkerhet” kommer detta att förändras.

2. Formell rutin för behörighetsadministration

Användarhandledning för behörighetsadministratörer i ParaInnAdmin finns upprättad sedan programmet skapades. Denna handledning beskriver hur en användare hanteras i programmet. Användarhandledningen kommer att kompletteras med information om vilka kontroller som skall göras i samband med upplägg av användare, ändring av utdelad behörighet,

borttag (inaktivering) av användare samt en rekommendation om hur granskning av användare skall gå till samt hur ofta den bör göras. Denna granskning bör göras två gånger per år.

Inom förvaltningsarbetet för Paraplysystemet pågår en utredning för en revision av ParaInn. En utveckling kommer att genomföras för att underlätta och öka säkerheten för användarhanteringen.

3. Upplåsning av konton

Användarhandledningen kommer att kompletteras med instruktioner om vilka kontroller som skall göras i samband med upplåsning av konton. För de som har åtkomst via e-post skall det nya tillfälliga lösenordet skickas med e-post. För de som inte har tillgång till e-post skall motfråga om användar-id och personnummer ställas.

4. Vodok-användare

I revisionsrapporten finns en riskbedömning att obehöriga användare kan ha fått tillgång till känslig information. Med anledning av detta vill vi förtydliga att de användare som vid detta tillfälle överfördes till ParaSoL var aktiva användare i VODOK och arbetade på de enheter som de blev överförda till. Anledningen till den automatiska konverteringen var att alla stadsdelar inte hunnit lägga in alla medarbetare både i VODOK och i ParaSoL. För att utvecklingsarbetet inte skulle stanna upp för att alla användare inte var inlagda fattades beslut om att en konvertering skulle göras. Risken var annars större att medarbetare, t ex sjuksköterskor, inte skulle få tillgång till sina journaler i VODOK. Behörighetsblanketter finns redan tillgängliga och har funnits sedan ParaInn utvecklades 2003. Behörighetsblanketterna uppdateras kontinuerligt då nya användargrupper tillkommer.

Information kommer att skickas ut till förvaltningarna med en instruktion om att de skall granska sina behörighetsrapporter och upprätta behörighetsblanketter för de användare som saknar sådana i ParaInn.

Vad gäller rekommendationen att informationen når berörda tjänstemän så följer förvaltningen av Paraplysystemet de befintliga kontaktvägarna för att informera som finns. Vid förändringar i systemet informeras förvaltningarna via sina kontaktpersoner. De bjuds in till möten samt informeras via mail för att sprida informationen till sina kollegor. När det rör förändringar i ParaInn informeras den personal som har en aktuell roll som administratör i systemet. I samband med VODOK-integratitionen bjöds c:a 60 lokala administratörer in till möten. Det erbjöds två tillfällen, fem personer kom till dessa två möten. Detta belyser svårigheten att nå ut med relevant information vid rätt tillfälle till dem som berörs, men också stadsdelsförvaltningarnas prioriteringar av denna typ av informationsmöten. Det är viktigt att vid varje informationstillfälle planera hur och på vilket sätt informationen skall ges för att den skall få önskvärt resultat.

5. Granskning av behörigheter

Denna del ingår som en del av punkt 2 och det skall av användarhandledningen framgå hur ofta och när granskning skall ske.

6. Rutiner/ansvar vid borttag av användare

Vi instämmer i de rekommendationer som revisionsrapporten ger. I samband med att användarhandledningen kompletteras kommer förvaltningarnas behörighetsadministratörer få hjälp att skapa bra rutiner.

7. Uppföljning av gjorda anteckningar

Denna punkt är en verksamhetsspecifik fråga varför vi inte tar ställning till detta.