Kommunrevisionen

2007-10-10

Kommunstyrelsen

För kännedom:
Kommunfullmäktige

Granskning av IT-säkerheten

På uppdrag at Lunds kommuns revisorer har Öhrlings PricewaterhouseCoopers genomfört en granskning avseende IT-säkerheten i Lunds kommun, se bifogad bilaga. Vid granskningen konstaterades att resultatet avseende flera av de kontroller som utförts är tillfredsställande.

I rapporten konstateras även brister och väsentliga förbättringsområden. Inom vissa områden t ex utarbetande av IT-handbok, roller, backuper, virus och spionprogram samt behörighetshantering pågår redan ett förbättringsarbete vilket är positivt. Samtidigt finns ett antal förbättringsområden som bör framhållas.

- Det är bristfälligt att det idag saknas systemsäkerhetsplaner för kommunens system. Kommunledningen bör utarbeta en plan och utse ansvarig för att säkerställa att arbetet med systemsäkerhetsplaner sker.

- Uppföljning och kontroll av IT-säkerheten inom kommunen sker inte på ett tillfredställande sätt. Det är här viktigt att kommunledningen via information och uppföljning försäkrar sig om att organisationen vet vilket ansvar den har för IT-säkerheten samt att policys och regler efterlevs.

- Vår bedömning är att rum för drift, backuptagning, reservkraft och anslutande utrustning inte är tillfredställande. Det är här viktigt att det görs en översyn och att kommunledningen säkerställer att det upprättas en dokumenterad bild avseende brister, risker och konsekvenser. Vi föreslår att möjligheter till en alternativ driftsmiljö för de mest kritiska systemen ses över. Detta för att minimera störningar vid större incidenter.

- Vi ser ett behov av att det genomförs utbildningsaktiviteter inom kommunen.

- Vi konstaterar att ansvariga ser ett behov att förbättra och se över skyddet mot åtkomst till databaser och servrar. Det är här viktigt att brister, risker och konsekvenser tydliggörs och att förbättringsåtgärder prioriteras.

- Analyser för att identifiera följderna av eventuella katastrofer bör genomföras i anslutning till detta är det viktigt att en avbrottsplan upprättas. Avbrottsplanen bör innehålla en beskrivning av vad som krävs för att starta driften på nytt, prioriteringar samt ansvaret för olika aktiviteter.

Postadress	Besöksadress	Telefon	Fax	e-post
Box 41 221 00 Lund	Stortorget 1	046 - 35 50 00 046 - 35 53 82 046 - 35 57 96	046-35 59 28	komrev@lund.se

2007-10-10

Utifrån vår granskning bedömer vi att det är viktigt att kommunledningen stärker greppet kring IT-säkerheten. Exempel på punkter som är viktiga att ha tydlig samsyn kring är följande:

- Tydliga målsättningar samt identifiering av risker och konsekvenser i de olika förbättringsprojekten.
- På vilket sätt bedrivs förbättringsarbetet och kan arbetet eventuellt bedrivas effektivare. (problem och hinder)?
- Vilka förbättringseffekter kommer arbetet att innebära?
- Vem ansvarar för att åtgärda olika frågor och när ska det vara klart?
- Vilka resurser krävs?

Svar över vidtagna åtgärder önskas före februari månads utgång 2008.

FÖR LUNDS KOMMUNS REVISORER

_____

Lars Larsson
Ordförande

Postadress Box 41 221 00 Lund
Besöksadress Stortorget 1
Telefon 046 - 35 50 00 046 - 35 53 82 046 - 35 57 96
Fax 046-35 59 28
e-post komrev@lund.se

Öhrlings

PRICEWATERHOUSECOOPERS

Revisionsrapport

Översiktlig granskning av IT-säkerheten

Lunds kommun

September 2007

Göran Persson Lingman

Öhrlings

PRICEWATERHOUSECOOPERS

Innehållsförteckning

1. Inledning

1.1 Bakgrund

Med begreppet IT menas informationsteknik som innefattar teknik för elektronisk framställning, lagring, överföring och presentation av information. Tekniken kan bestå av hårdvara, nät, kommunikation och programvaror av olika slag.

Med vår definition av IT-säkerhet menas här alla olika åtgärder som används för att skydda och säkerställa åtkomsten av information samt att interna och externa regelverk följs.

Betydelsen av IT ökar allt mer inom kommunens olika verksamhetsområden och förändringar sker kontinuerligt. Kommunen hanterar många känsliga uppgifter. Brister i säkerheten kan ge stora konsekvenser för såväl kommunen som för enskilda personer.

1.2 Syfte

Granskningen syftar till att översiktligt granska kommunens IT-säkerhet. I granskningen ingår bl a att kontrollera regler och stöddokument, generell behörighetshantering, rutiner för backuptagning samt driftsäkerhet.

Underlag från användarformulär kommer att delges ansvariga för ytterligare analys och eventuella förbättringsåtgärder.

1.3 Metod

Vi har

- intervjuat ansvariga tjänstemän vid IT-avdelningen samt IT-ansvariga vid förvaltningar
- gjort en genomgång av framtagna dokument
- ställt frågor till ett urval av användare via ett webbaserat frågeformulär (703 användare besvarade formuläret). Se grafik över svaren i bilaga 1
- gjort en fysisk besiktning av kommunens centrala datorrum

1.4 Avgränsning

Granskningen omfattar de i rapporten redovisade kontrollmålen.

Granskningen har inte berört säkerheten i separata system. Vi har alltså inte granskat att systemen loggar erforderliga händelser, att personer har olika behörigheter i systemens olika register (ändra, läsa m.m), d v s systemens egna kontrollfunktioner, ex uppdatering och ändring i leverantörsreskontra, kontroll av att obligatoriska fält är ifyllda korrekt.

2. Övergripande beskrivning av organisation och informations-/systemstruktur

IT-avdelningen inom Lunds kommun sköter i huvudsak all drift av kommunens system. Detta innebär att det i kommunens centrala serverrum hanteras viktig och känslig information såsom:

- information inom familjeomsorg, äldreomsorg, skola - och barnomsorg
- löne- och redovisningsinformation
- geografisk information
- kommunens hemsida
- befolkningsregister

Windows och Office körs i huvudsak på alla datorer inom administrationen. Lagring av egna upprättade dokument ska enligt anvisningar ske på centrala servrar (d v s olika dokument som användare arbetar med t ex ord och text, kalkyler och presentationer). Även kommunens intranet och mailsystem hanteras i centrala serverrum.

3. Granskningsresultat

3.1 Inledning

Nedan följer de olika kontrollmoment vi genomfört i samband med granskningen. Vi har ställt upp kontroller som ett antal frågeställningar. Därefter redovisas våra iakttagelser från granskningen, våra kommentarer, bedömningar och förslag till förbättringar. Iakttagelser kan vara både positiva och negativa.

Nedan visas frågeställningarna i granskningen. En sammanfattande bedömning ges i avsnitt 4.

- Finns det en aktuell och fastställd IT-säkerhetspolicy samt andra styrande riktlinjer inom kommunen?
- Finns det en tydlig ansvarsfördelning vad gäller IT-säkerhetsfrågorna inom kommunen?
- Har kommunen ett erforderligt skydd av IT-utrustningen för att förhindra skador, störningar, avbrott, obehörigt tillträde och stöld?
- Har kommunen tillfredsställande rutiner för säkerhetskopiering?
- Finns bra rutiner för rapportering av säkerhetsrelaterade händelser (incidenter)?
- Finns tillfredsställande skydd mot virus och spionprogram?
- Har användare kunskap om hot och risker för IT-säkerheten?
- Finns tillfredsställande rutiner för hantering av behörighet och lösen till gemensamt nätverk?
- Finns tillfredsställande rutiner för inköp och hantering av datorer som ej längre nyttjas?
- Finns anvisningar och/eller skydd mot att användare installerar program eller annat oönskat material till sin dator?
- Finns det en avbrottsplan för att säkerställa att funktioner kan återställas inom erforderlig tid?

3.2 Finns det en aktuell och fastställd IT-säkerhetspolicy samt andra styrande riktlinjer inom kommunen?

Iakttagelser:

Inom kommunen har dokumenten ”e-program” och ”e-handlingsplan” framtagits. Dokumenten är strategiska och åskådliggör hur kommunens mål ska stödjas av modern informationsteknik. Dokumenten har antagits av kommunstyrelsen. I dokumentet ”e-handlingsplan” finns bl a beskrivningar avseende ansvar, vilka IT-dokument som kommer att utarbetas och ansvaret för att implementera dessa i organisationen. I e-programmet finns ett avsnitt kring e-säkerhet som beskriver riktlinjer och anvisningar kring IT-säkerhet inom områdena

- Klassning av information
- Behörighetskontrollsystem
- Anslutning till kommunnätet
- Kommunikation/fjärråtkomst
- Kontinuitetsplanering

I e-handlingsplanen finns beskrivningar avseende projekt som syftar till att öka effektivitet, säkerhet och kommunens service till medborgare.

Andra övergripande dokument som berör IT-säkerhet finns inom kommunen. Här kan nämnas dokumentet anvisningar till användare ”Till datoranvändare inom Lunds kommun”. I dokumentet berörs

- vart man vänder sig i olika IT relaterade frågor, när ska man vända sig till IKT-samordnare, (**I**T och **K**ommunikations **T**eknik) och när ska man vända sig till centrala Servicedesk funktionen.
- hur man kommer in i kommunens nät
- information om medarbetarportalen där användare får kontinuerlig information om olika IT relaterade frågor.

Som stöd för IT-avdelningens arbete finns ett flertal process- och rutinbeskrivningar.

Det finns utkast till en IT-handbok som omnämns i e-programmet. Till delar används denna idag men det är inget formellt dokument som antagits av kommunledningen. Utkastet till IT-handboken innehåller

- Styrdokument
  - eProgram
  - eHandlingsplan
  - eOrganisation
- Systemstruktur(-arkitektur)
  - Arkitekturdokument/Integrationer/Meta
  - Informationssystem/-applikationer
- Anskaffning/Förvaltning/Drift/Dokumentation/Rutiner
- Informationssäkerhet/Säkerhet/Sårbarhet/Integritet/Behörighet
- Policydokument
- Teknik
  - Servrar/PC/Skrivare/Funktionsprogram

Vid vissa förvaltningar pågår ett arbete med att se över säkerheten kring systemen via arbete med systemsäkerhetsplaner (t ex via kartläggning av informationsklassificering, hot, risker och vad som krävs för att skydda sig). Detta är dock inget som idag genomförs på något systematiskt sätt inom kommunen.

I olika omfattning finns dokument upprättade vid förvaltningarna, t ex finns framtagna riktlinjer avseende IT-säkerhet för verksamhetssystem som t ex journalsystem och äldreomsorgssystem. Inom skolan finns riktlinjer för elever som de får underteckna innan de börjar använda datorerna.

Från verksamheten uttrycks ett behov av att arbetet med dokument kring IT-säkerhet slutförs för att man därefter skall kunna införa det som ska gälla i verksamheten.

Många användare har i enkäten uttryckt att det är otydligt vad som finns avseende säkerhetsrelaterade dokument.

Ett dokument ”IT-säkerhet” från 1999 finns inom kommunen. Dokumentet är antaget av kommunstyrelsen. Dokumentet anger roller och ansvar kring olika typer av IT-säkerhetsfrågor. T ex anges i dokumentet att det inom kommunen finns en utsedd IT-säkerhetsansvarig. Denna befattning saknas dock inom kommunen.

Dokumentet är enligt IT-avdelningens och andra ansvarigas uppfattning inte aktuellt och är bara delvis infört inom kommunen. Det finns ingen ambition hos ansvariga (t ex IT-chefen) att säkerställa införande och tillämpning av dokumentet eftersom dokumentet inte är aktuellt idag.

Kommentarer och rekommendationer:

- I eProgrammet finns ansatser till riktlinjer kring IT-säkerhet som är positiva men som behöver förtydligas i IT-handboken. I samband med att dokumenten förbättras är det givetvis även viktigt att ansvariga ser över hur olika dokument ska kommuniceras till ansvariga och användare samt att tillämpningen säkerställs. En utgångspunkt är att rätt information måste nå rätt målgrupp (användare, IKT-samordnare, chefer, systemägare m fl).

- Det arbete som pågår kring IT-handboken är positivt men det är givetvis viktigt att kommunledningen säkerställer att arbetet påskyndas och slutförs.

- Det är bristfälligt att det idag saknas systemsäkerhetsplaner för verksamhetskritiska system inom kommunen. Det är viktigt att kommunledningen utarbetar en plan och utser ansvarig för att säkerställa att arbetet med systemsäkerhetsplaner sker.

- Vi kan konstatera att det finns dokument som berör IT-säkerheten som är inaktuella och som inte används i praktiken. Här vill vi tillägga att vi upplevt att det är svårt att överskåda de dokument som finns inom kommunen och att det därmed finns risker att dokumenten inte fyller sitt syfte.

3.3 Finns det en tydlig ansvarsfördelning vad gäller IT-säkerhetsfrågorna inom kommunen?

Iakttagelser:

Kommunens IT-avdelning ansvarar för

- servrar/nät, datakommunikation, teknik/testverksamhet och telefoni.

- driften av kommunens gemensamma nätverk (data och tele), servrar och centrala verksamhetssystem (e-post, ärendehantering, brandvägg, Internetuppkoppling).

- felavhjälpning, användarstöd, underhåll och installation av både mjuk- och hårdvara (standardarbetsplats). Felanmälningar och beställningar sköts av kommunens servicedesk.

IT-avdelningen har erbjudit beredskap utanför normal kontorstid som verksamheten enligt uppgifter avböjt p g a ekonomiska skäl. En leveransöverenskommelse med verksamheten finns upprättad.

IT-avdelningen har sedan några år tillbaka påbörjat ett processorienterat arbetssätt som bygger på en väl genomtänkt struktur (ITIL). Arbetssättet ska stödja både effektivitet och säkerhet kring IT. Vissa delar (servicedesk, incidenthanteringsprocess och problemhanteringsprocess) är i huvudsak införda idag men kontinuerliga förbättringar pågår enligt uppgifter. Avseende andra delar kring ITIL återstår fortfarande en hel del arbete, t ex förbättrad förändringshantering.

IT-frågor (IT-säkerhetsfrågor) kommuniceras i e-styrgruppen. IT-chefen föredrar även IT-frågor i kommunens ledningsgrupp och i KS arbetsutskott.

Vid förvaltningarna finns IKT-samordnare som ska företräda verksamheten i IT-frågor.

Systemägare och systemförvaltare finns utsedda.

Det finns ingen uttalad ansvarig för IT-säkerhet i kommunen. Dokument som beskriver ansvar inom IT-säkerhet saknas. Systemsäkerhetsplaner som t ex tydliggör ansvar mellan systemägare och IT-avdelning saknas. IT-chefens uppfattning är att effektivitet och säkerhet bör vara integrerade vilket gör att ansvaret kring en god IT-säkerhet ligger på honom och verksamhetsansvariga. Enligt uppgifter från IT-chefen förväntar sig kommunledningen att uppföljningar av IT-verksamheten sker enligt riktlinjerna i eProgrammet kring säkerhet, utveckling och kvalité.

I Lunds kommun finns en förvaltningsmodell som följer Sveriges Kommuner och Landstings riktlinjer. Arbete pågår med en ny förvaltningsmodell som på ett bättre sätt integrerar verksamhetens processer med IT. Modellen kommer att beskriva och definiera olika roller och ansvar. Målsättningen är att denna modell ska tillämpas inom hela kommunen.

Några av de IKT-samordnare vi intervjuat uttrycker att det finns en otydlighet inom kommunen avseende roller och ansvar. Även användare har i enkäten uttryckt att det är otydligt.

Otydligheter har uppmärksammats från IT-avdelningen och ett förbättringsarbete har nyligen initierats.

Kommentarer och rekommendationer:

- Vår bedömning är att rollfördelningen avseende IT inom kommunen inte är tillräckligt tydliggjord. Vi kan dock konstatera att det har initierats ett förbättringsarbete.

- Det processorienterade arbetssätt som sker inom IT-avdelningen är positivt. Det är här viktigt att ytterligare processer implementeras, t ex förändringsprocessen. Givetvis är det viktigt att säkerställa att processer fungerar som avsetts via t ex uppföljning och olika mått.

- Vi bedömer att uppföljning och kontroll av IT-säkerheten inom kommunen inte sker på ett tillfredsställande sätt. Det är här viktigt att kommunledningen via information och uppföljning försäkrar sig om att organisationen (chefer, användare m fl) vet vilket ansvar de har för IT-säkerheten samt att policys och regler efterlevs. Vad vill kommunledningen har svar på och på vilket sätt ska rapporteringen ske.

- Vi vill även här peka på vikten av att verksamheterna utarbetar systemsäkerhetsplaner och att det givetvis därefter säkerställs att dessa efterlevs. Systemsäkerhetsplaner stödjer säkerheten samtidigt som ansvaret mellan verksamheten och IT-avdelningen tydliggörs.

3.4 Har kommunen ett erforderligt skydd av IT-utrustningen för att förhindra skador, störningar, avbrott, obehörigt tillträde och stöld?

Iakttagelser:

Ett flertal kontroller har genomförts, nedan anges sammanfattande iakttagelser.

Inom kommunen finns två centrala serverrum (ett rum för drift av kommunens system inklusive IP-telefoni och ett serverrum för backuptagning). Rummen är placerade i olika huskroppar. Ett separat rum finns för delar av reservkraft till serverhall för drift.

Rummen är till sin konstruktion inte anpassade för IT-drift dock är rummen inte placerade i en känslig miljö (t ex tung trafik i närheten, allmänhet som cirkulerar).

Idag finns det ett passagesystem med kort som loggar tillträde till serverrum för drift. Rummet för drift kan även öppnas med nyckel. Då nyckel används sker ej loggning. Loggning till rum för backuptagning saknas.

Rutin för tilldelning och ansvarig för behörighetstilldelning finns (vilka ska ha passerkort och nyckel). Endast driftspersonal har åtkomst till serverhallarna, och vem som har åtkomst finns registrerat i passagesystemet. Loggning sker ej rutinmässigt t ex genom att loggning inte sker då nyckel används.

Enligt uppgifter tillämpas rutinen kring behörighet till serverrum inte alltid önskvärt t ex då leverantörer ska ges tillträde till datorhallen. Ansvarig för serverhallen ser ett behov att se över rutiner för åtkomst eftersom tillämpning och/eller anvisningar inte är helt tydliga.

Serverhallarna saknar fönster. Det kablage som fanns i serverhallarna var vid vår inspektion otillfredsställande. Enligt ansvariga var detta ett undantag då arbete pågick i serverhallarna.

Tillfredsställande kylning finns men vid strömavbrott är lösningen otillräcklig. Strömstörningar är ej vanligt förekommande inom kommunen. Analys av strömförsörjningen har skett av ansvariga. Vid strömbortfall finns ej skydd i erforderlig tid.

I serverhallen för drift finns larm för vatten, kyla, värme, inbrott och brand. I serverhallen för backuptagning finns larm för brand. Vid larm går detta till en larmcentral och därefter ska personal kontaktas enligt larmlista.

Risk finns för att onödigt damm dras in i serverhallen t ex då dörren öppnas direkt från korridor.

Serverhallarna innehåller onödigt brännbart material. Vattenledningar finns i anslutning till serverhall för drift. Servrar och kommunikationsutrustning står ej i anslutning till golvet vilket utgör ett skydd vid oönskat vatten.

Brandsläckningssystem finns i serverrum för drift (ej i serverrum för backup).

För kortare strömbortfall finns skydd i serverhall för drift.

Kommentarer och rekommendationer:

- Vår bedömning är att rum för drift, backuptagning reservkraft och anslutande utrustning inte är tillfredsställande. Det är här viktigt att det görs en översyn och att kommunledningen säkerställer att det upprättas en dokumenterad bild avseende brister, risker och konsekvenser. Det är därefter viktigt att ett förbättringsarbete påbörjas snabbt.

- Rutiner och/eller tillämpning av rutiner då anställda och leverantörer tillträder serverrummen bör ses över.

- Det är viktigt att en sekretessförbindelse upprättas med leverantörer.

3.5 Har kommunen tillfredsställande rutiner för säkerhetskopiering?

Iakttagelser:

IT-avdelningen tar med något undantag backuper (inte Lundafastigheter och Komvux webserver) för kommunens samtliga system.

Inom IT-avdelningen finns en tekniker som ansvarar för olika system. Tekniker tillsammans med systemansvariga delger backupansvarig inom IT-avdelningen vilka rutiner som ska gälla. IT-avdelningen uppmanar systemansvariga att säkerställa att rätt information kan återläsas på ett tillfredsställande sätt vid bortfall.

IT-avdelningen saknar förteckningar där det står angivet vilken typ av information som hanteras och vilka risker det finns kring informationen, t ex vad skulle hända om informationen kom i orätta händer (sekretess), förvanskades (riktighet) eller förlorades (tillgänglighet)? Enligt ansvariga vid IT-avdelningen är detta ett arbete som bör göras av verksamheterna men som inte skett i tillräcklig utsträckning. Diskussioner avseende detta förs inom kommunen. I samband med att system flyttas till en ny teknisk plattform pågår även en översiktlig genomgång kring säkerheten avseende vissa system.

Det finns varierande krav avseende backuptagning från kommunens verksamheter (t ex sparas vissa backuper från renhållningsverket som arkivkopior.) För att kunna anpassa backuprutiner och arkivering av tagna backuper ser anvariga vid IT-avdelningen ett behov av genomarbetade krav på backuptagning från verksamheten.

Dokumentation avseende IT-avdelningens backuprutiner finns. Olika typer (omfattning) av backuper tas enligt ett dokumenterat upprättat schema.

Backuper med cirka 150 band som cirkulerar finns i bandrobot väl åtskilda från driftsmiljön. (Se även avsnitt 3.3 avseende serverhallar).

Bandroboten stödjer även rutinen att kvalitetssäkra banden (band ska inte användas för länge. Band får återanvändas/skrivas till i omgångar enligt ett uppsatt schema i robot). Loggning av backuptagning sker med automatik. Felaktigheter signaleras.

IT-avdelningen har svårt att idag garantera att information som är äldre än en dag kan återläsas. Detta beror på vilken typ av data som efterfrågas.

Det är från IT-avdelningen planerat att se över backuphanteringen, t ex finns planer på att förbättra återläsningstester. Tester och kontroller av att backuper helt kan användas t ex efter allvarligt fel (t ex diskkrasch) är enligt ansvariga otillräckliga idag, tid och resurser saknas. Ansvariga ser det även önskvärt att kunna genomföra/göra övningar rörande återskapande av system/driftmiljöer.

Tydliga krav av typen ”Full drift skall kunna återtas inom x dagar efter utslagning av serverhallen” saknas från verksamheterna. Underlag enligt ovan skulle underlätta att balansera skyddet till rätt nivå, (säkerhet balanserat mot kostnader). Ansvariga vid IT-avdelningen upplever att bilden över vad som kan återläsas och från när (från vilket tidpunkt) är otydlig hos verksamheten. Kunskap om hur backuprutiner fungerar behöver förmedlas till verksamheten enligt ansvarigs uppfattning.

Kommentarer och rekommendationer:

- Vår bedömning är att kommunens rutiner avseende backuphantering är otillfredsställande. En förbättring av återläsningkontroller bör göras. Vi konstaterar dock att ett förbättringsarbete avseende återläsningskontroller är initierat.

- Ökade och tydliga krav från verksamheten bör utarbetas (t ex via ett arbete med systemsäkerhetsplaner).

- Vi föreslår att möjligheter till en alternativ driftsmiljö för de mest kritiska systemen ses över, t ex e-post system, IP-telefoni, lönesystem, system inom vård och omsorg. Detta för att minimera störningar vid större incidenter.

- Vi föreslår att backuper förvaras betydligt längre än som idag sker, t ex månadsband, årsband bl a för att kunna återfå information som beror på logiska fel. (Kan finnas olika skäl att gå tillbaka till gamla backuper)

- Det är viktigt att driftsmiljön kring backuptagningen förbättras, t ex bättre skydd mot förlust av strömförsörjningen. (Se kommentarer även i avsnitt 3.4 avseende avbrott.)

3.6 Finns bra rutiner för att rapportering av säkerhetsrelaterade händelser (incidenter)?

Iakttagelser:

IT-avdelningen har sedan några år tillbaka påbörjat ett processorienterat arbete som bygger på ITIL (IT-Infrastructure Library). Se mer under roller och ansvar i avsnitt 3.2.

Några viktiga ITIL-delar kan mycket kortfattat beskrivas enligt nedan.

En viktigt grund i arbetet är att det finns ett ställe dit användare kan vända sig (och ska vända sig). En process som triggas igång efter att ärenden inkommer är incidenthanteringsprocessen. Där det ingår att snabbt lösa problemet. Incidenthanteringsprocessen har kopplingar till problemhanteringsprocessen. Där ingår att lösa ”roten till problemet så det intet uppkommer igen”.

Såväl servicedesk som incidenthanterings- och problemhanteringsprocess finns inom Lunds kommun (det finns även ett flertal andra viktiga processer som inte beskriv här). Kontinuerligt sker ett förbättringsarbete kring arbetet i servicedesken och processerna. Det är planerat att ta fram bättre mått som underlag till förbättring av servicedesken och processer i anslutning till servicedesken.

Många användare har i vår enkät uttryckt att det är svårt att komma fram till servicedesken och att det tar för lång tid att få hjälp vilket stör verksamheten.

En orsak till detta som anges från IT-avdelningen är att personalen varit mycket ansträngda då det genomförts förändringar i infrastrukturen som gett oönskade konsekvenser. Detta är ett förbättringsområde som anges, förbättringar kommer att ske bl.a. inom ramen för förändringshanteringsprocessen.

Inom kommunen finns även leveransöverenskommelser där det pågår ett förbättringsarbete. Kundmöten sker regelbundet (f n 4 ggr/år) för att följa upp och planera IT-driften.

Kommentarer och rekommendationer:

- Det finns goda målsättningar hur IT-avdelningen ska arbeta för att erhålla en effektiv och säker hantering vilket är positivt. Avseende servicedesk och incidenthantering har kommunen nått långt. Vi konstaterar dock att det för närvarande finns oönskade störningar i allt för hög grad enligt vår bedömning. Servicedesken är ansträngd och många användare upplever att det tar för lång tid innan fel avhjälps. Vi vill här trycka på vikten av att olika processer effektiviseras och förbättras enligt de ambitioner som finns. I detta arbete ligger att ta fram olika typer av förbättringsmått.

- Det är viktigt att kommunledningen och verksamheterna via information och uppföljning säkerställer att användare använder sig av de rutiner som finns, t ex att rapportera ärenden till kommunens servicedesk.

3.7 Finns tillfredsställande skydd mot virus och spionprogram?

Iakttagelser:

Virusskydd finns. Skyddet säkerställer att filer som läses/skrives och nyttjas scannas för skadlig kod. Enligt ansvarigas bedömning är skyddet i huvudsak tillfredsställande. Dock finns risker som till delar handlar om ett medvetande och kunskap hos ansvariga och användare. Avseende spionprogram uttrycker ansvariga att det finns ett behov av förbättring. En översyn av skyddet finns planerat till 2008, då avtalet kring nuvarande produkter går ut.

Kommentarer och rekommendationer:

- Det är här viktigt att det görs en översyn kring virus och spionprogram och att kommunledningen säkerställer att det upprättas en dokumenterad bild avseende brister, risker och konsekvenser. Därefter finns sannolikt ett behov av ett förbättringsarbete.

3.8 Har användaren erforderlig kunskap om hot och risker för IT-säkerheten?

Iakttagelser:

Utbildning till användare sker idag på ett varierande sätt inom kommunen. Utbildningar som är säkerhetsrelaterade genomförs olika och varierar beroende på system och förvaltning. Övergripande utbildningsaktiviteter saknas. Flera av de vi intervjuat uttrycker ett behov av säkerhetsrelaterade utbildningar till användare och andra ansvariga. I enkäten efterfrågas utbildning inom flera områden som berör IT-säkerhet.

Ett övergripande utbildningsprogram har diskuterats inom kommunen men har ej genomförts.

Kommentarer och rekommendationer:

- Vi ser ett behov av att det genomförs övergripande utbildningsaktiviteter inom kommunen. I anslutning till detta är det viktigt att först se över, förbättra och slutföra arbetet med kommunens olika IT-relaterade dokument. (Givetvis finns fortfarande ett behov av förvaltningsspecifika och systemspecifika utbildningar).

- Utbildningsunderlaget bör tas fram i samarbete mellan IKT-samordnare, systemägare och IT-avdelningen. Underlag som registreras i kommunens servicedesk bör kunna utgöra ett stöd i arbetet. De utbildningsprogram som tas fram bör vara obligatoriska. Ett förslag kan även vara att utbildningar avslutas med ett kunskapstest och/eller att användare signerar att informationen mottagits.

3.9 Finns tillfredsställande rutiner för hantering av behörighet och lösen till gemensamt nätverk?

Iakttagelser:

Alla användare är upplagda i en katalogtjänst. Uppsatta regler avseende lösenordets uppbyggnad, byte och längd finns. Automatisk rutin finns som säkerställer att byte av lösenord sker inom vissa tidsintervaller. Lösenord kan inte repeteras inom angiven tidsintervall. Antal inloggningsförsök är begränsade.

Dokumenterade rutiner finns avseende tilldelning av ID och lösenord. Rutinen är sådan att vid tilldelning av nytt id och lösenord ska arbetsledare kontakta IKT-samordnaren. IKT-samordnaren rapporterar id och lösenord till arbetsledare som delger användare.

Om en användare behöver ett nytt lösenord meddelas detta ibland direkt till användaren både via mail eller telefon av servicedesk eller IKT-samordnare. Rutinen bygger vanligen på att den som beställer är känd.

Det förekommer vid någon förvaltning att även andra än IKT-samordnaren har rätt att påverka behörigheter då IKT-samordnaren delat ut rättigheten.

Några av de intervjuade IKT-samordnarna bedömer att det finns vissa risker i dagens lösenordshantering. I vår användarenkät har 660 av 703 användare svarat att de har kännedom om vad som gäller kring lösenordshanteringen (svarat helt eller i huvudsak). Dock har vi fått svar att lösenordet även används av andra. Vissa användare uttrycker även en viss osäkerhet kring hanteringen av lösenord.

När personal ska sluta sker inte rapportering på ett tillfredsställande sätt enligt de IKT-samordnare som vi har intervjuat. Detta bekräftas av IT-avdelningen, t ex kommer information avseende detta allt för sent.

Uppföljningar avseende behörighetsstrukturer, (t ex att endast anställa finns med) görs ej systematiskt.

Det förs diskussioner om att förbättra behörighetshanteringen via förbättrat IT-stöd. I samband med detta är det även planerat att samverka/synkronisera med lönesystemet. Detta kommer att innebära att rutinen för att anmäla när någon slutar kommer att ses över.

Avseende ID och lösenordshantering i systemen finns varierande rutiner. Det är respektive systemägare som beslutar om dessa regler.

Som skydd mot datorer som lämnas obevakade finns skärmsläckare som aktiveras med automatik. Användare kan beställa/önska till sin IKT-samordnare att skärmsläckaren avaktiveras. Regler över vad som gäller för att IKT-samordnaren ska avaktivera skärmsläckaren är enligt uppgifter otydliga. Enligt vissa ansvarigas bedömning sker detta på ett allt för godtyckligt sätt idag. En orsak är att skärmsläckaren upplevs som störande hos vissa anställda.

Det finns vissa möjligheter för anställda att göra installationer av program i sin egen dator. Anvisningar vad som är tillåtet eller otillåtet finns. Möjlighet finns från IT-avdelningen att följa upp vad som finns i respektive dator. Detta sker ej rutinmässigt (ej skett).

Anställda tillåts inte arbeta utifrån (fjärråtkomst) mot kommunens resurser idag. Anledningen till detta är att skydd på rätt nivå först ska säkerställas av ansvariga. Viss testverksamhet förekommer.

Ansvariga ser ett behov av att förbättra övervakningen av systemens databaser. Oberoende intrångstester sker ej rutinmässigt.

IT-personal ska enligt anvisningar bära godkänd ID-handling väl synligt. Anvisningar från verksamheten avseende vad som krävs kring legitimering är otydlig. Detta är även iakttagelser som delgetts från IT-personal.

På fråga om risker att obehöriga kan ta del av informationen vid utskrift *(14. Då jag skriver ut känsliga dokument på skrivare så medför detta inga risker att obehöriga tar del av informationen (dvs skrivare står i en skyddad miljö eller kod används vid utskrift)* så har 115 användare svarat inte alls vilket innebär att de ser vissa risker. Inom socialförvaltningen har 10 användare svarat delvis eller inte alls på frågan.

Kommentarer och rekommendationer:

- Vi bedömer att kommunens rutiner för tilldelning av ID och lösenord inte är helt tillfredsställande. Flödet avseende vem som får beställa, hur det ska gå till att beställa och tilldela samt vem som tilldelar lösenord och ID bör ses över. (t ex ska inte tilldelning ske via telefon). Det förbättringsarbete som planerats och som även innefattar PA-processer är positivt i detta sammanhang.

- Det är viktigt att kommunledningen tydliggör (för ansvariga chefer), vikten av att tillämpa den rutin som finns då anställda slutar.

- Vi konstaterar att ansvariga ser ett behov att förbättra och se över skyddet mot åtkomst till databaser och servrar. Det är här viktigt att brister, risker och konsekvenser tydliggörs och att förbättringsåtgärder prioriteras. Därefter är viktigt att ett förbättringsarbete påbörjas. Efter förbättringsarbetet är genomfört är det dessutom viktigt att det genomförs tester mot systemens databaser (intrångstester från insidan och utsidan av kommunens brandvägg).

- Det är viktigt att det inom kommunen säkerställs att anställda inom kommunen är medvetna om att IT-personal alltid måste legitimera sig innan tillträde ges till datorer.

- Det är viktigt att verksamheterna gör översyn över var skrivare finns placerade idag samt i anslutning till detta vilka risker det finns med att utskrifter kan nås av obehöriga.

- Det är positivt att det finns skärmsläckare som aktiveras med automatik. Vi konstaterar dock att det förekommer att skärmsläckare avaktiveras. Rutiner för detta bör ses över. Skälen till att ta bort skyddet bör dokumenteras av den som genomför åtgärden (t e x IKT-samordnare).

- Granskningsområdet ovan kring behörighet är till delar kunskapsrelaterat. Kommentarer avseende utbildningsbehov är intaget i avsnitt 3.8 ”Har användaren erforderlig kunskap om hot och risker för IT-säkerheten”.

3.10 Finns tillfredsställande rutiner för inköp och hantering av datorer som ej längre nyttjas?

Iakttagelser:

En dokumenterad rutin avseende hur datorer och annan utrustning ska hanteras finns. Rutin finns även för hur datorer som ej används ska tas omhand. Rutinen beskrivs kortfattat i bilaga 2.

Den utrustning som finns är förtecknad i elektroniskt register vid IT-avdelningen.

Inventeringar av att registret stämmer genomförs enligt uppgifter från ansvarig vid IT-avdelningen.

Verksamheten får inte köpa IT-utrustning vid sidan om rutinen. Om inte rutinen används kan inte datorer installeras i kommunens nät.

En förbättring som pågår är att via elektronisk avläsning mot datorn uppdatera registret avseende datorer. Avläsning elektroniskt och uppdatering i register görs även då datorer ej längre används.

Kommentarer och rekommendationer:

- Vi bedömer rutinen för hantering av kommunens datorer vara tillfredsställande. Det är dock viktigt att ansvariga via uppföljning försäkrar sig om att rutinen tillämpas som avsett, t ex att datorer som inte används tas om hand enligt upprättad rutin.

3.11 Finns anvisningar och/eller skydd mot att användare installerar program eller annat oönskat material på sin dator?

Iakttagelser:

Det finns vissa möjligheter för anställda att göra installationer av program i sin egen dator. Anvisningar vad som är tillåtet eller otillåtet finns. Anvisningar kommer att tydliggöras ytterligare av ansvariga. Gemensamma program förtecknas i register. Möjlighet finns från IT-avdelningen att följa upp vad som finns i respektive dator. Detta sker ej rutinmässigt (ej skett).

Kommentarer och rekommendationer:

- Det är viktigt att uppföljning sker avseende innehållet i användarnas datorer för att säkerställa att endast tillåten programvara används.

3.12 Finns det en avbrottsplan för att säkerställa att funktioner kan återställas inom erforderlig tid?

Iakttagelser:

Det finns ingen dokumenterad avbrottsplan i kommunen. Ett arbete har påbörjats men är ännu inte klart.

Kommentarer och rekommendationer:

- Analyser för att identifiera följderna av eventuella katastrofer bör genomföras.

- En avbrottsplan bör upprättas. Avbrottsplanen bör innehålla en beskrivning av vad som krävs för att starta driften på nytt, prioriteringar samt ansvaret för olika aktiviteter.

4. Sammanfattande bedömning

Vi vill sammanfatta vår granskning med att vi bedömer resultatet avseende flera av de kontroller som vi utfört vara tillfredsställande. Vi har även konstaterat brister och väsentliga förbättringsområden. Samtidigt kan vi konstatera att det inom flera områden där vi konstaterat brister pågår ett förbättringsarbete som ansvariga på olika nivåer arbetar med. Här kan nämnas

- Det arbete som pågår kring IT-handbok. Här har vi i rapporten även angett vikten av att se över hur dokumenten ska kommuniceras till olika målgrupper.

- Ett arbete med att förtydliga roller och ansvar har nyligen påbörjats.

- Ett förbättringsarbete avseende återläsningskontroller av tagna backuper är initierat. Ansvariga ser dock ett problem avseende resurser för att kunna bedriva arbetet på ett tillräckligt sätt.

- En kontinuerlig förbättring av IT-avdelningens processer pågår. Ett prioriterat område är att förbättra processen kring förändringshanteringen. (Det har nyligen skett förändringar med oönskade konsekvenser i form av olika störningar till användare)

- En översyn av skyddet avseende virus och spionprogram är planerat.

- Det förs diskussioner om att förbättra behörighetshanteringen via förbättrat IT-stöd. I samband med detta är det även planerat att samverka/synkronisera med lönesystemet. Detta kommer även att innebära att rutinen för att anmäla när någon slutar kommer att ses över.

I de arbeten som ska initieras och som pågår är det givetvis viktigt att tydliga tidsplaner sätts upp och att det säkerställs att arbetet slutförs enligt de planer som finns.

Andra områden där vi konstaterat brister och som är viktiga för kommunen att förbättra sammanfattas i nedanstående punkter.

- Det finns en god målsättning inom kommunens avseende hur IT-avdelningen ska arbeta för att erhålla en effektiv och säker hantering vilket är positivt. Avseende servicedeskfunktionen och incidenthanteringen har kommunen nått långt. Vi konstaterar dock att det för närvarande finns oönskade störningar i allt för hög grad enligt vår bedömning. Servicedesken är ansträngd och många användare upplever att det tar för lång tid innan fel avhjälps. Vi vill även trycka på vikten av att olika processer effektiviseras och förbättras enligt de ambitioner som finns. I detta arbete ligger att ta fram olika typer av förbättringsmått.

- Det är bristfälligt att det idag saknas systemsäkerhetsplaner för kommunens system. Det är viktigt att kommunledningen utarbetar en plan och utser ansvarig för att säkerställa att arbetet med systemsäkerhetsplaner sker. Vi kan konstatera att det finns dokument som berör IT-säkerheten som är inaktuella och som inte används i praktiken. Här vill vi tillägga att vi upplevt att det är svårt att överskåda de dokument som finns och att det därmed finns risker att dokumenten inte fyller sitt syfte.

- Vi bedömer att uppföljning och kontroll av IT-säkerheten inom kommunen inte sker på ett tillfredsställande sätt. Det är här viktigt att kommunledningen via information och uppföljning försäkrar sig om att organisationen (chefer, användare m fl) vet vilket ansvar de har för IT-säkerheten samt att policys och regler efterlevs. (Vad vill kommunledningen har svar på och på vilket sätt ska rapporteringen ske).

- Vår bedömning är att rum för drift, backuptagning reservkraft och anslutande utrustning inte är tillfredsställande. Det är här viktigt att det görs en översyn och att kommunledningen säkerställer att det upprättas en dokumenterad bild avseende brister, risker och konsekvenser. Det är därefter viktigt att ett förbättringsarbete påbörjas.

- Vi föreslår att möjligheter till en alternativ driftsmiljö för de mest kritiska systemen ses över. (T ex e-post system, IP-telefoni, lönesystem, system inom vård och omsorg). Detta för att minimera störningar vid större incidenter.

- Vi ser ett behov av att det genomförs övergripande utbildningsaktiviteter inom kommunen.

- Vi konstaterar att ansvariga ser ett behov att förbättra och se över skyddet mot åtkomst till databaser och servrar. Det är här viktigt att brister, risker och konsekvenser tydliggörs och att förbättringsåtgärder prioriteras. Därefter är viktigt att ett förbättringsarbete påbörjas. Efter förbättringsarbetet är genomfört är det dessutom viktigt att det genomförs tester mot systemens databaser (intrångstester från insidan och utsidan av kommunens brandvägg).

- Det är viktigt att verksamheterna genomför en översyn över var skrivare finns placerade samt i anslutning till detta även ser över vilka risker det finns med att utskrifter kan nås av obehöriga.

- Det är positivt att det finns skärmsläckare som aktiveras med automatik. Vi konstaterar dock att det förekommer att skärmsläckare avaktiveras. Rutiner för detta bör ses över. Skälen till att ta bort skyddet bör dokumenteras av den som genomför åtgärden (t e x IKT-samordnare).

- Analyser för att identifiera följderna av eventuella katastrofer bör genomföras och i anslutning till detta är det viktigt att en avbrottsplan upprättas. Avbrottsplanen bör innehålla en beskrivning av vad som krävs för att starta driften på nytt, prioriteringar samt ansvaret för olika aktiviteter.

Mot bakgrund av ovanstående punkter bedömer vi det som viktigt att ledningen stärker greppet kring IT-säkerheten. Ett förslag till första steg är att ledningen, verksamhetsansvariga, IT-chef och andra aktörer noga diskuterar igenom statusen kring IT-säkerheten (informationssäkerheten). Exempel på punkter som är viktiga att ha tydlig samsyn och målsättning kring är följande:

- Vilka målsättningar finns med de olika förbättringsprojekten och vilka risker och konsekvenser finns innan projekten/arbetet är slutfört.

- Områden att förbättra men som ej är påbörjade (risker och konsekvenser).

- På vilket sätt bedrivs förbättringsarbetet och kan arbetet eventuellt bedrivas effektivare (problem och hinder).

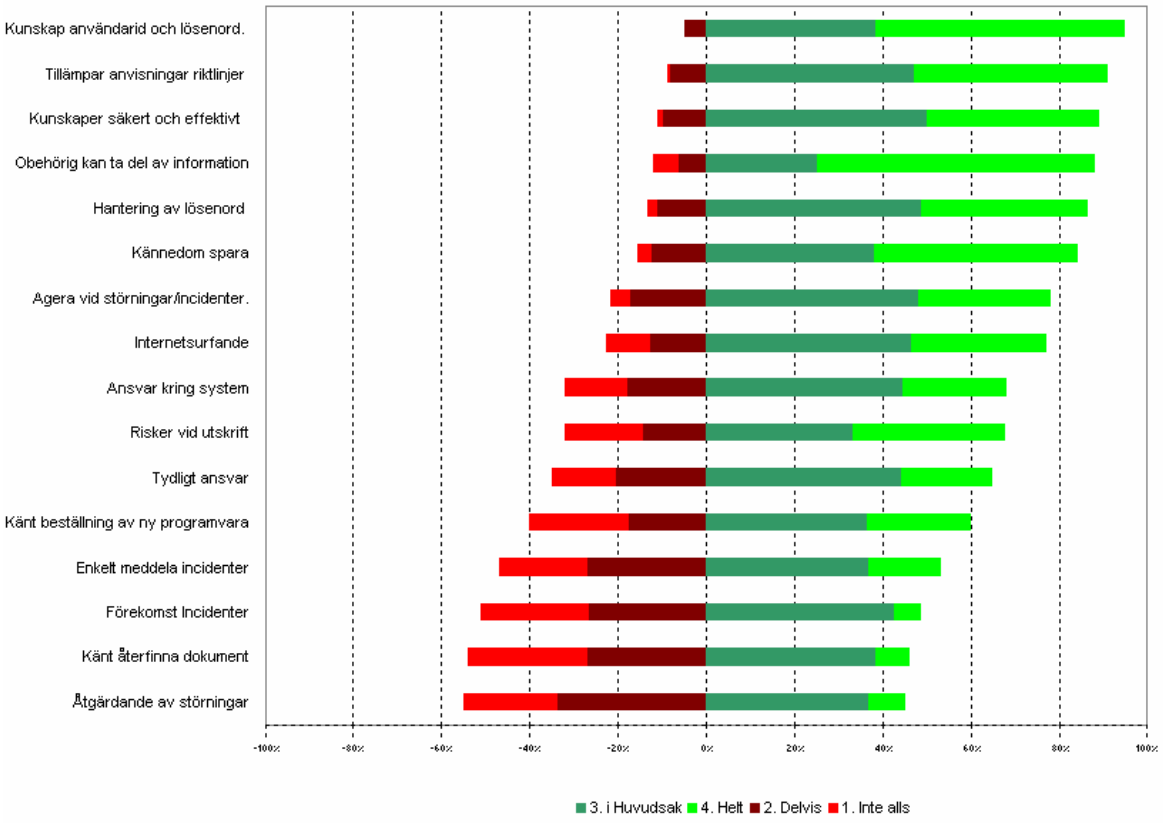
- Vilka förbättringseffekter kommer arbetet att innebära.

- Vem ansvarar för att åtgärda olika frågor och när ska det vara klart.

- Vilka resurser krävs.

Bilaga 1

Nedan visas en grafisk sammanställning över svaren från användare. Svar där användare angett att ett påstående bara till delvis eller inte alls är uppfyllt visas med negativa värden (röda). Där användare varit positiva svarat helt eller i huvudsak visas grön färg. Efter grafiken visas i tabell frågan som den ställdes till användaren.



Nedan visas hur frågan ställdes till användare (frågor sorteras för att överensstämma med grafiken ovan)

03. Jag har tillräcklig kunskap över hur jag hanterar mitt/mina användarid och lösenord.

08.Jag bedömer att jag tillämpar de anvisningar, rutiner och riktlinjer som finns enligt ovan (t ex hantering av lösenord, agerande vid viruslarm o.dyl)

11.Jag har tillräckliga kunskaper för att på ett säkert och effektivt sätt kunna utföra de arbetsuppgifter som jag utför med hjälp av min dator och det system som jag i huvudsak använder

15. Då jag lämnar min dator påslagen är det säkerställt att ingen obehörig kan ta del av information på skärmen och/eller använda min dator på ett olovlig sätt (t ex genom att skärmsläckare med lösenord används)

02. Jag känner till vad som gäller* avseende hantering av lösenord till nätverket och det/de system som jag vanligtvis arbetar med.

06. Jag vet var och hur jag ska spara mina filer, både i personliga mappar och i delade mappar.

04. Jag vet hur jag ska agera vid störningar/incidenter. (viruslarm ,tappad lösenord, datorproblem etc)

07.Jag känner till vad som gäller som kommunanställd då jag är ute på internet.

10. Det är tydligt vem som ansvarar för IT-säkerheten/informationssäkerheten i det IT-system som jag i huvudsak använder

14. Då jag skriver ut känsliga dokument på skrivare så medför detta inga risker att obehöriga tar del av informationen (dvs skrivare står i en skyddad miljö eller kod används vid utskrift)

09. Det är tydligt vem/vilka som ansvarar för olika IT-säkerhetsfrågor inom kommunen/och eller min förvaltning.

05. Jag känner till vad som gäller avseende beställning av ny programvara/applikation till min dator

12.Det är enkelt* att meddela störningar/ incidenter och förändringsärenden (t ex nytt konto, upplägg av var utskrift ska ske)

17. Det är ovanligt med störningar/incitenter då jag arbetar med min dator och mina system (applikationer,program)t

16. Det är väl känt för mig var jag återfinner styrande och stödjande dokument som berör kommunens IT-säkerhet

13. Ärenden och problem/störningar åtgärdas vanligen tillräckligt snabbt efter att de rapporterats.

Bilaga 2

Rutin inköp av datorer

Kortfattat kan inköpsrutinen beskrivas enligt nedan.

1. Vid behov beställer verksamheten datorer via intranätet

Man kan välja i ett a b och c sortiment

A sortimentet är våra standardprodukter levereras och konfigureras enligt fastställda normer

B och C har en viss valfrihet är förenat med olika former av kostnader

(blankett på intranätet, olika alternativ av utrustning finns i ett upprättat produktblad)

2. En beställning genereras hos logistik partner som informerar oss per e-mail (extern leverantör) Gammal utrustning

3. Vår support gör i ordning datorn (t ex installerar program enligt uppställd mall)

4. Transport av utrustning sker till avsedd plats i kommunen via vår påplats support den installeras och verifieras avseende funktion A

Alla datorer får ett namn A000000 Som följer den under livstiden namnet är kopplat till serienummret. Serienummer och namn är unikt och båda försvinner när produkten dör allt registreras i vårt AD där det är sökbart via olika kriterier

Gammal utrustning

1. tas om hand enligt fastställd rutin. Utrusningen sorteras och tas om hand av Lunds renhållningsverk LRV (t ex använda det som går att använda och skrotning på ett genomtänkt sätt)