Stenungsunds kommun

Uppföljning av fördjupad granskning IT-säkerhet

KPMG Bohlins AB
2006-09-05
Antal sidor: 9

Stenungsund IT-granskning.doc

Innehåll

1. Sammanfattning

År 2002 genomfördes en fördjupad granskning av kommunens IT-säkerhet, med fokus på skydd av information och behörighetskontrollsystem. I maj 2006 har det på uppdrag av kommunrevisionen genomförts en uppföljning av kommunens genomförda åtgärder, utifrån väsentliga iakttagelser redovisade i rapporten "Fördjupad granskning av IT-säkerheten" per 2002-11-05.

Den uppföljande granskningen har visat att kommunen har förbättrat styrningen av IT-verksamheten. Roller och ansvar har blivit tydligare vad gäller beställare och utförare av IT relaterade tjänster.

Kommunen har ett antal pågående projekt med att förbättra IT-säkerheten. Statusen och våra rekommendationer inom de områden vi anser bör prioriteras är följande:

Reservplan för IT

Kommunen arbetar med att formulera en systemsäkerhetsplan per system. Enligt systemsäkerhetsplanen ansvarar systemägarna för att ta fram avbrotts-/katastrofplaner, vilket de i nuläget inte har gjort.

Avsaknaden av väl testade avbrotts-/katastrofplaner innebär risk för att tiden för återgång till normal drift ökar. Systemägarna bör prioritera arbetet med att ta fram en avbrotts-/katastrofplan per system. Vidare bör IT-enheten, tillsammans med säkerhetsansvarig i kommunen, ta fram en övergripande avbrotts- och katastrofplan för kommunen.

Styrande dokument för IT

Kommunen antog en IT-säkerhetspolicy per 2006-02-27. Policyn skall konkretiseras i IT-säkerhetsinstruktioner för Förvaltning, Drift och Användare samt systemsäkerhetsplaner.

Kommunen har skapat en struktur för styrande dokument och bör prioritera arbetet med att slutföra dokumentationen av IT-säkerhetsinstruktioner och systemsäkerhetsplaner.

Behörighetsadministration

Det finns en rutin för att hantera tidigare anställdas behörigheter i nätverket men i verksamhetsspecifika system ansvarar respektive resultatenhet för behörigheterna.

Om behörigheter inte uppdateras finns det en risk för att obehöriga personer har tillgång till känslig information. Det finns fungerande rutiner för behörighetsadministrationen på central nivå. Kommunen bör även ta fram gemensamma rutiner för hur uppföljningar av användar-ID och behörigheter skall hanteras i resultatenheterna.

Säkerhetskopiering

Det finns etablerade, men inte dokumenterade, rutiner för säkerhetskopiering. Ej dokumenterade rutiner innebär en risk för avsaknad av tillgänglighet till information i samband med en incident. Dokumentationen av backuprutinerna bör prioriteras.

Fysisk säkerhet

Kommunen arbetar kontinuerligt med att förbättra den fysiska säkerheten. Samtliga applikationsservrar som innehåller databaser är centraliserade till ett datarum hos IT-enheten. Kommunen bör dock se över de generella nycklar som finns till korskopplingsskåp på Nösnäsgymnasiet.

Uttjänt datautrustning

Tomma diskar förvaras i nuläget hos IT-enheten. Vid granskningen framkom att det inte finns någon lösning för hur de tomma diskarna skall hanteras. Avsaknaden av en rutin för diskförstörelse innebär en risk att sekretessbelagd/känslig information sprids. Kommunen bör därför fastställa en rutin som säkerställer att diskarna förstörs på ett säkert sätt.

2. Inledning och bakgrund

På uppdrag av kommunrevisionen genomfördes 2002 en fördjupad granskning av IT-verksamheten, med fokus på skydd av information och behörighetskontrollsystem.

I maj 2006 har vi genomfört en uppföljning av vad som har åtgärdats av kommunen, utifrån tidigare lämnade rekommendationer.

Uppföljningen omfattar de områden som den föregående granskningen avsåg dvs:

- ansvarsfrågorna kring informationshanteringen för de i verksamheten kritiska delarna i IT-stödet,
- IT-säkerheten avseende den lagrade informationen, samt
- den interna kontrollen avseende behörighetsadministrationen för IT-systemen centralt och lokalt i verksamheterna.

3. Syfte och tillvägagångssätt

Syftet med granskningen har varit att kartlägga och bedöma hur den interna kontrollmiljön avseende generella IT-kontroller har förbättrats sedan den genomförda granskningen 2002.

Den uppföljande granskningen baseras på strukturerade intervjuer med:

Christer Ottosson ..... IT-chef

Sören Andersson ..... IT-koordinator (IT-säkerhetssamordnare)

Helene Larsson..... Planeringssekreterare hos Individ- och familjeomsorg

Eva Kellén.....Vård och äldreomsorgschef hos Social omsorg

Gun Carlsson.....Sekreterare Stenungsunds vårdcentral

Granskningen omfattar även genomläsning av erhållen dokumentation rörande IT-säkerheten i kommunen.

4. IT-revision 2006

4.1 Styrning av IT-verksamheten

Status 2002

Vid den tidigare granskningen framkom att IT-rådet, som nu benämns IT-beredningsgruppen, hade en otydlig roll i organisationen. IT-rådet hade svårt att nå ut till verksamheten och rådets medlemmar hade inte fullt ut kompetens inom IT-området.

Det framkom vidare att alla verksamheter inte hade en IT-ansvarig som kunde agera beställare av IT.

Slutsats 2006

IT-beredningsgruppens sammansättning är i princip som tidigare och består utöver IT-chefen, av administrativ chef, en chef från respektive verksamhetsområde samt en teknisk chef. IT-beredningsgruppen skall fungera som en remissinstans och bereda ärenden åt verksamhetschefsgruppen innan beslut fattas i kommunstyrelsen.

Sedan föregående granskning har IT-personalen i resultatenheterna förflyttats till den centrala IT-enheten som servar hela organisationen med IT-tjänster. IT-enheten har delats in i ansvarsområden, där varje område har en utsedd ansvarig och en utvecklingsgrupp som tillsammans ansvarar för kvaliteten i arbetet, kompetensutveckling och dokumentation.

IT-enheten har utsett en IT-koordinator per resultatenhet som skall ansvara för kommunikationen mellan resultatenheterna och IT-enheten. En gång per år hålls ett avstämningsmöte mellan respektive verksamhetschef och IT-koordinator. För att tydliggöra ansvarsfördelningen mellan

IT-enheten och verksamheterna har det formulerats ett dokument "Ansvarsfördelning IT-enhet och verksamheter" som bereds av IT-beredningsgruppen.

Sedan föregående granskning har kommunen utvecklat styrningen av IT-verksamheten. Det finns tydligare ansvarsfördelningar som skapar förutsättningarna för att fungera som ett ändamålsenligt IT-stöd åt verksamheterna inom kommunen. Det saknas dock resurser för att analysera verksamheternas långsiktiga strategiska behov inom IT-området.

4.2 IT säkerhet

4.2.1 Riskanalys

Status 2002

Granskningen 2002 visade att klassning av information i verksamhetsspecifika system ej hade genomförts. Vidare fanns ingen avbrottsplan framtagen.

Slutsats 2006

Det pågår ett arbete med att kartlägga kommunens mest kritiska verksamhetssystem. Därefter skall det, utifrån en prioriteringsordning fastställd av IT-beredningsgruppen, tas fram systemsäkerhetsplaner för respektive system. I nuläget finns systemsäkerhetsplaner för två av de mest verksamhetskritiska systemen, Procapita respektive Profdoc. Klassificering av information utgör en väsentlig del av systemsäkerhetsplanen eftersom båda systemen hanterar sekretessbelagd/känslig information.

Enligt systemsäkerhetsplanerna skall systemägarna bedöma hur länge respektive system kan stå still. Systemägarna skall även ansvara för att ta fram en avbrotts- och katastrofplan för respektive system. Vid granskningen framkom att det inte fanns några sådana planer framtagna.

Risken med att inte ha en väldokumenterad avbrotts- och katastrofplan är att tidsåtgången för återgång till normal drift ökar vid inträffandet av incidenter. Det är därför väsentligt att systemägarna prioriterar arbetet med att ta fram avbrotts- och katastrofplaner per system. IT-enheten bör, tillsammans med säkerhetsansvarig för kommunen, även ta fram en övergripande avbrotts- och katastrofplan för kommunen.

4.2.2 Policydokument

Status 2002

Vid föregående granskning framkom att det inte fanns någon enhetlig dokumentation avseende IT-säkerhet och IT-organisationen.

Slutsats 2006

Kommunen antog en IT-säkerhetspolicy per 2006-02-27. Ett arbete pågår med att konkretisera policyn i IT-säkerhetsinstruktionerna, Förvaltning, Drift och Användare samt systemsäkerhetsplaner för verksamhetskritiska system.

Enligt systemsäkerhetsplanen skall årliga uppföljningar av planerna genomföras. Hittills har två uppföljningar av systemsäkerhetsplanen avseende Procapita IFO genomförts. När det gäller Profdoc är kommunen inte systemägare, vilket försvårar uppföljningsprocessen och är en förklaring till varför ännu ingen uppföljning av systemsäkerhetsplanen har genomförts. I granskningen framkom att systemsäkerhetsplanen för Profdoc inte har kommunicerats på ett tydligt sätt till de lokalt systemansvariga inom primärvården.

Kommunen har strukturerat policydokument och rutiner till en enhetlig dokumentation avseende IT-strategi, IT-organisation och IT-säkerhet. Det är viktigt att kommunen färdigställer den dokumentation som har påbörjats, så att det finns förutsättningar för att behandla IT-relaterade frågor på ett ändamålsenligt sätt inom organisationen.

4.2.3 Informationssäkerhet

Slutsats 2002

Vid föregående granskning framkom att IT-enheten successivt bygger om äldre datorer till s k tunna klienter (dvs lokalt placerade datorer med en gemensam centralt placerad server).

Vidare framkom att användning av modem inte är helt homogen inom kommunen även om flertalet modemanvändare använder sig av kommunens modempool.

Slutsats 2006

I nuläget har ca 50 % av användarna s k tunna klienter inom det administrativa nätet men föredelningen är ojämn på resultatenhetsnivå. Inom skolnätet har ca 40 % av användarna tunna klienter.

Kommunen har sedan föregående granskning stängt samtliga modemanslutningar. För access utifrån används Citrix secure gateway där användare får ett engångslösenord via mobiltelefonen. För externa konsulter skickas lösenordet till helpdesk som förmedlar lösenordet vidare till berörd person.

Antalet tunna klienter har ökat inom kommunen, framförallt inom resultatenheten Individ- och familjeomsorg som hanterar stor del sekretessbelagd/känslig information. Det tillsammans med den nya lösningen för extern uppkoppling gör att informationssäkerheten har ökat inom kommunen.

4.2.3.1 Individ- och familjeomsorg

Status 2002

Vår föregående granskning visade att personal kunde spara arbetsrelaterad data på disketter för vidare bearbetning/förflyttning till annat ställe än arbetsplatsen.

Slutsats 2006

Enligt "IT-säkerhetsinstruktioner för användare" skall all information sparas på server. I nuläget används enbart tunna klienter inom Individ- och familjeomsorg, vilket innebär att känslig information automatiskt sparas centralt på servrar. Datorerna är dock inte spärrade för användning av USB (Universal Serial Bus).

Kommunen har vidtagit åtgärder för att begränsa risken för att information sprids till obehöriga. Möjligheten att använda USB kvarstår, vilket innebär att anställda kan spara arbetsrelaterad data och föra den vidare. Kommunen bör därför se över möjligheten att spärra datorerna för användning av USB minne.

4.2.4 Behörighetsadministration

Status 2002

Vid vår föregående granskning framkom att riktlinjer för behörighetsadministration och lösenordshantering inte fanns dokumenterade. Vidare framkom att det inte fanns några direktiv framtagna för hur säkerhetsadministrationen skulle fungera.

Slutsats 2006

Sedan föregående granskning har det införts rutiner för behörighetsadministration. Endast verksamhetschefer och lokalt IT-ansvariga, får beställa användarkonton för nätverksaccess. Beställningen kan skickas via webben till IT-enheten som administrerar behörigheterna. För att användarkontot skall aktiveras krävs det att användaren skriver under dokumentet "IT-säkerhetsåtagande för användare".

I nuläget finns en implementerad rutin för att hantera tidigare anställdas behörigheter till nätverket. IT-enheten får månadsvis en lista från personalavdelningen på vilka personer som har slutat. Vi har tagit del av arkiveringsrutinen som innebär inaktivering av användarkonto och arkivering av hemkatalogen i ett år innan kontot och katalogen tas bort definitivt. Respektive verksamhetsenhet ansvarar för hanteringen av behörigheter i de verksamhetsspecifika systemen.

Det finns en fungerade rutin för behörighetsadministrationen för nätverket, däremot saknas en gemensam rutin för hur resultatenheterna skall hantera behörighetsadministrationen i de verksamhetsspecifika systemen.

4.2.4.1 Behörighetsadministration i resultatenheterna

Status 2002

Vår föregående granskning visade att rutinerna för behörigheter och lösenordshantering var bristfälliga i samtliga resultatenheter.

Flera användare än nödvändigt hade kraftfulla behörigheter (administratörsrättigheter) inom individ- och familjeomsorg. Vidare framkom att regler för lösenordslängd ej fanns implementerade i Procapita.

Slutsats 2006 Kristinedalskolan och Nösnäsgymnasiet

I skolnätet, där elever är den stora kategorin användare, är det inte möjligt att ställa samma krav på lösenord som i det administrativa nätet. Kriterierna för lösenordens utformning sätts per domän och eftersom elever och personal tillhör samma domän är det inte möjligt att differentiera kraven på personalens och elevernas lösenord. I "IT-säkerhetsinstruktioner för användare" finns det dock reglerat att personalen skall följa uppsatta krav på lösenord.

I skolnätet skall personalen inte spara känslig information. Känslig information skall sparas i det administrativa nätet där kraven på lösenorden följer kommunens riktlinjer.

Slutsats 2006 Individ- och familjeomsorg och Social omsorg

Inom Individ och familjeomsorg har det genomförts en uppföljning av användare med kraftfulla behörigheter. I nuläget har fyra personer utökade behörigheter, varav en person på IT-avdelningen som har fullständig behörighet som administratör. Nya och gamla användarkonton i Procapita hanteras genom att närmsta chef tar kontakt med verksamhetschefen alternativt systemansvarige. Behörigheterna i Procapita är anpassade efter vilken arbetsroll den anställda har.

För systemet Profdoc delar Social omsorg nät/server med Primärvården. Primärvården får månadsvis information av verksamhetschefen om uppläggning och inaktivering av användarkonton. För att säkerställa att inga gamla användare finns kvar i Profdoc och Procapita görs det en fullständig genomgång av användarkonton en gång per kvartal.

Individ- och familjeomsorg och Social omsorg har rutiner för att hantera behörighetsadministrationen, vilket begränsar risken för obehörig åtkomst.

4.2.5 Säkerhetskopiering

Status 2002

Vid föregående granskning var resultatenheternas servrar placerade utanför IT-enhetens lokaler och därmed ingick de inte i kommunens centrala back-up system. Vid granskningen framkom bl a att social omsorg hyr plats av Primärvårdens server för systemet Profdoc och Primärvården ansvarar för backuprutinerna. Vidare framkom att det saknades dokumenterade rutiner för backuphanteringen på Nösnäsgymnaiset.

Slutsats 2006

Ansvaret för samtliga servers är i nuläget centrerat till IT-enheten, undantaget är servern som Social omsorg delar med Primärvården.

Sedan ett år tillbaka används TSM, dvs incrementell backup varje dygn till disk. En gång per kvartal tas det en fullständig backup som sparas på band och förvaras i ett bankfack. För att förenkla återläsningen av data sparas de fem senaste versionerna av de fullständiga backuperna.

Det saknas i nuläget dokumenterade backuprutiner både vad gäller tillvägagångssätt och vilket material som skall sparas. För att minska sårbarheten bör kommunen prioritera arbetet med att färdigställa dokumentationen av backuprutiner. Fler personer skall utifrån dokumentation kunna genomföra back-up.

4.2.6 Fysisk säkerhet

Status 2002

Vid föregående granskning framkom att merparten av resultatenheternas applikationsservrar var placerade i ett datarum i kommunhusets lokaler. Ett undantag var Nösnäsgymnasiet som hade kvar lokalt placerade applikationsservrar. Vidare framkom att lås med generella nycklar fanns kvar för vissa korskopplingsskåp.

Slutsats 2006

Det finns fortfarande ett fåtal applikationsservar lokalt placerade på Nösnäsgymnasiet, men på servrarna finns enbart ett fåtal program och ingen informationslagring. De generella nycklarna till vissa korskopplingsskåp finns fortfarande kvar och bör ses över.

4.2.7 Uttjänt datautrustning

Status 2002

Vid föregående granskning fanns det en dokumenterad rutin för hantering av uttjänt datautrustning. Enligt rutinen skall kassering och byte av datautrustning meddelas IT-enheten.

Slutsats 2006

All datautrustning som är uttjänt i det administrativa nätet skall skickas till IT-enheten. De tomma diskarna förvaras i nuläget hos IT-enheten eftersom det inte finns någon lösning på diskförstörelsen skall hanteras. På sikt skall IT-enheten även hantera skolnätets utrustning på samma sätt som utrustningen från det administrativa nätet.

Avsaknaden av en rutin för diskförstörelse innebär en risk att sekretessbelagd/känslig information sprids. Kommunen bör därför fastställa en rutin som säkerställer att diskarna förstörs på ett säkert sätt.

5. Förslag på åtgärder

Utifrån vår granskning föreslår vi att kommunen genomför följande åtgärder:

- Systemägarna bör ta fram avbrotts- och katastrofplan för respektive system. IT-enheten, tillsammans med kommunens säkerhetsansvarig, bör ta fram en övergripande avbrotts- och katastrofplan för hela organisationen.
- IT-enheten och utsedda systemägare bör prioritera arbetet med att slutföra dokumentationen av IT-säkerhetsinstruktioner och systemsäkerhetsplaner.
- Det bör för resultatenheterna finnas tydliga och dokumenterade rutiner för behörighetsadministration i verksamhetsspecifika system.
- Vi rekommenderar att kommunen fastställer en rutin som säkerställer att uttjänade diskar förstörs på ett säkert sätt.
- Kommunens verksamheter hanterar en stor del sekretessbelagd/känslig information varför vi rekommenderar kommunen att fortsätta öka antalet användare av tunna klienter.

Göteborg som ovan

KPMG Bohlins AB

Annika Hessler
Information Risk Management

Åsa Dahlberg
Information Risk Management