PRICEWATERHOUSECOOPERS

**Revisionsrapport**

# Kommunrevisionens

# Uppföljning av Granskning av IT-säkerheten

Klippans kommun

27 september 2010

Eva Lidmark, revisionskonsult

PRICEWATERHOUSECOOPERS

## Innehållsförteckning

### Sammanfattning

De förtroendevalda revisorerna i Klippans kommun har gett Komrev inom PricewaterhouseCoopers i uppdrag att följa upp en övergripande granskning av IT-säkerheten som gjordes under 2008. Granskningsobjektet är i första hand kommunstyrelsen.

Kommunens IT-stöd är av stor betydelse på olika sätt. Den moderna informationsteknologin ger möjligheter till att höja kvalité, säkerhet och effektivitet i verksamheten, sprida och öka tillgängligheten till information mm. Inom många områden är det idag självklart att IT är en förutsättning för att aktiviteter och processer skall fungera. IT blir en viktig del i verksamheten.

Utifrån gjorda intervjuer och dokumentgenomgång anser vi att granskningen har visat att kommunstyrelsen fastställt en åtgärdsplan utifrån de förbättringsområden som identifierades vid granskningen 2008 vilket vi bedömer vara tillfredsställande. Vi rekommenderar kommunstyrelsen att fortlöpande revidera planen vid de tillfällen genomförande av åtgärder inte kommer till stånd enligt tidplan.

Vi rekommenderar också kommunstyrelsen att göra en ekonomisk planering utifrån de åtgärder som ännu inte är vidtagna.


# 1 Inledning

## 1.1 Bakgrund

De förtroendevalda revisorerna i Klippans kommun har gett Komrev inom PricewaterhouseCoopers i uppdrag att göra en uppföljande granskning av den övergripande IT-säkerheten. Under 2008 genomfördes en övergripande granskning av IT-säkerheten. Denna uppföljning syftar till att identifiera vilka förändringar som har skett sedan förra granskningen. Granskningsobjektet är i första hand kommunstyrelsen.

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.

Vår definition med IT-säkerhet menas här alla olika åtgärder som används för att för att skydda och säkerställa åtkomsten av information samt att interna och externa regelverk följs. Kontrollfunktioner i separata system innefattas här inte av begreppet. Betydelse 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 såväl för kommunen som för enskilda personer.

### 1.2 Revisionsfråga och avgränsning

Granskningen syftar till att identifiera vilka förändringar som har skett sedan förra granskningen beträffande:

- Finns aktuella styrande och stödjande dokument som berör IT-säkerhet?
- Finns tydligt ansvar för att arbeta aktivt med IT-säkerhetsfrågor. *(t ex sker uppföljning avseende tillämpning av styrande dokument och rapporteras/efterfrågas detta av/till styrelse och nämnder)*
- Finns ett tillräckligt skydd kring rum som används för datordrift *( förhindra störningar, avbrott, obehörigt tillträde och stöld)?*
- Har kommunen tillfredställande rutiner för säkerhetskopiering?
- Finns tillfredställande rutiner för hantering av behörighet till gemensamt nätverk?

### 1.3 Metod

Granskningen har genomförts genom intervju med IT-chefen samt att för uppdraget relevant dokumentation har granskats.

Rapporten har varit föremål för sakgranskning.

## 2 Granskningsresultat

### 2.1 Allmänt

Kommunstyrelsen antog i oktober 2008 dokument ”Åtgärdsplan IT-säkerhet Klippans kommun”. Åtgärdsplanen upprättade som en följd av den granskning som genomfördes under våren 2008. De planerade och/eller genomförda åtgärder som redovisas under punkterna 2.2—2.6 är ur denna åtgärdsplan.

## 2.2 Finns aktuella styrande och stödjande dokument som berör IT-säkerhet?

### 2.2.1 Iakttagelser

Förslag till ny IT-policy är framtagen enligt IT-chefen men ännu ej processad genom kommunfullmäktige på grund av väntan på ett dokumenthanteringssystem. Implementering av dokumenthanteringssystemet är fördröjt pga. förändrade ekonomiska ramar 2009, enligt IT-chefen. IT-chefen anger att dokumentet ska processas vidare efter sommaren 2010.

Som exempel på förbättringar i den nya IT-policyn nämner IT-chefen ökad tydlighet för anställda vad gäller utnyttjande av Internet-resursen samt regler för lagring av privata filer.

Vad gäller förbättrad åtkomst till styrande dokument planeras för införande av ny portal till hösten 2010 enligt IT-chefen. På så sätt, menar IT-chefen, säkerställs att användarna på ett lättare sätt än idag kommer åt aktuella dokument. Kommunen kommer att införa en så kallad användarförsäkran när den nya portalen är införd. I samband med att användarförsäkran skrivs under kommer två områden att betonas enligt IT-chefen; var dokumenten finns att tillgå i portalen samt var ”portfölj” med digitala utbildningar finns att tillgå (se vidare under punkten 2.3.1).

Vad gäller systemsäkerhetsplaner är detta arbete påbörjat, enligt IT-chefen. Detta arbete är en del i ett pågående dokumentationsprojekt för kommunens systemansvariga där även framtagande av systemdokumentation och rutiner för systemförvaltning ska tas fram.

### 2.2.2 Kommentarer och bedömning

Vi kan konstatera att det pågår ett antal aktiviteter för att säkerställa att det finns aktuella styrande och stödjande dokument vilket vi finner tillfredsställande. Vad gäller förslag till ny IT-policy rekommenderar vi kommunstyrelsen att prioritera att detta dokument blir fastställt. Vi rekommenderar också kommunstyrelsen att kontinuerligt följa upp status på övriga aktiviteter.

## 2.3 Finns tydligt ansvar för att arbeta aktivt med IT-säkerhetsfrågor?

### 2.3.1 Iakttagelser

I förslaget till ny IT-policy framgår ansvarsfördelningen vad gäller att arbeta aktivet med IT-säkerhetsfrågor. I kommunen finns också en säkerhetspolicy vilken säkerhetschefen ansvarar för enligt IT-chefen. I säkerhetspolicyn framgår att IT-chefen ansvarar för IT-säkerheten.

En gemensam helpdeskfunktion är införd sedan februari 2009. Helpdesk bemannas av IT-pedagoger och kommunens datoranvändare vänder sig till helpdesk med alla ärenden. Ett systemstöd är infört för att på sätt möjliggöra uppföljning av inkomna ärenden, enligt IT-

chefen. Om någon användare skickar in anmärkningsvärt många ärenden till helpdesk kontaktas vederbörande av en IT-pedagog för uppföljning. IT-pedagogerna har också inventerat utbildningsbehovet bland de anställda och planerar för digitala utbildningar som ligger som en användarfunktion i den nya skolplattformen som implementeras under hösten 2010 enligt IT-chefen.

Det kommer, enligt IT-chefen, att tas fram olika utbildningspaket beroende på målgrupp. Det kommer att bli obligatoriskt att gå igenom utbildning vilket kopplas till användarförsäkran anger IT-chefen. Samtliga utbildningspaket kommer att innehålla ett säkerhetsavsnitt enligt IT-chefen.

### 2.3.2 Kommentarer och bedömning

Vi kan konstatera att det i förslaget till ny IT-policy är tydligt vem som ansvarar för att arbeta aktivt med IT-säkerhetsfrågor. Vad gäller förslag till ny IT-policy rekommenderar vi kommunstyrelsen att prioritera att detta dokument blir fastställt.

## 2.4 Finns ett tillräckligt skydd kring rum som används för datordrift

### 2.4.1 Iakttagelser

Vad gäller larm i serverhall finns larm för rök, värme, fukt och för strömavbrott i säkringsrum samt i UPS[1]. Dessa larm är aktiverade för 2 serverrum samt televäxelrum, enligt IT-chefen. Larmen går som SMS till 2 mobilnummer och är testade i riktiga fall anger IT-chefen. Problemet, enligt IT-chefen, är att det inte finns någon beredskapsorganisation som har till uppgift att ta emot dessa larm i kommunen. Det medför att ingen har ansvar för mobiltelefonerna under kvällar, nätter och helger. Detta får konsekvenser för bland annat personalen inom vård och omsorg som behöver åtkomst till sitt verksamhetssystem dygnets alla timmar. Enligt IT-chefen är frågan aktualiserad i kommundirektörens ledningsgrupp men inga beslut är tagna, då det inte är klargjort vem som ska betala för denna beredskapsorganisation.

Vad gäller parallell serverhall, vilket var ett viktigt förbättringsförslag i den förra granskningen, pågår en förstudie som ska leda till förslag till beslut enligt IT-chefen. Dock har begränsade ekonomiska ramar fördröjt beslutet. Enligt IT-chefen tittar kommunen nu på en lösning som går ut på att använda Åstorps kommuns sekundära miljö som ett parallellt serverrum. En utredning av detta startar i september med eventuellt beslut under hösten 2010. I väntan på en parallell serverhall är nuvarande situation med serverhall i kommun-

1 av engelska ”uninterruptible power supply”, på svenska Avbrottsfri kraftförsörjning

husets källare mycket otillfredsställande med tanke på bl.a. översvämningen 2007 enligt IT-chefen.

### 2.4.2 Kommentarer och bedömning

Vi konstaterar att det inte finns en parallell serverhall vilket vi bedömer inte vara tillfredsställande. Vi rekommenderar kommunstyrelsen att prioritera arbetet med förstudie och beslut i denna, för IT-säkerheten, viktiga fråga.

## 2.5 Har kommunen tillfredställande rutiner för säkerhetskopiering

### 2.5.1 Iakttagelser

I dagsläget sker en korsvis placering av bandrobotar enligt IT-chefen. Vad gäller förbättringar inom detta område uppger IT-chefen att det nu finns större fysisk säkerhet för banden genom korsvis placering av robotarna. IT-avdelningen gör i praktiken en rad återstartstester i samband med uppgraderingar av system som innebär byte av hårdvara. Vid sådana byten har man, enligt IT-chefen, fått kvitto på att det bandade materialet är korrekt. Detsamma gäller vid återläggning av filer i övrigt.

Arbetet med arkivplaner för backuper är inte påbörjat enligt IT-chefen. Frågan om arkivplan kommer att aktualiseras tillsammans med arkivarie, när denna tjänst tillsätts, enligt IT-chefen.

### 2.5.2 Kommentarer och bedömning

Vi bedömer att hantering av säkerhetskopiering är tillfredsställande.

## 2.6 Finns tillfredställande rutiner för hantering av behörighet till gemensamt nätverk?

### 2.6.1 Iakttagelser

Vad gäller lösenordshantering anger IT-chefen att kommunens systemansvariga hanterar sina egna regler för denna hantering. IT-chefen önskar starkare autentisering[2] än idag och beskriver ett önskvärt läge med så kallad single sign-on. Single Sign-On är en teknik för att underlätta inloggning vid flera system, då användaren enbart behöver logga in en gång.

[2] kontroll av uppgiven identitet, till exempel vid inloggning i system

Inom kommunens vård- och omsorgsverksamhet kommer medarbetarna att börja använda med de så kallade SITHS-korten[3] för att möjliggöra åtkomst till den med Region Skåne gemensamma dokumentation kring en vårdtagare. IT-chefen anger att den nya portalen kommer att bygga på 2-faktorsautentisering[4] och här skulle SITHS-kortet kunna användas av alla kommunens datoranvändare. IT-chefen betonar att i denna fråga har kommunen en hög ambitionsnivå och ligger långt framme i planeringen med ett fullskaligt införande beror på ytterligare faktorer framförallt den ekonomiska.

Avslut av användarkonton är en besvärlig fråga inom framförallt vård och omsorg och socialtjänsten menar IT-chefen. För att underlätta situationen vid återtag av vikarier ligger användarkonton kvar även om anställningen har upphört. IT-avdelningen har dock en rutin som handlar om att inaktivera alla konton som inte varit aktiva på mer än 3 månader.

I kommunens metakataloglösning[5] automatiseras hanteringen av konton via koppling till kommunens personaladministrativa system. Innan denna funktion aktiveras måste, enligt IT-chefen, en kommungemensam rutin för vikariehantering beslutas. Frågan ligger således inte på IT-chefens bord innan denna rutin är framtagen och beslutad.

### 2.6.2 Kommentarer och bedömning

Vi kan konstatera att det pågår viss implementering och vidare planering för utveckling av behörighetskontroll. Vi rekommenderar kommunstyrelsen att prioritera vilka insatser som ska göras.

---

[3] SITHS är kort med elektroniska chip som används för att logga in i system, signera dokument mm. Kortet är en giltig e-legitimation som används för identifikation, till exempel när patientuppgifter flyttas inom eller utom en organisation.

[4] Användarnamn/lösenord i kombination med dosa/mobil

5 En katalog som håller reda på innehåll och förändringar i andra kataloger

PRICEWATERHOUSECOOPERS

2010-09-27

_____ _____

_____ _____

*Namnförtydligande* *Namnförtydligande*