www.pwc.se

Övergripande säkerhets-granskning av kommunens säkerhet avseende externt och internt dataintrång

Lessebo kommun

Informationssäkerhets-specialister:

Henrik Friang
Viktor Bergvall
Victor Svensson

Kommunalrevisor:
Caroline Liljebjörn

November 2016

pwc

Innehåll

1. Sammanfattning

På uppdrag av de förtroendevalda revisorerna i Lessebo kommun har PwC granskat säkerheten avseende externt och internt dataintrång, främst i form av interna riktlinjer och styrdokument. Revisionsfrågan för granskningen är:

Finns det en tydlig förståelse i kommunen för vilka de prioriterade hoten mot kommunens IT-miljö är och är kommunens interna ramverk för IT-säkerhet ändamålsenligt i förhållande till de prioriterade hoten?

Efter genomförd granskning är vår bedömning att det finns utrymme för förbättring inom området för IT- och informationssäkerhet. Vår bedömning grundar sig på de brister vi noterat i kontrollmiljön utifrån definierade revisionsmoment (listas i avsnitt 2.4).

Vårt svar på revisionsfrågan är att kommunstyrelsens styrningsmodell för IT- och informationssäkerhet för att löpande identifiera prioriterade hot delvis är ändamålsenlig i förhållande till de prioriterade hoten.

Vår bedömning grundar sig framförallt på att;

- Det saknas en formell process för att löpande analysera risker och hot mot verksamheten. Iakttagelsen medför att kontroller och arbetsinsatser inom området för IT- och informationssäkerhet inte nödvändigtvis har utgångspunkt i relevanta hot.

- Det saknas en formell process där representanter från IT och verksamheterna regelbundet träffas för att diskutera inträffade incidenter, identifierade risker och hot utifrån ett verksamhetsperspektiv samt vidtagna och planerade åtgärder utifrån ett IT-perspektiv.

- Det saknas en formell och dokumenterad avbrottsplan som beskriver tillvägagångssättet för att återställa IT-miljön efter en allvarlig säkerhetsincident eller avbrott. Iakttagelsen medför att en incident kan få större konsekvenser för verksamheten än nödvändigt.

Vi har dock noterat att det finns informella processer för att löpande identifiera och hantera hot kopplade till IT-och informationssäkerhet och att det bedrivs ett aktivt förbättringsarbete inom området, vilket vi ser som positivt. Vidare har vi granskat den fysiska säkerheten utan väsentliga iakttagelser. En analys av tekniskt skydd i kommunens nätverk har även genomförts utan väsentliga iakttagelser. Detta tyder på att det trots påpekade förbättringsmöjligheter finns en god förståelse för IT- och informationssäkerhet inom kommunen.

Denna granskning avgränsas till Lessebo kommun och inkluderar ej processer och rutiner hos IT-leverantörer till kommunen. Vi har dock noterat att det hos kommunens IT-leverantörer förekommer formella processer för IT- och informationssäkerhetsarbete. Granskningen innefattar området för kravställning och uppföljning mellan Lessebo kommun och deras IT-leverantörer.

2. Inledning

2.1. Bakgrund

Hanteringen av risker inom området för IT-och informationssäkerhet får allt större betydelse då verksamheter blir allt mer beroende av stöd från IT-system.

En effektiv riskhantering bygger på ett helhetstänk. Kvaliteten, säkerheten och effektiviteten i organisationens interna processer ökar och organisationen skyddas mot till exempel obehöriga dataintrång samtidigt som beredskapsmedvetandet stärks inom organisationen.

Bakgrunden till granskningen är revisorernas riskanalys.

2.2. Syfte och Revisionsfråga

Granskningen ska ge svar på följande revisionsfråga;

Finns det en tydlig förståelse i kommunen för vilka de prioriterade hoten mot kommunens IT-miljö är och är kommunens interna ramverk för IT-säkerhet ändamålsenligt i förhållande till de prioriterade hoten?

2.3. Revisionskriterier

- Finns prioriterade hot mot kommunens IT säkerhet dokumenterade och uppdateras dokumentationen löpande?
- Är kommunens policys/riktlinjer för IT säkerhet ändamåls-enligt formulerade i förhållande till de prioriterade hoten?

2.4. Revisionsmoment

Granskningen har inriktas mot följande moment:

- Finns det en tydlig strategi för IT-säkerhet och är den kommunicerad till kommunens ledning och invånare?
- Hur ser organisationen och ansvarsfördelning ut i frågor rörande IT-säkerhet?
- Har kommunen ett ändamålsenligt arbetssätt för att hantera risker relaterade till prioriterade hot inom område för IT-säkerhet?
- Finns det en process för incidenthantering, hur uppdateras tekniska försvarsmekanismer och processer utifrån lärdom av inträffade säkerhets incidenter?
- Finns det en tydlig plan för att upprätthålla och återställa verksamhetskritiska funktioner vid tillfälle för en säkerhetsincident?

2.5. Avgränsning

Granskningen avgränsas till kommunstyrelsen och samtliga nämnder.

2.6. Metod

Inom ramen för granskningen har intervjuer genomförts med utvalda personer på Lessebo kommun, analys av dokumentation i form av styrande dokument, processbeskrivningar och arbetsrutiner samt genomfört analys av tekniskt skydd i nätverk och fysisk granskning av serverhallar. Revisionsrapporten har sakgranskats av berörda tjänstemän.

Intervjuer har genomförts med följande personer:

- Ekonomi- och IT-chef
- IT-samordnare på IT-enheten
- Utvecklingsstrateg, även ansvarig för informationssäkerhetsarbetet (5% av tjänsten)

3. Iakttagelser, bedömningar och rekommendationer

3.1. Styrning av IT- och informationssäkerhet

3.1.1. Iakttagelser

- **Riskanalys:** Någon formell och dokumenterad riskanalys har inte genomförts för IT- och informationssäkerhet på en kommunövergripande nivå, med syfte att styra processer och insatser inom området. Vi har dock noterat att en generell riskanalys har genomförts på en kommunövergripande nivå, vilken till viss del berör risker kopplat till tillgänglighet för verksamhetskritiska system. Det saknas vidare en tydlig och dokumenterad koppling mellan resultatet av den genomförda analysen och styrningen av IT- och informationssäkerhetsområdet, med avsikt att etablera kontroller och insatser utefter identifierade risker och hot.

- **Styrning av IT- och informationssäkerhetsarbetet:** Policys för IT- och informationssäkerhetsområdet finns dokumenterade. Det saknas dock en dokumenterad beskrivning över organisation, roller, ansvarsfördelning och rapporteringsvägar, inklusive kommunikationsplan för IT- och informationssäkerhetsområdet. Vidare har vi noterat att det saknas en formell process för förändringshantering samt att processen för behörighetsadministration ej omfattar periodisk genomgång av tilldelade behörigheter. Det finns heller ingen process för att regelbundet revidera styrande dokument.

3.1.2. Bedömning och rekommendationer

Bristande processer och formella rutiner för att identifiera och hantera risker, styra IT- och informationssäkerhetsarbetet och följa upp säkerhet hos tredjepartsleverantörer ökar risken för driftsstörningar och olika typer av säkerhetsincidenter, vilket kan leda till dels bristande tillgänglighet till verksamhetskritiska system och applikationer och dels till förlust av känslig information.

Vi rekommenderar Lessebo kommun att överväga följande åtgärder;

1) Etablera en process där externa och interna hot mot verksamheten årligen utvärderas. Utgångspunkt kan vara nuvarande process för kommunövergripande generella riskanalys. Vidare bör en prioritering genomföras av de identifierade hoten kopplat till risk, utifrån sannolikhet och påverkan på verksamheten i händelse av en incident. Varje identifierad risk ska analyseras utifrån vilken teknisk plattform (nätverk/server/databas/applikation/fast data) som kan komma

att påverkas vid en incident. Klassificeringen ligger sedan till grund för tekniska kontroller för respektive område.

2) Dokumentera processen avseende förändringshantering. Förstärk nuvarande dokumentation för processen avseende behörighetsadministration och inkludera även periodisk genomgång av tilldelade behörigheter.

3) Implementera en process för att regelbundet revidera styrande dokument inom IT- och informationssäkerhetsområdet.

4) Styrning och uppföljning av IT- och informationssäkerhetsområdet bör genomgående formaliseras. Förslagsvis genom att etablera en process där representanter från IT och verksamheterna regelbundet träffas för att diskutera inträffade incidenter, identifierade risker och hot utifrån ett verksamhetsperspektiv samt vidtagna och planerade åtgärder utifrån ett IT-perspektiv.

3.2. *Processer för IT- och informationssäkerhet*

3.2.1. *Iakttagelser*

- **Behörigheter i nätverk:** Processen för tillägg, förändring och borttag av behörigheter på nätverksnivå utförs av IT-avdelningen efter förfrågan från den anställdes chef. Vidare noterar vi att det inte sker någon periodisk genomgång av tilldelade behörigheter i nätverket, vilket innebär en ökad risk att kritiska behörigheter kan ligga kvar på en anställd som fått en ny befattning eller avslutat sin anställning. Det pågår dock ett arbete med att automatisera processen för behörighetsadministration. En fördefinierad rolluppsättning i Microsoft Forefront Identity Manager (FIM) kommer användas för att koppla ihop Windows Active Directory och lönesystemet, vilket innebär att risken för avsaknad av en periodisk genomgång av behörigheter minskar.

- **Behörigheter i applikationer:** Processen för tillägg, förändring och borttag av behörigheter på applikationsnivå administreras av respektive förvaltning. Det finns inga styrande dokument på kommunövergripande nivå som reglerar denna process.

- **Avbrottshantering:** Det saknas en definierad process och plan för hur IT-miljön ska återställas vid händelse av en säkerhetsincident. Vid en allvarligare incident finns det möjlighet att återställa IT-miljön på en reservsite, rutinen är dock inte dokumenterad.

3.2.2. *Bedömning och rekommendationer*

Avsaknad av periodisk uppföljning av behörigheter, medför en risk att tilldelade behörigheter ej är i linje med användares faktiska roll i verksamheten och att tidigare anställda har kvar sina behörigheter både i nätverket och på applikationsnivå. Detta kan i

sin tur leda till otillbörlig åtkomst till känslig information och kritiska aktiviteter i system och applikationer.

Slutligen föreligger risk för driftsstörningar i IT-miljön i händelse av en säkerhetsincident, genom avsaknad av avbrottsplaner.

Vi rekommenderar Lessebo kommun att överväga följande åtgärder;

1) Formalisera och dokumentera processen för administration av behörigheter i system och applikationer på förvaltningsnivå.

2) Implementera en rutin för periodisk genomgång av tilldelade behörigheter i system och applikationer för att säkerställa att aktuella behörigheter stämmer överens med den anställdes roll i organisationen. Genomgången ska dokumenteras för att säkerställa spårbarhet i processen.

3) Ta fram en avbrottsplan för verksamhetskritisk IT-miljö. Planen ska regelbundet testas och åtminstone årligen utvärderas. Planen bör åtföljas av dokumenterade rutiner för att återskapa servrar och filer utifrån backup i händelse av en incident.

3.3. Uppföljning av IT- och informationssäkerhet

3.3.1. Iakttagelser

Uppföljning av incidenter: Rutinen är att incidenter ska rapporteras in till IT-första linjens support, Växjö kommuns helpdesk, där ärenden registreras och följs upp i ett ärendehanteringssystem, vilket medför full spårbarhet i processen. Ärenden som ej kan lösas av första linjen eskaleras till andra linjens support i Lessebo, som även den arbetar i samma ärendehanteringssystem.

Det saknas dock en dokumenterad process för uppföljning av ärenden med avsikt att identifiera mönster, förebygga problem och uppdatera tekniskt skydd för ärenden i andra linjens support. Vidare saknas det en formell process för återkoppling och uppföljning av incidenter från första linjens support till andra linjens support i Lessebo. En formell process för incidenthantering är även en viktig förutsättning för att verksamheten kontinuerligt ska lära sig av tidigare erfarenheter och ständigt arbeta med att förbättra sin förmåga i att hantera hot relaterade till IT- och informationssäkerhet.

3.3.2. Bedömning och rekommendationer

De i huvudsak informella, men till viss del även formaliserade, processer som finns för hantering och uppföljning av inträffade incidenter bedöms till stora delar fungera ändamålsenligt, sett utifrån organisationens storlek. Dock kan avsaknad av en formell process medföra att likartade incidenter inte identifieras och hanteras i tid, vilket kan leda till oönskade avbrott i system och applikationer.

Vi rekommenderar Lessebo kommun att överväga följande åtgärder;

1) Implementera, med utgångspunkt i nuvarande informella process, en formell process för att löpande utvärdera inträffade säkerhetsincidenter med avsikt att dra lärdom från dessa och uppdatera tekniska försvarsmekanismer. Den formella processen bör inkludera dokumentationskrav av möten och utvärderingar samt åtgärder som har vidtagits.

4. Revisionell bedömning

Revisionsfrågan för granskningen är:

Finns det en tydlig förståelse i kommunen för vilka de prioriterade hoten mot kommunens IT-miljö är och är kommunens interna ramverk för IT-säkerhet ändamålsenligt i förhållande till de prioriterade hoten?

Vårt svar på revisionsfrågan är att kommunstyrelsens styrningsmodell för IT- och informationssäkerhet för att löpande identifiera prioriterade hot delvis är ändamålsenlig i förhållande till de prioriterade hoten.

Efter genomförd granskning är vår bedömning att det finns utrymme för förbättring. För redogörelse av vår detaljerade bedömning av uppfyllnadsgrad för kontroller inom respektive revisionsmoment, se Appendix 1.

Uppdragsledare
Caroline Liljebjörn

Projektledare
Henrik Friang

4. Revisionell bedömning

Revisionsfrågan för granskningen är:

Finns det en tydlig förståelse i kommunen för vilka de prioriterade hoten mot kommunens IT-miljö är och är kommunens interna ramverk för IT-säkerhet ändamålsenligt i förhållande till de prioriterade hoten?

Vårt svar på revisionsfrågan är att kommunstyrelsens styrningsmodell för IT- och informationssäkerhet för att löpande identifiera prioriterade hot delvis är ändamålsenlig i förhållande till de prioriterade hoten.

Efter genomförd granskning är vår bedömning att det finns utrymme för förbättring. För redogörelse av vår detaljerade bedömning av uppfyllnadsgrad för kontroller inom respektive revisionsmoment, se Appendix 1.

Uppdragsledare
Caroline Liljebjörn

Projektledare
Henrik Friang

Appendix 1: Bedömning av uppfyllnadsgrad

Nedan följer en sammanställning över PwC's bedömning av uppfyllnadsgrad för kontroller inom respektive revisionsmoment;

Revisionsmoment	Lessebo kommun
Moment 1 *Finns det en tydlig strategi för IT-säkerhet och är den kommunicerad till kommunens ledning och invånare?*	Delvis uppfyllt
Moment 2 *Hur ser organisationen och ansvarsfördelning ut i frågor rörande IT-säkerhet?*	Delvis uppfyllt
Moment 3 *Har kommunen ett ändamålsenligt arbetssätt för att hantera risker relaterade till prioriterade hot inom område för IT-säkerhet?*	Delvis uppfyllt
Moment 4 *Finns det en process för incidenthantering, hur uppdateras tekniska försvarsmekanismer och processer utifrån lärdom av inträffade säkerhetsincidenter?*	Delvis uppfyllt
Moment 5 *Finns det en tydlig plan för att upprätthålla och återställa verksamhetskritiska funktioner vid tillfälle för en säkerhetsincident?*	Ej uppfyllt