www.pwc.se

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

## Växjö kommun

Informationssäkerhets-specialister:

*Viktor Bergvall*
*Linus Owman*

Certifierad kommunal revisor:
*Lena Salomon*

*Januari 2018*

pwc

# *Innehåll*

# 1. Sammanfattning

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

*Är kommunstyrelsens styrmodell för IT- och informationssäkerhet för att löpande identifiera prioriterade hot ändamålsenlig i förhållande till de prioriterade hoten?*

Efter genomförd revision och genomgång av samtliga kontrollmål är vår bedömning att kommunstyrelsens styrmodell för IT- och informationssäkerhet för att löpande identifiera prioriterade hot ej är ändamålsenlig i förhållande till de prioriterade hoten.

Vår bedömning grundar sig framför allt på att;

- Det saknas styrande dokument på förvaltningsnivå som beskriver behörighetsadministration samt förändringshantering.
- Det saknas beskrivning i de styrande dokumenten om hur ofta de ska revideras.
- Det saknas processer för periodvis granskning av behörigheter och priviligierade användaraktiviteter.
- Det saknas en definierad plan och process avseende kommunens förfarande gällande hur IT-miljön ska återställas vid händelse av en säkerhetsincident.
- Utifrån resultat av genomförd BSA-analys* bedömds det finnas förbättringsområden inom säkerhet i mjukvara.

  ** Baseline Security Assessment är ett verktyg som läser konfigurations- och kontoinställningar på utvalda servrar.*

# 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 och framgångsrik riskhantering bygger på ett helhetstänkande. 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 risk- och väsentlighetsanalys.

## 2.2. Syfte och Revisionsfråga

Granskningen ska ge svar på följande revisionsfråga;

*Är kommunstyrelsens styrningsmodell för IT- och informationssäkerhet för att löpande identifiera prioriterade hot ändamålsenlig i förhållande till de prioriterade hoten?*

## 2.3. Revisionskriterier

- Det finns en ändamålsenlig process för att löpande identifiera hot mot kommunens IT- och informationssäkerhet.
- Prioriterade hot mot kommunens IT- och informationssäkerhet finns dokumenterade, och dokumentationen uppdateras löpande.
- Processer, policys och riktlinjer för att hantera identifierade hot, är ändamålsenliga i förhållande till de prioriterade hoten

## 2.4. Revisionsmoment

Granskningen har inriktas mot följande moment:

- Riskanalys kopplat till område för IT-och informationssäkerhet finns.
- Styrande dokument för IT- och informationssäkerhet – samt kommunikationsplan är upprättat.
- Organisationen, roller, ansvarsfördelning och rapporteringsvägar i frågor rörande IT- och informationssäkerhet är tydliga.
- Det finns ändamålsenliga rutiner för att hantera risker relaterade till prioriterade hot inom område för IT- och informationssäkerhet.
  Styrande dokument
  IT processer; behörighets administration, förändringshantering
  Kartläggning; säkerhet i mjukvara, fysisk säkerhet – i förhållande till ”good practice”.

- Tekniska försvarsmekanismer och processer uppdateras utifrån lärdom av inträffade säkerhetsincidenter.

- Det finns en tydlig plan för att upprätthålla och återställa verksamhetskritiska funktioner vid tillfälle för en säkerhetsincident.

## 2.5. Avgränsning

Granskningen avgränsas till kommunstyrelsen.

## 2.6. Metod

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

Intervjuer har genomförts med följande personer:

- IT-chef
- IT-arkitekt
- F.d Säkerhetschef
- Systemägare Ekonomiavdelningen
- Systemägare Arbete och välfärd
- Systemägare Omsorgsförvaltningen

# 3. Iakttagelser, bedömningar och rekommendationer

## 3.1. Styrning av IT- och informationssäkerhet

### 3.1.1. Iakttagelser

- **Riskanalys**: Det genomförs årligen riskanalys på Växjö kommuns IT-miljö som ligger till grund för verksamhetens handlingsplan. Under granskningstillfället var handlingsplanen för 2018 nyligen klar, vilken bland annat inkluderade framtagande av en kontinuitetsplan för IT. Vidare görs riskanalys till varje nytt system som övervägs att införas i IT-miljön. Riskanalyserna ligger sedan till grund för kravställning för respektive system.
  I ledningsgruppen inom IT behandlas olika typer av risker och på veckomötena finns en stående punkt som hanterar uppföljning av IT-risker.

- **Styrning av IT- och informationssäkerhetsarbetet:** Det finns formell dokumentation avseende informationssäkerhet, både för förvaltningar och bolag samt för IT drift, som utgår från Växjö kommuns säkerhetspolicy. Dokumentationen är baserad på ISO 27000-serien. I dokumentet IT-drift beskrivs processen för behörighetsadministration samt rutiner för förändringhantering. Beskrivningarna avser endast IT-avdelningen. Det nämns i dokumentet IT-drift att det är systemägarna för respektive system som ansvarar för systemets användare, att användarna har rätt behörigheter i systemen samt att användarna har rätt kunskap om säkerhetsreglerna. Det saknas dock styrande dokument på förvaltningsnivå som beskriver behörighetsadministration samt förändringshantering. Vi har också noterat att det, i de befintliga dokumenten, saknas beskrivning om hur de ska revideras. Dokumentet IT-drift skapades 2016-11-24 men det framgår inte om dokumentet har reviderats sedan dess. Vidare har dokumentet ”Informationssäkerhet – Förvaltning och Bolag” inte reviderats sedan 2015-09-18.

- **Organisation roller och ansvar:** Det finns dokument som beskriver IT-organisationens avdelningar inklusive ansvarsområden och rapporteringsvägar. Det finns även dokument som beskriver informationssäkerhetsansvar samt vilka roller som har vilket ansvar inom området för informationssäkerhet. Det noterades vid granskningstillfället att det under senare halvan av 2017 endast funnits en säkerhetsansvarig på deltidstjänst (25 %) samt att det saknas informationssäkerhetsansvarig. Rekrytering till dessa tjänster pågår.

- **Säkerhetsinställningar:** Utifrån resultat av genomförd BSA-analys* bedöms det finnas förbättringsområden inom säkerhet i mjukvara. Inkonsekvens i konfiguration av säkerhetsinställningar och användarkonton har identifieras. Vissa säkerhetsinställningar som är fastställda enligt policy efterlevs inte. Vidare har generiska konton samt konton med kritiska behörigheter identifierats. Detta ökar risken för otillbörlig åtkomst och försvårar spårbarhet.

** Baseline Security Assessment är ett verktyg som läser konfigurations- och kontoinställningar på utvalda servrar.*

### 3.1.2. Bedömning och rekommendationer

Processerna avseende riskanalys kopplat till IT- och informationssäkerhet anses vara ändamålsenliga. Det finns etablerade rutiner gällande årlig riskanalys, riskanalys vid införande av nytt system, samt regelbundna möten för att hantera identifierade risker.

Avsaknaden av styrande dokument avseende behörighetsadministration och förändringshantering ökar dock risken för otillbörlig åtkomst till system och applikationer samt driftstörningar. Bristande säkerhetskonfigurering av servrar samt inkonsekvens i policyefterlevnaden kring användarkonton, ökar risken för säkerhetsincidenter.

Vi rekommenderar Växjö kommun att överväga följande åtgärder;

1) Implementera styrande dokument på förvaltningsnivå för behörighetsadministration samt förändringshantering. Dokumenten avseende behörighetsadministration bör hantera kontroller för att tilldela, förändra och ta bort behörigheter i applikationer, samt periodvis uppföljning av behörigheter och priviligierade användaraktiviteter. Dokumenten avseende förändringshantering bör beskriva tillvägagångssättet samt kontroller för programförändringar alternativt uppgraderingar av applikationer.

2) Implementera en process för att regelbundet revidera styrande dokument inom IT- och informationssäkerhetsområdet för att säkerställa att dessa är ändamålsenliga. Det bör även framgå av dokumentation när senaste revidering genomfördes.

3) Gå igenom, och vid behov, uppdatera inställningar och konton på servernivå med syfte att stärka säkerheten.

## 3.2. Processer för IT- och informationssäkerhet

### 3.2.1. Iakttagelser

- **Behörigheter i nätverk:** Processen för tillägg, förändring och borttag av behörigheter på nätverksnivå sker delvis via en automatisk process, som synkroniseras mellan personalsystemet och katalogtjänst. Kontohantering för kommunala bolag samt för konsulter och leverantörskonton sker manuellt och på uppdrag av ansvarig beställare. Processen finns beskriven i dokumentet IT-drift. Vi har noterat att det inte sker någon periodisk genomgång av tilldelade behörigheter i nätverket, vilket innebär en risk att kritiska behörigheter kan ligga kvar på en anställd som fått en ny befattning eller avslutat sin anställning. Vidare har vi noterat att viss loggning av priviligierade användaraktiviteter görs, dock inte på detaljnivå. Det görs inte heller någon regelbunden uppföljning av loggarna.

- **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. Det finns dock vissa rutinbeskrivningar på förvaltningsnivå som beskriver

processen. Under granskningstillfället framkom det brister avseende avslut av användarkonton. Processen utgår från att den anställdes närmaste chef ska informera systemadministratör om att kontot ska tas bort, vilket inte alltid fungerar. Vidare noterades att det inte sker någon periodvis granskning av behörigheter och priviligierade användaraktiviteter på applikationsnivå.

- **Förändringshantering:** Förändringshantering innebär all medveten programförändring och uppgradering av system och applikationer som IT-enheten och underliggande enheter genomför. IT-avdelningen använder ett verktyg som heter Service Manager för att hantera programförändringar. I pulsmötena, IT-avdelningens veckovisa avstämningar med verksamheten, planeras framtida versionsförändringar. Vi har noterar att det saknas processdokumentation som reglerar denna process på förvaltningsnivå.

- **Avbrottshantering och fysisk säkerhet:** Det saknas en definierad plan och process avseende kommunens förfarande gällande hur IT-miljön ska återställas vid händelse av en säkerhetsincident. Vid inspektion av fysisk säkerhet i serverhall identifierades inga brister. Vid en incident finns det möjlighet att återställa delar av IT-miljön på en reservsite, rutinen är dock inte formellt dokumenterad eller testad.

### *3.2.2. Bedömning och rekommendationer*

Avsaknad av periodisk uppföljning av behörigheter och priviligierade användaraktiviteter, 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 oprövad avbrottsplan.

Vi rekommenderar Växjö kommun att överväga följande åtgärder;

1) Formalisera och dokumentera processen för administration av behörigheter i system och applikationer samt förändringshantering på förvaltningsnivå. Processerna bör vara formellt dokumenterade för att säkerställa enhetlighet samt minska personberoende.

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-teamets första- och andra linje support. Service Manager används som ärendehanteringssystem som medför full spårbarhet i processen. Varje incident klassificeras och får en dedikerad ägare i systemet. Incidenter klassificerade som kritiska tas upp på ledningsmöten där beslut tas om vilka åtgärder som behövs. Det hålls även regelbundna möten med gruppledare, driftschefer från driftavdelningen samt tjänsteägare där identifierade risker diskuteras. Vidare rapportering till ledningsmöten sker därefter.

### 3.3.2. Bedömning och rekommendationer

De processer som finns kring incidenthantering bedöms fundera ändamålsenligt.

# *4. Revisionell bedömning*

***Revisionsfrågan för granskningen är:***

*Är kommunstyrelsens styrmodell för IT- och informationssäkerhet för att löpande identifiera prioriterade hot ändamålsenlig i förhållande till de prioriterade hoten?*

Efter genomförd revision och genomgång av samtliga kontrollmål är vår bedömning att kommunstyrelsens styrmodell för IT- och informationssäkerhet för att löpande identifiera prioriterade hot ej 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*<br>*Lena Salomon* | *Projektledare*<br>*Viktor Bergvall* |

# *Appendix 1: Bedömning av uppfyllnads-grad*

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

| **Revisionsmoment** | **Växjö kommun** |
|---|---|
| **Moment 1**<br>*Riskanalys kopplat till område för IT-och informationssäkerhet finns?* | Uppfyllt |
| **Moment 2**<br>*Styrande dokument för IT- och informationssäkerhet samt kommunikationsplan är upprättat?* | Delvis uppfyllt |
| **Moment 3**<br>*Att organisationen, roller, ansvarsfördelning och rapporteringsvägar i frågor rörande IT- och informationssäkerhet är tydlig.* | Delvis uppfyllt |
| **Moment 4**<br>*Att det finns ändamålsenliga rutiner för att hantera risker relaterade till prioriterade hot inom område för IT- och informationssäkerhet.* | Delvis uppfyllt |
| **Moment 5**<br>*Att tekniska försvarsmekanismer och processer uppdateras utifrån lärdom av inträffade säkerhetsincidenter.* | Uppfyllt |
| **Moment 6**<br>*Finns det en tydlig plan för att upprätthålla och återställa verksamhetskritiska funktioner vid tillfälle för en säkerhetsincident?* | Ej uppfyllt |