www.pwc.se

Revisionsrapport

Granskning av intrångsskydd

Enköpings kommuns förtroendevalda revisorer

Niklas Ljung
Mattias Gröndahl

December 2018

pwc

Innehåll

Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Enköpings kommun genomfört en granskning av det externa och interna intrångsskyddet hos Enköpings kommun.

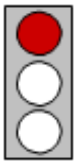
Revisionsfrågan som har varit styrande för granskningen har formulerats enligt följande:

Har kommunstyrelsen säkerställt att Enköpings kommuns nuvarande tekniska IT-säkerhet är tillräcklig och tillfredsställande för att reducera risker för obehörigt intrång till en acceptabel nivå?

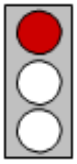
Efter genomförd granskning är vår sammanfattande bedömning att kommunstyrelsen **ej har säkerställt** att Enköpings kommuns nuvarande tekniska IT-säkerhet är tillräcklig och tillfredsställande för att reducera risker för obehörigt intrång till en acceptabel nivå.

Den sammanfattande bedömningen baseras på bedömningarna av de sex kontrollfrågorna för granskningen, vilka redovisas i rapporten.

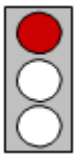
Kontrollfråga 1
Finns tillräckliga verktyg och processer för att upptäcka en eventuell attack och är de implementerade och fungerar de på ett tillfredsställande sätt?



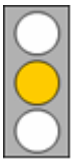
Kontrollfråga 2
Hanteras icke önskvärda incidenter på ett ändamålsenligt sätt?



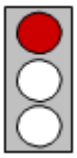
Kontrollfråga 3
Hur är säkerheten avseende intrång av extern och intern aktör?



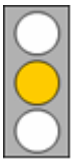
Kontrollfråga 4
Finns det en tydlig roll- och ansvarsfördelning i frågor kring den övergripande IT-säkerheten?



Kontrollfråga 5
Finns det kända och tillämpade styrande dokument och riktlinjer för kommunens förebyggande arbete kring IT-säkerhet?



Kontrollfråga 6
Finns det kända och tillämpade styrande dokument och riktlinjer att följa vid uppmärksammandet av risker eller ett intrång?



1. Inledning

1.1. Granskningsbakgrund

Revisorerna har uppmärksammat att risker och hot från det framväxande digitala landskapet, s.k. cyberrisker, får ökande uppmärksamhet från både företag och myndigheter. Detta främst orsakat av de senaste årens snabba digitala utveckling med följande exponering mot internet samt ökad användning av smartphones och andra bärbara enheter hos medarbetare, både privat och i yrkeslivet. Ökad aktivitet bland kriminella och andra antagonistiska aktörer bidrar också starkt till den växande hotbilden.

Man har från såväl näringsliv som offentlig sektor insett att den hot- och riskbild som växer fram behöver tolkas och göras begriplig så att relevanta och balanserade motåtgärder kan vidtas. I grund och botten handlar det om behovet att skydda sig mot angripare som oavbrutet arbetar för att hitta nya vägar att stjäla, förstöra eller på annat sätt manipulera informationstillgångar eller informationsinfrastruktur.

Revisorerna har i sin riskanalys för 2018 bedömt att det finns en risk att kommunstyrelsen inte har säkerställt att den tekniska IT- säkerheten är tillfredsställande gällande obehörigt intrång och har därför gett PwC ett uppdrag att granska området.

1.2. Syfte och revisionsfråga

Granskningen syftar till att besvara följande revisionsfråga:

Har kommunstyrelsen säkerställt att Enköpings kommuns nuvarande tekniska IT-säkerhet är tillräcklig och tillfredsställande för att reducera risker för obehörigt intrång till en acceptabel nivå?

1.2.1. Kontrollfrågor

Följande kontrollfrågor har använts vid granskningen för att besvara revisionsfrågan:

- Finns tillräckliga verktyg och processer för att upptäcka en eventuell attack och är de implementerade och fungerar de på ett tillfredsställande sätt?
- Hanteras icke önskvärda incidenter på ett ändamålsenligt sätt?
- Hur är säkerheten avseende intrång av extern och intern aktör?
- Finns det en tydlig roll- och ansvarsfördelning i frågor kring den övergripande IT-säkerheten?
- Finns det kända och tillämpade styrande dokument och riktlinjer för kommunens förebyggande arbete kring IT-säkerhet?
- Finns det kända och tillämpade styrande dokument och riktlinjer att följa vid uppmärksammandet av risker eller ett intrång?

1.3. Revisionskriterier

Revisionskriterierna utgörs av nedanstående:

- Kommunallagen
- IT-styrdokument

1.4. Avgränsning

Granskningen avgränsas till granskningens kontrollfrågor, samt till att testerna utförs både från utsidan och från insidan. I tid avgränsas granskningen till år 2018

1.4.1. Nominerade system

Alla system på Enköpings kommuns interna samt externa nätverk ansågs vara nominerade system och således inom ramen för tekniska tester.

1.5. Metod

Granskningen har genomförts genom intrångstester, dokumentstudier av för granskningen relevanta dokument samt telefon- och mailkontakt.

De externa testerna har utförts som en så kallad blackbox-pentest där endast domänadress anges, all övrig information anskaffas under testernas gång.

Intrångstesterna genomfördes i tre moment.

- Informationsinsamling - Nätverk, system och rutiner kartläggs i möjligaste mån. Kritiska system och data identifieras för att möjliggöra en värdering av sårbarhetens potential, det vill säga komplexitet i relation till förmodad skada.
- Tekniska tester - Sårbarheter eftersöks på de system som identifierats och de som upptäcks används för att tillskansa sig utökade användarrättigheter och för att utläsa känslig information.
- Rapportering - Bedömningar och insamlat material från de två tidigare momenten sammanställs och utvärderas. Intrångstester, beskrivningar av sårbarheter och slutsatser sammanställs i en rapport.

Dokumentgranskningen genomfördes i två moment.

- Dokumentationsinsamling - Insamling av den dokumentation som Enköpings kommun har och som är relevant för granskningen.
- Dokumentgranskning - Övergripande genomgång av den tillgängliga dokumentationen för att bilda sig en uppfattning om huruvida denna är uppdaterad och löpande revideras enligt god praxis.

Telefon- och mailkontakt samt intervju har genomförts med:

- Anette Lindberg, Informationssäkerhetsstrateg i Enköpings kommun
- Patrik Nyström, IT- och teleservice i Enköpings kommun

2. Resultat

2.1. Intrångstester

2.1.1. Iakttagelser

Konsulter från PwC kunde på relativt kort tid anskaffa sig högsta behörighet i den interna IT-miljön. Det påvisades två skilda angreppssätt där full kontroll av kommunens IT-miljö kunde anskaffas. Angreppen som genomfördes är av enkel karaktär och kan genomföras av en mindre sofistikerad angripare utan kunskap om IT-miljön.

Flera angrepp genomfördes under testerna men detekterades inte av IT-avdelningen, detta tyder på att det saknas förmåga samt verktyg att identifiera angrepp i den interna IT-miljön.

Den nuvarande lösenordspolicyn har brister.

Under testerna påträffades en större mängd konton med domänadministratörsrättigheter. Att ha så många konton med dessa rättigheter är mycket riskabelt och ökar en angripares chanser att erhålla högsta möjliga behörigheter i miljön.

PwC kunde under testerna anskaffa sig högsta behörighet i IT-miljön vilket innebär, i stort sett, full kontroll över IT-miljön. Det bör noteras att detta angrepp är att anse som ytterst kritiskt och har ett utfall som vid ett realistiskt angrepp skulle kunna leda till mycket omfattande skador, då en angripare bland annat skulle kunna extrahera känslig information, låsa ute systemanvändare från resurser samt kryptera viktiga filer.

2.1.2. Bedömning

PwC:s slutsats efter intrångstesterna är att kontrollfrågorna rörande IT-säkerhet **ej är uppfyllda**.

PwC:s bedömning är att Enköpings kommuns IT-miljö har en del brister som kan utnyttjas av en angripare.

2.2. Granskning av dokumentation och rutiner

2.2.1. Iakttagelser

PwC fick ta del av en del dokument rörande informationssäkerhet och merparten av dessa bedömdes hålla en god nivå.

Under intervjuerna framkom att det är IT-chefen som har det högsta ansvaret för kommunens IT-säkerhet men det saknas dokumentation och rutiner kopplade till arbetet med IT-säkerhet. Även roll- och ansvarsfördelning i organisationen för IT-säkerhetsfrågor saknas eller är bristfälliga.

2.2.2. *Bedömning*

PwC:s slutsats efter granskning av dokumentation och rutiner är att kontrollfrågorna kopplade till dokumentation och rutiner **ej är uppfyllda**.

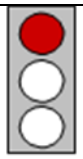
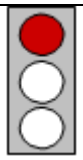
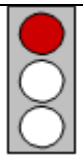
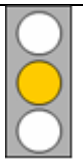
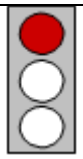
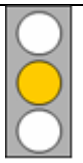
PwC:s bedömning är att Enköpings kommun har en del på plats som rör informationssäkerhet men det finns brister i roll och ansvarsfördelning för IT-säkerhet och det brister i dokumentation, policy och riktlinjer för IT-säkerhet.

3. Bedömningar

3.1. Revisionell bedömning

Efter genomförd granskning är PwC:s sammanfattande bedömning att Enköpings kommunstyrelse **ej har säkerställt** att Enköpings kommuns nuvarande tekniska IT-säkerhet är tillräcklig och tillfredsställande för att reducera risker för obehörigt intrång till en acceptabel nivå.

3.2. Bedömning utifrån kontrollfrågor

Kontrollfrågor	*Bedömning*
Finns tillräckliga verktyg och processer för att upptäcka en eventuell attack och är de implementerade och fungerar de på ett tillfredsställande sätt?	 IT-enheten saknar verktyg och förmåga att detektera intrång om IT-miljön blir angripen.
Hanteras icke önskvärda incidenter på ett ändamålsenligt sätt?	 Enköping har muntliga rapporteringsvägar men ingen dokumenterad process att följa vid en incident.
Hur är säkerheten avseende intrång av extern och intern aktör?	 IT-säkerheten håller inte en tillräckligt hög nivå och detta område behöver prioriteras för att minimera framtida incidenter. PwC kunde anskaffa sig högsta behörighet i domänen.
Finns det en tydlig roll- och ansvarsfördelning i frågor kring den övergripande IT-säkerheten?	 Det finns ett uttalat ansvarstagande från IT-chefen men det brister i roll- och ansvarsfördelning i verksamheten.
Finns det kända och tillämpade styrande dokument och riktlinjer för kommunens förebyggande arbete kring IT-säkerhet?	 Nej.
Finns det kända och tillämpade styrande dokument och riktlinjer att följa vid uppmärksammandet av risker eller ett intrång?	 Enköping har en del styrande dokument som gäller informationssäkerhetsincidenter och det är bra, men det brister i övrigt.

3.3. Rekommendationer

Utifrån genomförd granskning lämnas följande rekommendationer.

3.3.1. Rekommendationer efter genomförda intrångstester

Följande är rekommenderade förslag på åtgärder och syftar till att förbättra IT-säkerheten långsiktigt för att höja IT-säkerheten.

- Förbättra nuvarande lösenordspolicy och se över rutinen för hantering av konton och lösenord.
- Minska antalet konton med domänadministratörsrättigheter till ett fåtal.
- Förbättra nätverksarkitekturen så att nätverkssegmentering tillämpas i större utsträckning och begränsa nätverksåktomsten ytterligare.
- Stark autentisering på samtliga externa exponerade inloggningsportaler.
- Se över förmågan att upptäcka och förhindra intrång (detektionsförmåga). Konfigurera automatiska larm för säkerhetsloggar som avviker från normalt användarbeteende. Överväg att implementera system för att upptäcka säkerhetsincidenter.
- Förbättra skyddet och säkerheten även för mobila enheter som tex mobiler och Ipads.
- Starta ett IT-säkerhetsforum som involverar tekniker, systemägare, informationssäkerhet strateg och andra delar av organisationen för att tillsammans driva IT-säkerhetsområdet framåt.

3.3.2. Rekommendationer efter genomförd dokumentation och rutingranskning

- PwC rekommenderar att Enköpings kommun genomför en genomgång av styrande IT-dokument för att få en bild av vad som saknas i dokumentationsväg samt vad som behöver revideras.
- Vidare rekommenderar PwC att en årlig revidering av dokumentationen införs samt att man ser till att ägare, datum, versionsnummer samt versionshistorik finns med i all dokumentation. Detta för att man enkelt ska kunna se om informationen är relevant eller ej.
- Kommunen bör ta fram övergripande uppdragsbeskrivning för IT-enheten samt korrekta och uppdaterade rolbeskrivningar för IT-enhetens personal.

2018-12-11

	Niklas Ljung
_____	_____
Uppdragsledare	*Projektledare*