



Kommunfullmäktige

Revisionsrapport – Uppföljning IT-säkerhetsgranskning

Förslag till beslut

Förslag till kommunfullmäktige

Revisionsrapporten skickas till kommunstyrelsen för beredning.

Beskrivning av ärendet

Enligt det reglemente för revisionen som antagits av kommunfullmäktige 4 mars 2019 paragraf 21 (KS2018/879) ska kommunfullmäktige löpande behandla revisionens granskningar. Fullmäktige ska också besluta om när svar ska vara inkomna och ta ställning till om svaren är tillräckliga.

Detta innebär att när revisorerna överlämnat sin granskning till kommunen så ska rapporten formellt väckas i kommunfullmäktige. Detta sker vanligtvis vid närmast följande sammanträde. Sedan skickas revisionsrapporten för beredning för att kommunstyrelsen och berörda nämnder ska få möjlighet att yttra sig över och dra lärdom av rapporten. När ett svar på rapporten är sammanställt och berett av kommunstyrelsen kommer det åter till fullmäktige. Där kan svaret debatteras av kommunfullmäktige och, under förutsättning att man är nöjd med svaret, läggas till handlingarna.

Rolf Carlsson
Kommunfullmäktiges ordförande
Enköpings kommun

Uppföljande granskning av kommunens IT-säkerhet

PwC genomförde på uppdrag av de förtroendevalda revisorerna i Enköpings kommun 2019 en granskning av kommunens IT-säkerhet. I granskningen påvisades en del brister som nu PwC på uppdrag av Enköpings kommunrevisorer genomfört en uppföljningsgranskning på. Syftet är att utreda huruvida kommunstyrelsen har säkerställt att brister från IT-säkerhetsgranskningen 2019 har omhändertagits av IT-organisationen. Resultatet av granskningen redovisas i bifogad rapport.

Den sammanfattande bedömningen är att kommunstyrelsen **inte helt** har säkerställt att brister från IT-säkerhetsgranskningen 2019 har omhändertagits av IT-organisationen. Det är positivt att se att mycket har hänt sedan den tidigare granskningen 2019 även om det fortfarande finns brister och allt inte är på plats eller helt implementerat. Att kommunen nu har tillgång till kraftfulla verktyg för att möjliggöra att ett intrång eller annan onormal aktivitet kan upptäckas och spåras är glädjande.

Efter genomförd granskning rekommenderar vi kommunstyrelsen:

- Säkerställa att den vakanta rollen som informationssäkerhetschef tillsätts. Rollen bör vara centralt placerat för att kunna agera kravställare mot både verksamhet och IT-organisation.
- Säkerställa att IT-organisationen bedriver ett strukturerat IT-säkerhetsarbete bl.a. med hjälp av en IT-säkerhetssamordnare som håller ihop IT-organisationens IT-säkerhetsarbete.
- Säkerställa att IT-organisationen tar fram och löpande reviderar, IT-strategier, policy, regelverk, instruktioner och annan IT-relaterad dokumentation.
- Säkerställa att informationssäkerhetsorganisationen tar fram övergripande riktlinjer för lösenord och kontohantering. Säkerställ att det läggs stor vikt på konton med särskilda rättigheter samt att det införs rutiner för att löpande revidera befintliga konton.
- Tar fram en långsiktig plan för hur IT-organisationen ska arbeta med att öka säkerheten i kommunens infrastruktur och nätverkssegmentering (både internt och mot kommunens dotterbolag).

Kommunfullmäktige

Revisorerna översänder rapporten för kännedom och åtgärd. Revisorerna önskar även svar från kommunstyrelsen baserat på de iakttagelser och rekommendationer som redovisas i rapporten.

För Enköpings kommuns revisorer

Tony Forsberg
Ordförande

Bengt-Åke Gelin
vice ordförande

För kännedom:

Kommunstyrelsen
Bolagsstyrelserna i de kommunala bolagen

Granskning – Uppföljning IT- säkerhets- granskning

Enköpings kommun

Datum 2020-11-27

Projektledare

Niklas Ljung

Projektmedarbetare

Joakim Wiklund



Innehållsförteckning

1.	Inledning	5
2.	Revisionsfrågor	6
3.	Revisionell bedömning	10
4.	Rekommendationer	11
5.	Bilagor	12

Sammanfattning

PwC genomförde på uppdrag av de förtroendevalda revisorerna i Enköpings kommun 2019 en granskning av kommunens IT-säkerhet. Under genomförd granskning uppdagades en del brister som Enköpings kommunrevisorer nu vill att PwC ska genomföra en uppföljningsgranskning på.

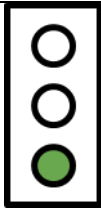
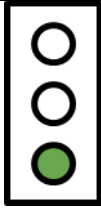
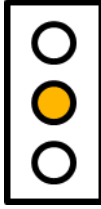
Syftet är att utreda huruvida kommunstyrelsen har säkerställt att brister från IT-säkerhetsgranskningen 2019 har omhändertagits av IT-organisationen.

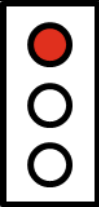
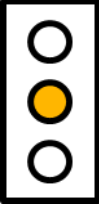
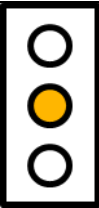


PwC:s revisionella bedömning är att kommunstyrelsen **inte helt** har säkerställt att brister från IT-säkerhetsgranskningen 2019 har omhändertagits av IT-organisationen.

Det är positivt att se att mycket har hänt sedan den tidigare granskningen 2019 även om det fortfarande finns brister och allt inte är på plats eller helt implementerat.

Att kommunen nu har tillgång till kraftfulla verktyg för att möjliggöra att ett intrång eller annan onormal aktivitet kan upptäckas och spåras är glädjande.

Bedömning av granskningens revisionsfrågor

Revisionsfråga	Kommentar	
Revisionsfråga 1 Finns verktyg och processer implementerade för att möjliggöra upptäckten av en eventuell attack?	Uppfyllt IT-organisationen har tagit ett stort kliv sedan senaste revisionen och har nu de tekniska förutsättningarna att upptäcka, analysera och förhindra ett intrång.	
Revisionsfråga 2 Finns en implementerad och dokumenterad incidentprocess att följa vid en IT-relaterad incident?	Uppfyllt IT-organisationen har ett utpekat ansvar för incidenthanteringsprocessen och en rutin för hur och av vem den ska tillämpas.	
Revisionsfråga 3 Finns en adekvat lösenordspolicy implementerad?	Delvis uppfyllt Arbetet med att implementera den nya lösenordspolicyn pågår, men det återstår en del områden och det finns fortfarande brister.	

<p>Revisionsfråga 4</p> <p>Finns en adekvat mängd konton med domänadministratörsrättigheter?</p>	<p>Ej uppfyllt</p> <p>Domänadministratörskonton används felaktigt och är för många. Dessa ska inte vara personliga och aldrig tillsammans med inställningen password never expire.</p>	
<p>Revisionsfråga 5</p> <p>Finns ett adekvat skydd för kommunens mobila enheter implementerat?</p>	<p>Delvis uppfyllt</p> <p>Det finns en förståelse och en grundnivå är satt med MobileIron, men man behöver gå längre för att säkra upp sina mobila enheter.</p>	
<p>Revisionsfråga 6</p> <p>Finns ett löpande arbete med att öka nätverkssegmenteringen i kommunens nät?</p>	<p>Delvis uppfyllt</p> <p>Det saknas ett strukturerat och långsiktigt arbete med att höja nätverkssegmenteringen.</p>	
<p>Revisionsfråga 7</p> <p>Revideras IT-relaterad dokumentation löpande?</p>	<p>Ej uppfyllt</p> <p>Det föreligger brister i IT-dokumentationen.</p>	
<p>Revisionsfråga 8</p> <p>Bedrivs ett strukturerat IT-säkerhetsarbete i Enköpings kommun?</p>	<p>Ej uppfyllt</p> <p>Det saknas ett strukturerat IT-säkerhetsarbete.</p>	

Rekommendationer

- Säkerställ att kommunen har en informationssäkerhetschef som är kravställare på både verksamhet och IT-organisation.
- När säkerhetshöjande åtgärder genomförs och dessa påverkar kommunmedarbetaren säkerställ att information och budskap i första hand kommer från säkerhetsorganisationen och inte från IT-organisationen.
- Inför en roll som agerar IT-säkerhetsamordnare på IT-enheten och som ansvarar för IT-säkerhetsarbetet.
- Strukturera arbetet med de nya IT-säkerhetsverktygen, Vectra, Logpoint och AD-audit samt peka ut ansvaret till ett par personer/verktyg för att på detta vis sprida kunskapen.
- Färdigställ arbetet med lösenordspolicyn.
- Ta fram en ny modell för hur Enköpings kommun arbetar med konton med särskilda rättigheter, ta hjälp av en vedertagen standard för att få vägledning, t ex CIS.
- Tillåt inga personliga domänadministratörskonton med *password never expire*.
- Avlägsna alla personliga domänadministratörskonton.
- Genomför en genomgång av alla konton med administratörrättigheter.
- Ta fram en långsiktig strategi för hur Enköpings kommun ska arbeta med kommunens infrastruktur och nätverkssegmentering.
- Säkerställ att IT-organisationen har resurser att göra sin del i arbetet med den nya förvaltningsmodellen samt med all tillhörande dokumentation.

1. Inledning

1.1. Bakgrund

PwC genomförde på uppdrag av de förtroendevalda revisorerna i Enköpings kommun år 2019 en granskning av kommunens IT-säkerhet. Under genomförd granskning uppdagades en del brister som Enköpings kommunrevisorer nu vill att PwC ska genomföra en uppföljningsgranskning på.

En fungerande IT-säkerhet är av stor betydelse för Enköpings kommuns verksamhet. Den moderna informationsteknologin ger möjligheter att höja kvalitet, säkerhet och effektivitet i de olika verksamheterna samt sprida och öka tillgängligheten till information. IT är en förutsättning för att verksamheten ska fungera på ett effektivt och säkert sätt. Rörligheten bland IT-användare är stor och önskan om tillgång till IT-tjänster från allmänhet och medarbetare ökar. Den snabba utvecklingen av tekniken innebär att det ständigt uppkommer nya risker som måste beaktas.

Revisorerna har i sin riskanalys för år 2020 bedömt att det finns en risk att kommunstyrelsen inte har säkerställt att kommunens IT-organisation har åtgärdat tidigare påpekade brister.

1.2. Syfte och revisionsfrågor

Syftet är att utreda huruvida kommunstyrelsen har säkerställt att brister från IT-säkerhetsgranskningen år 2019 har omhändertagits av IT-organisationen.

1. Finns verktyg och processer implementerade för att möjliggöra upptäckten av en eventuell attack?
2. Finns en implementerad och dokumenterad incidentprocess att följa vid en IT-relaterad incident?
3. Finns en adekvat lösenordspolicy implementerad?
4. Finns en adekvat mängd konton med domänadministratörsrättigheter?
5. Finns ett adekvat skydd för kommunens mobila enheter implementerat?
6. Finns ett löpande arbete med att öka nätverkssegmenteringen i kommunens nät?
7. Revideras IT-relaterad dokumentation löpande?
8. Bedrivs ett strukturerat IT-säkerhetsarbete i Enköpings kommun?

1.3. Revisionskriterier

- Kommunallagen
- IT-styrdokument
- IT-teknisk dokumentation

1.4. Avgränsning

I tid avgränsas granskningen till år 2020 och till granskningens revisionsfrågor, samt till Enköpings kommunnät. Kommunbolag inkluderas inte i granskningen.

I övrigt se revisionsfrågorna ovan.

1.5. Metod

Granskningen genomförs med hjälp av:

- PwC:s tekniska koncept Baseline Security Assessment,
- intervjuer med relevanta personer,
- kontroll av relevant dokumentation,
- genomgång av systemuppsättning genom utläsning och analys av kontoinformation i Active Directory.

2. Revisionsfrågor

2.1. Revisionsfråga 1: Finns verktyg och processer implementerade för att möjliggöra upptäckten av en eventuell attack?

2.1.1. Iakttagelser

Vid föregående granskning upptäcktes inte det intrång som gjordes i samband med penetrations-testning. Sedan dess har Vectra, LogPoint och AD-audit införskaffats. Detta har medfört att kommunen idag har en större möjlighet att upptäcka eventuella attacker och att kunna se vad som händer i systemen.

Vectra är ett verktyg som är en AI-driven nätverksdetektering av attacker och onormala nätverksaktiviteter. Vectra är implementerat och i drift hos IT-avdelningen.

Tekniker har genomgått kurser och man har fått hjälp av leverantören med att konfigurera systemet. Det finns fortfarande utrymme för intrimning men verktyget är ett stöd i det dagliga IT-säkerhetsarbetet.

LogPoint är en SIEM-lösning. Även denna produkt är uppsatt men här finns det ett större behov att anpassa och konfigurera för att verktyget ska ge maximal nytta.

AD-audit är ytterligare ett verktyg som nu är på plats sedan den tidigare granskningen genomfördes, detta verktyg övervakar AD:t (Active Directory) kontinuerligt och flaggar eventuella händelser som rör AD:t.

IT-organisationen har utifrån den senaste revisionen arbetat för att sätta både system och arbets-sätt. Inga hot har hittats men underliga händelser har flaggats upp och omhändertagits. Det pågår ett arbete med arbetssätt och rutiner för att följa upp och jobba med pushnotiser. De nya rutinerna ska ingå i arbetsbeskrivningen för två dedikerade personer som ska följa upp och ansvara för uppföljningen.

Vidare vill man införa ett utpekat ansvarsområde för respektive verktyg samt genomföra utbildning av några personer för att bredda kompetensen och lättare förstå vad som har hänt.

2.1.2. Bedömning

PwC:s bedömning är att revisionsfråga 1 är **uppfylld**.

IT-organisationen har tagit ett stort kliv sedan senaste revisionen och har nu de tekniska förutsättningarna att upptäcka, analysera och förhindra ett intrång.

2.2. Revisionsfråga 2: Finns en implementerad och dokumenterad incidentprocess att följa vid en IT-relaterad incident?

2.2.1. Iakttagelser

Det finns en incidentprocess som ska följas vid en incident.

Ansvaret för incidentprocessen ligger på IT-supportchefen och processen är knuten till servicedesk. När en användare rapporterar in ett ärende eller incident gör servicedeskpersonalen en bedömning om det är ett vanligt supportärende eller om detta ska rapporteras som en incident.

Det finns två scenarier för servicedesk att följa, hantering utav en incident och hantering utav en kritisk incident.

2.2.2. Bedömning

PwC:s bedömning är att revisionsfråga 2 är **uppfylld**.

IT-organisationen har ett utpekade ansvar för incidentprocessen och en rutin för hur och av vem den ska tillämpas.

2.3. Revisionsfråga 3: Finns en adekvat lösenordspolicy implementerad?

2.3.1. Iakttagelser

Det finns en uppdaterad policy framtagen sen senaste granskningen. Den nya policyn säger att det ska vara tolv tecken, giltigt i 120 dagar, 3 & 4 i komplexitet och går inte att återanvända.

Arbetet med att implementera lösenordspolicyn på alla användare pågår. Man har kommit relativt långt och man har ett strukturerat angreppssätt. Dock finns det fortfarande användargrupper som har kvar den gamla standarden.

Det finns fortfarande brister i lösenordspolicyn. Exempelvis är Lockout inte aktiverat.

Bedömningen är att man relativt snart kan slutföra stora delar utav förändringsarbetet med lösenordspolicyn.

2.3.2. Bedömning

PwC:s bedömning är att revisionsfråga 3 **delvis uppfylld**.

Arbetet med att implementera den nya lösenordspolicyn pågår men det återstår en del områden och det finns fortfarande en del brister. Men man är på god väg att höja säkerheten.

2.4. Revisionsfråga 4: Finns en adekvat mängd konton med domänadministratörsrättigheter?

2.4.1. Iakttagelser

Det finns totalt 27 domänadministratörskonton vilket fortfarande är för många för en kommun av Enköpings storlek. Den stora bristen är framförallt att 8 av dessa konton är personliga konton varav 6 har *password never expire* påslaget. Detta ses som en stor säkerhetsrisk.

Eftersom domänadministratörskonton är de konton som har de högsta rättigheterna i domänen är rekommendationen att dessa konton inte ska vara personliga. Lösenorden till dessa konton ska vara långa, komplexa och autogenererade.

Att IT-organisationen fortfarande har dessa personliga konton tyder på att man har brister i policy och rutiner för konton med särskilda rättigheter.

Det kan konstateras att användningen av konton med särskilda rättigheter, administratörskonton och domänkonton inte används ändamålsenligt och med sparsamhet.

2.4.2. Bedömning

PwC:s bedömning är att revisionsfråga 4 **ej är uppfylld**.

Domänadministratörskonton används felaktigt och är för många. Dessa ska inte vara personliga och aldrig tillsammans med inställningen *password never expire*.

2.5. Revisionsfråga 5: Finns ett adekvat skydd för kommunens mobila enheter implementerat?

2.5.1. Iakttagelser

Samtliga mobila enheter har MobileIron som standard och de tillhör ett accessnät och inte det vanliga infrastrukturnätet. Enheterna har inte behörighet till de interna systemen.

Det finns ett arbete och en intern förståelse på IT-enheten för vikten att ytterligare höja säkerheten på de mobila enheterna, eftersom mycket av skadlig kod i dag finns i våra mobila enheter. Dock saknas en konkret plan och strategi. Det saknas också finansiering för det fortsatta arbetet.

Generellt har IT-organisationen ett lågt stöd från ledningen för arbetet med säkerheten på mobila enheter.

2.5.2. Bedömning

PwC:s bedömning är att revisionsfråga 5 är **delvis uppfylld**.

Det finns en förståelse och en grundnivå är satt med MobileIron, men man behöver gå längre för att säkra upp sina mobila enheter.

2.6. Revisionsfråga 6: Finns ett löpande arbete med att öka nätverkssegmenteringen i kommunens nät?

2.6.1. Iakttagelser

Sedan föregående granskning gjordes har inte särskilt mycket arbete lagts på att säkra upp och segmentera nätet ytterligare. Ett bristområde som fortfarande finns är kopplingen till kommunens dotterbolag.

I dag använder man brandväggar och VLAN för att segmentera nätet.

Det brister i kravställning från kommunens säkerhetsorganisation och informationssäkerhetsorganisation på kommunens infrastruktur.

Det pågår ej något långsiktigt arbete med hur kommunens nät och segment ska byggas upp och förändras för att kommunens ska höja säkerheten på denna punkt.

Det är positivt att se att kommunen har investerat i en ny roll, Change manager, för att komma till rätta med förändringar i miljön, vilket är ett led i att höja säkerheten. Det finns ett utkast på en framtiden changeprocess som ska säkerställa att arbetet fungerar.

2.6.2. Bedömning

PwC:s bedömning är att revisionsfråga 6 är **delvis uppfylld**.

Det saknas ett strukturerat och långsiktigt arbete med att höja nätverkssegmenteringen.

2.7. Revisionsfråga 7: Revideras IT-relaterad dokumentation löpande?

2.7.1. Iakttagelser

Ingen förändring har genomförts sedan senaste granskningen gjordes.

Det pågår ett arbete med att införa en ny förvaltningsmodell, det är en anpassad version utav PM3(EM3).

När den nya förvaltningsmodellen är implementerad kommer nästa steg att vara att få till all ny dokumentation vilket kommer medföra att det blir en systematisk dokumentation.

2.7.2. Bedömning

PwC:s bedömning är att revisionsfråga 7 **ej är uppfylld**.

Det föreligger brister i IT-dokumentationen.

2.8. Revisionsfråga 8: Bedrivs ett strukturerat IT-säkerhetsarbete i Enköpings kommun?

2.8.1. Iakttagelser

Det saknas ett strukturerat IT-säkerhetsarbete i kommunen. Det pågår en hel del säkerhetsrelaterat arbete, men man saknar strukturer och det saknas klassning utav information och system.

IT-organisationen saknar en IT-säkerhetssamordnare som håller ihop och synkroniserar allt säkerhetsarbete på IT-enheten samt agerar rådgivare mot verksamheter i dessa frågor.

Det saknas en tydlig kravställning på IT-organisationen både från informationssäkerhetsorganisationen och från verksamheten.

Enköpings kommun har idag en vakans för rollen som IT-strateg och informationssäkerhetschef och detta är en stor brist i det strukturerade IT-säkerhetsarbetet.

Att IT-organisationen i dag har fått flertalet nya verktyg är väldigt positivt och även att man vill få till mer struktur i hur och vem som arbetar systematiskt med dessa verktyg.

2.8.2. Bedömning

PwC:s bedömning är att revisionsfråga 8 **ej är uppfylld**.

Det saknas ett strukturerat IT-säkerhetsarbete.

3. Revisionell bedömning

PwC:s revisionella bedömning är att kommunstyrelsen **inte helt** har säkerställt att brister från IT-säkerhetsgranskningen 2019 har omhändertagits av IT-organisationen.

4. Rekommendationer

Utifrån genomförd granskning lämnas följande rekommendationer:

- Säkerställ att kommunen har en informationssäkerhetschef som är kravställare på både verksamhet och IT-organisation.
- När säkerhetshöjande åtgärder genomförs och dessa påverkar kommunmedarbetaren säkerställ att information och budskap i första hand kommer från säkerhetsorganisationen och inte från IT-organisationen.
- Inför en roll som agerar IT-säkerhetsamordnare på IT-enheten och som ansvarar för IT-säkerhetsarbetet.
- Strukturera arbetet med de nya IT-säkerhetsverktygen, Vectra, Logpoint och AD-audit samt peka ut ansvaret till ett par personer/verktyg för att på detta vis sprida kunskapen.
- Färdigställ arbetet med lösenordspolicyn.
- Ta fram en ny modell för hur Enköpings kommun arbetar med konton med särskilda rättigheter, ta hjälp av en vedertagen standard för att få vägledning, t ex CIS.
- Tillåt inga personliga domänadministratörskonton med password never expire.
- Avlägsna alla personliga domänadministratörskonton.
- Genomför en genomgång av alla konton med administratörsrättigheter.
- Ta fram en långsiktig strategi för hur Enköpings kommun ska arbeta med kommunens infrastruktur och nätverkssegmentering.
- Säkerställ att IT-organisationen har resurser att göra sin del i arbetet med den nya förvaltningsmodellen samt med all tillhörande dokumentation.

5. Bilagor

5.1. Bilaga 1 – Intervjuer

Intervjuer har genomförts med nedanstående roller.

Roll	Verksamhet
IT-driftchef	IT
Ansvariga brandväggar och portaler	IT
IT-koordinator & Change Manager	IT
IT-supportchef	IT
Ansvarig AD & mail	IT

2020-11-27

Anders Hägg
Uppdragsledare

Niklas Ljung
Projektledare

Denna rapport har upprättats av Öhrlings PricewaterhouseCoopers AB (org nr 556029-6740) (PwC) på uppdrag av Enköpings kommunrevisorer enligt de villkor och under de förutsättningar som framgår av projektplan från den 2020-08-24. PwC ansvarar inte utan särskilt åtagande, gentemot annan som tar del av och förlitar sig på hela eller delar av denna rapport.