Paragraf 139 Ärendenummer KS2021/102

Svar på revisionsrapport - Granskning - Uppföljning IT-säkerhetsgranskning

Förslag till kommunfullmäktiges beslut

Kommunstyrelsens svar till revisorerna anmäls och läggs till handlingarna

Kommunstyrelsens beslut

Kommunstyrelsen antar kommunledningsförvaltningens yttrande som sitt eget och överlämnar det till kommunfullmäktige och revisorerna.

Ärendet

Under november till december 2018 utförde PwC på uppdrag av revisorerna i Enköpings kommun en granskning av kommunens IT-säkerhet. Under hösten 2020 utförde PwC en uppföljningsrevision då kommunens revisorer ville försäkra sig om bristerna hade omhändertagits av IT-organisationen.

Att PwC:s revision gör bedömningen att man **inte helt** har åtgärdat alla brister kan Kommunledningsförvaltningen bara hålla med om men vi anser att vi är på god väg att och att det som återstår nästan helt kommer att kunna hanteras under 2021.

Kommunledningsförvaltningen tycker att det i stort är bra rekommendationer som framförs och att dessa ligger väl i linje med redan fattade beslut och påbörjat arbete. Några har redan åtgärdats och flera är planerade.

Nedan följer kommentarer för varje revisionsfråga som PwC ställt:

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

Ett stort arbete har genomförts för att vi ska kunna detektera och spåra intrångsförsök, lösningen har blivit så bra att den fått beröm av flera IT-säkerhetsspecialister som vi varit i kontakt med.

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

Arbete med att dokumentera våra redan existerande processer har gjorts, vi har också utvecklat nya processer för att höja säkerheten vid ändringshantering.

Revisionsfråga 3: Finns en adekvat lösenordspolicy implementerad?

Ett nytt regelverk för lösenordshantering i centralt hanterade system togs fram under 2019 första kvartal och stora delar fick dessa nya regler implementerade inom några månader. Vi har haft flera utmaningar, till exempel då lösenordshanteringen på vissa enheter inte stödjer lösenordsbyten på ett bra sätt. Avsaknad av självservice funktionen har också varit ett hinder för att kunna aktivera de sista reglerna. Vi har nu löst dessa problem och räknar med att kunna slutföra arbetet relativt snart.

Revisionsfråga 4: Finns en adekvat mängd konton med domänadministratörsrättigheter?

Den mätning som gjordes av PwC under hösten väckte en del funderingar inom IT-organisationen och det visade sig att man hade räknat antal konton med en parameter som inte per automatik återställs när kontor **inte längre** är ett domänadministratörskonto. Vad man egentligen räknade var antalet konton som någon gång varit domänadministratör men som inte nödvändigtvis fortfarande var det. Med andra ord så kan dessa konton delvis vara de samma som man hittade vid förra mätningen (2018) och som man då omedelbart hanterade. Värt att notera är dock att det fanns konton av den kategori som man här belyser även om dessa inte var så många som man presenterat i rapporten, dessa är nu åtgärdade och en rutin för hantering av domänadministratörs konton är under framtagande.

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

Även om ett stort arbete har genomfört inom detta område så återstår det mycket arbete för att få hanteringen och säkerheten av våra mobila enheter dit vi önskar. Det ökade behovet av distansarbete belyser verkligen behovet av säkra och tillförlitliga mobila enheter vilket gör att detta område är högt prioriterat inom IT-organisationen samtidigt som verksamheten inte riktigt verkar vara beredda att betala för säkerhet på mobila enheter.

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

Det är riktigt att det inte har gjort mycket för att öka nätverkssegmenteringen men när det inte finns en tydlig kravbild från verksamheten av vilken infrastruktur som behöver skyddas mer än övrig infrastruktur så blir arbetet endast en kvalificerad gissningslek. Det är och bör endast vara verksamheten som kan var kravställare

på vilken skyddsnivå deras information och system kräver. Kommunens säkerhetsorganisation, informationssäkerhetsorganisation och IT-organisation kan och bör aldrig ta ansvaret att vara kravställare för verksamhetenssystem utan bör endast vara stödjande och vägledande i dessa frågor. När verksamheten börjar ställa de krav som de förväntas göra kommer dessa hanteras inom ramen för systemförvaltningsmodellen EM3 (variant av PM3), vilket tillslut leder fram till förändringar av produktionsmiljön vilka i sin tur regleras av ändringshanteringsprocessen som nu har implementerats.

Revisionsfråga 7: Revideras IT-relaterad dokumentation löpande?

Att säga att inga IT-relaterad dokumentation uppdatering sker löpande vore att fara med osanning då alla systemförändringar ska dokumenteras och i många fall också gör det men säkert inne alla, detta räknar vi dock med att ändringsprocessen ska råda bot på. Införandet av EM3 (PM3) borgar också för att systemdokumentationen kommer att bli bättre vilket vi redan kan se trots att projektet inte är avslutat.

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

Det bedrivs idag inget tydligt strukturerat IT-säkerhetsarbete i Enköpings kommun men det pågår en hel del säkerhetsrelaterat arbete. Det saknas någon som har tid och kompetens att hålla ihop IT-säkerhetsarbete så att det kan ske på ett strukturerat och effektivt sätt.

Här följer reflektioner/åtgärder som planeras på de föreslagna rekommendationerna i samma ordning kommunens revisorer presenterar dessa i missivet.

Vilka krav som ställs på informationssäkerheten i verksamheten kan endast objektägarna (verksamhetscheferna) ansvara för. Objektägarna formulerar kraven i dialog med objektägare IT och informationssäkerhetsstrateg. Kansli och utredningsavdelningen har rekryterat en informationssäkerhetsstrateg för att stötta och säkerställa informationssäkerheten i kommunen.

IT- och digitaliseringsavdelningen saknar förnärvarande ekonomiska medel för att utöka sin organisation med en IT-säkerhetssammordnare. Det är också svårt att få fram tillräcklig med resurser för att bemanna alla förvaltningsobjekt i EM3 (PM3) på IT-sidan. En utredning av hur man kan lösa dessa bemanningsproblem kommer att initieras.

Det sker i dag en årlig internrevision med stöd av ISO 27001 vars syfte bland annat är att säkerställa att regelverk och strategiska dokument revideras. En dokumenthanteringsplan kommer att tas fram för att säkerställa att nödvändiga dokument finns och uppdateras periodiskt. Förvaltningsmodellen EM3 (PM3) kommer också att vara ett stort stöd i detta arbete.

Riktlinjer för lösenordshantering finns framtaget sedan snart två år och automatisk kontohantering (skapande och borttagning) finns sedan många år för den stora massan av konton. Det har funnits tekniska utmaningar som bromsat införandet av de ”nya” riktlinjerna men det ska nu vara löst så att den sista gruppen användare också kan få dessa. Det som nu ses över är rutin för hantering och återkommande granskning av de relativt få konton med särskilda rättigheter.

Att kontinuerligt jobba med att öka säkerheten i kommunens infrastruktur är en naturlig del av det dagliga arbetet (här kan vi t.ex. nämna att vi nu återgår till att ha ett fysiskt separerat förvaltningsnät från att vi under en tid haft ett logiskt separerat nät). Att ta fram en långsiktig plan för säkerheten i kommunens infrastruktur är ett naturligt steg efter att en ny IT-strategisk plan har tagits fram.

Digitaliseringschef Magnus Nideborn redogör för ärendet.

Kommunledningsförvaltningens förslag till kommunfullmäktiges beslut
Kommunstyrelsens svar till revisorerna anmäls och läggs till handlingarna

Kommunledningsförvaltningens förslag till kommunstyrelsens beslut
Kommunstyrelsen antar kommunledningsförvaltningens yttrande som sitt eget och överlämnar det till kommunfullmäktige och revisorerna.

Kommunstyrelsens arbetsutskotts beredning
Arbetsutskottet har berett ärendet den 8 juni 2021 och lämnat förslag till beslut.

Kommunstyrelsens arbetsutskotts förslag till kommunfullmäktiges beslut
Kommunstyrelsens svar till revisorerna anmäls och läggs till handlingarna

Kommunstyrelsens arbetsutskotts förslag till kommunstyrelsens beslut
Kommunstyrelsen antar kommunledningsförvaltningens yttrande som sitt eget och överlämnar det till kommunfullmäktige och revisorerna.

_____

Kommunledningsförvaltningen
Magnus Nideborn
0171-62 69 70
magnus.nideborn@enkoping.se

Kommunstyrelsen

Kommunstyrelsens svar på - Uppföljande granskning av kommunens IT-säkerhet

Förslag till beslut

Förslag till kommunfullmäktige
Kommunstyrelsens svar till revisorerna anmäls och läggs till handlingarna

Förslag till kommunstyrelsen
Kommunstyrelsen antar kommunledningsförvaltningens yttrande som sitt eget och överlämnar det till kommunfullmäktige och revisorerna.

Beskrivning av ärendet

Under november till december 2018 utförde PwC på uppdrag av revisorerna i Enköpings kommun en granskning av kommunens IT-säkerhet. Under hösten 2020 utförde PwC en uppföljningsrevision då kommunens revisorer ville försäkra sig om bristerna hade omhändertagits av IT-organisationen.

Att PwC:s revision gör bedömningen att man **inte helt** har åtgärdat alla brister kan Kommunledningsförvaltningen bara hålla med om men vi anser att vi är på god väg att och att det som återstår nästan helt kommer att kunna hanteras under 2021.

Kommunledningsförvaltningen tycker att det i stort är bra rekommendationer som framförs och att dessa ligger väl i linje med redan fattade beslut och påbörjat arbete. Några har redan åtgärdats och flera är planerade.

Nedan följer kommentarer för varje revisionsfråga som PwC ställt:

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

Ett stort arbete har genomförts för att vi ska kunna detektera och spåra intrångsförsök, lösningen har blivit så bra att den fått beröm av flera IT-säkerhetsspecialister som vi varit i kontakt med.

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

Arbete med att dokumentera våra redan existerande processer har gjorts, vi har också utvecklat nya processer för att höja säkerheten vid ändringshantering.

Revisionsfråga 3: Finns en adekvat lösenordspolicy implementerad?

Ett nytt regelverk för lösenordshantering i centralt hanterade system togs fram under 2019 första kvartal och stora delar fick dessa nya regler implementerade inom några månader. Vi har haft flera utmaningar, till exempel då lösenordshanteringen på vissa enheter inte stödjer lösenordsbyten på ett bra sätt. Avsaknad av självservice funktionen har också varit ett hinder för att kunna aktivera de sista reglerna. Vi har nu löst dessa problem och räknar med att kunna slutföra arbetet relativt snart.

Revisionsfråga 4: Finns en adekvat mängd konton med domänadministratörsrättigheter?

Den mätning som gjordes av PwC under hösten väckte en del funderingar inom IT-organisationen och det visade sig att man hade räknat antal konton med en parameter som inte per automatik återställs när kontor **inte längre** är ett domänadministratörskonto. Vad man egentligen räknade var antalet konton som någon gång varit domänadministratör men som inte nödvändigtvis fortfarande var det. Med andra ord så kan dessa konton delvis vara de samma som man hittade vid förra mätningen (2018) och som man då omedelbart hanterade. Värt att notera är dock att det fanns konton av den kategori som man här belyser även om dessa inte var så många som man presenterat i rapporten, dessa är nu åtgärdade och en rutin för hantering av domänadministratörs konton är under framtagande.

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

Även om ett stort arbete har genomfört inom detta område så återstår det mycket arbete för att få hanteringen och säkerheten av våra mobila enheter dit vi önskar. Det ökade behovet av distansarbete belyser verkligen behovet av säkra och tillförlitliga mobila enheter vilket gör att detta område är högt prioriterat inom IT-organisationen samtidigt som verksamheten inte riktigt verkar vara beredda att betala för säkerhet på mobila enheter.

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

Det är riktigt att det inte har gjort mycket för att öka nätverkssegmenteringen men när det inte finns en tydlig kravbild från verksamheten av vilken infrastruktur som behöver skyddas mer än övrig infrastruktur så blir arbetet endast en kvalificerad gissningslek. Det är och bör endast vara verksamheten som kan var kravställare på vilken skyddsnivå deras information och system kräver. Kommunens säkerhetsorganisation, informationssäkerhetsorganisation och IT-organisation kan och bör aldrig ta ansvaret att vara kravställare för verksamhetenssystem utan bör endast vara stödjande och vägledande i dessa frågor. När verksamheten börjar ställa de krav som de förväntas göra kommer dessa hanteras inom ramen för systemförvaltningsmodellen EM3 (variant av PM3), vilket tillslut leder fram till förändringar av produktionsmiljön vilka i sin tur regleras av ändringshanteringsprocessen som nu har implementerats.

Revisionsfråga 7: Revideras IT-relaterad dokumentation löpande?

Att säga att inga IT-relaterad dokumentation uppdatering sker löpande vore att fara med osanning då alla systemförändringar ska dokumenteras och i många fall också gör det men säkert inne alla, detta räknar vi dock med att ändringsprocessen ska råda bot på. Införandet av EM3 (PM3) borgar också för att systemdokumentationen kommer att bli bättre vilket vi redan kan se trots att projektet inte är avslutat.

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

Det bedrivs idag inget tydligt strukturerat IT-säkerhetsarbete i Enköpings kommun men det pågår en hel del säkerhetsrelaterat arbete. Det saknas någon som har tid och kompetens att hålla ihop IT-säkerhetsarbete så att det kan ske på ett strukturerat och effektivt sätt.

Här följer reflektioner/åtgärder som planeras på de föreslagna rekommendationerna i samma ordning kommunens revisorer presenterar dessa i missivet.

Vilka krav som ställs på informationssäkerheten i verksamheten kan endast objektägarna (verksamhetscheferna) ansvara för. Objektägarna formulerar kraven i dialog med objektägare IT och informationssäkerhetsstrateg. Kansli och utredningsavdelningen har rekryterat en informationssäkerhetsstrateg för att stötta och säkerställa informationssäkerheten i kommunen.

IT- och digitaliseringsavdelningen saknar förnärvarande ekonomiska medel för att utöka sin organisation med en IT-säkerhetssammordnare. Det är också svårt att få fram tillräcklig med resurser för att bemanna alla förvaltningsobjekt i EM3 (PM3) på IT-sidan. En utredning av hur man kan lösa dessa bemanningsproblem kommer att initieras.

Det sker i dag en årlig internrevision med stöd av ISO 27001 vars syfte bland annat är att säkerställa att regelverk och strategiska dokument revideras. En dokumenthanteringsplan kommer att tas fram för att säkerställa att nödvändiga dokument finns och uppdateras periodiskt. Förvaltningsmodellen EM3 (PM3) kommer också att vara ett stort stöd i detta arbete.

Riktlinjer för lösenordshantering finns framtaget sedan snart två år och automatisk kontohantering (skapande och borttagning) finns sedan många år för den stora massan av konton. Det har funnits tekniska utmaningar som bromsat införandet av de ”nya” riktlinjerna men det ska nu vara löst så att den sista gruppen användare också kan få dessa. Det som nu ses över är rutin för hantering och återkommande granskning av de relativt få konton med särskilda rättigheter.

Att kontinuerligt jobba med att öka säkerheten i kommunens infrastruktur är en naturlig del av det dagliga arbetet (här kan vi t.ex. nämna att vi nu återgår till att ha ett fysiskt separerat förvaltningsnät från att vi under en tid haft ett logiskt separerat nät). Att ta fram en långsiktig plan för säkerheten i kommunens infrastruktur är ett naturligt steg efter att en ny IT-strategisk plan har tagits fram.

Ulrika K Jansson
Kommundirektör
Enköpings kommun

Magnus Nideborn
Digitaliseringschef
Enköpings kommun

ENKÖPINGS KOMMUN 2020-12-15
Revisorerna

Kommunfullmäktige

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 informationssäkerhetchef 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).

ENKÖPINGS KOMMUN 2020-12-15
Revisorerna

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

pwc

Revisionsrapport

Innehållsförteckning

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.

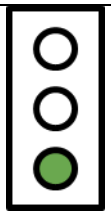
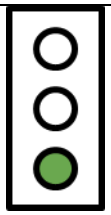
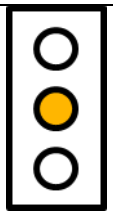
Syftet är att utreda huruvida kommunstyrelsen har säkerställt att brister från IT-säkerhetsgranskningen 2019 har omhändertagits av IT-organisationen.

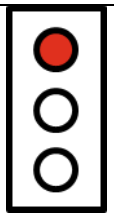
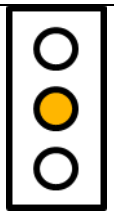
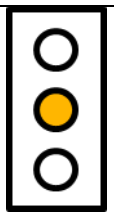
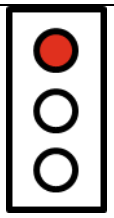
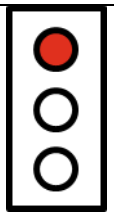
PwC:s revisionella bedömning är att kommunstyrelsen **inte helt** har säkerställt att brister från IT-säkerhetsgranskningen 2019 har omhändertagits av IT-organisationen.

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.	

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

Rekommendationer

- Säkerställ att kommunen har en informationssäkerhetchef 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.

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 kvalité, 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 penetrationstestning. 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 arbetssätt. 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 utpekat 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 informationssäkerhetorganisation 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 framtagen 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 informationssäkerhetchef 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.