GNESTA KOMMUN

2019-06-05

Revisionsskrivelse

Kommunstyrelsen

För kännedom
Kommunfullmäktige

Revisionsrapport: Granskning av teknisk IT-säkerhet och intrångsskydd

PwC har på uppdrag av de förtroendevalda revisorerna i Gnesta kommun genomfört en granskning av det interna intrångsskyddet. Revisionsfrågan som har varit styrande för granskningen har formulerats enligt följande: Har kommunstyrelsen säkerställt att Gnesta kommuns nuvarande tekniska IT-säkerhet är tillräcklig och tillfredsställande för att reducera risker för obehörigt intrång till acceptabel nivå?

Efter genomförd granskning är vår sammanfattande bedömning att kommunstyrelsen ej säkerställt att Gnesta 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. En sekretessbelagd detaljerad rapport med resultat från genomförd intrångstest har lämnats över till IT-chefen i Lindesbergs kommun för att ge kommunen möjlighet att omedelbart vidta säkerhetshöjande åtgärder.

Rekommendationer till Gnesta kommun efter granskningen är följande:

- att ansvarsområdet för IT-säkerhet tydliggörs inom hela kommunen.
- att kommunen uppdaterar sina policydokument samt upprättar de dokument som saknas enligt informationssäkerhetspolicyn.
- att man ser över sin förmåga att detektera och agera på incidenter och intrång.
- att man ser över och stärker sin lösenordspolicy.

Gjorda iakttagelser och bedömningar redovisas i bifogad rapport, som härmed överlämnas till kommunstyrelsen för svar och till fullmäktige för kännedom. Rapporten har behandlats och godkänts vid revisorernas möte 2019-06-05. Revisorerna önskar svar från kommunstyrelsen senast 20 september 2019.

REVISORERNA

Sune Åkerlind
Ordförande

Kjell Bernhardsson
Vice ordförande

Granskning av teknisk IT-säkerhet och intrångsskydd

Gnesta kommun

Juni 2019

Mikael Grönvik
Maricka Lundholm
Alexander Mattsson

pwc

Revisionsrapport

Innehållsförteckning

pwc

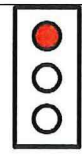
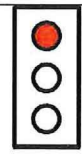
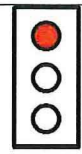
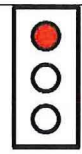
Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Gnesta kommun genomfört en granskning av det interna intrångsskyddet hos Gnesta kommun. Revisionsfrågan som har varit styrande för granskningen har formulerats enligt följande:

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

Efter genomförd granskning är vår sammanfattande bedömning att kommunstyrelsen **ej säkerställt** att Gnesta 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.

Kontrollmål	Bedömning
Hur upptäcks en eventuell attack?	
Hanteras icke önskvärda incidenter på ett ändamålsenligt sätt?	
Hur är säkerheten avseende intrång av interna aktörer?	
Finns en tydlig roll- och ansvarsfördelning i frågor kring den övergripande IT-säkerheten?	
Finns styrande IT-dokumentation på plats och revideras dessa regelbundet?	
Är befintlig dokumentation uppdaterad och löpande reviderad enligt god praxis?	

En sekretessbelagd detaljerad rapport med resultat från genomförd intrångstest har lämnats över till IT-chefen i Lindesbergs kommun för att ge kommunen möjlighet att omedelbart vidta säkerhetshöjande åtgärder. Rekommendationer till Gnesta kommun efter granskningen är följande:

- PwC rekommenderar att ansvarsområdet för IT-säkerhet tydliggörs inom hela kommunen.
- PwC rekommenderar att kommunen uppdaterar sina policydokument samt upprättar de dokument som saknas enligt informationssäkerhetspolicyn.
- PwC rekommenderar att man ser över sin förmåga att detektera och agera på incidenter och intrång.
- PwC rekommenderar att man ser över och stärker sin lösenordspolicy.

Inledning

Bakgrund

Av kommunallagen och god revisionssed följer att revisorerna årligen skall granska styrelser, nämnder och fasta fullmäktigeberedningar.

Kommunstyrelse och facknämnder skall förvalta och genomföra verksamheten i enlighet med fullmäktiges uppdrag, lagar och föreskrifter. För att fullgöra uppdraget måste respektive organ bygga upp system och verktyg för ledning, styrning, uppföljning, kontroll och rapportering samt säkerställa att dessa verktyg tillämpas på avsett sätt. En bristfällig styrning och kontroll kan riskera att verksamheten inte bedrivs och utvecklas på avsett sätt.

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 hot-bilden.

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 2019 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.

Syfte och Revisionsfråga/-or

Granskningen syftar till att besvara följande revisionsfråga:

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

Revisionskriterier

Revisionskriterierna utgörs av nedanstående:

- Kommunallagen
- Budget 2019
- IT-styrdokument

Kontrollmål

Följande kontrollfrågor har använts vid granskningen för att besvara revisionsfrågan:

- Hur upptäcks en eventuell attack?
- Hanteras icke önskvärda incidenter på ett ändamålsenligt sätt?
- Hur är säkerheten avseende intrång av interna aktörer?
- Finns en tydlig roll- och ansvarsfördelning i frågor kring den övergripande IT-säkerheten?
- Finns styrande IT-dokumentation på plats och revideras dessa regelbundet?
- Är befintlig dokumentation uppdaterad och löpande reviderad enligt god praxis?

Avgränsning

Revisionen avser att granska kommunstyrelsen och avgränsas till år 2019 samt till granskningens kontrollfrågor.

Nominerade system

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

Metod

Vid granskning av teknisk IT-säkerhet och intrångsskydd används PwC:s koncept Cybersecurity assessment. Detta koncept innebär genomgång av systemuppsättning och tekniska tester mot Gnesta kommuns IT-miljö. Genom en intern penetrationstest gås Gnesta kommuns tekniska miljö igenom och eventuella brister identifieras. Testerna utförs från insidan.

Faktiskt genomförande

Granskning av intrångsskydd hos Gnesta kommun har genomförts dels genom intrångstest och dels genom analys av kommunens dokumentation. Huruvida den för granskningen relevanta dokumentationen är uppdaterad och löpande revideras enligt god praxis har varit av särskilt intresse.

Intrångstestet har genomförts i följande delar:

- Informationsinsamling - nätverk, system och rutiner har kartlagts i möjligaste mån. Kritiska system och data har identifierats för att möjliggöra en värdering av sårbarhetens potential, det vill säga svårighetsgraden i intrångsförsöket i relation till den förmodade skadan.

- Tekniska tester - sårbarheter har eftersökts på identifierade system. Identifierade sårbarheter har använts i syfte att skapa utökade användarrättigheter och i förlängningen för att testa att utläsa känslig information.

- Rapportering - resultatet av informationsinsamlingen och de tekniska testerna har sammanställts och bedömts. Intrångstester, beskrivning av sårbarheter och slutsatser har sammanställts i en teknisk rapport som delas med Gnesta kommun.

Dokumentgranskning genomfördes i följande delar:

- Dokumentationsinsamling – insamling av den dokumentation som Gnesta kommun har och som var 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.

Intervjuer har genomförts med:

- IT-chef i Gnesta kommun
- IT-driftpersonal i Gnesta kommun
- IT-supportpersonal i Gnesta kommun

Iakttagelser

Hur upptäcks en eventuell attack?

Iakttagelser

Vid intervjuer framkom det att grupperingen för IT-drift har till uppgift att övervaka IT-miljön och vid ett eventuellt intrång eller annan form av attack, så ska detta eskaleras till IT-chefen. IT-driften utvärderar även intrånget i ett första skede för att få en tidig indikation på hur allvarlig incidenten är. IT-chefen har sedan i sin tur ansvar att kommunicera ut detta till de berörda.

Under intrångsgranskningen som PwC utfört så har ett fåtal attacker upptäckts via ett system som sedan larmat driftpersonalen om detta. Inom ramen för den granskning av intrångsskydd som PwC genomfört har Gnesta kommun meddelat att ett fåtal angrepp på IT-miljön har upptäckts.

Bedömning

Då Gnesta kommun endast har upptäckt ett fåtal av alla de angrepp som har utförts under granskningen så bedöms kontrollfrågan som **delvis uppfyllt.**

Hanteras icke önskvärda incidenter på ett ändamålsenligt sätt?

Iakttagelser

Enligt kommunens Informationssäkerhetspolicy som är fastställd november 2013, är hanteringen av informationen en viktig del i risk- och sårbarhetsanalyser samt att informationssäkerhet är en integrerad del av kommunens verksamhet.

Dokumentet redovisar även att alla som hanterar informationstillgångar ansvarar för att upprätthålla informationssäkerheten och ska rapportera incidenter som kan påverka säkerheten för kommunens informationstillgångar till systemägaren som sedan ansvarar för att rapportera vidare till informationssäkerhetssamordnaren. Kommunen har ingen informationssäkerhetssamordnare i dagsläget utan det är IT-chefen som tar på sig det ansvaret då formellt ansvar saknas. Kopplat till de tekniska tester som utförts inom ramen för granskningen har Gnesta kommun meddelat upptäckt av icke önskvärda incidenter till PwC.

Bedömning

Enligt Informationssäkerhetspolicyn är det informationssäkerhetssamordnaren som ansvarar för hanteringen av incidenter, och Gnesta kommun har i dagsläget ingen som formellt innehar den rollen. IT-chefen fick under granskningen information från IT-driften att det pågick scanningar i nätet, bedömningen blir därmed **delvis uppfyllt.**

Hur är säkerheten avseende intrång av interna aktörer?

Iakttagelser

Gnesta kommun har 802.1x i sitt nätverk vilket innebär skydd mot icke godkänd utrustning. Vid granskningen så slogs detta av för att PwC skulle kunna utföra sin

granskning vilket simulerade att attacken skulle komma från en intern dator.

PwC har under de tester som genomförts observerat ett flertal brister i IT-miljön. Dessa har lett till att PwC har kunnat anskaffa sig högsta behörighet i kommunens IT-miljö och delvis blivit upptäckta. I den tekniska rapport som har levererats till kommunens IT-chef redogörs respektive sårbarhet närmare för. Varav de **8** sårbarheterna som hittats så är **5** av dessa allvarliga.

Bedömning

PwC utgick från att enbart ha ett system inkopplat utan några behörigheter till att tillförskaffa sig domänadministratörsbehörigheter via flertalet sårbarheter, vilket gör att bedömningen för denna kontrollfråga blir **ej uppfyllt.**

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

Iakttagelser

I kommunens informationssäkerhetspolicy beskrivs att kommunstyrelsen har det övergripande ansvaret för informationssäkerheten. För det operativa ansvaret så är det informationssäkerhetssamordnaren som har det. Gnesta kommun saknar en informationssäkerhetssamordnare vilket i praktiken har inneburit att IT-chefen tagit på sig det ansvaret. Både IT-chefen och de intervjuade personerna var av den uppfattningen att IT-säkerhetsansvaret låg hos IT-chefen.

Bedömning

Gnesta kommun har upprättad dokumentation som beskriver ansvarsfördelningen vad gäller IT- och informationssäkerhet i kommunen, den stämmer inte överens med hur ansvarsfördelningen ser ut idag på IT-avdelningen då det generella ansva-

ret ligger hos IT-chefen. Detta gör att bedömningen för denna kontrollfråga blir **ej uppfyllt.**

Finns styrande IT-dokumentation på plats och revideras dessa regelbundet?

Iakttagelser

Dokumentgranskningen genomfördes på plats hos Gnesta kommun. PwC informerade om att syftet med dokumentgranskningen var att gå igenom vilken IT-dokumentation som finns att tillgå för Gnesta kommun samt vilket tillstånd dokumentationen är i. IT-relaterad dokumentation, som exempelvis IT-policy, IT-strategi, rutiner, instruktioner, kris- och katastrofplan, backupplan m.m. efterfrågades.

PwC fick ta del av ett fåtal dokument och merparten av dessa var daterade 2013. Det konstaterades att Gnesta kommun inlett ett arbete 2013 med att föra in en dokumentstruktur, men att projektet stannat upp och inte kommit igång igen. Dokumentation som granskats har även hänvisat till roller och ytterligare dokumentation som inte funnits i praktiken

Dokument	Typ	Kommentar
Informationssäkerhetsinstruktion för användare	Policy	Senast uppdaterad 2013-11-19
InformationssakerhetsPolicy_KF_131111	Policy	Senast uppdaterat 2013-11-11 Hänvisar till 2 st dokument som ännu ej finns framtagna: • Förvaltning (Infosäk F) • Kontinuitet och Drift (Infosäk KD)
Ansvarsförbindelse användare Gnesta kommun	Ansvarsförbindelse	
Driftdokumentation	Anteckningar	Saknar versionsbeteckning Saknar dokumentägare Saknar datum för förändring

Bedömning

Det finns dokumentation på Informationssäkerhetspolicy samt Informationssäkerhetsinstruktion för användare, dock är båda senast reviderade november 2013 samt ej fullständiga. PwC tog inte del av fler styrande dokument i denna granskning. Bedömningen för kontrollfrågan är **ej uppfyllt.**

Är befintlig dokumentation uppdaterad och löpande reviderad enligt god praxis?

Iakttagelser

Övrig dokumentation som granskningen fick ta del av var en omfattande driftdokumentation. Driftdokumentationen innefattade rutiner, kontaktuppgifter och information gällande hanteringen av systemen. Denna dokumentation var utan versionsbeteckning, datum och ägare, vilket innebar att PwC inte kunde utläsa om dokumentationen var aktuell.

Bedömning

Dokumentationen för de styrande dokumenten var senaste ändrade 2013.

För driftdokumentation så saknas datum för senaste uppdatering.

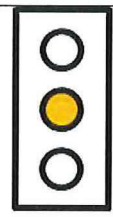
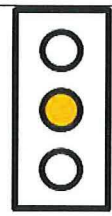
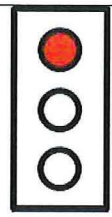
Revisionell bedömning

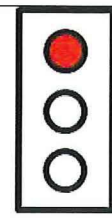
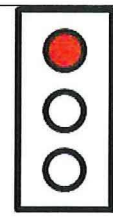
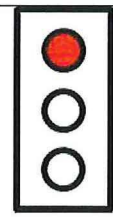
I frågan om kommunstyrelsen säkerställt att Gnesta kommuns nuvarande tekniska IT-säkerhet är tillräcklig och tillfredsställande för att reducera risker för obehörigt intrång till acceptabel nivå, så är vår sammanfattande bedömning efter granskningen, **ej uppfyllt.**

De tekniska tester som PwC har genomfört påvisar brister i kommunens IT-säkerhet både vad det gäller förmågan att stå emot angrepp samt förmågan att upptäcka och agera på angrepp.

Dokumentgranskningen visar att det saknas dokumentation som beskriver processen för arbetet med IT-säkerhet och det operativa IT-säkerhetsarbetet hänvisar till en roll som inte existerar på kommunen.

Bedömningar mot kontrollmål

Kontrollmål	Kommentar	
Hur upptäcks en eventuell attack?	**Delvis uppfyllt** PwC har erhållit en sammanställning av Gnesta kommun vilka angrepp de har upptäckt under testerna. En iaktagelse här är att Gnesta kommun endast har upptäckt ett fåtal av alla de angrepp som har utförst. Bedömningen blir därför delvis uppfyllt.	
Hanteras icke önskvärda incidenter på ett ändamålsenligt sätt?	**Delvis uppfyllt** Enligt Informationssäkerhetspolicyn är det informationssäkerhetssamordnaren som ansvarar för hanteringen av incidenter, och Gnesta kommun har i dagsläget ingen som innehar den rollen. IT-chefen fick under granskningen information från IT-driften att det pågick scanningar i nätet.	
Hur är säkerheten avseende intrång av interna aktörer?	**Ej uppfyllt** PwC utgick från att enbart ha ett system inkopplat utan några behörigheter till att tillförskaffa sig domänadministratörsbehörigheter via flertalet sårbarhet, vilket gör att bedömningen för denna kontrollfråga blir ej uppfyllt.	

Finns en tydlig roll- och ansvarsfördelning i frågor kring den övergripande IT-säkerheten?	**Ej uppfyllt** Gnesta kommun har upprättad dokumentation som beskriver ansvarsfördelningen vad gäller IT- och informationssäkerhet i kommunen, den stämmer inte överens med hur ansvarsfördelningen ser ut idag på IT-avdelningen då det generella ansvaret ligger hos IT-chefen. Detta gör att bedömningen för denna kontrollfråga blir ej uppfyllt.	
Finns styrande IT-dokumentation på plats och revideras dessa regelbundet?	**Ej uppfyllt** Informationssäkerhetspolicy samt Informationssäkerhetsinstruktion för användare, är båda senast reviderade november 2013. PwC tog inte del av fler styrande dokument i denna granskning.	
Är befintlig dokumentation uppdaterad och löpande reviderad enligt god praxis?	**Ej uppfyllt** Dokumentationen för de styrande dokumenten var senaste ändrade 2013. För driftdokumentation så saknas datum för senaste uppdatering.	

Rekommendationer

- PwC rekommenderar att ansvarsområdet för IT-säkerhet tydliggörs inom hela kommunen.
- PwC rekommenderar att kommunen uppdaterar sina policydokument samt upprättar de dokument som saknas enligt informationssäkerhetspolicyn.
- PwC rekommenderar att man ser över sin förmåga att detektera och agera på incidenter och intrång.
- PwC rekommenderar att man ser över och stärker sin lösenordspolicy.

Bilagor

Bilaga 1 – Riskgradering intrångstester

Följande graderingar används i dokumentet för att redovisa den risk en viss sårbarhet utgör.

Gradering	Beskrivning
Hög	En sårbarhet med hög risk är något man bör åtgärda omedelbart. De är relativt lätta för en angripare att utnyttja och kan förse denne med full access till de berörda systemen.
Medel	En sårbarhet med medel risk är oftast svårare att utnyttja och ger inte samma tillgång till det drabbade systemet.
Låg	En sårbarhet med låg risk ger ofta information till en angripare och kan hjälpa denne i kartläggning inför en attack. Dessa bör åtgärdas i mån av tid, men är inte lika kritiska som övriga brister.
Information	En teknisk eller administrativ brist som bör åtgärdas eller ett förslag på förbättring.

2019-06-05

Tobias Bjöörn
Uppdragsledare

Mikael Grönvik
Projektledare