www.pwc.se

Revisionsrapport

Granskning av intrångsskydd

Håbo kommuns förtroendevalda revisorer

Niklas Ljung
Mattias Gröndahl

April/2018

pwc

Innehåll

Sammanfattning

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

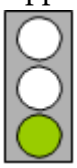
Revisionsfrågan som har varit styrande för granskningen har formulerats enligt följande:

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

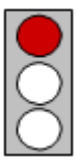
Den sammanfattande bedömningen baseras på bedömningarna av de sex kontrollfrågorna för granskningen, vilka redovisas i rapporten.

Kontrollfråga 1
Upptäcks en eventuell attack?

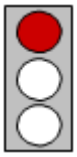


Kontrollfråga 2
Hanteras icke önskvärda incidenter på ett ändamålsenligt sätt?

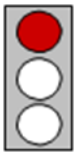
Kontrollfråga 3
Hur är säkerheten avseende intrång av extern och intern aktör?



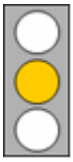
Kontrollfråga 4
Finns det en tydlig roll- och ansvarsfördelning i frågor kring den övergripande IT-säkerheten?



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 uppmärksammade risker eller vid ett intrång?



En sekretessbelagd detaljerad rapport med resultat från genomförd intrångstest har lämnats över till IT-chefen i Håbo kommun.

1. Inledning

1.1. Granskningsbakgrund

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, 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 Håbo 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:

- Upptäcks en eventuell attack?
- 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 uppmärksammade risker eller vid ett intrång?

1.3. Revisionskriterier

Revisionskriterierna utgörs av nedanstående:

- Kommunallagen
- Budget 2018
- IT-styrdokument

1.4. Avgränsning

I tid avgränsas granskningen till år 2018 samt till granskningens kontrollfrågor.

1.4.1. Nominerade system

Alla system på Håbo 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 Håbo 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 har genomförts med:
- IT-chefen i Håbo kommun.

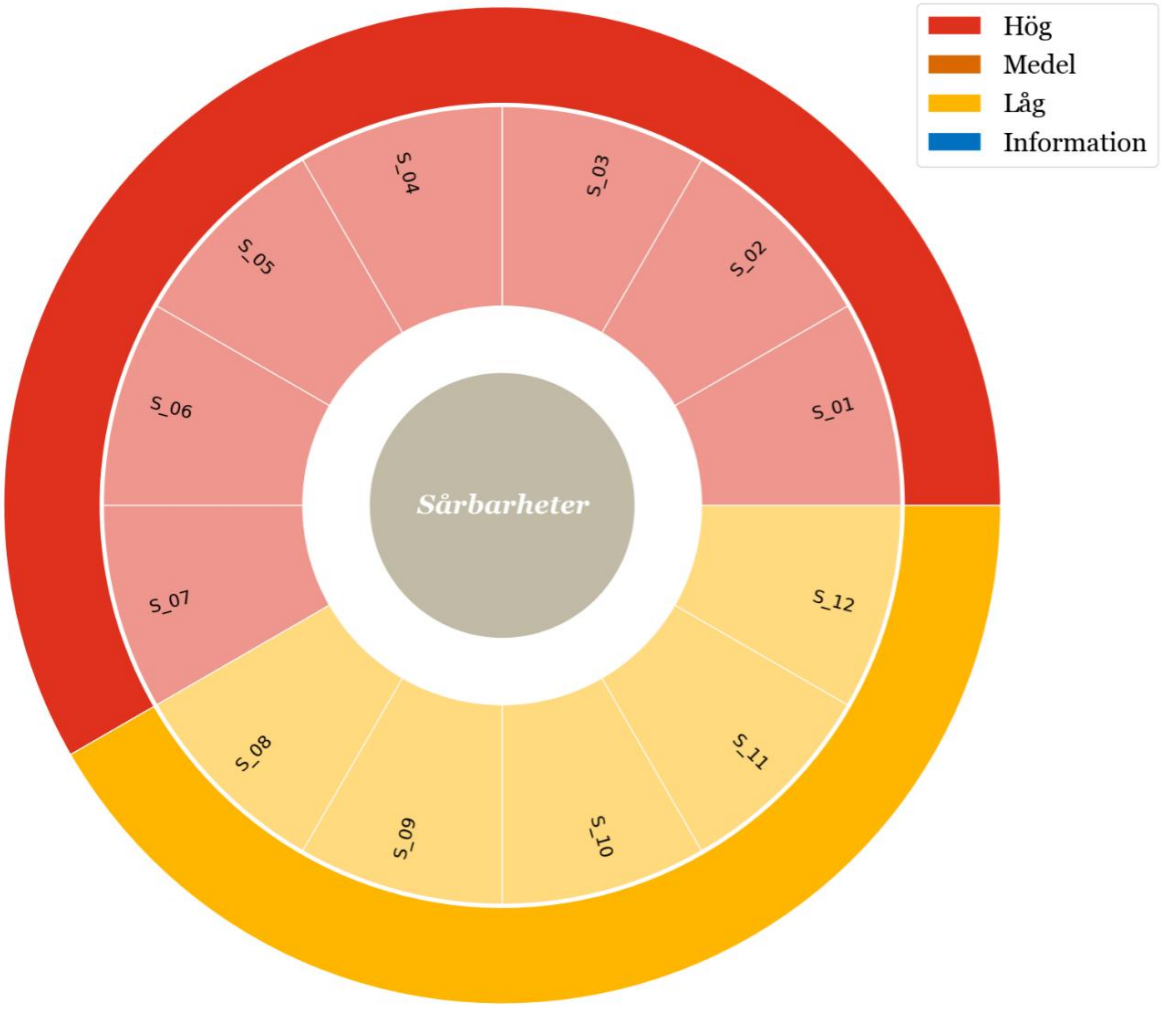
2. Resultat

2.1. Intrångstester

2.1.1. Iakttagelser

Det var på den förhållandevis korta tiden möjligt för PwC att kartlägga IT-miljön, identifiera sårbarheter och utnyttja dessa.

Under testerna identifierades **12** st. sårbarheter. Av dessa är **7** st. riskgraderade som **hög**, **0** st. som **medel**, **5** st. som **låg** och **0** st. som **information**.



Se *Bilaga 1 – Riskgradering intrångstester* för information om gradering.

Det finns ett antal åtgärder som kan genomföras för att höja den totala säkerheten till en högre nivå.

Mer information lämnas i den detaljerade sekretessbelagda rapport som PwC har lämnat över direkt till IT-chefen i Håbo kommun.

2.1.2. Bedömning

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

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

2.2. Dokumentgranskning

2.2.1. Iakttagelser

I samband med att dokumentgranskningen påbörjades hade PwC mail- och telefonkontakt med IT-chefen i Håbo kommun.

PwC informerade om att syftet med dokumentgranskningen var att se vilken IT-dokumentation som finns i Håbo kommun samt vilket tillstånd dokumentationen är i. PwC bad att få titta på IT-relaterad dokumentation, som exempelvis IT-policy, IT-strategi, rutiner, instruktioner, kris- och katastrofplan, backupplan etc.

PwC fick ta del av en mängd dokumentation och merparten av denna bedömdes som bra, dock kunde vi konstatera att många av dokumenten saknar, dokumentägare, datum, versionsnummer och versionshistorik. Vi kunde också notera att mycket av dokumentationen var från 2014 och alltså bör uppdateras.

Vi kunde inte heller se någon dokumentation som tog upp området IT-säkerhet.

I dokumentationen som vi granskade såg vi bristande information om hur Håbo arbetar med IT säkerhet. När det gäller informationssäkerhet har Håbo kommit längre i sin dokumentation.

2.2.2. Bedömning

PwC:s slutsats efter dokumentgranskningen är att kontrollfrågorna rörande dokumentation **ej är uppfyllda**.

PwC:s bedömning är att Håbo kommun inte har all nödvändig dokumentation på plats samt att den som finns bör revideras.

IT-organisationen bör göra en kraftansträngning och inventera sin dokumentation, skapa den dokumentation som i dag saknas och uppdatera den dokumentation som har blivit föråldrad.

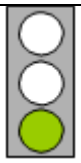
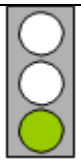
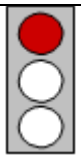
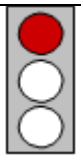
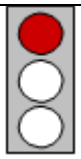
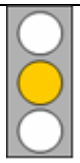
Det bör finnas ett dokument som beskriver hur Håbo kommun arbetar med IT säkerhet generellt och vad det ställs för krav på systemförvaltaren. Men också vad gränsdragningen går mellan IT avdelning och systemförvaltaren.

3. Bedömningar

3.1. Revisionell bedömning

Efter genomförd granskning är PwC:s sammanfattande bedömning att kommunstyrelsen **ej säkerställt** att Håbo 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*
Upptäcks en eventuell attack?	 IT-avdelningen uppmärksammade PwC:s angrepp och notifierade PwC att de blivit upptäckta.
Hanteras icke önskvärda incidenter på ett ändamålsenligt sätt?	 Under PwC:s tester hanterades den upptäckta incidenten på ett ändamålsenligt sätt. Det finns en muntlig process för hur incidenter skall hanteras och vilka som skall informeras. Tyvärr är inte rutinen tillräckligt dokumenterad, se sista kontrollfrågan.
Hur är säkerheten avseende intrång av extern och intern aktör?	 IT-säkerheten håller inte en tillräcklig 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?	 PwC har inte tagit del av någon roll eller ansvarsfördelning som berör kommunens IT-säkerhetsarbete. Håbo arbetar med att ta fram en ny förvaltningsmodell där detta kommer att klargöras.
Finns det kända och tillämpade styrande dokument och riktlinjer för kommunens förebyggande arbete kring IT-säkerhet?	 PwC har inte tagit del av någon dokumentation eller information som beskriver kommunens förebyggande arbete kring IT-säkerhet. Håbo arbetar med att ta fram en ny förvaltningsmodell där detta kommer att klargöras.
Finns det kända och tillämpade styrande dokument och riktlinjer att följa vid uppmärksammade risker eller vid ett intrång?	 PwC har inte tagit del av någon dokumenterad incidenthantering. Det finns dock med som punkt i Håbos APT:er. Arbetet behöver dokumenteras bättre.

3.3. Rekommendationer

Utifrån genomförd granskning lämnas följande rekommendationer.

3.3.1. Rekommendationer efter genomförda intrångstester

Efter utvärdering av resultatet, av den **externa** miljön, anses säkerhetsnivån ligga på en medelnivå. Det saknas stark autentisering på ingångar som ger tillgång till den interna mailen, en åtgärd av detta skulle höja säkerhetsnivån.

Efter utvärdering av resultatet, av den **interna** miljön, anses säkerhetsnivån ligga på en medelnivå. Säkerhetsuppdateringar har rullats ut bra, dock behöver behörighetsmodellen ses över då en vanlig användare har mer rättigheter än vad som anses nödvändigt. Det finns även ett större antal domänadministratörer än vad som anses nödvändigt.

PwC rekommenderar att åtgärder bör vidtas skyndsamt för att åtgärda sårbarheter och öka IT-säkerheten. Vi har identifierat ett antal åtgärder som skulle leda till att den totala säkerheten höjs till en högre nivå. Vi rekommenderar att man genomför dessa efter den prioriterade lista som finns i den sekretessbelagda rapporten.

PwC rekommenderar även att man ser över rutiner kring hantering av tredjeparts produkter för att säkerhetsställa att även dessa får säkerhetsuppdateringar.

Vissa av webbservrarna saknar konfiguration som skulle göra dem säkrare, PwC rekommenderar att man ser över rutiner kring utrullning av webbservrar och inför härdning som en del i arbetet.

3.3.2. Rekommendationer efter genomförd dokumentgranskning

PwC rekommenderar att Håbo kommun genomför en genomgång av styrande IT-dokument för att få en blid av vad som saknas, skapar de dokument som bedöms behövas i organisationen och löpande reviderar dessa. En kommun bör ha uppdaterade och aktuella strategiska dokument som beskriver var kommunen är på väg och vad man har för ambitioner. Detta för att IT-avdelningen eller andra delar av kommunens verksamhet som är beroende av IT-miljön skall veta vilket fokus som skall hållas.

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 skall se om informationen är relevant eller ej.

Detta arbete är svårt för dagens IT-organisation att hinna med och det prioriteras lätt ned. En lösning kan vara att tillfälligt förstärka gruppen med någon som driver arbetet med dokumentationen.

2018-04-24

	Niklas Ljung
_____	_____
Uppdragsledare	*Projektledare*

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.