www.pwc.se

Revisionsrapport

Granskning av intrångsskydd

Region Norrbottens förtroendevalda revisorer

Erik Jansen
Revisionskonsult

Gustav Blockert
Revisionskonsult

Alexander Mattsson
Teknisk sakkunnig revisionskonsult

November 2018

pwc

Innehåll

2018-11-13

Marie Lindblad
Certifierad kommunal revisor
Uppdragsledare

Erik Jansen
Revisionskonsult
Projektledare för revisionellt genomförande

Gustav Blockert
Projektledare för teknisk genomförande

Sammanfattning

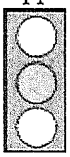
PwC har på uppdrag av de förtroendevalda revisorerna i Region Norrbotten genomfört en granskning av det externa och interna IT-intrångsskyddet inom Region Norrbotten.

Revisionsfrågan som har varit styrande för granskningen har formulerats enligt följande: *Har regionstyrelsen säkerställt att Region Norrbottens 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 revisionella bedömning att regionstyrelsen **i begränsad utsträckning** säkerställt att Regions Norrbottens nuvarande tekniska IT-säkerhet är tillräcklig och tillfredsställande för att reducera risker för obehörigt intrång till en acceptabel nivå.

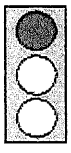
Den sammanfattande bedömningen baseras på bedömningarna av de fyra kontrollfrågorna för granskningen, vilka redovisas i rapportens inledande avsnitt.

Kontrollfråga 1
Upptäcks en eventuell attack och hanteras icke önskvärda incidenter på ett ändamålsenligt sätt?



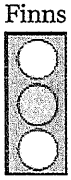
Bedömning: IT-avdelningen uppmärksammade PwC:s angrepp och notifierade PwC att de blivit upptäckta. Upptäckten verkar dock ske med manuella metoder, vilket innebär att kontrollfrågans uppfyllnad endast kan bedömas som delvis uppfylld.
Bedömning: Delvis

Kontrollfråga 2
Är säkerheten avseende intrång av extern och intern aktör ändamålsenlig?



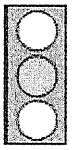
Bedömning: Nej

Kontrollfråga 3
Finns det styrande dokument, såsom policy och riktlinjer för IT-säkerhet?



Bedömning: Delvis

Kontrollfråga 4
Är befintlig dokumentation uppdaterad och löpande reviderad enligt god praxis?



Bedömning: Delvis

En detaljerad rapport med resultat från genomförd intrångstest har lämnats över till enhetschef Datacenter/Nätverk i Region Norrbotten.

1. Inledning

1.1. Granskningsbakgrund

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

Styrelse och nämnder 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 regionstyrelsen 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 regionstyrelsen säkerställt att Region Norrbottens nuvarande tekniska IT-säkerhet är tillräcklig och tillfredsställande för att reducera risker för obehörigt intrång till en acceptabel nivå?

1.2.1. Kontrollfrågor

Följande kontrollfrågor har använts vid granskningen för att besvara revisionsfrågan:

- Finns det styrande dokument, såsom policy och riktlinjer för IT-säkerhet?
- Är säkerheten avseende intrång av extern och intern aktör ändamålsenlig?
- Upptäcks en eventuell attack och hanteras icke önskvärda incidenter på ett ändamålsenligt sätt?
- Är befintlig dokumentation uppdaterad och löpande reviderad enligt god praxis?

1.3. Revisionskriterier

Revisionskriterierna utgörs av nedanstående:

- Kommunallag
- Regionfullmäktiges strategiska plan 2018-2020
- Finansplan 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 Region Norrbottens 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 ett så kallat blackbox-pentest där endast domänadress anges, all övrig information anskaffas under testernas gång.

Inledningsvis genomfördes i juni 2018 ett för granskningen förankrande uppstartsmöte med:

- Regionstyrelsens dåvarande vice ordförande
- Biträdande regiondirektör

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 Region Norrbotten 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:

- Enhetschef Datacenter/Nätverk

Under granskningens gång har ett avstämningsmöte skett med:

- Divisionschef, division Länsteknik
- IT/MT-direktör
- Enhetschef Datacenter/Nätverk

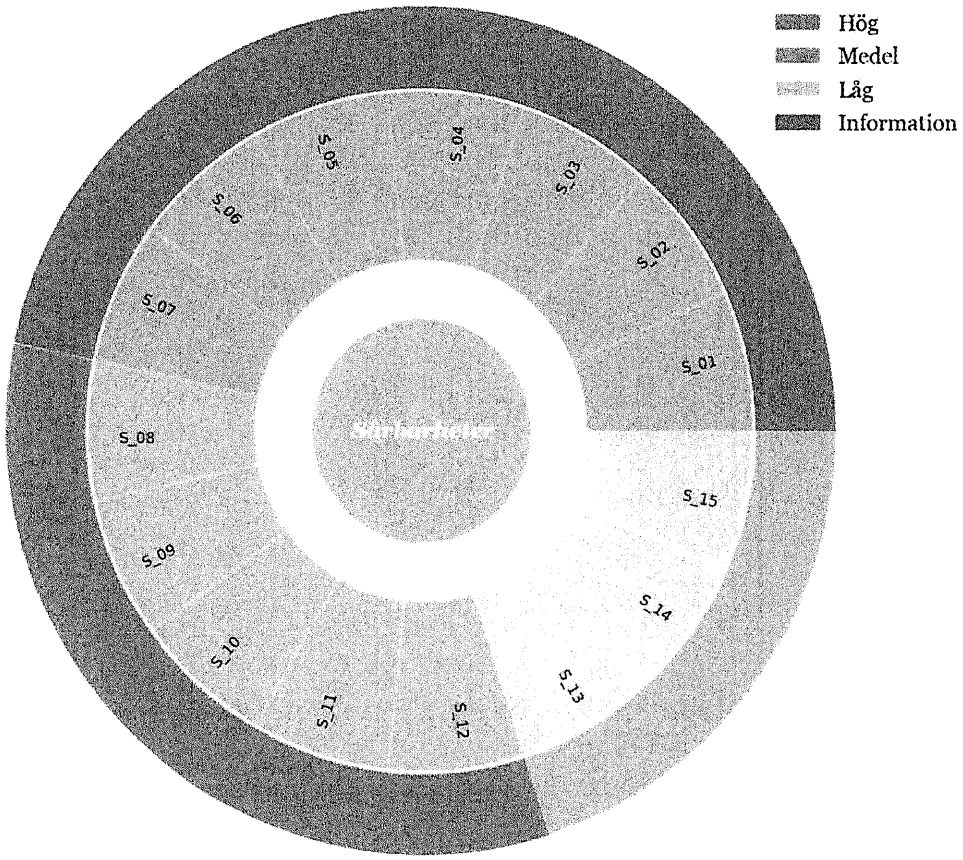
2. Resultat

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 **15** st. sårbarheter. Av dessa är **7** st. riskgraderade som **hög**, **5** st. som medel, **3** st. som **låg** och **0** st. som **information**.



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

Mer information lämnas i den detaljerade rapport som *PwC har lämnat över direkt till* Region Norrbotten.

2.1.2. Bedömning

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

2.2. Dokumentgranskning

2.2.1. Iakttagelser

I samband med att dokumentgranskningen påbörjades hade PwC mail- och telefonkontakt med tjänstemän inom Division Länsteknik i Region Norrbotten.

PwC informerade om att syftet med dokumentgranskningen var att se vilken IT-dokumentation som finns i Region Norrbotten 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 god. Vi kunde notera att det finns en spridning på när och vilka dokument som uppdateras, majoriteten av dokumentationen är daterad till 2016 men ett antal har inte uppdaterats sedan 2008/2009.

I dokumentationen vi granskade uppdagades bristande information om hur Region Norrbotten arbetar med IT säkerhet. När det gäller informationssäkerhet inom Region Norrbotten är informationssäkerhetspolicyn utdaterad utifrån förändringar i lagstiftning i övrigt.

Det skall dock noteras att policyn är under revidering när denna granskning genom-förs.

2.2.2. Bedömning

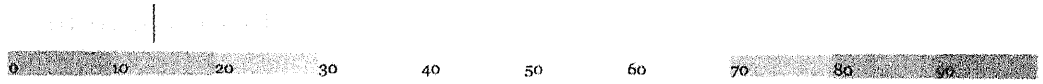
PwC:s bedömning efter dokumentgranskningen är att kontrollfrågorna rörande dokumentation **delvis är uppfyllda.**

PwC:s bedömning är att Region Norrbotten bör revidera den styrande dokumentationen som idag finns på plats. I samband med en revidering av dokumentationen bör även en inventering genomföras över dokumentation i övrigt och tillskapa den dokumentation som i dag saknas.

3. Bedömningar

3.1. Revisionell bedömning

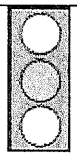
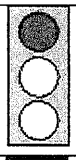
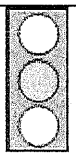
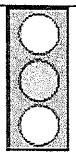
Granskningens revisionsfråga bedöms utifrån nedan bedömningsskala:



Inte (0-20) | *I begränsad utsträckning (20-49)* | *Till övervägande del (51-79)* | *Ja* (80-)

Efter genomförd granskning är PwC:s sammanfattande bedömning att regionstyrelsen **i begränsad utsträckning säkerställt** att Region Norrbottens 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 och hanteras icke önskvärda incidenter på ett ändamålsenligt sätt?	 IT-avdelningen uppmärksammade PwC:s angrepp och notifierade PwC att de blivit upptäckta. Upptäckten verkar dock ske med manuella metoder, vilket innebär att kontrollfrågans uppfyllnad endast kan bedömas som delvis uppfylld. **Bedömning: Delvis**
Är säkerheten avseende intrång av extern och intern aktör ändamålsenlig?	 IT-säkerheten håller inte en tillräcklig hög nivå och detta område behöver prioriteras för att minimera framtida incidenter. **Bedömning: Nej**
Finns det styrande dokument, såsom policy och riktlinjer för IT-säkerhet?	 PwC har tagit emot en del dokument inom IT-säkerhetsområdet. Vi kunde notera att det finns en spridning på när och vilka dokument som uppdateras, majoriteten av dokumentationen är daterad till 2016 men ett antal har inte uppdaterats sedan 2008/2009. **Bedömning: Delvis**
Är befintlig dokumentation uppdaterad och löpande reviderad enligt god praxis?	 De dokument som PwC har tagit del av är delvis uppdaterade och delvis inaktuella/daterad. Den informationssäkerhetspolicy som finns idag bedöms som föråldrad, men vi noterar samtidigt att policyn uppges vara under revidering. **Bedömning: Delvis**

3.3. Rekommendationer

Inom ramen för granskningens sakavstämning har vi fått viss information som vi ser positivt på gällande arbete som påbörjats inom regionen avseende införandet av ledningssystem, kartläggning av skyddsvärda system utifrån ett riskperspektiv samt omvärldsbevakning inom säkerhetsområdet. Dessa åtgärder ryms inom ramen för de rekommendationer vi lämnar nedan.

3.3.1. *Rekommendationer efter genomförda intrångstester och dokumentgranskning*

- Efter utvärdering av resultatet för den **externa och interna** miljön, anses säkerhetsnivån ligga på medelnivå. Vår rekommendation är att åtgärder vidtas för att höja säkerhetsnivåerna.

- Åtgärder 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 utifrån en fastställd prioritering.

- Vi rekommenderar vidare att regionstyrelsen säkerställer att en genomgång av styrande IT-dokument genomförs för att få en bild av vad som saknas, skapar de dokument som bedöms behövas i organisationen och löpande reviderar dessa.

- Avslutningsvis rekommenderar vi att en årlig revidering av dokumentationen införs samt att organisationen ser till att ägare, datum, versionsnummer samt versionshistorik finns med i all dokumentation.