Revisionsrapport

Granskning av intrångsskydd

Nynäshamns kommuns förtroendevalda revisorer

Niklas Ljung
Mattias Gröndahl

November 2018

pwc

Innehåll

Sammanfattning **2**
1. Inledning **4**
1.1. Granskningsbakgrund 4
1.2. Syfte och revisionsfråga 4
1.2.1. Kontrollfrågor 4
1.3. Revisionskriterier 5
1.4. Avgränsning 5
1.4.1. Nominerade system 5
1.5. Metod 5
2. Resultat **7**
2.1. Intrångstester 7
2.1.1. Iakttagelser 7
2.1.2. Bedömning 7
2.2. Dokumentgranskning 7
2.2.1. Iakttagelser 7
2.2.2. Bedömning 8
3. Bedömningar **9**
3.1. Revisionell bedömning 9
3.2. Bedömning utifrån kontrollfrågor 9
3.3. Rekommendationer 10
3.3.1. Rekommendationer efter genomförda intrångstester 10
3.3.2. Rekommendationer efter genomförd dokumentgranskning 10
3.4. Övriga rekommendationer 10

Sammanfattning

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

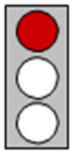
Revisionsfrågan som har varit styrande för granskningen har formulerats enligt följande:

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

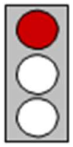
Den sammanfattande bedömningen baseras på bedömningarna av de sex kontrollfrågorna för granskningen, vilka redovisas i rapporten.

Kontrollfråga 1
Finns tillräckliga verktyg och processer för att upptäcka en eventuell attack och är de implementerade och fungerar de på ett tillfredsställande sätt?

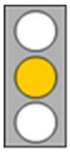


Kontrollfråga 2
Hanteras icke önskvärda incidenter på ett ändamålsenligt sätt?

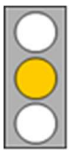
Kontrollfråga 3
Hur är säkerheten avseende intrång av extern och intern aktör?



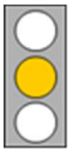
Kontrollfråga 4
Finns det en tydlig roll- och ansvarsfördelning i frågor kring den övergripande IT-säkerheten?



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 uppmärksammandet av risker eller ett intrång?



1. Inledning

1.1. Granskningsbakgrund

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 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.

Nynäshamns kommun har valt att outsourca driften till Tieto som har ett operativt ansvar. Detta innebär att det finns en större risk att Nynäshamns kommun inte har kontroll på IT-säkerheten och detta ökar behovet av kontrollåtgärder mot Tieto.

1.2. Syfte och revisionsfråga

Granskningen syftar till att besvara följande revisionsfråga:

Har kommunstyrelsen säkerställt att Nynäshamns 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:

- Finns tillräckliga verktyg och processer för att upptäcka en eventuell attack och är de implementerade och fungerar de på ett tillfredsställande sätt?
- 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 uppmärksammandet av risker eller ett intrång?

1.3. Revisionskriterier

Revisionskriterierna utgörs av nedanstående:

- Kommunallagen
- IT-styrdokument

1.4. Avgränsning

I tid avgränsas granskningen till år 2018 samt till granskningens kontrollfrågor, samt till att testerna utförs både från utsidan och från insidan.

1.4.1. Nominerade system

Alla system på Nynäshamns 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 Nynäshamns 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 samt intervju har genomförts med:

- Peter Österberg, IT-chef i Nynäshamns kommun
- Roger Forsborn, IT-Arkitekt i Nynäshamns kommun
- Cecilia Brattsell, Service Delivery Manager på Tieto

2. Resultat

2.1. Intrångstester

2.1.1. Iakttagelser

Konsulter från PwC kunde på relativt kort tid anskaffa sig högsta behörighet i den interna IT-miljön. Det påvisades två skilda angreppssätt där full kontroll av kommunens IT-miljö kunde anskaffas. Angreppen som genomfördes är av enkel karaktär och kan genomföras av en mindre sofistikerad angripare utan kunskap om IT-miljön.

Flera angrepp genomfördes under testerna men detekterades inte av Tieto (som har det operativa ansvaret), detta tyder på att det saknas förmåga samt verktyg att identifiera angrepp i den interna IT-miljön.

Under testerna påträffades extremt många konton med domänadministratörsrättigheter, dessa konton är knutna till Tieto som är den driftoperatör som Nynäshamns kommun har valt att outsourca driften till.

PwC kunde under testerna anskaffa sig högsta behörighet i IT-miljön vilket innebär, i stort sett, full kontroll över IT-miljön. Det bör noteras att detta angrepp är att anse som ytterst kritiskt och har ett utfall som vid ett realistiskt angrepp skulle kunna leda till mycket omfattande skador, då en angripare bland annat skulle kunna extrahera känslig information, låsa ute systemanvändare från resurser samt kryptera viktiga filer.

Under granskningen identifierades också styrkor i IT-miljön. Följande styrkor förhindrade ett flertal angrepp som annars skulle vara möjliga.

- Stark autentisering i form av tvåfaktorautentisering på vissa externt exponerade inloggningsportaler.
- Förhållandevis god patchnnivå på påträffade tjänster.

2.1.2. Bedömning

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

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

2.2. Dokumentgranskning

2.2.1. Iakttagelser

PwC fick ta del av ett flertal dokument och merparten av dessa bedömdes hålla en god nivå, dock kunde vi konstatera att en del dokument behöver revideras för att kunna anses vara aktuella.

Det finns en incidentrapport som ska fyllas i när en incident har inträffat.

2.2.2. *Bedömning*

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

PwC:s bedömning är att Nynäshamns kommun har mycket av dokumentationen på plats men bör genomföra en dokumentationsgenomgång för att se vad som saknas och vad som behöver uppdateras.

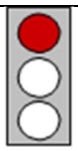
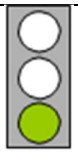
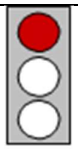
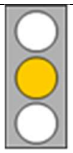
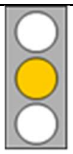
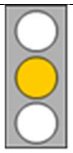
Kommunens dokument *IT-säkerhetspolicy* samt dokumentet *IT-säkerhetsreglerdetalj* bör uppdateras eftersom dessa är ifrån 2002.

3. Bedömningar

3.1. Revisionell bedömning

Efter genomförd granskning är PwC:s sammanfattande bedömning att Nynäshamns kommunstyrelse **ej har säkerställt** att Nynäshamns 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*
Finns tillräckliga verktyg och processer för att upptäcka en eventuell attack och är de implementerade och fungerar de på ett tillfredsställande sätt?	 IT-enheten (Tieto) saknar verktyg och förmåga att detektera intrång om IT-miljön blir angripen.
Hanteras icke önskvärda incidenter på ett ändamålsenligt sätt?	 Nynäshamn och Tieto har en incidenthanteringsprocess, som man följer i samband med incidenter.
Hur är säkerheten avseende intrång av extern och intern aktör?	 IT-säkerheten håller inte en tillräckligt 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?	 I kommunens IT-säkerhetspolicy från 2002 beskriver roll- och ansvarsfördelningen men policyn behöver uppdateras samt göras känd.
Finns det kända och tillämpade styrande dokument och riktlinjer för kommunens förebyggande arbete kring IT-säkerhet?	 Bedömningen är att det finns dokumentation som beskriver kommunens förebyggande arbete kring IT-säkerhet. PwC:s bedömning är dock att det finns förbättringspotential.
Finns det kända och tillämpade styrande dokument och riktlinjer att följa vid uppmärksammandet av risker eller ett intrång?	 En del av de dokument som PwC har tagit del av håller en god nivå, men det finns även en del dokument som har halkat efter och bör revideras.

3.3. Rekommendationer

Utifrån genomförd granskning lämnas följande rekommendationer.

3.3.1. Rekommendationer efter genomförda intrångstester

Följande är rekommenderade förslag på åtgärder och syftar till att förbättra IT-säkerheten långsiktigt för att höja IT-säkerheten.

- Förbättra nuvarande lösenordspolicy och se över rutinen för hantering av konton och lösenord.
- Minska antalet konton med domänadministratörsrättigheter till ett fåtal.
- Förbättra nätverksarkitekturen så att nätverkssegmentering tillämpas i större utsträckning och begränsa nätverksåtkomsten ytterligare.
- Design av stark autentisering på samtliga ingångar som ger åtkomst till det interna nätverket.
- Se över förmågan att upptäcka och förhindra intrång (detektionsförmåga). Konfigurera automatiska larm för säkerhetsloggar som avviker från normalt användarbeteende. Överväg att implementera system för att upptäcka säkerhetsincidenter.
- Förhindra exponering av inloggningsuppgifter.

3.3.2. Rekommendationer efter genomförd dokumentgranskning

- PwC rekommenderar att Nynäshamns kommun genomför en genomgång av styrande IT-dokument för att få en bild av vad som saknas i dokumentationsväg samt vad som behöver uppdateras.
- 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 ska kunna se om informationen är relevant eller ej.
- Kommunen bör ta fram övergripande uppdragsbeskrivning för IT-enheten samt korrekta och uppdaterade rolbeskrivningar för IT-enhetens personal.

3.4. Övriga rekommendationer

Nynäshamns kommun bör tillsätta tjänsten informationssäkerhetsansvarig för att bl.a. säkerställa att kommunen klassar samtliga system samt agerar kravställare på IT-organisationen vad avser IT-säkerhet.

2019-01-29

Anders Hägg
Uppdragsledare

Niklas Ljung
Projektledare