LINDESBERGS KOMMUN
Revisorerna

2018-08-30

Kommunstyrelsen

2018 -08- 30

För kännedom:
Kommunfullmäktige

KS 2018/159-4

Revisionsrapport "Granskning av teknisk IT-säkerhet och intrångsskydd"

PwC har på uppdrag av de förtroendevalda revisorerna i Lindesbergs kommun genomfört en granskning av det externa och interna intrångsskyddet hos Lindesbergs kommun. Revisionsfrågan som har varit styrande för granskningen har formulerats enligt följande: Har kommunstyrelsen säkerställt att Lindesbergs 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 Lindesbergs 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.

	Kontrollfrågor	***Bedömning***
1	Upptäcks en eventuell attack?	
2	Hanteras icke önskvärda incidenter på ett ändamålsenligt sätt?	
3	Hur är säkerheten avseende intrång av extern och intern aktör?	
4	Finns det en tydlig roll- och ansvarsfördelning i frågor kring den övergripande IT-säkerheten?	
5	Finns det kända och tillämpade styrande dokument och riktlinjer för kommunens förebyggande arbete kring IT-säkerhet?	
6	Finns det kända och tillämpade styrande dokument och riktlinjer att följa vid uppmärksammade risker eller vid ett intrång?	

Bedömningarna i sin helhet tillsammans med rekommendationer har sammanfattats i en revisionsrapport, som behandlats och godkänts av revisorerna vid sammanträdet 2018-08-30.

Revisorerna har beslutat att överlämna rapporten till kommunstyrelsen med önskan om skriftligt svar senast 26 november med kommentarer till granskningen om vilka åtgärder nämnden planerar att vidta. Svaret skall ställas till revisorerna samt PwC, Tobias Bjöörn, Box 885, 721 23 Västerås.

FÖR REVISORERNA

Mats Melander
Ordförande

www.pwc.se

Revisionsrapport

Granskning av teknisk IT-säkerhet och intrångsskydd

Lindesbergs kommun

Mikael Grönvik
Mattias Gröndahl

Augusti 2018

pwc

Innehåll

Sammanfattning

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

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

Har kommunstyrelsen säkerställt att Lindesbergs 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 Lindesbergs 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.

	Kontrollfrågor	***Bedömning***
1	Upptäcks en eventuell attack?	
2	Hanteras icke önskvärda incidenter på ett ändamålsenligt sätt?	
3	Hur är säkerheten avseende intrång av extern och intern aktör?	
4	Finns det en tydlig roll- och ansvarsfördelning i frågor kring den övergripande IT-säkerheten?	
5	Finns det kända och tillämpade styrande dokument och riktlinjer för kommunens förebyggande arbete kring IT-säkerhet?	
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 Lindesbergs kommun för att ge kommunen möjlighet att omedelbart vidta säkerhetshöjande åtgärder

1. Inledning

1.1. Granskningsbakgrund

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

1.2.1. Kontrollfrågor

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 intern och externa aktörer?
- 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 Lindesbergs kommuns interna samt externa nätverk ansågs vara nominerade system och således inom ramen för tekniska tester.

1.5. Metod

Granskningen har genomförts genom interna och externa intrångstester, dokumentstudier av för granskningen relevanta dokument samt telefon- och mailkontakt.

Utgångspunkten för de interna testerna var en PwC-kontrollerad enhet inkopplad på det administrativa nätverket. Detta utfördes under förutsättningen att IT-personal från Lindesbergs kommun hjälpte till att ansluta utrustningen, samt inaktivera 802.1x på den aktuella nätverksporten. 802.1x är ett protokoll som annars blockerar icke godkänd utrustning att anslutas till nätverket, vilket i det här fallet var avslaget. Testerna simulerar en angripare som kommit in på nätverket, genom att ha tagit över en persons dator, t.ex. genom ett phishing mail.

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 Lindesbergs 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-chef i Lindesbergs kommun.
- IT-drift och säkerhetsansvarig Lindesbergs kommun.

Ett utkast av rapporten har varit föremål för sakgranskning av de intervjuade tjänstemännen.

2. Resultat

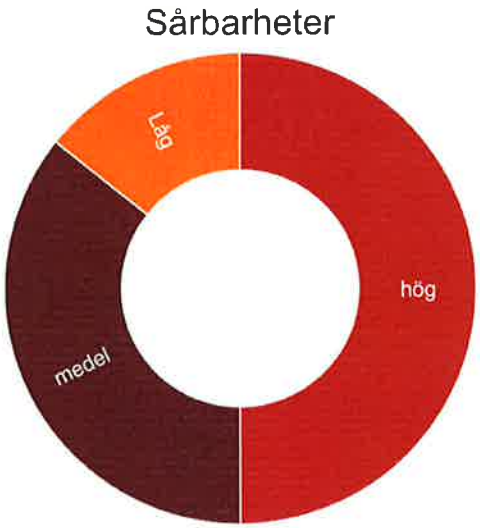
2.1. Intrångstester

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 **14** st. sårbarheter. Av dessa är **7** st. riskgraderade som **hög**, **5** st. som **medel**, **2** st. som **låg**.

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



Lindesberg kommun har idag vidtagit åtgärder för att höja säkerheten, såsom att ha ett aktivt DDOS-skydd, redundans på dataförbindelserna, och implementerat 802.1x i nätverket. Utöver dessa säkerhetshöjande funktioner så finns det 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 Lindesbergs kommun.

2.1.2. Bedömning

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

Ett antal servrar visar på säkerhetsmässiga brister i konfigurationen. System i produktion återfanns med standardkonfiguration där det gick att läsa ut mer information än nödvändigt samt att det i sin tur ökar attackytan för en angripare som försöker ta sig in. Det iden-

tifierades även ett antal servrar med sårbarheter i programvara som visar på brister i processen för programvaruuppdateringar.

Under testerna kunde PwC anskaffa sig högsta behörighet i domänen. Domänadministratör är den högsta behörighetsgruppen i en domän, och ska endast tilldelas senior personal på IT som har behov av den behörigheten för att utföra sitt arbete.

Ingen gång under granskningen fick IT-chefen någon inrapporterad incident, vilket innebär att denna typ av intrång inte uppmärksammas av IT-avdelningens rutiner.

2.2. Dokumentgranskning

2.2.1. Iakttagelser

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

PwC informerade om att syftet med dokumentgranskningen var att se vilken IT-dokumentation som finns i Lindesbergs 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 information bedömdes som bra med en fastställd ägare till dokumentet samt datum då det blivit beslutat. Dock kunde vi konstatera att delar av dokumentationen är från 2014 och bör uppdateras för att säkerställa att riktlinjerna stämmer och har anpassats efter den snabba utvecklingen som sker inom IT. Utöver det så går det på flertalet dokument inte att utläsa versionsnummer och versionshistorik.

Vi kunde konstatera att det fanns dokumentation som tog upp området IT-säkerhet. I dokumentet *KS 2018-206-1 Strategi Informationssäkerhet* finns ett avsnitt som beskriver roll och ansvarsfördelning gällande informationssäkerhet. Under telefonintervju framkom det att detta inte är helt implementerat ännu och att det finns en otydlighet inom detta område.

Dokument	Typ	Kommentar
Avtal IT-konto	Avtal	Datum för när detta dokument är framtaget framgår ej
Hantering av telefoni och e-post	Riktlinje	Saknar versionsbeteckning Senast uppdaterat 2014-10-29
KS 2018-205-1 Riktlinje för Informationssäkerhet	Riktlinje	Hänvisar till 3 st dokument som ännu ej finns framtagna: • Användarinstruktion • Informationssäkerhetsanalys • Handlingsplan för informationssäkerhet

KS 2018-205-2 Riktlinje för informationssäkerhet tj	Tjänsteskrivelse	Ok
KS 2018-206-1 Strategi Informationssäkerhet	Strategi	Ok
KS 2018-206-2 Strategi för informationssäkerhet tj	Tjänsteskrivelse	Ok
Sociala medier och LinNet	Riktlinje	Ok
Säker hantering av mobila enheter	Riktlinje	Saknar versionsbeteckning Senast uppdaterat 2014-10-29
Tjänsteskrivelse Strategi för eSamhälle	Tjänsteskrivelse	Från 2012 att anta strategi för eSamhället utgiven av SKL
Strategi för eSamhället	Strategi	SKL:s styrelse har uppdragit åt SKL:s kansli att ta fram en strategi för att stödja utvecklingen av e-förvaltning inom kommunal sektor

2.2.2. *Bedömning*

PwC:s bedömning är att Lindesbergs kommun har nödvändig dokumentation på plats men att delar av den bör ses över och uppdateras.

Roll och ansvarsfördelningen vid en oönskad händelse bör tydliggöras för samtliga anställda. Det bör finnas en kunskap och förståelse hos de anställda hur Lindesberg kommun hanterar en eventuell IT-säkerhetsincident.

Riktlinjerna för informationssäkerhet hänvisar till annan dokumentation som vi inte kunnat ta del av. Denna dokumentation är inte framtagen ännu, men arbetet är pågående.

3. Bedömningar

3.1. Revisionell bedömning

Efter genomförd granskning är PwC:s sammanfattande bedömning att kommunstyrelsen **ej säkerställt** att Lindesbergs 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 upptäckte ej granskningen som genomfördes, vare sig under arbetet eller efteråt.
Hanteras icke önskvärda incidenter på ett ändamålsenligt sätt?	 Granskningen som utfördes återspeglar en reell attack, som bör ha identifierats som en incident, vilket den inte gjorde.
Hur är säkerheten avseende intrång av extern och intern aktör?	 Det finns många säkerhetshöjande åtgärder som är utförda i Lindesbergs kommun. För att säkerställa en god säkerhet finns det dock ytterligare åtgärder som behövs. Under granskningen kunde PwC tilldela sig själva högsta behörighet.
Finns det en tydlig roll- och ansvarsfördelning i frågor kring den övergripande IT-säkerheten?	 Det finns en beskriven roll och ansvarsfördelning som utförligt beskriver hur det ska fungera i organisationen. Detta behöver implementeras tydligt så varje roll förstår sitt ansvar under en eventuell informationssäkerhetsincident.
Finns det kända och tillämpade styrande dokument och riktlinjer för kommunens förebyggande arbete kring IT-säkerhet?	 PwC har tagit del av en utförlig dokumentation som beskriver kommunens policy och riktlinjer kring IT-säkerhet.
Finns det kända och tillämpade styrande dokument och riktlinjer att följa vid uppmärksammade risker eller vid ett intrång?	 Det finns skrivna och beslutade dokument för kommunens säkerhet där övergripande hantering av intrång tas upp. Dock har PwC inte kunnat ta del av de beskrivande dokumenten då dessa ej ännu är färdigställda.

3.3. Rekommendationer

Utifrån genomförd granskning lämnas följande rekommendationer.

3.3.1. Rekommendationer efter genomförda intrångstester

PwC rekommenderar att policyn för lösenord ses över för att undvika att svaga lösenord används i IT-miljön, samt för att begränsa möjligheten för en angripare att utföra lösenordsattacker. Lösenorden för servicekonton och andra högpriviligierade konton bör ha krav att vara längre och mer komplexa än vanliga konton. Rekommendationen är lösenord över 25 tecken, använda specialtecken och vara slumpmässigt framställda.

PwC rekommenderar att se över så att servrar konfigureras säkert samt att servrar och applikationer uppdateras löpande, oavsett om det är från Microsoft eller en 3-parts leverantör. Ett flertal servrar upptäcktes vara sårbara för välkända attacker vilket visar på bristande hantering av uppdateringar. Dessutom identifierades servrar ha standardkonfiguration, vilket medförde informationsläckage.

De externt publicerade delarna bör ses över och få skydd för att begränsa lösenordsgissning. Vi rekommenderar även att man implementerar stark autentisering för de applikationer som innehåller känslig information.

3.3.2. Rekommendationer efter genomförd dokumentgranskning

PwC rekommenderar att Lindesbergs kommun går igenom och uppdaterar den dokumentation som är från 2014 så är det blir aktuell information. Dokumentationen som finns beskriven men ej ännu är framtagen bör tas fram och beslutas i det fall en allvarlig incident skulle inträffa, så det finns riktlinjer att följa.

PwC rekommenderar att se 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.

2018-08-30

Tobias Bjöörn

Uppdragsledare

Mikael Grönvik

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.