KS § 9:6 Dnr. KS 2018/0165

Svar på revisionsrapport - Granskning av intrångsskydd

Kommunstyrelsens beslut

Godkänna kommunstyrelsens kontors handlingsplan enligt tjänsteutlåtande 2018-08-22.

Sammanfattning

Under första kvartalet 2018 genomfördes en granskning av intrångsskyddet av PwC på uppdrag av kommunens revisorer. För att höja IT-säkerheten föreslår revisorerna att kommunstyrelsen tar fram en handlingsplan med begäran om svar senast den 30 september 2018.

Beslutsunderlag

- Kommunstyrelsens arbetsutskott har behandlat ärendet 2018-09-05, § 7:3.
- Kommunstyrelsens kontors tjänsteutlåtande daterat 2018-08-22.

Förslag till beslut

Michaela Fletcher (M) yrkar bifall till arbetsutskottets beslutsförslag innebärande att godkänna kommunstyrelsens kontors handlingsplan enligt tjänsteutlåtande 2018-08-22.

Propositionsordning

Ordföranden frågar om Kommunstyrelsen beslutar enligt Michaela Fletchers (M) yrkande och finner att så är fallet.

Expedieras

- Förtroendevalda revisorerna
- PWC
- Kommunkansliet

Österåker

Tjänsteutlåtande

Kommunstyrelsens kontor
Datum 2018-08-22
Dnr 2018/0165 (4) ✓

Till Kommunstyrelsen

Svar på KS 2018/0165-01 - Revisionsrapport - Granskning av intrångsskydd

Sammanfattning

Under första kvartalet 2018 genomfördes en granskning av intrångsskyddet av PwC på uppdrag av kommunens revisorer. För att höja IT-säkerheten föreslår revisorerna att kommunstyrelsen tar fram en handlingsplan med begäran om svar senast den 30 september 2018.

Beslutsförslag

Kommunstyrelsens arbetsutskott föreslår kommunstyrelsen besluta
Godkänna kommunstyrelsens kontors handlingsplan enligt tjänsteutlåtande 2018-08-22

Bakgrund

IT enheten har under 2017 påbörjat arbetet med att kartlägga sårbarheter i IT säkerheten, bland annat genom att tillsammans med kommunens säkerhetsstrateg genomföra informationssäkerhetsklassning på kommunens verksamhetssystem för att kartlägga skyddsbehovet på de enskilda systemen. I december 2017 genomfördes en granskning av intrångsskyddet med hjälp av en extern leverantör för att kartlägga tekniska sårbarheter.
Utifrån det påbörjades en åtgärdsplan 2017 av IT enheten som bland annat innefattar

- Nytt utökat skalskydd (Brandvägg)
- Verktyg baserat på AI (Artificiell Intelligens) för att upptäcka systemavvikelser
- Uppdateringar av rutiner vid extern anslutning mot system.

IT-enhetens svar på PwC:s granskning

- IT-avdelningen uppmärksammade PwC:s angrepp och notifierade PwC att de blivit upptäckta cirka en timme efter att försöken påbörjades, vilket är mer än godkänt.

  Svar: IT-enheten vill tydliggöra att som rapporten visar så upptäcktes intrångsförsöket snabbt varpå larm skickades ut och kommunens säkerhetsstrateg informerades. Det hade normalt resulterat i åtgärder från vår sida, dvs. det är inte alls omöjligt att deras fullbordade intrång hade misslyckats.

- 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 finns inte rutinen dokumenterad.

Svar: Arbete med att dokumentera rutiner och riktlinjer är påbörjat, vilket kan ses i bilaga handlingsplan IT-säkerhet.

- IT-säkerheten håller en låg nivå och säkerheten avseende intrång av extern och intern aktör behöver prioriteras för att minimera framtida incidenter. PwC kunde skaffa högsta behörighet i domänen vilket inte borde vara möjligt

Svar: Som man kan läsa i den sekretessbelagda tekniska beskrivningen (*Intrångsanalys* avsnitt *Internt penetrationstest* sidan 9) skedde intrånget med en anslutning direkt till vårt administrativa nät, i våra låsta lokaler innanför brandväggen.
Det intrång som gjordes hade inte varit möjligt att fullborda utan dessa förutsättningar, vilket i normala fall skulle begränsa intrånget till att utföras av/genom anställd eller person med fysisk tillgång till våra lokaler.

De sårbarheter som upptäcktes tillgängliga externt, dvs utanför våra lokaler, eller från internet kunde inte ge åtkomst till information eller annan behörighet, utan endast för att skapa en bättre bild av vår IT-miljö och eventuellt utnyttjas för överbelastningsattacker.

De sårbarheter med riskgradering hög beror också på tidigare val gjorda av våra verksamheter, ett exempel är vårt tidigare ekonomisystem Visma RoR som lever kvar och är enbart till för våra revisorer och ekonomisk historik. Det finns inget supportavtal kvar på RoR och vi kan således inte uppdatera servern.
Vi är väl medvetna om dessa och har begränsat dessa system så mycket som möjligt för extern åtkomst. Helst skulle vi vilja stänga ned dessa, men det blir då på bekostnad av verksamheternas IT-stöd.
För att stävja liknande beslut framgent upprättades 2016 en IT-styrgrupp för att bland annat ge IT-enheten möjlighet att styra vilka systemval som görs av verksamheterna så att vi bygger en IT-miljö så att vi bygger en homogen IT-miljö som ges möjlighet att förvalta och underhålla på ett ändamålsenligt sätt.

- PwC har inte kunnat ta del av någon roll- eller ansvarsfördelning som avser kommunens IT-säkerhetsarbete.

Svar: Det har under året upprättats en Dataskyddsorganisation inom kommunen, främst för att stödja arbetet med nya dataskyddsförordningen GDPR. Men den nya organisationen kommer arbeta med att granska och övervaka efterlevnaden av

organisationens strategier i dataskyddsfrågor.

- PwC har inte kunnat ta del av någon dokumentation eller information som beskriver kommunens förebyggande arbete kring IT-säkerhet.

  Svar: Arbete med att förebygga risker kring IT-säkerheten är uppgifter som ingår i det dagliga arbetet varpå särskild dokumentation inte finns i nuläget, vi har dock tagit till oss av PwCs rutiner och arbetet med att tydliggöra rutiner och riktlinjer är påbörjat.

- Det finns inte några skrivna rutiner eller riktlinjer idag. Enligt uppgift pågår ett arbete med att dokumentera processen.

  Svar: Arbete med att förebygga risker kring IT-säkerheten är uppgifter som ingår i det dagliga arbetet varpå särskild dokumentation inte finns i nuläget, vi har dock tagit till oss av PwCs rutiner och arbetet med att tydliggöra rutiner och riktlinjer är påbörjat.

Förvaltningens slutsatser

IT-enheten jobbar ständigt med att ha en så säker miljö som möjligt utifrån de tekniska arv och förutsättningar som finns. I den sekretessbelagda tekniska rapport som IT-enheten har fått av PwC framgår att

- **7 st av de 8 sårbarheterna som är riskgraderade som hög genomfördes när PwC var direkt anslutna till det interna nätet**
- **IT-enheten fick av loggsystem larm inom en timme att det förekom avvikande aktiviteter i systemmiljön vilket i normala fall hade resulterat i åtgärder.**
- **Den sårbarhet som klassas som riskgrad hög vid det externa penetrationstestet kommer åtgärdas under början av hösten, arbetet är påbörjat.**
- **IT-enheten jobbar vidare med att dokumentera de inarbetade rutinerna som enligt PwC uppenbarligen fungerar.**
- **Utökning av skalskydd (brandvägg och redundant internetuppkoppling) är ett pågående arbete som kommer slutföras under hösten 2018.**
- **Det penetrationstest som beställdes av IT-enheten i december visar på en riskmedvetenhet och att IT-säkerhetsarbetet är ett kontinuerligt arbete som ständigt förändras där vi nyttjar expertis för att kartlägga sårbarheter.**

Tjänsteutlåtande

Förvaltningen anser med ovanstående redovisning att arbetet kring IT-säkerheten och revisorernas granskning är besvarad.

Bilagor

1. Handlingsplan IT-säkerhet

Jan-Olof Friman
Kommundirektör

Stefan Nyberg
IT-chef

Österåker

Handlingsplan ITsäkerhet

Österåker

1. Handlingsplan

IT-enheten har under 2017 och 2018 genomfört en del åtgärder som upptäcktes under de båda granskningarna av intrångsskydd, bland annat har de säkerhetshot som bedömdes som hög åtgärdats. De berodde på att gamla servrar hade startats under tiden för granskningen för att utföra ett test hos IT-enheten. Rutiner kring start av äldre system har uppdaterats.

Nedan följer handlingsplan av planerade åtgärder, IT-säkerhet är ett fortlöpande arbeta varpå handlingsplanen uppdateras allt eftersom arbetet fortlöper.

Åtgärd	Status	Ansvarig	Slutdatum
Uppdatering rutiner drift	Slutförd	IT-enheten	Maj 2018
Dataskyddsorganisation	Slutförd	Kommunledning	Augusti 2018
Lösenordspolicy systemkonton	Pågående	IT-enheten	Oktober 2018
Riktlinje extern anslutning	Slutförd	IT-enheten	Augusti 2018
Uppdatering IT styrdokument	Pågående	IT-enheten	December 2018
Uppdatering brandvägg	Upphandling pågår	IT-enheten	November 2018
Informationssäkerhetsklassning	Slutförd	Säkerhetsstrateg	Maj 2018
Redundant internetkoppling	Upphandling pågår	IT-enheten	Oktober 2018
Säker inloggning webmail	Pågående	IT-enheten	Oktober 2018
Anslutning eIDAS	Pågående	IT-enheten	September 2018

ÖSTERÅKERS KOMMUN
Revisorerna

Kommunstyrelsen
Kommunfullmäktige (för kännedom)

Granskning av intrångsskydd

Vi har låtit genomföra en granskning av intrångsskyddet i kommunens datasystem. Efter genomförd granskning är vår sammanfattande bedömning att Kommunstyrelsen ej säkerställt att Österåkers kommuns nuvarande tekniska IT-säkerhet är tillräcklig och tillfredsställande för att reducera risker för obehörigt intrång till en acceptabel nivå. Under testerna identifierades 18 stycken sårbarheter. Av dessa är 8 stycken riskgraderade som hög, 3 stycken som medel, 6 stycken som låg och 1 som information.

Granskningen visar därutöver följande:

- IT-avdelningen uppmärksammade PwC:s angrepp och notifierade PwC att de blivit upptäckta cirka en timme efter att försöken påbörjades, vilket är mer än godkänt.
- 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 finns inte rutinen dokumenterad.
- IT-säkerheten håller en låg nivå och säkerheten avseende intrång av extern och intern aktör behöver prioriteras för att minimera framtida incidenter. PwC kunde skaffa sig högsta behörighet i domänen vilket inte borde vara möjligt.
- PwC har inte kunnat ta del av någon roll- eller ansvarsfördelning som avser kommunens IT-säkerhetsarbete.
- PwC har inte kunnat ta del av någon dokumentation eller information som beskriver kommunens förebyggande arbete kring IT-säkerhet.
- Det finns inte några skrivna rutiner eller riktlinjer i dag. Enligt uppgift pågår ett arbete med att dokumentera processen.

Utifrån granskningen rekommenderar vi:

- att rutiner för att härda servrar ses över så att servrar konfigureras säkert samt att servrar och applikationer uppdateras löpande. Ett flertal servrar upptäcktes vara sårbara för välkända attacker vilket visar på bristande hantering av uppdateringar. Dessutom konstaterades flera servrar ha bristande konfiguration och standardkonfiguration, vilket medför informationsläckage.
- 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 vara långa, över 25 tecken, använda specialtecken och vara slumpmässigt framställda.

- att 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. Detta omfattar både interna samt externa tjänster såsom Office 365 och webbmail.
- att Österåkers 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. Österåkers kommun bör ha uppdaterade och aktuella strategiska dokument som beskriver vart kommunen är på väg och vad man har för ambitioner, detta för att IT-avdelningen och andra delar av kommunens verksamhet som är beroende av IT-miljön skall veta vilket fokus som skall hållas.
- att en årlig revidering av dokumentationen införs samt att det tillses att ägare, datum, versionsnummer samt versionshistorik finns med i all dokumentation, för att man enkelt skall kunna 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.

Därutöver rekommenderar vi att kommunstyrelsen säkerställer att IT-avdelningen får tillgång till verktyg som möjliggör identifiering/detektering av intrång eller onormal nätverkstrafik för att höja IT-säkerheten till en acceptabel nivå.

Vi översänder granskningsrapporten till kommunstyrelsen med begäran om svar senast den 30 september 2018, innehållande en tidssatt handlingsplan för att öka IT-säkerheten i kommun.

För Österåkers kommuns revisorer, 2018-05-15

Bengt Olin
Ordförande i kommunrevisionen

www.pwc.se

Revisionsrapport

Granskning av intrångsskydd

Österåkers kommuns förtroendevalda revisorer

Niklas Ljung
Mattias Gröndahl

April/2018

pwc

Innehåll

Sammanfattning

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

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

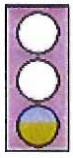
Har kommunstyrelsen säkerställt att Österåkers kommuns nuvarande tekniska IT-säkerhet är tillräcklig och tillfredsställande för att reducera risker för obehörigt intrång till acceptabel nivå?

Efter genomförd granskning är vår sammanfattande bedömning att kommunstyrelsen **ej säkerställt** att Österåkers kommuns nuvarande tekniska IT-säkerhet är tillräcklig och tillfredsställande för att reducera risker för obehörigt intrång till en acceptabel nivå.

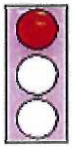
Den sammanfattande bedömningen baseras på bedömningarna av de sex kontrollfrågorna för granskningen, vilka redovisas i rapporten.

Kontrollfråga 1
Upptäcks en eventuell attack?

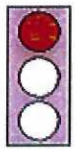
Kontrollfråga 2
Hanteras icke önskvärda incidenter på ett ändamålsenligt sätt?



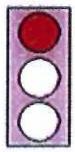
Kontrollfråga 3
Hur är säkerheten avseende intrång av extern och intern aktör?



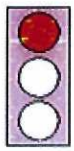
Kontrollfråga 4
Finns det en tydlig roll- och ansvarsfördelning i frågor kring den övergripande IT-säkerheten?



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 Österåkers 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 Österåkers 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:

- 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 Österåkers 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 Österåkers 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 Österåkers kommun.
- IT-arkitekten i Österåkers kommun.

2. Resultat

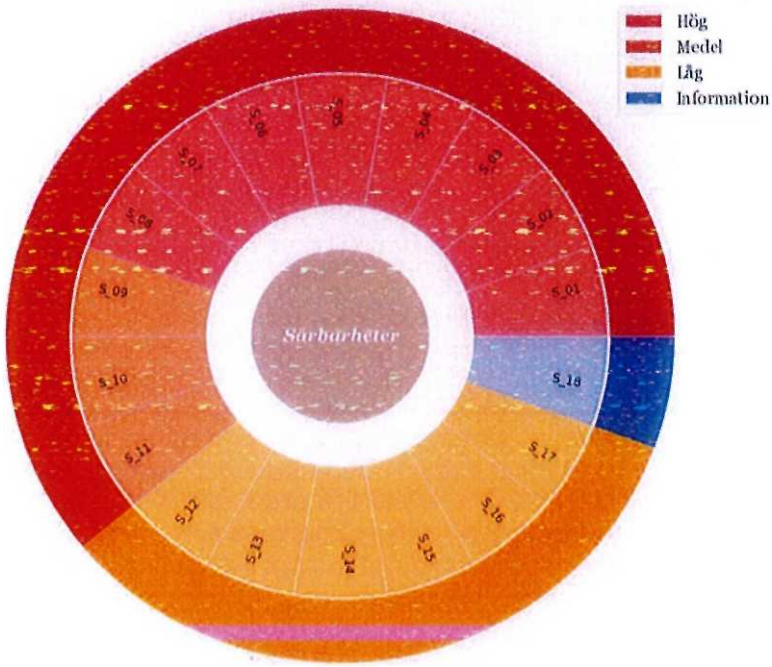
2.1. Intrångstester

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 **18** st. sårbarheter. Av dessa är **8** st. riskgraderade som **hög**, **3** st. som **medel**, **6** st. som **låg** och **1** 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 Österåkers kommun.

2.1.2. Bedömning

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

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

Ett flertal servrar upptäcktes vara sårbara för välkända attacker vilket visar på bristande hantering av uppdateringar. Dessutom identifierades flera servrar ha bristande konfiguration och standardkonfiguration, vilket medför informationsläckage.

Under testerna kunde PwC anskaffa sig högsta behörighet i domänen. Domänadministratör är den högsta behörighetsgruppen i en domän, vanligtvis förunnat senior personal på IT.

Efter utvärdering av resultatet anses säkerhetsnivån vara i nivå med en likvärdig kommun i Österåkers storlek.

2.2. Dokumentgranskning

2.2.1. Iakttagelser

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

PwC informerade om att syftet med dokumentgranskningen var att se vilken IT-dokumentation som finns i Österåkers 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, 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.

2.2.2. Bedömning

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

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

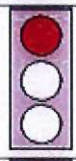
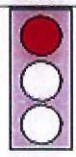
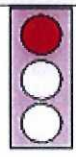
IT-organisationen bör göra en kraftansträngning och inventera sin dokumentation, skapa den dokumentation som i dag saknas och uppdatera den dokumentation som har blivit föråldrad.

3. Bedömningar

3.1. Revisionell bedömning

Efter genomförd granskning är PwC:s sammanfattande bedömning att kommunstyrelsen **ej säkerställt** att Österåkers 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 angrep och notifierade PwC att de blivit upptäckta cirka en timme efter att försöken påbörjades, vilket är mer än godkänt.
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 finns inte rutinen dokumenterad, se sista kontrollfrågan.
Hur är säkerheten avseende intrång av extern och intern aktör?	 IT-säkerheten håller en låg 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.
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.
Finns det kända och tillämpade styrande dokument och riktlinjer att följa vid uppmärksammade risker eller vid ett intrång?	 Det finns inte några skrivna rutiner eller riktlinjer i dag. Enligt uppgift pågår ett arbete med att dokumentera processen.

3.3. Rekommendationer

Utifrån genomförd granskning lämnas följande rekommendationer.

3.3.1. Rekommendationer efter genomförda intrångstester

PwC rekommenderar att rutinen för att härda servrar ses över så att servrar konfigureras säkert samt att servrar och applikationer uppdateras löpande. Ett flertal servrar upptäcktes vara sårbara för välkända attacker vilket visar på bristande hantering av uppdateringar. Dessutom identifierades flera servrar ha bristande konfiguration och standardkonfiguration, vilket medför informationsläckage.

Vidare rekommenderas 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 vara långa, över 25 tecken, använda specialtecken och vara slumpmässigt framställda.

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. Detta omfattar både interna samt externa tjänster så som Office 365 och webbmail.

3.3.2. Rekommendationer efter genomförd dokumentgranskning

PwC rekommenderar att Österåkers 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.

PwC rekommenderar att en årlig revidering av dokumentationen bör införas samt 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.

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.

2018-04-30

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.