DocuSign Envelope ID: 9F36B909-18F2-46D3-812D-D61080393EF9

Granskning av it- och cybersäkerhet

Rapport

Örnsköldsviks kommun

KPMG AB

2023-12-04

Antal sidor: 12

© 2023 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Document classification: KPMG Public

DocuSign Envelope ID: 9F36B909-18F2-46D3-812D-D61080393EF9

Örnsköldsviks kommun
Granskning av it- och cybersäkerhet

2023-12-04

Innehållsförteckning

© 2023 KPMG AB. All rights reserved.

Document classification KPMG Public

DocuSign Envelope ID: 9F36B909-18F2-46D3-812D-D61080393EF9

Örnsköldsviks kommun
Granskning av it- och cybersäkerhet

2023-12-04

1 Sammanfattning

KPMG har av Örnsköldsviks kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunens it- och cybersäkerhetsarbete. Uppdraget ingår i revisionsplanen för år 2023.

Granskningen har syftat till att bedöma om kommunstyrelsen har en tillräcklig styrning och intern kontroll avseende it- och cybersäkerhetsarbetet, och har tillsett att arbetet bedrivs ändamålsenligt.

Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsen i allt väsentligt har en tillräcklig styrning och intern kontroll avseende detta, samt att arbetet sker på ett ändamålsenligt sätt.

Bedömningen baseras bland annat på att it-säkerhetsarbetet i hög grad når upp till kommunens beslutade standard för arbetet samt att åtgärder är etablerade i enlighet med Myndigheten för samhällsskydd och beredskaps rekommendationer för stärkt cyberförsvar. Beslutade organisations- och samverkansformer inom it-området möjliggör att hela kommunorganisationen omfattas av den systematik och riskmedvetenhet som it-säkerhetsarbetet utgår från. Förhållningssättet innebär även att risker och hot utvärderas kontinuerligt och ligger till grund för etablerade säkerhetsåtgärder. Vi bedömer dock att det föreligger en variation till efterlevnad av styrande dokument samt att uppföljning av informations- och it-säkerhetsarbetet till kommunstyrelsen behöver formaliseras.

Nedan följer våra bedömningar och rekommendationer.

Revisionsfråga	**Bedömning: i allt väsentligt**	**Rekommendationer**
Finns en ändamålsenlig organisation för IT-säkerhetsarbetet?	Kommunen har etablerat en organisation med förutsättningar att kunna säkerställa driften av kommunens it-miljö samt för att kunna bedriva ett förebyggande it-säkerhetsarbete i förhållande till nuvarande hot och risker. Det finns risk för att viss dokumentation och följsamhet till rutiner inte upprätthålls på grund av storlek på nuvarande organisation.	- Utvärdera it-enheten nuvarande bemanning så att den är anpassad till omfattning och krav i styrande dokument och den standard som kommunen beslutat om.
Revisionsfråga	**Bedömning: delvis**	**Rekommendationer**
Finns aktuella styrdokument i form av policys och riktlinjer för informationssäkerhet där IT-säkerhet ingår? och säkerställs det att dessa följs?	Det finns styrande dokument som ger förutsättningar för ett ändamålsenligt informations- och it-säkerhetsarbete. Dokumenten är dock i behov av översyn och efterlevnaden till dem varierar.	- Slutföra den pågående översynen av styrande dokument - Säkerställa att styrande dokument efterlevs

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

DocuSign Envelope ID: 9F36B909-18F2-46D3-812D-D61080393EF9

Revisionsfråga	Bedömning: i allt väsentligt	Rekommendationer
Finns etablerade arbetssätt och metoder för riskbedömning och vidtas erforderliga tekniska säkerhetsåtgärder som ett resultat av dessa?	Riskbedömningar och informationsklassning är tydligt reglerade i styrande dokument.	Inga rekommendationer
Revisionsfråga	**Bedömning: i allt väsentligt**	**Rekommendationer**
Finns det en tillräcklig uppföljning av att de säkerhetsåtgärder som är vidtagna fungerar ändamålsenligt?	Det finns ett systematiserat arbetssätt där säkerhetsåtgärder etableras och följs upp utifrån regulatoriska krav och rekommendationer från Myndigheten för samhällsskydd och beredskap. Styrande dokument behöver dock revideras för att anpassas till nuvarande behov av kravställning av it-säkerhetsåtgärder.	- Slutföra den pågående översynen av styrande dokument
Revisionsfråga	**Bedömning: ja**	**Rekommendationer**
Finns en tillräcklig kontroll för att upptäcka eventuella hot om intrång eller andra incidenter i IT-system?	Det finns en tillräcklig kontroll för att upptäcka hot om intrång och andra incidenter.	Inga rekommendationer
Revisionsfråga	**Bedömning: ja**	**Rekommendationer**
Finns etablerade rutiner med tydliggjorda eskaleringsvägar vid säkerhetshändelser och incidenter?	Incidenter hanteras i linje med vad som anges av styrande dokument. Kommunstyrelsen har säkerställt rutiner för att kunna hantera händelser utanför kontorstid.	Inga rekommendationer
Revisionsfråga	**Bedömning: delvis**	**Rekommendationer**
Finns dokumenterade reserv- och återgångsrutiner vid allvarligare störningar och avbrott i IT-system och har dessa testats för att säkerställa att de fungerar ändamålsenligt?	Det finns utkast till en kontinuitetsplan. Reserv- och återgångsrutiner har testats med tillfredsställande resultat. Överenskomna servicenivåer är en god vägledning för återgångsrutiner, vilket i stora delar saknas vid tid för granskningen.	- Fastställa kontinuitetsplan och tillse att det i övrigt finns tillgång till tillräckliga underlag så att ansvariga vid händelse kan tillse en robust återställning av it-miljön.

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

DocuSign Envelope ID: 9F36B909-18F2-46D3-812D-D61080393EF9

Revisionsfråga	Bedömning: delvis	Rekommendationer
Finns beslutade uppföljningsrutiner för IT-säkerhetsarbetet och är återrapporteringen till kommunstyrelsen tillräcklig?	Ledningens genomgång har rapporterats till kommunstyrelsen med en samlad uppföljning av informationssäkerhetsarbetet. Det har även vid andra tillfällen lämnats information om it-säkerhet till kommunstyrelsen eller dess arbetsutskott. Vi konstaterar att uppföljningsrutiner i förhållande till kommunstyrelsen inte regleras i styrande dokument vilket bör revideras i samband med översyn av styrande dokument.	- Formalisera former för uppföljning mot kommunstyrelsen

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

DocuSign Envelope ID: 9F36B909-18F2-46D3-812D-D61080393EF9

2 Bakgrund

KPMG har av Örnsköldsviks kommun förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunens it- och cybersäkerhetsarbete. Uppdraget ingår i revisionsplanen för år 2023.

Organisationer i offentlig sektor hanterar ovärderliga informationstillgångar och blir alltmer beroende av informationssystem. Ny teknik innebär nya möjligheter men introducerar även nya risker som ställer krav på ett balanserat risktagande och ett väl fungerande säkerhetsarbete.

Informationssäkerhet innebär att information ska skyddas utifrån principerna om riktighet, tillgänglighet, konfidentialitet och spårbarhet. Samhällets digitalisering innebär att det har skapats ett beroende av kontinuerligt fungerande informations- och kommunikationsteknik. Utvecklingen och den förändrade användningen av ny teknik innebär också att hot blir svårare att upptäcka, att risker blir mer svårbedömda och att beroenden blir svårare att kartlägga.

Den digitala utvecklingen måste följas av ett anpassat och balanserat säkerhetsarbete för att säkerställa att system och digitala tjänster som nyttjas för informationshantering och lagring är inte exponerade och tillgängliga för cyberhot och angrepp. Där tekniken implementeras på ett ogenomtänkt eller otillräckligt sätt uppstår brister som kan utnyttjas av hotaktörer. Hotbilden med risker för intrång förändras kontinuerligt och IT-säkerhetsarbetet behöver därför vara en ständigt pågående process för att säkerställa att kommunens informationstillgångar har ett tillräckligt skydd.

Brister i informationshanteringen och säkerhetsarbetet kan få allvarliga konsekvenser, till exempel att integritetskänslig information sprids eller att verksamhetskritiska processer stoppas. Detta kan leda till både ekonomisk skada och förtroendeskada för kommunen. För att möta utmaningarna framgent krävs att kommunen har ett systematiskt och tvärfunktionellt IT- och cybersäkerhetsarbete, med en tydlig roll- och ansvarsfördelning

Med anledning av ovanstående drar kommunens revisorer slutsatsen i sin riskanalys, att arbetet med it- och cybersäkerhet behöver granskas.

2.1 Syfte

Granskningen har syftat till att bedöma huruvida kommunstyrelsen har en tillräcklig styrning och intern kontroll avseende it- och cybersäkerhetsarbetet och har tillsett att arbetet bedrivs ändamålsenligt.

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

DocuSign Envelope ID: 9F36B909-18F2-46D3-812D-D61080393EF9

Granskningen har besvarat följande revisionsfrågor:

- Finns det en ändamålsenlig organisation för IT–säkerhetsarbetet?
- Finns aktuella styrdokument i form av policys och riktlinjer för informationssäkerhet där IT-säkerhet ingår och säkerställs det att dessa följs?
- Finns det etablerade arbetssätt och metoder för riskbedömning och vidtas erforderliga tekniska säkerhetsåtgärder som ett resultat av dessa?
- Finns en tillräcklig kontroll för att upptäcka eventuella hot om intrång eller andra incidenter i IT-system?
- Finns det en tillräcklig uppföljning av att de säkerhetsåtgärder som är vidtagna fungerar ändamålsenligt?
- Finns etablerade rutiner med tydliggjorda eskaleringsvägar vid säkerhetshändelser och incidenter?
- Finns dokumenterade reserv- och återgångsrutiner vid allvarligare störningar och avbrott i IT-system och har dessa testats för att säkerställa att de fungerar ändamålsenligt?
- Finns beslutade uppföljningsrutiner för IT-säkerhetsarbetet och är återrapporteringen till kommunstyrelsen tillräcklig?

2.2 Avgränsning

Granskningen har omfattat kommunstyrelsens övergripande ansvar för styrning och uppföljning av it-säkerhetsarbetet och avser revisionsåret 2023.

2.3 Revisionskriterier

Vi har bedömt om rutinerna uppfyller:

- Kommunallagen 6 kap. 6 §
- Tillämpbara interna regelverk, policys och beslut
- MSB:s rekommendationer avseende Ledningssystem för informationssäkerhet och it-säkerhetsåtgärder
- NIS-direktivet när detta är tillämpbart

2.4 Ansvarig nämnd/styrelse

Granskningen har avsetts kommunstyrelsen.

2.5 Metod

Viktigt att veta vid denna typ av granskning är att detaljnivån, exempelvis avseende detaljerade information rörande it-tekniska säkerhetsimplementationer endast kommer att beskrivas översiktligt. Detta för att eventuell känslig information om kommunens skydd inte ska offentliggöras.

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

DocuSign Envelope ID: 9F36B909-18F2-46D3-812D-D61080393EF9

Granskningen har genomförts med dokumentstudier och intervjuer/avstämningar med följande funktioner:

- Kommunstyrelsens presidium
- Kommundirektör
- Digitaliseringschef
- Informationssäkerhets-samordnare
- Enhetschef it-enheten

Samtliga intervjuade har getts möjlighet att faktakontrollera rapporten.

Dokumentanalysen har bland annat omfattat övergripande styrdokument fastställda av kommunfullmäktige och kommunstyrelsen. Exempel på styrande dokument är reglemente för styrelser och nämnder i Örnsköldsviks kommun, informationssäkerhetsstrategi och Riktlinjer för informationssäkerhetsklassning. Dokumentgranskning har även inkluderat uppföljning av det övergripande informationssäkerhetsarbetet.

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

DocuSign Envelope ID: 9F36B909-18F2-46D3-812D-D61080393EF9

3 Resultat

3.1 Styrning och organisation av it-säkerhetsarbetet

3.1.1 Styrande dokument inom informationssäkerhet och it-säkerhet

Kommunfullmäktige har antagit en policy för informationssäkerhet och dataskydd[1] som gäller för hela kommunkoncernen. Enligt policyn ska kommunens informationssäkerhetsarbete vara systematiskt och utgå från standardserien ISO/IEC 27000. Policyn ger också principiella grunder för dataskyddsarbetet, och ska enligt dokumentet revideras årligen eller vid behov.

Policyns innehåll förtydligas av informationssäkerhetsstrategin[2] som även den omfattar hela kommunkoncernen. Till dessa centrala dokument är ett antal riktlinjer och rutiner kopplade, vilka konkretiserar policy och strategi ytterligare.

Genom granskningen har vi fått bild av att de styrande dokumenten är etablerade, men att de behöver revideras ur aktualitetshänseende, bland annat utifrån förändrade säkerhetsförutsättningar. En ambition som uttrycks är att integrera informationssäkerhetsarbetet tydligare i kommunens övergripande säkerhetsarbete, vilket också ska få genomslag i styrande dokument.

3.1.2 Organisation och ansvar informationssäkerhet

Enligt kommunstyrelsens reglemente ansvarar styrelsen för kommunens digitalisering, intern drift och övergripande administrativa system. Styrelsen är också ansvarig för att följa upp beslut fattade av kommunstyrelsen, samt vad som anges i lagar och andra författningar inom respektive verksamhetsområde. Det ankommer också styrelsen att tillse att organisationen för att detta är ändamålsenlig.

Enligt policyn för informationssäkerhet och dataskydd ansvarar nämnder och kommunala bolag för arbetet med informationssäkerhet inom respektive verksamhetsområde. Övergripande ansvar för att samordna och utöva tillsyn av informationssäkerhetsarbetet har kommunledningsförvaltningen.

I informationssäkerhetsstrategin förtydligas roller och ansvar ytterligare. Här framgår att kommunstyrelsen har det yttersta ansvaret för kommunkoncernens informationssäkerhetsarbete, liksom att kommundirektör ska fördela resurser och tillse att informationssäkerhetsarbetet bedrivs effektivt.

Av strategin klargörs även att ansvar för informationssäkerhet följer linjeansvaret, varvid förvaltningschefer ska tillse att erforderliga roller och ansvar samt resurser finns angivna inom respektive förvaltning. Strategin anger därtill att samtliga förvaltningar och kommunala bolag ska uppdra en funktion att bedriva informationssäkerhetsarbetet inom respektive verksamhet.

[1] 2019-12-16
[2] 2019-12-03

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

DocuSign Envelope ID: 9F36B909-18F2-46D3-812D-D61080393EF9

Avseende den centrala organiseringen av arbetet finns inom kommunledningsförvaltningen en utvecklingsavdelning som leds av digitaliseringschef, tillika it-säkerhetsansvarig. Avdelningen består av två enheter, enheten Digital utveckling samt it-enheten. Till enheten Digital utveckling hör en informationssäkerhetssamordnare, som, enligt informationssäkerhetsstrategin, ska samordna arbetet och utveckla kommunens strategiska säkerhetsarbete.

Informationssäkerhetsstrategin anger vidare att kommunen ska ha ett informationssäkerhetsråd som ska utveckla informationssäkerhetsarbetet på övergripande nivå samt följa verksamheternas behov av stöd. Vi har tagit del av en dokumenterad beskrivning av representationen i rådet och dess uppgifter. Rådet har enligt underlag för momentet Ledningens genomgång[3] för 2022–2023 funnits sedan år 2018. Det finns även ett informationssäkerhetsråd med nyckelfunktioner i informationssäkerhetsarbetet (inkluderat it-säkerhet). Dessa grupperingar uppges enligt dokumentationen fungera som ett stöd och möjliggör för informationssäkerhetssamordnare och dataskyddsombud att nå ut till de olika verksamheterna och skapa ett samarbete i syfte att nå en god säkerhetskultur.

Uppgifter från intervjuer bekräftar att det dokumenterade arbetssättet tillämpas i praktiken. Den bild vi fått är att informationssäkerhetssamordnare har en aktiv roll, både som kravställare mot it-enheten i syfte att tillse att administrativa informationssäkerhetsåtgärder motsvaras av tillbörliga it-tekniska åtgärder. Vi uppfattar även att funktionen bedriver ett aktivt arbete som samordnare och utförare av stöd till de decentraliserade funktioner för informationssäkerhetsarbete som har etablerats inom förvaltningar och bolag.

3.1.3 Organisation och ansvar it-säkerhet

Av informationssäkerhetsstrategin framgår att digitaliseringschef är ytterst ansvarig för kommunens it-enhet. Som nämnts i föregående rapportavsnitt är it-enheten en av två enheter inom utvecklingsavdelningen.

It-enheten leds av en enhetschef och är indelad i två team: drift respektive support. Operativt it-säkerhetsarbete hanteras inom it-enheten, varvid enhetschef har operativt ansvar för it-säkerhet. Enheten består av 30 medarbetare. Intervjuade uppger dock att det finns behov av ytterligare resursförstärkning då nuvarande behov och krav uppfattas motsvara ytterligare ett par helårsarbetare.

En konsekvens av hög belastning uppges ha blivit att efterlevnad till beslutade dokument och processer, liksom sammanställning av dokumentation, är varierande bland it-enhetens medarbetare. Enhetens ledning upplever att det finns behov av motsvarande en it-säkerhetssamordnare som kan ha ett övergripande perspektiv och stödja medarbetare i att arbeta enligt rutiner och styrande dokument.

Vid sidan av linjeorganisationen finns en riktlinje för systemförvaltning[4] som konkretiserar kommunens systemförvaltarorganisation. Riktlinjen redogör för ansvar och befogenheter som åvilar de funktioner som ingår i förvaltningsmodellen.

[3] En aktivitet då det samlade informationssäkerhetsarbetet (eller säkerhetsfrågor mer övergripande) presenteras för ledningen.
[4] Ej daterad

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

DocuSign Envelope ID: 9F36B909-18F2-46D3-812D-D61080393EF9

Funktionernas arbetsuppgifter framgår av ett årshjul som innehåller flera aktiviteter med bäring på informationssäkerhet- och it-säkerhet.

Även om informationssäkerhetsaktiviteter ingår i systemförvaltningen råder olika uppfattningar om i vilken utsträckning som arbetet beaktas. 2011 flyttades informationssäkerhetssamordnaren, som tidigare tillhörde it-enheten, till utvecklingsavdelningen inom kommunledningsförvaltningen. Vissa intervjuade menar att det bidragit till en tydligare gränsdragning där informationssäkerhetssamordnare kan agera kravställare av it-säkerhetsåtgärder som behöver vidtas för att skydda informationstillgångar. Andra upplever att informationssäkerhetsarbetet nu i första hand drivs av informationssäkerhetssamordnare och som en parallell process vid sidan av mer it-säkerhetsbetonat arbete. Från samtliga konstateras arbetssättet ha förbättringspotential då informationssäkerhet och it-säkerhet konstateras gå hand i hand och ha ett ömsesidigt beroende.

3.1.4 Bedömning

Vår bedömning är att det delvis finns aktuella styrdokument för informations- och it-säkerhet och att dessa delvis följs.

Vi anser att ledningssystemet omfattar dokument och processer som grundlägger ett ändamålsenligt informations- och it-säkerhetsarbete. Mot bakgrund av att styrdokumenten är från år 2019 ser vi behov av att dessa revideras. MSB rekommenderar att policy för informationssäkerhet inte ska vara äldre än tre till fem år med tanke på den snabba förändring som sker inom området. En översyn kan även behövas mot bakgrund av aktuellt säkerhetsläget, då risker och krav förändras i snabb takt och ställer utökade krav på informations- och it-säkerhetsarbete i syfte att undvika cybersäkerhetsrisker och andra skador på kommunens informationstillgångar.

Mot bakgrund av granskningens avgränsning har vi inte granskat hur informationssäkerhetsarbetet fungerar i kommunens förvaltningar och bolag, vi har dock fått uppgifter som påvisar risk för att styrdokumenten i efterlevs fullt ut i nuläget och att detta behöver stärkas.

Vi bedömer att det i allt väsentligt finns en ändamålsenlig organisation för it-säkerhetsarbetet.

Vi anser att kommunen har etablerat en organisation med förutsättningar att kunna säkerställa driften av kommunens it-miljö samt för att kunna bedriva ett förebyggande it-säkerhetsarbete.

Vi uppfattar dock att det finns risk för att viss dokumentation och följsamhet till rutiner inte upprätthålls på grund av storlek på nuvarande organisation.

Vi bedömer att kommunstyrelsen genom beslutade anslag för it-säkerhetsarbetet skapat förutsättningar för ett ändamålsenligt it-säkerhetsarbete. Vi uppfattar att berörda funktioner har förtroende och mandat från kommunledning för att vid behov ta avgörande beslut avseende it- och cybersäkerheten i syfte att skydda kommunens informationstillgångar.

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

DocuSign Envelope ID: 9F36B909-18F2-46D3-812D-D61080393EF9

Mot bakgrund av granskningens avgränsning har vi inte granskat hur informationssäkerhetsarbetet fungerar i kommunens förvaltningar och bolag. Vi bedömer emellertid att beslutade samverkansformer inom it-området möjliggör att hela kommunorganisationen omfattas av den systematik och riskmedvetenhet som it-enheten arbetar utifrån.

3.2 It-säkerhetsarbetet i praktiken

3.2.1 Riskbedömning

Enligt informationssäkerhetsstrategin ska kommunens informationstillgångar riskbedömas och informationsklassas som grund för att kunna vidta erforderliga säkerhetsåtgärder. Riskanalyser ska också följas upp i syfte att identifiera vilka system som inte riskbedömts.

Ansvar för att tillse riskbedömning och informationsklassning är ägaren till respektive informationstillgång, vilket också anges av Riktlinjer för systemförvaltning.

Vid implementering av ett nytt system tydliggörs av Riktlinjer för it-införandeprocessen[5] att informationsklassning och riskbedömning ska genomföras som del i förberedelser inför upphandling.

Vår uppfattning utifrån intervjuer och dokumentgranskning är att informationsklassningar och riskbedömningar genomförs strukturerat enligt nämnd process. Genomförande av riskbedömning och informationsklassning framgår av riktlinjer för informationsklassning[6], i vilken KLASSA[7] föreslås som arbetsmodell.

Enligt Riktlinjer för systemförvaltning ska it-strateg alltid involveras vid införande av ett system. Vi uppfattar att det inte alltid är fallet då initiativ till att genomföra informationsklassningar tas av den verksamhet som nyttjar systemet. Däremot uppges att it-personal konsekvent involveras i riskbedömning i de fall där informationsklassning påvisar särskilda behov.

I kommunen har ett stödsystem etablerats där den samlade dokumentationen för informationssäkerhet, dataskydd och systemförvaktningen finns. I systemet finns rutiner och processer som stöd i de moment som ska genomföras, bland annat riskanalys och informationsklassningar. Den samlade dokumentationen uppfattas bidra till goda möjligheter för nyckelpersoner att få del av dokumentation och även för uppföljningsarbetet.

Enligt det underlag som vi tagit del av i Ledningens genomgång 2022-2023 framgår att riskanalyser har genomförts för ett flertal olika system, processer och informationstillgångar. Vidare beskrivs att åtgärder för identifierade risker har prioriterats utifrån vilka som är störst och mest kritiska för att trygga informationstillgångar och efterleva regulatoriska krav.

[5] 2019-03-26
[6] Reviderad 2020-01-24
[7] Modell för riskbedömning och informationsklassning, framtagen av Sveriges kommuner och regioner, SKR.

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

DocuSign Envelope ID: 9F36B909-18F2-46D3-812D-D61080393EF9

Enligt dokumentation för ledningens genomgång har arbetet med informationsklassning och riskbedömning varit ett prioriterat fokusområde under år 2022. Informationssäkerhetssamordnare har i hög grad deltagit i klassningsarbetet som stöd till verksamheterna men även dataskyddsombud uppges delta aktivt vid klassningar.

3.2.2 Bedömning

Vi bedömer att det i allt väsentligt finns etablerade arbetssätt och metoder för riskbedömning, och att arbetssättet ligger till grund för att tekniska säkerhetsåtgärder vidtas som resultat av detta.

Riskbedömningar och informationsklassning är, enligt vår bedömning, tydligt reglerade i styrande dokument, och tillvägagångssätt följer till stor del dessa.

3.3 Implementerade säkerhetsåtgärder

I informationssäkerhetsstrategin framgår principiell kravställning avseende säkerhetsåtgärder som ska vidtas för att skydda kommunens it-miljö. Dock anses dokumentet inte motsvara tillräcklig säkerhetsnivå, varför etablerade it-säkerhetsåtgärder baseras på Myndigheten för samhällsskydd och beredskaps rekommendationer samt lagstiftningar som är gällande för kommunens olika verksamheter. Däribland NIS-direktivet[8] som är ett av de regelverk mot vilket kommunen utvärderar etablerade säkerhetsåtgärder. Med anledning av direktivet har kommunen identifierat och anmält tre verksamheter[9] som samhällsviktiga.

Enligt kommunens mål och budget-dokument[10] har kommunfullmäktige anslagit 20 miljoner kronor årligen mellan 2023 och 2027 till it-investeringar. I intervju med kommunstyrelsens presidium framhålls att det specifikt avser stärkta it-säkerhetsåtgärder. Företrädare för it-enheten uppger att förstärkningen täckt kostnader för livscykelhantering.

Vi har i granskningen fått en detaljerad beskrivning av de tekniska säkerhetsåtgärder som it-enheten har etablerat. Vi kan konstatera att dessa har etablerats utifrån en prioritering och att de är överensstämmande med åtgärder som Myndigheten för samhällsskydd och beredskaps rekommenderar för stärkt cyberförsvar, samt i linje med de säkerhetsmässiga krav som ställs på it-miljön informationssäkerhetsstrategin.

Vi uppfattar därtill att det finns ett systematiserat arbete med teknisk uppföljning av implementerade säkerhetsåtgärder. Dels utvärderas dessa kontinuerligt, enligt ett årshjul, i förhållande till legala krav. Dels har it-enheten köpt in ett verktyg för automatiserad testning av it-miljön, vilket identifierar åtgärder som behöver vidtas för ökad säkerhet, exempelvis om det finns mjukvara som inte är uppdaterad.

[8] NIS-direktivet (Directive on security of network and information systems) är ett EU-direktiv som omsätts I svensk lag genom Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster.
[9] Välfärdsförvaltningen, Övik Energi och Miva bedriver samhällsviktig verksamhet.
[10] Budget 2023, plan 2024-2026, daterad 2022-10-24

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

DocuSign Envelope ID: 9F36B909-18F2-46D3-812D-D61080393EF9

3.3.1 Bedömning

Vår bedömning är att det finns en tillräcklig uppföljning av att vidtagna säkerhetsåtgärder fungerar ändamålsenligt.

Kommunen har ett systematiserat arbetssätt där säkerhetsåtgärder etableras och följs upp utifrån regulatoriska krav och rekommendationer från Myndigheten för samhällsskydd och beredskap. Utifrån vad som delgetts oss i intervjuer anser vi att kommunen, så långt vi kan bedöma, vidtagit erforderliga tekniska säkerhetsåtgärder som står i paritet med aktuell hot- och riskbild.

Vi bedömer att arbetet ytterligare skulle kunna stärkas av att de styrande dokumenten i högre grad är anpassade efter aktuella hot, risker och krav för informationssäkerhetsarbetet. Vi uppfattar att nuvarande styrande dokument inte regelmässigt inkluderas som grund för det löpande arbetet. Det kan därför finnas risk för en försvagad styrning av it-säkerhetsfrågor.

3.4 Övervakning och loggning

I informationssäkerhetsstrategin regleras krav på övervakning och loggning i syfte att detektera intrångsförsök. Kommunen har för ändamålet avtalat en extern tjänst för löpande dygnet runt-övervakning av it-miljön. Tjänsten inkluderar resurser med kapacitet att ta hand om större störningar i det direkta skedet. Via tjänsten får kommunen veckovis uppföljning av inträffade händelser samt en fördjupad rapport en gång i kvartalet.

Utöver ovan anges behov av att implementera ett effektivare verktyg för detektering, som i realtid ger möjlighet att upptäcka skadlig kod som infiltrerat it-miljön. Dylikt verktyg förespråkas av Myndigheten för samhällsskydd och beredskap för ett ändamålsenligt cyberförsvar, och anses värdefullt för det skyddsbehov som kommunens informationstillgångar konstateras ha.

3.4.1.1 Bedömning

Vi bedömer att det finns en tillräcklig kontroll för att upptäcka hot om intrång och andra incidenter.

Genom nuvarande avtal har kommunstyrelsen, enligt vår mening, tillsett att det finns tillgång till övervakning och möjlighet att hantera akuta störningar dygnet runt.

3.5 Incidenthantering

Enligt informationssäkerhetsstrategin ska incidenter hanteras i enlighet med kommunens riktlinje för incidentrapportering, som presenteras på kommunens intranät. Som del i informationen finns också länk till ärendehanteringssystemet där incidenter anmäls. Vid driftstörningar åligger det, enligt Riktlinjer för systemförvaltning, systemförvaltare på it-enheten att följa upp avbrottet och upprätta incidentrapport. Incidenter ska även analyseras i förbättrande syfte.

Enligt Ledningens genomgång har ett förbättringsarbete genomförts under år 2022 genom att en ny rutin för incidenthantering har fastställts för att etablera ett gemensamt förfarande för hur incidenter/avvikelser ska rapporteras och följas upp. Det pågår enligt dokumentationen fortsatt arbete med att få den nya processen att bli vedertagen och

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

DocuSign Envelope ID: 9F36B909-18F2-46D3-812D-D61080393EF9

att utbilda verksamheterna i rapportering och arbete med incidenter och avvikelser. Vi kan också konstatera att åtgärder för att stärka kommunens incidenthantering vidtagits utifrån genomförd uppföljning.

Vi har delgetts att antalet anmälda informationssäkerhetsincidenter fördubblats under ett års tid. Anmälningar sker via kommunens intranät där det också framgår att chef för enheten där incidenten uppkommit är anmälningsansvarig till följd av det linjebaserade ansvaret för informationssäkerhet.

Incidenthanteringsprocessen beskrivs såsom:

> Anmälda informationssäkerhetsincidenter samordnas initialt av informationssäkerhetsfunktion inom berörd verksamhet. Vid behov involveras informationssäkerhetssamordnare eller dataskyddsombud. De verksamheter som omfattas av NIS-regleringen behöver bedöma incidenter, där de som bedöms vara rapporteringspliktiga, ska rapporteras enligt de rapporteringsregler som lag och föreskrifter ställer krav om, till fastställda tillsynsmyndigheter. Personuppgiftsincidenter behöver också bedömas då det finns krav om att sådana ska rapporteras till Integritetsskyddsmyndigheten (IMY).

Inom it-enheten finns en intern beredskap för informationssäkerhetsincidenter i form av driftsstörningar, cyberhot och annan påverkan i form av driftenheten som har stående dygnet runt-beredskap. Intervjuade hänvisar även till den avtalade övervakningstjänst som vi beskrev för i föregående rapportavsnitt, vilken har viss incidentberedskap.

Enligt enhetens interna incidenthanteringsprocess eskaleras incidenter via driftsamordnare till it-driftschef. Vid behov involveras informationssäkerhetssamordnare och digitaliseringschef, enligt vad som framkommer i intervju. Antalet it-säkerhetsincidenter som föranleder en incidentrapport uppges vara begränsat till ett fåtal per vecka. I de fall det sker analyseras incidenten ur ett förebyggande perspektiv tillsammans med systemförvaltare. Av intervjuuppgifter framgår att incidenthanteringsprocessen inte finns som ett formaliserat dokument, utan är en process som integrerats ärendehanteringssystemet.

3.6 Bedömning

Vår bedömning är att det finns etablerade rutiner med tydliggjorda eskaleringsvägar vid säkerhetshändelser och incidenter.

Det gäller såväl kommunövergripande rutiner liksom den interna incidenthantering som finns inom it-enheten, samt inkluderar rutiner för att kunna hantera händelser utanför kontorstid. Incidenthantering sker, enligt vår bedömning, i linje med vad som anges av styrande dokument, och med ett proaktivt förhållningssätt som borgar för att inträffade incidenter ses som del av ett förbättringsarbete.

Att antalet incidentanmälningar ökat tyder enligt vår mening på att kunskapen om informationssäkerhet stärkts. Ökad kunskap är i sig förebyggande mot att incidenter inträffar.

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

DocuSign Envelope ID: 9F36B909-18F2-46D3-812D-D61080393EF9

3.7 Kontinuitetshantering

3.7.1 Reserv- och återgångsrutiner

Det framgår av informationssäkerhetsstrategin att kommunen ska ha en avbrottsplan med processer för att säkerställa verksamheten vid störningar och avbrott i informationssystem. Vi har tagit del av ett utkast till kontinuitetsplan för it-enheten som innehåller beskrivningar av reserv- och återgångsrutiner vid avbrott samt roller och ansvar som inträder vid dylik händelse. Planen har inte färdigställts. Främst på grund av vad som anges vara resursbrist.

Enligt utkastet till kontinuitetsplan ska så kallade service level agreements (SLA), överenskommelser om servicenivåer som ska gälla vid avbrott/störning, ha fastställts av ansvariga för kommunens olika verksamheter. I Riktlinjer för systemförvaltning föreslås att SLA för respektive system ska utvärderas årligen av verksamhetsföreträdare och it-personal.

It-enheten tillämpar fyra olika servicenivåer baserade på systemens väsentlighet för den verksamhet som använder systemet. Den högsta servicenivån avser verksamhetskritiska system som kräver dygnet runt-beredskap för händelse av avbrott. Ett fåtal system har kravställts enligt högsta servicenivån. Uttrycks inga särskilda behov kategoriseras systemet enligt normalnivå, it-enheten ska då åtgärda eventuella avbrott inom 48 timmar. Vi uppfattar att detta är vanligast förekommande, och att det fått till följd att det saknas skriftliga överenskommelser om servicenivåer. En utmaning som nämns är att verksamheter ibland vill ha en högre intern servicenivå för system som driftas av en extern leverantör än den nivå som kravställts i avtalet med leverantören. Detta medför att det internt inte finns förutsättningar att upprätthålla servicenivån då kommunen är beroende av dialog och samarbete med den externa leverantören om något sker.

Även om dokumentation av servicenivåer och kontinuitetsplan inte är fullständig anser samtliga intervjuade att etablerade arbetssätt är funktionella och fungerar väl.

Årsskiftet 2022/2023 inträffade ett omfattande tekniskt avbrott som fick stor påverkan på en av kommunens samhällsviktiga verksamheter. Enligt intervjuade visade det efterföljande analysarbetet att både incident- och kontinuitetshantering utfördes i enlighet med de processer som finns angivna i den preliminära kontinuitetsplanen, och på ett sätt som innebar att berörd verksamhet kunde upprätthållas utan större påverkan. Vi har fått en ingående beskrivning av avbrottets tekniska karaktär, men av hänsyn till att inte öka riskexponeringen beskrivs inte detta mer i rapporten.

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

DocuSign Envelope ID: 9F36B909-18F2-46D3-812D-D61080393EF9

3.7.2 Bedömning

Vi bedömer att det delvis finns dokumenterade reserv- och återgångsrutiner för allvarligare störningar och avbrott, samt att rutinernas ändamålsenlighet testats.

Genom det avbrott som vi beskrivit är vår bedömning att reserv- och återgångsrutiner vid allvarligare störning testats. Vi delar kommunens bild av att incidenten hanterats i enlighet med befintliga rutiner och att dessa visat sig vara ändamålsenliga.

Vårt intryck är att utkastet till kontinuitetsplan innehåller väsentliga processer för att säkerställa prioritering av funktionalitet i händelse av avbrott, men att planen behöver formaliseras.

För en ändamålsenlig kontinuitetsplan är definierade servicenivåer en god vägledning. Vi konstaterar att befintliga arbetssätt inte följer vad som anges av Riktlinjer för systemförvaltning, liksom att servicenivåer riskerar att inte motsvara faktiska behov då de utgår från standardnivåer snarare än genomtänkta val. Vår bedömning är att behov av servicenivåer bör utvärderas och dokumenteras i enlighet med vad som anges av riktlinjen.

3.8 Uppföljning och återrapportering av informations- och it-säkerhetsarbetet

3.8.1 Uppföljning och återrapportering

Enligt policyn för informationssäkerhet och dataskydd ansvarar nämnderna för att följa upp respektive verksamhets informationssäkerhetsarbete. Av dokumentet framgår också att extern granskning av informationssäkerhetsarbetet ska genomföras med jämna mellanrum. Att så sker bekräftas genom erhållen revisionsrapport.

Uppföljning har genomförts i form av Ledningens genomgång som rapporterats till kommunstyrelsen och nämnderna. Vi har tagit del av Ledningens genomgång för år 2022, vilken sammanfattar informationssäkerhetsarbetet för året och redogör för prioriterade områden och förbättringsåtgärder för att stärka informationssäkerheten under 2023. Det är informationssäkerhetssamordnare som sammanställt och rapporterat om uppföljningen.

Utöver Ledningens genomgång uppges it-säkerhetsarbetet ha återrapporterats till kommunstyrelsens arbetsutskott vid ett fåtal tillfällen under senaste året. Återrapporteringen upplevs ha stärkt informations- och it-säkerhetsarbetet på så vis att det medvetandegjort vikten av ett systematiskt informations- och it-säkerhetsarbete inom hela kommunen. Vår uppfattning utifrån genomförda intervjuer är att kommunstyrelsen och tjänstepersonsledningen hyser stort förtroende och förståelse för det arbete som utförs. De ekonomiska satsningar som anslagits för it-säkerhet senaste åren anses också tala för det.

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

DocuSign Envelope ID: 9F36B909-18F2-46D3-812D-D61080393EF9

3.8.2 Bedömning

Vi bedömer att uppföljningsrutinerna för it-säkerhetsarbetet delvis är ändamålsenliga.

Vi noterar att Ledningens genomgång har genomförts där en samlad uppföljning av kommunens informationssäkerhetsarbete finns och att denna har rapporterats till kommunstyrelsen. I styrande dokument saknas reglering av uppföljning och rapportering i förhållande till kommunstyrelsen varför vi anser att detta bör regleras vid nästa revidering.

Vi ser det som positivt att kommunstyrelsen eller dess arbetsutskott regelbundet fått information om it-säkerhet. Med anledning av omvärldsläge och förhöjd risk för cyberhot och it-incidenter bör kommunstyrelsen fortsätta att efterfråga kontinuerlig återrapportering avseende aktuella hot och risker tillsammans med kommunens förutsättningar och beredskap för att hantera allvarliga it-säkerhetshändelser.

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

DocuSign Envelope ID: 9F36B909-18F2-46D3-812D-D61080393EF9

4 Samlad bedömning och rekommendationer

Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsen i allt väsentligt har en tillräcklig styrning och intern kontroll avseende detta, samt att arbetet sker på ett ändamålsenligt sätt.

Bedömningen baseras bland annat på att it-säkerhetsarbetet i hög grad når upp till kommunens beslutade standard för arbetet samt att åtgärder är etablerade i enlighet med Myndigheten för samhällsskydd och beredskaps rekommendationer för stärkt cyberförsvar. Beslutade organisations- och samverkansformer inom it-området möjliggör att hela kommunorganisationen omfattas av den systematik och riskmedvetenhet som it-säkerhetsarbetet utgår från. Förhållningssättet innebär även att risker och hot utvärderas kontinuerligt och ligger till grund för etablerade säkerhetsåtgärder.

Utifrån våra iakttagelser och vår bedömning rekommenderar vi kommunstyrelsen att:

- Slutföra översynen av styrande dokument
- Säkerställa att styrande dokument efterlevs
- Utvärdera it-enhetens nuvarande bemanning så att den är anpassad till omfattning och krav i styrande dokument och den standard som kommunen beslutat om
- Fastställa kontinuitetsplan för it och tillse att det i övrigt finns tillgång till tillräckliga underlag så att ansvariga vid händelse kan tillse en robust återställning av it-miljön
- Formalisera former för uppföljning mot kommunstyrelsen

KPMG, dag som ovan

DocuSigned by:
Jenny Thörn
E1872868AB3D4FC...
Jenny Thörn
Verksamhetsrevisor

DocuSigned by:
Sofie Ernerudh
74FAE6583E654B4...
Sofie Ernerudh
Verksamhetsrevisor

DocuSigned by:
Lena Medin
9CB391F9DD1D41B...
Lena Medin
Certifierad kommunal revisor

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public