Dnr: REV/00026/2024

KOMMUNREVISIONEN
ÖSTERSUND

REVISIONSRAPPORT

UPPFÖLJANDE GRANSKNING
Informationssäkerhet och digital lagring

Uppföljande granskning informationssäkerhet och digital lagring

Rapport

Östersunds kommun

KPMG AB

2024-12-20

Antal sidor 19

Östersunds kommun
Uppföljande granskning informationssäkerhet och digital lagring

2024-12-20

Innehållsförteckning

1 Sammanfattning

KPMG har av revisionskontoret i Östersund kommun fått i uppdrag att granska vidtagna åtgärder utifrån tidigare genomförd granskning avseende it-säkerhet och digital lagring.

Granskningens syfte har varit att bedöma om kommunstyrelsen, och nämnderna i den omfattning de berörs, har vidtagit åtgärder utifrån revisorernas rekommendationer. I granskningen ingår även att bedöma om kommunstyrelsen har säkerställt att NIS2-direktivet[1] implementeras utifrån gällande krav.

Vår samlade bedömning är att kommunstyrelsen delvis har beaktat tidigare lämnade rekommendationer men att åtgärderna inte varit tillräckliga.

Vi gör därigenom bedömningen att kommunstyrelsen brustit i sin interna kontroll över att de åtgärder som de beslutat om i sitt yttrande verkställts. De rekommendationer som lämnats i tidigare granskning har syftat till att ge kommunen stärkta förutsättningar att uppnå ett systematiskt informationssäkerhetsarbete. Att kommunstyrelsen inte i tillräcklig grad har säkerställt att åtgärderna vidtagits medför att nuvarande säkerhet kan innebära risk att informationstillgångar inte skyddas på ett ändamålsenligt sätt i förhållande till aktuella hot och risker.

Vår bedömning är att kommunstyrelsen delvis säkerställt att det bedrivs ett tillräckligt arbete för att säkerställa att NIS2-direktivet implementeras.

Genom vår granskning kan vi konstatera att kommunen inom flera områden inte når upp till de krav som nuvarande NIS-direktiv ställer, även om direktivet i nuläget endast riktas till en begränsad del av verksamheten. Vi konstaterar dock att kommunstyrelsen inför budget 2025 har efterfrågat utökning av rambudget för att möjliggöra anpassningar mot bakgrund av direktivets krav.

Utifrån våra iakttagelser och bedömningar konstaterar vi att samtliga tidigare lämnade rekommendationer kvarstår helt eller delvis.

Vi rekommenderar kommunstyrelsen att:

- Säkerställa att tidigare lämnade rekommendationer beaktas i högre grad och att åtgärder vidtas i högre utsträckning.
- Säkerställa att informationsägarskapet etableras så att informationssäkerhetsarbetet genomförs av verksamhetsansvariga inom samtliga verksamheter i kommunen.
- Följa utvecklingen med NIS2-direktivet och svensk lagstiftning för att bedöma vilka anpassningar som det finns behov av för att nå efterlevnad av lagen.

[1] The Directive on Security of Network and informations Systems

2 Bakgrund

KPMG har fått i uppdrag av revisionskontoret i Östersund kommun att genomföra en uppföljande granskning av den granskning som genomfördes 2021 avseende it-säkerhet och digital lagring.

Bedömningen då var att kommunens informations-och it-säkerhetsarbete behövde utvecklas för att nå de standarder som kommunen uttalat som gällande för sitt arbete. Vidare konstaterades att det fanns behov av ett flertal förbättringsåtgärder för att arbetet ska ske systematiskt och riskbaserat i enlighet med ledningssystem för informationssäkerhetsarbete.

Kommunstyrelsen har lämnat svar på vilka åtgärder som ska genomföras utifrån lämnade rekommendationer i den tidigare granskningen. Granskningen var inriktad på kommunens övergripande arbete med informationssäkerhet. Flera av rekommendationerna krävde åtgärder även i nämnderna.

EU:s medlemsländer har fram till oktober 2024[2] att implementera det nya direktivet kring nätverks-och informationssäkerhet – NIS2. Detta direktiv kommer att medföra ett antal viktiga förändringar inom cybersäkerhet. Exempelvis kommer tillämpningskraven stärkas och sanktioner kommer att tillämpas i hela EU mot företag och organisationer som inte tillämpar NIS2.

Kommunens revisorer har i sin riskanalys bedömt att det därför finns risk för att tillräckliga åtgärder inte har vidtagits för att säkerställa att kommunens organisation och interna kontroll är ändamålsenlig gällande informationssäkerhet.

Granskningen ingår i den fastställda revisionsplanen för 2024.

2.1 Syfte, revisionsfrågor och avgränsning

Granskningens syfte har varit att bedöma om kommunstyrelsen, och nämnderna i den omfattning de berörs, har vidtagit åtgärder utifrån revisorernas rekommendationer. I granskningen ingår även att bedöma om kommunstyrelsen har säkerställt att NIS2-direktivet implementeras utifrån gällande krav.

Granskningen har omfattat följande revisionsfrågor:

- Har åtgärder vidtagits utifrån den tidigare granskningen? Är åtgärderna tillräckliga?
- Bedrivs det ett tillräckligt arbete för att säkerställa att NIS2-direktivet implementeras?

Granskningen är avgränsad till 2024.

Ansvarig nämnd är kommunstyrelsen och nämnderna i den omfattning de berörs.

[2] Ny lagstiftning mot bakgrund av EU-direktivet har flyttats fram sedan uppdragsbeskrivningen formulerades. Regeringskansliet väntas lämna en proposition avseende detta våren 2025.

2.2 Revisionskriterier

I granskningen har revisionskriterierna utgjorts av:

- Kommunallagen (2017:725)
- MSB:s metodstöd och rekommendationer avseende ledningssystem för informationssäkerhet samt it-säkerhetsåtgärder. Se bilaga A för redogörelse av metodstödet.
- Interna styrdokument, för fullständig förteckning se bilaga B

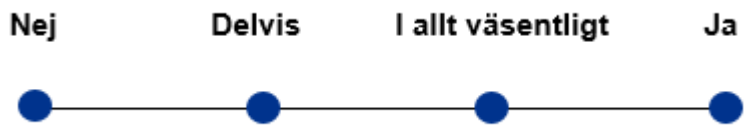
2.3 Metod

Granskningen har genomförts genom dokumentstudier och intervjuer.

- Dokumentanalysen har omfattat övergripande styrdokument, vägledande dokument samt styrelsens protokoll.
- Intervjuer har genomförts med kommundirektör, it-chef, säkerhetschef, it-strateg, representanter från barn- och utbildningsförvaltningen, teknisk förvaltningen, vård- och omsorgsförvaltningen, samt social- och arbetsmarknadsförvaltningen.

2.3.1 Bedömningsnivåer

De bedömningar som avlämnas i granskningen har utgått ifrån följande bedömningsnivåer.



2.3.2 Faktakontroll

Samtliga intervjuade har erhållit möjlighet att faktakontrollera rapporten.

2.3.3 Organisation

Då granskningen har genomförts under ledning av revisionskontoret har löpande avstämningar genomförts med projektledaren vid Östersunds kommuns revisionskontor.

2.3.4 Begreppsdefinition informationssäkerhet och it-säkerhet

I ett systematiskt informationssäkerhetsarbete ingår fyra områden av säkerhetsåtgärder. Dessa är:

1. Organisatorisk säkerhet (ibland benämnd administrativ säkerhet)
2. Teknisk säkerhet (it-säkerhet och cybersäkerhet)
3. Personalrelaterad säkerhet
4. Fysisk säkerhet

Den tidigare granskningens benämning it-säkerhet har av intervjupersoner i den uppföljande granskningen poängterats som olycklig då det skapat en begreppsförvirring kring vad granskningen handlade om. Detta då flertalet rekommendationer i den tidigare granskningen avsåg informationssäkerhet.

Detta medför att även resultatet av uppföljningen som presenteras i denna rapport avser informationssäkerhet på en övergripande nivå men i vissa delar de tekniska säkerhetsåtgärderna, vilket även kallas it-säkerhet.

Dock ska poängteras att de fyra områden som presenteras ovan behöver beaktas i informationssäkerhetsarbetet för att detta ska vara systematiskt och tillse att informationstillgångar skyddas utifrån aspekterna konfidentialitet, riktighet och tillgänglighet.

Det systematiska informationssäkerhetsarbetet bör enligt de rekommendationer Myndigheten för samhällsskydd och beredskap ger inom området, utgå från en informationssäkerhetspolicy. Informationssäkerhetspolicyn och informations-säkerhetsmål ska upprättas som är förenliga med organisationens strategiska inriktning. Enligt vedertagen standard för informationssäkerhet, ISO27001, ska informationssäkerhetspolicyn finnas i dokumenterad form, vara anpassad till organisationens syfte och innefatta ett åtagande att uppfylla tillämpliga krav relaterade till informationssäkerhet.

IT-säkerhet är ett delområde inom informationssäkerhetsarbetet vilket innebär att styrande dokument även bör inkludera reglering av krav för IT-säkerhetsområdet.

3 Resultat av uppföljande granskning

3.1 Granskning av it-säkerhet och digital lagring

KPMG gjorde under 2021 en granskning av it-säkerhet och digital lagring på uppdrag av de förtroendevalda revisorerna i Östersunds kommun. Granskningen syftade till att svara på om kommunens organisation och interna kontroll var ändamålsenlig gällande IT-säkerhet. Granskningen resulterade i nio rekommendationer som riktades till kommunstyrelsen.

Rapporten blev sekretessbelagd och i denna uppföljning redogör vi endast på en övergripande nivå vilka åtgärder som vidtagits utifrån rekommendationerna.

3.1.1 Redovisning av nuläge i förhållande till lämnade rekommendationer och kommunstyrelsens yttrande

Rekommendationer

- ***Besluta om riktlinjer med utgångspunkt i beslutad informationssäkerhetspolicy där dessa konkretiserar hur ansvar ser ut och hur arbetet med bland annat it-säkerhet ska bedrivas och vilka krav som ska gälla.***
- ***Ompröva styrdokumenten regelbundet så att de är uppdaterade och aktuella, exempelvis årligen eller minst en gång per mandatperiod.***

Yttrande från kommunstyrelsen

- Policydokument inom områdena informationssäkerhet, IT-säkerhet samt Informationsförvaltning finns idag men behöver uppdateras och beslutas. Detta arbete sker under det gemensamma översynsarbetet av samtliga styrande dokument. I de kommande styrdokumenten kommer ansvar och krav att beskrivas.
- Ett arbete har påbörjats med en översyn av olika interna styrdokument inom kommunen. Nulägesbilden sammanställer behovet av uppdatering men också i stor utsträckning ett större omtag vad gäller information över lag. Strukturen runt information behöver omfatta förvaltning, hantering, säkerhet, arkivering och drift. Arbetet omfattar sakkunniga inom alla områden. Dessa styrande dokument behöver samordnas och ensas gemensamt för att nå målgrupperna i kommunens alla verksamheter.
- Rutin skapas så att ledningens genomgång genomförs årligen.
- Ompröva och uppdatera styrdokument en gång per mandatperiod.

Nuläge

Enligt intervjuade finns beslut från 2019 om att etablera ett ledningssystem för informationssäkerhet, ett så kallat LIS.

Under hösten år 2023 påbörjades ett arbete med att se över befintliga styrdokument inom informations- och it-säkerhet samt upprätta nya där behovet fanns. Arbetet inkluderade framtagande av riktlinjer för att tydliggöra informationssäkerhetspolicyn[3] samt revidering av it-säkerhetspolicy[4] och säkerhetspolicy[5]. Fokus var att erhålla en enhetlig dokumentflora som kopplade an gentemot varandra. Riktlinjer har tagits fram men ännu inte antagits av kommunstyrelsen.

Av underlag som vi tagit del av som beskriver *Metod för informationsklassificering ur säkerhetssynpunkt* anges att arbetet ska utgå från en Informationssäkerhetspolicy samt att andra styrande dokument ska etableras som ska utgöra grunden i ett Ledningssystem för informationssäkerhet, LIS.

Intervjuade beskriver att arbetet stannat av på grund av att tjänsten informationssäkerhetsstrateg är vakant sedan nästan ett år och arbetet har därför inte färdigställts fullt ut. Framgent är avsikten att styrelsen ska anta riktlinjerna samt att it-säkerhetspolicyn ska revideras. Avsikten är även att upprätta rutiner och checklistor för att konkretisera arbetssätt inom informationssäkerhet.

Det finns i kommunen upprättade hanteringsregler ur ett konfidentialitet-/sekretessperspektiv för säker informationshantering vid Östersunds kommun[6]. I reglerna beskrivs vad som utgör lägsta skyddet för information som klassificeras som öppen, intern, känslig, extra känslig samt försvarssekretess.

Vi noterar att kommunens informationssäkerhetspolicy vid tid för uppföljningen har passerat fem år. Enligt MSB har en informationssäkerhetspolicy en livslängd på tre till fem år. Ledningens genomgång har inte etablerats i enlighet med yttrandet.

Vi informeras i intervjuer att det finns behov hos förvaltningarna av en tydlig styrning inom informations- och it-säkerhetsområdet. Bland annat genom konkretiserande styrdokument som riktlinjer och rutiner som kan utgöra vägledning i arbetet.

Kommentar

Kommunstyrelsen har inte beaktat rekommendationen och inte vidtagit tillräckliga åtgärder.

Nya styrdokument har inte etablerats. Vi konstaterar att bristen på en etablerad styrning ger sämre förutsättningar för förvaltningarna att ta sig an informationssäkerhetsarbetet i enlighet med det linjeansvar som arbetet utgår från.

[3] Informationssäkerhetspolicy, kommunfullmäktige, 2019-05-28
[4] It-säkerhetspolicy, kommunstyrelsen, 2004-09-21
[5] Säkerhetspolicy, kommunstyrelsen, 2004-09-21
[6] Datum samt dokumentägare saknas.

Rekommendation

- ***Göra en nulägesanalys i syfte att få kunskap om organisationens processer, vilken information som hanteras och behov av skydd utifrån de krav som finns.***

Yttrande från kommunstyrelsen

- Kommunledningsgruppen har beslutat att införa ett Ledningssystem för verksamhetsinformation (LVI) enligt ISO standard 30300. I samband med det kommer en kartläggning att genomföras över vilken information som respektive verksamhet använder sig av. En del i det arbetet är att knyta den identifierade informationen till en befintlig process i verksamheten. Kartläggningen sammanställs i informationshanteringsplaner som bland annat ligger till grund för klassificering och hantering av informationen ur säkerhetssynpunkt.
- Arbetet med att identifiera informationen hänger ihop med det arbete som pågår enligt ”Riktlinje för ett processorienterat arbetssätt” inom kommunen. Arbetet med att identifiera informationen måste göras i följande ordning: Processbeskrivning, Informationsidentifiering och klassificering.
- Arbete pågår avseende kartläggning av informationen och efterföljande klassificering.

Nuläge

Som grund för kommunens informationssäkerhetsarbete pågår ett arbete med att införa Ledningssystem för verksamhetsinformation (LVI) enligt ISO standard 30300, i enlighet med kommunstyrelsens svar på åtgärder. I arbetet som genomförts har identifiering av informationen gjorts tillsammans med klassificering. Enligt intervjuade pågick arbetet med processkartläggningar.

I arbetet har ingått att formalisera informationshanteringsplaner samt att identifiera samverkansformer inom linjeverksamheten, processer samt mer tvärsektoriella grupperingar. Intervjuade menar att arbetet pågår i enlighet med kommunstyrelsens yttrande.

Kommentar

Kommunstyrelsen har delvis beaktat rekommendationen men inte vidtagit tillräckliga åtgärder.

Vi ser att vissa aktiviteter har genomförts i enlighet med kommunstyrelsens yttrande avseende kartläggning av information och tillhörande informationshantering. Vi ser särskilt positivt på att informationsmängder har identifierats och klassningsarbetet påbörjats.

Vi uppfattar dock att rekommendationen att göra en nulägesanalys inte har gjorts i enlighet med de analyser som MSB:s metodstöd för systematiskt informations-säkerhetsarbete rekommenderar, vilket rekommendationen utfick från. Exempelvis framgår av metodstödet att verksamhetsanalys, omvärldsanalys, riskbild samt GAP-analys ska utgöra ett stöd för verksamheten att identifiera interna och externa förutsättningar som sedan informationssäkerhetsarbetet kan utformas efter.

Rekommendation

- ***Utifrån resultatet i ovanstående analyser besluta om handlingsplan och tillsättande av resurser för att möte de behov av åtgärder som identifierats.***

Yttrande från kommunstyrelsen

- Ta fram en handlingsplan utifrån ovanstående resultat.
- Resursäskande genomfört på IT-enheten i avsikt att bredda och öka förmågan.
- Det finns en utmaning inom arbetsmarknaden när det gäller kompetens inom informationssäkerhet och IT-säkerhet

Nuläge

Vid tid för granskningen saknas handlingsplan avseende informationssäkerhetsarbetet i enlighet med rekommendationen. Intervjuade beskriver att handlingsplan har funnits tidigare då ansvar för dessa utgår från processägarskapet som är etablerat i kommunen. Varje processägare har en handlingsplan för sitt ansvarsområde som ska avspegla uppdrag och aktiviteter i verksamhetsplaner. Att handlingsplan saknas i nuläget uppges bero på att tjänsten informationssäkerhetsstrateg är vakant och att tidigare handlingsplan därigenom är daterad och inte aktuell.

It-enheten har äskat om förstärkning av resurser. Resursförstärkningen har medfört att tjänster kunnat tillsättas utifrån krav och behov. Även inom Område Juridik och säkerhet samt Område kansli har förstärkningar av tjänster gjorts inom respektive område. Intervjuade uppger att dessa medfört utökade möjligheter att anpassa arbetet utifrån nya krav som väntas genom NIS2-direktivet samt även utgöra resurser i arbetet med kommunens kontinuitetshantering.

Kommentar

Kommunstyrelsen har delvis beaktat rekommendationen men inte vidtagit tillräckliga åtgärder.

Vi konstaterar att handlingsplan saknas vid tid för uppföljningen men att det enligt uppgift funnits handlingsplan tidigare i enlighet med yttrandet.

De förstärkningar av resurser som it-enheten hade för avsikt att göra har genomförts. Det har även gjorts ytterligare förstärkningar av personella resurser inom Område Juridik och säkerhet samt Område kansli, vilka vi bedömer kan bidra till förutsättningar att bedriva informationssäkerhetsarbetet i kommunen.

Rekommendation

- ***Besluta om vilka system som är verksamhetskritiska och vidta erforderliga åtgärder utifrån varje systems specifika förutsättningar avseende exempelvis uppdateringar, lagring, säkerhet och kontinuitet.***

Yttrande från kommunstyrelsen

- Att besluta om vilka system som för kommunen är verksamhetskritiska ska utgå ifrån vilken information som är kritisk för de olika verksamheterna. Det är verksamhetens information och dess klassificering som ligger till grund för beslut om vilka system som är verksamhetskritiska i kommunen. Arbetet med att fånga upp verksamhetskritisk information börjar vid respektive verksamhet och förvaltning.
- Den framtagna systemförvaltningsmodellen ska följas av alla verksamheter.
- Den framtagna processen för nytillkommande system ska följas av alla verksamheter.

Nuläge

Identifiering av verksamhetskritiska system

Ett arbete har genomförts med inventering av samtliga system samt genomförande av informationsklassning och riskanalyser av 52 av kommunens system. Vi har tagit del av underlag som beskriver Metod för informationsklassificering ur ett säkerhetsperspektiv, anvisning samt mall för arbetet.

För genomförandet anlitades externa konsulter som processledare och metodstöd. Samtliga förvaltningar hade representanter med i arbetet för genomgång av de system som nyttjas i respektive verksamhet.

Det finns en delad bild mellan intervjuade över den metod som använts för informationsklassning och riskbedömning. Från centrala funktioner uppges detta vara den kommungemensamma modell som ska användas och att den är tillämpbar för kommunens arbete. Intervjuade från förvaltningarna har dock uppfattningen att det behövs ett omtag och att arbetet med klassning bör göras om med stöd i en annan modell och metod. Detta då konsulten som bidrog i arbetet inte finns kvar i kommunen och kan stötta förvaltningarna i det fortsatta arbetet. En av förvaltningarna har valt att utbilda egna funktioner i SKRs[7] modell KLASSA så att arbetet med informationsklassning kan fortgå.

Enligt intervjuade så finns en etablerad process där informationssäkerhetskrav beaktas i upphandlingsprocessen för nya system. Den utgår främst från lagkrav och juridiska aspekter. Vi har i granskningen inte tagit del av någon dokumentation över det beskrivna arbetssättet.

Ytterligare en åtgärd som genomförts är att it-avdelningen har skickat en uppmaning till samtliga förvaltningar att inkomma med en lista samt en prioriteringsordning vid uppstart efter ett eventuellt avbrott. It-avdelningen har skickat ut en mall för

[7] Sveriges kommuner och regioner

förvaltningarna att fylla i. Mallen omfattar Vilket system som avses och vad det används till, prioritering av systemet utifrån den påverkan som verksamheten skulle ha vid avbrott (*Ingen, Låg, Mellan, Hög*) samt en beskrivning över vad i verksamheten som påverkan avser.

Intervjuade anger att samtliga förvaltningar har återkommit med listor som ger prioriteringsordning per förvaltning. Det kvarstår dock ett arbete för att fastställa en kommunövergripande prioriteringsordning med utgångspunkt från de listor som förvaltningarna har tagit fram.

Systemförvaltning

I den tidigare granskningen framkom att det fanns utmaningar i att etablera roller och ansvar i systemförvaltningsorganisationen. De intervjuade uppger att det vid uppföljningen har förbättrats något, men att det fortfarande finns system som saknar utsedda ansvariga och därmed inte omfattas av en aktiv systemförvaltning. Det saknas vid tid för uppföljningen en samlad bild över vilka system som avses. Vi delges att systemförvaltning inte genomförs för vissa system trots utsedda ansvariga systemägare på grund av resursbrist.

Kommentar

Kommunstyrelsen har i delvis beaktat rekommendationen och delvis vidtagit tillräckliga åtgärder.

Vi noterar att flertal åtgärder har vidtagits utifrån lämnad rekommendation. Dels har informationsklassning och riskbedömning gjorts för de mest kritiska verksamhetssystemen. Dels har it-avdelningen efterfrågat underlag över verksamheternas mest prioriterade system i händelse av avbrott.

Det är dock väsentligt att påbörjat arbete slutförs. Särskilt ser vi behov av att en överenskommen prioriteringsordning fastställs som del i kommunens övergripande kontinuitetshantering.

Rekommendation

- ***Göra en kartläggning av implementerade tekniska säkerhetsåtgärder och ställa dessa i förhållande till skyddsvärdet för den information som åtgärder avser att skydda.***

Kommunstyrelsens yttrande

- Som en del i informationssäkerhetsarbetet kommer information att klassificeras ur säkerhetssynpunkt vilket leder till att informationen får en given skyddsnivå utifrån olika fastställda interna och externa krav. Dessa skyddsnivåer resulterar i vilka tekniska säkerhetsåtgärder som krävs. Detta arbete är påbörjat och sker tillsammans med Region Jämtland Härjedalen för att arbeta fram korrekta men också kvalitetssäkrade metoder och mallar.
- Nuvarande tekniska säkerhetsåtgärder är till stor del tillräckliga. I samband med att informationen klassificeras kan högre säkerhetskrav framkomma som kan innebära krav på ökade investeringar och fler resurser.

Nuläge

Som vi tidigare beskrivit så har ett arbete genomförts med informationsklassning och riskbedömning. Av den uppföljande granskningen framgår dock att det kvarstår ett arbete med att hantera de åtgärder som identifierats i arbetet. Intervjuade anger att det efterföljande arbetet med åtgärdshantering har stannat upp med anledning av att funktionen informationssäkerhetsstrateg är vakant. Förvaltningarna lyfter att de har behov av operativt stöd och kunskap inom området för att komma vidare. Någon kartläggning av vidtagna säkerhetsåtgärder har inte genomförts på systemnivå.

Av intervjuerna framgår att system som berörs av gällande NIS-direktiv har genomgått klassning samt att åtgärder har vidtagits. Tillsyn har genomförts av tillsynsmyndighet utan anmärkning.

Intervjuade anger att kommunens arbete med it-tekniska säkerhetsåtgärder för grundläggande it-infrastruktur och plattform inte har genomförts på ett strategiskt sätt tidigare. Det pågår därför en teknisk kontroll i syfte att kartlägga vidtagna åtgärder och utifrån det få en tydligare bild över åtgärderna, vilket är i enlighet med kommunstyrelsens svar på åtgärder. Arbetet utgår från ett internationellt vedertaget regelverk[8] med åtgärder som syftar till att förhindra de mest farliga attackerna. Regelverket är förankrat i ledningsgruppen för it och mappar mot de säkerhetsåtgärder som finns i ISO 27002.

Kommentar

Kommunstyrelsen har delvis beaktat rekommendationen men inte vidtagit tillräckliga åtgärder.

Väsentliga aktiviteter behöver slutföras för att de rekommendationer som lämnades ska uppnå det som åsyftades. Vi ser särskilt behov av att de skyddsåtgärder som informationsklassning och riskanalyser visat behov på omsätts i handlingsplaner där åtgärder prioriteras utifrån ett riskperspektiv. Därtill ser vi behov av att det pågående arbetet med kartläggning av it-tekniska säkerhetsåtgärder även inkluderar åtgärder på systemnivå så att inga okända sårbarheter finns.

Vi ser positivt på att åtgärder prioriterats för NIS-identifierade verksamheter.

Rekommendation

- ***Etablera kommungemensamma rutiner för incidenthantering och rapportering samt säkerställa att det finns en tillräcklig kunskap och medvetenhet om vad som är incidenter och hur dessa kan upptäckas.***

Kommunstyrelsens yttrande

- Ta fram en gemensam process för incidenthantering utifrån perspektivet informationssäkerhet och IT-säkerhet.

[8] Riktlinjer utvecklade av Center for Internet Security för bästa praxis för datorsäkerhet.

- Bygga en säkerhetskultur som inriktar sig på säker informationshantering vid kommunens alla verksamheter genom information och utbildningsinsatser.

Nuläge

Som tidigare nämnts saknas riktlinjer och rutiner för hur informationssäkerhetsarbetet ska bedrivas. Riktlinjer och rutiner för informationssäkerhet inkluderar vanligen reglering och beskrivning på kommungemensam hantering av incidenter och tillhörande rapportering.

Vi har i faktakontrollen fått uppgift om att det finns etablerade arbetssätt och en process för att rapportera om incidenter. Enligt intervjuade är tillvägagångssättet förankrat och välfungerande. Vi har i granskningen inte erhållit någon dokumentation över om det beskrivna arbetssättet tillämpas som kommunens incidenthanterings-rutiner för informationssäkerhet eller it-säkerhetshändelser. Vi har inte heller erhållit någon dokumentation över det arbetssätt som uppges finnas.

I syfte att stärka kunskap och medvetenheten kring informations- och it-säkerhet i hela organisationen genomförs bland annat en grundläggande informationssäkerhets-utbildning[9] för samtliga nyanställda samt korta utbildningar som skickas ut kontinuerligt till medarbetarna via e-post, som bland annat omfattar information om ransomware[10].

Vi har i granskningen inte erhållit någon dokumenterad uppföljning för att verifiera genomförandegrad eller om genomförda utbildningar har uppnått förväntad effekt och kunskap hos medarbetare över vad incidenter är och hur dessa kan upptäckas.

Kommentar

Kommunstyrelsen har inte beaktat rekommendationen och inte vidtagit tillräckliga åtgärder.

Vissa åtgärder har genomförts i enlighet med lämnad rekommendation och kommunstyrelsens yttrande. Vi anser dock inte att det är tillräckligt med en gemensam process som grund för kommunens incidenthantering. Dokumenterade rutiner för incidenthantering är en väsentlig del i ett systematiskt informationssäkerhetsarbete. I dessa behöver beskrivning ingå över vad som är incidenter och hur dessa ska hanteras, ansvaret beskrivas tillsammans med rutiner för uppföljning av inträffade incidenter för att ta vara på erfarenheter i förbättringsarbetet.

Rekommendation

- ***Upprätta kontinuitetsplaner för att säkerställa reserv- och återställningsrutiner i händelse av allvarlig störning.***

Kommunstyrelsens yttrande

- Kommundirektören uppdrar alla förvaltningar att upprätta kontinuitetsplaner.

[9] *Digital informationssäkerhetsutbildning för alla* (Disa) - MSB
[10] Skadliga data som låser filer där den berörda krävs på lösensumma för att kunna låsa upp filerna.

- Kontinuitetsplanering ska göras utifrån klassificering och värdering av informationen.
- Kommunens kontinuitetsplanering pågår och håller på att uppdateras. Information är en av flera olika parametrar som omfattas av detta arbete[11].

Nuläge

Enligt intervjuade saknas i nuläget dokumenterade kontinuitetsplaner. Arbetet uppges dock vara pågående av samtliga verksamheter i enlighet med kommunstyrelsens yttrande.

Samordnare från samtliga förvaltningar träffas kontinuerligt i ett säkerhetsforum, där bland annat arbete med kontinuitetsplanering ingår. Arbetet innebär bland annat att ta fram riktlinjer och rutiner för kontinuitetsplanering som sedan ska kommuniceras till förvaltningarna. Arbetet kommer att fortgå även under 2025.

Inom IT-enheten har en resurs prioriterats just för att tillse att arbetet med kontinuitetsplaner ska få en framdrift.

Kommentar

Kommunstyrelsen har beaktat rekommendationen men inte vidtagit tillräckliga åtgärder.

Vi konstaterar att dokumenterade kontinuitetsplaner saknas men att arbetet är aktuellt och pågår inom samtliga verksamheteter. Sammantaget med att åtgärder inte vidtagits i tillräcklig grad kopplat till skyddsåtgärder och prioriteringsordning ser vi att kommunen i nuläget saknar väsentliga underlag för att ha en tillräcklig kontinuitetsplanering.

Rekommendation

- ***Etablera en strukturerad uppföljning av det arbete som genomförs och som årligen återrapporterats till kommunstyrelsen.***

Yttrande från kommunstyrelsen

- Ta fram en rutin för årlig uppföljning till kommunstyrelsen.

Nuläge

Då det saknas styrande dokument avseende informations- och it-säkerhetsarbetet som tydliggör hur arbetet ska bedrivas saknas även en styrning avseende hur uppföljning av arbetet ska genomföras. Vi har i granskningen efterfrågat dokumenterad uppföljning av informations- och it-säkerhetsarbetet. Genom intervjuer har vi informerats om att det saknas ett strukturerat uppföljningsarbete och att det därmed inte har upprättats någon dokumenterad sammanställning.

Genomgång av protokoll visar att det inte har genomförts någon kontinuerlig återrapportering till kommunstyrelsen avseende informationssäkerhetsarbetet, vilket bekräftas genom intervjuer.

[11] Denna åtgärd i kommunstyrelsens yttrande presenterades ursprungligen i samband med annan rekommendation. I uppföljningen har den dock inkluderats i beskrivning av övriga åtgärder relaterade till kontinuitetshantering.

Kommentar

Kommunstyrelsen har inte beaktat rekommendationen och inte vidtagit tillräckliga åtgärder.

Det saknas fortfarande rutin för årlig rapportering till kommunstyrelsen och ledningens genomgång har inte heller genomförts vilket ingick som åtgärd i kommunstyrelsens yttrande. Det har inte heller genomförts någon annan samlad uppföljning av det arbete som genomförts eller rapportering till kommunstyrelsen om informationssäkerheten i kommunen.

3.1.2 Samlad bedömning av de åtgärder som vidtagits i förhållande till tidigare lämnade rekommendationer och kommunstyrelsen yttrande

Vår samlade bedömning är att kommunstyrelsen delvis beaktat tidigare lämnade rekommendationer men att åtgärderna inte varit tillräckliga.

Vi gör därigenom bedömningen att kommunstyrelsen brustit i sin interna kontroll över att de åtgärder som de beslutat om i sitt yttrande verkställts. De rekommendationer som lämnats i tidigare granskning har syftat till att ge kommunen stärkta förutsättningar att uppnå ett systematiskt informationssäkerhetsarbete. Att kommunstyrelsen inte i tillräcklig grad har säkerställt att åtgärderna vidtagits medför att nuvarande säkerhet kan innebära risk att informationstillgångar inte skyddas på ett ändamålsenligt sätt i förhållande till aktuella hot och risker.

Rekommendation	Bedömning
Göra en nulägesanalys i syfte att få kunskap om organisationens processer, vilken information som hanteras och behov av skydd utifrån de krav som finns.	Delvis
Göra en kartläggning av implementerade tekniska säkerhetsåtgärder och ställa dessa i förhållande till skyddsvärdet för den information som åtgärder avser att skydda.	Delvis
Utifrån resultat i ovanstående analyser besluta om handlingsplan och tillsättande av resurser för att möta de behov av åtgärder som identifierats.	Delvis
Ompröva styrdokumenten regelbundet så att de är uppdaterade och aktuella, exempelvis årligen eller minst en gång per mandatperiod.	Nej
Besluta om riktlinjer med utgångspunkt i beslutad informationssäkerhetspolicy där dessa konkretiserar hur ansvar ser ut och hur arbetet med bland annat IT-säkerhet ska bedrivas och vilka krav som ska gälla.	Nej
Besluta om vilka system som är verksamhetskritiska och vidta erforderliga åtgärder utifrån varje systems specifika förutsättningar avseende exempelvis uppdateringar, lagring, säkerhet och kontinuitet.	Delvis

Etablera kommungemensamma rutiner för incidenthantering och rapportering samt säkerställa att det finns en tillräcklig kunskap och medvetenhet om vad som är incidenter och hur dessa kan upptäckas.	Nej
Upprätta kontinuitetsplaner för att säkerställa reserv- och återställningsrutiner i händelse av allvarlig störning.	Nej
Etablera en strukturerad uppföljning av det arbete som genomförs och som årligen återrapporteras till kommunstyrelsen.	Nej

3.2 Anpassningar i förhållande till NIS2-direktivet

3.2.1 NIS-direktivet

Medlemsländer i EU, däribland Sverige, har sedan 2018 haft EU-direktivet NIS att följa. Direktivet syftade till att öka säkerheten i nätverk och informationssystem inom samhällsviktiga verksamheter, där konsekvenser vid it-bortfall skulle kunna leda till allvarliga konsekvenser med samhällsstörningar som följd.

Den svenska tillämpningen av direktivet regleras i Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. I den lagstiftning som gällt sedan 2019 fanns endast sju sektorer som omfattades av kraven. Bland dessa sektorer ingår vissa kommunala verksamheter, bland annat dricksvattenförsörjning, el och energi samt kommunal hälso- och sjukvård. För att omfattas av kraven ska vissa kriterier uppnås. Vi har i granskningen fått information om att Östersunds kommun har verksamheter som identifierats som samhällsviktiga tjänster och därigenom omfattas av ovan direktiv och lagkrav. Myndigheten för samhällsskydd och beredskap har fastställt flera föreskrifter utifrån lagstiftningen med mer detaljerade krav på verksamheter. Det finns, av regeringen, utsedda tillsynsmyndigheter för respektive sektor.

Nuvarande krav utifrån lag och föreskrifter är bland annat att varje verksamhet ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av standarderna ISO27001 och 27002 om ledningssystem för informationssäkerhet eller motsvarande. Bland annat ska ett ledningssystem för informationssäkerhet vara etablerat. En leverantör ska utifrån identifierade risker och behov tydliggöra ledningens och övriga organisationens ansvar avseende informationssäkerhetsarbetet samt tilldela nödvändiga resurser, mandat och befogenheter för de funktioner som arbetet med informationssäkerhet kräver. Det behöver även säkerställas att informations-säkerhetsarbetet regelbundet och vid behov utvärderas och anpassas.

3.2.2 NIS2-direktivet

2022 beslutade EU-parlamentet om ett nytt direktiv, benämnt NIS2, med förstärkta krav och en utökning av verksamheter och sektorer som ska omfattas av lagen för att ytterligare stärka säkerheten och även samordningen inom området. I Sverige har en utredning på uppdrag av regeringen genomförts som ska ligga till grund för nytt

lagförslag i form av Cybersäkerhetslagen. Regeringskansliet väntas lämna en proposition under våren 2025.

Mot bakgrund av att ny lagstiftning kommer att införas, har vi i granskningen haft i uppdrag att efterfråga om det arbete som bedrivs är tillräckligt för att säkerställa efterlevnad av NIS2-direktivet.

Intervjuade har starkt ifrågasatt syftet med att efterfråga vilka anpassningar som gjorts i förhållande till nya krav. Detta med hänvisning till att det svenska lagförslaget inte presenterats ännu.

Vi har trots detta fått uppgifter som indikerar att kommunstyrelsen bland annat efterfrågat utökning av rambudget för att förbereda kommunen på nya lagkrav. Kommunfullmäktige har i samband med beslut om budget 2025 beslutat om tilläggsanslag om 2 300 000 kronor till kommunstyrelsen. I samband med beslutet finns följande skrivelse ”*Dessutom kommer skärpta lagkrav och ett omvärldsläge som gör att säkerhetsfrågor och informationssäkerhet blir allt viktigare att innebära stora utmaningar för kommunen, inte minst genom införandet av NIS2-direktivet och övriga lagkrav från EU som syftar till att öka den övergripande cybersäkerhetsnivån. Samtidigt innebär dessa krav en möjlighet att stärka och förbättra kommunens förmåga att hantera information och upprätthålla höga säkerhetsstandarder*”.

Finansiering ska enligt beslutet ske via ianspråktagande av kostnadsbufferten för 2025.

Därtill framhålls att NIS2-direktivet varit en del i omvärldsbevakning de senaste åren där risker identifierats och dokumenterats i verksamhetssystemet Stratsys som nyttjas i kommunen.

It-enheten har rekryterat en it-säkerhetshandläggare vars uppdrag kommer att vara att arbeta med it-säkerhetsfrågor som rör NIS2-direktivet. Däribland ingår att ta fram aktiviteter i syfte att kunna följa direktivet samt att planera och följa upp aktiviteterna. Som tidigare nämnts har även Område Juridik och säkerhet samt Område kansli förstärkt organisationen med hänvisning om att förbättra och förstärka arbetet i förhållande till nya krav.

Med grund i genomgång av protokoll kan vi inte notera något ärende där kommunstyrelsen hanterat fråga mot bakgrund av NIS2-direktivet.

3.2.3 Bedömning

Vår bedömning är att kommunstyrelsen delvis säkerställt att det bedrivs ett tillräckligt arbete för att säkerställa att NIS2-direktivet implementeras.

Vi baserar vår bedömning på att kommunstyrelsen under 2024 har efterfrågat utökad ramtilldelning från budget 2025 för anpassningar mot bakgrund av nya krav enligt NIS2-direktivet. Vi kan dock inte vid granskning av ärenden på kommunstyrelsens sammanträden notera något ärende avseende informationssäkerhet eller NIS2-direktivet.

Oaktat kommunstyrelsen hanterat ärende eller ej så kan vi genom vår granskning konstatera att kommunen inom flera områden inte når upp till de krav som nuvarande

NIS-direktiv ställer, även om det i nuläget endast riktas till en begränsad del av verksamheten.

Vi konstaterar att vissa anpassningar har gjorts, bland annat genom att förstärka verksamheten med resurser som förväntas behövas inom exempelvis it-säkerhetsområdet. Det finns dock angelägna förbättringsåtgärder att vidta inom organisatorisk säkerhet för att uppnå kraven samt att informationsägarskapet behöver etableras så att det ansvar som informationssäkerhetsarbetet utgår från etableras i samtliga verksamheter.

4 Samlad bedömning och rekommendationer

Granskningens syfte har varit att bedöma om kommunstyrelsen, och nämnderna i den omfattning de berörs, har vidtagit åtgärder utifrån revisorernas rekommendationer. I granskningen har även ingått att bedöma om kommunstyrelsen har säkerställt att NIS2-direktivet implementeras utifrån gällande krav.

Vår samlade bedömning är att kommunstyrelsen delvis beaktat tidigare lämnade rekommendationer men att åtgärderna inte varit tillräckliga.

Vår bedömning är att kommunstyrelsen delvis har säkerställt att det bedrivs ett tillräckligt arbete för att säkerställa att NIS2-direktivet implementeras.

Utifrån våra iakttagelser och bedömningar konstaterar vi att samtliga tidigare lämnade rekommendationer kvarstår helt eller delvis.

Vi rekommenderar kommunstyrelsen att:

- Säkerställa att tidigare lämnade rekommendationer beaktas i högre grad och att åtgärder vidtas i högre utsträckning.
- Säkerställa att informationsägarskapet etableras så att informationssäkerhetsarbetet genomförs av verksamhetsansvariga inom samtliga verksamheter i kommunen.
- Följa utvecklingen med NIS2-direktivet och svensk lagstiftning för att bedöma vilka anpassningar som det finns behov av för att nå efterlevnad av lagen.

Datum som ovan

KPMG AB

Jenny Thörn
Verksamhetsrevisor

Ida Larsson
Verksamhetsrevisor

Mikael Lind
Certifierad kommunal revisor