Granskning av IT-säkerhet

Rapport

Järfälla kommun

KPMG AB

2023-01-31

Antal sidor 15

Innehållsförteckning

1 Sammanfattning

KPMG har av Järfälla kommuns revisorer fått i uppdrag att granska om kommunstyrelsen säkerställer att kommunen har en tillräcklig styrning och intern kontroll vad gäller IT-säkerhet. Granskningen ingår i revisionsplanen 2022.

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen i vissa delar har en tillräcklig styrning av IT-säkerhet men att den interna kontrollen behöver stärkas.

Vi baserar bland annat vår bedömning på att det i styrande dokument eller annan dokumentation saknas beskrivning av ansvar och uppdrag för IT-avdelningen och arbetet med IT-säkerhet. Det finns endast på övergripande nivå beskrivet de krav utifrån standarder och rekommendationer som styr arbetet med IT-säkerhet. Detta har dock inte konkretiserats så att krav kan följas upp av kommunstyrelsen.

Vår bedömning är att det operativa arbetet med IT-säkerhet sker på ett ändamålsenligt sätt. Dock har vi identifierat vissa brister i nuvarande informationssäkerhetsarbete vilket kan medföra risk att IT-säkerheten försvagas. Bland annat har roller i arbetet ännu inte etablerats och vissa aktiviteter som kravställs i policy har inte genomförts fullt ut.

Vår bedömning är att kommunen både internt och genom avtal och uppdrag till externa leverantörer har säkerställt att det finns en organisation och kompetens för IT-säkerhetsarbetet. Kommunen har tillsammans med externa leverantörer regelbundet gjort riskanalyser och utvärderat implementerade säkerhetsåtgärder för att identifiera sårbarheter. Riskanalys och informationsklassning har även gjorts vid nya införanden och större förändringsprojekt så att skyddsåtgärder som bedömts nödvändiga för att skydda informationstillgångar och system kunnat implementeras.

Kommunen har genom krav på externa leverantörer etablerat tekniska verktyg och en organisation för övervakning och monitorering av säkerhetshändelser i IT-miljön vilket ger goda förutsättningar att kunna agera och hantera eventuella kritiska händelser. De skyddsåtgärder som är implementerade har utifrån befintliga hot fungerat effektivt och visat på motståndskraft mot incidenter.

Vid tid för granskningen har kommunstyrelsen inte tagit del av uppföljning eller rapportering av IT-säkerhetsarbetet under 2022. Vi noterar dock att styrande dokument, som sätter ramarna för uppföljning och återrapportering av informations- och IT-säkerhetsarbetet beslutats i början av 2022.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Tillse att det finns en dokumenterad ansvarsfördelning för IT-säkerhetsarbetet i styrande dokument eller kompletterande underlag och konkretisera vilka tekniska krav som ställs i arbetet.
- Tillse att tillämpningsanvisningar för informationssäkerhet fastställs och kommuniceras i verksamheten då informationssäkerhetsarbetet har en påverkan på förutsättningarna för IT-säkerheten.
- Säkerställa att utvecklingsarbetet utifrån beslutad informationssäkerhetspolicy fortgår, exempelvis genom att besluta om en handlingsplan som visar på prioriterade åtgärder för att arbetet ska genomföras i enlighet med de beslutade kraven.
- Etablera en årlig uppföljning av det samlade informationssäkerhetsarbetet i kommunen, där IT-säkerhet är en del. Utifrån rapporteringen besluta om åtgärder som bedöms nödvändiga för att stärka arbetet. Efterlevnad av informationssäkerhetspolicyn bör ingå som del i uppföljningen.

2 Bakgrund

Vi har av Järfälla kommuns revisorer fått i uppdrag att granska om kommunstyrelsen säkerställer att kommunen har en tillräcklig styrning och intern kontroll vad gäller IT-säkerhet.

Organisationer i offentlig sektor hanterar ovärderliga informationstillgångar och en stor del av informationen hanteras i IT-system vilket ställer höga krav på att dessa är tillgängliga och säkra. Ny teknik innebär nya möjligheter men introducerar även nya risker som ställer krav på ett balanserat risktagande och ett väl fungerande säkerhetsarbete. Brister i hanteringen kan leda till både ekonomisk skada och förtroendeskada för organisationen. Hotbilden med risker för intrång förändras kontinuerligt och säkerhetsarbetet behöver därför vara en ständigt pågående process för att säkerställa att kommunens informationstillgångar har ett tillräckligt skydd. För att kunna hantera det på ett ändamålsenligt sätt krävs att kommunen har ett systematiskt informationssäkerhetsarbete där flera funktioner i kommunen är involverade och rätt organiserade för uppdraget.

Informationssäkerhet innebär att skydda information utifrån krav på dess konfidentialitet, riktighet och tillgänglighet och måste skyddas mot obehörig åtkomst, såväl externt som internt. IT-säkerhet avser en avgränsad del av informations-säkerheten och består av delarna systemsäkerhet och kommunikationssäkerhet. Vidtagna IT-säkerhetsåtgärder ska stå i relation till de risker och behov som ansvariga har fastställt. Detta då IT-säkerheten avser att med tekniska funktioner och åtgärder skydda informationen och säkra kärnverksamhetens kontinuitet.

Med anledning av ovanstående drar kommunens revisorer slutsatsen i sin riskanalys, att kommunens rutiner avseende IT-säkerheten behöver granskas.

2.1 Syfte och revisionsfrågor

Granskningen syftar till att bedöma om kommunstyrelsen säkerställer att kommunen har en tillräcklig styrning och intern kontroll för sin IT-säkerhet.

Granskningen ska besvara 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 rutiner och processer för riskbedömning och informationsklassning 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 ändamålsenliga rutiner för att hantera och dokumentera informations- och IT-säkerhetsincidenter?
— Finns dokumenterade reserv- och återgångsrutiner vid allvarligare störningar och avbrott i IT-system? Har dessa testats för att säkerställa att de fungerar ändamålsenligt?
— Finns beslutade uppföljningsrutiner för kommunens IT-säkerhetsarbetet och är återrapporteringen till kommunstyrelsen tillräcklig?

2.2 Revisionskriterier

I granskningen har vi utgått från nedanstående revisionskriterier:

— Tillämpbara interna regelverk, policys och beslut
— MSB:s rekommendationer avseende Ledningssystem för informationssäkerhet
— NIS-direktivet i tillämpliga delar avseende kartläggning och analys av risker

Granskningen omfattar kommunstyrelsens ansvar för IT-säkerhet.

2.3 Metod

Granskningen har genomförts i följande steg:

1. Inhämtning av skriftliga svar på förutbestämda frågor till IT-avdelningen.
2. Inhämtning av underlag i form av styrande dokument, rutiner, planer mm.
3. Analys av material och svar på frågeställningar.
4. Hearing med tjänstepersoner och förtroendevalda för att inhämta kompletterande uppgifter.
5. Sårbarhetsscanning i samarbete med nyckelpersoner från kommunens IT-funktion.
6. Analys och upprättande av detta PM.

3 Resultat av granskningen

3.1 Organisation och styrning

3.1.1 Styrdokument

Kommunfullmäktige har beslutat om Informationssäkerhetspolicy[1] som gäller för samtliga nämnder och bolag i kommunkoncernen. Enligt policydokumentet är syftet med policyn att kommunen ska leva upp till rådande lagstiftning inom alla områden avseende informationssäkerhet.

Policyn anger att informationssäkerhetsarbetet ska vara systematiskt och strukturerat. Arbetssätt ska utgå från den svenska och internationella standarden Ledningssystem för informationssäkerhet (LIS) enligt ISO standard 27 000, Sveriges Kommuner och regioner (SKR) samt Myndigheten för samhällsskydd och beredskaps metodstöd för informationssäkerhetsarbete. Intervjuade beskriver att arbete fortgår med att implementera policyn och att fokus har varit att etablera ledningens ansvar.

Policyn ska konkretiseras genom ”Tillämpningsanvisningar för informationssäkerhet” som ska utgöra grunden för hantering av information. Tillämpningsanvisningar finns enligt uppgift upprättade men hade vid tiden för granskningen inte beslutats och kommunicerats. För att stärka säkerhetsmedvetenheten i verksamheterna, i väntan på att tillämpningsanvisningarna finns tillgängliga, skickade kommunstyrelseförvaltningen genom informationssäkerhetssamordnaren ut ett informationsmeddelande innehållande 15 punkter för informationssäkerhet. Bland annat att skydda sina inloggningsuppgifter, lösenordshantering, vikten av att teknisk utrustning hålls uppdaterad, vaksamhet och hantering vid misstänkta länkar i mejl med mera.

3.1.2 Roller och ansvar

I policydokumentet beskrivs roller och ansvar för informationssäkerhet.

Kommunfullmäktige beslutar om policy. Kommunstyrelsen och nämnder har det övergripande ansvaret för allt informationssäkerhetsarbete och informationstillgångarna i respektive nämnd. Policyn beskriver därtill rollerna informationsägare, informationsförvaltare och informationssäkerhetssamordnare.

Informationsägaren är förvaltningsdirektör eller VD. Genom sitt verksamhetsansvar är informationsägaren ansvarig för de informationstillgångar som hanteras i respektive verksamhet och är den som ska avgöra vilken information som hanteras, hur den ska hanteras och vem som ska hantera den. Informationsägaren ska för sin verksamhet utse informationsförvaltare som har i uppdrag att genomföra det operativa informationssäkerhetsarbetet.

[1] Informationssäkerhetspolicy beslutad av kommunfullmäktige 2022-02-21 § 29, Dnr Kst 2021/548

Det pågår ett arbete i kommunen med att etablera rollerna informationsägare och informationsförvaltare vilket i hearingen framkommer som väsentligt för att utveckla informationssäkerhetsarbetet och skapa den systematik som policyn anger som gällande för kommunen. Därtill finns behov av att fastställa och implementera tillämpningsanvisningarna så att verksamheterna får mer konkreta riktlinjer att förhålla sig till och en tydlighet över vad som behöver genomföras i respektive förvaltnings informationssäkerhetsarbete.

I hearingen lyfts att det skett en tydlig förflyttning i organisationen med större engagemang och förståelse för informationssäkerhet. Detta beskrivs ha skett dels genom beslut av policyn, dels genom informationsdelning av viktiga aspekter för att upprätthålla en god informationssäkerhet som informationssäkerhetssamordnaren delat.

Informationssäkerhetssamordnaren har ett övergripande ansvar för ledning, stöd, samordning och utveckling av informationssäkerhetsarbetet. I ansvaret ingår att upprätta och underhålla kommunens ledningssystem för informationssäkerhet. Samordnaren ska enligt policyn planera det årliga arbetet och aktiviteter för en stärkt informationssäkerhet och samordna detta med informationsägare och informationsförvaltare.

Intervjuade beskriver att informationssäkerhetssamordnaren är organiserad inom IT-avdelningen i kommunen. Avdelningen leds av IT-chef.

IT-avdelningens uppdrag är enligt de skriftliga svar vi erhållit att:

- se till att kommunens förvaltningar och skola har tillgång till en stabil, robust och säker IT-infrastruktur samt IT-support.
- stödja förvaltningarna i deras arbete och vid utveckling av IT-baserade verksamhetssystem.
- stödja förvaltningar i deras verksamhetsutveckling där IT är eller kan vara en möjliggörare

Järfälla kommuns IT-avdelning har enligt uppgift genomgått en förändringsresa de senaste åren. Efter beslut i kommunfullmäktige har stora delar av IT-verksamheten outsourcats till externa leverantörer.

I kommunen finns på IT-avdelningen, förutom de roller vi beskrivit ovan, IT-säkerhetsansvarig, IT-arkitekt samt tjänsteområdesansvariga som hanterar organisationen kring specifika tjänsteområden. Det finns även en ansvarig för IT-arbetsplats. Intervjuade beskriver att det finns ett väl etablerat samarbete mellan informationssäkerhetssamordnare och övriga funktioner inom IT-avdelningen och även i relation till säkerhetsavdelningen i kommunen.

Kommunen har en objektsförvaltningsmodell men den är enligt uppgift inte etablerad fullt ut ännu. Strukturen utgår från PM3-modellen där förvaltningsobjekt identifieras. Rollerna objektsägare, förvaltningsledare och objektspecialister är utpekade inom IT-

organisationen samt inom verksamheterna. Till objekten finns styrgrupper som fattar beslut om utveckling och åtgärder. Arbetet dokumenteras i årsvisa förvaltningsplaner som följs upp av styrgruppen.

3.1.3 Bedömning

Det finns en nyligen beslutad informationssäkerhetspolicy. Vår bedömning är dock att det saknas beskrivning i policyn eller annan kompletterande dokumentation hur ansvarsfördelning för IT-säkerhetsarbetet ser ut och vilka tekniska kravnivåer som ska gälla för kommunen. Det finns dock hänvisning till lagar och standarder som kommunens arbete ska utgå från, vilka ställer höga krav på ett systematiskt informationssäkerhetsarbete och tillhörande säkerhetsåtgärder.

Vår bedömning är att det finns en ändamålsenlig organisation för IT-säkerhetsarbetet där interna funktioner har ett tydliggjort ansvar för olika delar av arbetet. IT-avdelningen kravställer i övrigt den organisation och kompetens som det finns behov av genom avtal med externa leverantörer.

Det finns till viss del en påverkan på IT-säkerheten beroende på hur systematiskt kommunens informationssäkerhetsarbete är. Då vissa roller i informationssäkerhetsarbetet ännu inte har etablerats fullt ut kan detta riskera att försvaga IT-säkerheten.

Informationssäkerhetspolicyn beslutades under 2022 vilket medför att det vid tiden för granskningen inte har genomförts någon uppföljning av efterlevnad av det som policyn reglerar.

3.2 Tekniska skyddsåtgärder (IT- och cybersäkerhet)

3.2.1 Informationsklassning för att bedöma skyddsbehov

Enligt informationssäkerhetspolicyn ska den information som hanteras inom kommunen klassificeras enligt metoden KLASSA. Policyn anger att informationssäkerhetssamordnaren ansvarar för att klassning genomförs och att sådan klassning ska göras vid:

- upphandling
- driftsättning av nya tjänster
- utökad informationsbehandling i etablerade tjänster
- befintliga tjänster som inte klassificerats utifrån gällande lagstiftning

Utifrån klassningen ska informationens skyddsvärde bedömas och lämpliga skyddsåtgärder vidtas.

Enligt uppgifter vid hearingen görs informationsklassning alltid i samband med större förändringar samt som en del i upphandlingsprocessen. Det finns en utsedd funktion internt som deltar vid alla IT- upphandlingar.

I de skriftliga svar vi tagit del av, som svar på förberedande frågor, finns beskrivning att gap som identifieras i klassning mellan risker och skyddsbehov dokumenteras i förvaltningsplanen för respektive system. Beslut om åtgärder fattas av utsedd styrgrupp som hanterar förvaltning av respektive system.

Ytterligare uppgifter gör gällande att det har varit ett uppdrag till förvaltningarna att göra klassningar. Det har inte gjorts någon uppföljning så att det finns en nulägesbild över hur stor andel av informationstillgångarna i system som är klassade. Dock framhålls att de verksamheter som har verksamhetskritiska system eller hanterar känslig information är väl medvetna om krav på klassning och vidtagande av skyddsåtgärder.

För vissa äldre system i förvaltningarna uppges att informationsägarna kan behöva en påminnelse om att göra om klassningar så att bedömningar utgår från aktuella lagar och regler eller andra förändringar som kan påverka skyddsvärdet.
Som vi beskrivit tidigare så anlitar kommunen externa leverantörer som på uppdrag utför tjänster inom tre områden åt kommunen. De tre leverantörerna är avtalade för applikationsdrift, nätverk och klienter. Kommunen har ställt krav om säkerhetsnivåer och vissa certifieringar inom både informationssäkerhet och andra standarder, exempelvis krav på datacenter för kontinuitet. Dessa certifieringar innebär att leverantörerna regelbundet genomgår externa revisioner där utvärdering sker att de efterlever certifieringskrav.

3.2.2 Riskanalys

Representanter från kommunens IT-avdelning har en regelbunden kontakt och dialog med leverantörerna för att följa upp implementerade säkerhetslösningar och utvärdera dessa i förhållande till risker och hot.

IT-avdelningen gör regelbundet risk- och sårbarhetsanalyser tillsammans med de externa leverantörerna. Riskanalyser dokumenteras och följs sedan upp regelbundet i de forum som är etablerade mellan kommunen som beställare och leverantörerna som utförare. De forum som finns är etablerade på olika nivåer där möten på strategisk nivå genomförs där IT-chef deltar i strategiska samtal om behov och ambitioner samt leverantörens skyldighet i förhållande till det. Sedan kommuniceras detta till taktiska och operativa forum där andra representanter från IT-avdelningen och leverantören ingår som får i uppdrag att verkställa åtgärder eller implementationer.

I de skriftliga svar vi erhållit framgår att risk-och sårbarhetsanalyser är en obligatorisk del i projekt och ingår som en del av projektdokumentationen. Utsedd projektledare ansvarar för att riskanalyser genomförs och dokumenteras inom ramen för projektdokumentationen

3.2.3 Tekniska skyddsåtgärder

Enligt uppgift så har det skett en löpande modernisering av de komponenter som utgör kommunens IT-miljö med nya servrar, brandväggar och andra tekniska implementationer vilket har medfört att föråldrade verksamhetssystem i förvaltningarna har behövt bytas ut för att vara kompatibla med den nya tekniken.

Kommunen uppges, likt de flesta andra kommuner, regelbundet vara utsatt för attacker och intrångsförsök. Nuvarande skyddsåtgärder har dock klarat att hantera dessa försök. Det finns implementerade övervakningsverktyg med automatiska larm och en etablerad SOC, Security Operations Center. Uppdrag för SOC är övervakning av säkerhetshändelser dygnet runt. SOC består både av tekniska verktyg för monitorering och personella resurser som analyserar säkerhetsloggar för att identifiera avvikelser och analysera säkerhetshändelser.

IT-chef uppges ha arbetat strategiskt och målmedvetet i många år för att kommunen ska ha förutsättningar att stå emot externa hot. Vid hearingen anges också beslutet att outsourca IT-verksamheten har bidragit till kommunens möjligheter att ta del av kompetens inom området genom de externa leverantörerna. Därtill uppges leverantörerna ha mycket god kännedom om de tekniska möjligheter och produkter som erbjuds utifrån praxis och branschstandards. Något som kommunen kan dra fördel av att ha tillgång till i sitt utvecklingsarbete.

Sårbarhetsscanning

I samband med granskningen genomfördes en sårbarhetsscanning. Sårbarhetsscanningar är automatiserade verktyg som identifierar och klassificerar sårbarheter i datorer, nätverk och applikationer genom att matcha dem mot redan kända systembrister. Det kan till exempel röra sig om problem som säkerhetsuppdateringar som inte installerats, föråldrade protokoll, certifikat och tjänster.

Påträffade sårbarheter verifieras manuellt för att kontrollera dess riktighet. Resultatet levereras i form av en rapport där sårbarheter som påträffats presenteras tillsammans med en bedömning av risknivå. Med hänsyn till känsligheten i den information som presenteras i rapporten från sårbarhetsscanningen så återger vi endast resultatet på en mycket övergripande nivå i den här rapporten.

Resultatet visade på ett antal sårbarheter vilka inte bedömdes vara kritiska. Det övergripande resultatet visade på tillräckliga säkerhetsnivåer i förhållande till kända sårbarheter. Det fanns dock behov av vissa åtgärder avseende åtkomst och behörigheter. Ett antal konton hade alltför hög behörighet och rättigheter på domännivå och det fanns flertalet inaktiva eller passiva användarkonton. Därtill upptäcktes ett antal mobila enheter som var omanagerade (kan inte styras och kontrolleras av IT-avdelningen eller leverantörer vilket kan leda till risker) samt mindre allvarliga sårbarheter för webbläsare.

Sårbarhetsscanning är en enklare form av penetrationstest. Kommunen har dock även genomfört mer omfattande penetrationstest under 2019. Nya tester är enligt uppgift planerade att genomföras under 2023.

3.2.4 Bedömning

Vår bedömning är att det finns beslut om metod för informationsklassning och att detta ska göras rutinmässigt utifrån särskilda kriterier. Informationsklassning har dock endast genomförts till viss del men är ett pågående arbete i förvaltningarna. I nya införanden och större förändringsprojekt har informationsklassning genomförts och krav ställts om de skyddsåtgärder som det finns behov av.

Vår bedömning är att kommunen genom avtal och uppdrag till externa leverantörer löpande utvärderar implementerade säkerhetsåtgärder för att identifiera sårbarheter och kan därigenom vidta åtgärder för att stärka säkerheten.

De skyddsåtgärder som är implementerade har utifrån befintliga hot fungerat effektivt och visat på motståndskraft mot incidenter. Kommunen har genom krav på externa leverantörer etablerat tekniska verktyg och en organisation för övervakning och monitorering av säkerhetshändelser i IT-miljön vilket ger goda förutsättningar att kunna agera och hantera eventuella kritiska händelser.

3.3 Incident- och kontinuitetshantering

3.3.1 Incidenthantering

I de skriftliga svar vi erhållit framgår att det finns dokumenterade incidenthanteringsrutiner för personuppgiftsincidenter men att det saknas i nuläget för informationssäkerhetsincidenter.

Det pågår ett utvecklingsarbete att etablera en e-tjänst för verksamheternas hantering av informationssäkerhetsincidenter. I samband med utvecklingsarbetet kommer rutiner att tydliggöras.

IT-säkerhetsincidenter rapporteras enligt gällande instruktioner via servicedesk. Tjänsteområdesansvariga ansvarar för att eskalera till berörda parter både internt och externt.

I de fall IT-incidenter upptäcks av externa leverantörer så eskaleras dessa till kommunens IT-chef för bedömning av den fortsatta hanteringen och beslut om vilka som behöver få information om säkerhetshändelsen internt i kommunen.

3.3.2 Kontinuitetshantering

Enligt informationssäkerhetspolicyn beskrivs att kontinuitetshantering handlar om att planera för att kunna upprätthålla verksamhet och processer för att skapa en nödvändig förmåga till funktionalitet även vid händelse av exempelvis el-avbrott och IT-störningar.

Kontinuitetshanteringen ska enligt policyn vara en naturlig del i verksamhetens arbete med risk- och sårbarhetsanalys i enlighet med lagen om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap.

IT-avdelningen har servicenivåöverenskommelser, så kallade SLA, med verksamheterna. Avtalen tecknas oftast inom ramen för objektsförvaltningen. Genom dessa finns dokumentation över acceptabla avbrottstider samt rutiner för backuper mm. IT-avdelningen säkerställer i sin tur att backuper tas i enlighet med avtalen.

Det finns etablerade arbetssätt med avbrott och reservrutiner, exempelvis tas alltid backup först och återläsning testas innan större förändringar i system.

3.3.3 Bedömning

Rutin för att hantera och dokumentera informationssäkerhetsincidenter finns inte etablerad i kommunen. Vår bedömning är därför att det saknas ändamålsenliga rutiner för informationssäkerhetsincidenter.

Det finns etablerade rutiner för hantering av personuppgiftsincidenter och IT-incidenter. Vi uppfattar att det finns tydliggjorda eskaleringsvägar för dessa typer av incidenter, både internt i kommunen och även mellan kommunen och externa IT-leverantörer.

Det pågår ett utvecklingsarbete med att införa en e-tjänst för anmälan och hantering av informations- och personuppgiftsincidenter vilken vi bedömer kan bidra till att stärka förutsättningar i hanteringen av incidenter.

Vår bedömning är att det finns dokumenterade reserv- och återgångsrutiner vid allvarligare störningar och avbrott i IT-system där dokumentation kravställs och hanteras av de externa leverantörerna. Det finns upprättade överenskommelser mellan verksamheter och IT-avdelningen där krav om backuprutiner och tillgänglighet ingår. Återläsning av information testas regelbundet och verifieras innan större förändringar.

3.4 Uppföljning och rapportering

Enligt den standard som kommunens beslutat som gällande för sitt informationssäkerhetsarbete ställs krav på en årlig rapportering i form av ledningens genomgång. Ledningens genomgång syftar till att ansvariga beslutsfattare ska få en samlad bild av det informationssäkerhetsarbete som genomförts samt utifrån det ges möjlighet att fatta beslut om handlingsplan för informationssäkerhet med prioriterade åtgärder för att stärka den på övergripande nivå.

Det saknas uppgift i beslutad policy om hur uppföljning av informationssäkerhet ska genomföras men det framgår att informationssäkerhetssamordnaren har det övergripande uppdraget att utvärdera, revidera och följa upp informationssäkerheten tillsammans med informationsägare. Informationssäkerhetsamordnaren har också det övergripande uppdraget att revidera arbetssätt inom informationssäkerheten.

I de skriftliga svar vi erhållit framgår att struktur för styrning och uppföljning av informationssäkerhet (inklusive IT-säkerhet) inte är på plats men att arbete pågår mot bakgrund av fastställandet av informationssäkerhetspolicyn.

I hearingen framkommer att kommunstyrelsen uppfattar sig få viss information men att det finns behov av ytterligare informationsinsatser för att styrelsen ska känna sig informerade och ha kännedom om kommunens förutsättningar och motståndskraft mot exempelvis externa hot. Bland annat lyfts som förslag att en samlad rapportering kan ske årligen.

I de svar vi erhållit beskrivs att IT-chef rapporterar till kommundirektör men att det saknas dokumentation av den information eller rapportering som gjorts.

Det finns ett antal forum på tjänstepersonsnivå där information och uppföljning av olika aspekter som berör säkerhetsfrågor, IT och system genomförs. Exempel på dessa som framgår av de skriftliga svaren är:

- Förvaltningsgrupperna för olika objektsfamiljer
- Kris- och krigsorganisationen
- Ledningsgruppsmöten i förvaltningarna
- Dataskyddsamordningsgruppen
- Upphandlingar och projekt
- Arkitektforum med leverantörer
- Olika nätverk via myndigheter

3.4.1 Bedömning

Vår bedömning är att det för närvarande saknas beslutade uppföljningsrutiner för kommunens informationssäkerhetsarbete, där även IT-säkerheten ingår.

Därtill bedömer vi att kommunstyrelsen brustit i att följa upp och kontrollera det arbete som bedrivs inom informationssäkerhet (inklusive IT-säkerhet) då ingen uppföljning eller rapportering har genomförts under 2022. Detta trots att det finns identifierade omvärldsfaktorer med en ökad hotbild för cyberattacker eller andra intrångsförsök som riktas mot kommuner och andra organisationer. Kommunstyrelsen bör tillse att de erhåller en regelbunden uppföljning utifrån sitt övergripande ansvar för säkerhetsfrågorna i kommunen, så att de vid behov kan fatta beslut om relevanta åtgärder som de ser behov av för att stärka informations- och IT-säkerheten i kommunen.

4 Slutsats och rekommendationer

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen i vissa delar har en tillräcklig styrning av IT-säkerhet men att den interna kontrollen behöver stärkas.

Vi baserar vår bedömning på att det i styrande dokument eller annan dokumentation saknas beskrivning av ansvar och uppdrag för IT-avdelningen i arbetet med IT-säkerhet. Det finns endast på övergripande nivå beskrivet de krav utifrån standarder och rekommendationer som styr arbetet med IT-säkerhet. Detta har dock inte konkretiserats så att krav kan följas upp av kommunstyrelsen.

Vi kan utifrån granskningen konstatera att det operativa arbetet med IT-säkerhet sker på ett ändamålsenligt sätt. Kommunen har både genom interna funktioner och genom avtal och uppdrag till externa leverantörer säkerställt tillgång till kompetens och organisation för IT-säkerhetsarbetet. IT-avdelningen har tillsammans med leverantörer gjort riskanalyser och regelbundet utvärderat implementerade säkerhetsåtgärder för att identifiera sårbarheter. Kommunen har genom krav på externa leverantörer etablerat tekniska verktyg och en organisation för övervakning och monitorering av säkerhetshändelser i IT-miljön vilket ger goda förutsättningar att kunna agera och hantera eventuella kritiska händelser.

Vid tid för granskningen har kommunstyrelsen inte tagit del av uppföljning eller rapportering av IT-säkerhetsarbetet under 2022. Vi noterar dock att styrande dokument, som sätter ramarna för uppföljning och återrapportering av informations- och IT-säkerhetsarbetet beslutats i början av 2022.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Tillse att det finns en dokumenterad ansvarsfördelning för IT-säkerhetsarbetet i styrande dokument eller kompletterande underlag och konkretisera vilka tekniska krav som ställs i arbetet.
- Tillse att tillämpningsanvisningar för informationssäkerhet fastställs och kommuniceras i verksamheten då informationssäkerhetsarbetet har en påverkan på förutsättningarna för IT-säkerheten.
- Säkerställa att utvecklingsarbetet utifrån beslutad informationssäkerhetspolicy fortgår, exempelvis genom att besluta om en handlingsplan som visar på prioriterade åtgärder för att arbetet ska genomföras i enlighet med beslutade kraven.
- Etablera en årlig uppföljning av det samlade informationssäkerhetsarbetet i kommunen, där IT-säkerhet är en del. Utifrån rapporteringen besluta om åtgärder som bedöms nödvändiga för att stärka arbetet. Efterlevnad av informationssäkerhetspolicyn bör ingå som del i uppföljningen.

Datum som ovan

KPMG AB

Jenny Thörn
Kommunal revisor

William Andreasson
Kommunal revisor

Mikael Lind
Certifierad kommunal revisor
Kundansvarig