Granskning av kommunens informations- och IT-säkerhetsarbete

Rapport

Täby kommun

KPMG AB

Datum 2023-10-18

Antal sidor 22

Täby kommun
Granskning av kommunens informations- och IT-säkerhetsarbete
2023-10-18

Innehållsförteckning

1 Sammanfattning

KPMG har av Täby kommuns förtroendevalda revisorer fått i uppdrag att genomföra en översiktlig granskning för att upprätthålla en god informations- och IT-säkerhet. Uppdraget ingår i revisionsplanen för år 2023.

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen och nämnder i allt väsentligt bedriver ett systematiskt informationssäkerhetsarbete och att det sker på ett ändamålsenligt sätt.

Vi gör vår bedömning baserat på att det finns styrande och stödjande dokument som tydliggör krav på hur arbetet ska bedrivas samt tydliggör ansvar för aktiviteter och åtgärder som behöver vidtas för att informationssäkerhetsarbetet ska vara systematiskt.

Vi konstaterar att det finns ett engagemang för frågorna, en organisation och ansvarsfördelning som ger förutsättningar för ett systematiskt arbete. Vi bedömer att riskbedömningar och kartläggningar har bidragit till en kännedom om sårbarheter och behov av förbättringsåtgärder och att dessa har prioriterats för att stärka kommunens informations- och IT-säkerhet. Åtgärder har följts upp och i delar rapporterats till kommundirektör och kommunstyrelsen.

Även om vår bedömning är att arbetet i allt väsentligt sker på ett systematiskt sätt har vi identifierat ett antal förbättringsområden för att informations- och IT-säkerhetsarbetet ska stärkas ytterligare. Då granskningen baseras på uppgifter på en övergripande nivå är vissa av rekommendationerna till nämnderna av mer generell karaktär.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen utifrån deras övergripande ansvar att:

- Aktualisera informationssäkerhetspolicyn och utvärdera behov av riktlinjer för arbetet i enlighet med lämnat uppdrag till kommundirektören.
- Överväga om informationssäkerhetsutbildningar ska vara obligatoriska, samt besluta med vilken regelbundenhet de ska genomföras samt etablera rutiner för att även inkludera nyanställda och nytillträdda förtroendevalda.
- Utvärdera behov av att stärka kommunens förmåga att upptäcka säkerhetshändelser genom bl.a. övervakning och loggar, både avseende tekniska implementationer och att det finns en incidentorganisation och beredskap med tillräckliga förutsättningar att skyndsamt agera på hot och risker.
- Etablera ledningens genomgång i enlighet med anvisningar så att en samlad uppföljning av informationssäkerhetsarbetet finns dokumenterad och rapporteras till kommunstyrelsen.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen och samtliga nämnder att:

- Säkerställa att informationsklassning och riskbedömning har gjorts för de informationstillgångar som hanteras inom respektive verksamhet.
- Utifrån informationsklassning och riskbedömning säkerställa att de skyddsbehov som identifieras följs upp med relevanta säkerhetsåtgärder.

- Säkerställa att utbildningsinsatser regelbundet genomförs för att bibehålla och utveckla en säkerhetskultur och medvetenhet om informationssäkerhetsrisker.

2 Bakgrund

KPMG har av Täby kommuns förtroendevalda revisorer fått i uppdrag att genomföra en översiktlig granskning för att upprätthålla en god informations- och IT-säkerhet. Uppdraget ingår i revisionsplanen för år 2023.

Organisationer i offentlig sektor hanterar ovärderliga informationstillgångar och blir alltmer beroende av sina 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 all skyddsvärd information ska vara tillgänglig, konfidentiell och spårbar. Den digitala transformationen 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 riskerna blir mer svårbedömda och att beroenden blir svårare att överskåda. Den digitala utvecklingen måste följas av ett anpassat och balanserat säkerhetsarbete för att säkerställa att de system och digitala tjänster som nyttjas för informationshantering och lagring inte är exponerade och tillgängliga för cyberhot och angrepp. Där tekniken implementeras på ett ogenomtänkt eller otillräckligt sätt uppstår brister som kan utnyttjas av hotaktörer.

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

2.1 Syfte, revisionsfrågor och avgränsning

Granskningen har syftat till att bedöma om kommunstyrelsen och nämnder bedriver ett systematiskt informationssäkerhetsarbete så att det sker på ett ändamålsenligt sätt.

Granskningen ska besvara följande revisionsfrågor:

- Finns aktuella styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas? Vem blir ansvarig vid en allvarlig händelse.
- Finns ett systematiskt arbete med riskanalyser och informationsklassning? Finns exempel på en utförd riskanalys och informationsklassning att del av?
- Har styrelse och nämnder tillsett att det finns en tillräcklig säkerhetskultur?
- Genomförs utbildningsinsatser och finns rutiner för uppföljning av hur många som genomfört kurser? Är uppföljningen tillfredsställande?
- Finns en etablerad övervakning för att upptäcka hot om intrång eller andra säkerhetsincidenter i IT-miljön?
- Finns en etablerad uppföljning av informations- och IT-säkerhetsarbetet och rapporteras denna till styrelse och nämnder med regelbundenhet?

Granskningen omfattar en översiktlig granskning av kommunstyrelsens övergripande ansvar för informationssäkerhet och IT-säkerhet samt kommunstyrelsen och nämndernas verksamhetsansvar för de informationstillgångar som hanteras inom respektive nämnd.

Granskningen avgränsas till revisionsfrågorna.

2.2 Revisionskriterier

De revisionskriterier som granskningen utgår från är:

- Kommunallagen 6 kap. 6 §
- Tillämpbara interna regelverk, policys och beslut
- MSB:s metodstöd och rekommendationer avseende Ledningssystem för informationssäkerhet och IT-säkerhetsåtgärder
- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster där detta är tillämpbart

2.3 Ansvarig nämnd/styrelse

Granskningen avser kommunstyrelsen, barn- och grundskolenämnden, gymnasie- och näringslivsnämnden, kultur- och fritidsnämnden, stadsbyggnadsnämnden, socialnämnden, äldrenämnden, överförmyndarnämnden, lantmäterinämnden, valnämnden, Södra Roslagens miljö- och hälsoskyddsnämnd.

2.4 Metod

Granskningen har genomförts genom dokumentstudier och intervjuer med berörda tjänstepersoner.

Rapporten är faktakontrollerad av intervjupersoner.

3 Resultat av granskningen

3.1 Organisation och styrning av informationssäkerhetsarbetet

3.1.1 Styrande dokument

Policy

Informationssäkerhetspolicy, fastställd av kommunfullmäktige 2018-05-18, beskriver på övergripande nivå kommunens viljeriktning och mål med informationssäkerhetsarbetet. Policydokumentet anger att information ska skyddas utifrån principerna om tillgänglighet, riktighet, och konfidentialitet.

Kommundirektören har enligt policyn uppdraget från kommunstyrelsen att fastställa Riktlinjer för informationssäkerhet för Täby kommun. Vi har i granskningen inte tagit del av några riktlinjer. Däremot har Trygghets- och säkerhetsenheten upprättat anvisningar för informationssäkerhetsarbetet som sedan fastställts av trygg- och säkerhetschef samt avdelningschef för Verksamhetsstöd och utveckling i maj 2023. Dessa presenteras nedan.

Anvisningar

Anvisning för ledning och styrning av kommunens systematiska informationssäkerhetsarbete beskriver hur informationssäkerhetsarbetet i kommunen och dess bolag ska struktureras. Av anvisningen framgår att

kommunen önskar bedriva ett systematiskt informationssäkerhetsarbete genom införande av ett ledningssystem för informationssäkerhet (LIS). Anvisningen beskriver vidare roller och ansvar i systemförvaltningsorganisationen och tydliggör ansvar för objekt.

Anvisningen tydliggör även krav på bland annat behörighetshantering, kontinuitetshantering, incidenthantering och användarinstruktioner.

Anvisning informationssäkerhet för medarbetare inklusive personalsäkerhet beskriver hur medarbetare ska hantera information och verktyg. Personalsäkerhet beaktas som en del av informationssäkerhetsarbetet och anvisningarna innehåller beskrivningar av personalsäkerheten under anställning samt vid avslut.

Anvisning för informationssäkerhet för IT-miljö i egen regi konkretiserar den övergripande informationssäkerhetspolicyn och sätter ramarna för hur det IT-tekniska informationssäkerhetsarbetet ska genomföras. Anvisningen anger vi hur informationstillgångar ska hanteras och beskriver också regler för IT-utrustning och lagringsmedia.

Anvisning för informationssäkerhet i leverantörsrelationer beskriver hur arbetet med leverantörer under hela livscykeln (från upphandling till avslut) ska ske för att nå en god informationssäkerhet. Upphandlande part ska ställa krav på informationssäkerhet gentemot alla leverantörer som kan tillgå, behandla, lagra, kommunicera eller tillhandahålla infrastrukturkomponenter för kommunens information.

3.1.2 Organisation och ansvarsfördelning

I styrande dokument finns följande beskrivningar av ansvarsfördelning i informationssäkerhetsarbetet.

1. Kommundirektören är huvudansvarig för informationssäkerhetsarbetet.
2. Trygghets- och säkerhetschefen är övergripande ansvarig för styrning, inriktning, tillsyn och samordning av kommunens informationssäkerhetsarbete.
3. Kommunens medarbetare ansvarar för att upprätthålla en god informationssäkerhet och rapportera noterade eller misstänkta brister till närmsta chef.
4. Verksamhetsområdeschef och vd i bolag ansvarar för att verksamheten efterlever kommunens informationssäkerhetspolicy, anvisningar, rutiner och instruktioner. Detta utifrån att informationssäkerhetsansvaret ingår i det ordinarie verksamhetsansvaret.
5. Informationssäkerhetssamordnare fungerar som ett stöd till medarbetare, chefer och kommunledning.
6. Ansvar för informationssäkerheten i särskilda objekt enligt kommunens IT-förvaltningsmodell åligger objektägare.

I styrande dokument beskrivs även roller och ansvar avseende IT-säkerhetsarbetet där detta är fördelat mellan chefer inom IT-funktionen. Funktionens övergripande ansvar är att tillse en tillräcklig säkerhet i kommunens IT-miljö, så att legala krav, krav från verksamheter och informationssäkerhetspolicy följs.

1. IT-chef har rollen objektägare för kommunens infrastruktur och digitala arbetsplats och är operativt ansvarig för informationssäkerhet utifrån behov från verksamheten och krav enligt styrande dokument.
2. IT-säkerhetstekniker och medarbetare vid den centrala IT-funktionen ansvarar för omvärldsbevakning, analyserar hotbilder och ansvarar för att hantera tekniska sårbarheter inom tilldelat område.
3. ”Major incident manager” leder arbetet med kritiska IT-incidenter i ett akut skede.

Intervjuade bekräftar att ansvaret är etablerat i enlighet med styrande dokument. I intervjuer beskrivs att kommunen genom ett trygghets- och säkerhetsprogram under åren 2019 och 2020 påbörjade ett mer fokuserat arbete med informationssäkerhet. I arbetet valde kommunen att utgå från Myndigheten för Samhällsskydd och beredskaps metodstöd för systematiskt informationssäkerhetsarbete.

Som tillägg till detta beskrivs att det finns en etablerad samordning och gemensamma arbetssätt mellan Trygghet- och säkerhetsenheten samt IT- och digitalisering. Särskilt lyfts detta utifrån ökad hotbild för cyberangrepp. Aktiviteter finns samlade i en handlingsplan för ökad cybersäkerhet som visar prioriterade åtgärder framåt.

Ansvar vid allvarlig händelse

Rollen ”Major Incident Manager” leder arbetet med kritiska IT-incidenter i ett akut skede och har i uppdrag att samla de kompetenser som behövs för att hantera den kritiska händelsen. I dokumentet *Ramverk för Täby kommuns IT-leverans* beskrivs de viktigaste arbetssätten och principerna för kommunens IT-verksamhet. Målet med incidentprocessen uppges vara att:

• Så snabbt och effektivt som möjligt påbörja hantering av, och åtgärda incidenter i kommunens IT-leverans.

• Ge snabb och tydlig information till användare och ansvariga vid incident- och problemhantering.

• Skapa robusthet i kommunens IT-leverans genom att problem analyseras och åtgärdas i grunden, i stället för hantering av symtom.

Av handlingsplanen för ökad cybersäkerhet anges att kommunens incidenthanteringsprocess behöver utvecklas under 2023 och även övas. Efter dialog med verksamheten framkommer att ett aktivt arbete pågår med att utveckla incidentshanteringsprocessen. En beskrivning utav incidenthanteringsprocessen pågår men verksamheten har valt att avvakta med att färdigställa denna till dess att den nationella utredningen gällande tillämpning av den nya NIS-2 lagstiftningen är färdigställd. Detta för att säkerställa att processbeskrivningen inkorporerar samtliga, enligt lagen, väsentliga delar. Utredningen beräknas presenteras runt den 20 februari, varpå processbeskrivningen är tänkt att presenteras efter detta.

Efter publicering kommer praktisk övning utav incidenthanteringsrutinen att genomföras utav samtliga involverade.

3.1.3 Bedömning

Vi bedömer att det finns aktuella styrande dokument som tydliggör ansvar, kravställning och hur informationssäkerhetsarbetet ska bedrivas. I nuläget är det dock endast policyn som är politiskt antagen. Riktlinjer som kommundirektören uppdragits att upprätta saknas men däremot har anvisningar upprättats och fastställts i syfte att konkretisera policyns viljeriktning.

Vi bedömer att det finns en organisation med tilldelade roller och ansvar för det arbete och de aktiviteter som behöver genomföras i informationssäkerhetsarbetet. Det finns en särskilt utsedd funktion som tar ansvar för att hantera och samordna arbetet vid allvarlig incident i enlighet med etablerad incidenthanteringsprocess.

3.2 Riskbedömning och informationsklassning

Anvisning för ledning och styrning av informationssäkerhet inkluderar krav om informationsklassning och riskanalyser med beskrivningen att om detta genomförs så genereras goda förutsättningar att kunna utforma rätt skyddsåtgärder, både så att skyddet är tillräckligt och för att undvika överskydd och därigenom onödigt höga kostnader. Riskanalyser bör genomföras i samband med informationsklassning. Åtgärdsbehov som synliggörs ska hanteras utan dröjsmål och analysens resultat ska dokumenteras.

Det framgår att informationsklassningar alltid ska genomföras inför upphandling eller inköp av IT-system, samt vid större förändringar som påverkar informationen i systemet eller användningen av det. Det finns en tillämpningsanvisning fastställd för nyanskaffning som beskriver krav på informationsklassning. Detta ska göras tillsammans med trygg- och

säkerhetsenheten. Bedömningen ska sedan ligga till grund för val av lösning, utformning av avtal, teknisk införande, med mera.

Vi har tagit del av kommunens metodstöd för informationsklassning. Metodstödet innehåller beskrivningar kring varför informationsklassningar ska genomföras och information kring perspektiven rörande konfidentialitet, riktighet och tillgänglighet. Av metodstödet framgår att kommunen använder KLASSA för informationsklassning och riskanalys (KLASSA är ett verktyg för informationsklassning och riskanalys som tillhandahålls av Sveriges kommuner och regioner).

Vi har tagit del för genomförda riskanalyser och informationsklassningar enligt av kommunen beslutad modell (KLASSA) för kommunledningskontoret och de granskade nämndernas förvaltningar. Utifrån genomgånget underlag, som inte kommer beskrivas närmare i rapporten med hänvisning till att dessa kan visa sårbarheter, noterar vi att informationsklassningar finns genomförda för respektive nämnds område.

Enligt intervjuade deltar informationssäkerhetssamordnare och en funktion från IT och digitalisering i samtliga klassningar. Anledningen uppges vara att bedömningar ska ske på likvärdigt sätt och skapa en enhetlighet. Samtidigt skapas ett lärande för verksamheterna i processen och kunskap kan spridas vidare för förståelse om vikten av klassning och riskbedömning av de informationstillgångar som hanteras.

I arbetet med internkontroll hade kommunledningskontoret under 2022 identifierat tre risker inom informationssäkerhet varav en avsåg informationsklassning. Trygghet- och säkerhetsenheten har genom informationssäkerhetssamordnaren genomfört uppföljning av risker vid två tillfällen under 2022. I uppföljningsrapporten redogörs för arbetet med

informationsklassning där det framgår att arbetet med att förankra Täbys framtagna modell för informationsklassning har fortsatt och genomgång med nyckelfunktioner inom kommunen har genomförts, bland annat från central IT-funktion och inköpsenhet. Ett fokuserat arbete uppges ha bedrivits med att genomföra informationsklassningar med över 90 genomförda informationsklassningar sedan vintern 2021.

I den rapportering som genomförts vad gäller internkontrollmoment görs bedömningen att identifierad risk är hanterad och att risken därigenom kan utgå från internkontrollplanen. Som motivering till att risken hanterats uppger verksamheten att ett intensivt arbete har pågått under de senaste 1,5 åren med informationsklassningar. Däribland framhålls att verksamheten skapat goda förutsättningar för genomförandet av informationsklassningar i större omfattning samt att rutiner och annat stödmaterial har tagits fram. Framtagna rutiner och stödmaterial syftar till att minska risken för att informationsklassningar inte genomförs korrekt i framtiden.

3.2.1 Bedömning

Vi bedömer att kommunstyrelsen och nämnderna har tillsett att det finns ett systematiskt arbete med riskanalyser och informationsklassning. Det har genomförts ett stort antal klassningar och arbetet har löpande följts upp för att säkerställa att arbetet fortgår. Vi kan, utifrån de exempel vi tagit del av, konstatera att dessa har genomförts i enlighet med kommunens beslutade modell samt att åtgärdsplaner finns upprättade som visar behov av säkerhetsåtgärder.

Det är dock av vikt att arbetet med nya informationsklassningar och riskanalyser genomförs samt att befintliga aktualiseras utifrån den information som hanteras

och för att säkerställa att skyddsbehov är tillräckliga för att möta nya risker och krav.

3.3 Kunskap och medvetenhet om informationssäkerhetsrisker

Av kommunens anvisning för informationssäkerhet för medarbetare framgår att alla medarbetare ska arbeta för att uppnå ett säkert beteende. Här ingår exempelvis att följa aktuella rutiner för klienter, lösenordshantering, e-post, sociala medier och distansarbete. Därtill framgår att anställda kontinuerligt ska erbjudas utbildning inom informationssäkerhet och dataskydd och att genomförd utbildning ska dokumenteras.

Vi har tagit del av en uppföljning av genomförd informationssäkerhetsutbildning för chefer. Av underlaget framgår bland annat att 97 % av deltagande chefer startade utbildningen och genomförde en eller flera lektioner och att 71 % slutförde den. Av underlag för utbildning för förtroendevalda startade 56 % utbildningen och 53 % slutförde den. Av underlag från utbildning som riktas till alla anställda hade 42 % startat utbildningen per 19 juni -23, utbildningen är pågående vid tid för granskningen och ytterligare moment kvarstår och beräknas slutföras under november 2023. Det finns funktion för påminnelser för att öka genomförandegraden.

3.3.1 Bedömning

Vi bedömer att styrelse och nämnder delvis har säkerställt en tillräcklig säkerhetskultur. Utbildningsinsatser har genomförts och de insatser som erbjudits har följts upp regelbundet.

Vi ser det som väsentligt att deltagarnivån ökar och att samtliga utbildningar slutförs. Vi noterar att utbildningen för medarbetare ännu inte är avslutad, men

kan konstatera att avslutningsfrekvensen för chefer och framför allt förtroendevalda behöver öka för att etablera en tillräcklig säkerhetskultur. Därtill vill vi poängtera att det är av vikt att rutiner etableras för att inkludera nyanställda i utbildningsinsatser. Samt att hitta former för repetition för att aktualisera kunskap och hålla medvetenheten på en hög nivå. Detta då användare är en riskfaktor vid cyberhot och intrångsförsök.

3.4 Förmåga att detektera säkerhetshändelser

Styrande dokument anger hur IT-säkerhetsrisker och tekniska sårbarheter ska förebyggas. Detta ska bland annat ske genom löpande övervakning av IT-miljön, för att hot eller säkerhetsbrister ska noteras. Virusskydd ska alltid finnas och kontroller ska ske automatiskt. Virusdefinitionsfiler ska också uppdateras kontinuerligt för att garantera att detektionsförmågan är aktuell. Det anges att system ska logga fel, användaraktiviteter och säkerhetshändelser. Logginformationen ska sparas och ska granskas löpande genom stickprovskontroller. Detta görs i syfte att upptäcka incidenter och händelser där åtgärder behöver vidtas.

Intervjuade beskriver att det sker en regelbunden omvärldsbevakning av hot och risker som sedan gås igenom varannan vecka i gruppering för informationssäkerhet och cybersäkerhet. Utifrån denna genomgång bedöms om det finns behov av åtgärder för att möta risker eller sårbarheter.

IT-funktionen har gjort en kartläggning av IT-säkerhetsåtgärder utifrån en vedertagen standard för att bedöma kommunens säkerhetsnivå. Ett flertal av de åtgärder som vidtagits motsvarade den grundläggande nivån. Utifrån resultatet kan åtgärder prioriteras för att nå en högre säkerhetsnivå.

Av handlingsplanen för ökad cybersäkerhet finns prioriterade åtgärder där utveckling av systematiken avseende loggar och övervakning ingår. Det finns även förslag på åtgärder för att utöka förmåga till incidentrespons. Med hänsyn till att alltför detaljerade uppgifter kan utgöra känsliga uppgifter så redogör vi inte mer i detalj för åtgärder.

3.4.1 Bedömning

Vi bedömer att det finns krav genom fastställda anvisningar avseende övervakning och loggkontroll samt ytterligare tekniska skydd för att detektera och kunna agera på säkerhetshändelser. Vi bedömer att det finns en etablerad övervakning för att upptäcka hot om intrång eller andra incidenter i IT-miljön. Utifrån nuvarande hot och risker kan det dock finnas behov av att stärka dessa delar både med tekniska implementationer och en incidentorganisation som har tillräckliga förutsättningar att skyndsamt agera på hot och risker varpå behov av detta bör utvärderas.

3.5 Uppföljning och rapportering

Anvisning för ledning och styrning av informationssäkerhet beskriver former för uppföljning av informationssäkerhetsarbetet. Det framgår att informationssäkerhetsarbetet ska följas upp och utvärderas löpande. Respektive verksamhetsområde ansvarar för detta. Kommunledningsgruppen ska därtill kontinuerligt hållas uppdaterad om informationssäkerhetsarbetet.

Kommunens säkerhetschef ska enligt anvisningarna planlägga ledningens genomgång och tillsammans med kommundirektör avgöra omfattning, form och frekvens. Då anvisningar nyligen fastställts har inte detta moment hunnit genomföras. Däremot uppges att uppföljning under 2022 och 2023 har utgjorts av uppföljning inom ramen för internkontrollens informationssäkerhetsrisker, vilken har återrapporterats till kommunstyrelsen. Samt genom den handlingsplan för ökad cybersäkerhet som vi beskrivit tidigare.

Kommunen har därtill beslutat att informationssäkerhetsarbetet löpande ska följas upp genom ett verktyg som Myndigheten för samhällsskydd och beredskap tillhandahåller ”Infosäkkollen”. Verktyget är framtaget för att stödja

uppföljning och förbättring av systematiskt informations- och cybersäkerhetsarbete för organisationer.

Vi har tagit del av den senaste sammanställningen av resultat för ”Inforsäkkollen” för 2023 där det ingår en jämförelse med värden från 2021. Diagram visar att det har skett förbättringar inom samtliga områden mellan åren men att det fortfarande finns förbättringsåtgärder för att nå upp till den högstanivån av systematik i informationssäkerhetsarbetet.

3.5.1 Bedömning

Vår bedömning är att det i allt väsentligt finns en etablerad uppföljning av informations- och IT-säkerhetsarbetet. Det finns en etablerad struktur för att över tid utvärdera kommunens arbete för att nå en högre grad av systematik.

Bedömningen görs med bakgrund av att anvisningar, där former för uppföljning och rapportering beskrivs, nyligen har fastställts, men genomgång med ledningen har inte hunnit genomföras vid tid för granskningen. Rapportering till kommunstyrelsen har utgjorts av uppföljning av de risker för informationssäkerhet som inkluderats i internkontrollplan för 2022.

Vi bedömer att en samlad uppföljning och rapportering bör göras minst årligen till kommunstyrelsen så att de är informerade om kommunens förutsättningar i arbetet och vid behov kan besluta om åtgärder som ytterligare kan stärka säkerheten i kommunen. De risker som varit inkluderade i internkontrollplanen anser vi vara relevanta. Vi konstaterar dock att de inte i tillräcklig grad kan utgöra en samlad uppföljning av kommunens informationssäkerhetsarbete.

4 Slutsats och rekommendationer

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen och nämnder i allt väsentligt bedriver ett systematiskt informationssäkerhetsarbete och att det sker på ett ändamålsenligt sätt.

Vi baserar vår bedömning på att det finns styrande och stödjande dokument som tydliggör krav på hur arbetet ska bedrivas samt ansvarsfördelning för aktiviteter och åtgärder som behöver vidtas för att informationssäkerhetsarbetet ska vara systematiskt. Vi konstaterar att det finns en uppföljning av arbetet och en god kännedom om sårbarheter och identifierade förbättringsåtgärder för att stärka kommunens informations- och IT-säkerhet.

Vi bedömer att kommunstyrelsen och nämnderna har tillsett att det finns ett systematiskt arbete med riskanalyser och informationsklassning. Utbildningsinsatser inom informationssäkerhet har erbjudits och det finns en tillräcklig uppföljning över deltagandet. Dock skulle genomförandegraden behöva öka för att kommunen ska ha en tillräcklig säkerhetskultur så att användarna känner till informationssäkerhetsrisker.

Vi bedömer att det finns en etablerad övervakning för att upptäcka hot om intrång eller andra incidenter i IT-miljön. Utifrån nuvarande hot och risker kan det dock finnas behov av att stärka dessa delar både med tekniska implementationer och en incidentorganisation som har tillräckliga förutsättningar att skyndsamt agera på hot och risker varpå behov av detta bör utvärderas.

Även om vår bedömning är att arbetet i allt väsentligt sker på ett systematiskt sätt har vi identifierat ett antal förbättringsområden för att informations- och IT-säkerhetsarbetet ska stärkas ytterligare.

Då granskningen baseras på uppgifter på en övergripande nivå är vissa av rekommendationerna till nämnderna av mer generell karaktär.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen utifrån deras övergripande ansvar att:

- Aktualisera informationssäkerhetspolicyn och utvärdera behov av riktlinjer för arbetet i enlighet med lämnat uppdrag till kommundirektören.
- Överväga om informationssäkerhetsutbildningar ska vara obligatoriska, samt besluta med vilken regelbundenhet de ska genomföras samt etablera rutiner för att även inkludera nyanställda och nytillträdda förtroendevalda.
- Utvärdera behov av att stärka kommunens förmåga att upptäcka säkerhetshändelser genom bl.a. övervakning och loggar, både avseende tekniska implementationer och att det finns en incidentorganisation och beredskap med tillräckliga förutsättningar att skyndsamt agera på hot och risker.
- Etablera ledningens genomgång i enlighet med anvisningar så att en samlad uppföljning av informationssäkerhetsarbetet finns dokumenterad och rapporteras till kommunstyrelsen.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen och samtliga nämnder att:

- Säkerställa att informationsklassning och riskbedömning har gjorts för de informationstillgångar som hanteras inom respektive verksamhet.
- Utifrån informationsklassning och riskbedömning säkerställa att de skyddsbehov som identifieras följs upp med relevanta säkerhetsåtgärder.

- Säkerställa att utbildningsinsatser regelbundet genomförs för att bibehålla och utveckla en säkerhetskultur och medvetenhet om informationssäkerhetsrisker.

Datum som ovan

KPMG AB

Jenny Thörn
Verksamhetsrevisor

Viktor Tagesson
Verksamhetsrevisor

Micaela Hedin
Certifierad kommunal revisor & Kundansvarig