Granskning av informations- och it-säkerhet

Revisionsrapport

Tranemo kommun

KPMG AB

2024-10-16

Antal sidor 18

Tranemo kommun
Granskning av informations- och it-säkerhet

2024-10-16

Innehållsförteckning

1 Sammanfattning

KPMG har av Tranemo kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunstyrelsens ansvar för att kommunen har ett systematiskt informations- och IT-säkerhetsarbete.

Granskningen har syftat till att bedöma om kommunstyrelsen tillsett att ett systematiskt informations- och IT-säkerhetsarbete bedrivs.

Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsen vid tid för granskningen delvis tillsett att ett systematiskt informations- och IT-säkerhetsarbete bedrivs.

Vi kan konstatera att det finns ett ledningssystem för informationssäkerhet med styrande dokument som tydliggör ansvar och roller och krav på det operativa informationssäkerhetsarbetet. I nuläget finns en etablerad organisation och tydliggjorda processer för aktiviteter samt uppföljning mot kommunstyrelsen. Genom detta anser vi att kommunstyrelsen skapat förutsättningar för att etablera ett systematiskt informationssäkerhetsarbete inom kommunen.

Det operativa arbete som utförs i dagsläget motsvarar däremot **inte** en omfattning som kan betraktas som systematisk i vissa väsentliga avseenden, där vi bedömer att det delvis finns en tillräcklig förmåga att upptäcka och hantera kritiska säkerhetshändelser. Det gäller framför allt arbetet med informationsklassningar som är i en utvecklingsfas liksom insatser för att stärka säkerhetskulturen där arbete pågår för att förbättra dessa processer.

Ett systematiskt arbete med informationsklassningar är en grund för att visa om det finns behov av ytterligare tekniska säkerhetsåtgärder. I nuläget har inte klassningar och riskanalyser genomförts i tillräcklig omfattning för att ge ett fullständigt underlag att utgå från även om arbetet har genomförts för en stor del av informationstillgångarna.

IT-beredskap ger förutsättningar att hantera kritiska incidenter som uppstår utanför ordinarie kontorstid. Dock är det en sårbarhet att det inte finns någon teknisk övervakning av it-infrastrukturen, vilket riskerar leda till att intrångsförsök och andra hot inte upptäcks i tillräcklig tid för att kunna avvärjas.

Gällande avtalssamverkan inom IT-verksamheten och behovet av IT-stöd och support finns en tydliggjord ansvarsfördelning och strukturerade samverkansforum där löpande uppföljning av avtalssamverkan görs.

Vad avser att säkerhetsåtgärder har vidtagits som ett resultat av riskbedömningar, bedömer vi att det har skett delvis.

I syfte att säkerställa att informationssäkerhetsarbetet utvecklas och etableras i enlighet med styrande dokument och de lagkrav som verksamheter har att följa, är det väsentligt att kommunstyrelsen säkerställer en tillräcklig **intern kontroll** över arbetet.

Utifrån genomförd granskning rekommenderar vi kommunstyrelsen att:

- Upprätta handlingsplaner för beslutade informationssäkerhetsmål
- Tillse att informationssäkerhetsutbildning genomförs i högre grad inom samtliga verksamheter.
- Tillse att riktade utbildningsinsatser i informationssäkerhet genomförs för förtroendevalda
- Fortsätta verka för att arbete med informationsklassningar systematiseras ytterligare
- Tillse att sektionernas efterlevnad inkluderas i den årliga uppföljningen.
- Redogörelser, rapporteringar och uppföljningar som upptas vid kommunstyrelsens sammanträden dokumenteras i protokollen.
- Säkerställa att handlingar som skapas inom kommunstyrelsen förses med datum för upprättande.
- Tillse att uppföljning sker av att avtalade leverantörer som står för extern drift av it-system vidtar adekvata it-säkerhetsåtgärder i syfte att skydda kommunens informationstillgångar

I nedan tabell redovisas vår bedömning per revisionsfråga

Revisionsfrågor	Bedömning
Finns aktuella styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas?	Ja
Finns en ändamålsenlig organisation för informationssäkerhetsarbetet?	I allt väsentligt
Finns en tydliggjord ansvarsfördelning mellan kommunens funktioner och de funktioner som tillhandahålls genom avtalssamverkan med Ulricehamns kommun inom it?	Ja
Finns etablerade samverkansforum och en struktur för dialog utifrån det avtal som tecknats?	Ja
Har avtalssamverkan med Ulricehamns kommun följts upp avseende kommunens behov av support och stöd inom it till kommunens medarbetare och förtroendevalda?	Ja

Har åtgärder vidtagits för att minska svarstiden avseende IT-stödet från Ulricehamns kommun?	Ja
Finns beslutade informationssäkerhetsmål?	Ja
Finns tillhörande handlingsplaner för informationssäkerhetsmål?	Nej
Finns det en tillräcklig säkerhetskultur hos kommunens medarbetare?	Delvis
Har säkerhetsåtgärder vidtagits som ett resultat av riskbedömningar?	Delvis
Sker en uppföljning att avtalade leverantörer avseende extern drift av it-system vidtar de säkerhetsåtgärder som det har bedömts finnas behov av?	Nej
Finns en tillräcklig förmåga att upptäcka och hantera kritiska it-säkerhetshändelser?	Delvis
Finns en tydliggjord struktur för ansvar vid kritiska händelser och hur information ska eskaleras mellan Ulricehamns kommuns it-funktion och kommunen?	Ja
Genomförs uppföljning av kommunens informations- och IT-säkerhetsarbete?	Ja Dock kan apportering för kommunstyrelsen ej verifieras. Vidare saknas datum för upprättande av uppföljningsdokumentet.
Är sektionernas efterlevnad av interna styrdokument och lagkrav inom informationssäkerhet inkluderad?	Nej

För närmare beskrivning av bakgrunden till våra bedömningar hänvisar vi till respektive avsnitt i revisionsrapporten.

2 Bakgrund

KPMG har av Tranemo kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunstyrelsens ansvar för att kommunen har ett systematiskt informations- och IT-säkerhetsarbete. Uppdraget ingår i revisionsplanen för år 2024.

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 säkerhetsarbete för att säkerställa att inte de system och digitala tjänster som nyttjas för informationshantering och lagring är exponerade och tillgängliga för cyberhot och angrepp. Ett flertal offentliga organisationer har under de senaste åren utsatts för cyberattacker med stora konsekvenser som följd. Exempelvis har skyddsvärd information förlorats eller röjts till obehöriga eller den bristande hanteringen lett att organisationer drabbats av ekonomisk skada eller förtroendeskada. Inledningsvis 2024 utsattes en större leverantör av serverdrift och molntjänster för en ransomware-attack vilken fått en allvarlig påverkan på ett stort antal statliga myndigheters, kommuners och regioners tillgång till sina informationssystem.

Inom ramen för det kommunala åtagandet finns en rad samhällsviktiga och kritiska funktioner, vilka om de inte fungerar kan leda till skada för såväl enskilda individer som samhället i stort. Det är därför av största vikt att det bedrivs ett systematiskt informationssäkerhetsarbete för att undvika allvarlig påverkan på verksamheten och samhället i stort.

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. Det är således väsentligt att kommunen bedriver ett systematiskt och riskbaserat informationssäkerhetsarbete. Med anledning av ovanstående drar kommunens revisorer slutsatsen i sin riskanalys, att informationssäkerhetsarbetet behöver granskas.

2.1 Syfte och revisionsfrågor

Granskningen har syftat till att bedöma om kommunstyrelsen tillsett att ett systematiskt informations- och IT-säkerhetsarbete bedrivs.

Granskningen har besvarat följande revisionsfrågor:

- Finns aktuella styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas?
- Finns en ändamålsenlig organisation för informationssäkerhetsarbetet?
- Finns en tydliggjord ansvarsfördelning mellan kommunens funktioner och de funktioner som tillhandahålls genom avtalssamverkan med Ulricehamns kommun inom it?
- Finns etablerade samverkansforum och en struktur för dialog utifrån det avtal som tecknats?
- Har avtalssamverkan med Ulricehamns kommun följts upp avseende kommunens behov av support och stöd inom it till kommunens medarbetare och förtroendevalda?
- Har åtgärder vidtagits för att minska svarstiden avseende IT-stödet från Ulricehamns kommun?
- Finns beslutade informationssäkerhetsmål med tillhörande handlingsplaner?
- Finns det en tillräcklig säkerhetskultur hos kommunens medarbetare?
- Har säkerhetsåtgärder vidtagits som ett resultat av riskbedömningar?
- Sker en uppföljning att avtalade leverantörer avseende extern drift av it-system vidtar de säkerhetsåtgärder som det har bedömts finnas behov av?
- Finns en tillräcklig förmåga att upptäcka och hantera kritiska it-säkerhetshändelser?
- Finns en tydliggjord struktur för ansvar vid kritiska händelser och hur information ska eskaleras mellan Ulricehamns kommuns it-funktion och kommunen?
- Genomförs uppföljning av kommunens informations- och IT-säkerhetsarbete som inkluderar sektionernas efterlevnad av interna styrdokument och lagkrav inom informationssäkerhet?

2.2 Revisionskriterier

Granskningen har utgått från nedanstående revisionskriterier:

- Kommunallagen 6 kap. 6 §
- Tillämpbara interna regelverk, policys och beslut
- Myndigheten för samhällsskydd och beredskaps (MSB) 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 Avgränsning

Granskningen har inriktats till kommunstyrelsens övergripande ansvar för styrning och uppföljning av informations- och IT-säkerhet men även det operativa arbetet för att säkerställa ett systematiskt informationssäkerhetsarbete. Granskningen har därtill inkluderat avtalssamverkan med it-funktion i Ulricehamns kommun.

Avgränsningen har omfattat organisatorisk säkerhet, personalsäkerhet och teknisk säkerhet. Fysisk säkerhet har inte ingått i granskningen.

Granskningen har omfattat år 2024.

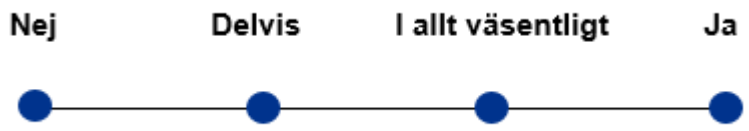
2.4 Metod

Granskningen har genomförts genom dokumentstudier och intervjuer med kommunstyrelsens presidium, kommunchef, IT-chef, IT-säkerhetsansvarig, informationssäkerhetssamordnare, sektionschef och informations-säkerhetshandläggare för samhällssektionen respektive omsorgssektionen.

Dokumentstudier har gjorts av:

- Informationssäkerhetspolicy
- Riktlinjer för informationssäkerhet
- Rutiner för incidenthantering
- Riktlinjer och avtal för avtalssamverkan avseende IT-verksamhet
- Ledningens genomgång av informationssäkerhetsarbetet

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



Rapporten har faktakontrollerats av it-chef, it-säkerhetsansvarig och informationssäkerhetssamordnare.

3 Resultat

3.1 Styrande dokument och mål

Iakttagelser

Vi har i granskningen tagit del av styrande dokument inom informationssäkerhet.

Kommunen har en beslutad policy för informationssäkerhet och dataskydd[1] som beskriver kommunens viljeriktning, mål samt roller och ansvar för informationssäkerhetsarbetet. Policyn har antagits av kommunfullmäktige. Enligt policyn är det övergripande målet att upprätthålla rätt nivå på skydd för informationstillgångarna. All verksamhet i kommunen omfattas av policyn.

Av policyn framgår kommunens tre strategiska mål för informationssäkerheten:

- Att personal har rätt kunskap för att hantera informationstillgångar korrekt
- Att verksamheterna genomför informationsklassningar enligt kommunens gemensamma klassningsmodell
- Att dokumenterade systemförvaltningsplaner ska upprättas i enlighet med systemförvaltarmodellen och utgöra grundläggande dokumentation för informationssäkerhetsarbetet

Policyn kompletteras av ”Riktlinjer för informationssäkerhet och dataskydd”[2], som konkretiserar hur informationssäkerhetsarbetet ska gå till. Här framgår att arbetet ska följa standarden ISO/IEC 27000 och att ett ledningssystem med avstamp i standarden ska införas. Riktlinjen beskriver vidare olika delmomenten som utgör grunden i ett systematiskt informationssäkerhetsarbete.

I riktlinjen konkretiseras de strategiska målen av ett antal långsiktiga respektive kortsiktiga delmål.

I en årlig rapport som kallas ”Ledningens genomgång[3]”, som är en sammanställning över nuläge och prioriterad inriktning för informationssäkerhetsarbetet, redovisas uppföljning och ytterligare konkreta delmål.
Vi har dock inte tagit del av några formella handlingsplaner som visar aktiviteter i syfte att uppnå fastställda mål.

Vidare framgår inte något datum avseende när rapporten har upprättats.

Rapporten ”Ledningens genomgång” innehåller en GAP-analys över nivån avseende kommunens informationssäkerhet i förhållande till önskat läge.

[1] Kommunfullmäktige, 2021-02-08
[2] Kommunstyrelsen, 2020-12-21 §244
[3] Rapport till kommunstyrelsen, ej daterad. Läs mer om Ledningens genomgång i rapportavsnitt 3.7

Av rapporten framgår att kommunen inte har ett systematiskt informations-säkerhetsarbete, men att utveckling skett sedan 2022.

Av rapporten framgår vidare att förbättring har skett inom samtliga områden, att grunden till ett ledningssystem är satt, men att det ännu saknas vissa rutindokument.

Vidare redovisas att arbete med väsentliga aktiviteter som informationsklassningar och riskanalyser behöver förbättras, liksom kunskap och utbildning av personal.

I intervjuer uttrycks att kommunen arbetat målmedvetet med informationssäkerhet senaste åren och skapat ett ledningssystem som omfattar både informationssäkerhet och dataskydd. På kommunens intranät finns en samlingsplats för styrande dokument och annat stödmaterial som avser frågorna. Den största utmaningen utrycks emellertid vara att skapa en levande informations-säkerhetskultur inom hela kommunen.

3.1.1 Bedömning

Vi bedömer att kommunstyrelsen vid tid för granskningen har tillsett att det finns aktuella kommunövergripande styrdokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas.

De övergripande styrdokumenten utgör en sammanhållen helhet för styrning av informationssäkerhetsarbetet vilket inkluderar både organisatorisk säkerhet och teknisk säkerhet. De styrande dokumenten inkluderar även en dokumenterad och tydlig ansvarsfördelning.

Dokumenten ger en grund och är en förutsättning för ett systematiskt informations-säkerhetsarbete. Arbetet kan emellertid inte betraktas som fullt ut systematiskt i nuläget.

Vi bedömer att det finns beslutade informationssäkerhetsmål, men att tillhörande handlingsplaner saknas.

Strategiska mål anges i kommunens informationssäkerhetspolicy och dessa konkretiseras på kort sikt i riktlinjen för informationssäkerhet.

Avsaknad av formella handlingsplaner är en brist såtillvida att sådana planer utgör grund för en strukturerad och tydlig genomförande och uppföljning.

3.2 Organisation

Iakttagelser

Ovan beskrivna policy och riktlinje beskriver ansvarsfördelning för informationssäkerhetsarbetet både på politisk nivå och för förvaltningen.

Kommunfullmäktige är ytterst ansvarig för informationssäkerhetsarbetet. Kommunstyrelsen ansvarar för samordning av informationssäkerhetsarbetet och för att upprätta riktlinjer för arbetet och tillse att styrande dokument efterlevs.

Kommunchef ansvarar för att informationssäkerhetsarbetet bedrivs i enlighet med styrande dokument.

Nämnderna är ytterst ansvariga för informationssäkerheten inom sina respektive verksamhetsområden då ansvaret för informationssäkerhet följer ordinarie verksamhetsansvar.
Ansvariga chefer och vd:ar för kommunala bolag ansvarar därigenom för att den information som hanteras inom respektive verksamhet uppfyller krav på informationssäkerhet. Därutöver ska varje sektion utse lokala informations-säkerhetshandläggare som ska genomföra operativa arbetsuppgifter avseende informationssäkerhet inom respektive sektion. Handläggarna ingår i ett kommunövergripande nätverk för frågorna.

Informationssäkerhetssamordnaren är en av flera nyckelfunktioner i arbetet och har i uppgift att leda och samordna arbetet på kommunövergripande nivå. Samordnaren är även sammankallande för den Informationssäkerhetsgrupp som ”Riktlinje för informationssäkerhet” fastställt ska finnas. I gruppen samordnas och följs kommunens informationssäkerhetsarbete upp. Gruppen ska även rapportera till IT-styrgruppen, vilken vi redogör för senare i detta avsnitt.

Andra nyckelroller som beskrivs i riktlinjerna är säkerhetschef, it-chef och it-säkerhetsansvarig. Dessa funktioner har ansvarsområden som är väsentliga för kommunens säkerhet, informationssäkerhet samt it-säkerhet där ansvaret för respektive funktion regleras av styrande dokument.

Intervjuade ger samstämmiga uppgifter om att det finns en tydlig ansvarsfördelning och bra styrning av informationssäkerhetsarbetet som även tillämpas i arbetet. En viktig förklaring anges vara att det finns ett aktivt, etablerat verksamhetsnära arbete där sektionernas informationssäkerhetshandläggare är drivande.
Rollen som informationssäkerhetshandläggare är ett uppdrag vid sidan om andra uppgifter och den tid som kan avsättas för informationssäkerhetsarbetet varierar.

Arbetet förefaller ha kommit olika långt i sektionerna men det uttrycks att det bedrivs i enlighet med fastställd struktur i ledningssystemet. Informationssäkerhetssamordnaren leder det övergripande arbetet medan samordning sker genom regelbundna avstämningar med informationssäkerhetshandläggarna som utför sektionens operativa arbete.

Gällande kommunens IT-verksamhet är den sedan 2022 organiserad genom avtalssamverkan med Ulricehamns kommun. Kommunerna har varsin informationssäkerhetssamordnare men en gemensam it-avdelning där kontor finns i båda kommunerna.
Syfte, uppdrag och omfattning på avtalssamverkan regleras i riktlinjer för ramuppdrag

it[4] samt framgår även av dokumentet Samverkansorganisation IT och digitalisering[5] och Samverkansavtal IT[6].

Av dokumenten framgår att IT-chef leder IT-avdelningen som är organiserad i fyra verksamhetsbaserade forum:

- IT-forum drift (operativ IT-drift),
- IT-forum utveckling (samordnar utvecklingsfrågor),
- informationssäkerhetsgruppen (informationssäkerhetsfrågor) samt
- tjänstefieringsgruppen (förvaltar avtalssamverkans gemensamma kostnadsmodell).

Därtill finns IT-styrgruppen som är beslutande forum på förvaltningsnivå där beslut av större strategisk karaktär fattas. IT-styrgruppen består av kommunchefer och utvecklingscherfer, IT-chef samt IT-strateg.
Riktlinjer för ramuppdrag it specificerar vilka funktioner som ska finnas inom respektive forum. Detaljerade uppdragsbeskrivningar för IT-chef, IT-strateg och E-samordnare framgår av, ovan nämnt dokument, Samverkansorganisation IT och digitalisering.

Genom intervjuer beskrivs att tanken med de olika forumen är att de ska användas som kanaler för utvecklings- och förbättringsbehov som identifieras av respektive kommun. Enligt uppgift fungerar forumen enligt avsett syfte såtillvida att det finns etablerad dialog där kommunerna löpande är involverade samt att avtal och riktlinjer ses över årligen inom ramen för samverkan.

3.2.1 Bedömning

Vi bedömer att det vid tid för granskningen i allt väsentligt finns en ändamålsenlig organisation för informationssäkerhetsarbetet.

Den ansvarsfördelning som beskrivs i styrande dokument är etablerad. I enlighet med MSB:s rekommendationer har kommunen en utsedd informationssäkerhetssamordnare som leder samordnar och följer upp arbetet. Vi kan konstatera att det finns rutiner för samordning mellan nyckelfunktioner med ansvar inom säkerhetsarbetet, informationssäkerhetsarbetet och it-säkerhetsarbetet vilket även är reglerat i policy och riktlinjer.

Vi konstaterar att samtliga sektioner har utsedda representanter som kan bidra i det operativa informationssäkerhetsarbetet inom respektive verksamhet. Kommunen har vidare etablerat en kommunövergripande samordning genom nätverk för utsedda representanter vilket ger goda förutsättningar till både kompetenshöjande insatser, och att gemensamma arbetssätt och metoder kan etableras och genomföras på likartat sätt i kommunens samtliga verksamheter.

[4] Kommunstyrelsen 2024-01-11
[5] IT-styrgruppen 2023-12-08
[6] IT-styrgruppen 2023-12-08

Vi bedömer att det finns en tydliggjord ansvarsfördelning mellan kommunens funktioner och de funktioner som tillhandahålls genom avtalssamverkan.

Ansvarsfördelning både för kommunens interna funktioner och funktioner som tillhandahålls genom avtalssamverkan framgår tydligt genom de underlag som reglerar avtalssamverkan samt arbetet med informationssäkerhet.

Vi bedömer även att det finns etablerade samverkansforum och en struktur för dialog.

3.3 IT-Support och stöd

Iakttagelser

Riktlinjen för ramuppdrag IT innehåller en detaljerad kravställning av IT-avdelningens verksamhet och leverans. Vi har granskat hur riktlinjerna för år 2022, 2023 och 2024 har reviderats utifrån utvecklingsbehov från samverkanskommunerna. Här framgår att avtalet utvecklats med avseende på ansvarsfördelning mellan IT och verksamheten i specifika supportärenden till enskilda användare, samt beträffande support avseende verksamhetssystem.

Riktlinjen förtydligar även avtalssamverkans organisation för IT-support och stöd. Stödfunktionerna är indelade i tre olika supportlinjer som baseras på aktuell problemställning.

Generell användarsupport ges av IT-koordinatorer och supportspecialister. Ärenden som kräver utökad support hanteras av IT-tekniker. För användarärenden och felavhjälpning kopplade till system och it-infrastruktur, som kräver mer fördjupad expertis, finns IT-tekniker, e-samordnare och verksamhetsutvecklare.

Riktlinjen redogör för en krav- och funktionsbeskrivning för IT-support och stöd. Enligt denna är målsättningen att minst hälften av alla supportärenden ska lösas genom första linjens support. Vid intervju förevisas en plattform med lathundar och självhjälpsguider på kommunens intranät. Plattformen har skapats av IT-avdelningen och uppges ha styrt om en stor andel supportärenden från telefon till e-post, vilka är ingångarna för användare som behöver personlig support.

Öppettider för telefonsupporten anges i ”Riktlinjen för ramuppdrag IT”. Utgångspunkt är att ”vanliga” it-problem ska lösas inom en arbetsdag samt följas upp per tertial. Därtill ska kvaliteten på IT-supporten följas upp genom att en nöjdhetsenkät skickas till var fjärde ägare av ett IT-ärende. Uppföljning görs tertialvis av ett team för stöd- och supportfrågor som är organiserat inom IT-forum drift.

Resultat för tertial 1 och 2 (januari-augusti 2024), enligt erhållet enkätunderlag, visar att 96 procent av 337 respondenter (motsvarande 322 respondenter) svarat ”ja” på frågan ”*Anser du att IT löste ditt ärende/problem tillfredsställande?*”.

Vidare uppger intervjuade att IT-avdelningen tidigare mätte svarstider, men att det inte längre görs då mätningarna ansågs överflödiga.

På begäran från oss har IT-avdelningen tagit fram aktuell data för svarstider och samtalsfrekvens under årets två första kvartal (januari-mars samt april-juni 2024). Dataanalys visar att telefonsupporten mottog 3 849 samtal under hela mätperioden[7]. 53 procent av dessa, motsvarande 2 049 samtal, besvarades inom 0-10 sekunder. 84 procent av samtalen hade en väntetid på 60 sekunder eller mindre.

3.3.1 Bedömning

Vi bedömer att avtalssamverkan följts upp avseende Tranemo kommuns behov av IT-support och stöd till medarbetare och förtroendevalda.

Krav på uppföljning av behov av support och stöd är formaliserat i riktlinjen och genomförs i enlighet med den. Därtill finns etablerade kanaler i form av de olika IT-forumen för identifierade utvecklingsbehov som identifieras av kommunen.

Vi bedömer att åtgärder vidtagits för att minska svarstiden avseende IT-stöd.

Erhållen data visar att svarstider för supportärenden är god, vilket också resultatet av nöjdhetsenkäten kan tolkas indikera.

3.4 Säkerhetskultur

Iakttagelser

Både informationssäkerhetspolicyn och riktlinjen för informationssäkerhet redovisar mål som avser att anställda ska ha ett högt riskmedvetande och kunskap om erforderliga styrdokument och regelverk. Riktlinjen anger även att informationssäkerhetsarbetet ska vara välkommunicerat inom kommunen och att anställda ska ha en god säkerhets-medvetenhet genom utbildning och information.

Målen konkretiseras i ”Ledningens genomgång” för 2024 som redovisar delmålet att 75 procent av personalen ska ha genomgått utbildning.

Vi har tagit del av uppföljningsunderlag[8] för deltagande i e-learningutbildningar per 2023-11-16. Underlaget visar uppföljning av hur många anställda som påbörjat, slutfört och inte påbörjat utbildningar per sektion. På aggregerad nivå framgår att 29 procent av kommunens anställda avklarat utbildningen vid uppföljningsdatumet. 66 procent hade inte påbörjat utbildningen.
Behovet av fortsatta utbildningsinsatser konstateras härvid i underlaget som redogör för ”Ledningens genomgång”.

[7] Samtalsvolym avser supportärenden från användare i både Tranemos och Ulricehamns kommuner.
[8] Presentationsmaterial till kommunledningen.

Enligt intervjuade tillhandahålls utbildning i form av e-learningutbildningar till alla anställda samt genom muntliga informationstillfällen där informationssäkerhets-samordnare och de verksamhetsnära informationssäkerhetshandläggarna besöker chefsmöten och arbetsplatsträffar, så kallade APT. Detta bekräftas av intervjuade informationssäkerhetshandläggare som ger bild av ett strukturerat upplägg där handläggarna återkommande deltar på chefsmötena och APT:ar för att utbilda och finnas till hands för att besvara frågor. Vård- och omsorgssektionen har tagit fram en verksamhetsanpassad informationssäkerhetsutbildning då den kommungemensamma ansågs för generell.

I intervjuer framförs att kunskap och säkert användarbeteende är högprioriterade områden i syfte att etablera en aktiv informationssäkerhetskultur i kommunen. Att uppnå ett säkert användarbeteende konstateras vara utmanande då säkerhets-medvetenheten skiljer sig åt bland medarbetarna, delvis beroende på typ av arbetsuppgifter och datorvana.

3.4.1 Bedömning

Vi bedömer att det delvis finns en tillräcklig säkerhetskultur hos kommunens medarbetare.

Det har genomförts ett flertal aktiviteter för att kommunens medarbetare och förtroendevalda ska få kunskap om informationssäkerhet och medvetenhet om risker inom området. Det finns även ett aktivt, verksamhetsnära utbildningsarbete som är kontinuerligt.

Sektionsbaserad uppföljning av genomförda utbildningar ger möjlighet till behovsstyrda utbildningsinsatser och att kunna säkerställa att samtliga anställda genomför utbildningarna.

Vi ser dock att andelen personal som genomfört utbildningen är låg, varvid vi delar uppfattningen att det föreligger behov av fortsatta utbildningsinsatser.

Vi bedömer att riktade utbildningsinsatser även bör inkludera förtroendevalda.

Dessa är användare av kommunens IT-miljö och bör därför omfattas av samma utbildningsinsatser som anställda.

3.5 Riskanalys och informationsklassning

Iakttagelser

Enligt MSB:s metodstöd för systematiskt informationssäkerhetsarbete är informationsklassning en förutsättning för att skapa rätt skydd för informationen som hanteras i respektive verksamhet. Med en gemensam klassningsmodell kan organisationens informationstillgångar skyddas utifrån interna och externa krav på informationens konfidentialitet, riktighet och tillgänglighet.

Detta krav ställs även i kommunens informationssäkerhetspolicy. Kommunen har fastställt i riktlinjer att metod för informationsklassning ska vara KLASSA, som tillhandahålls av SKR. Enligt riktlinjen ska information klassas i enlighet med modellen och krav på säkerhetsåtgärder kopplas till de olika nivåerna i klassningsmodellen.

Av rapporten ”Ledningens genomgång” framgår att arbetet med klassningar har förbättrats, men att arbete fortfarande kvarstår innan det kan betraktas som systematiskt.

Av intervjuade uppfattar vi att det finns ett etablerat arbetssätt där kommunens informationssäkerhetssamordnare leder klassningar med stöd av berörd informationssäkerhetshandläggare. IT-säkerhetsansvarig deltar vid de flesta klassningar, alternativt erhåller dokumentation efter klassning. Vi har även tagit del av underlag från klassningar som verifierar metod och genomförande av klassningar.

Utifrån resultatet av klassningar upprättas handlingsplaner, som vi har tagit del av, där säkerhetsnivåer och behov av it-säkerhetsåtgärder framgår.

De intervjuade beskriver en process där klassning av ett system ska genomföras vartannat år. Brister som identifieras i samband med klassning ska återrapporteras till informationssäkerhetssamordnaren tillsammans med åtgärdsförslag inom sex månader. Återrapporteringen utgör underlag för beslut om riskacceptans.

De informationssäkerhetshandläggare som vi intervjuat uppger att redovisad process tillämpas där även återklassning sker efter två år. Enligt samtliga intervjuade har klassningar gjorts för samtliga system som identifierats som verksamhetskritiska. Det har även gjorts klassningar av en stor andel av kommunens andra system och applikationer.

Däremot konstateras att det inte görs någon uppföljning att leverantörer som står för extern drift av it-system vidtar erforderliga säkerhetsåtgärder. Detta beskrivs vara en konsekvens av resursbrist.

3.5.1 Bedömning

Vi bedömer att säkerhetsåtgärder delvis vidtagits som ett resultat av riskbedömningar.

Kommunen har beslutat om en modell för informationsklassning och arbetet har påbörjats men ännu inte nått en tillräcklig systematik. Vi konstaterar att det är en prioriterad aktivitet och samtliga verksamheter har fått stöd under de senaste åren för att genomföra klassningar. Det ingår även som prioriterad aktivitet, enligt rapporten ”Ledningens genomgång”. Vi ser positivt på att de mest kritiska systemen har klassats, liksom att det finns en tydlig process som också innefattar upprättande av handlingsplaner.

Vi bedömer att det inte sker någon uppföljning att avtalade leverantörer som står för extern drift av it-system, vidtar säkerhetsåtgärder som det har bedömts finnas behov av.

Att uppföljning av leverantörer avseende extern drift av it-system sker, är en viktig åtgärd i syfte att säkerställa att informationstillgångar som förvaltas av externa leverantörer har adekvat skydd.

3.6 Hantering av kritiska IT-säkerhetshändelser

Iakttagelser

Riktlinjen för informationssäkerhet innehåller två mål med bäring på hantering av kritiska IT-säkerhetshändelser:

- Dels ska kommunen ha en kontinuitetsplanering för tillgång till information och funktioner som är nödvändiga för att kunna upprätthålla verksamheten.
- Dels ska det finnas en process för incidenthantering.

Att ha ett förebyggande förhållningssätt och förmåga att kunna hantera incidenter och störningar är, enligt riktlinjen, en utpekad princip för arbetet.

Riktlinjer för ramuppdrag IT 2024 reglerar tillgänglighet till IT-beredskap. Här framgår att IT-beredskap ska finnas tider då IT-supporten inte är tillgänglig och för akuta ärenden som inte kan anstå. Kostnader för beredskapsärenden faktureras till berörd verksamhet.

I intervju framförs att medarbetare från IT-avdelningen rullar på ett löpande beredskapsschema och att det finns en informell eskaleringsväg där IT-tekniker i beredskap i ett första steg försöker avhjälpa problemet och sedan vid behov, eskalerar ärendet till IT-chef.

Utöver de bägge riktlinjerna finns en incidenthanteringsrutin[9] som beskriver roller och processflöde för it-säkerhets-, informationssäkerhets- och personuppgiftsincidenter. Dokumentet åskådliggör hur incidenter anmäls och att de ska följas upp inom berörd verksamhet.

Vid sidan av IT-beredskapen uppger intervjuade att kommunens TIB (tjänsteperson i beredskap) alltid kontaktas vid IT-händelser under jourtid. Utifrån olika händelse-baserade scenarios finns dokumenterade eskaleringsvägar där TIB fungerar som en samordnande kontakt.

Vi har tagit del av muntliga beskrivningar som ger en helhetsbild av kommunens förmåga att hantera och upptäcka kritiska it-säkerhetshändelser. Med hänsyn till att detaljerade redogörelser av dessa kan exponera kommunen för säkerhetshot väljer vi att beskriva bilden översiktligt.
Kommunen har flera väsentliga säkerhetsfunktioner som både ger möjlighet att upptäcka hot och som skyddar mot intrångsförsök, samt verktyg för löpande

[9] Ej daterad

säkerhetskontroller och sårbarhetsscanningar. Det finns även redundanta lösningar som ger kontinuitetsmässig robusthet.

Våra samlade iakttagelser av den information vi tagit del av är att dessa har etablerats utifrån en prioritering och i förhållande till de krav som ställs i policyn avseende ISO-standard för informationssäkerhet och säkerhetsåtgärder. Vi kan även konstatera att nuvarande säkerhetsåtgärder är överensstämmande med åtgärder som MSB rekommenderar för stärkt cyberförsvar. Däremot saknas aktiv övervakning av it-miljön under såväl kontorstid som annan tid.

3.6.1 Bedömning

Vi bedömer att det delvis finns en tillräcklig förmåga att upptäcka och hantera kritiska säkerhetshändelser.

Ett systematiskt arbete med informationsklassningar är en grund för att visa om det finns behov av ytterligare tekniska säkerhetsåtgärder. I nuläget har inte klassningar och riskanalyser genomförts i tillräcklig omfattning för att ge ett fullständigt underlag att utgå från även om arbetet har genomförts för en stor del av informationstillgångarna.

IT-beredskap ger förutsättningar att hantera kritiska incidenter som uppstår utanför ordinarie kontorstid. Dock är det en sårbarhet att det inte finns någon teknisk övervakning av it-infrastrukturen, vilket riskerar leda till att intrångsförsök och andra hot inte upptäcks i tillräcklig tid för att kunna avvärjas.

Vi bedömer att det finns en tydliggjord struktur för ansvar vid kritiska händelser och hur information ska eskaleras mellan IT-avdelningen och kommunen.

Roller och eskaleringsvägar befästs i styrande dokument och vi gör bedömningen att dessa i praktiken fungerar i enlighet med dessa beskrivningar.

3.7 Uppföljning

Iakttagelser

Enligt MSB:s metodstöd för systematiskt informationssäkerhetsarbete ska ledningen hållas informerad om informationssäkerhetsarbetets status och därmed kunna besluta om åtgärder utifrån föreslagna förbättringsområden.

Enligt informationssäkerhetspolicyn ska efterlevnaden av denna och underliggande styrdokument regelbundet följas upp. Riktlinjerna anger att informationssäkerhet ska vara en ordinarie del av verksamhetsuppföljningen, samt följas upp centralt och inom nämnder och bolag. Informationssäkerhetssamordnare ska därtill löpande rapportera status gällande informationssäkerhet till kommunstyrelsen och kommunchef.

Av granskningen framkommer att informationssäkerhetssamordnaren, i enlighet med uppdrag och ansvar, årligen följer upp och rapporterar om det samlade informations-

säkerhetsarbetet. Detta sammanställs i en rapport som kallas ”Ledningens genomgång”.

Vi har tagit del av ”Ledningens genomgång” avseende genomfört arbete under 2023 samt plan för följande år. Av dokumentet framgår inte när i tid rapporten har upprättats.

Prioritering konstateras ligga på att kommunstyrelsen, ledningen och medarbetarna ska utbildas i informationssäkerhet. Ytterligare prioritet är att förbereda organisationen på införandet av NIS2-direktivet samt fortsatt implementering av ledningssystemet för informationssäkerhet. Som tidigare nämnts innehåller rapporten även en GAP-analys över kommunens nuläge i förhållande till ett systematiskt informationssäkerhetsarbete.

Enligt muntliga uppgifter presenteras rapporten ”Ledningens genomgång” årligen för kommunstyrelsen under årets första kvartal. Att så skedde under 2024 har inte gått att styrka genom protokollsgranskning.

Däremot kan vi verifiera att informationssäkerhetssamordnaren rapporterade aktuell status för informationssäkerhetsarbetet på kommunstyrelsens sammanträde 2024-08-29[10].

3.7.1 Bedömning

Vi bedömer att det vid tid för granskningen sker en uppföljning av informations- och it-säkerhetsarbetet.

Enligt muntlig uppgift presenteras rapporten för kommunstyrelsen årligen under årets första kvartal. Dock har detta **inte** kunnat verifierats genom protokollsgranskning.

Det är centralt att rapporteringar och uppföljningar upptas i kommunstyrelsens protokoll och att det finns en spårbarhet att ansvarig nämnd, dvs. kommunstyrelsen har tagit del av aktuell uppföljningsrapport.

Vidare ska beslut om eventuella åtgärder och insatser med anledning av uppföljningens resultat upptas och dokumenteras i protokollen.

Det saknas vidare datum för upprättande av dokumentet. Det är en grundläggande utgångspunkt att handlingar som skapas inom kommunstyrelsen förses med datum för upprättande.

Vi noterar att uppföljningen är samlad, dokumenterad och innehåller analys och identifierade förbättringsområden, där implementering av NIS2-direktivet är en prioritering.

Uppföljningen inkluderar emellertid **inte** respektive sektions efterlevnad av interna styrdokument och lagkrav inom informationssäkerhet.

[10] Sammanträdesprotokoll kommunstyrelsen §144, daterat 2024-08-29

4 Samlad bedömning och rekommendationer

Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsen vid tid för granskningen delvis tillsett att ett systematiskt informations- och IT-säkerhetsarbete bedrivs.

Vi kan konstatera att det finns ett ledningssystem för informationssäkerhet med styrande dokument som tydliggör ansvar och roller och krav på det operativa informationssäkerhetsarbetet. I nuläget finns en etablerad organisation och tydliggjorda processer för aktiviteter samt uppföljning mot kommunstyrelsen. Genom detta anser vi att kommunstyrelsen skapat förutsättningar för att etablera ett systematiskt informationssäkerhetsarbete inom kommunen.

Det operativa arbete som utförs i dagsläget motsvarar däremot inte en omfattning som kan betraktas som systematisk i vissa väsentliga avseenden, där vi bedömer att det delvis finns en tillräcklig förmåga att upptäcka och hantera kritiska säkerhetshändelser. Det gäller framför allt arbetet med informationsklassningar som är i en utvecklingsfas liksom insatser för att stärka säkerhetskulturen där arbete pågår för att förbättra dessa processer.

Ett systematiskt arbete med informationsklassningar är en grund för att visa om det finns behov av ytterligare tekniska säkerhetsåtgärder. I nuläget har inte klassningar och riskanalyser genomförts i tillräcklig omfattning för att ge ett fullständigt underlag att utgå från även om arbetet har genomförts för en stor del av informationstillgångarna.

IT-beredskap ger förutsättningar att hantera kritiska incidenter som uppstår utanför ordinarie kontorstid. Dock är det en sårbarhet att det inte finns någon teknisk övervakning av it-infrastrukturen, vilket riskerar leda till att intrångsförsök och andra hot inte upptäcks i tillräcklig tid för att kunna avvärjas.

Gällande avtalssamverkan inom IT-verksamheten och behovet av IT-stöd och support finns en tydliggjord ansvarsfördelning och strukturerade samverkansforum där löpande uppföljning av avtalssamverkan görs.

Vad avser att säkerhetsåtgärder har vidtagits som ett resultat av riskbedömningar, bedömer vi att det har skett delvis.

I syfte att säkerställa att informationssäkerhetsarbetet utvecklas och etableras i enlighet med styrande dokument och de lagkrav som verksamheter har att följa, är det väsentligt att kommunstyrelsen säkerställer en tillräcklig intern kontroll över arbetet.

Utifrån genomförd granskning rekommenderar vi kommunstyrelsen att:

- Upprätta handlingsplaner för beslutade informationssäkerhetsmål
- Tillse att informationssäkerhetsutbildning genomförs i högre grad inom samtliga verksamheter.
- Tillse att riktade utbildningsinsatser i informationssäkerhet genomförs för förtroendevalda

- Fortsätta verka för att arbete med informationsklassningar systematiseras ytterligare
- Tillse att sektionernas efterlevnad inkluderas i den årliga uppföljningen.
- Redogörelser, rapporteringar och uppföljningar som upptas vid kommunstyrelsens sammanträden dokumenteras i protokollen.
- Säkerställa att handlingar som skapas inom kommunstyrelsen förses med datum för upprättande.
- Tillse att uppföljning sker av att avtalade leverantörer som står för extern drift av it-system vidtar adekvata it-säkerhetsåtgärder i syfte att skydda kommunens informationstillgångar

Dag som ovan
KPMG AB

Jenny Thörn
Verksamhetsrevisor/Specialist

Sofie Ernerudh
Verksamhetsrevisor

Viktoria Bernstam
Kundansvarig
Certifierad kommunal yrkesrevisor