Granskning av informations- och it-säkerhet

Rapport

Alingsås kommun

Jenny Thörn
Viktoria Bernstam

KPMG AB

2023-12-14

Antal sidor 19

Alingsås kommun
Granskning av informations- och it-säkerhet

2023-12-14

Innehållsförteckning

1 Sammanfattning

KPMG har av Alingsås kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunens arbete för att upprätthålla en god informations- och it-säkerhet.

Granskningen har syftat till att bedöma om kommunstyrelse och nämnder bedriver ett systematiskt informationssäkerhetsarbete.

Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsen vid tid för granskningen bedriver ett systematiskt informationssäkerhetsarbete men att nämndernas arbete är i behov av utveckling för att vara systematiskt i enlighet med beslutade styrdokument.

Vi baserar vår bedömning på att kommunstyrelsen i sitt övergripande ledningsansvar har etablerat styrande dokument och en ändamålsenlig organisation för informationssäkerhetsarbetet. Vi bedömer därigenom att strukturen för ett systematiskt och riskbaserat informationssäkerhetsarbete finns. Arbetet är i en etableringsfas och vi ser därför att arbetssätt och metoder ännu inte fullt är etablerade inom respektive nämnds arbete.

Det pågår ett flertal väsentliga aktiviteter i enlighet med beslutade styrdokument men vi bedömer att arbetet inte i nuläget når upp till den systematik som interna styrdokument ställer. Bland annat är arbetet med informationsklassning och riskbedömning i behov av att genomföras mer kontinuerligt och genomförandegraden för informationssäkerhetsutbildning höjas för att medarbetare och förtroendevalda ska ha kunskap om informationssäkerhet och i högre grad vara medvetna om hot och risker inom området.

Kommunstyrelsen har fastställt former för uppföljning och tillsett att de regelbundet erhåller information om det arbete som genomförs tillsammans med åtgärder för att stärka informations- och it-säkerheten. Vi uppfattar genom detta att kommunstyrelsen och ansvariga nyckelfunktioner är väl medvetna om kommunens nuläge och det finns en dokumenterad planering för att arbetet ska utvecklas kontinuerligt för att nå de av kommunfullmäktige beslutade målen för informationssäkerhet.

Vi rekommenderar kommunstyrelsen att:

- Revidera och aktualisera informationssäkerhetspolicyn mot bakgrund av att den kan riskera att vara föråldrad i förhållande till nuvarande hot, risker och krav.
- Tillse att informationssäkerhetsutbildning genomförs i högre grad inom samtliga verksamheter.
- Tillse att egna informationstillgångar klassas och riskbedöms samt följa upp att samtliga kommunens verksamhetskritiska system samt system som hanterar skyddsvärd information och personuppgifter har en aktuell klassning och riskbedömning.

- Följa upp att säkerhetsåtgärder vidtagits som informationsklassning och riskbedömning visat behov av.
- Säkerställa att kommunövergripande incidenthanteringsrutiner upprättas och etableras.
- Anpassa och stärka uppföljningsmetoder och kontroll av efterlevnad av beslutade styrdokument inom informationssäkerhet i takt med att kommunens mognadsgrad i informationssäkerhetsarbetet ökar.

2 Bakgrund

KPMG har av Alingsås kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunens arbete 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 inte de system och digitala tjänster som nyttjas för informationshantering och lagring 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. Det är således väsentligt att kommunen har en tillräcklig intern styrning och kontroll av sitt it-säkerhetsarbete så att arbetet sker på ett ändamålsenligt sätt. Med anledning av ovanstående drar kommunens revisorer slutsatsen i sin riskanalys, att arbetet med informations- och it-säkerhet behöver granskas.

2.1 Syfte och revisionsfrågor

Granskningen har syftat till att bedöma om kommunstyrelse och nämnder bedriver ett systematiskt informationssäkerhetsarbete.

Granskningen avser att besvara följande revisionsfrågor:

- Finns aktuella styrande kommunövergripande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas?
- Finns en ändamålsenlig organisation för informationssäkerhetsarbetet?
- Finns beslutade informationssäkerhetsmål med tillhörande handlingsplaner?
- Har kommunstyrelsen inom ramen för sin uppsiktsplikt tillsett att det finns en tillräcklig säkerhetskultur inom nämnderna
    - Har det genomförts någon utvärdering av nämndernas säkerhetsarbete?
- Finns ett systematiskt arbete med riskanalyser och informationsklassning?

- Har tekniska säkerhetsåtgärder vidtagits som står i relation till aktuella hot och risker och utvärderas dessa regelbundet?
- Finns en etablerad övervakning för att upptäcka hot om intrång eller andra säkerhetsincidenter i it-miljön?
- Finns incidenthanteringsrutiner som inkluderar krav på hur incidenter ska dokumenteras och följas upp tillsammans med tydliggjorda eskaleringsvägar?
- Finns dokumenterade reserv- och återgångsrutiner vid allvarligare störningar och avbrott i it-system? Har dessa testats för att säkerställa att de fungerar ändamålsenligt?
- Finns en etablerad uppföljning av informations- och it-säkerhetsarbetet och rapporteras denna till styrelse och nämnder med regelbundenhet?
- Vilka säkerhetsåtgärder finns för molnlagring och efterlevs dessa?

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 omfattar kommunstyrelsens övergripande ansvar för informationssäkerhet och it-säkerhet.

2.4 Metod

Granskningen har genomförts genom dokumentstudier och intervjuer med kommunstyrelsens presidium, kommundirektör, IT-chef samt ansvarig IT-säkerhetssamordnare.

Dokumentstudier har gjorts av:

- Säkerhetspolicy
- Informationssäkerhetspolicy
- Riktlinjer för informationssäkerhet

- Handlingsplan för informationssäkerhet år 2022 och 2023
- Ledningens genomgång av informationssäkerhetsarbetet

Samtliga intervjupersoner har beretts möjlighet att faktakontrollera rapporten.

3 Resultat

3.1 Styrande dokument och mål

Iakttagelser

Vi har i granskningen tagit del av styrande dokument inom säkerhet och beredskap samt informationssäkerhet som beskrivs översiktligt i detta avsnitt.

Kommunen har en beslutad säkerhetspolicy[1] för säkerhets- och beredskapsarbetet där det framgår att informationssäkerhet är en del av arbetet. En informations-säkerhetspolicy[2] beskriver kommunens viljeriktning, mål och övergripande principer för informationssäkerhetsarbetet. Enligt informationssäkerhetspolicyn ska arbetet med informationssäkerhet vara systematiskt och bygga på den vedertagna standardserien ISO/IEC 27000 med strävan att ett ledningssystem för informationssäkerhet integreras i kommunens styrning.

All verksamhet i kommunen omfattas av policyn, inklusive bolag och förbund. Policyn kompletteras av Riktlinjer för informationssäkerhet i Alingsås kommun[3], vilken är indelad i fyra avsnitt:

1. Styrning av informationssäkerhet
2. Medarbetares ansvar för informationssäkerhet
3. Informationssäkerhet i verksamhet
4. Informationssäkerhet i it-miljön

Det pågår enligt uppgift ett arbete för att etablera ett ledningssystem för informationssäkerhet, LIS, vilket riktlinjerna är grunden för. Då det är ett omfattande arbete att få ett komplett LIS på plats så är uppfattningen att arbetet kommer att fortgå under de närmaste åren tills det är infört fullt ut.

Vi konstaterar att krav och reglering enligt riktlinjerna har hög ambitionsnivå på systematik och aktiviteter som ska genomföras. Intervjuade uppger att det finns en ambition att nå upp till de kontroller som valts ut och att arbetet för att nå dit konkretiseras genom den handlingsplan som årligen beslutas där aktiviteter prioriteras.

Vi har i granskningen tagit del av handlingsplaner för informationssäkerhets- och dataskyddsarbetet för åren 2022 samt 2023 och kan konstatera att planerna innehåller prioriterade åtgärder för att stärka informationssäkerheten inom ett antal områden, både organisatoriskt och även tekniskt. Det framgår av Handlingsplan för informationssäkerhet & dataskydd 2023[4] att den kompletterar

[1] Kommunfullmäktige, 2019-10-30, § 209
[2] Kommunfullmäktige, 2019-11-12, § 237.
[3] Kommunstyrelsen, 2020-12-07, § 192.
[4] Kommunstyrelsen, 2023-02-06

informationssäkerhetspolicyn och innehåller kortsiktiga mål med tillhörande aktiviteter för att uppnå fullmäktiges långsiktiga målsättningar. I rapporten lyfts delar av handlingsplanens innehåll i respektive avsnitt.

3.1.1 Kommentarer och bedömning

Vi bedömer att kommunstyrelsen vid tid för granskningen har tillsett att det finns aktuella styrande kommunövergripande dokument 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. Vi bedömer därtill att de styrande dokumenten inkluderar en dokumenterad och tydlig ansvarsfördelning.

Vi noterar att policyn inom kort är 5 år gammal och det kan därigenom finnas behov av att revidera denna. MSB rekommenderar att policydokument inom informations-säkerhet inte ska vara äldre än tre till fem år, detta mot bakgrund av att hot, risker och krav på arbetet är i snabb förändring och styrningen därigenom kan behöva uppdateras mer frekvent.

Vi bedömer att det finns beslutade informationssäkerhetsmål.

Långsiktiga mål anges i kommunens informationssäkerhetspolicy och dessa konkretiseras på kort sikt genom årliga handlingsplaner för informationssäkerhet och dataskydd vilka beslutas av kommunstyrelsen. Vi konstaterar vidare att mätningar genomförs för att säkerställa att arbetet utvecklas i enlighet med de beslutade målen.

3.2 Organisation

Iakttagelser

Policyn beskriver ansvarsfördelning för informationssäkerhetsarbetet både på politisk nivå och för förvaltningen. Kommunstyrelsen ansvarar för samordning av informationssäkerhetsarbetet och för att upprätta riktlinjer för arbetet och tillse att styrande dokument efterlevs. Kommundirektören har kommunstyrelsens uppdrag att tillse att arbetet bedrivs så effektivt som möjligt.

Nämnderna är ytterst ansvariga för informationssäkerheten inom sina respektive verksamhetsområden då ansvaret för informationssäkerhet följer ordinarie verksamhetsansvar. Ansvariga chefer ansvarar därigenom för att den information som hanteras inom respektive verksamhet uppfyller krav på informationssäkerhet. Inom nästan alla förvaltningar, bolag och förbund finns enligt uppgift utsedda funktioner som utför aktiviteter inom informationssäkerhet och även ingår i ett kommunövergripande nätverk för frågorna.

Några nyckelfunktioner i arbetet är säkerhetschef, informationssäkerhetssamordnare och it-säkerhetssamordnare. Dessa funktioner har det övergripande ansvaret för kommunens säkerhet, informationssäkerhet samt it-säkerhet där ansvaret för respektive funktion regleras av informationssäkerhetspolicyn.

Utöver dessa roller beskrivs ansvar för systemägare vilket vanligtvis utgörs av förvaltningschef samt systemförvaltare som enligt policyn, ska fungera som utförare åt systemägaren och se till att systemets funktionalitet samt planerade/beslutade aktiviteter genomförs och upprätthålls.

Enligt policyn finns ett informationssäkerhetsråd. I forumet sker den övergripande samordningen och uppföljningen av informationssäkerhetsarbetet. Informationssäkerhetssamordnaren är sammankallande för rådet som sammanträder regelbundet, ca fyra gånger per år. I rådet ingår representanter från kommunens verksamheter men även säkerhetschef och it-säkerhetssamordnare.

Intervjuade ger samstämmiga uppgifter om att det finns en tydlig ansvarsfördelning och bra styrning av informationssäkerhetsarbetet. Dels genom aktuella styrdokument, dels genom återrapportering av arbetet samt beslut om de årliga handlingsplanerna. Arbetet följs upp enligt det ordinarie årshjulet och det sker även avstämning vid behov med hela kommunstyrelsen, dess arbetsutskott eller med presidiet.

Informationssäkerhetssamordnaren besöker alla nämnder och ledningsgrupper minst en gång per år. Vid dessa tillfällen ges en omvärldsbevakning inom området samt en statusuppdatering av aktiviteter som beslutats i handlingsplanen.
Dricksvattenförsörjning samt delar av hälso- och sjukvård är identifierade som samhällsviktiga tjänster inom Alingsås kommun i enlighet med NIS-lagstiftningen. Centrala funktioner för informationssäkerhet har enligt uppgift prioriterat stöttning till dessa verksamheter för att uppnå de lagkrav som finns.

Ansvariga tjänstepersoner upplever att det finns ett stort engagemang från kommunstyrelsen och kommunledning som leder till goda förutsättningar att genomföra ett systematiskt arbete. Prioriteringar uppges utgå från risk- och väsentlighetsanalys och de åtgärder som det funnits behov av att genomföra har kunnat verkställas genom tilldelning av resurser. Ett exempel som lyfts är att det i årets budget ingår ett uppdrag stärka it-säkerheten i kommunen.

Intervjuade beskriver att arbetet med informationssäkerhet har kommit olika långt mellan förvaltningarna och att mognaden är varierande. Detta bekräftas av den uppföljning som gjorts för 2022 i form av en rapport[5] som utgör så kallat ”Ledningens genomgång”.
Av genomförda mätningar av informationssäkerhet som redovisas i rapporten framgår att kommunen utvecklats inom områdena informationssäkerhet och dataskydd under 2022. Stort fokus under 2022 uppges ha varit att få till ett systematiskt arbetssätt med informationssäkerhet vilket har införts och lyfts som en förutsättning för att fullmäktiges långsiktiga målsättningar ska uppnås. Metoder och arbetssätt behöver genomföras

[5] Kommunstyrelsen, 2023-03-06 § 44

med regelbundenhet och bli en naturlig del av kommunens arbete för att arbetet ska utvecklas vidare. Planeringen sträcker sig över flera år för att höja kommunens arbete med informationssäkerhet.

Utöver det arbete som behöver genomföras inom respektive förvaltning anges även mer övergripande processer som behöver utvecklas. Bland annat vid upphandling av nya system där informationssäkerhets- och dataskyddsfrågor behöver integreras tidigare i processerna. Detta ingår som en prioriterad aktivitet i handlingsplan för informationssäkerhet 2023. Planen beskriver att ett fördjupat samarbete med upphandlingsenheten ska påbörjas med syftet att än bättre inbegripa frågor om dataskydd, informationssäkerhet och övrig säkerhet i upphandlingsprocessen. Intervjuade har bekräftat att det vid tid för granskningen pågår ett utvecklingsarbete i enlighet med handlingsplanens aktivitet.

3.2.1 Kommentarer och bedömning

Vi bedömer att det vid tid för granskningen 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 konstaterar att det finns en god samordning mellan nyckelfunktioner med ansvar inom säkerhetsarbetet, informationssäkerhetsarbetet och it-säkerhetsarbetet vilket även är reglerat i policy och riktlinjer.

Vi uppfattar därtill att samtliga nämnder 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, men även att gemensamma arbetssätt och metoder kan etableras och genomföras på likartat sätt i kommunens samtliga verksamheter.

3.3 Säkerhetskultur

Iakttagelser

Enligt kommunens informationssäkerhetspolicy ska ansvar för informationssäkerhet vara väl kommunicerat i verksamheten. Medarbetare ska erhålla utbildning och information med en säkerhetsmedvetenhet för att hantera information korrekt.

Intervjuade beskriver att kompetenshöjande aktiviteter är högt prioriterat då organisationens storlek och omfattning i sig är en utmaning för att få till en tillräcklig säkerhetsmedvetenhet.

Utbildningar genomförs dock regelbundet till samtliga medarbetare och förtroendevalda, främst i form av så kallade ”nano learnings”, som är korta digitala

utbildningar som skickas via mejl. Dessa riktar sig både mot förtroendevalda och medarbetare. Därtill uppges de tillfällen som informationssäkerhetssamordnare besöker styrelser, nämnder och ledningsgrupper utgöra en bra information och utgöra kunskapshöjande insatser med information om aktuella risker och de säkerhetsåtgärder som pågår för att höja säkerheten i kommunen.

Uppföljning av genomförd utbildning visar att ca 48 % av alla anställda och förtroendevalda genomfört utbildningen. Det har även genomförts fejkade phisingtest för att mäta hur många som identifierade att detta var ett hot och hur många som klickade på länkar mm vilket i skarpt läge hade kunnat leda till konsekvenser för informationssäkerheten.

3.3.1 Kommentarer och bedömning

Vi bedömer att kommunstyrelsen inom ramen för sin uppsiktsplikt delvis tillsett att det finns en tillräcklig säkerhetskultur inom nämnderna.

Det har genomförts ett flertal aktiviteter för att kommunens medarbetare och förtroendevalda ska få kunskap om informationssäkerhet och medvetenhet om risker inom området.

Vi bedömer att uppföljning gjorts.

Dock visar uppföljning att alltför få genomfört dessa för att insatser ska ha bidragit till en tillräcklig säkerhetskultur inom samtliga nämnder.

3.4 Riskanalys och informationsklassning

Iakttagelser

Vid varje ny mandatperiod finns krav om att kommunerna ska göra en övergripande Risk- och sårbarbetsanalys, RSA. Detta är ett lagkrav inom arbetet med beredskap. I Alingsås kommun har en sådan process genomförts under 2023 där risker för cyberhot beaktats. Vid tid för granskningen skulle arbetet fortsätta med åtgärder utifrån de risker som identifierats, arbetet samordnas via säkerhetsenheten.

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 intervjuade uppfattar vi att kommunen har påbörjat ett arbete med informationsklassning och riskbedömning. Varje förvaltning har under 2022 genomfört en riskanalys utifrån informationssäkerhet och dataskydd. Under året har tre informationstillgångar (ex system, journal, arkivskåp, lagringsyta o.s.v.) per verksamhet analyserats. Under 2022 har även informationsklassningar genomförts i samband med upphandling och även vid några tillfällen för att avgöra om det är lämpligt att vara kvar i en teknisk lösning eller ej utifrån säkerhetsaspekterna.

Intervjuade beskriver att genomförande av informationsklassning kommer att intensifieras under 2023 och bli en del av kommunens ledningssystem för informationssäkerhet.

3.4.1 Kommentarer och bedömning

Vi bedömer att det inte finns ett systematiskt arbete med riskanalyser och informationsklassning.

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 i handlingsplan för 2023.

3.5 It-säkerhet och kontinuitet

Iakttagelser

Riktlinjer för informationssäkerhet (fastställd 2020-12-07) inkluderar ett avsnitt som reglerar informations-säkerhet i it-miljön. Därtill finns ett antal skrivelser även i andra avsnitt i riktlinjerna med bäring på systemens säkerhet och kontinuitet. Bland annat framgår i delen för informationssäkerhet i verksamheter att verksamheten ska kunna fortsätta även om till exempel IT-system slås ut, en strömkabel grävs av eller byggnader brinner ner.

Enligt riktlinjerna ska krav på säkerställd drift gällande system och processer identifieras genom informationsklassning. Dvs att skyddsnivå för systemets tillgänglighet fastslås. Höga skyddskrav för tillgänglighet innebär högre krav på säkerhetskopiering och redundans. Som vi beskrivit i föregående avsnitt är inte samtliga system informationsklassade vid tid för granskningen och ovan underlag saknas därigenom för majoriteten av system som nyttjas i kommunen.

Vi har i granskningen fått en detaljerad beskrivning av de tekniska säkerhetsåtgärder som kommunens it-avdelning har etablerat. 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.

Med hänsyn till att alltför detaljerad information om etablerade säkerhetsåtgärder kan utgöra en sårbarhet för kommunen beskriver vi endast översiktligt ett urval av de åtgärder vi tagit del av.

- I syfte att hindra kommunikation mellan system, servrar och datorer som inte är beroende av att kunna kommunicera med varandra har kommunen en långtgående segmentering av sina nätverk vilket ger en stärkt förmåga att hindra att intrångsförsök lyckas nå skyddsvärda uppgifter.
- Det har genomförts och pågår förstärkningar för en redundant infrastruktur. Bland annat genom geografiskt åtskilda datorhallar samt stärkta rutiner för säkerhetskopiering för att information ska vara återläsningsbar i händelse av avbrott eller incident.
- Ett flertal tekniska skydd har etablerats mot olika cyberhot och angreppsmetoder.
- Kommunen har installerat programvara för övervakning, larmssättning och detektion samt gjort personella förstärkningar i syfte att kunna hantera säkerhetshändelser och incidenter.

I den beslutade handlingsplanen för 2023 framgår vissa aktiviteter i syfte att stärka it-säkerheten, det är främst inom området för konto- och behörighetshantering. Dessa åtgärder bidrar till ökad säkerhet och bättre motståndskraft mot cyberhot i form av phising eller id-kapning. Vid tid för granskningen har arbetet till viss del genomförts.

Nuvarande säkerhetslösningar har delvis utvärderats genom tekniska tester. Under 2022 genomfördes penetrationstester och sårbarhetsskanning med hjälp av externa leverantörer. Därtill har ett antal interna tester genomförts i syfte att identifiera sårbarheter. I nuläget uppger intervjuade att det pågår ett arbete med en relativt ny teknik som syftar till att hotaktörer ”luras” till säkra ytor i it-miljön.

Vad gäller hantering och säkerhet för molntjänster har kommunledningskontoret tagit fram ett ställningstagande gällande molntjänster och tredjelandsöverföring av personuppgifter till tredje land. Enligt intervjuade är ställningstagandet inte politiskt fastställt utan fungerar som en rekommendation för verksamheten.

- Försiktighetsprincipen råder och varje enskild molntjänst prövas var för sig.
- Alingsås kommun går inte in i nya molntjänster som innebär tredjelandsöverföring av personuppgifter till land som enligt EU-kommissionen inte uppnår adekvat skyddsnivå.
- Det är ej lämpligt att information som omfattas av sekretess delas i molntjänster/drifttjänster som inte lyder under svensk lag.

Att molntjänster prövas var för sig innebär enligt intervjuade att informationsklassning alltid ska göras vid införande men även att befintliga tekniska lösningar klassas och riskbedöms så att säkerhetsåtgärder identifieras och införs löpande.

Mot bakgrund av nytt rättsläge vilket kan påverka hur tolkning av lagstiftning för tredjelandsöverföring av personuppgifter kan göras, ska kommunens tidigare ställningstagande omprövas i samband med ett möte i slutet av november. I samband med mötet ska även dialog om lämplig beslutsnivå för ställningstagandet i kommunen göras.

3.5.1 Kommentarer och bedömning

Vi bedömer att vid tid för granskningen har kommunstyrelsen genom beslut av både resurser och prioriterade åtgärder gett verksamheten förutsättningar att etablera erforderliga tekniska säkerhetsåtgärder i syfte att skydda kommunens it-infrastruktur mot säkerhetshändelser.

Dock saknas i nuläget tillräckliga underlag som visar om det finns behov av ytterligare tekniska säkerhetsåtgärder, detta då informationsklassning och riskbedömning inte gjorts för samtliga informationstillgångar. Kommunen bör därför säkerställa att dessa aktiviteter genomförs och att en prioritering görs för system inom de verksamheter som är identifierade som samhällsviktiga och digitala tjänster och står under krav i NIS-direktivet eller där personuppgifter hanteras där lagkrav utifrån dataskyddsförordningen måste beaktas.

Vi bedömer att etablerade säkerhetsåtgärder delvis har utvärderats men att det inte sker regelbundet för att fastställa att de fungerar ändamålsenligt över tid i förhållande till aktuella hot och risker.

Däremot bedömer vi att det i hög grad finns tekniska funktioner och även tillgång till kompetens som ger kommunen goda förutsättningar till övervakning och kontroll för att upptäcka hot om intrång eller andra incidenter.

3.6 Incidenthantering och reservrutiner

Iakttagelser

Informationssäkerhetspolicyn (fastställd 2019-11-12) reglerar att informationssäkerhetsarbetet ska vara förebyggande och ha en förmåga att hantera informationssäkerhetsincidenter, störningar, och eventuella kriser. I riktlinjer för informationssäkerhet framgår att informationssäkerhetsrelaterade incidenter är oönskade händelser som kan leda till brister i konfidentialitet, riktighet, tillgänglighet och spårbarhet hos information. Systemägare ansvarar för att incidenter relaterade till system upptäcks, samlas in, hanteras, sammanställs och dokumenteras.

Intervjuade beskriver att incidenthantering är ett område där det pågår ett aktivt arbete för att utveckla. I nuläget har inte olika typer av incidenter definierats gentemot organisationen och det finns i nuläget olika rapporteringsvägar för olika typer av incidenter, exempelvis it-incidenter, personuppgiftsincidenter och NIS-incidenter. I underlaget för ”Ledningens genomgång”, som vi beskrivit tidigare i rapporten, ingår en redogörelse för inträffade incidenter i kommunen fördelat på it-incidenter, borttappad/stulen utrustning samt personuppgiftsincidenter.

Vi kan konstatera utifrån underlaget att kommunen varit utsatt för intrångsförsök och att det funnits anledning till att gå upp i stabsläge mot bakgrund av it-incidenter, dock har kommunen kunnat konstatera att ingen påverkan eller konsekvens drabbat kommunen vid dessa händelser.

I rapporten framgår även att genomförda mätningar av informationssäkerheten i kommunen visat att kommunen särskilt behöver fokusera på förbättring inom incidenthantering, medarbetarnas kunskaper och säkerhetskultur. Rapporten beskriver att flera pågående arbetsinsatser planeras för att höja kommunens förmåga inom dessa utpekade områden men att det kommer behövas ytterligare riktade insatser för att nå önskade säkerhetsnivåer. Aktiviteter föreslås i 2023 års handlingsplan.

I handlingsplanen framgår som en prioriterad aktivitet för 2023 att ta fram övergripande incidenthanteringsprocess och implementera denna i syfte att utveckla förmågan att hantera incidenter.

Internt inom it-avdelningen så finns etablerade rutiner och processer i händelse av it-incidenter. Incidenter hanteras och dokumenteras i ärendehanteringssystem inom it där det finns olika processer och rutiner som följs baserat på allvarsgrad för incidenterna. Enligt uppgift skrivs incidentrapporter och incidenter rapporteras även regelbundet till kommunstyrelsen. Detta kan göras av kommundirektör i samband med informationspunkt och vid behov deltar även it-chef.

Kommunen har etablerat en beredskap dygnet runt och har även tydliggjorda eskaleringsvägar till ordinarie krishanteringsrutiner, exempelvis kopplas tjänsteman i beredskap in vid allvarliga säkerhetshändelser eller incidenter.

I händelse av ett avbrott där it-miljön behöver återställas finns dokumentation för att göra återställning som ansvariga inom it har tillgång till. Rutinerna har enligt uppgift testats vid driftsstopp, exempelvis vid större förändringsarbetet i it-miljön där komponenter byts ut eller uppgraderas. Då en komplett återställning av it-miljön alltid kan vara förenat med viss risk så har inga simulerade krissituationer genomförts med avbrott och återställning.

Inom nämndernas verksamheter kontinuitetsplaner för hur verksamhetskritiska processer ska fungera även vid olika typer av störningar. I dessa processer ingår bedömningar och planering för de it-system som nyttjas inom respektive verksamhet. I den planering som finns upprättad finns därigenom reservrutiner framtagna för berörda system. Övningar har genomförts både under 2022 och 2023 utifrån scenariot

storskalig IT-attack. Intervjuade uppger att övning genomfördes dels i syfte att öva krisledning, dels för att testa respektive verksamhets kontinuitetsplanering.

3.6.1 Kommentarer och bedömning

Vår bedömning är att det delvis finns etablerade rutiner vid säkerhetshändelser och incidenter.

Vi bedömer att rutiner för den övergripande hanteringen i kommunen där verksamheterna är involverade är i behov av att tydliggöras och etableras vilket även framgår som prioriterad aktivitet i kommunens handlingsplan och genom tidigare uppföljning. Vi konstaterar att kommunstyrelsen regelbundet informeras om inträffade incidenter samt att samtliga inträffade incidenter dokumenteras i årlig uppföljning och att incidenter ingår som underlag för att identifiera förbättringsåtgärder.

Vi bedömer att i it-funktionens interna hantering av säkerhetshändelser sker utifrån etablerade rutiner och processer samt att incidenter dokumenteras och analyseras. Vi ser det som positivt att kommunen har tillsett beredskap för incidenter även utanför ordinarie kontorstid.

Vi bedömer att vid tid för granskningen finns i allt väsentligt dokumenterade reserv- och återgångsrutiner i händelse av avbrott och allvarligare störning. Vi bedömer att rutinerna har övats och för att testa så att de fungerar ändamålsenligt.

Vi ser positivt på att rutiner har testats vid planerade och simulerade övningar. Därtill har de även testats i skarpt läge där kommunen inte påverkades av allvarliga konsekvenser. Vi konstaterar därigenom att rutinerna har fungerat tillfredsställande vid dessa tillfällen och även att det funnits möjlighet att revidera rutiner och kontinuitetsplanering mot bakgrund av genomförda övningar.

3.7 Uppföljning och återrapportering

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 efterlevnad årligen ska följas upp genom intern kontroll samt att revision av hela eller stora delar av Alingsås kommuns informationssäkerhet ska göras minst vartannat år.

Informationssäkerhetssamordnare ska därtill löpande rapportera läge och status gällande informationssäkerhet till säkerhetschef som årligen ska sammanställa en rapport till kommunstyrelsen.

Vi konstaterar att informationssäkerhetssamordnaren, i enlighet med uppdrag och ansvar, årligen följer upp och rapporterar om det samlade informations-säkerhetsarbetet. Som vi beskrivit tidigare sammanställs detta i en rapport som presenteras för kommunstyrelsen vid ”Ledningens genomgång”. Handlingsplan för informationssäkerhet beslutas av kommunstyrelsen och innehåller en uppföljning av arbetet och genomförda aktiviteter. Under 2022 har merparten av de aktiviteter som ingått i handlingsplanen genomförts eller påbörjats. De aktiviteter som inte genomförts under 2022 har flyttats till 2023 års handlingsplan.

Som uppföljning av informationssäkerhetsarbetet har kommunen genomfört ”Infosäkkollen” som är en mätning som tillhandahålls av MSB. Mätningen uppges vara ett sätt att utvärdera arbetet över tid och se att en förflyttning sker i riktning mot de mål som kommunfullmäktige beslutat om i informationssäkerhetspolicyn.

I den samlade rapporten för informationssäkerhetsarbetet 2022 ingår en uppföljning av efterlevnad av lagkrav inom informationssäkerhet och dataskydd. Bilden av regelefterlevnaden i kommunens rapport, inom området dataskydd är att kommunens personuppgiftsansvariga följer dataskyddsförordningen i relativt hög omfattning.

Intervjuade beskriver att de, utifrån att kommunen inte ännu har en tillräcklig systematik i arbetet, att efterlevnad av styrdokument inte varit relevant att följa upp på nämnds- och verksamhetsnivå. Som beskrivits tidigare i rapporten har fokus varit på att etablera ett ramverk för arbetet och att arbetet framåt prioriteras för att arbetssätt och metoder enligt riktlinjen ska genomföras. I nuläget framgår att viss uppföljning av nämndernas arbete sker i samband med de dialoger som sker med samtliga nämnder och med ledningsgrupper. Nästa steg uppges vara att införa ett verktyg för självkontroll/egenkontroll för att senare komma i gång med externa revisioner.

Utifrån lagkrav kommer högre krav om uppföljning inom vissa verksamheter, vilket kommer att prioriteras i arbetet i första skedet, enligt intervjuade.

3.7.1 Kommentarer och bedömning

Vi bedömer att vid tid för granskningen finns en etablerad uppföljning av informations- och it-säkerhetsarbetet och att denna rapporteras till kommunstyrelsen årligen i enlighet med policyns krav.

Uppföljningen är samlad, dokumenterad och innehåller analys och identifierade förbättringsområden.

Vi konstaterar att nämnderna delvis erhåller en rapportering och uppföljning av det kommunövergripande arbetet men att det i nuläget saknas en uppföljning av det nämndspecifika arbetet och efterlevnad av styrande dokument. Vi bedömer dock att de skäl som angetts i granskningen är acceptabla och att avsaknad av uppföljning inte grundar sig i bristande kontroll utan ett medvetet avvägt val utifrån verkningsgrad på en sådan uppföljning i förhållande till den mognadsgrad informationssäkerhetsarbetet ligger på i nuläget.

4 Samlad bedömning och rekommendationer

Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsen vid tid för granskningen i sitt övergripande ledningsansvar bedriver ett systematiskt informations-säkerhetsarbete.

Vi bedömer dock att det finns behov av att stärka systematiken i det operativa informationssäkerhetsarbetet inom både kommunstyrelsen och nämnderna.

Vi baserar vår bedömning på att arbetet med riskbedömning, informationsklassning och utbildningsinsatser behöver genomföras mer systematiskt. Därtill finns behov av att etablera gemensamma incidenthanteringsrutiner så att incidenter som inträffar upptäcks, analyseras och utvärderas i syfte att bidra i förbättringsarbetet och motverka att de händer igen.

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 i sin uppsiktsplikt över nämnderna säkerställer en tillräcklig intern kontroll över nämndernas arbete.

Utifrån genomförd granskning rekommenderar vi kommunstyrelsen att:

- Revidera och aktualisera informationssäkerhetspolicyn mot bakgrund av att den kan riskera att vara föråldrad i förhållande till nuvarande hot, risker och krav.
- Tillse att informationssäkerhetsutbildning genomförs i högre grad inom samtliga verksamheter.
- Tillse att egna informationstillgångar klassas och riskbedöms samt följa upp att samtliga kommunens verksamhetskritiska system samt system som hanterar skyddsvärd information och personuppgifter har en aktuell klassning och riskbedömning.
- Följa upp att säkerhetsåtgärder vidtagits som informationsklassning och riskbedömning visat behov av.
- Säkerställa att kommunövergripande incidenthanteringsrutiner upprättas och etableras.
- Anpassa och stärka uppföljningsmetoder och kontroll av efterlevnad av beslutade styrdokument inom informationssäkerhet i takt med att kommunens mognadsgrad i informationssäkerhetsarbetet ökar.

Dag som ovan

KPMG AB

Jenny Thörn
Verksamhetsrevisor

Viktoria Bernstam
Kundansvarig