Granskning av informationssäkerhet

Rapport

Ljusdals kommun

KPMG AB

2024-06-10

Antal sidor 21

Antal Bilagor:1

Ljusdals kommun
Granskning av informationssäkerhet

2024-06-10

Innehållsförteckning

Ljusdals kommun
Granskning av informationssäkerhet

2024-06-10

1 Sammanfattning

KPMG har av Ljusdals kommuns revisorer fått i uppdrag att granska kommunstyrelsens ansvar för att kommunen har ett systematiskt informationssäkerhetsarbete.

Syftet med granskningen har varit att bedöma om kommunstyrelsen tillsett att ett systematiskt informationssäkerhetsarbete bedrivs.

Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsen inte tillsett ett systematiskt informationssäkerhetsarbete.

Vi konstaterar att flera av de iakttagelser som gjordes i cybersäkerhetsgranskningen år 2018 fortfarande är aktuella även i den här granskningen. Då kommunens arbete är i en etableringsfas och då det till stora delar saknas systematik i det arbete som bedrivs, är vår bedömning att kommunstyrelsen har brustit i sitt ansvar avseende informationssäkerhetsarbetet. Kommunstyrelsen har inte i tillräcklig utsträckning utifrån tidigare genomförd granskning följt upp arbetet utifrån den åtgärdsplan som styrelsen beslutat om.

I det följande redovisas våra bedömningar kopplat till revisionsfrågorna, efterföljt av rekommendationer.

Revisionsfrågor	Bedömning
Finns aktuella styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas?	Delvis
Finns en ändamålsenlig organisation för informationssäkerhetsarbetet?	Delvis
Finns beslutade informationssäkerhetsmål med tillhörande handlingsplaner?	Nej
Har styrelse och nämnder tillsett att det finns en tillräcklig säkerhetskultur?	Delvis
Finns fastställda metoder för riskhantering och har informationssäkerhetsrisker beaktats och följts av åtgärder?	Nej
Har tekniska säkerhetsåtgärder vidtagits som står i relation till aktuella hot och risker och utvärderas dessa regelbundet?	Delvis
Har kommunstyrelsen säkerställt en tillräcklig förmåga att upptäcka och hantera kritiska it-säkerhetshändelser?	Delvis
Finns en tillräcklig uppföljning och återrapportering av kommunens informationssäkerhetsarbete?	Nej

Utifrån resultatet av vår granskning rekommenderar vi kommunstyrelsen att:

- Anta upprättade riktlinjer och säkerställ att de implementeras i organisationen.
- Upprätta mål med tillhörande handlingsplaner för informationssäkerhetsarbetet.
- Säkerställ att en kommungemensam modell för riskbedömning och informationsklassning etableras samt att riskbedömning av kommunens informationstillgångar genomförs.
- Säkerställa att identifierade behov av åtgärder genomförs samt att nuvarande åtgärdsplan revideras utifrån aktualiserade riskbedömningar.
- Säkerställ att utbildningsinsatser genomförs bland samtliga medarbetare.
- Säkerställ att incidentrutiner upprättas som omfattar eskaleringsvägar samt former för hur inträffade incidenter ska analysera och dokumenteras.
- Säkerställ att former för uppföljning av informationssäkerhetsarbetet upprättas.
- Säkerställ att kommunstyrelsen erhåller kontinuerlig återrapportering avseende kommunens informationssäkerhetsarbete.

2 Bakgrund

KPMG har av Ljusdals kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunstyrelsens ansvar för att kommunen har ett systematiskt informationssäkerhetsarbete. 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 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, revisionsfrågor och avgränsning

Granskningen har syftat till att bedöma om kommunstyrelsen tillsett att ett systematiskt informationssäkerhetsarbete 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 beslutade informationssäkerhetsmål med tillhörande handlingsplaner?
- Har styrelse och nämnder tillsett att det finns en tillräcklig säkerhetskultur?
- Finns fastställda metoder för riskhantering och har informationssäkerhetsrisker beaktats och följts av åtgärder?
- Har tekniska säkerhetsåtgärder vidtagits som står i relation till aktuella hot och risker och utvärderas dessa regelbundet?
- Har kommunstyrelsen säkerställt en tillräcklig förmåga att upptäcka och hantera kritiska it-säkerhetshändelser?
- Finns en tillräcklig uppföljning och återrapportering av kommunens informationssäkerhetsarbete?

Granskningen har omfattat kommunstyrelsen.

2.2 Revisionskriterier

Vi har i granskningen utgått från följande kriterier:

- Kommunallagen 6 kap. 6 §
- Tillämpbara interna regelverk, policys och beslut
- MSB:s metodstöd och rekommendationer avseende Ledningssystem för informationssäkerhet och it-säkerhetsåtgärder

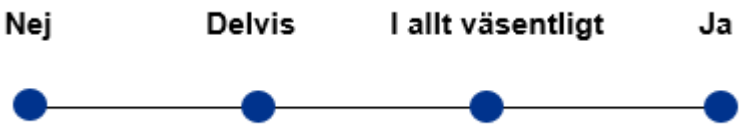
2.3 Metod

Granskningen har genomförts genom dokumentsstudier samt genom intervjuer med berörda tjänstepersoner och förtroendevalda. Dokumentanalysen har bland annat omfattat ett antal kommunövergripande dokument som en informationssäkerhetspolicy samt en risk- och sårbarhetsanalys.

Intervjuerna har genomförts med kommunens informationssäkerhetssamordnare, säkerhetschef och it-chef samt med kommunstyrelsens presidium.

Samtliga av de intervjuade har givits möjligheten att faktakontrollera rapporten.

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



2.4 Revisionsgranskning 2018

Under 2018 genomfördes en övergripande granskning av Ljusdals kommuns cybersäkerhetsarbete[1]. I granskningen gjordes bedömningen att den interna kontrollen avseende kommunens cybersäkerhet var bristande. Bland annat saknades det aktuell och ändamålsenlig dokumentation i form av planer, rutiner, instruktioner och processer. Arbetet med identifiering av risker, riskbedömningar och riskhantering samt systemöversikt för att identifiera brister i it-säkerheten ansågs behöva utvecklas. Informella arbetssätt ansågs medföra att arbetet inte bedrevs på ett systematiskt eller enhetligt sätt.

För ytterligare iakttagelser som lyftes i granskningen hänvisas läsaren till granskningsrapporten.

Följande rekommendationer lämnades till kommunstyrelsen:

- Kommunstyrelsen säkerställer att planer uppdateras/revideras samt kompletteras med rutiner, instruktioner och riskbedömningar för att utveckla hur informationssäkerhetsarbetet ska bedrivas. Risker/hot kopplat till information- och IT-säkerhet samt kontinuitetsplanering bör särskilt beaktas i kommunens kommande risk- och sårbarhetsanalys avseende mandatperioden 2019–2022.
- I syfte att öka förmågan att upptäcka avvikelser behöver kommunstyrelsen säkerställa att identifiering och rapportering av risker i kommunens IT-miljö utvecklas. IT-system med hög driftsäkerhet och starkt skydd mot externa attacker är av mycket stor vikt för säkerheten i samhället och för möjligheterna att hantera olika krisförlopp.
- Kommunstyrelsen säkerställer att övningar och utbildningar genomförs i syfte att öka kännedomen kring kommunövergripande styrning/ramverk för informationssäkerhet samt för IT-säkerhet. Övningar och utbildningar kan med fördel även syfta till att öka verksamheternas/användarnas kännedom om vilka risker som finns kopplat till användning av IT.

[1] Granskningen genomfördes av PwC.

3 Resultat av granskningen

3.1 Styrning och organisation av informationssäkerhetsarbetet

Enligt MSBs metodstöd (se bilaga A) bör en informationssäkerhetspolicy antas med tillhörande riktlinjer för att ge vägledning om vilka krav som ställs i arbetet.

Grundprincipen avseende ansvaret för informationssäkerhetsarbetet är enligt MSBs metodstöd att ansvaret ska följa det ordinarie verksamhetsansvaret från ledning ner till enskild medarbetare.

3.1.1 Ledningssystem för informationssäkerhet (LIS)

Ljusdals kommun har en av fullmäktige antagen informationssäkerhetspolicy[2]. Policyn antogs 2021 och beskriver principerna för kommunens informationssäkerhetsarbete och vilka generella krav som kommunledningen och kommunstyrelsen ställer på samtliga verksamheter inom koncernen.

Syftet med policyn är att den ska ge vägledning och ange de grunder och principer som styr kommunens arbete med informationssäkerhet. Alla som på uppdrag av kommunen hanterar information om verksamheten i sin yrkesutövning omfattas av kommunens policy.

En av principerna som anges i policyn är att informationssäkerhet uppnås genom att anställda i kommunen är medvetna om att all information ska hanteras tryggt. En trygg hantering av informationen innebär enligt policyn att bevara informationens konfidentialitet, riktighet och tillgänglighet. Ytterligare en av principerna är att arbetet med informationssäkerhet ska vara långsiktigt, kontinuerligt och omfatta alla verksamheter och informationstillgångar som kommunen äger eller hanterar.

Utöver kommunens informationssäkerhetspolicy finns det upprättade utkast till riktlinjer för kommunens informationssäkerhetsarbete. Dessa utkast är ännu inte antagna eller implementerade vid tiden för denna granskning.

3.1.2 Organisation och ansvarsfördelning

Av informationssäkerhetspolicyn framgår att kommunstyrelsen är ytterst ansvarig för informationssäkerheten.

Vidare framgår att kommunchefen ansvarar för instruktioner och anvisningar kring informationssäkerhet och att säkerhetsenheten ansvarar för att det strategiska arbetet med informationssäkerhet utvecklas genom kommunövergripande policys, riktlinjer, rutiner och utbildningar. Ansvaret på verksamhetsnivå följer det delegerade verksamhetsansvaret. Samtliga medarbetare har i sin tur ett ansvar att följa de principer som framgår av informationssäkerhetspolicyn.

Intervjuade beskriver ansvarsfördelningen i policyn som tydligt och uppger att ansvaret är väl etablerat hos verksamhetsansvariga. Enligt intervjuade saknas det dock tydliga

[2] Informationssäkerhetspolicy, 2021-04-26.

krav om mål och intervjuade anser att policyn tenderar att bli mer av en strategi för informationssäkerheten snarare än en policy.

Vid tidpunkten för granskningen har kommunen en tjänsteperson som utav sin heltidstjänst arbetar deltid som informationssäkerhetssamordnare. Informationssäkerhetssamordnaren arbetsleds av säkerhetsenheten men tillhör enheten Service, utveckling och innovation (SUI). I dagsläget finns dock planer på att denna tjänst ska övergå till säkerhetsenheten efter sommaren. Intervjuade anser att informationssäkerheten är en given del av säkerhetsarbetet och att den därför bör ligga kvar på samma enhet som tidigare.

Intervjuade uppger att det vid tid för granskningen endast finns utsedda funktioner inom utbildningsnämndens förvaltning (strateger för informations- och kommunikationsteknik) för att driva det lokala informationssäkerhetsarbetet framåt. Övriga förvaltningar saknar liknande utsedda funktioner.

3.1.3 It-enheten

Kommunens it-enhet består av it-chef samt nio tekniker, varav en av tjänsterna är vakant. Med anledning av den utveckling som it-frågor haft senaste åren uppger intervjuade att enheten är något lågt bemannad.

Intervjuade delger även att det beslutats om att införa en systemförvaltningsmodell i kommunen. Beslutet är taget i Ljusdals kommunledningsgrupp i mars 2024. Vi har i granskningen tagit del av vägledande dokument så som systemförvaltningshandbok, mall för systemförvaltningsplan samt en checklista för en så kallad systemskiss[3]. Intervjupersoner uppger att arbetet är i en uppstartsfas, där vissa verksamheter har skapat systemförvaltningsplaner medan andra inte har påbörjat arbetet ännu. Stöddokumenten kan därför enligt uppgift komma att justeras framgent.

Intervjuade uppger att kommunfullmäktige fattat ett inriktningsbeslut[4] om att Hälsinglands kommuner ska gå samman i en gemensam it-driftsorganisation. Syftet med samarbetet är att organisation, it-driftsprocesser och infrastruktur ska drivas gemensamt för kommunerna. Det pågår vid tid för granskningen en utredning med anledning av detta och arbetet har hittills inneburit en inventering av samtliga kommuners driftförutsättningar. Av fullmäktiges beslut framgår att arbetet ska vara genomfört senast 2026-01-01.

3.1.4 Informationssäkerhetsmål

Utöver de strategiska mål som framgår av kommunens informationssäkerhetspolicy har vi inom ramen för denna granskning inte mottagit några mål för kommunens informationssäkerhetsarbete.

[3] Omfattar bland annat systemnamn, servrar, integrationer och certifikat.
[4] Protokoll, Kommunfullmäktige, 2022-06-20

3.1.5 Bedömning

Vår bedömning är att det delvis finns aktuella styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas.

Vi konstaterar att det finns en för kommunen antagen informationssäkerhetspolicy som reglerar kommunens informationssäkerhetsarbete. Policyn innehåller ett antal principer för arbetet med informationssäkerhet samt reglerar ansvarsfördelningen mellan förtroendevalda och tjänstepersoner. Dock konstaterar vi även att kommunen utöver denna policy saknar styrande och vägledande dokument som reglerar bland annat roller och ansvar samt sådant som informationssäkerhetsklassning och riskhantering.

Vidare bedömer vi att det delvis finns en ändamålsenlig organisation för informationssäkerhetsarbetet.

Vi konstaterar att det finns en samordnande person i enlighet med MSBs metodstöd, som arbetar deltid med kommunens informationssäkerhet. Ansvaret för informationssäkerheten är känt hos verksamhetsansvariga. Vi ser däremot att aktiviteter inte har genomförts utifrån ansvaret, vilket kan vara följden av att det saknas tydlig kravställning och stöd från centralt håll genom styrande dokument. För att säkerställa ett systematiskt informationssäkerhetsarbete inom samtliga verksamheter vill vi lyfta vikten av att det utses funktioner inom respektive nämnds förvaltning, som innehar ansvaret för att driva det lokala informationssäkerhetsarbetet framåt.

Vi bedömer att det inte finns beslutade informationssäkerhetsmål med tillhörande handlingsplaner.

Det redogörs i kommunens informationssäkerhetspolicy för ett antal principer, men vi konstaterar att det utöver detta saknas mål som avser kommunens informationssäkerhetsarbete.

3.2 Säkerhetskultur

MSBs metodstöd ställer krav om ständig utbildning och kommunikation för att höja medvetenheten och kunskapen om informationssäkerhet.

Det har bland annat satts in ett åtgärdspaket med webbaserade utbildningar för chefer. Intervjuade anger att utbildningarna just nu enbart omfattar cheferna men att tanken är att de även ska omfatta medarbetare. Av kommunens risk- och sårbarhetsanalys framgår att kunskapsnivån inom informationssäkerhet upplevs ha ökat bland chefer med anledning av insatsen.

Kommunen har nyligen tecknat ett avtal med en plattform för att genomföra tester via e-post i syfte att utbilda och medvetandegöra kommunens medarbetare att inte klicka på länkar som skickas från externa aktörer.

Enligt intervjuade finns en upplevelse av att kunskapen bland kommunens medarbetare har ökat. Säkerhetsavdelningen har arbetat med att synliggöra avdelningen samt genomföra informationsinsatser för att öka medarbetarnas medvetenhet avseende säkerhet över lag, inklusive informationssäkerhet.

It-enheten informerar aktivt vikten av att medarbetare och förtroendevalda inte ska nyttja sin privata e-postadress i sitt arbete/förtroendeuppdrag.

3.2.1 Bedömning

Vi bedömer att styrelsen delvis har tillsett att det finns en tillräcklig säkerhetskultur.

Vi gör bedömningen att kommunstyrelsen bör säkerställa att det genomförs utbildningsinsatser för samtliga medarbetare. Utöver att ständig utbildning och kommunikation höjer medarbetares medvetenhet och kunskap om informationssäkerhet, bidrar det även till ökad acceptans av och förståelse för de säkerhetsåtgärder som implementeras.

3.3 Informationssäkerhetsarbetet

3.3.1 Riskanalys

Enligt MSBs metodstöd så ska en verksamhet identifiera de hot och oönskade händelser som kan leda till negativa konsekvenser för organisationen.

Som nämnts saknas det vid genomförandet av granskningen upprättade och politiskt beslutade riktlinjer för riskanalys.

Kommunen har genomfört en risk- och sårbarhetsanalys[5] utifrån perspektivet krisberedskap, där utgångspunkten har varit ett antal beskrivna riskscenarion på övergripande nivå. Dessa scenarion omfattade bland annat risker och hot inom informationssäkerhet utifrån it-avbrott och it-attacker.

Intervjuade förklarar att det inte har gjorts någon riskanalys av enbart informationssäkerhetsrisker på varken kommunövergripande nivå eller verksamhetsnivå.

Vidare uppger intervjuade att det finns behov av att stärka nuvarande riskanalysarbete samt kontinuitsarbete. Detta för att kunna identifiera sårbarheter i verksamheterna och utifrån det vidta åtgärder för att stärka motståndskraften mot eventuella attacker samt bibehålla verksamhet vid ett eventuellt avbrott.

Vid anskaffning av nya system eller andra it-funktioner uppger intervjuade att det finns en checklista för de delar som är nödvändiga att gå igenom innan upphandling sker. Av checklistan framgår att en behovsanalys ska skickas till it-ledningsgruppen i syfte att kontrollera om systemet/funktionen redan finns och kan nyttjas i det aktuella fallet. It-ledningsgruppen kan även kontrollera om det finns liknande behov i andra verksamheter. Intervjuade anger att checklistan ännu inte är implementerad i samtliga verksamheter. I checklistan saknar vi moment såsom att genomföra riskanalys och klassning av system/funktion innan upphandling genomförs.

3.3.2 Informationsklassning

Enligt MSBs metodstöd är informationsklassning en förutsättning för att kunna skapa rätt skydd för informationen som hanteras i kommunens.

Det saknas riktlinjer för informationsklassning samt en antagen klassningsmodell som är anpassad för kommunens behov. Intervjuade uppger att arbetet med informationsklassning är eftersatt och att det endast är ett fåtal informationstillgångar som genomgått klassning. Vid genomförda klassningar har SKRs[6] modell KLASSA[7] använts.

Enligt kommunledningsgruppens beslut om systemförvaltningsorganisation har it-chefen fått i uppgift att samordna en uppdaterad lista över vilka verksamhetssystem som finns på respektive förvaltning. Det framgår även av beslutet att alla

[5] Risk- och sårbarhetsanalys, 2023-12-18.
[6] Sveriges kommuner och regioner
[7] Metod för informationsklassning. Metoden hjälper verksamheten att välja rätt åtgärder för att skydda informationen.

förvaltningschefer ska förbereda sin organisation på att ta fram systemförvaltningsplaner för samtliga system.

3.3.3 Åtgärdsplan

I samband med revisionsgranskningen som genomfördes 2018 avseende cybersäkerhet upprättades en åtgärdsplan. Vi har i granskningen tagit del av åtgärdsplanen som senast uppdaterades i mars 2024[8]. Uppdateringen är genomförd utifrån de åtgärder som identifierades 2019. Planen omfattar beskrivning av identifierade problem, vad avsikten med åtgärderna är samt behovsbeskrivning av resurser. Intervjuade förklarar att de färdigställda åtgärdslistorna skickas till säkerhetsenheten, där enheten ser över vilka åtgärder som verksamheten kan göra i egen regi, vilket behov av stöd de behöver från centralt håll samt om det finns behov för verksamheten att äska ytterligare medel för genomförandet. Av åtgärdsplanen framgår hur status för åtgärderna ser ut år 2024. Av de 16 identifierade problem som tas upp i åtgärdsplanen är det två problem som åtgärdats, fyra är pågående och tio problem ska enligt planen åtgärdas under 2024. Bland annat framgår att it-policyn behöver ses över utifrån att informationssäkerhetspolicyn saknar reglering avseende det tekniska skyddet. Därtill framgår att det saknas rutiner för hantering av it-incidenter. Aktiviteterna för 2024 har fördelats mellan säkerhetschefen och it-chefen.

3.3.4 Bedömning

Vår bedömning är att det inte finns fastställda metoder för riskhantering samt att informationssäkerhetsrisker delvis har beaktats och följts av åtgärder.

Vi gör bedömningen att det saknas ett tillräckligt arbete med att riskbedöma utifrån att identifiera eventuella hot och oönskade händelser som kan påverka kommunens verksamhet negativt. Vi gör även bedömningen att befintlig checklista kompletteras med aktiviteterna riskanalys och klassning så att detta regelmässigt genomförs vid anskaffning av nya system, för att minska risken för att ett undermåligt system implementeras.

Kommunen saknar i dagsläget en antagen modell för informationsklassning. Att inrätta en gemensam klassningsmodell är enligt MSBs metodstöd viktigt för att kunna tillse att organisationens informationstillgångar skyddas utifrån interna och externa krav på informationens konfidentialitet, riktighet och tillgänglighet.

Vår bedömning är att identifierade åtgärdsbehov inte har genomförts i tillräcklig utsträckning då endast två identifierade problem åtgärdats samt att fyra är pågående. Därtill innehar planen åtgärdsbehov som identifierades 2019. Vår bedömning är därför att nuvarande åtgärdsplan bör revideras utifrån aktualiserade riskbedömningar.

[8] Åtgärdsplan, 2019-11-27, uppdaterad 2024-03-11.

3.4 It-tekniska säkerhetsåtgärder

3.4.1 Riskanalys

Intervjuade uppger att vidtagna säkerhetsåtgärder bland annat grundas i den tidigare nämnda åtgärdsplanen. Därtill har it-enheten interna rutiner för riskanalysarbete, vilket inte dokumenteras på ett systematiskt sätt. Därtill sker en kontinuerlig omvärldsbevakning, bland annat i form av prenumerationer från relevanta nyhetskanaler.

3.4.2 Implementerade åtgärder

Med anledning av att en detaljerad beskrivning av de it-tekniska säkerhetsåtgärder som implementerats kan utgöra känsliga uppgifter för kommunen, presenteras nedan endast ett urval.

Vi har fått uppgift om ett antal förstärkningar som gjorts eller som planeras att genomföras för att höja den tekniska säkerheten. Bland annat så tillhandahåller it-enheten sedan 2019 den utrustning (datorer och telefoner) som nyttjas i kommunen. It-enheten har därmed uppsikt över utrustningen gällande livscykel och därigenom möjlighet att byta ut föråldrad utrustning där nya säkerhetsuppdateringar inte kan installeras. Det uppges dock finnas viss utrustning som fortfarande ägs av verksamheterna, där it-enheten saknar kontroll över utrustningens säkerhet vilket ses som en risk.

It-enheten arbetar med kontinuerliga uppdateringar av antivirusskydd och brandväggar. Med grund i genomförd riskanalys har behov identifierats av att segmentera[9] nätverk från varandra, som en del i att skydda sig mot att ett eventuellt intrång sprids till andra nätverk. Kommunstyrelsen fattade i mars 2024 beslut[10] om att införa tvåfaktorsautentisering[11] som en del i att skydda kommunen mot intrångsförsök.

Intervjuade uppger att it-enheten i flera delar av arbetet haft extern konsulthjälp, både utifrån kunskapsförstärkning och även i det praktiska arbetet med att genomföra vissa åtgärder. Det har dock inte genomförts några tester likt penetrationstest eller sårbarhetsskanning för att utvärdera vidtagna åtgärder.

3.4.3 Bedömning

Vår bedömning är att det delvis har vidtagits tekniska säkerhetsåtgärder i relation till aktuella hot och risker. Vi kan konstatera att åtgärderna inte utvärderas med regelbundenhet.

Bedömningen grundas i att vidtagna åtgärder har utgångspunkt i en åtgärdsplan. Dock saknas genomförda riskanalyser som i tillräcklig grad beaktar informationssäkerhetsrisker. Det saknas även bedömningar av skyddsvärde och behov

[9] Nätverkssegmentering innebär att separera nätverken mellan varandra för att minska risken för att ett eventuellt intrång sprids till andra nätverk.
[10] Protokoll, kommunstyrelsen, 2024-03-13
[11] Tvåfaktorautentisering innebär att användaren måste ange två olika former av autentisering för att logga in på en tjänst.

av säkerhetsåtgärder då informationsklassning för kommunens informationstillgångar inte gjorts. Detta innebär att det kan finnas sårbarheter och behov av åtgärder som ännu inte identifierats.

3.5 Incidenthantering

3.5.1 Övervakning och loggning

It-enheten har både teknisk och manuell övervakning av kommunens it-miljö. Vid en incident eller avvikelse i it-miljön har enheten en upprättad beredskap. Beredskapen omfattar enligt lokalt avtal[12] både vardag och helg utanför kontorstid.

Enligt intervjuade har enheten diskuterat möjligheterna att införa ytterligare tekniska funktioner som skulle stärka kommunens övervakning. Då införande av förstärkt övervakning är kostsam och skulle innebära behov av tilläggsäskande från it-enheten utvärderas olika alternativ och möjligheter.

Av den åtgärdsplan vi tagit del av framgår att det finns ett upphandlat system för centraliserad logghanteringssystem. Systemet är vid tid för granskningen ännu inte implementerat. Anledningen är att det fattas komponenter som varit restnoterade hos leverantör. Intervjuade förklarar att kommunen utöver det nya systemet innehar flera funktioner som notifierar om driftstörningar i såväl fysiskt serverrum som inom inloggningar för båda användarkonton och enheter.

3.5.2 Rutiner för incidenthantering

Av informationssäkerhetspolicyn framgår att det är kommunstyrelsen som är ytterst ansvarig vid incidenter.

Vi har inom ramen för denna granskning mottagit ett utkast till en rutin för hantering av informationssäkerhetsincidenter. Utkastet är ännu inte formellt antaget. Kommunen har en e-tjänst via kommunens intranät som intervjuade anger att anställda kan vända sig till för anmälan av incidenter eller för information avseende frågor om incidenter.

Vi har för denna granskning tagit del av utdrag från kommunens system för incidentrapportering. Utdragen avser rapportering av de personuppgiftsincidenter som upptäckts. Enligt intervjuade har incidentrapporteringen bland anställda ökat till följd av utbildningsinsatser bland personalen (se avsnitt 3.2 *Säkerhetskultur*).

Intervjuade förklarar att kommunen har en GDPR-grupp. Gruppen består av kontaktombud, leds av informationssäkerhetssamordnaren och samordnas av säkerhetschefen. I gruppen ingår även en kommunjurist samt kommunens arkivansvariga. Intervjuade förklarar att gruppen arbetar med att gå igenom inträffade incidenter samt undersöker om det finns liknande incidenter som har noterats på flera ställen i kommunen. I det fall det konstaterats flera liknande incidenter kan gruppen till exempel besluta om att genomföra informationskampanjer på just det området i syfte att förhindra liknande incidenter. Sedan gruppen upprättades har den initierat ett antal åtgärder. Bland annat har gruppen beslutat att sätta upp affischer i anslutning till

[12] Protokoll, lokalt kollektivavtal gällande beredskap på it-enheten 2023-06-08, 2023-06-14.

kommunens skrivare, då det fanns en tendens att utskrifter lämnades obevakade. Vidare har gruppens iakttagelser även resulterat i att DISA-utbildning har erbjudits chefer.

Utöver GDPR-gruppens analysarbete förklarar intervjuade att säkerhetschefen även jobbar med analyser och incidenter inom säkerhetsskydd.

Inom it-enheten följs inträffade it-incidenter upp och analyseras i syfte att minska risken för att händelsen inträffar igen. Intervjuade uppger att det saknas en systematik avseende att dokumentera analysen samt i vissa fall även vidtagen åtgärd.

Vid avbrott i elförsörjningen har it-enheten åtgärder för att säkerställa strömförsörjning. It-enheten har även internt en lista över nätverk och system som behöver prioriteras vid uppstart av system och nätverk i it-infrastrukturen. Enheten har även erhållit prioriteringslistor från respektive verksamhet som omfattar de system man är beroende av. Rutinerna har inte testats eller behövt nyttjas i skarpt läge vid tid för granskningen. Intervjuade anger att ett test planeras att genomföras i en utvald del av en verksamhet.

3.5.3 Bedömning

Vår bedömning är att kommunstyrelsen delvis har säkerställt en tillräcklig förmåga att upptäcka och hantera kritiska it-säkerhetshändelser.

Bedömningen grundas i att det delvis finns en övervakning för att upptäcka hot om intrång eller andra säkerhetsincidenter i it-miljön. Därtill har kommunstyrelsen genom it-enheten säkerställt möjligheten för en skyndsam hantering vid en inträffad it-incident utanför kontorstid genom beredskap.

Vi konstaterar att det finns en e-tjänst för att anmäla incidenter. Vi konstaterar dock även att det saknas en dokumenterad och formellt antagen rutin för hur incidenter ska hanteras i kommunen, som även omfattar interna och externa eskaleringsvägar. Då styrdokument inte finns tillämpade i verksamheten finns en förhöjd risk att det saknas medvetenhet hos medarbetarna vad en incident är och hur den ska anmälas.

Vi noterar att det sker ett visst analysarbete av inträffade it-incidenter. Vi bedömer dock att formerna för gruppen behöver struktureras i ett styrande dokument i syfte att tydliggöra roller och ansvar.

Vår bedömning är även att kommunstyrelsen bör säkerställa att en kommunövergripande prioriteringslista upprättas för den ordning som nätverk och system ska startas upp efter ett kommunövergripande avbrott. Därtill anser vi att kommunstyrelsen behöver säkerställa att reserv- och återgångsrutiner testas i samtliga verksamheter samt på kommunövergripande nivå i syfte att säkerställa att verksamhet kan bibehållas i samband med ett avbrott. Test kan även utgöra grund för eventuella justeringar i en upprättad prioriteringslista.

3.6 Uppföljning och återrapportering

För att ledningen på strategisk nivå ska få en samlad bild och kunskap om informationssäkerhetsarbetet i kommunen behöver det enligt MSBs metodstöd ske en kommunövergripande uppföljning av arbetet som rapporteras under ledningens genomgång. Uppföljning utgör även underlag för eventuella beslut på strategisk nivå angående åtgärder och resursfördelning.

3.6.1 Uppföljning

Det saknas dokumenterad styrning om hur uppföljningsarbetet kring informationssäkerheten ska se ut.

3.6.2 Ledningens genomgång och annan återrapportering

Ledningens genomgång har inte etablerats i kommunen.

Intervjuade uppger att säkerhetschefen och it-chefen ska medverka vid kommunstyrelsens sammanträde under våren 2024 för att informera om arbetet kring informationssäkerhet samt redogöra för hur arbetet avser att se ut under året. Intervjuade uppger att arbetet kommer att utgå från den åtgärdslista som togs fram med anledningen av revisionens tidigare granskning av informationssäkerhet.

Kommunstyrelsen har erhållit kontinuerlig återrapportering angående omorganisationen av gemensam it-drift för Hälsinglands kommuner via punkten kommunchefen informerar.

3.6.3 Bedömning

Vår bedömning är att det inte finns en tillräcklig uppföljning och återrapportering av kommunens informationssäkerhetsarbete.

Bedömningen baseras på att det i kommunen saknas ett etablerat uppföljningsarbete. Det är av stor vikt att kommunstyrelsen erhåller kontinuerlig återrapportering så att styrelsen erhåller underlag för att kunna fatta beslut om erforderliga åtgärder i syfte att stärka kommunens robusthet.

4 Samlad bedömning och rekommendationer

Syftet med granskningen har varit att bedöma om kommunstyrelsen tillsett att ett systematiskt informationssäkerhetsarbete bedrivs.

Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsen inte tillsett ett systematiskt informationssäkerhetsarbete.

Vi kan konstatera att flera av de iakttagelser som gjordes i granskningen år 2018 fortfarande är aktuella även i den här granskningen. Då kommunens arbete är i en etableringsfas och då det till stora delar saknas systematik i det arbete som bedrivs, är vår bedömning att kommunstyrelsen har brustit i sitt ansvar avseende informationssäkerhetsarbetet. Kommunstyrelsen har inte i tillräcklig utsträckning utifrån tidigare genomförd granskning följt upp arbetet utifrån den åtgärdsplan som styrelsen beslutat om.

Det saknas, utöver policyn, styrande och vägledande dokument som reglerar bland annat informationsklassning, riskhantering samt incidenthantering. Därtill anser vi att nuvarande riskbedömning inte är tillräcklig för att identifiera eventuella hot och oönskade händelser. Det finns behov av både en kommunövergripande samt verksamhetsövergripande riskanalys där informationssäkerhetsrisker är det primära perspektivet samt arbete med att klassa informationstillgångar. En väl genomförd riskbedömning är nödvändig för att det ska vara möjligt för kommunen att prioritera och vidta effektiva åtgärder.

Vi gör även bedömningen att kommunen saknar dokumenterad styrning om hur uppföljningsarbetet kring informationssäkerhetsarbetet ska se ut.

Utifrån resultatet av vår granskning rekommenderar vi kommunstyrelsen att:

- Anta upprättade riktlinjer och säkerställ att de implementeras i organisationen.
- Upprätta mål med tillhörande handlingsplaner för informationssäkerhetsarbetet.
- Säkerställ att en kommungemensam modell för riskbedömning och informationsklassning etableras samt att riskbedömning av kommunens informationstillgångar genomförs.
- Säkerställa att identifierade behov av åtgärder genomförs samt att nuvarande åtgärdsplan revideras utifrån aktualiserade riskbedömningar.
- Säkerställ att utbildningsinsatser genomförs bland samtliga medarbetare.
- Säkerställ att incidentrutiner upprättas som omfattar eskaleringsvägar samt former för hur inträffade incidenter ska analysera och dokumenteras.
- Säkerställ att former för uppföljning av informationssäkerhetsarbetet upprättas.
- Säkerställ att kommunstyrelsen erhåller kontinuerlig återrapportering avseende kommunens informationssäkerhetsarbete.

Ljusdals kommun
Granskning av informationssäkerhet

2024-06-10

Datum som ovan

KPMG AB

Mikael Lindberg
Certifierad kommunal yrkesrevisor

Jenny Thörn
Verksamhetsrevisor

Ida Larsson
Verksamhetsrevisor

Cecilia Stelin
Verksamhetsrevisor

A Metodstöd för systematiskt informationssäkerhetsarbete och säkerhetsåtgärder

Som revisionskriterium i granskningen utgår vi från MSB:s metodstöd och rekommendationer för ett systematiskt informationssäkerhetsarbete och säkerhetsåtgärder med fokus på nedanstående områden.

Standard och krav

Metodstödet bygger på de internationella standarderna för informationssäkerhet i ISO/IEC 27000-serien och då främst på SS-EN ISO/IEC 27001 och SS-EN ISO/IEC 27002 om ledningssystem för informationssäkerhet.

Ledningssystem för informationssäkerhet

Ett ledningssystem för informationssäkerhet (ofta förkortat LIS) är den del av ledningssystemet som styr verksamhetens informationssäkerhet. För att informationssäkerhetsarbetet ska lyckas och vara framgångsrikt är det viktigt att informationssäkerheten integreras med de olika styrformerna, som planering och uppföljning. Det innebär till exempel att ledningen löpande informerar sig om informationssäkerhetsarbetet, gör regelbundna verksamhetsplaneringar och kontroller samt ser över styrdokumenten med jämna mellanrum. Ledningen bör också se till att organisationen antar en policy för informationssäkerhetsarbetet. I ytterligare styrdokument, riktlinjer och liknande kan sedan den högsta ledningen ge vägledning till chefer och övriga medarbetare om vilka krav som ställs i arbetet. Det är viktigt att alla i en organisation känner till och förstår innehållet i policys och riktlinjer.

Ansvar och organisation

Metodstödet beskriver hur ansvaret för arbetet med informationssäkerhet bör fördelas i organisationen samt tydliggör betydelsen av ledningens förståelse och engagemang i informationssäkerhetsarbetet för att det ska lyckas. Det bör finnas en person inom organisationen med ansvar för att samordna informationssäkerhetsarbetet. Grundprincipen är att ansvaret för informationssäkerhetsarbete ska följa det ordinarie verksamhetsansvaret från ledning ner till enskilda medarbetare. Informationssäkerhetssamordnaren har därmed inget formellt ansvar för informationssäkerheten utan ska verka som ett stöd för att den övriga organisationen innefattande ledning, chefer och medarbetare tar sitt ansvar för informationssäkerhet i verksamheten. Det är viktigt att tydligt klargöra informationssäkerhetssamordnarens roll och vilket mandat och rapporteringsplikt som ska ingå i rollen.

Utbildning och kommunikation

MSB:s metodstöd ställer krav om ständig utbildning och kommunikation för att höja medvetenheten och kunskapen om informationssäkerhet. Utbildning och kommunikation ökar också acceptansen av och förståelsen för de säkerhetsåtgärder som implementeras.

Riskanalys och informationsklassning

Genom en riskanalys ska verksamheten identifiera de hot och oönskade händelser som kan leda till negativa konsekvenser för organisationen. Riskanalyser kan göras verksamhetsövergripande, för en process eller för ett enskilt objekt. Risker och potentiella händelser som kan leda till negativa konsekvenser beskrivs och bedöms sedan avseende sannolikheten att de inträffar samt potentiella konsekvenser.

Metodstödet anger vidare att informationsklassning är 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. Skyddsnivåerna beskriver säkerhetsåtgärder som informationens värde kräver. Identifierat behov av säkerhetsåtgärder utgör ett viktigt underlag vid exempelvis kravställning av tjänster, som interna och externa it-tjänster. De identifierade behoven av säkerhetsåtgärder bör dokumenteras i en åtgärdsplan. IT-säkerhetsåtgärder rent tekniskt kan vara en del men klassningen kan även ha identifierat behov av kompletterande risk- och konsekvensanalyser, förbättrade rutiner eller andra åtgärder som bedöms nödvändiga för att säkerställa säkerheten för informationstillgångarna.

Uppföljning och förbättringsarbete

För att ledningen på strategisk nivå ska få en samlad bild och kunskap om informationssäkerhetsarbetet i kommunen behöver det ske en kommunövergripande uppföljning av arbetet som sedan rapporteras under ledningens genomgång. Uppföljningen utgör även underlag för eventuella beslut på strategisk nivå angående åtgärder och resursfördelning. Resultatet från ledningens genomgång ska dokumenteras och bevaras.

Interna styrdokument

Enligt MSB bör ledningen se till att organisationen antar en policy för informationssäkerhetsarbetet. I ytterligare styrdokument, riktlinjer och liknande kan ledningen ge vägledning till chefer och övriga medarbetare över de krav och förhållningssätt som gäller i informationssäkerhetsarbetet.

I riktlinjer är det vanligt att det förs in bestämmelser om till exempel:

- användning av internet och e-post
- åtgärder till skydd mot skadlig kod
- fysisk säkerhet • incidenthantering
- kontinuitetsplanering
- mobilt arbete
- inventarier och licenser
- behörighetsadministration
- loggning

Det är viktigt att alla i en organisation känner till och förstår innehållet i policys och riktlinjer. Erfarenheten visar tydligt vikten av att anställda uppvisar ett säkert beteende i sitt dagliga arbete.