Förstudie avseende informationssäkerhetsarbetet

Rapport

Leksands kommun

KPMG AB

2021-03-24

Antal sidor 14

Leksands kommun
Förstudie avseende informationssäkerhetsarbetet

2021-03-24

Innehållsförteckning

Leksands kommun
Förstudie avseende informationssäkerhetsarbetet

2021-03-24

1 Sammanfattning

KPMG har av de förtroendevalda revisorerna i Leksands kommun fått i uppdrag att genomföra en förstudie av kommunens informationssäkerhetsarbete. Uppdraget ingår i revisionsplanen för 2020.

Resultatet av förstudien är att kommunstyrelsen inte har säkerställt att det finns ett systematiskt och riskbaserat informationssäkerhetsarbete. Vi noterar ett flertal områden där arbetet inte når upp till de rekommendationer som finns i enlighet med ISO 27001-standarden som kommunens informationssäkerhetspolicy uttrycker ska gälla för kommunens informationssäkerhetsarbete.

De väsentligaste iakttagelserna är:

- Det saknas riktlinjer som kan tydliggöra hur arbetet med informationssäkerhet ska bedrivas i kommunen och som konkretiserar det policyn anger.
- I nuläget finns inte en ändamålsenlig organisation för informationssäkerhets-frågorna. Den centralt utsedda informationssäkerhetssamordnaren har vid sidan om uppdraget andra viktiga funktioner inom kommunen. Vi ser en svårighet att få tillräckligt med resurser i form av tid för att upprätta ett mer systematiskt informationssäkerhetsarbete där verksamheterna behöver stöd i att ta sig an frågorna.
- Arbetet med informationsklassning och riskbedömning för kommunens informationstillgångar är i en uppstartsfas och har endast genomförts för ett fåtal system. Vi anser därför inte att det sker ett systematiskt arbete med att identifiera och analysera behov och risker för att säkerställa informationssäkerheten.
- Det finns inte tillräcklig kunskap om informationssäkerhetsincidenter då ingen grundläggande utbildning har erbjudits kommunens medarbetare och förtroendevalda. Det saknas i rutiner för hur incidenter, om de upptäcks, ska hanteras.

Vi rekommenderar kommunstyrelsen att:

- Ge informationssäkerhetssamordnaren i uppdrag att genomföra en nulägesanalys i enlighet med MSB:s metodstöd för informationssäkerhet. Utifrån nulägesanalysen kan kommunstyrelsen få kunskap om vilka åtgärder som bör prioriteras för att arbetet ska ske på ett mer systematiskt sätt så att kommunens informationstillgångar hanteras och skyddas tillräckligt.

  Vi anser att mål- och handlingsplan är viktiga instrument för att säkerställa att arbetet får tillräckliga resurser i genomförandet och en acceptans i verksamheten så att var och en tar sitt ansvar i enlighet med beslutad policy.

2 Bakgrund

KPMG har av Leksands kommuns förtroendevalda revisorer fått i uppdrag att genomföra en förstudie av kommunens arbete med informationssäkerhet. Uppdraget ingår i revisionsplanen för år 2020.

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. Brister i hanteringen kan leda till förtroendeskada för organisationen.

Informationssäkerhet innebär att skydda information utifrån krav på dess konfidentialitet, riktighet och tillgänglighet och måste skyddas mot obehörig åtkomst, såväl externt som internt. Vidtagna IT-säkerhetsåtgärder ska stå i relation till informationstillgångarnas värde och de risker och behov som ansvariga för informationen har fastställt. Detta då IT-säkerheten avser att säkra och trygga driften och hanteringen av kommunens kärnverksamheter.

Hotbilden med risker för intrång förändras kontinuerligt och säkerhetsarbetet behöver därför vara en ständigt pågående process för att säkerställa att kommunens informationstillgångar har ett tillräckligt skydd. För att kunna hantera det på ett ändamålsenligt sätt krävs att kommunen har ett systematiskt informations-säkerhetsarbete där flera funktioner i kommunen är involverade och rätt organiserade för uppdraget.

Med anledning av ovanstående drar kommunens revisorer slutsatsen i sin riskanalys, att arbetet med informationssäkerheten behöver utvärderas.

2.1 Syfte, revisionsfråga och avgränsning

Syftet med förstudien är att genom inhämtning av information ge en översiktlig nulägesanalys om kommunstyrelsen i Leksands kommun har tillsett att arbetet med informationssäkerhet med fokus på styrning, organisation och incidenthantering är ändamålsenligt.

Förstudien ska besvara följande frågor:

- Finns aktuella styrande dokument som tydliggör vilka krav som ställs och hur arbetet ska bedrivas?
- Finns en ändamålsenlig organisation för att arbeta med informationssäkerhetsfrågorna? Är ansvaret känt och accepterat hos verksamheten?
- Finns ett systematiskt arbete med att identifiera och analysera behov och risker för att säkerställa informationssäkerheten?
- Finns kunskap om informationssäkerhetsincidenter och rutiner för hur dessa ska hanteras och rapporteras?

2.2 Avgränsning

De iakttagelser som presenteras i denna förstudie baseras på den information som inhämtats under intervjuer och genom granskning av erhållen dokumentation, såsom styrdokument, riktlinjer och planer. Förstudien är avgränsad till att ge en översiktlig bild av området för att bedöma om det finns behov av en fördjupad granskning av arbetet.

Förstudien avser revisionsåret 2020.

2.3 Revisionskriterier

Vi har bedömt om rutinerna uppfyller:

- Kommunallagen 6 kap. 6 §
- Tillämpbara interna regelverk, policys och beslut
- MSB:s rekommendationer avseende Ledningssystem för informationssäkerhet
- NIS-direktivet i tillämpliga delar avseende kartläggning och analys av risker

2.4 Metod

Förstudien har genomförts genom dokumentstudier och intervjuer/avstämningar med berörda tjänstemän.

Förstudien har genomförts av Jenny Thörn, verksamhetsrevisor under ledning av Nils Nordqvistcertifierad kommunal revisor som deltar i förstudien utifrån sin roll som kundansvarig.

Samtliga intervjuade har getts möjlighet att faktagranska rapporten.

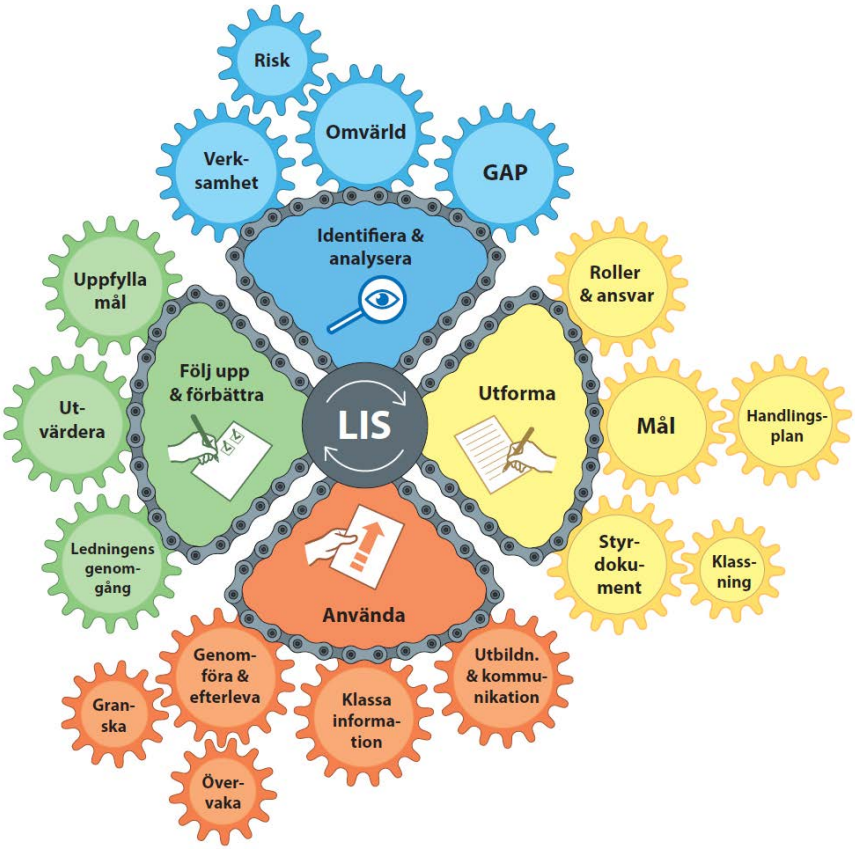
3 Inledning

Myndigheten för samhällsskydd och beredskap (MSB) ansvarar, i den utsträckning som ingen annan myndighet bär ansvaret, för frågor om skydd mot olyckor, krisberedskap och civilt försvar. Ansvaret avser åtgärder före, under och efter en olycka, kris, krig eller krigsfara. Inom området för informationssäkerhet innefattar MSB:s uppgifter bland annat att vara råd-och stödgivande i informationssäkerhetsarbetet, ansvara för utveckling och förvaltning av säkra kommunikationer samt hantera samt förebygga IT-incidenter.

3.1 Metodstöd för systematiskt informationssäkerhetsarbete

MSB har tagit fram ett metodstöd till organisationer avseende informationssäkerhetsarbetet. Metodstödet är baserat på den internationella standardserien för informationssäkerhet, ISO/ IEC 27000 och ämnar till att förtydliga hur informationssäkerhetsarbetet kan utformas. Metodstöd riktar sig till personer som arbetar med informationssäkerhet i en organisation.

Metodstödet består av fyra olika metodsteg för informationssäkerhetsarbetet vilka illustreras i nedanstående figur.



4 Resultat av förstudien

Vi har i förstudien valt att utgå från MSB:s rekommendationer för ett systematiskt informationssäkerhetsarbete[1] och utifrån detta gjort en analys av nuläget för Leksands kommuns informationssäkerhetsarbete i förhållande till de delar som bör ingå enligt metodstödet.

4.1 Steg 1, Identifiera och analysera

Syftet med det första steget, identifiera och analysera, är enligt MSB att säkerställa att informationssäkerheten utformas utifrån verksamhetens rådande förutsättningar. Det innebär att genom omvärldsanalys, verksamhetsanalys, riskanalys och GAP-analys fastställa bland annat vilka externa intressenter, legala krav och övriga förutsättningar som finns som påverkar informationssäkerheten. Det ska även leda till att väsentliga informationstillgångar identifieras, vilka risker de ska skyddas mot, samt valda säkerhetsåtgärder.

Iakttagelser

Vi noterar att kommunen inte på något strukturerat sätt har genomfört de analyser som utgör det första steget i arbetet med informationssäkerhet enligt MSB:s rekommendationer för ett systematiskt informationssäkerhetsarbete.

Riskanalys har till viss del genomförts utifrån dataskyddsförordningens krav vilket utgör en del av de legala krav som kommunen har att efterleva. Det har även till viss del gjorts en analys av omvärldsfaktorer för informationshantering vid lagring i molntjänster.

Vi anser dock att det finns ytterligare aspekter som behöver analyseras för att utformningen av informationssäkerhetsarbetet ska kunna genomföras.

[1] *Metodstöd för systematiskt informationssäkerhetsarbete*, publicerat mars 2019, hämtat från metodstod_systematiskt_informationssakerhetsarbete_oversikt_msb.pdf

4.2 Steg 2, Utforma

Enligt MSB:s metodstöd behövs följande delar för ett systematiskt informationssäkerhetsarbete:

- Organisation
- Ledning och styrning
- Informationssäkerhetsmål
- Styrdokument
- Klassningsmodell
- Välj säkerhetsåtgärder och skapa skyddsnivåer
- Handlingsplan
- Kontinuitetshantering för informationstillgångar
- Incidenthantering

Hur delarna ska utformas beror på resultaten i det första metodsteget Identifiera och analysera. Som helhet bör dessa leda till strategiska informationssäkerhetsmål och beskrivning av roller i säkerhetsarbetet under avsnittet organisation.

Iakttagelser

Avseende steg 2 har vi gjort följande iakttagelser avseende hur kommunen har utformat sitt informationssäkerhetsarbete inom de nio områden som MSB anger i metodstödet.

Organisation

Enligt MSB:s rekommendationer är grundprincipen att ansvaret för själva informationssäkerhetsarbetet ska följa det ordinarie verksamhetsansvaret. Detta gäller ända från ledning ner till enskilda medarbetare. Denna princip innebär att den person som är ansvarig för ett visst verksamhetsområde också är ansvarig för själva informationssäkerheten inom det specifika området. En verksamhet kan bedrivas i en organisatorisk del (till exempel avdelning, sektion eller enhet), ett löpande arbetsflöde (till exempel process) eller ett tidsbegränsat arbete (till exempel projekt).

Ledningens förståelse för och engagemang i informationssäkerhet är grundläggande för att lyckas. Med andra ord måste ledningen få kunskap om hur de kan leda och styra verksamheten på ett effektivt sätt för att åstadkomma god informationssäkerhet. Ledningens stöd är också oumbärligt för att frågan ska få acceptans och ett engagemang från andra roller i organisationen.

De personer som arbetar specifikt med informationssäkerhet har en viktig stödfunktion i sin organisation – ungefär på samma sätt som de personer som har stödfunktioner inom andra verksamhetsområden, som ekonomi, personal (hr) eller kommunikation. Dessa personer ansvarar för att själva arbetet med informationssäkerhet fungerar på ett lämpligt sätt. De ska däremot inte ha ett formellt ansvar för informationssäkerheten, utan det huvudsakliga syftet med detta ansvar och arbete är i stället att stötta ledningen, verksamhetscheferna och medarbetarna.

Vi har noterat att roller och ansvar är väl beskrivna i *Informationssäkerhetspolicyn*[2] där följande sju roller finns angivna:

Medarbetare: Medarbetare har ett ansvar att följa de två styrdokumenten samt vara uppmärksam på incidenter och brister om informationssäkerheten samt informera IT-helpdesk om sådana.

Ledningar: Ledningar avser kommunfullmäktige, kommunstyrelse och utskott, vilka ytterst ansvarar för informationssäkerheten i verksamheten som bedrivs inom deras respektive verksamhetsområden.

Verksamhetsansvariga: Verksamhetsansvariga bär ansvaret för informationssäkerheten inom sin verksamhet. Ansvaret innefattar att tillse att ens medarbetare har ett säkerhetsmedvetande och tillräcklig förståelse och kunskap för att en erforderlig nivå av informationssäkerhet i verksamheten kan uppnås.

Systemägare: Systemägare beskrivs ansvara för att verksamhetssystem efterlever de två styrdokumenten. I deras ansvar ingår att besluta om verksamhetssystemets informationssäkerhetsnivåer genom klassning i KLASSA-systemet.

Systemförvaltare: Systemförvaltare bär ansvaret över att systemets informationssäkerhetsrelaterade åtgärder och mål nås samt genomförs.

IT-chef (Systemägare IT): IT-chefens ansvar är att samordna säkerhetsarbetet i kommunens IT-miljö. Hen har även tillsynsansvar för att IT-miljö är tillförlitlig och motsvarar interna och externa krav.

Informationssäkerhetsamordnare: Samordnarna har det strategiska och övergripande ansvaret att utveckla, leda och samordna informationssäkerhetsarbetet.

Vi noterar att ansvaret enligt policyn följer det ordinarie verksamhetsansvaret. Det finns i kommunen en informationssäkerhetssamordnare som rapporterar till biträdande kommundirektör. Nuvarande informationssäkerhetssamordnare har även andra uppdrag vid sidan om samordnarrollen vilket innebär att del av tjänsterna rapporteras till andra överordnade chefer. I kommunen finns en enhet för säkerhet och beredskap där informationssäkerhetsfrågorna är organiserade.

Vid intervju framgår att det i nuläget inte finns några ytterligare funktioner utsedda att praktiskt genomföra och utveckla informationssäkerheten i respektive verksamhet som en del i linjeansvaret. Däremot finns utsedda arkivredogörare och dataskyddsredogörare som tidigare träffats regelbundet i nätverk. Det har dock inte

[2] Beslutad i kommunfullmäktige 2018-10-16 § 12 Dnr 2018/1107

varit så aktivt på senare tid. Informationssäkerhetssamordnarens kontakt med avdelningarna sker främst genom systemförvaltare där sådana finns.

Ledning och styrning

Vi noterar att informationssäkerhetssamordaren i organisationsskiss är underordnad IT-chef. Informationssäkerhet är överordnat IT-säkerhet vilket innebär att placeringen riskerar att samordnaren kan få svårigheter att hålla sig opartisk genom närheten till strategisk IT-funktion. Detta så informationssäkerhetssamordnaren genom sitt arbete är kravställare till IT av säkerhetsåtgärder. Det är även samordnaren som har till uppgift att granska så att verksamheten efterlever de lagar och interna styrdokument som finns och behöver i det uppdraget ha en position nära högsta ledningen för att upprätthålla ett oberoende och ha mandat i organisationen.

Det finns i nuläget inget implementerat Ledningssystem för informationssäkerhet, ett så kallat LIS. Det finns inte heller någon plan för att implementera detta. I intervjuer beskrivs att det finns en organisation och styrning genom systemförvaltningsarbetet vilket även är tänkt att omfatta informationssäkerhetsarbetet.

Informationssäkerhetsmål

I informationssäkerhetspolicyn framgår sex mål för informationssäkerhetsarbetet. Vi har dock noterat att dessa mål inte konkretiseras så att det finns en handlingsplan eller liknande för vilka aktiviteter som behöver genomföras för att nå målen. Utan detta finns inte tillräckliga underlag för att följa upp och utvärdera informationssäkerhetsarbetet samt besluta om prioriterade åtgärder.

Styrdokument

Genom våra dokumentstudier har vi kunnat konstatera att kommunen har två styrdokument för informationssäkerhet och dataskydd, *Informationssäkerhetspolicy*och *Riktlinjer för hantering av personuppgifter*[3].

Informationssäkerhetspolicy utgör ett övergripande dokument på nio sidor som inbegriper information om begreppet informationssäkerhet, informationssäkerhetsmålen, principer och arbetssätt, roll-och ansvarsfördelningen för informationssäkerhetsarbetet i kommunen samt kommunens arbete med uppföljning och rapportering.

Det framgår även att informationssäkerhet inte är begränsat till säkerhet i IT-system utan inkluderar även information i alla typer av former oavsett hur informationen kommuniceras, bearbetas och lagras. Policyn listar även sex informationssäkerhetsmål där det beskrivs att kommunen bland annat ska upprätthålla och uppnå en informationssäkerhet som innebär en robust, säker och tillförlitlig informationshantering.

[3] Daterad 2020-05-12

Av policyn framgår att det även ska finnas underliggande riktlinjer för informationssäkerhet. Dessa saknas enligt uppgift.

Riktlinjer för hantering av personuppgifter består av tio sidor och avser att konkretisera policyn och ge råd och vägledning vid hantering av personuppgifter i kommunen. Styrdokument ska också förtydliga ansvarsförhållandena rörande personuppgiftsbehandling. Riktlinjerna är detaljerade och det framgår bland annat hur personuppgifter på webben ska hanteras, vad som gäller vid fotografering och publicering av bilder, hur rapportering av personuppgiftsincidenter ska genomföras samt rutiner vid begäran/begränsning av personuppgiftsbehandlingar. Det finns en även en detaljerad lista som innefattar aktörers roller och ansvar i och med kommunens dataskyddsarbete.

Av intervjuer framkommer att informationssäkerhetspolicyn inte har implementerats i verksamheten.

Klassningsmodell

I informationssäkerhetspolicyn framgår i avsnittet om principer och arbetssätt att kommunen ska arbeta på ett sådant sätt att informationssäkerhetsmålen uppfylls. Arbetet med informationssäkerhet ska vara stödjande, normerande och kontrollerande mot kommunens verksamheter. Det framgår även att kommunen ska tillämpa informationsklassning och att modellen för detta är SKR:s KLASSA.

Verktyget KLASSA beskrivs även på kommunens intranät.

Välj säkerhetsåtgärder och skapa skyddsnivåer

Vi uppfattar genom intervjuer att de IT-säkerhetsåtgärder som vidtagits sker utifrån IT-avdelningens kunskap och förutsättningar. Verksamheterna har inte själva efter riskbedömning och behov av åtgärder gjort några val och kravställt åtgärder till IT.

Sektorn för bildning upplever att de saknar tekniska lösningar i sina system eller i kommunens IT-miljö som möjliggör att de skulle kunna använda flerfaktorautentisering[4]. Detta skulle på många sätt utveckla deras informationshantering och säkerhet som i nuläget i stora delar behöver ske manuellt genom analoga blanketter och personakter för elever.

Sociala sektorn har infört flerfaktorautentisering inom hemtjänsten. Därtill har ett flertal säkerhetsåtgärder genomförts genom e-tjänstekort för legitimerad personal, vissa inom socialtjänsten, ekonomer mm. En kontroll genomförs innan behörigheter tilldelas där uppgifter i kommunens AD[5] stäms av mot de behörighet som ska tilldelas.

[4] En förstärkt inloggning för att öka säkerheten istället för att endast nyttja användarnamn och lösenord, det kan ske via sms, bank-ID eller liknande beroende på val av tjänst.
[5] Active Directory, en katalog över alla IT-objekt i kommunen från vilken övergripande behörighet och användarkonton styrs.

Handlingsplan

Det saknas i nuläget upprättad handlingsplan på övergripande nivå över vilka åtgärder och aktiviteter som behöver genomföras i kommunens informationssäkerhetsarbete. I intervjuer beskrivs att arbetet är i uppstartsfas och att inledande möten ska ske med systemförvaltare för att utveckla arbetet genom dessa.

Handlingsplaner för informationssäkerheten i system och för verksamhetens informationstillgångar saknas.

Kontinuitetshantering för informationstillgångar

I policyn saknas information och krav om kontinuitetshantering för informationstillgångar. I stora delar saknas kontinuitetsplaner för verksamhetens informationstillgångar, sociala sektorn anger att de har upprättat detta. Vi har efterfrågat dokumentation men har i förstudien inte getts möjlighet att ta del av denna dokumentation.

Incidenthantering

Det framgår av intervju att det i arbetet med informationssäkerhet saknas rutiner för hantering av informationssäkerhetsincidenter och IT-incidenter.

Det finns rutiner för personuppgiftshantering. Rapporter om personuppgiftsincidenter skickas till dataskyddsombud för bedömning och vidare hantering. Det anges dock fortfarande finnas ett mörkertal i hur många incidenter som upptäcks och rapporteras.

Det har enligt intervjuperson inte skett något aktivt arbete med att informera verksamheten om vad som är informationssäkerhetsincidenter och hur dessa ska hanteras. I nuläget anmäls de incidenter som upptäcks till IT men det är okänt vad som händer med dessa efter att de har anmälts. Incidenter som inträffat är bland annat virus, phisingmail i syfte att få tag i kontouppgifter mm eller annan otillåten användning av IT-utrustning.

4.3 Använda

När verksamheten har utformat styrningen ska det tillämpas. Det innebär:

- Kontinuerligt arbete med att klassa organisationens information för att identifiera känslig och kritisk information för att kunna säkerställa tillräckligt skydd.
- Genomföra och efterleva de handlingsplaner och styrdokument som avser informationssäkerhetsarbetet
- Utbilda och kommunicera informationssäkerhetsfrågor till organisationens medarbetare. Det är ständigt pågående arbete som är nödvändigt för att skapa ett systematiskt informationssäkerhetsarbete.

Iakttagelser

Vi har genom våra intervjuer noterat att det inte sker något systematiskt arbete med riskanalyser och informationsklassning.

Sociala sektorn anger i sina svar att de har genomfört informationsklassning och riskbedömt sina informationstillgångar, vi har dock inte erhållit efterfrågade exempel på detta arbete för att kunna bedöma i vilken utsträckning det har genomförts. I svaren anges att det vid klassningen deltar flertalet aktörer, däribland kommunens IT-avdelning, IT-chef och IT- tekniker. Utifrån den genomförda klassning och riskbedömning har tvåfaktorsinloggning införts i hemtjänsten samt e-tjänstekort för legitimerad personal och för vissa handläggare. Dessutom behöver nu personal legitimera sig vid uthämtande av nycklar mm.

Arbetet anges av övriga intervjupersoner vara i en uppstartsfas och har bland annat genomförts inför upphandling av nya verksamhetssystem så att en kravställning kan ske utifrån bedömda behov.

Vi noterar att det arbete som i övrigt genomförts till stor del har varit i samband med det dataskyddsarbete som kommunen genomfört tillsammans med tekniska säkerhetsåtgärder som upprättats av IT-avdelningen.

Det saknas handlingsplaner och styrdokumenten är inte implementerade så att det går att följa upp i vilken utsträckning dessa efterlevs.

Det framgår vidare att det inte har organiserats några informations- och utbildningsinsatser för medarbetare och förtroendevalda för att uppnå en medvetenhet och grundläggande kunskap om informationssäkerhet. Inom dataskydd har utbildningar däremot hållits på varje skola men i intervjuer beskrivs trots detta verksamheten osäkra över hur information får hanteras och att detta i vissa fall leder till en ineffektiv och omständlig process.

4.4 Följa upp och förbättra

Informationssäkerhetsarbetet ska utvärderas och följas upp för att säkerställa arbetets fortsatta lämplighet, tillräcklighet och verkan. Det kan enligt MSB ske genom övervakning, mätning och måluppföljning.

Iakttagelser

I *Informationssäkerhetspolicyn* framgår viss information om uppföljning och rapportering. Det framgår att efterlevnaden av båda styrdokumenten ska följas upp på regelbunden basis. Det är informationssäkerhetssamordnaren som varje år ska rapportera status och läge gällande informationssäkerhet till kommundirektören och allmänna utskottet. Särskilda skäl kan motivera att fler rapporteringar genomförs, till exempel allvarliga incidenter, behov och brister.

Vid intervju beskrivs att kommunen inte följer upp efterlevnad av styrdokument, varken via till exempel intern kontroll eller interna revisioner. Plan för rapportering beskrivs

också saknas och den återrapportering som sker i nuläget är inom dataskydd där en rapportering sker till ledningsgruppen två gånger per år. Vi anser att rapporteringsvägar bör upprättas till kommunstyrelsen eller dess utskott så att frågorna i enlighet med MSB:s rekommendationer har ledningens engagemang och förståelse. Detta är avgörande för att informationssäkerhetsfrågorna ska få acceptans av övriga funktioner i kommunen.

5 Sammanfattande iakttagelser och rekommendationer

Utifrån de frågeställningar som förstudien avser att besvara är våra sammanfattande iakttagelser följande:

Finns aktuella styrande dokument som tydliggör vilka krav som ställs och hur arbetet ska bedrivas?

Det finns en informationssäkerhetspolicy som innehållsmässigt överensstämmer med rekommendationer från MSB. Den är beslutad 2018 och anses därigenom vara tillräckligt uppdaterat för att kunna tillämpas. Den rekommenderade livslängden på en informationssäkerhetspolicy är 3–5 år enligt MSB.

Vi saknar däremot underliggande riktlinjer som kan tydliggöra hur arbetet med informationssäkerhet ska bedrivas i kommunen. Dessa kan med fördel målgruppsanpassas så att de är lätta att ta till sig för verksamhetsföreträdare. Exempel på målgrupper kan vara: förvaltning, användare, IT-organisation. Detta behöver dock organisationen själva ta ställning till.

Finns en ändamålsenlig organisation för att arbeta med informationssäkerhetsfrågorna? Är ansvaret känt och accepterat hos verksamheten?

I nuläget finns inte en ändamålsenlig organisation för informationssäkerhetsfrågorna. Den centralt utsedda informationssäkerhetssamordnaren har vid sidan om uppdraget andra viktiga funktioner inom kommunen. Vi ser en svårighet att få tillräckligt med resurser i form av tid för att upprätta ett mer systematiskt informationssäkerhetsarbete där verksamheterna behöver stöd i att ta sig an frågorna. I nuläget finns inga representanter förutom systemförvaltarna och det behöver tydliggöras hur ansvarsfördelning för arbetet ska se ut och vilka delar i arbetet som systemförvaltarna ska ansvara för.

Finns ett systematiskt arbete med att identifiera och analysera behov och risker för att säkerställa informationssäkerheteten?

Kommunen har en beslutad modell för informationsklassning vilket är positivt. Arbetet med informationsklassning och riskbedömning för kommunens informationstillgångar är dock i en uppstartsfas och har endast genomförts för ett fåtal system. Vi anser därför inte att det sker ett systematiskt arbete med att identifiera och analysera behov och risker för att säkerställa informationssäkerheten. I nuläget baserar inte IT-säkerhetsåtgärderna på en bedömning av risker och det kan därigenom inte fastställas att nuvarande skyddsåtgärder står i relation till hur skyddsvärd informationen är. Det kan riskera att informations skyddas med för höga säkerhetsåtgärder och därigenom är kostnadsdrivande eller att det finns för låg säkerhet för information som hade behövt en högre säkerhet.

Finns kunskap om informationssäkerhetsincidenter och rutiner för hur dessa ska hanteras och rapporteras?

Det finns inte tillräcklig kunskap om informationssäkerhetsincidenter då ingen grundläggande utbildning har erbjudits kommunens medarbetare och förtroendevalda. Det saknas i rutiner för hur incidenter, om de upptäcks, ska hanteras.

5.1 Rekommendationer

Vi rekommenderar kommunstyrelsen att:

- Ge informationssäkerhetssamordnaren i uppdrag att genomföra en nulägesanalys i enlighet med MSB:s metodstöd för informationssäkerhet. Utifrån nulägesanalysen kan kommunstyrelsen få kunskap om vilka åtgärder som bör prioriteras för att arbetet ska ske på ett mer systematiskt sätt så att kommunens informationstillgångar hanteras och skyddas tillräckligt.

  Vi anser att en mål- och handlingsplan är viktiga instrument för att säkerställa att arbetet får tillräckliga resurser i genomförandet och en acceptans i verksamheten så att var och en tar sitt ansvar i enlighet med beslutad policy.

2021-03-24

KPMG AB

Jenny Thörn	Nils Nordqvist
Kommunal revisor	Certifierad kommunal revisor