Styrning och ledning av informationssäkerhet

PM

Köpings kommun

KPMG AB

2022-03-08

Antal sidor 8

Antal bilagor 1

Köpings kommun
Styrning och ledning av informationssäkerhet

2022-03-08

Innehållsförteckning

1 Sammanfattning

Vi har av Köpings kommuns revisorer fått i uppdrag att granska kommunens informationssäkerhetsarbete. Uppdraget ingår i revisionsplanen för år 2021.

Syftet med granskningen har varit att bedöma hur mogen kommunen är inom viktiga områden för att säkerställa ett tillräckligt informationssäkerhetsarbete.

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunen inte är tillräckligt mogen i sitt informationssäkerhetsarbete där vi saknar ett flertal av de aktiviteter som rekommenderas av MSB för att arbetet ska vara systematiskt och riskbaserat.

Kommunens informationssäkerhetsarbete är i behov av utveckling. Ansvar behöver tydliggöras och resurser tillskapas till funktioner som får i uppdrag att påbörja ett mer strategiskt arbete. Arbetet bör utgå från en nulägesanalys som presenteras för kommunstyrelsen som därefter kan besluta om prioritering, tilldelning av resurser samt krav på åtgärder.

Vi rekommenderar att kommunen tar stöd i de rekommendationer och metodstöd som MSB erbjuder kostnadsfritt för att verksamheter ska etablera ett systematiskt och riskbaserat informationssäkerhetsarbete.

2 Inledning/bakgrund

Vi har av Köpings kommuns revisorer fått i uppdrag att granska att kommunen har säkerställt organisationens styrning och ledning av informationssäkerhetsarbetet. Uppdraget ingår i revisionsplanen för år 2021.

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. Kommunernas arbete med informationssäkerhet påverkas av de lagar och förordningar som finns. Myndigheten för samhällsskydd och beredskap har utifrån ISO 27000- standarden ett antal föreskrifter och metodstöd för att etablera ett ledningssystem för informationssäkerhet i kommunerna och vidta nödvändiga säkerhetsåtgärder.

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 informationssäkerhetsarbete där flera funktioner i kommunen är involverade och rätt organiserade för uppdraget. Ansvaret finns hos var och en och berör hela organisationen varpå medvetenhet är väsentlig för en tillräcklig efterlevnad. Det är därför väsentligt att granska hur medveten och mogen organisationen är för att styra och leda sitt informationssäkerhetsarbete.

Med anledning av ovanstående drar kommunens revisorer slutsatsen i sin riskanalys, att kommunens styrning och ledning av informationssäkerhetsarbetet behöver granskas.

2.1 Syfte, revisionsfråga och avgränsning

Granskningen syftar till att konstatera hur mogen kommunen är inom viktiga områden för att säkerställa ett tillräckligt informationssäkerhetsarbete.

Granskningen ska besvara följande revisionsfrågor:

— Har kommunstyrelsen säkerställt en tillräcklig mognad och medvetenhet i organisationen för ett tillräckligt informationssäkerhetsarbete?

— Har systemet och supportorganisationen en tillräcklig kapacitet?

Granskningen omfattar kommunstyrelsen och samtliga nämnder.

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller

— Tillämpbara interna regelverk, policys och beslut
— ISO 27000-serien, ett ledningssystem för informationssäkerhet, cybersäkerhet och dataskydd
— MSB:s1 rekommendationer avseende Ledningssystem för informationssäkerhet

2.3 Metod

- Granskningen har inletts genom att verksamhetsföreträdare fått svara skriftligt på ett antal frågeställningar. I bilaga 1 redovisas det frågekomplex som har sänts till kommunen och utgör underlag i vår analys.
- Dokumentgranskning av policys, riktlinjer, rutiner eller annan dokumentation som visar hur kommunen bedriver sitt arbete inom informationssäkerhet.
- Muntlig dialog har genomförts med företrädare av förtroendevalda, tjänstepersoner och kommunrevisorerna för att komplettera de skriftliga svaren.
- Detta PM utgör vår analys och bedömning utifrån de svar vi erhållit för de frågeställningar som kommunen fått besvara, de underlag som bifogats svar samt den genomförda muntliga dialogen.

Detta PM har faktakontrollerats av utvalda verksamhetsföreträdare.

Granskningen har genomförts av Jenny Thörn, kommunal revisor och Ida Larsson, kommunal revisor. Karin Helin Lindqvist har deltagit som kvalitetssäkrare i sin roll som kundansvarig i Köpings kommun.

2.4 MSB:s rekommendationer för en stärkt informationssäkerhet i kommunerna

MSB har 2017 presenterat skriftliga rekommendationer (www.informationsäkerhet.se, 2017-01-18) för en stärkt informationssäkerhet i kommunerna. Rekommendationerna baserades på en granskning av kommunernas arbete 2015 som visade att få kommuner hade ett systematiskt informationssäkerhetsarbete.

Då vi i granskningen utgår från MSB:s rekommendationer beskriver vi dessa översiktligt nedan.

1. **Utse en funktion för informationssäkerhet**
   Funktionens placering bör vara direkt underställd den högsta ledningen (kommunledningskontoret).

2. **Ta fram en analys av nuläget i kommunen**
   Gör en övergripande verksamhetsanalys för att få kunskap om organisationens processer, vilken information som hanteras, samt vilket behov av skydd och vilka krav som finns.

3. **Informera ledningen hur nuläget ser ut**
   Visa exempel på reella hot och inträffade incidenter.
   Beakta centrala lagkrav, t.ex. dataskyddsförordningen, som får stor påverkan på hur kommunen hanterar personuppgifter.

4. **Skapa en handlingsplan utifrån nuläget**
   Handlingsplanen bör beslutas av ledningen. Ta fram styrdokument, policy och riktlinjer samt åtgärda de viktigaste bristerna och sårbarheterna

5. **Klassa informationen**
   Identifiera vilken information som hanteras i verksamheten och klassa efter hur allvarliga konsekvenserna skulle bli av bristande informationssäkerhet.

6. **Höj säkerhetsmedvetandet inom kommunen**
   Ge stöd till organisationen så att förmåga att efterleva kraven i framtagna riktlinjer finns. Detta kan ske t.ex. genom utbildning, vägledningar och annan information.

7. **Ta fram informationssäkerhetsrelaterade krav som sedan används vid upphandlingar.** Se till att identifiera krav samt etablera en process för att få med dessa i upphandlingar.

8. **Gör uppföljningar**
   Se över om kommunen efterlever det som står i de framtagna riktlinjerna. Planera in återkommande uppföljning/revison av verksamheten. Resultaten av uppföljning ska ingå som en del av den återkommande rapporteringen till ledningen.

3 Resultat av granskningen

3.1 Iakttagelser

3.1.1 Organisation och styrande dokument

Det framgår av de svar som inkommit från kommunen att en organisation avseende informationssäkerhetsarbetet behöver komma på plats i kommunen då detta i nuläget saknas. Det finns till viss del utsedda representanter i förvaltningarna som på uppdrag av informationsägarna genomför ett praktiskt arbete utifrån interna anvisningar. Det ser olika ut beroende på förvaltning, men exempel som ges i de skriftliga svaren är systemförvaltare och kvalitetsgrupp. I den muntliga dialogen utvecklas bilden av ansvarsfördelning där det framgår att det finns en otydlighet i nuläget som behöver åtgärdas. Kommunledningsförvaltningen har fått i uppdrag att kartlägga hur arbetsfördelningen ser ut i nuläget. Registrator och verksamhetsutvecklare arbetar med frågorna.

Utifrån säkerhetsskyddslagen (som är utanför granskningens avgränsning) finns ett pågående arbete som rör informationssäkerhet. I dialogen beskrivs därtill vikten av att arbeta med informationssäkerhet för att säkerställa digitaliseringsarbetet i kommunen, vilket även kommenterats i digitaliseringsstrategin.

Enligt de skriftliga svaren har webbaserade utbildningar genomförts på förvaltningsnivå avseende GDPR. Kommunen har även planerat in att genomföra en så kallad nano-utbildning inom informationssäkerhet men det var vid tiden för granskningen inte genomfört. Därtill har vissa utbildningsinsatser erbjudits inom offentlighet och sekretess för att säkerställa informationshanteringen.

3.1.2 Arbetsmetoder för riskbedömning och informationsklassning

Av de skriftliga svaren framgår att gällande sekretessuppgifter och vid införande av nya system använder sig kommunen av riskanalyser i syfte att värdera risker och konsekvenser. På ett övergripande plan har kommunen påbörjat ett arbete med riskanalyser avseende informationshantering. Modellen KLASSA används till viss del av IT-avdelningen på förbundet. Det är IT-samordnare som deltar i klassningsarbetet tillsammans med kollegor beroende på vilket system det är.

Mer digitala arbetssätt har medfört vissa avvägningar avseende informationssäkerheten, bland annat avseende Teamsmöten med brukare.

Köpings kommun tilldelar behörighet i systemet efter behov och medarbetarens arbetsuppgift. Av de skriftliga svaren framgår att det finns en delad bild av om rutinerna är dokumenterade eller ej. Tilldelning av behörigheter sker efter genomförd riskanalys då principen inom kommunen är att medarbetarna inte ska ha tillgång till mer information än arbetsuppgifterna kräver. Det framgår av svaren att en del verksamhetssystem loggar aktivitet, men att det saknas rutiner för att kontrollera loggarna. I arbetet med att säkerställa att information inte tilldelas obehörig använder sig kommunen av tvåfaktorsautentisering. Tvåfaktorsautentisering innebär att den som

loggar in behöver identifiera sig på ytterligare sätt utöver sitt lösenord, exempelvis genom en verifieringskod som skickas till personens mobiltelefon.

3.1.3 Incidenthantering

Av de skriftliga svaren uppger kommunen att inträffade incidenter dokumenteras internt genom ett protokoll i kommunens avvikelsesystem. Om en leverantör är inblandad får kommunen en rapport från leverantören. Efter inträffade incidenter har kommunen vidtagit åtgärder som ändrade rutiner både internt och hos leverantörer.

I den muntliga dialogen uppges att det främst är rutin för personuppgifter som är fastställd och känd. Incidenthantering för IT hanteras i stora delar inom VMKF där berörda i kommunen får kännedom om dessa och i vissa delar tar över hanteringen vid behov. För informationssäkerhetsincidenter uppges att rutiner och kunskap behöver utvecklas internt.

Enligt svaren i granskningen har inga allvarligare incidenter inträffat i kommunen och de incidenter som anmälts till tillsynsmyndigheter har inte krävt några större åtgärder.

3.1.4 Kapacitet för support och stöd i arbetet

VMKF har genom avtal inrättat en supportfunktion i form av Helpdesk för IT-frågor. Informationssäkerhet ingår inte i detta ansvar vilket innebär att kommunerna internt behöver upprätta en organisation som kan ge stöd i förvaltningarnas arbete. Vi uppfattar genom de skriftliga svaren och av deltagarna i dialogen att någon sådan funktion inte finns tillgänglig i informationssäkerhetsarbetet.

VMKF och medlemskommunerna har antagit en *Riktlinje för systemförvaltning*[1] som bland annat syftar till att tydliggöra ansvarsfördelning och aktiviteter som behöver genomföras i systemförvaltningsarbetet. I riktlinjerna finns till viss del aktiviteter inom informationssäkerhet beskrivna. Vi uppfattar dock att de aktiviteter som anges i riktlinjen inte genomförs fullt ut.

3.1.5 Bedömning

Vår bedömning är att kommunstyrelsen inte har säkerställt en tillräcklig mognad och medvetenhet i organisationen för ett tillräckligt informationssäkerhetsarbete. Det saknas en tydlighet över hur ansvaret är fördelat och vilka krav som ställs på aktiviteter och åtgärder för att upprätthålla en god informationssäkerhet.

Vår bedömning är att det med nuvarande styrning och organisation inte finns en tillräcklig kapacitet i form av stöd och support internt i kommunen för att bedriva ett systematiskt informationssäkerhetsarbete. Detta har inte heller via avtal eller överenskommelser efterfrågats från extern part, exempelvis VMKF, som har uppdrag inom närliggande områden.

[1] Kommunstyrelsen 2018-06-04

4 Slutsats och rekommendationer

Vår sammanfattande bedömning är att kommunen i nuläget har en bristande mognad i sitt informationssäkerhetsarbete. Vi kan utifrån den information som vi tagit del av i granskningen konstatera att kommunen i stora delar saknar ett systematiskt och riskbaserat informationssäkerhetsarbete. Ett flertal av de grundläggande aktiviteter som MSB rekommenderar för en stärkt informationssäkerhetsförmåga i kommunerna är inte etablerade i nuläget.

Vissa enskilda aktiviteter och åtgärder som tillhör informationssäkerhetsområdet genomförs, vi upplever dock inte att insatser sker utifrån en plan och struktur. Det är inte heller dokumenterat så att det löpande kan följas upp och rapporteras till nämnder och styrelser som i sin tur ges möjlighet att besluta om prioriteringar och resurser. Utbildningsinsatser för att skapa en medvetenhet och kunskap om informationssäkerhet har inte genomförts för varken medarbetare eller förtroendevalda, vi rekommenderar att detta genomförs regelbundet så att enskilda har grundläggande kunskaper och inte utgöra en säkerhetsrisk i informationshanteringen. Därtill behövs rutiner för att fånga upp nyanställda medarbetare och nyvalda förtroendevalda.

Kommunens informationssäkerhetsarbete är i behov av utveckling. Ansvar behöver tydliggöras och resurser tillskapas till funktioner som får i uppdrag att påbörja ett mer strategiskt arbete. Arbetet bör utgå från en nulägesanalys som presenteras för kommunstyrelsen som därefter kan besluta om prioritering och krav på åtgärder. Vi rekommenderar att kommunen tar stöd i de rekommendationer och metodstöd som MSB erbjuder kostnadsfritt för att verksamheter ska etablera ett systematiskt och riskbaserat informationssäkerhetsarbete.

Datum som ovan

KPMG AB

Jenny Thörn
Kommunal revisor

Ida Larsson
Kommunal revisor

Karin Helin Lindqvist
Certifierad kommunal revisor

Köpings kommun
Styrning och ledning av informationssäkerhet

2022-03-08