Styrning och ledning av informationssäkerhet

PM

Arboga kommun

KPMG AB

2022-03-08

Antal sidor 9

Arboga kommun
Styrning och ledning av informationssäkerhet

2022-03-08

Innehållsförteckning

1 Sammanfattning

Vi har av Arboga 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 Arboga 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 såväl ekonomiskt som förtroendeskada för kommunen.

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 avser kommunstyrelsen och samtliga nämnder.

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 Arboga 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

I den muntliga dialogen beskrivs att det tidigare funnits en funktion i form av en IT-strateg anställd i Västra Mälardalens kommunalförbund, VMKF, med uppdrag att samordna informationssäkerhetsarbetet för tre kommuner. Rollen finns inte längre kvar inom förbundet och är vakant i kommunen. Medel har avsatts i budget 2022 för att inrätta en intern funktion med uppdrag att leda informationssäkerhetsarbetet. Förhoppningen är att ha tydliggjort uppdraget för denna funktion och att den ska finnas på plats under 2022.

Övergripande styrdokument i form av informationssäkerhetspolicy och tillhörande riktlinjer saknas. Arbetet med att upprätta styrdokument inom området har påbörjats, men är vid tiden för granskningen inte slutfört. En riktlinje för systemförvaltning och IT-anskaffning finns beslutade och är enligt uppgift i dialogen implementerade i verksamheten. Det finns ett IT-råd etablerat med representanter från förvaltningarna och enligt uppgift pågår ett arbete med att få till en systematik för IT-frågorna. och Det upplevs att det finns behov av att uppdatera IT-rådets roll och funktion så att ett mer aktivt arbete kan bedrivas.

Av de skriftliga svaren framgår att kommunen har genomfört en nano-utbildning inom informationssäkerhet under 2019. Det innebär ett antal korta utbildningstillfällen som genomförs digitalt. Utbildningen sändes ut till samtliga medarbetare inom kommunen samt till medarbetare inom kommunens helägda bolag. Förtroendevalda var inte inkluderade vid dessa tillfällen. Under 2020 genomförde kommunen även en digital säkerhetsutbildning. Det framgår att syftet med utbildningarna främst var att öka medvetenheten inom informationssäkerhet och säkerhetsarbete överlag. Utbildningarna följdes upp med ett test i syfte att se om det skett några kunskapsförändringar. Frågor ställdes till mottagarna innan och efter utbildningen vilket gjorde att kommunen kunde mäta effekten av utbildningarna. Av de skriftliga svaren framgår att mätningarna visade klara förflyttningar i förståelse och beteendeförändring. I samband med dialogen framkommer att nya utbildningstillfällen planeras och att försök har gjorts inom VMKF för att testköra den nya utbildningen som består av 16 kortare, digitala utbildningspass.

I de skriftliga svaren uppger förvaltningschefer att det även har genomförts egenutvecklade utbildningar som varit verksamhetsspecifika inom informationssäkerhet och personuppgiftshantering.

3.1.2 Arbetsmetoder för riskbedömning och informationsklassning

Av de skriftliga svaren framgår att det finns upparbetade metoder för att genomföra riskanalyser och vidta lämpliga åtgärder för ett anpassat skydd kopplat till verksamheter eller aktiviteter som rör säkerhetsskydd.

I de skriftliga svaren uppger kommunen att de för sina verksamhetskritiska system som har genomförts en klassning av information för ett antal år sedan. Det har även genomförts exempelvis vid upphandling, utveckling av system samt vid användandet av Teams. På uppmaning från VMKF har självskattningsverktyget KLASSA till viss del börjat nyttjas i kommunen, främst inför upphandling och implementering av nya system.

Av svaren i granskningen framgår att ett mer strukturerat arbete har gjorts för hantering av personuppgifter vilket är en viktig del av informationshanteringen i kommunen. Det finns en beslutad *Policy för personuppgiftsbehandlingar*[1] samt *Riktlinje för hantering av skyddade identiteter*[2].

Kommunen och dess bolag har ett gemensamt dataskyddombud med Köping, Kungsör samt Västra Mälardalens kommunalförbund. I Arboga kommun är kanslichefen dataskyddssamordnare. Kommunen har även dataskyddshandläggare inom samtliga verksamheter. Dessa ansvarar för förvaltningens/bolagets förteckning över personuppgiftbehandlingar utifrån ajourhållande och rättningar samt rapporterar personuppgiftsincidenter till dataskyddsombudet.

Som stöd i arbetet och för dokumentation används ett systemstöd, Visma Draftit. I systemet finns funktion och stöd för att göra konsekvensbedömningar, som är en riskanalys för hantering av personuppgifter, där lämpliga säkerhetsåtgärder beslutas för att skydda dessa.

Behörighetshantering styrs dels från personalsystemet och via en katalog, så kallad Active Directory, där medarbetare tilldelas användarkonto och behörighet i kommunövergripande system. Behörigheter till verksamhetssystem tilldelas inom respektive verksamhet utifrån funktion och ansvar. Det är ofta systemförvaltare som har rollen att tilldela och uppdatera behörigheter. Inom exempelvis socialtjänsten finns rutiner för att följa upp tilldelade behörigheter och göra loggkontroller. Det finns till viss del rutiner för hanteringen men i nuläget uppges att det saknas kommunövergripande regler eller riktlinjer för kommunens åtkomst- och behörighetshantering.

3.1.3 Incidenthantering

Kommunen uppger i de skriftliga svaren att det finns en kommunövergripande rutin för hantering av informationssäkerhetsincidenter när dessa är personuppgiftsincidenter. En fastställd mall används vid eventuella incidenter. Information och förankring av rutinen har skett till samtliga chefer. Politiska forum och samtliga medarbetare har fått grundläggande utbildning i GDPR. Det finns även information att tillgå på hemsidan och intranätet för medarbetarna. I samband med utbildning och information till grupperna har även informationssäkerhet beaktats.

Av de skriftliga svaren framgår att vid informationssäkerhetsincidenter av allvarligare karaktär, som enligt föreskrift från MSB ska rapporteras till CERT-SE (Sveriges nationella Computer Security Incident Response Team)[3] följer kommunen de rutiner

[1] Antagen av kommunfullmäktige 2018-06-14 § 73
[2] Antagen av socialnämnden 2015-03-18, reviderad 2018-09-26
[3] CERT-SE har som uppgift att stödja samhället i arbetet med att hantera och förebygga IT-incidenter.

som anges av CERT-SE. Internt i kommunen har inte rutiner för att anmäla och rapportera om incidenter tydliggjorts.

Enligt svaren i granskningen har inga allvarligare incidenter inträffat i kommunen.

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*[4] 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.

Det är positivt att utbildning har erbjudits och att dessa till viss del har följts upp. Medarbetares hantering av information är en väsentlig del i att upprätthålla en tillräcklig säkerhet och inte utsätta tillgångarna för risk. Vi rekommenderar att detta genomförs regelbundet så att enskilda har grundläggande kunskaper och inte utgör en säkerhetsrisk i informationshanteringen. Därtill behövs rutiner för att fånga upp nyanställda medarbetare och vi ser även vikten att inkludera förtroendevalda som grupp i de utbildningsinsatser som genomförs.

Vi ser bristande rutiner för incidenthantering samt att användarnas ansvar inte är dokumenterat som en risk för att utbildningsinsatserna inte ger en tillräcklig medvetenhet för att säkerställa informationssäkerheten.

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.

[4] 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. Vi anser att det är positivt att utbildning har genomförts för att skapa en medvetenhet för medarbetare att inte utsätta informationstillgångarna för risk och att dessa till viss del har följts upp för att se effekter. Vi rekommenderar att detta genomförs regelbundet för att dels inkludera nytillkomna medarbetare, dels för att löpande aktualisera informationssäkerhetsfrågorna och ansvar hos medarbetarna. Därtill bör förtroendevalda ingå som grupp när utbildningsinsatser genomförs.

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

Karin Helin Lindqvist
Certifierad kommunal revisor