www.avesta.se

Avesta kommun 2022-08-23
Kommunrevisionen

Till:
Kommunfullmäktige

För kännedom:
Kommunstyrelsen, Omsorgsstyrelsen och Bildningsstyrelsen

Revisionsrapport – Granskning av informationssäkerhet

KPMG har på uppdrag av Avesta kommuns revisorer genomfört en granskning av informationssäkerheten. Uppdraget ingår i revisionsplanen för år 2022.

Efter genomförd granskning är vår sammantagna bedömning att kommunstyrelsen, omsorgsstyrelsen samt bildningsstyrelsen saknar en tillräcklig intern styrning och kontroll som säkerställer ett ändamålsenligt och systematiskt arbetssätt med kommunens informationssäkerhet. Bland annat saknas till viss del styrande dokument med tydliga mål, ansvarsfördelning och former för uppföljning avseende informationssäkerhetsarbetet som i dagsläget bedrivs. Ansvariga informationsägare i verksamheten bör ta ett större grepp om ansvaret över väsentliga moment och hantering av risker och krav för en god informationssäkerhet. Det arbete som i dagsläget bedrivs bör utökas och utvecklas.

För den tekniska delen av informationssäkerhetsarbetet gör vi bedömningen att IT-enheten har vidtagit åtgärder i syfte att säkerställa att information skyddas. Åtgärderna syftar till att minska möjligheterna för digitala och fysiska intrång. Vi ser att arbetet med riskanalyser kan utvecklas genom att dessa dokumenteras.

Slutligen ser vi ett behov av att kommunen upprättar former och arbetssätt avseende uppföljning och återrapportering av det informationssäkerhetsarbete som bedrivs, då detta saknas i dagsläget.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Upprätta och besluta om en informationssäkerhetspolicy där den politiska viljeriktningen framgår genom att tydligt beskriva mål för arbetet, ansvarsfördelning samt former för uppföljning.
- Säkerställa att riktlinjer för informationssäkerhet upprättas och implementeras som kan konkretisera policyns intentioner.
- Se över nuvarande organisationsstruktur och utreda behovet av en informationssäkerhetssamordnare.
- Upprätta former för genomförande av riskbedömning samt informationsklassning och säkerställa att dessa moment genomförs.

- Ställa krav om uppföljning och återrapportering av kommunens samlade informationssäkerhetsarbete så att beslut kan tas om mål och handlingsplan över erforderliga åtgärder för att förbättra informationssäkerheten.
- Införa kontroller avseende tilldelade behörigheter i syfte att minska risken för otillbörlig tillgång till information samt säkerställa att medarbetare har tillgång till rätt information och system utifrån uppdrag och funktion.
- Säkerställa att utbildning genomförs löpande för samtliga användare för att etablera en medvetenhet och grundläggande kunskap om informationssäkerhet.
- Upprätta incidenthanteringsrutiner och tillhörande process/system för att anmäla och rapportera incidenter. Dessa bör dokumenteras, analyseras och bedömas på kommunövergripande nivå.

Utifrån vår bedömning och slutsats rekommenderar vi omsorgsstyrelsen och bildningsstyrelsen att:

- Etablera rollen informationsägare och tydliggöra det ansvar som dessa har att efterleva.
- Utse funktion/roller som på informationsägarens uppdrag ska arbeta med styrelsens/förvaltningens informationssäkerhet i enlighet med de krav som ställs i styrande dokument och enligt lagkrav.
- Systematiskt genomföra informationsklassning och riskbedömning av den information som hanteras i system samt utifrån dessa ställa krav om nödvändiga säkerhetsåtgärder.
- Årligen följa upp informationssäkerhetsarbetet och besluta om erforderliga åtgärder för att förbättra informationssäkerheten utifrån aktuella risker och behov.
- Införa kontroller avseende tilldelade behörigheter i syfte att minska risken för otillbörlig tillgång till information samt säkerställa att medarbetare har tillgång till rätt information och system utifrån uppdrag och funktion.
- Tydliggöra incidenthanteringsrutiner och tillhörande process/system för att anmäla och rapportera incidenter. Dessa bör dokumenteras, analyseras och bedömas på nämndnivå.

Revisionen rekommenderar fullmäktige att begära in ett yttrande över bifogad revisionsrapport från kommunstyrelsen, omsorgsstyrelsen och bildningsstyrelsen till fullmäktiges sammanträde 2022-11-28.

Yttrandet bör även lämnas till revisionen för kännedom.

För de förtroendevalda revisorerna i Avesta kommun

Maarit Hessling
Ordförande i kommunrevisionen

Granskning av kommunens informationssäkerhet

Rapport

Avesta kommun

KPMG AB

Datum 2022-07-05

Antal sidor 20

Avesta kommun
Granskning

2022-07-05

Innehållsförteckning

Avesta kommun
Granskning

2022-07-05

1 Sammanfattning

KPMG har av Avesta kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av styrelsernas rutiner för sitt informationssäkerhetsarbete. Uppdraget ingår i revisionsplanen för år 2022.

Granskningens syfte har varit att bedöma om styrelserna har en tillräcklig intern styrning och kontroll som säkerställer ett ändamålsenligt och systematiskt arbetssätt med informationssäkerheten i kommunen.

Vår sammanfattande bedömning är att kommunstyrelsen, omsorgsstyrelsen samt bildningsstyrelsen saknar en tillräcklig intern styrning och kontroll som säkerställer ett ändamålsenligt och systematiskt arbetssätt med kommunens informationssäkerhet. Vi baserar vår bedömning på följande iakttagelser:

- Det saknas till viss del styrande dokument med tydliga mål, ansvarsfördelning och former för uppföljning avseende informationssäkerhetsarbetet som i dagsläget bedrivs.
- Därtill saknas en informationssäkerhetssamordnare med rollen att samordna, leda och följa upp arbetet.
- Informationsägarna bör ta ett större grepp om ansvaret över väsentliga moment och hantering av risker och krav för en god informationssäkerhet. Det arbete som i dagsläget bedrivs bör utökas och utvecklas.
- Den tekniska delen av informationssäkerhetsarbetet gör vi bedömningen att IT-enheten har vidtagit åtgärder i syfte att säkerställa att information skyddas. Åtgärderna syftar till att minska möjligheterna för digitala och fysiska intrång. Vi ser att arbetet med riskanalyser kan utvecklas genom att dessa dokumenteras.
- Vi ser ett behov av att kommunen har behov av att upprätta former och arbetssätt avseende uppföljning och återrapportering av det informationssäkerhetsarbete som bedrivs, då detta saknas i dagsläget.

Mot bakgrund av vår granskning rekommenderar vi kommunstyrelsen att:

- Upprätta och besluta om en informationssäkerhetspolicy där den politiska viljeriktningen framgår genom att tydligt beskriva mål för arbetet, ansvarsfördelning samt former för uppföljning.
- Säkerställa att riktlinjer för informationssäkerhet upprättas och implementeras som kan konkretisera policyns intentioner.
- Se över nuvarande organisationsstruktur och utreda behovet av en informationssäkerhetssamordnare.
- Upprätta former för genomförande av riskbedömning samt informationsklassning och säkerställa att dessa moment genomförs.

- Ställa krav om uppföljning och återrapportering av kommunens samlade informationssäkerhetsarbete så att beslut kan tas om mål och handlingsplan över erforderliga åtgärder för att förbättra informationssäkerheten.
- Införa kontroller avseende tilldelade behörigheter i syfte att minska risken för otillbörlig tillgång till information samt säkerställa att medarbetare har tillgång till rätt information och system utifrån uppdrag och funktion.
- Säkerställa att utbildning genomförs löpande för samtliga användare för att etablera en medvetenhet och grundläggande kunskap om informationssäkerhet.
- Upprätta incidenthanteringsrutiner och tillhörande process/system för att anmäla och rapportera incidenter. Dessa bör dokumenteras, analyseras och bedömas på kommunövergripande nivå.

Mot bakgrund av vår granskning rekommenderar vi omsorgsstyrelsen och bildningsstyrelsen att:

- Etablera rollen informationsägare och tydliggöra det ansvar som dessa har att efterleva.
- Utse funktion/roller som på informationsägarens uppdrag ska arbeta med styrelsens/förvaltningens informationssäkerhet i enlighet med de krav som ställs i styrande dokument och enligt lagkrav.
- Systematiskt genomföra informationsklassning och riskbedömning av den information som hanteras i system samt utifrån dessa ställa krav om nödvändiga säkerhetsåtgärder.
- Årligen följa upp informationssäkerhetsarbetet och besluta om erforderliga åtgärder för att förbättra informationssäkerheten utifrån aktuella risker och behov.
- Införa kontroller avseende tilldelade behörigheter i syfte att minska risken för otillbörlig tillgång till information samt säkerställa att medarbetare har tillgång till rätt information och system utifrån uppdrag och funktion.
- Tydliggöra incidenthanteringsrutiner och tillhörande process/system för att anmäla och rapportera incidenter. Dessa bör dokumenteras, analyseras och bedömas på nämndnivå.

2 Bakgrund

KPMG har av Avesta kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av styrelsernas rutiner för sitt informationssäkerhetsarbete. Uppdraget ingår i revisionsplanen för år 2022.

Informationssäkerhet (där IT-säkerhet ingår som en del) är ett begrepp som används om informationssäkerhet för information som hanteras i kommunens IT-system. Allt mer information hanteras idag med olika tekniska lösningar och aldrig förr har kommunerna hanterat sådana mängder information som görs idag. Informationssäkerhet innebär att skydda information utifrån dess krav på konfidentialitet, riktighet och tillgänglighet i alla kommunens system. För att kunna hantera detta på ett ändamålsenligt sätt krävs att kommunen har ett systematiskt informationssäkerhetsarbete där flera funktioner i kommunen är involverade och rätt organiserade för uppdraget. Informationssäkerhet är inte en IT-fråga utan en fråga om att säkra och trygga driften av kommunens kärnverksamheter.

Verksamheternas ökade beroende av informationsteknik (IT) innebär ökade risker i form av dataintrång, bedrägerier och spridning av skadlig kod. Många verksamheter inom kommunen är idag helt beroende av väl fungerande IT. För flera verksamheter handlar ett väl fungerande IT-stöd såväl om säkerhet som möjlighet till en fungerande verksamhet utan driftstörningar. 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.

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

2.1 Syfte, revisionsfrågor och avgränsning

Granskningens syfte har varit att bedöma om styrelserna har en tillräcklig intern styrning och kontroll som säkerställer ett ändamålsenligt och systematiskt arbetssätt med informationssäkerheten i kommunen.

Granskningen besvarar följande revisionsfrågor:

- Finns aktuella styrande dokument som tydliggör ansvar, vilka krav som ställs och hur arbetet ska bedrivas?
- Finns en ändamålsenlig organisation för att arbeta med informationssäkerhet?
- Finns ett systematiskt arbete med riskanalyser och informationsklassning?
- Sker en kravställning av IT-säkerhetsåtgärder utifrån genomförd riskbedömning och klassning av informationstillgångar som hanteras i system?
- Finns ett systematiskt arbetssätt med IT-säkerhet för central IT-infrastruktur (nätverk, servrar, klienter mm.)?
- Finns incidenthanteringsrutiner och sker en tillräcklig rapportering av inträffade incidenter?

- Görs systematiska uppföljningar av implementerade säkerhetsåtgärder för att kontinuerligt förbättra informationssäkerheten?
- Finns ett ändamålsenligt arbete med att följa upp att beslut och styrdokument relaterat till informationssäkerhet efterlevs?

Granskningen omfattar kommunstyrelsen, bildningsstyrelsen och omsorgsstyrelsen. Granskningen avser år 2022.

2.2 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

2.3 Metod

Granskningen har genomförts genom:

Dokumentstudier av:

— Informationssäkerhetshandlingsplan
— Rutinbeskrivning för personuppgiftsincident
— GDPR rutiner
— Digitaliseringspolicy
— Riktlinjer för kommunikation och e-post inom omsorgsstyrelsens verksamheter

Intervjuer har genomförts med:

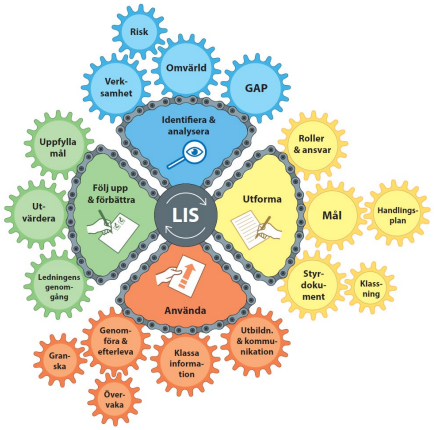
— Kommundirektör
— Administrativ chef
— IT-chef
— Säkerhetschef/Säkerhetsskyddschef
— Representanter från omsorgsförvaltningen
— Representanter från bildningsförvaltningen

Rapporten är faktakontrollerad av intervjupersoner.

2.4 Metodstöd för systematiskt informationssäkerhetsarbete

MSB har tagit fram ett metodstöd till organisationer avseende informationssäkerhetsarbetet. Metodstödet baserat på den internationella standardserien för informationssäkerhet, ISO/IEC 27000, och ämnar till att förtydliga hur informationssäkerhetsarbetet kan utformas.

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



2.4.1 Identifiera och analyser

Syftet med att analysera informationssäkerhetsarbetet är enligt MSB att säkerställa att informationssäkerheten utformas utifrån verksamhetens rådande förutsättningar. Det ska även leda till att väsentliga informationstillgångar identifieras, vilka risker de ska skyddas mot, samt valda säkerhetsåtgärder.

2.4.2 Utforma

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

- Organisation
- Informationssäkerhetsmål
- Styrdokument
- Klassningsmodell
- Handlingsplan
- Kontinuitetshantering för informationstillgångar

2.4.3 Använda

När verksamheten har utformat styrningen enligt avsnitt 2.4.2 ska det tillämpas. Det innebär:

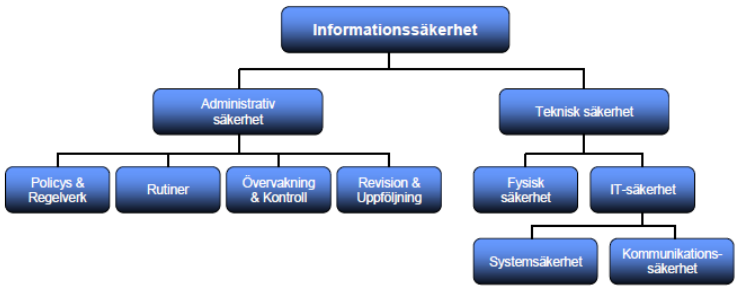
- Kontinuerligt arbete med att klassa organisationens information för att identifiera känslig och kritisk information för att kunna säkerställa tillräckligt skydd.
- Genomföra och efterleva de handlingsplaner och styrdokument som avser informationssäkerhetsarbetet.
- Utbilda och kommunicera informationssäkerhetsfrågor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

2.4.4 Följa upp och förbättra

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

2.4.5 Roller och ansvar

Informationssäkerhetsbegreppet och dess innehåll kan översiktligt beskrivas i nedanstående skiss:



Informationssäkerhetsarbetet kan struktureras i ett Ledningssystem för informationssäkerhet, kallat LIS. I ett sådant har verksamheten tydliggjort krav som ställs genom styrande dokument och hur ansvaret är fördelat.

En central del i ett ledningssystem, är enligt MSB, ledningens uttalade stöd. Ledningen bör också se till att organisationen antar en policy för informationssäkerhetsarbetet. I ytterligare styrdokument, riktlinjer och liknande kan sedan den högsta ledningen ge vägledningen till chefer och övriga medarbetare. Det är viktigt att alla i en organisation känner till och förstår innehållet i policys och riktlinjer. Erfarenhet visar tydligt vikten av att anställda uppvisar ett säkert beteende i sitt dagliga arbete. En stor del av arbetet med att driva ett ledningssystem handlar därför om att informera medarbetare om de regler som ingår i ledningssystemet.

Den svenska och internationella standardserien SS-ISO/IEC 27000 visar på ett sådant ledningssystem där säkerhetsnivån tar sin utgångspunkt i en verksamhetsanpassad

riskanalys, och där informationssäkerhetsarbetet följer en tydlig process. Tillämpning av standarderna enligt denna serie underlättar arbetet med informationssäkerhet inom organisationer och förbättrar också möjligheterna att externt bedöma säkerhet och revidera denna på ett enhetligt sätt.

Enligt MSB:s metodstöd för hur ett systematiskt informationssäkerhetsarbete kan bedrivas framgår det hur ansvaret för arbetet med informationssäkerhet bör fördelas. 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, verksamhetschefer 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.

Var i organisationen informationssäkerhetssamordnaren eller motsvarande är placerad beror på organisationens struktur men bör generellt vara placerad nära ledning, exempelvis i ledningsstaben. Vanliga organisatoriska placeringar, enligt MSB:s metodstöd är exempelvis:

- Säkerhet
- Kvalitet
- Juridik

I de fall rollen är placerad i en strategisk IT-funktion bör funktionen vara åtskilda från organisationens interna IT-produktion och drift. Anledningen till det är att informationssäkerhetssamordnaren både ska granska och vara kravställande gentemot IT-drift och riskerar annars att brista i opartiskhet.

3 Resultat av granskningen

3.1 Organisation

3.1.1 Styrande dokument

Det framkommer i intervjuer att Avesta kommun saknar ett antaget ledningssystem. Det uppges att kommunen avser att upphandla den här typen av tjänstesystem i syfte att få hjälp och stöd i arbetet med att upprätta ett ledningssystem där även informationssäkerhet kan ingå.

Koncernledningsgruppen har antagit en informationssäkerhetshandlingsplan[1]. Handlingsplanen saknar mål och tidsperspektiv för när arbetet ska vara genomfört och fokuseras i huvudsak gentemot personuppgiftsfrågor. Av planen framgår rollfördelning utifrån olika arbetsgrupper samt vilka uppgifter som arbetsgrupperna har. Nedan presenteras grupperna lite kort samt ett exempel på uppgift som gruppen har.

- Koncernledningsgruppen (KCL) har bland annat som uppgift att ta fram en gemensam budget för kommunens informationssäkerhetsarbete.
- IT-gruppen består av IT-chef, IT-samordnare/strateger i förvaltningar och bolag samt risk- och säkerhetssamordnare. Gruppen ska ta fram kommunövergripande stöd/styrdokument/system/handlingsplaner för kommunens personuppgiftsarbete.
- Administrativa gruppen består bland annat av personuppgiftsombud och dataskyddsombud. Gruppen ska kontinuerligt följa upp, utvärdera och sammanställa statusen för kommunens personuppgiftsarbete och ta fram åtgärdsförslag vid behov.
- Personuppgiftsombudens uppgifter är bland annat att svara för förvaltningens/bolagets registerförteckning samt delta i personuppgiftsincidentutredningar.
- Gruppen kommunsekreterare är sammankallande och leder arbetet i administrativa gruppen, men deltar i personuppgiftsincidentutredningar, konsekvensbedömningar och i förhandssamråd med Datainspektionen.

Koncernledningsgruppen har utöver detta även antagit en beskrivning av rutiner[2] för behandling av personuppgifter utifrån GDPR. Beskrivningen syftar till att på en övergripande nivå vägleda medarbetare i Avesta kommun i behandlingen av personuppgifter i enlighet med dataskyddsförordningen.

I händelse av en personuppgiftsincident har kommunen upprättat rutiner för hur hantering av incidenten ska ske. Avesta kommun har upprättat en rutin avseende

[1] Koncernledningsgruppen, 2019-01-24

[2] Koncernledningsgruppen 2019-09-26, senast reviderat, 2022-03-02

hantering av personuppgiftsincidenter[3]. Rutinerna beskriver vad en personuppgiftsincident är, vilket ansvar som medarbetare och förtroendevalda i kommunen har samt hur anmälan ska gå till. Till rutinerna hör en mall för intern rapportering av en personuppgiftsincident som efter ifyllande ska sändas till verksamhetschef med kopia till dataskyddsombudet.

Inom kommunen finns även dokumentet E-posthantering för Avesta kommun - riktlinje[4] samt kommunikationspolicy. Riktlinjerna beskriver hur sekretessbelagd information och känsliga uppgifter ska hanteras via e-post. Det finns även anvisningar hur användare ska agera om det finns misstanke om att virus skickats via e-post. Omsorgsstyrelsen har antagit särskilda riktlinjer som avser kommunikation och e-posthantering inom verksamheter under omsorgsstyrelsens ansvarsområde[5].

Vidare uppges i intervjuer att det finns en upprättad informationssäkerhetspolicy som inte har fastställts politiskt och därmed inte har implementerats i organisationen. Det uppges att policyn kommer att revideras utifrån den internationella standardserien för informationssäkerhet, ISO/IEC 27000.

3.1.2 Roller och ansvar

Det finns vid tid för granskningen inget politiskt antaget dokument som reglerar roller och ansvar avseende informationssäkerhetsarbetet.

Generellt kan dock sägas att ansvar för informationssäkerhet är ett linjeansvar som följer med verksamhetsansvaret i likhet med övrigt säkerhetsarbete. Det är därigenom förvaltningschef eller motsvarande som är informationsägare och har ett ansvar att säkerställa att informationshanteringen sker på ett korrekt sätt utifrån interna styrdokument och lagkrav.

I intervjuer beskrivs att säkerhetsfrågorna tidigare låg under kommunledningsförvaltningen men numer är organiserade under förvaltningen för teknisk service. Det är chefen för teknisk service som i dagsläget även innehar funktionerna säkerhetschef och säkerhetsskyddschef. I syfte att få avlastning har chef för teknisk service rekryterat en enhetschef som ansvarar för den operativa verksamheten inom förvaltningen. Det uppges i intervjuer att den nuvarande funktionsfördelningen fungerar bra. Sedan april 2022 sitter chef för teknisk service med i koncernledningsgruppen. Detta har efterfrågats under en längre tid men dock inte genomförts förrän nu.

Även IT-chefen sitter med i koncernledningsgruppen. IT-chefen ansvarar för IT-enheten som i dagsläget består av 13 medarbetare. Då IT-enheten avses bli ett stöd i kommunens digitaliseringsarbete samt verksamhetsutveckling kommer enheten att

[3] Rutin för hantering av personuppgiftsincidenter, t.f. kommundirektör 2021-03-19

[4] Fastställd av kommunfullmäktige 2021-06-10 §86

[5] Riktlinjer för kommunikation och e-posthantering inom verksamheter under omsorgsstyrelsens ansvarsområde, omsorgsstyrelsen 2020-01-21

utökas med ytterligare ett antal medarbetare. Enligt uppgift finns en viss osäkerhet avseende om detta utökade uppdrag finns dokumenterat i enskild skrivelse.

I syfte att effektivisera IT-enhetens resurser har enheten delats in i tre arbetsgrupper: verksamhet och verksamhetsstöd, renodlad teknik (nätverk, servrar, programvara etc.) samt en grupp som ska bistå i användandet av teknik och utrustning i syfte att effektivisera de investeringar som gjorts inom området.

Utöver detta innehar kommunen funktionerna säkerhetssamordnare samt dataskyddsombud. Arbetet med att revidera informationssäkerhetspolicyn uppges i intervjuer kan komma att visa på ett behov av att inrätta en informationssäkerhetssamordnare i kommunen.

Varje förvaltning har utsett en personuppgiftshandläggare som bland annat har till uppgift att svara för förvaltningens registerförteckning, dokumentera personuppgiftsarbetet samt stödja enhetscheferna i deras arbete med personuppgiftsfrågor. Omsorgsförvaltningen tillika bildningsförvaltningen har även funktionen IT-strateg.

3.1.3 Bedömning

Vår bedömning är att Avesta kommun till viss del har upprättat styrande och stödjande dokument avseende informationssäkerhet. Vi ser dock ett behov av att upprätta en kommunövergripande informationssäkerhetspolicy där bland annat roller, ansvar och uppföljning regleras och beskrivs på ett tydligt sätt. En informationssäkerhetspolicy med tillhörande riktlinjer tydliggör ansvar och krav på arbetet samt bidrar till att skapa systematik i det informationssäkerhetsarbete som bedrivs i kommunen. Utöver detta ser vi även att det finns behov av att upprätta rutiner för hantering av incidenter som inte avser personuppgiftsincidenter.

Vidare gör vi bedömningen att den upprättade handlingsplanen behöver utvecklas ytterligare genom att ange mål samt tidsperiod för när arbetet ska vara genomfört. Att tidsbegränsa arbetet bidrar till att säkerställa att arbetet i handlingsplanen genomförs samt att arbetet kan följas upp.

Vi gör även bedömningen att det finns behov för kommunstyrelsen att utreda behovet av att skapa en ny tjänst i kommunen som får en samordnande och stödjande roll i informationssäkerhetsarbetet. Med nuvarande rollfördelning finns en risk att det samordnande och förebyggande informationssäkerhetsarbetet inte kan prioriteras i tillräckligt hög grad i förhållande till andra ansvarsuppgifter som förvaltningschef teknisk service tillika säkerhetschef/säkerhetsskyddschef har.

3.2 Analys av behov och risker för informationssäkerhet

Eftersom skadeverkningarna av bristande säkerhet i system även medför risker hos andra informationsägare och verksamheter behöver riskbedömning och kravställningar om åtgärder ske med samsyn och med delaktighet från olika funktioner i kommunen.

3.2.1 Riskhantering och informationsklassning

I intervjuer uppges att det i dagsläget inte genomförs någon kommunövergripande riskbedömning utifrån informationssäkerhet. Det uppges i intervjuer att klassning av system och information främst genomförs vid införskaffande av nya verksamhetssystem, i övrigt saknas systematik inom klassningsarbetet. Intervjupersoner uppger att kommunens IT-chef har fått i uppdrag att i augusti 2022 presentera en fullständig organisation för systemförvaltning, i dagsläget är det endast kommunens större verksamhetssystem som har förvaltare. Omsorgsförvaltningen har systemadministratörer som ansvarar för olika delar i verksamhetens system.

Omsorgsförvaltningens IT-strateg har påbörjat ett arbete med att även klassa de befintliga systemen inom verksamhetsområdet. Utöver representanter från förvaltningen medverkar även representanter från IT-enheten och vid behov kontaktas leverantören i syfte att besvara särskilda frågeställningar. Det är kommunens dataskyddsombud som godkänner klassningen.

En fråga som uppges ha diskuterats mycket inom omsorgsförvaltningen är behörighetstilldelning. En genomgång visade att flertalet medarbetare hade felaktiga behörigheter vilket genererade en mer begränsad tilldelning. Det uppges att det är ansvarig chef som ska rapportera till IT-enheten vilken behörighet som ska tilldelas alternativt förändras eller avslutas, men det framkommer att många brister i detta. När en medarbetare byter verksamhetsområde i organisationen finns det skäl att se över behörigheten den har, vilket inte alltid genomförs.

Omsorgsförvaltningen har genomfört riskanalyser i syfte att kunna upprätthålla verksamheten vid eventuella driftstopp eller större IT-bortfall. Åtgärder som vidtagits är bland annat att varje dag skriva ut det digitala planeringsschemat samt hälso- och sjukvårdsinsatser för kommande dag samt skapat blanketter för analog hantering av det som i dagsläget hanteras via e-tjänster. Vidare uppges att förvaltningen även arbetar med hur de ska säkerställa tillgång till information angående placerade barn vid driftstopp eller utan tillgång till den information som finns i verksamhetssystem.

Även måltidsverksamheten inom bildningsförvaltningen har, utifrån en riskanalys, vidtagit åtgärder såsom att skriva ut och spara antal beställda portioner analogt.

Utöver detta arbetar IT-chefen med att färdigställa en systemkarta över kommunens samtliga verksamhetssystem för att det ska finnas en dokumentation över system och systemberoenden.

3.2.2 Medvetenhet och förståelse

En viktig del i ett systematiskt informations- och IT-säkerhetsarbete är att det finns en tillräcklig medvetenhet hos de som har tillgång till kommunens information. I kommunen är detta bland annat förtroendevalda, medarbetare, elever och externa konsulter.

Intervjupersoner uppger att det har blivit en ökad medvetenhet i kommunen, bland annat med anledning av den nya kommunchefens intresse för den här typen av frågor men även på grund av den cyberattack som Kalix kommun blev utsatt för i slutet av 2021.

Vidare uppges att IT-enheten har tilldelats resurser i syfte att åstadkomma en säker IT-miljö. Det framkommer dock i intervjuer att även de förtroendevalda behöver kompetens inom området för att kunna ställa krav på kommunens IT-säkerhet som IT-enheten får i uppdrag att verkställa. Det uppges i nuläget saknas till viss del och kraven är inte tydliggjorda.

Intervjupersoner uppger att det upplevs finnas en medvetenhet hos kommunens förvaltningschefer angående deras ansvar i arbetet med informationssäkerhet, men att förvaltningarna har kommit olika långt i sitt arbete.

Utredargruppen i Avesta kommun har genomfört en förstudie där syftet var att ta fram ett ledningssystem. Förstudien lyfter bland annat informationssäkerhet inte bara handlar om vikten av säkra IT-system, utan även vikten av att användaren agerar rätt. Vidare lyfter förstudien att införande och förvaltande av ett informationssäkerhetsarbete är resurskrävande och påverkar arbetssätt och relationer mellan organisationens olika roller. Förstudien saknar ett uttalat uppslag för kommunens nästa steg i processen, men lyfter MSB:s metodstöd som beskriver arbetet utifrån följande steg: identifiera och analysera, utforma, använda samt följa upp och förbättra.

Sedan ett antal månader tillbaka har IT-enheten introducerat en nano-utbildning avsedd för kommunens tjänstepersoner som omfattar IT- och informationssäkerhet. IT-enheten har möjlighet att se vilka som har genomgått utbildningen men det framgår inte i intervjuer att någon uppföljning angående detta har genomförts eller rapporterats till kommunledningen. Intervjupersoner uppger att antalet incidenter har minskat sedan utbildningen genomfördes. Utöver detta har även ett antal funktioner i kommunen erbjudits en mer djupgående utbildning avseende GDPR. I syfte att informera och uppmärksamma publicerar IT-chefen kortare texter på intranätet angående nya typer av bedrägerier eller annat som är aktuellt inom området.

Då kommunen haft viss problematik avseende att förtroendevalda använder sig av privata e-postadresser arbetar kommunen med att informera om riskerna med detta och uppmanar förtroendevalda att i stället använda den kommunala e-postadressen.

Vidare uppger intervjupersoner att klassningsarbetet har bidragit till en ökad medvetenhet och kunskap inom området.

3.2.3 Bedömning

Vi gör bedömningen att kommunen saknar ett systematiskt och ändamålsenligt arbetssätt för att uppnå god informationssäkerhet. Det saknas framtagna anvisningar och mallar för att göra riskbedömning och informationsklassning och det görs främst inför implementering och vidareutveckling av system. Det saknas även rutiner för att regelbundet ompröva de genomförda informationsklassningarna och riskanalyser som gjorts för att möta nya risker och behov när systemen är i drift. Detta ansvar behöver etableras hos informationsägarna och rutiner behöver inrättas. Vi ser positivt på att omsorgsförvaltningens IT-strateg har påbörjat ett arbete med att även klassa befintliga system, vi ser dock ett behov av att detta behöver utvecklas ytterligare i kommunen.

Med anledning av det som uppges i intervjuer angående problematik avseende justering av behörigheter utifrån befogenhet, är vår bedömning att styrelserna inför kontroller som avser tilldelade behörigheter. Detta i syfte att minska risken för otillbörlig tillgång till information samt säkerställa att medarbetare har tillgång till den information som krävs utifrån medarbetarens funktion och uppdrag.

Utifrån det som framkommit i granskningen gör vi bedömningen att det till viss del finns en medvetenhet avseende informationssäkerhet som bland annat grundas i de utbildningar som genomförts i kommunen. Med anledning av den risk som finns i samband med att använda privata e-postadresser i samband med politikernas förtroendeuppdrag anser vi att även förtroendevalda ska omfattas av utbildningen.

3.3 IT-säkerhetsåtgärder

IT-säkerhet har historiskt inte har varit en prioriterad fråga från kommunstyrelsen och ledningen. Trots detta uppges i intervjuer att kommunen har kommit långt i sitt IT-säkerhetsarbete. I IT-enhetens operativa arbete ingår att kontinuerligt riskbedöma i syfte att kunna vidta åtgärder. Dock finns ingen etablerad metod för riskanalysarbete och bedömningar av sårbarheter.

Intervjupersoner uppger att arbetet bygger på att identifiera den svagaste länken och att vidta åtgärder mot detta. Vidare uppges att de införanden och åtgärder som vidtagits för att utveckla IT-säkerheten bygger på en systematisk omvärldsbevakning och en kompetens hos medarbetare inom IT. Det finns därigenom inga dokumenterade riskanalyser för att kunna bedöma sårbarheter och utifrån det prioritera bland åtgärder för de komponenter som kommunens IT-miljö består av. Den prioritering som görs och de beslut som fattas ansvarar IT-chefen för.

Enligt uppgift har kommunen upprättat former i syfte att kunna skydda de servrar som finns i kommunens egna maskinhallar. Exempelvis sparas informationen kontinuerligt i syfte att kunna återskapas med minsta möjliga bortfall. Kommunen har även vidtagit åtgärder i syfte att skydda maskinhallarna från yttre påverkan såsom fysiska intrång, brand etc. IT-enheten undersöker möjligheter med nya tekniska lösningar för att ytterligare stärka säkerheten för IT-infrastruktur och de komponenter som utgör kommunens IT-miljö.

3.3.1 Bedömning

Vår bedömning är att det i stora delar finns ett systematiskt arbetssätt med IT-säkerhet för central IT-infrastruktur. IT-enheten har vidtagit flertalet åtgärder i syfte att säkerställa att information skyddas från både digitala som fysiska intrång. Om något skulle ske finns etablerade system och rutiner för att säkerställa att information inte går förlorad eller skadas.

Vi ser dock gärna att arbetet utvecklas genom att arbetet tar sin utgångspunkt i upprättade och dokumenterade riskanalyser. Utifrån dessa kan exempelvis mål- och handlingsplaner upprättas för att säkerställa att rätt prioriteringar görs utifrån sårbarhet och behov över tid. Dokumentationen kan även bidra till att förenkla det uppföljande arbetet.

3.4 Incidenthantering

Som tidigare nämnts har Avesta kommun upprättat rutiner för hantering av personuppgiftsincidenter. Det framgår av rutinerna hur rapportering av en incident ska ske. Intervjupersoner uppger att det finns en viss osäkerhet avseende om hur långt ut i organisationen som rutinerna är implementerade, men att det upplevs finnas kunskap om vad en personuppgiftsincident är.

Det är ansvarig chef som ska tillse att personuppgiftsincidenter följs upp och att åtgärder vid behov vidtas. Vidare uppges att det saknas dokumenterade rutiner för rapportering och anmälan av andra typer av incidenter. Det uppges dock vara kommunicerat att användare vid händelse, exempelvis ett klick på en länk, ska IT-enheten så snart som möjligt informeras genom IT-support.

Som en del i arbetet med att minska risken för att incidenter uppstår har kommunen inrättat multifaktorinloggning, men det uppges finnas ytterligare behov av förebyggande arbete i form av att medvetandegöra riskerna som finns.

Intervjupersoner uppger att IT-enheten har etablerade rutiner för hantering av andra typer av incidenter än personuppgiftsincidenter, men att dessa dock inte är dokumenterade. Det uppges att ett sådant dokument skulle bli svårhanterligt med anledning av den mängd information som dokumentet skulle innehålla, vilket är orsaken till att det inte har upprättats. Rutinerna har sin grund i erfarenhet och kompetens och bygger i stora drag på att stoppa systemet och sedan ta in experthjälp vid uppstart.

I dagsläget saknas en kontinuitetsplan som styr i vilken ordning kommunens system ska startas upp igen efter ett driftstopp. Kommunen har dock gjort en bedömning av kommunens system i syfte att se vilka system som är samhällsviktiga samt verksamhetskritiska.

Samtliga inträffade incidenter sammanställs och analyseras på en övergripande nivå i syfte att identifiera behov av stärkta rutiner eller andra åtgärder.

3.4.1 Bedömning

Vår bedömning är att det i stora delar saknas incidenthanteringsrutiner beskrivna i styrande dokument. Utöver personuppgiftsincidenter saknas beskrivning avseende hur en användare ska agera vid en incident samt vilka som ska ingå i utredning av incidenten. Vi får dock uppfattningen av att det finns tydliga arbetssätt hos IT-enheten hur de ska hantera en incident.

Vi gör även bedömningen att det förebyggande arbetet kan stärkas i syfte att öka kunskapen om incidenter hos kommunens medarbetare. Informations- och utbildningsinsatser bör genomföras gällande vad som anses vara en incident och hur dessa ska hanteras. Ett sådant arbete ligger till grund för att minska risken att incidenter inte upptäcks, utreds och på så sätt bidrar till det löpande förbättringsarbetet.

3.5 Uppföljning, intern kontroll och rapportering

3.5.1 Intern kontroll och uppföljning

Kommunstyrelsen beslutade vid sammanträdet 2022-03-14 om internkontrollplan för 2022. Utifrån granskningens område har följande risker inkluderats i planen:

- Riktlinjer för e-post.

Kontrollmomentet innebär att följa upp att riktlinjerna efterlevs.

Omsorgsstyrelsen fattade beslut på sammanträde 2022-01-18 om internterkontrollpunkter för år 2022. Utifrån aktuellt granskningsområde har omsorgsstyrelsen inkluderat följande risker:

- Systematiskt arbete med integritetskontroller genom loggar i verksamhetssystem inom omsorgsförvaltningens verksamheter. Risken uppges vara att obehöriga kan nå systemet.
- Rutin för e-post. Risken uppges vara att personuppgifter skickas i e-postmeddelanden inom och utanför förvaltningen.

Bildningsstyrelsen antog sin internkontrollplan på sammanträdet i december 2021. Planen saknar kontrollmoment som kan kopplas ihop med det aktuella granskningsområdet.

I intervjuer uppges att det saknas en samlad uppföljning av det informationssäkerhetsarbete som sker både övergripande i kommunen och på förvaltningarna. Kommunen medverkar i en uppföljning som bedrivs av Länsstyrelsen och som bland annat omfattar kommunens arbete med risk- och sårbarhetsanalys, men kommunen saknar upprättade former för intern uppföljning.

3.5.2 Rapportering

I intervjuer uppges att kommunstyrelsen inte har efterfrågat någon återrapportering av det informations- och IT-säkerhetsarbete som bedrivs i kommunen. I samband med cyberattacken i Kalix kommun förde IT-chefen dagliga anteckningar över bland annat incidenter inom kommunen, omvärldsbevakning av hot samt vilka åtgärder som IT-enheten hade vidtagit. Anteckningarna delgavs kommunalråd, oppositionsråd samt kommunledningen. Rapporteringen skedde på initiativ av IT-chefen och var inget som hade efterfrågats av politiken.

3.5.3 Bedömning

Utifrån det som framkommit i granskningen gör vi bedömningen att det finns behov av att upprätta former för hur uppföljning av informationssäkerhetsarbete ska se ut. Genom att reglera uppföljningsarbetet minimeras risken att uppföljningsarbetet uteblir och på så sätt inte blir en del av ett fortlöpande utvecklingsarbete.

Vi gör bedömningen att styrelserna till viss del har uppmärksammat risker kopplat till granskningsområdet i respektive internkontrollplan. Vi ser dock att samtliga styrelser med fördel kan utöka internkontrollplanerna med ytterligare kontrollpunkter i syfte att säkerställa att informationssäkerheten upprätthålls och vid brister vidtar nödvändiga åtgärder.

4 Slutsats och rekommendationer

4.1 Slutsats

Vår sammanfattande bedömning är att kommunstyrelsen, omsorgsstyrelsen samt bildningsstyrelsen saknar en tillräcklig intern styrning och kontroll som säkerställer ett ändamålsenligt och systematiskt arbetssätt med kommunens informationssäkerhet.

Det saknas till viss del styrande dokument som visar den politiska viljeriktningen med informationssäkerhetsarbetet med tydliga mål, ansvarsfördelning och former för uppföljning avseende det arbete som i dagsläget bedrivs. Vi ser därför ett behov av att en informationssäkerhetspolicy med tillhörande riktlinjer upprättas, fastställs samt implementeras i verksamheten. Det saknas därtill en funktion, exempelvis en informationssäkerhetssamordnare, med rollen att samordna, leda och följa upp arbetet.

Vi ser utöver detta positivt på att IT-enheten kommer att utökas och att det därmed kommer att finnas ett större stöd för verksamheterna i deras arbete.

Vidare är vår bedömning att informationsägarna bör ta ett större grepp om ansvaret över väsentliga moment och hantering av risker och krav för en god informationssäkerhet. Det arbete som i dagsläget bedrivs bör utökas och utvecklas.

Angående den tekniska delen av informationssäkerhetsarbetet gör vi bedömningen att IT-enheten har vidtagit åtgärder i syfte att säkerställa att information skyddas. Åtgärderna syftar till att minska möjligheterna för digitala och fysiska intrång, vilket ger förutsättningar för att i tid upptäcka och hantera hot och risker i former av intrång. Vi ser att arbetet med riskanalyser kan utvecklas genom att dessa dokumenteras.

Slutligen ser vi ett behov av att kommunen har behov av att upprätta former och arbetssätt avseende uppföljning och återrapportering av det informationssäkerhetsarbete som bedrivs, då detta saknas i dagsläget.

4.2 Rekommendationer

Mot bakgrund av vår granskning rekommenderar vi kommunstyrelsen att:

- Upprätta och besluta om en informationssäkerhetspolicy där den politiska viljeriktningen framgår genom att tydligt beskriva mål för arbetet, ansvarsfördelning samt former för uppföljning.
- Säkerställa att riktlinjer för informationssäkerhet upprättas och implementeras som kan konkretisera policyns intentioner.
- Se över nuvarande organisationsstruktur och utreda behovet av en informationssäkerhetssamordnare.
- Upprätta former för genomförande av riskbedömning samt informationsklassning och säkerställa att dessa moment genomförs.

- Ställa krav om uppföljning och återrapportering av kommunens samlade informationssäkerhetsarbete så att beslut kan tas om mål och handlingsplan över erforderliga åtgärder för att förbättra informationssäkerheten.
- Införa kontroller avseende tilldelade behörigheter i syfte att minska risken för otillbörlig tillgång till information samt säkerställa att medarbetare har tillgång till rätt information och system utifrån uppdrag och funktion.
- Säkerställa att utbildning genomförs löpande för samtliga användare för att etablera en medvetenhet och grundläggande kunskap om informationssäkerhet.
- Upprätta incidenthanteringsrutiner och tillhörande process/system för att anmäla och rapportera incidenter. Dessa bör dokumenteras, analyseras och bedömas på kommunövergripande nivå.

Mot bakgrund av vår granskning rekommenderar vi omsorgsstyrelsen och bildningsstyrelsen att:

- Etablera rollen informationsägare och tydliggöra det ansvar som dessa har att efterleva.
- Utse funktion/roller som på informationsägarens uppdrag ska arbeta med styrelsens/förvaltningens informationssäkerhet i enlighet med de krav som ställs i styrande dokument och enligt lagkrav.
- Systematiskt genomföra informationsklassning och riskbedömning av den information som hanteras i system samt utifrån dessa ställa krav om nödvändiga säkerhetsåtgärder.
- Årligen följa upp informationssäkerhetsarbetet och besluta om erforderliga åtgärder för att förbättra informationssäkerheten utifrån aktuella risker och behov.
- Införa kontroller avseende tilldelade behörigheter i syfte att minska risken för otillbörlig tillgång till information samt säkerställa att medarbetare har tillgång till rätt information och system utifrån uppdrag och funktion.
- Tydliggöra incidenthanteringsrutiner och tillhörande process/system för att anmäla och rapportera incidenter. Dessa bör dokumenteras, analyseras och bedömas på nämndnivå.

Avesta kommun
Granskning

2022-07-05

Datum som ovan

KPMG AB

Jenny Thörn
Kommunal yrkesrevisor

Ida Larsson
Kommunal yrkesrevisor