Granskning av informationssäkerhet

Rapport

Svedala kommun

KPMG AB

Datum 2022-06-08

Antal sidor 23

Svedala kommun
Granskning av informationssäkerhet

2022-06-07

Innehållsförteckning

1 Sammanfattning 3

2 Bakgrund 5

2.1 Syfte, revisionsfrågor och avgränsning 5

2.2 Revisionskriterier 6

2.3 Metod 6

2.4 Metodstöd för systematiskt informationssäkerhetsarbete 7

3 Resultat av granskningen 10

3.1 Organisation 10

3.2 Analys av behov och risker för informationssäkerhet 12

3.3 IT-säkerhetsåtgärder 15

3.4 Incidenthantering 16

3.5 Uppföljning, intern kontroll och rapportering 18

4 Slutsats och rekommendationer 20

4.1 Rekommendationer 22

Svedala kommun
Granskning av informationssäkerhet

2022-06-07

1 Sammanfattning

KPMG har av Svedala kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunstyrelsen och nämndernas rutiner för sitt informationssäkerhetsarbete. Uppdraget ingår i revisionsplanen för år 2022.

Syftet med granskningen har varit att bedöma om kommunstyrelsen och nämnderna har en tillräcklig intern styrning och kontroll som säkerställer ett ändamålsenligt och systematiskt arbetssätt med informationssäkerheten i kommunen.

Vår sammanfattande bedömning är att kommunstyrelsen och nämnderna i vissa delar har en tillräcklig intern styrning och kontroll som säkerställer ett ändamålsenligt och systematiskt arbetssätt med informationssäkerheten i kommunen. Vi baserar vår bedömning på följande iakttagelser:

- Det finns styrande dokument i syfte att tydliggöra ansvar och de krav som ställs. Vi bedömer dock att policyn inte fullt ut har implementerats i verksamheten så att en efterlevnad finns i enlighet med dokumentet.
- Utsedd funktion att leda och samordna det kommunövergripande informationssäkerhetsarbetet har inte tillräckliga förutsättningar att prioritera arbetet i förhållande till andra uppdrag så att det ansvar som rollen tilldelats kan upprätthållas fullt ut.
- Kommunstyrelsen och nämnderna har brustit i att etablera det ansvar som informationsägarna har i sitt linjeansvar samt utifrån beskrivning i styrande dokument. Det har i sin tur medfört att väsentliga moment för hantering av risker och krav för en god informationssäkerhet inte har genomförts.
- Bland annat saknas i nuläget ett systematiskt arbete med riskanalys och informationsklassningar för att bedöma skyddsvärde för den information som hanteras. Krav om säkerhetsåtgärder ställs därigenom inte i nuläget mer än vid upphandling och nya införanden.
- I nuläget sker uppföljning till viss del men är inte dokumenterad.
- Det finns beskrivet i styrande dokument hur incidenter ska hanteras. Vi uppfattar dock att rutinerna avseende informationssäkerhetsincidenter inte har uppfattats i verksamheten så att dessa följs och en samstämmighet finns över hur incidenter ska hanteras. Det leder till en risk att incidenter inte upptäcks eller anmäls i tillräckligt hög grad. Det finns etablerade tekniska tjänster med övervakning och larm för att i tid upptäcka och kunna hantera incidenter från IT-enhetens perspektiv.

Vi bedömer att det i stora delar finns ett systematiskt arbetssätt med IT-säkerhet för kommunens IT-infrastruktur. Det har skett löpande modernisering av IT-miljön i syfte att plattformar och system ska vara uppdaterade och säkra. Därtill finns implementerade tjänster för aktiv övervakning och larm om något avvikande sker i IT-miljön som möjliggör för beredskapsgruppen att agera vid ett intrångsförsök eller annat hot. Vi skulle dock gärna se att arbetet utvecklas genom att de åtgärder och investeringar som genomförs tar sin utgångspunkt i dokumenterade riskanalyser. Utifrån dessa kan

exempelvis mål- och handlingsplaner upprättas för att säkerställa att rätt prioriteringar görs utifrån sårbarhet och behov över tid.

För att arbetet ska bli mer ändamålsenligt rekommenderar vi kommunstyrelsen att:

- Revidera styrande dokument så att de är aktuella och omfattar de lagkrav som kommunen har att efterleva i sin informationshantering. I arbetet bör styrelsen beakta om det finns behov av att komplettera styrning av IT-säkerhet och tydliggöra IT-enhetens uppdrag.
- Säkerställa att resurser för att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete finns i enlighet med ambitioner i styrande dokument.
- 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.
- Systematiskt genomföra informationsklassning och riskbedömning av den information som hanteras i system samt utifrån dessa ställa krav om nödvändiga säkerhetsåtgärder.
- Säkerställa att utbildning genomförs löpande för samtliga användare för att etablera en medvetenhet och grundläggande kunskap om informationssäkerhet.
- Tydliggöra incidenthanteringsrutiner och tillhörande process/system för att anmäla och rapportera incidenter. Dessa bör dokumenteras, analyseras och bedömas på kommunövergripande nivå.

För att arbetet ska bli mer ändamålsenligt rekommenderar vi nämnderna att:

- Etablera rollen informationsägare och tydliggöra det ansvar som dessa har att efterleva i enlighet med policyn.
- Utse funktion/roller som på informationsägarens uppdrag ska arbeta med nämndens/förvaltningens informationssäkerhet i enlighet med de krav som ställs i styrande dokument.
- 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.
- 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 Svedala kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunstyrelsen och nämndernas 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. Alltmer 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 kommunstyrelsen och nämnderna 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 och samtliga nämnder. Granskningen avser år 2022.

2.2 Revisionskriterier

Vi har bedömt om styrelsen och nämnderna uppfyller

- 6 kap. 6 § kommunallagen (2017:725)
- Tillämpbara interna regelverk, policys och beslut
- MSB[1]:s rekommendationer avseende Ledningssystem för informationssäkerhet och säkerhetsåtgärder

2.3 Metod

Granskningen har genomförts genom:

Dokumentstudier av:

- Informationssäkerhetspolicy
- Rutiner för personuppgiftshantering samt incidenthantering
- Beredskapsplan för dokumenthantering

Intervjuer har genomförts med:

- Kommunstyrelsens presidium
- Kommundirektör
- Säkerhetschef
- Kommunikationschef
- Informationssamordarare kommunledningskontoret

Vi har därtill efterfrågat skriftliga svar från förvaltningschefer för ett antal frågeställningar. Svar har inkommit från förvaltningarna vård och omsorg samt utbildning. Vi har inte mottagit svar från miljö och teknik.

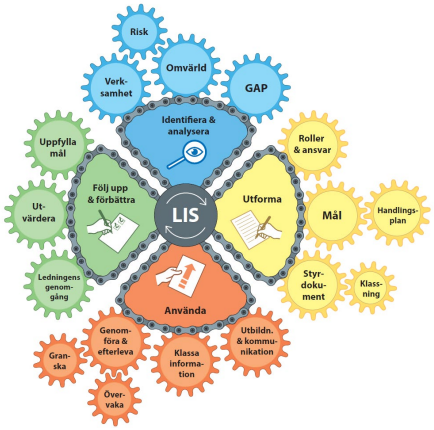
Rapporten är faktakontrollerad av intervjupersoner.

[1] Myndigheten för samhällsskydd och beredskap. MSB har på uppdrag av regeringen ansvar att vara råd- och stödgivande i informationssäkerhetsarbetet och hantera samt förebygga IT-incidenter.

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:

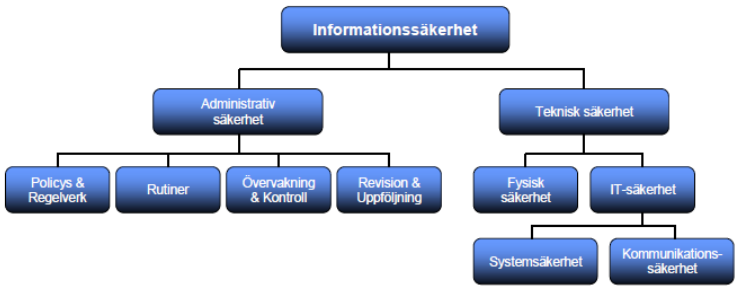
- Kontinuerligt arbete med att klassa organisationens information för att identifiera känslig och kritisk information för att kunna säkerställa tillräckligt skydd.
- Genomföra och efterleva de handlingsplaner och styrdokument som avser informationssäkerhetsarbetet.
- Utbilda och kommunicera informationssäkerhetsfrågor 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 kanbedrivas 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

Kommunens informationssäkerhetsarbete tar sin utgångspunkt i en beslutad informationssäkerhetspolicy[2] och det framgår av policyn att arbetet så långt det är ekonomiskt och praktiskt möjligt ska följa den etablerade standarden SS-ISO/IEC 27000. Målet med policyn är att minska sannolikheten för, eller konsekvenserna av, uppkomna eller identifierade hot mot den information kommunen har en skyldighet att skydda.

Policyn är ett omfattande dokument som bland annat anger hur verksamheterna ska agera för att initiera, bibehålla och förbättra informationssäkerheten i Svedala kommun. Vidare ska det även ses som ett minimikrav vid utveckling eller anskaffning av nya system och e-tjänster och målet för redan driftsatta system.

I policyn anges roller och ansvar samt vilka krav som ställs på respektive roll. Policyn har även en orienteringsmatris så att medarbetaren kan lotsa sig till de delar som denne främst berörs av. I intervjuer får vi till oss att det vid tid för granskningen pågår en revidering av nuvarande informationssäkerhetspolicy då den tidigare versionen antogs 2016. Då den nya policyn är ett arbetsmaterial har vi i granskningen inte fått ta del av den.

Svedala kommun har upprättat rutiner[3] för hantering av personuppgifter i e-post och hantering av personuppgiftsincidenter. Enligt rutinerna är det personuppgiftsansvarig (nämnd eller bolaget) som ansvarar för att det finns rutiner för att kunna upptäcka, rapportera och utreda personuppgiftsincidenter. Av rutinerna framgår till vem/vilka en uppstådd personuppgiftsincident ska rapporteras.

3.1.2 Roller och ansvar

Av informationssäkerhetspolicyn framgår att det är kommunstyrelsen som har det övergripande ansvaret för de interna säkerhetsfrågorna och att det är de som upprättar säkerhetspolicyn. Kommundirektören och säkerhetschefen har det primära ansvaret för säkerhetsfrågorna på uppdrag av kommunstyrelsen. Vidare framgår att uppdraget för att samordna, stödja, utbilda och följa upp kommunens arbete inom säkerhets- och riskhanteringsområdet i huvudsak utförs av säkerhetschefen. I intervjuer uppges att det är kommunens räddningschef som även innehar funktionen säkerhetschef och därmed har det samordnande ansvaret för kommunens informationssäkerhetsarbete. Säkerhetschefen ansvarar även för att stödja och följa upp kommunens arbete inom säkerhets- och riskhanteringsområdet.

---

[2] Kommunstyrelsen, 2016-05-23

[3] 2022-01-27

I intervjuer uppges att den här funktionsfördelningen inte till fullo har bidragit till att kommunen kan bedriva det säkerhetsarbete som de har behov av. En organisationsöversikt som genomfördes 2020 ledde till att hälften av säkerhetschefens operativa delar lades på en av säkerhetschefens medarbetare, som vid tid för granskningen till viss del finansieras med statliga medel. I intervjuer framgår att den här organisationsuppbyggnaden inte har varit idealisk i syfte att kunna bedriva ett systematiskt informationssäkerhetsarbete. Svedala kommun har därför beslutat att rekrytera en ny säkerhetschef som kommer börja sin anställning i juni. Den nya säkerhetschefen kommer att organiseras under kommunens stabschef.

Ansvar för informationssäkerhet är ett linjeansvar som följer med verksamhetsansvaret. Det är förvaltningschef eller motsvarande som är informationsägare och därigenom ett ansvar att säkerställa att informationshanteringen sker på ett korrekt sätt utifrån interna styrdokument och lagkrav.

Av informationssäkerhetspolicyn framgår att informationssäkerhetsarbetet i förvaltningarna ska samordnas och följas upp av förvaltningen utsedd funktion. I intervjuer framgår att det inom kommunens verksamheter finns utsedda GDPR-ansvariga och systemförvaltare. Förvaltningarna anger dock i skriftliga svar att de inte har någon intern organisation eller ansvar utpekat för det praktiska informationssäkerhetsarbetet förutom för dataskyddsarbetet. Utöver detta har kommunen en informationssamordnare som är organiserad inom kommunledningskontoret. Samordnarens ansvar har utökats till att även involvera dataskyddsfrågor samt systemförvaltning för två verksamhetssystem. Det finns inget utpekat informationssäkerhetsansvar, men många av de frågor som samordnaren arbetar med tangerar det området. Informationssamordnaren leder även tillsammans med kommunjuristen en förvaltningsövergripande GDPR-grupp. Gruppen har tagit fram information till intranät och hemsida avseende dataskydd för behandling av personuppgifter i syfte att informera om hur personuppgifter hanteras i kommunen. GDPR-gruppen har även tagit fram mallar för incidentrapportering samt konsekvensbedömning avseende dataskydd för behandling av personuppgifter.

Kommunen har en IT-enhet organiserad under kommunledningsförvaltningen och består av tio medarbetare utöver IT-chefen som leder avdelningen. I informationssäkerhetspolicyn finns en övergripande beskrivning av IT-enhetens ansvar. Bland annat framgår att kommunens digitala nät och grundläggande teknik- och tjänsteplattform tillhandahålls och förvaltas av IT-enheten. I övrigt ska uppdraget regleras genom ett IT-avtal mellan beställare som utgörs av kommunledningen, och leverantören som i detta fall syftar till den interna IT-enheten.

I intervjuer framkommer dock att det saknas en ordentlig uppdragsbeskrivning avseende IT-chefens och andra funktioners roller och ansvarsområde, vilket är något som IT-chefen har arbetat aktivt med under sin tid i kommunen i syfte att försöka förtydliga. IT-chefen har tilldelat nya roller för att förbättra stödet till verksamheterna, dels ett beställarstöd som deltar i upphandling, avtal och som affärsstöd. Dels funktion för verksamhetsstöd som har direktkontakt med systemanvändare och ”super users” för större verksamhetssystem så att verksamheterna kan få mer strategiskt stöd i utvecklingsfrågor kring systemen och vid kontakt med externa leverantörer.

3.1.3 Bedömning

Vår bedömning är att det finns styrande dokument som syftar till att tydliggöra ansvar och de krav som ställs på informationssäkerhetsarbetet. Vi bedömer dock att policyn inte fullt ut har implementerats i verksamheten så att en efterlevnad finns i enlighet med dokumentet. Nuvarande policyn är daterad 2016 vilket är att anses som föråldrad enligt MSB som rekommenderar att en informationssäkerhetspolicy revideras var 3-5 år. Vi ser därför positivt på att arbete med att ta fram nya styrdokument pågår. När dessa har fastställts är det viktigt att det finns en implementeringsplan så att förutsättningar för efterlevnad finns. Vi noterar därtill att det i stora delas saknas styrande dokument för att tydliggöra styrning och uppföljning av den tekniska IT-säkerheten.

Vår bedömning är att kommunstyrelsen och nämnderna endast till viss del har säkerställt att det finns en ändamålsenlig organisation för informationssäkerhetsarbetet. Vi baserar vår bedömning på att kommunstyrelsen inte har säkerställt att den som är utsedd att leda och samordna informationssäkerhetsarbetet har tillräckliga förutsättningar i sin arbetstid i förhållande till andra uppdrag och ansvar, att tillse att arbetet utförs riskbaserat och systematiskt i enlighet med interna beslut angivna styrdokument. Därtill bedömer vi att det inte finns förutsättningar i nuvarande organisation, att följa upp och utvärdera arbetet regelbundet vilket ingår som en uppgift för rollen enligt gällande policy.

Vår bedömning är att kommunstyrelsen och nämnderna brustit i att etablera det ansvar som informationsägarna har i sitt linjeansvar samt utifrån beskrivning av roller och ansvar i styrande dokument. Det har i sin tur medfört att väsentliga moment för hantering av risker och krav för att upprätthålla en god informationssäkerhet inte har genomförts.

Vår bedömning är att kommunstyrelsen i stora delar har säkerställt en ändamålsenlig organisation för arbetet med den tekniska säkerheten i form av kompetens och ekonomiska resurser för IT-säkerhet. Vi ser dock att ansvar och befogenheter ytterligare kan tydliggöras för IT-enhetens uppdrag så deras roll och stödfunktion tydliggörs, samt ett tydliggörande av deras roll i förhållande till förvaltningarnas informationssäkerhetsansvar.

Vi ser positivt på att styrande dokument ska revideras under året samt att kommunstyrelsen beslutat om förstärkning av resurs för säkerhetsarbetet på central nivå.

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 kommuner.

3.2.1 Riskhantering och informationsklassning

Svedala kommun har inte något systematiskt arbete avseende riskbedömning och efterföljande analys. Av intervjupersoner uppges att det under senaste mandatperioden har diskuterats vilken metod som ska användas vid riskanalysarbete, men att det inte har resulterat i något beslut, vilket uppges vara en bidragande orsak till avsaknaden av systematik. Bristen på systematik har även påverkats av att det inte har funnits någon tjänst avsatt för arbetet. Riskbedömning och riskanalys kommer enligt intervjupersoner att finnas med på ett tydligare sätt i den nya informationssäkerhetspolicyn.

Med utgångspunkt i ett osäkert omvärldsläge och med vetskapen om riskerna med cyberattacker har det identifierats ett behov av att ta fram beredskapsplaner för kommunens olika verksamhetssystem. Vi har i granskningen tagit del av ett utkast till beredskapsplan för kommunens dokument- och ärendehanteringssystem. Beredskapsplanen syftar till att så gott det går förbereda verksamheten på eventuella störningar som påverkar systemets funktionalitet och därmed verksamhetens tillgång till den information som finns i systemet.

Enligt nuvarande informationssäkerhetspolicy ska samtliga av kommunens informationssystem vara klassificerade samt att klassificering av informationssystem ska ske före upphandling/anskaffning av systemet eller e-tjänsten. Därefter ska klassificering ske vartannat år alternativt vid förändringar som exempelvis förändrad lagstiftning eller riskbild.

Av policyn framgår även att all information oavsett form ska ges ett lämpligt skydd. Det är den som äger informationen som ska bedöma skyddsnivån utifrån informationens krav på tillgänglighet, riktighet, sekretess/konfidentialitet och spårbarhet. Även själva informationssystemen ska klassificeras, då det ger förutsättningar för att ge rätt skyddsnivå åt den information som de olika systemen hanterar. I policyn finns en klassificeringsmodell för bedömning av skyddsnivå utifrån de tidigare nämnda skyddsnivåerna och utifrån kravnivåerna kritisk, mycket viktig, viktig och mindre viktig.

Intervjupersoner uppger att det i nuläget inte finns något systematiskt arbete med att klassa den information som kommunens verksamheter har tillgång till. I intervjuer beskrivs att klassificering av information främst sker i samband med att ett nytt verksamhetssystem ska upphandlas. Detta sker ofta med stöd av IT eller extern leverantör. Intervjupersoner beskriver att det i nuläget saknas rutiner för att uppdatera bedömningar utifrån nya hot och risker när system och tjänster är i drift. Nya riskbedömningar sker inte utifrån en rutin eller regelbundenhet, utan främst när någon uppmärksammar att det finns behov alternativt vid incidenter/rapporterade avvikelser.

De riskanalyser som har gjorts har främst varit i form av konsekvensbedömningar avseende personuppgiftshantering i enlighet med dataskyddsförordningens krav. Dessa dokumenteras i ett stödsystem, iFacts. Intervjupersoner menar dock att det är en krävande och i vissa delar komplex bedömning som ska göras där verksamheterna hade behövt ytterligare stöd för att säkerställa att bedömningar görs i enlighet med lagkrav. Det krävs också resurser för att regelbundet hålla personuppgiftsförteckningar och bedömningar aktuella och uppdaterade i stödsystemet så att korrekt information finns tillgänglig för de som behöver ta del av den.

Av uppgifter i de skriftliga svaren från förvaltningarna, anges att vissa särskilda rutiner kring behörighetshantering finns etablerat i de verksamheter som hanterar journaluppgifter och känsliga personuppgifter. Där finns bland annat loggkontroller etablerade för att kontrollera att endast medarbetare med rätt att ta del av information kring enskilda har gjort det. Av granskningen framgår att inga avvikelser finns som tyder på att behörigheter behöver justeras.

I intervjuer uppges att i de få fall som kommunen har behövt hantera hemligt material så har detta skett utifrån Försvarsmaktens riktlinjer för klassificering. Dock är detta inte etablerat inom hela kommunen utan har endast använts på verksamhets- och individnivå. I den nya informationssäkerhetspolicyn kommer detta enligt uppgift att finnas med, där riktlinjerna även är uppdaterade utifrån ny lagstiftning.

3.2.2 Medvetenhet och förståelse

Intervjupersoner uppger att medvetenheten har ökat inom kommunen. Med anledning av omvärldsförändringar uppges det finnas ett behov av att belysa de risker som finns balanserat med att inte skapa en rädsla i organisationen. Den ökade medvetenheten har bland annat medfört som nämnts ovan, att kommunen inrättat en särskild tjänst i form av säkerhetschef, som tillträds av en nyrekrytering i juni 2022.

Trots att medvetenheten har ökat uppger intervjupersoner att medvetenheten och kunskapen behöver utökas. Det uppges finnas behov av en kunskapshöjning avseende vad som är en incident i syfte att kunna identifiera när en incident har uppstått. En kunskapshöjning bidrar till det förebyggande arbetet som syftar till att undvika att incidenter uppstår, men bidrar även till att medarbetarna vet om när något har uppstått och i nästa steg kan rapportera händelsen.

I samband med att den nya informationssäkerhetspolicyn samt tillhörande riktlinjer och rutinhandbok ska implementeras har kommunen valt att genomföra en utbildningsinsats genom nanoutbildning[4]. Utbildningarna har skickats ut varannan vecka under 2022 i syfte att öka medvetenheten och kunskapen angående kommunens informationssäkerhet samt IT-säkerhet. I syfte att säkerställa att samtliga tar del av utbildningen kommer kommunen att följa upp deltagarstatistik. Kommunen har även haft i beaktande att nyanställda under året får ta del av utbildningen.

3.2.3 Bedömning

Vår bedömning är att det inte finns ett systematiskt arbetssätt med riskanalyser och informationsklassning. Riskbedömning och informationsklassning görs främst inför implementering av nya system. Det finns inte någon beslutad metod för riskanalys och klassning med mallar och instruktioner för att dessa ska ske på ett likartat sätt förutom för konsekvensbedömningar avseende personuppgiftshantering. Rutiner saknas för att regelbundet ompröva de genomförda informationsklassningar och riskanalyser som

[4] Nanoutbildning är en kort e-kurs som når berörda personer via e-post.

gjorts för att möta nya risker och behov när systemen är i drift. Vi bedömer att ansvar för dessa uppgifter behöver etableras hos informationsägarna och att rutiner inrättas.

Då informationsklassning endast genomförts till viss del sker i nuläget inte någon kravställning av IT-säkerhetsåtgärder som baseras på en bedömning av hur skyddsvärd informationen som hanteras i systemen är.

3.3 IT-säkerhetsåtgärder

I intervjuer beskrivs att utveckling av IT-säkerhet varit en prioriterad fråga från kommunstyrelsen och ledningen under många år. Den interna bedömningen inom IT-enheten är att det finns ekonomiska förutsättningar att vidta nödvändiga åtgärder för en god IT-säkerhet. Bland annat framhålls att det efter den senaste tidens ökade hotbild har fattats ett investeringsbeslut för att tidigarelägga ett införande av multifaktorinloggning för att stärka kommunens åtkomsthantering. Detta är en rekommendation som MSB har på sin åtgärdslista för att verksamheter ska stärka sin förmåga att stå emot cyberhot.

Inom IT-enheten finns en uppdelning av ansvar för säkerhetsarbetet utifrån de olika plattformar och IT-komponenter som de ansvarar för. Enligt uppgift har kommunen arbetat aktivt med att modernisera och implementera system och tjänster för att höja säkerheten och säkerställa driften av kommunens IT-miljö. Bland annat finns rutiner och arbetssätt för att regelbundet och enligt en fastlagd plan uppdatera system och installera säkerhetspatchar mm. Därtill framgår att det finns ett antal säkerhetsfunktioner för klienter (de datorer, telefoner, iPads mm som IT-enheten tillhandahåller till kommunens medarbetare och förtroendevalda), datacenter, nätverk, trådlösa nätverk samt servrar mm. Bland annat har åtgärder vidtagits med väl utvecklade system för backuper, redundans, segmentering med begränsningar på nätverk samt central lösenordshantering.

Därtill har ett antal funktioner för övervakning och aktiva automatiska larm installerats i syfte att tidigt upptäcka eventuella hot och risker mot IT-miljön. IT-enheten har tillsatt en grupp om sju personer som har beredskap för övervakningen dygnet runt vilket har stärkt kommunens förmåga att snabbt kunna agera om ett intrångsförsök sker.

Ett sätt att ytterligare stärka säkerheten är att kommunen har infört en funktion vid upphandling och anskaffning av system där IT agerar ”grindvakt” innan system köps in. Detta för att säkerställa att det nya systemet är tillräckligt säkert och möter de krav som kommunen har beslutat om.

I nuläget finns, som vi beskrivit tidigare i rapporten, ingen etablerad metod för att göra riskanalyser i kommunen. Därigenom har inte heller riskanalyser gjorts för att kunna bedöma sårbarheter och göra prioriteringar av åtgärder för de komponenter som kommunens IT-miljö består av. Vid större införanden har riskanalyser gjorts i samarbete med systemleverantören inför att systemet ska tas i drift. Vad gäller de införanden och åtgärder som vidtagits för att utveckla IT-säkerheten framhålls en systematisk omvärldsbevakning och hög kompetens hos medarbetare inom IT.

Intervjuuppgifter gör gällande att det pågår ett aktivt arbete men att dokumentationen av IT-enhetens arbete kan utvecklas i form av nedtecknade rutiner och processer. Ett exempel som ges är att incidenthanteringsprocessen inte är dokumenterad men att det vid en incident finns en känd process som medarbetare agerar utifrån.

3.3.1 Bedömning

Vår bedömning är att det i stora delar finns ett systematiskt arbetssätt med IT-säkerhet för central IT-infrastruktur. Det har skett löpande modernisering av IT-miljön i syfte att plattformar och system ska vara uppdaterade och säkra. Därtill finns implementerade tjänster för aktiv övervakning och larm om något avvikande sker i IT-miljön som möjliggör att beredskapsgruppen kan agera vid ett intrångsförsök eller annat hot. Om något skulle ske finns etablerade system och rutiner för att säkerställa att inte information ska gå förlorad eller skadad.

Vi skulle dock gärna se att arbetet utvecklas genom att de åtgärder och investeringar som genomförs 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.

3.4 Incidenthantering

I nuvarande informationssäkerhetspolicy finns anvisningar över hur informationssäkerhetsincidenter ska hanteras samt vad som är skillnad mellan en incident och en allvarlig incident.

I policyn anges att incidenter ska rapporteras till Tjänsteman i beredskap, till informationssäkerhetsansvarig samt om incidenten gäller specifik förvaltning även till kontaktperson i förvaltningen. Mycket allvarliga incidenter ska enligt policyn rapporteras genom kommunövergripande incidentrapporteringssystem. Om incidenten är IT-relaterad så ska även IT-support få kännedom om incidenten genom telefon eller e-post. Därtill framgår att kommunen ska ha etablerad kontakt med CERT-SE (Sveriges nationella CSRIT - Computer Security Incident Respons Team) vars uppgift är att stödja samhället i arbetet med att hantera och förebygga IT-incidenter.

I intervjuer uppges att medarbetarna har informerats om att en incident ska anmälas till närmaste chef och sedan till säkerhetschef. Intervjupersoner uppger att det finns behov av ytterligare informationsinsatser angående vart en incident ska anmälas inom kommunens organisation, då det vid flera tillfällen har anmälts direkt till säkerhetschefen i stället för till närmsta chef. Det framkommer även att en anmälan vid vissa tillfällen har fastnat hos medarbetarens chef och att säkerhetschefen inte har nåtts av att incidenten har inträffat. Det uppges att det därmed troligtvis finns ett mörkertal avseende händelser som inte har nått fram till säkerhetschefen. I policyn saknas även anvisningar angående utredning, dokumentation samt vem som ansvarar för att anmäla incidenter till berörda myndigheter när detta krävs. I intervjuer uppges att det i den reviderade informationssäkerhetspolicyn kommer finnas mer detaljerad beskrivning avseende incidenthantering.

Svedala kommun har som tidigare nämnt upprättat rutiner för hantering av personuppgiftsincidenter i syfte att skapa en systematisk och samlad rapportering av den här typen av händelser. När en personuppgiftsincident upptäcks ska den anmälas till nämndens eller bolagets dataskyddsombud och i rutinerna hänvisas medarbetaren till en sida med kontaktuppgifter. Dataskyddsombudet ansvarar för att riskbedöma, utreda, dokumentera och i de fall det behövs anmälas till Integritetsskyddsmyndigheten. Det är varje medarbetares ansvar att rapportera risk för, misstanke om eller inträffade incidenter. Utöver detta innehåller rutinerna en beskrivning över vad som ses som en personuppgiftsincident.

I intervjuer framgår att kommunen i dagsläget inte har infört SLA[5] på något av kommunens verksamhetssystem. I IT-sammanhang reglerar SLA vanligtvis vilken tillgänglighet ett system ska ha, hur lång tid som högst få passera innan felavhjälpning ska påbörjas, hur snabbt felet ska vara åtgärdat och hur många gånger ett fel får förekomma under en given tidsperiod. Ansvaret ligger hos kommunens verksamheter att identifiera och meddela IT-avledningen hur tillgängligt deras verksamhetssystem behöver vara. Intervjupersoner uppger att det i dagsläget inte finns någon kravställning upprättad mellan verksamheterna och IT-enheten.

Avsaknaden av SLA innebär även att det i dagsläget inte finns någon dokumenterad prioritering i uppstart av verksamhetssystemen vid ett driftstopp. Dock uppges att kommunens mest kritiska verksamhet av naturliga orsaker prioriteras först. Av intervjuer framgår även att IT-enheten inte på egen hand skulle besluta om prioritering utan att krisledningsstaben analyserat situationen och ger direktiv över hur de vill att läget ska hanteras och vilken prioritering som ska göras.

I intervjuer anges att IT-enheten vid ett tillfälle upptäckte ett intrång i ett IT-system. Upptäckten gjordes i ett tidigt skede och beslut fattades att omedelbart stänga ner systemet. En analys som kommunen gjorde av händelsen visade att inga skador hade hunnit ske och att den omedelbara nedstängningen troligen bidrog till detta. Vidare uppges att kommunen upptäckt en brist i ett system där det fanns möjlighet till intrång. Kommunen valde även vid det tillfället att stänga ned det berörda systemet och kunde inte identifiera att några intrång eller skador hade skett.

I syfte att säkerställa att informationen som lagras i kommunen inte går förlorad vid en systemstängning har kommunen implementerat ett backupsystem som kontinuerligt säkerhetskopierar data dygnet runt.

Inom vård- och omsorgsförvaltningen har en arbetsgrupp skapats i syfte att arbeta fram åtgärder i de fall deras verksamhetssystem skulle upphöra att fungera. Arbetsgruppen har börjat arbeta med hemtjänst- och hemsjukvårdsinsatser och har bland annat kommit fram till att skriva ut den digitala veckoplaneringen i syfte att ha manuell tillgång till den ifall systemet skulle sluta fungera.

Som vi berört tidigare i rapporten har även en beredskapsplan för kommunens dokument- och ärendehanteringssystem tagits fram. Utifrån ett antal scenarion för IT-

[5] SLA står för Service Level Agreement och är en metod för att ange vilken kvalitetsnivå en leverans ska hålla.

störningar har beskrivningar tagits fram för hur hanteringen ska ske i händelse av incident eller störning där tillgång till systemet saknas.

3.4.1 Bedömning

Vår bedömning är att det finns incidenthanteringsrutiner beskrivna i styrande dokument. Informationssäkerhetsincidenter beskrivs på övergripande nivå och det finns mer specifika rutiner för hantering av personuppgiftsincidenter.

Vi uppfattar bedömer dock att rutinerna avseende informationssäkerhetsincidenter inte har uppfattats i verksamheten så att rutinerna följs och en samstämmighet finns över hur incidenter ska hanteras.

De tekniska implementationer som gjorts i syfte att tidigt upptäcka incidenter och avvikelser i IT-miljön ser vi som ett gott stöd för att i tid upptäcka och kunna hantera incidenter från IT-enhetens perspektiv. IT-enheten bör för sitt interna arbete tydliggöra hur deras rutiner och processer ser ut för att upptäcka, bedöma och vid behov eskalera incidenter.

Det finns i nuläget risk att informationssäkerhetsincidenter inte upptäcks i tillräckligt hög grad av användare. Det kan medföra att incidenter sker som inte utreds och därmed kan utgöra grund i det löpande förbättringsarbetet. Vi bedömer att informations- och utbildningsinsatser bör genomföras över vad som är incidenter och hur dessa ska hanteras så att en tillräcklig medvetenhet och kunskap finns i verksamheten.

Inträffade incidenter bör därtill dokumenteras och analyseras på kommunövergripande nivå så att ansvariga, exempelvis en gruppering där representation finns från säkerhetsenhet, IT-enhet samt berörda för specifika system eller informationsägare kan göra en samlad bedömning om det finns behov av stärkta rutiner, utbildningsinsatser eller annan teknisk åtgärd för att ytterligare stärka kommunens förmåga att vara robusta om eller när en incident sker.

Vi ser positivt på det arbete som påbörjats i några förvaltningar där beredskapsplaner och dialoger genomförs i syfte att vara förberedda och ha en beredskap om incident eller allvarlig IT-störning sker där verksamheten blir utan tillgång till verksamhetssystem och information.

3.5 Uppföljning, intern kontroll och rapportering

3.5.1 Intern kontroll och uppföljning

Kommunstyrelsen beslutade vid sammanträde 2021-11-08 om internkontrollpunkter för år 2022. Utifrån aktuellt granskningsområde har kommunstyrelsen inkluderat följande risker där det även framgår att andra nämnder och verksamhetsområden kan behöva involveras efter behov:

- Risk för allvarliga IT-attacker/hot – Det har uppkommit fler och fler hot via mail eller brandväggar.

Kontrollmomentet består enligt internkontrollplanen av att en uppföljning av angrepp i förhållande till faktiska incidenter där attacken lett till infekterade datorer eller allvarliga konsekvenser.

- Risk för att verksamhetskritiska system havererar – Information försvinner eller förvanskas. Otillgängliga system som gör att medarbetare inte kan utföra sina arbeten. Effekten kan bli att löner kanske inte kan betalas ut, vattenpumpar slutar fungera, webbsidan inte går att nås av medborgarna, utbetalningar av fakturor uteblir.

Kontrollmomentet innebär att IT-enheten utför koncentrerade kontroller av verksamhetskritiska system och processer och sammanställer en rapport över IT-infrastrukturens mående genom ett antal mätbara nyckeltal.

Det hade vid tiden för granskningen inte genomförts någon uppföljning av internkontrollpunkterna för 2022. Enligt reglemente för internkontroll är det varje nämnd och kommunstyrelsen som ansvarar för att följa upp det interna kontrollsystemet inom verksamhetsområdet.

Uppföljning av informationssäkerhetsarbetet görs enligt intervjupersoner vid behov eller som en direkt uppföljning utifrån den kravställning som görs vid införandet av nytt system, projekt eller dylikt. Det är verksamhetens ansvar att göra en uppföljning inom den struktur/system eller implementering som verksamheten gör.

Det finns begränsad systematisk uppföljning och kontroll av att verksamheterna arbetar i enlighet med den policy som finns beslutad. Det arbete som har skett årligen samt med mandatperiodsintervall kring arbetet med nya säkerhetsriktlinjer, risk- och sårbarhetsanalysarbete samt kontinuitetsarbete har enligt intervjupersoner varit en del av en indirekt kontroll av att arbetet följs.

Det finns en förhoppning att uppföljning av det informationssäkerhetsarbete som bedrivs kommer att utökas med anledning av att det inom kommunen kommer att finnas en tjänst dedikerad till uppdraget.

Vad gäller uppföljning av vidtagna IT-säkerhetsåtgärder så genomförs regelbundet sårbarhetsscanningar och proaktiva analyser för att identifiera sårbarheter. En större säkerhetsgenomgång genomfördes för två år sedan av hela Microsoft-miljön.

3.5.2 Rapportering

I intervjuer uppges att återrapportering kring det informationssäkerhetsarbete som bedrivs sker en gång om året till kommunstyrelsen. Kommunstyrelsen har efterfrågat information om hur arbetet bedrivs och har även beslutat om tilläggsanslag för att ytterligare stärka IT-säkerheten genom åtgärder för en säkrare åtkomsthantering. Den rapportering och uppföljning som gjorts är dock inte dokumenterad mer än i form av en protokollsanteckning i kommunstyrelsens protokoll.

I samband med kommunstyrelsens beslut om internkontrollpunkter för år 2022 noterades även i protokollet att styrelsen hade önskemål om att IT-chef presenterar för styrelsen hur kommunen i nuläget arbetar med allvarliga IT-attacker/hot. Vi noterar genom protokollsläsning att så har skett vid kommunstyrelsens nästkommande

sammanträde den 2021-11-29 där IT-chef och IT-driftstekniker medverkar och föredrar i ärendet.

3.5.3 Bedömning

Vår bedömning är att kommunstyrelsen till viss del har etablerat arbetssätt och rutiner för att kontinuerligt följa upp genomförda säkerhetsåtgärder. Vi konstaterar att arbetet med den tekniska säkerheten är prioriterat och åtgärder vidtas som i vissa delar följs upp. Vi gör bedömningen att rapportering och uppföljning bör dokumenteras då det bidrar till att tydliggöra det arbete som bedrivs samt vilka ytterligare åtgärder som behöver vidtas.

Kommunstyrelsen har beslutat om internkontrollpunkter för år 2022 som ytterligare kan stärka uppföljning av arbetet för att hantera IT-attacker och hot samt bedöma behov av åtgärder för att inte verksamhetskritiska system ska haverera eller riskera att skada verksamhet eller enskild. Då ingen uppföljning eller kontroller gjorts för punkterna vid tiden för granskningen har vi inte kunnat bedöma om den interna kontrollen är tillräcklig.

Vår bedömning är att kommunstyrelsen och nämnderna inte har ett ändamålsenligt arbete med att följa upp att beslut och styrdokument relaterat till informationssäkerhet efterlevs. Det har inte gjorts några interna revisioner eller utvärderats på annat sätt hur kommunstyrelsen, nämnderna och dess verksamheter efterlever de krav som ställs i informationssäkerhetspolicyn. Vi kan dock notera från granskningens iakttagelser att det finns brister i efterlevnad då väsentliga moment i arbetet inte har genomförts så att arbetet är systematiskt och riskbaserat.

Återrapportering av arbetet har gjorts till kommunstyrelsen, det finns dock inte någon dokumenterad uppföljning av kommunens samlade informationssäkerhetsarbete där underlag kan ligga till grund för beslut om förbättringsåtgärder för att utveckla arbetet. Vi noterar vidare att det finns en medvetenhet om att kommunen i nuläget har en bristande uppföljning och kontroll av informationssäkerhetsarbetet. Detta är något som förväntas förbättras genom den förstärkning på säkerhetsenheten som gjorts med start i juni 2022 samt med grund i det pågående arbetet med att revidera styrdokument för informationssäkerhet.

4 Slutsats och rekommendationer

Vår sammanfattande bedömning är att kommunstyrelsen och nämnderna i vissa delar har en tillräcklig intern styrning och kontroll som säkerställer ett ändamålsenligt och systematiskt arbetssätt med informationssäkerheten i kommunen.

Kommunstyrelsen har genom beslut av styrande dokument tydliggjort styrningen för ett systematiskt informationssäkerhetsarbete. Vi bedömer dock att policyn inte fullt ut har implementerats i verksamheten så att en efterlevnad finns i enlighet med dokumentet. Kommunstyrelsen och nämnderna har brustit i att etablera det ansvar som informationsägarna har i sitt linjeansvar samt utifrån beskrivning i styrande dokument. Därtill har utsedd funktion för att samordna, leda och följa upp arbetet inte haft

tillräckliga förutsättningar att ta sig an ansvaret vid sidan om andra ansvar och uppgifter.

Att informationsägarna inte har fullföljt sitt ansvar har medfört att väsentliga moment för bedömning och hantering av risker och krav för en god informationssäkerhet inte har genomförts. Därtill finns i nuläget en bristande uppföljning av efterlevnad av styrande dokument samt de säkerhetsåtgärder som genomförts i syfte att förbättra informationssäkerheten. Den uppföljning som sker behöver enligt vår bedömning utvecklas då det i nuläget inte sker på ett strukturerat vis och den inte är dokumenterad.

Vår bedömning är slutligen att det har genomförts ett antal väsentliga åtgärder för att säkerställa den tekniska delen av informationssäkerhetsarbetet. IT-enheten har vidtagit ett stort antal åtgärder för de IT-komponenter som utgör kommunens IT-miljö i syfte att upprätthålla en god IT-säkerhet. Genom att implementera moderna och väl utvecklade system och tjänster för en robust och driftssäker IT-miljö ges förutsättningar att i tid upptäcka och hantera hot och risker i form av intrång eller attack. IT-enheten har därtill organiserat en beredskapsgrupp med ansvar för att övervaka och kontrollera aktivitet i IT-miljön som har beredskap dygnet runt, vilket vi ser som positivt.

Vi bedömer att IT-enhetens arbete ytterligare kan utvecklas genom att de åtgärder som beslutas att genomföras baseras på riskanalyser och bedömningar över prioriteringar utifrån identifierade sårbarheter och behov. Därtill anser vi att arbetssätt, rutiner och uppföljning bör dokumenteras på ett bättre sätt för att säkerställa en kontinuitet och minska sårbarheten i händelse av personalförändringar, nya krav eller behov av stärkta rutiner och förändrade arbetssätt utifrån nya risker eller organisatoriska förändringar.

4.1 Rekommendationer

Mot bakgrund av vår granskning rekommenderar vi kommunstyrelsen att:

- Revidera styrande dokument så att de är aktuella och omfattar de lagkrav som kommunen har att efterleva i sin informationshantering. I arbetet bör styrelsen beakta om det finns behov av att komplettera styrning av IT-säkerhet och tydliggöra IT-enhetens uppdrag.
- Säkerställa att resurser för att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete finns i enlighet med ambitioner i styrande dokument.
- 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.
- Systematiskt genomföra informationsklassning och riskbedömning av den information som hanteras i system samt utifrån dessa ställa krav om nödvändiga säkerhetsåtgärder.
- Säkerställa att utbildning genomförs löpande för samtliga användare för att etablera en medvetenhet och grundläggande kunskap om informationssäkerhet.
- Tydliggöra 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 nämnderna att:

- Etablera rollen informationsägare och tydliggöra det ansvar som dessa har att efterleva i enlighet med policyn.
- Utse funktion/roller som på informationsägarens uppdrag ska arbeta med nämndens/förvaltningens informationssäkerhet i enlighet med de krav som ställs i styrande dokument.
- 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.
- Tydliggöra incidenthanteringsrutiner och tillhörande process/system för att anmäla och rapportera incidenter. Dessa bör dokumenteras, analyseras och bedömas på nämndnivå.

Svedala kommun
Granskning av informationssäkerhet

2022-06-07

Datum som ovan

KPMG AB

DocuSigned by:
Jenny Thörn
E1872868AB3D4FC...
Jenny Thörn
Kommunal yrkesrevisor

DocuSigned by:
Ida Larsson
E0450C42F7F9456...
Ida Larsson
Kommunal yrkesrevisor

DocuSigned by:
Ida Brorsson
94C78967DB4746A...
Ida Brorsson
Certifierad kommunal revisor