Granskning informationssäkerhet

Rapport

Bromölla kommun

KPMG AB

2021-05-24

Antal sidor 19

Antal bilagor 1

Bromölla kommun
Granskning informationssäkerhet

2021-05-24

Innehållsförteckning

Bromölla kommun
Granskning informationssäkerhet

2021-05-24

1 Sammanfattning

KPMG har av de förtroendevalda revisorerna i Bromölla kommun fått i uppdrag att genomföra en granskning av kommunstyrelsen och dess utskotts rutiner för informationssäkerhetsarbetet. Uppdraget ingår i revisionsplanen för 2021.

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen och utskotten inte har säkerställt ett ändamålsenligt och systematiskt arbete med kommunens informationssäkerhet.

Vi baserar bland annat vår bedömning på följande iakttagelser:

- Det saknas en ändamålsenlig organisation för informationssäkerhetsarbetet. Med nuvarande resurser ser vi det osannolikt att förutsättningar finns för ett systematiskt arbete med kommunens informationssäkerhet. Det finns ingen centralt utsedd funktion med ansvar att leda och samordna arbetet. Det saknas även utsedda representanter som på informationsägarens uppdrag kan utföra det praktiska arbetet utifrån interna styrdokument och regelverk.
- Styrande dokument är i delar föråldrade och det är otydligt hur de förhåller sig till varandra. Styrdokumenten i dess nuvarande form brister i att tydliggöra ansvarsfördelning och hur arbetet ska bedrivas.
- Det saknas ett systematiskt arbete med riskanalyser och informationsklassning för att säkerställa att säkerhetsåtgärder är vidtagna som står i relation till hur skyddsvärd informationen är. Utan denna bedömning kan inte verksamheten göra ett val av säkerhetsåtgärder som står i relation till risker och sårbarheter.
- Det finns en rutin för incidenthantering beskriven i styrande dokument. Då de styrande dokumenten inte är aktuella och inte kommuniceras i verksamheten finns en påtaglig risk att incidenter sker utan att de upptäcks och anmäls. Inträffade incidenter dokumenteras inte på övergripande nivå så att de kan användas i ett systematiskt förbättringsarbete och säkerställa att de inte sker igen.
- I nuläget sker ingen systematisk uppföljning och det är inte tydliggjort i styrdokument hur uppföljning och rapportering ska gå till. Det finns inte tillräckliga underlag och analyser gjorda för att bedöma vilka behov av förbättringsåtgärder som finns för informationssäkerheten så detta är inte beslutat i handlingsplan eller mål.

Med nuvarande status på informationssäkerhetsarbetet bedömer vi att det finns en påtaglig risk att kommunens informationstillgångar inte på ett tillräckligt sätt skyddas och att kraven på dess konfidentialitet, riktighet och tillgänglighet tillgodoses. Med den stora mängd information som hanteras i en kommun innebär bristerna att kommunen kan råka ut för både ekonomisk skada samt förtroendeskada som en konsekvens.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen och utskotten att:

- Etablera en organisation för informationssäkerhetsarbete med central samordnare och utsedda representanter i verksamheten samt tilldela dessa funktioner resurser i form av tid och kompetens så att förutsättningar för ett systematiskt arbete säkerställs.
- Revidera och upprätta styrande dokument så att dessa är aktuella och kan utgöra en sammanhållen helhet för styrningen av kommunens informationssäkerhetsarbete.
- Upprätta en årlig handlingsplan med prioriterade åtgärder och aktiviteter för att utveckla informationssäkerhetsarbetet.
- Besluta om en modell för informationssäkerhetsklassning och riskbedömning för kommunens informationstillgångar och sedan genomföra informationsklassningar i prioriteringsordning utifrån en bedömning av de system som är mest verksamhetskritiska.
- Säkerställa att nya och befintliga medarbetare får del av utbildning och information om informationssäkerhet så att en tillräcklig medvetenhet och kunskap finns över enskildas hantering och för att upptäcka incidenter.
- Besluta om kommunövergripande rutin för hantering av informationssäkerhetsincidenter och säkerställa att inträffade incidenter dokumenteras på övergripande nivå samt analyseras och följs upp som en del i det systematiska förbättringsarbetet.
- Säkerställa att uppföljning av beslutad handlingsplan och kommunens informationssäkerhetsarbete sker genom att etablera en årlig rapportering i form av ledningens genomgång till kommunstyrelsen.

2 Bakgrund

KPMG har av Bromölla kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunstyrelsens och samtliga nämnders rutiner för sitt informationssäkerhetsarbete. Uppdraget ingår i revisionsplanen för år 2021.

Organisationer i offentlig sektor hanterar ovärderliga informationstillgångar och blir alltmer beroende av sina informationssystem. Ny teknik innebär nya möjligheter men introducerar även nya risker som ställer krav på ett balanserat risktagande och ett väl fungerande säkerhetsarbete. Brister i hanteringen kan leda till förtroendeskada för organisationen.

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

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

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

2.1 Syfte, revisionsfråga och avgränsning

Granskningen syftar till att bedöma om kommunen har ett ändamålsenligt och systematiskt arbetssätt med sin informationssäkerhet.

Granskningen ska besvara 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 för att säkerställa informationssäkerheten?
- Finns incidenthanteringsrutiner och sker en tillräcklig rapportering av inträffade incidenter?
- Görs systematiska uppföljningar av genomförda åtgärder för att kontinuerligt förbättra informationssäkerheten?
- Finns etablerade rapporteringsvägar för att kontinuerligt besluta om åtgärder för att utveckla arbetet?

Granskningen omfattar kommunstyrelsen och dess utskott. Granskningen avser år 2021.

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 (se bilaga 1) och intervjuer med berörda tjänstepersoner. Följande funktioner har medverkat i intervjuer:

- Kommunchef
- Säkerhets- och beredskapsansvarig
- Kommunikatör
- IT-chef (kommunalförbund)
- IT-strateg (kommunalförbund)
- IT-samordnare stöd och omsorg

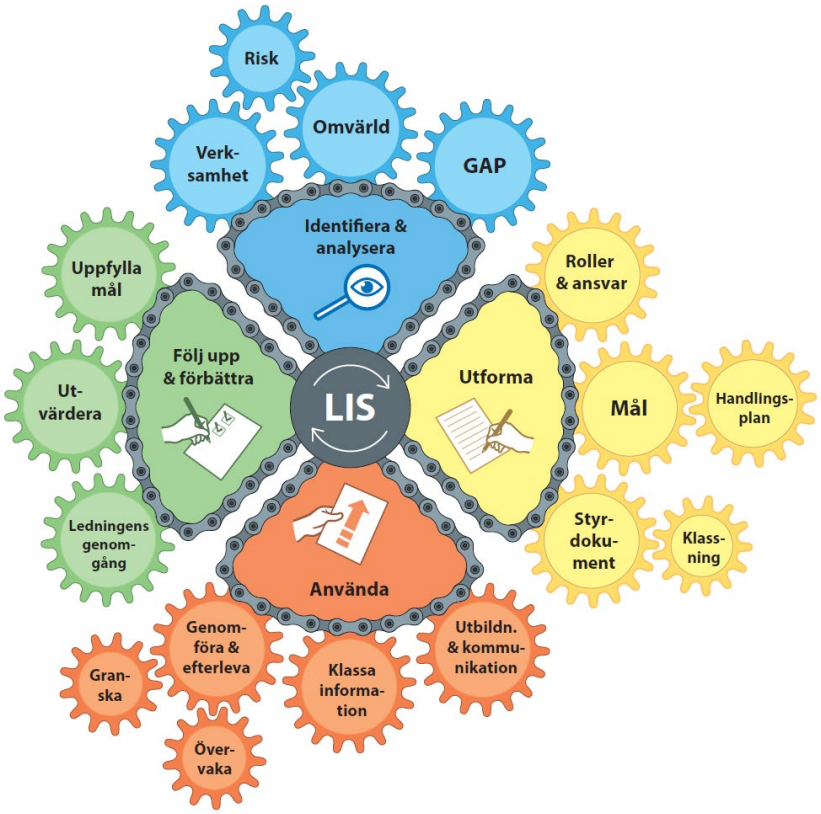
Samtliga intervjupersoner har erbjudits att faktagranska rapporten.

Granskningen har utförts av Jenny Thörn, verksamhetsrevisor och specialist. Lars Jönsson, certifierad kommunal revisor har deltagit i granskningen som kvalitetssäkrare utifrån sin roll som kundansvarig.

2.4 Metodstöd för systematiskt informationssäkerhetsarbete

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

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



2.4.1 Identifiera och analysera

Syftet med att analysera avseende 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 informationssäkerhetsarbete.

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

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

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

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 ledningen, 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 åtskild från organisationens interna IT-produktion och drift. Anledningen till det är att informationssäkerhetssamordnaren både ska granska och vara kravställande gentemot IT-driften och riskerar annars att brista i opartiskhet.

3 Resultat av granskningen

3.1 Organisation

3.1.1 Roller och ansvar

I *Policy för säkerhet och krisberedskap*[1] anges att ansvaret för säkerhetsarbetet följer verksamhetsansvaret på alla nivåer i kommunen. Kommunstyrelsen har det övergripande ansvaret för inriktning i den kommunala verksamheten vilka tydliggörs i beslutade riktlinjer för säkerhetsarbetet.

Av *Kommunövergripande riktlinjer för säkerhetsarbete*[2] framgår att ”det är av stor vikt att det inom kommunen finns en uttalad säkerhetsorganisation med tydlig ansvarsfördelning”. Vidare finns beskrivet att alla anställda inom verksamheten är skyldiga att aktivt arbeta för ökad säkerhet. Kommunens säkerhets- och beredskapssamordnare svarar under kommunchefen för samordning av säkerhets- och krisberedskapsarbetet.

I intervjuer beskrivs att kommunens säkerhets- och krisberedskapssamordnare har i uppdrag att etablera ett säkerhetsarbete utifrån säkerhetsskyddslagen. Tjänsten är finansierad av statliga bidrag för beredskapsarbete och därigenom är arbetsuppgifterna i stort låsta till de åtgärder som kommunen har behov av inom krisberedskap och krishantering. Det finns inte någon ytterligare funktion som deltar i säkerhetsarbetet centralt.

Det finns inom vissa verksamheter ett tilldelat ansvar till systemförvaltare som utifrån verksamhetens behov arbetar med informationssäkerhet. Detta sker främst för åtkomsthantering, lagring samt hantering av känsliga uppgifter i verksamhetssystem, e-post mm. Intervjupersoner anger att det inte är uttalat vem eller vilka som är mottagare av information och hur kommunen ska organisera informationssäkerhetsarbetet.

Intervjupersoner menar att de är medvetna om risker och brister och upplever att det är frustrerande att inte det skapas förutsättningar för en organisation och tilldelade resurser. Det är inte uttalat vem som ska styra arbetet och därför otydligt vem eller vilka som är delaktiga i kommunens informationssäkerhetsarbete. Det finns därför ingen sändare eller mottagare av information. I nuläget upplevs en avsaknad av resurser både gällande tid och kompetens.

3.1.2 Styrdokument

I ett ledningssystem för informationssäkerhet rekommenderas att arbetet utgår från en policy för informationssäkerhet där mål och syfte framgår tillsammans med ett tydliggjort ansvar för arbetet. Enligt MSB:s metodstöd bör informationssäkerhetspolicyn ej uppdateras årligen då det är ett strategiskt dokument som avser viljeriktningen med informationssäkerheten. Samtidigt beskrivs informationssäkerhet som ett föränderligt

[1] Beslutad av kommunfullmäktige 2016-09-15
[2] Beslutad av kommunstyrelsen 2018-08-17

område, vilket innebär att den riskerar att bli förlegad om den uppdateras för sällan. En rimlig livslängd på en informationssäkerhetspolicy är enligt MSB ca. 3–5 år.

Policyn behöver sedan konkretiseras i riktlinjer och/eller anvisningar för att det ska finnas mer detaljerade beskrivningar som kan utgöra styrning och stöd för det praktiska arbetet med informationssäkerhet.

Policy för säkerhet och krisberedskap

I *Policy för säkerhet och krisberedskap* framgår att ett systematiskt säkerhetsarbete är en förutsättning för att kunna trygga god beredskap, krishantering och säkerhet för människor som bor, verkar eller vistas i kommunen. Syftet med policyn är att skydda, förhindra eller begränsa skador på egendom och miljö. Gällande informationssäkerhet ska detta bland annat uppnås genom att säkerställa informationens riktighet, sekretess och tillgänglighet.

Kommunövergripande riktlinjer för säkerhetsarbete

I *Kommunövergripande riktlinjer för säkerhetsarbete* finns avsnitt om informationssäkerhet. Följande finns beskrivet i avsnittets inledning ”en hög säkerhet på de digitala informationssystemen ett krav för att kunna hålla en hög informationssäkerhet”. Vidare beskrivs att målsättningen med riktlinjerna är att skydda kommunens informationstillgångar mot alla tänkbara hot – interna eller externa, avsiktliga eller oavsiktliga. För att informationen skall kunna skyddas framgår av riktlinjen att det krävs att samtliga verksamheter inom kommunen har kontroll över den egna säkerheten samt tar ansvar för de digitala informationssystem som används.

Informationssäkerhet ska enligt riktlinjen uppnås genom:

- Vi följer kommunal författningssamling Nr 005.6 *(anm. referens till Riktlinje för informationssäkerhet)*
- IT-funktionen svarar för de tekniska kunskaperna och åtgärderna gällande digitala informationssystem.
- Systemägare är utsedda för samtliga digitala informationssystem.
- Informationen skyddas mot obehörig åtkomst.
- Informationens riktighet, sekretess och tillgänglighet säkerställs i samtliga miljöer.
- Rutiner för utlämning av handlingar finns.
- Rutiner och regler för åtkomst och säkerhet i kommunens datanät är tydlig.
- Alla IT-incidenter, konstaterade eller misstänkta, rapporteras till och undersöks av IT-funktionen.

Riktlinjer för informationssäkerhet

Det saknas i nuläget en policy för informationssäkerhet men kommunen har som framgår ovan *Riktlinjer för informationssäkerhet*[3]. Riktlinjerna anger att arbetet ska inriktas och bedrivas så att det blir en integrerad del av kommunens normala verksamhet. Alla som hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten. Det är också ett ansvar för chefer på alla nivåer att aktivt verka för en positiv attityd till säkerhetsarbetet.

Mål för informationssäkerhetsarbetet är:

- all personal har kunskap om gällande informationssäkerhetsregler,
- informationsförsörjningen är säker, effektiv och bidrar till ökat skydd och stöd för medarbetare, samverkande partners och tredje man,
- gällande lagar, förordningar och föreskrifter följs,
- ingångna avtal är kända och följs,
- krishanteringsförmågan upprätthålls,
- det finns tillgång till en gemensam, säker och väl definierad infrastruktur för extern och intern datakommunikation,
- alla investeringar både i form av information och teknisk utrustning skyddas i tillräcklig grad,
- hotbilden för varje enskilt informationssystem som är av vikt för vår verksamhet analyseras fortlöpande samt att
- händelser i informationssystemen som kan leda till negativa konsekvenser förebyggs

Till *Riktlinjer för informationssäkerhet* finns två beslutade instruktioner, en *Informationssäkerhetsinstruktion - användare* och en *Informationssäkerhetsinstruktion - förvaltning* (av system). Av riktlinjer framgår att det även ska finnas en informationssäkerhetsinstruktion för kontinuitet och drift men någon hänvisning till denna har inte gjorts i granskningen.

Av vår dialog med tjänstepersoner inom kommunledningsförvaltningen framgår att *Riktlinjer för informationssäkerhet* är föråldrad och i behov av revidering. Riktlinjerna anges därigenom inte vara styrande för arbetet och är inte implementerad i verksamheten så att den är känd och tillämpas.

Granskning har dock inkluderat *Riktlinjer för informationssäkerhet* då den fortfarande är gällande som styrdokument i avsaknad av nya och uppdaterade styrdokument. I riktlinjerna finns mål angivna samt till viss del ansvar och roller i arbetet. Vi noterar dock att roller och ansvar som beskrivs till stor del gäller systemägare,

[3] Antagen av KF 2013-09-30 § 151

systemförvaltare och övriga roller i ett IT-perspektiv och inte informationsägare vilka har det formella ansvaret för informationen som hanteras och skyddet av dessa.

Övriga styrande dokument

Vi noterar att det finns en *Riktlinje för IT-användning* som beslutades av kommunfullmäktige 2004-08-30. Med hänsyn till dokumentets ålder och den tekniska utveckling som skett sedan fastställandet har vi inte inkluderat denna i vår dokumentgranskning.

Vi har tagit del av ett antal policys och rutiner som är framtagna och beslutade efter att de övergripande styrdokumenten för informationssäkerhet fastställts. Flertalet av dessa är framtagna för att tydliggöra rutiner inom stöd och omsorg och är beslutade av verksamhetschef. Bland annat rutin för mobila enheter, rutin för e-post samt en rutin för krypterad information som innehåller personuppgifter.

Övriga exempel är policy för hantering av personuppgifter samt styrdokument utifrån säkerhetsskyddslagstiftningen, bland annat avseende hemliga handlingar.

3.1.3 Bedömning

Vår bedömning är att det inte finns en ändamålsenlig organisation för informationssäkerhetsarbetet. Rekommendation från MSB är att det ska finnas en centralt utsedd samordnare med uppdrag att leda arbetet och vara ett stöd till verksamheten men även att denne ska granska så att arbetet sker i enlighet med internt beslutade styrdokument och planer. Det saknas i nuläget utsedd funktion med ett övergripande ansvar att samordna och leda informationssäkerhetsarbetet i kommunen. Det finns inte heller några utsedda representanter som kan utföra det praktiska arbetet med åtgärder för informationssäkerheten i enlighet med interna styrdokument eller regler som finns att förhålla sig till.

Vår bedömning är att de styrande dokumenten i nuvarande form brister avseende att tydliggöra vilka krav som ställs och hur arbetet ska bedrivas. De dokument som är gällande vid tiden för granskningen är i vissa delar föråldrade och i behov av revidering. De är inte heller implementerade i tillräckligt hög grad så att de efterlevs i organisationen. Det saknas ett inbördes samband mellan dokument för att utgöra en sammanhållen helhet för styrningen av informationssäkerhetsarbetet. Riktlinjer och instruktioner på övergripande nivå har kompletterats med nya policys, riktlinjer och rutiner vilket är positivt då förutsättningarna ser annorlunda ut idag mot 2013 och tidigare när flertalet dokument fastställdes. Vi anser dock att det i nuläget är alltför otydligt hur användare ska förhålla sig till de olika dokumenten. Utan uppdaterade styrdokument som ingår i en sammanhållen helhet där roller och ansvar är tydliggjort är det svårt att utkräva ansvar och vid behov vidta disciplinära åtgärder om brister i efterlevnaden upptäcks.

I enlighet med styrande dokument så följer ansvaret för informationssäkerhet och kommunens övriga säkerhetsarbete verksamhetsansvaret. Det innebär att det är cheferna som har det formella ansvaret för att informationstillgångarna skyddas mot

interna och externa hot och säkerställa dess konfidentialitet, riktighet och tillgänglighet. Vi anser att det finns en risk att den bristande organiseringen och avsaknad av styrande dokument för informationssäkerhetsarbetet leder till att det i nuläget inte finns en tillräcklig tydlighet över hur ansvaret är fördelat så att nödvändiga åtgärder kan vidtas utifrån ansvarsfördelning.

3.2 Analys av behov och risker för informationssäkerhet

Informationssäkerhet handlar om att skydda information ur olika aspekter och tre centrala perspektiv eller egenskaper hos information som är väsentliga att beakta i analyser och riskbedömning är:

- Konfidentialitet
  Att förhindra att information inte röjs för obehöriga.
- Riktighet
  Att vi kan lita på att den information vi använder i vår verksamhet är korrekt och inte manipulerad.
- Tillgänglighet
  Att säkerställa att informationen är tillgänglig när vi behöver den.

3.2.1 Informationsklassificering

För att tydliggöra att olika typer av information har olika värde för verksamheten bör en klassning av information och system genomföras. Kommunen kan därefter skapa förutsättningar för lämpliga skyddsnivåer. Detta görs oftast med en systemöversikt där ansvar och roller är definierade och dels med stöd av någon metod för informationsklassning.

I intervjuer framkommer att kommunen inte har beslutat om någon modell för informationsklassning och inte påbörjat arbetet med att klassa sina system eller den information som hanteras i dessa. Det beskrivs därtill att en kartläggning behöver göras för att identifiera samtliga system.

Intervjupersoner uppger att det till viss del skett bedömningar utifrån lagrum för specifika verksamhetsområden inom exempelvis socialtjänst, vård- och omsorg samt i samband med att nya dataskyddsförordningen började gälla. Ett arbete uppges vara påbörjat med registerförteckningar utifrån GDPR.

Intervjuperson beskriver att det utifrån systemförvaltarrollen finns en naturlig koppling till informationssäkerhetsarbete och dataskydd i förvaltningens verksamheter. Ett arbete är bland annat påbörjat med systemförvaltningsplan för verksamhetssystemet Treserva (används inom stöd och omsorg). Det pågår även ett utvecklingsarbete för att ta fram en informationshanteringsplan.

Det framkommer i intervjuer att det vid implementering av nya system till viss del sker en bedömning och ställningstaganden avseende informationssäkerhet där IT-enheten i

dialog med systemförvaltare för systemet tar beslut om säkerhetsnivåer. Det finns dock ingen dokumenterad process för dessa bedömningar eller tydliggjorda krav för olika säkerhetsnivåer.

Eftersom skadeverkningarna av bristande säkerhet uppstår hos informationsägaren, dvs verksamheten, är det informationsägaren som måste bedöma risker och ställa krav bland annat genom informationsklassning. Efter klassningen ska åtgärdsplaner upprättas. Åtgärdsplanerna handlar om olika saker där IT-säkerhetsåtgärder rent tekniskt är en del. Det kan även vara att göra mer utförliga risk- och konsekvensanalyser, förbättra rutiner eller andra åtgärder som bedöms nödvändiga för att säkerställa säkerheten för informationstillgångarna.

3.2.2 Riskhantering

I intervjuer beskrivs att det inte har skett några riskanalyser specifikt för informationssäkerhet.

På kommunövergripande nivå har man påbörjat arbetet med en riskanalys utifrån identifiering av samhällsviktiga verksamheter inom kommunen. Mallen är framtagen utifrån MSB:s vägledning[4] och på uppdrag från Länsstyrelsen. Vi har i granskningen tagit del av riskdokumentet där arbetet är påbörjat inom området kommunikation och information. Exempel på parametrar som bedöms inom respektive område är kritiska beroende, acceptabla avbrottstider, påverkan på skyddsvärde mm. Intervjupersoner anger dock att underlaget behöver kompletteras för att vara heltäckande och i nuläget har inte åtgärdsförslag för att möta sårbarheter tagits fram.

3.2.3 IT-styrning/Systemförvaltning

Kommunens IT är outsourcad till ett kommunalförbund där även Sölvesborgs kommun är ägare. Det pågår en nedläggning av kommunalförbundet och Bromölla kommun utreder alternativ för sin IT-drift. Det finns ett inriktningsbeslut och en avsiktsförklaring för ny samverkanspart för IT-drift men det formella beslutet har ännu inte tagits.

Intervjupersoner anger att det inte är så tydligt hur ansvarsfördelningen är mellan kommunen och förbundet. Det saknas i nuläget en kravställning och beställning från kommunen som informations- och systemägare för exempelvis tillgänglighet, återställningstider, servicenivåer mm. Dialog mellan förbundet och kommunen sker främst genom systemförvaltarna där diskussioner sker om själva systemet och inte specifikt om informationssäkerhet.

Kommunalförbundet har ett pågående utvecklingsprojekt som finansierats av ägarkommunerna. I projektet har betydande implementeringar gjorts för att förbättra driftssäkerheten samt IT-säkerheten för IT-infrastrukturen avseende nätverk, servrar, brandvägg mm. Det har även implementerats funktioner för övervakning av trafik och beteendemönster i IT-miljön för ett mer proaktivt arbete än reaktiva åtgärder när hot mot informationstillgångar eller intrång redan skett.

[4] Vägledning för identifiering av samhällsviktig verksamhet (MSB 1408-juni 2019)

3.2.4 Åtkomst- och behörighetshantering

Det finns generella beskrivningar av behörighetshantering i de styrande dokumenten (dock har vi tidigare fastställt att de inte är styrande för kommunens praktiska tillämpning då de är föråldrade och i behov av uppdatering).

Enligt intervjupersoner ansvarar IT-enheten för tilldelning av behörigheter till centrala system och det finns regler för hur lösenord behöver upprättas och bytas regelbundet. Det finns inte i nuläget tvåfaktorautentisering[5] implementerat förutom i de verksamheter där SITHS-kort krävs men är en fråga som utreds. Det har inte kommit någon kravställning från kommunen till kommunalförbundets IT-enhet där verksamhetssystem kräver ytterligare inloggning för att höja säkerheten.

Behörighet till verksamhetssystem tilldelas av systemförvaltare efter beslut från ansvarig chef. Inom stöd och omsorg finns upprättade rutiner för hantering av behörigheter till verksamhetssystemet Treserva samt rutiner för loggkontroll i enlighet med gällande regelverk. Syfte med loggkontroller är enligt rutinen att granska tillgång till journaluppgifter och att gällande författning och regelverk följs. Ansvarig för loggkontroll och dokumentation finns hos närmaste chef till den som loggkontrollen avser. Loggar att granska tas ut av systemförvaltare för systemet. Vi har inom ramen för granskningen inte gjort några kontroller av efterlevnad av rutinerna kring åtkomst till information genom behörighetsstyrning och tillhörande loggkontroller.

3.2.5 Medvetenhet och förståelse

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

Enligt riktlinjerna för informationssäkerhet ansvarar systemägaren för att användarna får nödvändig utbildning i informationssäkerhet. Det framgår vidare att alla som hanterar information har ett ansvar att upprätthålla informationssäkerheten. Av riktlinjerna anges att de är bindande för alla delar av kommunens verksamheter och att de som använder kommunens informationstillgångar på ett sätt som strider mot riktlinjerna kan bli föremål för disciplinära åtgärder.

På säkerhet- och beredskapssamordnarens initiativ genomfördes 2019 MSB:s webbutbildning för informationssäkerhet. I intervju beskrivs att syftet var att lyfta informationssäkerhetsfrågorna inom organisationen för en ökad förståelse och medvetenhet. Målet var att etablera en organisation för informationssäkerhet och få på plats en samordnare som kunde jobba med de administrativa delarna som saknas centralt för att sedan stötta verksamheterna i tillämpningen. I intervjuer beskrivs att utbildningen genomfördes av ungefär hälften av kommunens medarbetare. Det sägs att medvetenheten ökade och att det kom respons på utbildningens innehåll från vissa

[5] Inloggning till system eller tjänst kräver verifiering med kompletterande enhet som exempelvis kodkort, sms, bank-ID eller annan lösning för att erhålla en högre säkerhetsnivå vid åtkomst.

centrala funktioner, exempelvis arkivarie och registrator. Dessvärre uppnåddes enligt intervjupersoner inte det avsedda syftet och målet med utbildningsinsatsen.

Systemförvaltare har fått möjlighet att gå fördjupad utbildning inom informationssäkerhet för socialtjänster. Efter detta har information delats vidare på arbetsplatsträffar och möten med verksamheter med upplysningar om informationssäkerhet och hur medarbetare ska förhålla sig till informationen som hanteras. Det har tagits fram användarinstruktioner för hantering av personuppgifter och systemförvaltare har fått i uppdrag att göra detsamma med enklare anvisningar inom informationssäkerhet.

3.2.6 Incidenthantering

I *Riktlinjer för informationssäkerhet* finns en övergripande beskrivning av incidenter. I den framgår att ”incidenter kan vara interna eller externa intrång och intrångsförsök, felaktig användning av IT-system och IT-resurser med mera. Det är viktigt att kunna återkoppla erfarenheter från incidenter av olika slag för att kunna spåra brister och svagheter”.

I *Informationssäkerhetsinstruktion- användare* framgår att anställda vid misstanke om intrång ska vidta ett antal åtgärder och omedelbart anmäla incidenten till central IT-support. Vid eventuella fel och brister i verksamhetssystem uppges vidare i instruktionen att detta rapporteras till respektive systemförvaltare.

I intervjuer beskrivs att det är känt i verksamheten att IT-relaterade problem ska anmälas till IT så snart som möjligt. Om det finns misstanke om hot går då IT-enheten ut med en varning till övriga användare om misstänkta avsändare av e-post eller annat hot. Trots att rutinen anges vara känd finns behov av utbildning och information för att medvetandegöra om vad som är incidenter och hur användare kan upptäcka dessa så att de rapporteras i högre grad.

När ett ärende anmäls finns en intern rutin för incidentprocess inom IT som är kopplad till ärendehanteringssystemet. Det första som sker är en klassning för hur akut eller allvarligt hotet är där allvarsgraden styr om ärendet ska hanteras av första, andra eller tredje linjens support. En utsedd incident manager håller i hela processen. Information sker till berörd kommun parallellt med att IT-enheten arbetar vidare med lösning. En rapport skrivs efter hanteringen.

Bedömning över om incidenten är så allvarlig att den ska rapporteras till tillsynsmyndighet görs av systemägaren om incidenten är kopplad till verksamhetssystemen och av IT-enheten om störningen avser central IT.

3.2.7 Kontinuitetshantering för informationstillgångar

En kontinuitetsplan ska innehålla dokumenterade rutiner som vägleder organisationen vid händelse av störning eller avbrott. Syftet är att kunna upprätthålla verksamheten på en tolerabel nivå och att kunna återställa resursen så fort som möjligt. Planerna bör testas regelbundet för att säkerställa att de kan tillämpas vid behov.

I intervjuer beskrivs att det inte finns några gemensamma anvisningar eller krav på att kontinuitetsplaner ska tas fram för informationstillgångar. Det framkommer dock att det inom exempelvis stöd och omsorg till viss del finns beskrivningar av tillvägagångssätt om det inte finns tillgång till informationen i verksamhetssystemet. Det finns även en utsedd kontaktperson på IT-enheten som kan kontaktas som snabbt kan påbörja felsökning för att systemet ska kunna återställas skyndsamt.

3.2.8 Bedömning

Vår bedömning är att kommunstyrelsen och dess utskott inte har ett tillsett att det finns ett systematiskt arbete med riskanalyser och informationsklassning för att säkerställa informationens konfidentialitet, riktighet och tillgänglighet.

Kommunen har inte beslutat om modell för informationsklassning så att ett gemensamt ramverk finns över hur informationstillgångarna ska riskbedömas. Det har inte gjorts någon informationsklassning av den information som hanteras i informationssystemen eller andra riskanalyser för att bedöma informationens skyddsvärde och behov av säkerhetsåtgärder.

I nuläget saknas etablerade arbetssätt för att uppnå god informationssäkerhet. Hot och risker är därför inte identifierade och leder till att verksamheterna inte kan bedöma vilka behov av säkerhetslösningar de har så att dessa står i relation till hur skyddsvärd informationen är. De säkerhetsåtgärder som finns idag utgår i stort från den kunskap och erfarenhet som IT-enhetens medarbetare besitter kring de tekniska lösningar som finns tillgängliga samt implementerade skyddsnivåer för IT-infrastrukturen. Att inte bedöma skyddsvärdet kan innebära att informationen har alltför lågt skydd med risk för sårbarheter eller alltför högt skydd vilket kan vara kostnadsdrivande i förhållande till vad som avses att skyddas.

Det finns en rutin för incidenthantering beskriven i *Informationssäkerhetsinstruktion – Användare.* Då de styrande dokumenten inte är aktuella och något som kommuniceras i verksamheten är vår bedömning att det finns en påtaglig risk att incidenter sker utan att de upptäcks i tid och anmäls. Den dokumenterade rutinen följer dock den rutin som används när användare har IT-relaterade problem vilket innebär att det troligen är så att allvarligare incidenter anmäls utifrån att de påverkar användningen av IT. I nuläget sker ingen övergripande sammanställning av de incidenter som sker vilket är en brist för att kunna analysera inträffade incidenter och inkludera dessa i ett systematiskt förbättringsarbete för att förhindra att incidenter sker igen.

Det har erbjudits utbildningsinsatser till medarbetare för att kunskap och medvetenhet ska finnas för medarbetarnas ansvar för informationssäkerhet. Vi ser det som positivt att utbildning genomförts men anser att det är en brist att inte initiativet och de resurser

som lades på detta följdes av ytterligare aktiviteter för att påbörja ett mer systematiskt arbete med informationssäkerhet.

Det behöver säkerställas att en tillräcklig kunskap finns över vad som är informationssäkerhetsincidenter så att dessa upptäcks och rapporteras. Den mänskliga faktorn i verksamheter är en väsentlig säkerhetsrisk om inte en tillräcklig kunskap och medvetenhet finns då oaktsamhet hos enskilda kan utsätta både IT-miljön och kommunens informationstillgångar för sårbarheter där allvarliga konsekvenser kan uppstå både ekonomiskt och avseende förtroendet för organisationen.

3.3 Uppföljning och rapportering

Enligt MSB:s metodstöd för ett systematiskt informationssäkerhetsarbete som vi beskrivit inledningsvis i rapporten så är ledningens förståelse för och engagemang i informationssäkerhet grundläggande för att lyckas. Med andra ord måste ledningen få kunskap om hur de kan leda och styra verksamheten på ett effektivt sätt för att åstadkomma god informationssäkerhet. Ledningens stöd är också oumbärlig för att frågan ska få acceptans och ett engagemang från andra roller i organisationen.

I ett ledningssystem för informationssäkerhet är en årlig rapportering till ledningen en avgörande punkt för att följa upp det arbete som skett inom informationssäkerhet samt få beslut om prioriteringar och åtgärder för att förbättra arbetet under kommande år.

3.3.1 Uppföljning

I *Kommunövergripande riktlinje för säkerhetsarbete* framgår att kontroll och uppföljning ska ske genom checklistor för egenkontroller, rapportering genom skaderapporteringssystemet samt att säkerhets- och beredskapssamordnaren ska bistå med råd och kunskap för kontroll och uppföljning av kommunens säkerhetsarbete.

I *Riktlinjer för informationssäkerhetsarbetet* framgår att uppföljning är en viktig del i informationssäkerhetsarbetet för att bevaka att beslutade åtgärder genomförs, regler följs och att riktlinjer och instruktioner vid behov revideras.

I intervjuer beskrivs att det inte i nuläget sker någon uppföljning av informationssäkerhetsarbetet. Den uppföljning som görs anges främst ske på ärendenivå och i form av en löpande dialog med närmaste chef där avstämningar över aktiviteter inom exempelvis systemförvaltning och informationshanteringsfrågor sker.

Det framkommer att det en trolig anledning till detta främst beror på att det saknas en styrning centralt och att någon uppföljning eller information inte efterfrågas.

3.3.2 Rapportering

I *Kommunövergripande riktlinje för säkerhetsarbete* framgår inte några etablerade rapporteringsvägar för uppföljningen. Det är inte heller beskrivit i de övergripande styrdokumenten för informationssäkerhet hur uppföljning ska rapporteras.

I intervjuer framkommer att det i nuläget inte finns någon formaliserad rapportering till varken ledningsgrupp i tjänstepersonsorganisationen eller till kommunstyrelsen och dess utskott avseende informationssäkerhetsarbetet.

3.3.3 Bedömning

Vår bedömning är att det inte sker en systematisk uppföljning då former för detta saknas. Det finns varken mål- eller handlingsplan på övergripande nivå för informationssäkerhetsarbetet eller dokumentation för enskilda informationssystem som kan följas upp.

Utan att kommunen har genomfört det första steget i MSB:s rekommendation vilket innebär att analysera och identifiera behov inom informationssäkerhet, finns inte tillräckliga underlag för att bedöma vilka behov av förbättringsåtgärder som finns för informationssäkerheten och sedan löpande följa upp dessa. Syftet med det första steget är att analysera för att säkerställa att informationssäkerheten utformas utifrån verksamhetens rådande förutsättningar och leda fram till att väsentliga informationstillgångar identifieras, risker de ska skyddas mot samt ge förutsättningar att välja rätt säkerhetsåtgärder.

I enlighet med MSB:s rekommendationer anser vi det av stor vikt att beslut fattas om handlingsplan och mål för informationssäkerhetsarbetet och att detta tillställs tillräckliga resurser så att en organisation kan inrättas med uppdrag att leda och samordna det kommunövergripande arbetet.

Det behöver samtidigt säkerställas att uppföljning av arbetet rapporteras årligen till kommunstyrelsen med en sammanställning av genomförda aktiviteter, identifierade sårbarheter att åtgärda samt förslag till handlingsplan för det fortsatta arbetet för att utveckla kommunens informationssäkerhet. Det är av stor vikt att detta etableras i kommunstyrelsen så att en tillräcklig information och förståelse finns för att vid behov kunna prioritera resurser och insatser utifrån det övergripande ansvaret för informationssäkerheten.

4 Slutsats och rekommendationer

4.1 Slutsats

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen och dess utskott inte har säkerställt ett ändamålsenligt och systematiskt arbete med kommunens informationssäkerhet.

De rekommendationer som MSB har tagit fram till organisationer för att det ska finnas ett systematiskt arbete i enlighet med ett ledningssystem för informationssäkerhet finns inte etablerade eller planerade i kommunen. Det saknas aktuella styrdokument som tydliggör ansvar och hur arbetet ska bedrivas och i nuläget finns inte en organisation med tillräckliga resurser för att påbörja och leda arbetet.

Förutom ovan brister i styrning och ledning vill vi även framhålla avsaknaden av mål och handlingsplan för arbetet, modell för informationsklassning samt klassning av information i verksamhetskritiska system och tillhörande riskbedömning. Utan dessa aktiviteter sker inte val av säkerhetsåtgärder från en bedömning över risker och hur skyddsvärd informationen som hanteras är.

Med nuvarande status på informationssäkerhetsarbetet bedömer vi att det finns en påtaglig risk att kommunens informationstillgångar inte på ett tillräckligt sätt skyddas och att krav på dess konfidentialitet, riktighet och tillgänglighet tillgodoses. Med den stora mängd information som hanteras i en kommun leder bristerna till att kommunen kan råka ut för både ekonomisk skada samt förtroendeskada som en konsekvens.

4.2 Rekommendationer

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen och utskotten att:

- Etablera en organisation för informationssäkerhetsarbete med central samordnare och utsedda representanter i verksamheten samt tilldela dessa funktioner resurser i form av tid och kompetens så att förutsättningar för ett systematiskt arbete säkerställs.
- Revidera och upprätta styrande dokument så att dessa är aktuella och kan utgöra en sammanhållen helhet för styrningen av kommunens informationssäkerhetsarbete.
- Upprätta en årlig handlingsplan med prioriterade åtgärder och aktiviteter för att utveckla informationssäkerhetsarbetet.
- Besluta om en modell för informationssäkerhetsklassning och riskbedömning för kommunens informationstillgångar och sedan genomföra informationsklassningar i prioriteringsordning utifrån en bedömning av de system som är mest verksamhetskritiska.

- Säkerställa att nya och befintliga medarbetare får del av utbildning och information om informationssäkerhet så att en tillräcklig medvetenhet och kunskap finns över enskildas hantering och för att upptäcka incidenter.
- Besluta om kommunövergripande rutin för hantering av informationssäkerhetsincidenter och säkerställa att inträffade incidenter dokumenteras på övergripande nivå samt analyseras och följs upp som en del i det systematiska förbättringsarbetet.
- Säkerställa att uppföljning av beslutad handlingsplan och kommunens informationssäkerhetsarbete sker genom att etablera en årlig rapportering i form av ledningens genomgång till kommunstyrelsen.

2021-05-24

KPMG AB

Jenny Thörn	Lars Jönsson
Kommunal revisor	Certifierad kommunal revisor

Bilaga 1 Dokumentgranskning

Titel	Datum för fastställande	Beslutad av/Ansvarig
Policy för säkerhet och krisberedskap	2016-09-15	Kommunfullmäktige
Kommunövergripande riktlinje för säkerhetsarbetet	2018-08-17	Kommunstyrelsen
Riktlinje för informationssäkerhet	2013-09-30	Kommunfullmäktige
Informationssäkerhetsinstruktion - Användare	2013-03-25	Framgår ej
Informationssäkerhetsinstruktion - Förvaltning	2013-08-12	Framgår ej
Rutin E-post (kvittens användare)	2017-04-18	Funktionschef
Mobila enheter – säkerhet och personligt ansvar	2016-11-28	Lotta Söderholm (Kommunikation och service)
Policy för användande av internet för användare	1998-05-13	AU
Policy för hantering av personuppgifter	2020-06-16	Kommunfullmäktige
Riktlinjer för IT-användning	2004-08-31	Kommunfullmäktige
Rutin för mobila enheter (Stöd och omsorg)	2018-06-28	Verksamhetschef stöd och omsorg
Rutin krypterad innehåll personuppgift (Stöd och omsorg)	2021-01-29	Verksamhetschef stöd och omsorg
Rutin för loggkontroll (Stöd och omsorg)	2018-06-28	Verksamhetschef stöd och omsorg
Rutin loggkontroll användarkonto (Stöd och omsorg)	2020-01-14	Verksamhetschef stöd och omsorg

Riktlinje hantering av hemliga handlingar (utkast)	2021	Arbetsmaterial Säkerhet och beredskap
Instruktion samt kvittering hemliga handlingar (utkast)	2021	Arbetsmaterial Säkerhet och beredskap
Riskanalys samhällsviktig verksamhet	2021	Arbetsmaterial Säkerhet och beredskap