Kramfors kommun

Revisionen

Datum
2021-11-15

Till:
Kommunstyrelsen
Bildningsnämnden
Produktionsnämnden
Välfärdsnämnden

För kännedom:
Kommunfullmäktiges presidium

Revisionsrapport ”Informationssäkerhet”

KPMG har på uppdrag av kommunens revisorer granskat rutinerna för informationssäkerhetsarbetet. Uppdraget ingår i revisionsplanen för år 2021.

Revisionen önskar att kommunstyrelsen och ovanstående nämnder lämnar synpunkter på de slutsatser som finns redovisade i rapporten senast den 28 mars 2022. Av svaret bör det framgå vilka eventuella åtgärder som ska vidtas och när de beräknas vara genomförda.

Med vänliga hälsningar

Bertil Wiklund
Ordförande

Postadress
Kramfors kommun
Revisionen
872 80 Kramfors

E-post
kramfors.kommun@kramfors.se

Hemsida
www.kramfors.se

Besöksadress
Torggatan 2

Telefon
0612-800 00

Fax
0612-157 57

Organisationsnr
212000-2429

Granskning informationssäkerhet

Rapport

Kramfors kommun

KPMG AB

2021-11-15

Antal sidor 24

Kramfors kommun
Granskning informationssäkerhet

2021-11-15

Innehållsförteckning

Kramfors kommun
Granskning informationssäkerhet

2021-11-15

1 Sammanfattning

KPMG har av de förtroendevalda revisorerna i Kramfors kommun fått i uppdrag att genomföra en granskning av kommunstyrelsens och samtliga nämnders rutiner för informationssäkerhetsarbetet. Uppdraget ingår i revisionsplanen för 2021.

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

Vår bedömning baseras bland annat på följande iakttagelser:

- Vi saknar engagemang och prioritering av frågorna från kommunstyrelsens sida trots att de har det övergripande ansvaret för kommunens säkerhetsarbete. Resurser tillsätts inte och det finns i nuläget ingen efterfrågan på vad verksamheten bör leverera i sitt informationssäkerhetsarbete. De åtgärder och planer som kommunstyrelsen gav uttryck för i yttrande 2018 i samband med tidigare granskning har inte genomförts och den förväntade effekten har därmed inte uppfyllts.
- I nuläget saknas en fastställd informationssäkerhetspolicy, det finns dock riktlinjer för informationssäkerhet. Styrande dokument tydliggör ansvar och krav för informationssäkerhetsarbetet, de är däremot inte implementerade och tillräckligt kända vilket innebär att det ansvar som finns beskrivet inte efterlevs.
- Det saknas en ändamålsenlig organisation. Informationssäkerhetssamordnare finns utsedd men vår bedömning är att den tid som kan avsättas för uppdraget inte möjliggör att ansvaret kan upprätthållas. Det behöver därtill säkerställas att informationsägarna är medvetna om sitt ansvar och vidtar de åtgärder som det finns behov av för att skydda informationen.
- Det saknas ett systematiskt arbete med riskanalyser och informationsklassning för att säkerställa informationens konfidentialitet, riktighet och tillgänglighet. Modell för informationsklassning har inte fastställts och arbetet med informationsklassning är i en uppstartsfas och endast gjorts för en liten del av den information som hanteras i kommunens informationssystem.
- Det finns fastställt i styrande dokument hur incidenter ska hanteras. Det är dock inte tydliggjort i verksamheten hur processen och eskaleringsvägar ser ut när incidenter inträffar. Då det inte erbjudits utbildning och information inom informationssäkerhet på ett strukturerat sätt för att etablera en grundläggande kunskap och en medvetenhet om frågorna anser vi att det kan finnas risk att incidenter inte upptäcks och rapporteras i tillräckligt hög grad.
- Förbättringsåtgärder har identifierats och anmälts som ärende till kommunstyrelsen i april 2021 med förslag till beslut. Detta har inte behandlats i kommunstyrelsen. Den årliga rapporteringen i form av ledningens genomgång har inte genomförts sedan 2019.

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

- Göra en översyn av styrande dokument så att dessa utgör en sammanhållen helhet för styrningen av kommunens informationssäkerhetsarbete.
- Säkerställa att informationsägarna är medvetna om sitt ansvar och vidtar de åtgärder och aktiviteter som krävs för ett systematiskt informationssäkerhetsarbete för den information de ansvarar för.
- Upprätta en årlig handlingsplan med prioriterade åtgärder och aktiviteter för att utveckla informationssäkerhetsarbetet.
- Genomföra informationsklassningar i prioriteringsordning utifrån en bedömning av de system som är mest verksamhetskritiska.
- Säkerställa att rutiner och regler finns för behörighetshantering på kommunövergripande nivå. Rutiner bör om möjligt utvecklas genom en mer automatiserad process som kvalitetssäkrar hantering, uppföljning samt kontroll av tilldelade behörigheter.
- 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 Kramfors kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunstyrelsens och samtliga nämnders rutiner för informationssäkerhetsarbetet. Uppdraget ingår i revisionsplanen för år 2021.

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

Informationssäkerhet innebär att skydda information utifrån krav på dess konfidentialitet, riktighet och tillgänglighet och måste skyddas mot obehörig åtkomst, såväl externt som internt. Kommunernas arbete med informationssäkerhet påverkas av de lagar och förordningar som finns. Dataskyddsförordningen (GDPR) och NIS-direktivet ställs i direkt relation till hur säkerhetsarbetet sker i kommunala förvaltningar som berörs av direktiven. Myndigheten för samhällsskydd och beredskap har utifrån ISO 27000-standarden ett antal föreskrifter och metodstöd för att etablera ett ledningssystem för informationssäkerhet i kommunerna och vidta nödvändiga säkerhetsåtgärder.

Hotbilden med risker för intrång förändras kontinuerligt och säkerhetsarbetet behöver därför vara en ständigt pågående process för att säkerställa att kommunens informationstillgångar har ett tillräckligt skydd. För att kunna hantera det på ett ändamålsenligt sätt krävs att kommunen har ett systematiskt 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 kommunstyrelsen har säkerställt att det finns ett ändamålsenligt arbete med informationssäkerhet och en tillräcklig intern kontroll. Syftet är därtill att följa upp de åtgärder som biståndsnämnden vidtagit avseende behörighetshantering och loggkontroll utifrån rekommendationer i tidigare genomförd granskning 2017 där ett flertal förbättringsområden identifierades.

Granskningen ska besvara följande revisionsfrågor:

- Finns aktuella styrande dokument som tydliggör vilka krav som ställs och hur arbetet ska bedrivas?
- Finns en ändamålsenlig organisation för att arbeta med informationssäkerhetsfrågorna?
- Finns ett systematiskt arbete med att identifiera och analysera behov och risker för att säkerställa informationssäkerheten?
- Finns riktlinjer och rutiner för åtkomsthantering genom behörigheter och loggkontroll? Sker en tillräcklig kontroll av efterlevnad för hanteringen?
- Görs systematiska uppföljningar av genomförda åtgärder för att kontinuerligt förbättra informationssäkerheten, exempelvis genom intern kontroll?
- Finns rutiner för incidenthantering och rapportering?
- Finns dokumenterade kontinuitetsplaner för verksamhetskritiska informationssystem?
- Finns etablerade rapporteringsvägar för att kontinuerligt besluta om åtgärder för att utveckla arbetet?

Granskningen omfattar kommunstyrelsen och samtliga nämnder. Granskningen avser år 2021.

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller:

- Kommunallagen 6 kap. 6 §
- Tillämpbara interna regelverk, policys och beslut
- MSB[1]:s rekommendationer avseende Ledningssystem för informationssäkerhet
- NIS-direktivet i tillämpliga delar avseende kartläggning och analys av risker

[1] Myndigheten för samhällsskydd och beredskap

2.3 Metod

Granskningen har genomförts genom dokumentstudier där följande dokumentation har ingått:

- Riktlinje för informationssäkerhet
- Tjänsteföreskrift informationssäkerhet
- Tjänsteföreskrift systemförvaltning
- Tjänsteföreskrift för behandling av personuppgifter
- Checklista informationssäkerhet
- Utvecklingsplan för digitalisering
- Rutin för behörighetshantering i verksamhetssystem
- Behovs- och riskanalys behörighetshantering
- Riktlinjer för kontinuitetshantering

Intervjuer har genomförts med följande funktioner:

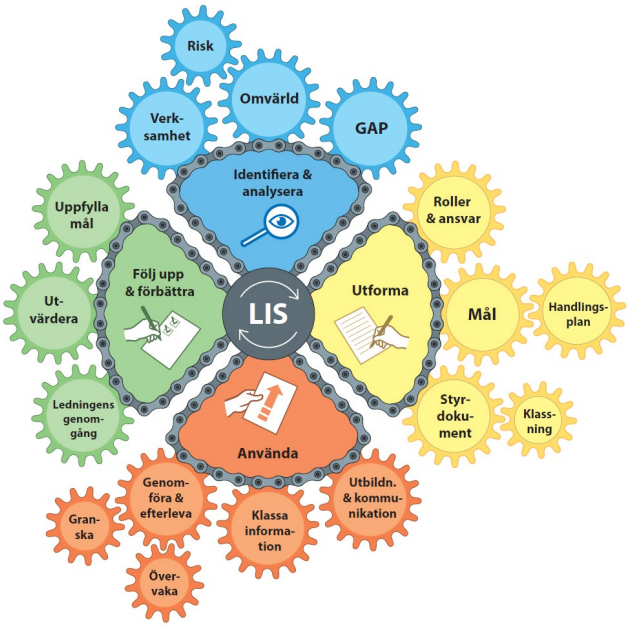
- Informationssäkerhetssamordnare
- IT-chef (avslutat anställning under granskningstiden)
- Dataskyddsombud
- Administrativ chef, Välfärdsförvaltningen

Granskningen har utförts av Jenny Thörn, verksamhetsrevisor och specialist. Lena Medin, certifierad kommunal revisor deltar i granskningen som kvalitetssäkrare utifrån sin roll som kundansvarig.

3 Metodstöd för systematiskt informationssäkerhetsarbete

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.



3.1.1 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.

3.1.2 Utforma

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

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

3.1.3 Använda

När verksamheten har utformat styrningen enligt avsnitt 3.1.2 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.

3.1.4 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.

3.1.5 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.

4 Resultat av granskningen

4.1 Organisation

4.1.1 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 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.

För styrning av kommunens informationssäkerhetsarbete har vi tagit del av följande dokument: riktlinje för informationssäkerhet, tjänsteföreskrift för informationssäkerhet samt checklista informationssäkerhet för användare. Det har tidigare funnits en plan för informationssäkerhet vilken upphävdes i samband med att riktlinjer för informationssäkerhet fastställdes 2018. Därtill finns ytterligare styrande dokument för systemförvaltning och personuppgiftshantering. Vi redogör kort för dokumenten på nästa sida.

Intervjupersoner beskriver att kommunen har ett stort antal styrande dokument som upplevs svårtillgängliga och alltför omfattande. Detta gäller även för informationssäkerhetsarbetet vilket uppges påverka graden av efterlevnad negativt. Av de dokument som är beslutade anges att de flesta är en pappersprodukt som endast delvis är kända, främst på chefsnivå. Det enda dokument som används i praktiken uppges vara checklistan för användare.

Vi har i granskningen inte tagit del av någon beslutad handlingsplan eller liknande dokument där kommunstyrelsen prioriterat samt tids- och resurssatt åtgärder som det finns behov av för att upprätthålla informationssäkerheten i kommunen.

Riktlinjer för informationssäkerhet

Det finns en *Riktlinje för informationssäkerhet* som fastställdes 2018-04-23 av kommunfullmäktige. Riktlinjen redovisar ledningens viljeriktning och stöd för informationssäkerhetsarbetet. Dokumentet syftar till att klarlägga mål, organisation, ansvar och roller för arbetet. Även avsnitt om uppföljning framgår av dokumentet.

Tjänsteföreskrift för informationssäkerhet

I inledningen av tjänsteföreskriften beskrivs att kommunfullmäktige har antagit Informationssäkerhetsplan där det fastslagits ledningens syn på informationssäkerhet, grundläggande mål samt övergripande roller och ansvar.

Tjänsteföreskriften informationssäkerhet ska enligt beskrivningen vara ett förtydligande av roller, ansvar och regelverk beträffande informationssäkerhet i kommunen och tydliggöra vad som behöver göras för att efterleva informationssäkerhetsriktlinjen.

Checklista informationssäkerhet för användare

Kommunledningsförvaltningen har tagit fram en C*hecklista informationssäkerhet för användare* som är daterad 2018-08-30. Den tydliggör de anställdas ansvar i förhållande till informationshantering i system. Bland annat innehåller checklistan instruktioner för lösenord, e-post, internet samt molntjänster.

Tjänsteföreskrift systemförvaltning

En *Tjänsteföreskrift för systemförvaltning*[2] har beslutats i samband med införandet av en kommungemensam modell för systemförvaltning. Av föreskriften framgår att IT-systemen är en viktig del för att bedriva en rationell och effektiv verksamhet. För att lättare kunna mäta nytta, effektivitet och kostnader samt för att underlätta bra samordning mellan olika system ska en kommungemensam modell för systemförvaltning användas. För samtliga IT-system ska det finnas en utsedd systemägare och en systemförvaltare.

Tjänsteföreskrift för behandling av personuppgifter, behörigheter och behandlingshistorik

I *Tjänsteföreskrift för behandling av personuppgifter, behörigheter och behandlingshistorik*[3] framgår att syftet är att tydliggöra informationshantering och systemförvaltning när personuppgifter behandlas. Den relaterar därigenom med övriga tjänsteföreskrifter som styr informationssäkerhetsarbetet. Tjänsteföreskriften ska konkretisera arbetet i kommunen så att anställda, elever och medborgare ska känna sig trygga när de anförtror kommunen sina personuppgifter och säkerställa att lagar följs för att skydda den personliga integriteten, regler för sekretess samt interna regler för den praktiska hanteringen av personuppgifter, behörigheter och behandlingshistorik.

[2] Beslutad av kommunchef 2018-02-26
[3] Beslutad av kommunchef 2018-08-31

4.1.2 Roller och ansvar

I *Riktlinjer för informationssäkerhet* finns en beskrivning av organisation och ansvar för kommunens informationssäkerhetsarbete. Kommunstyrelsen har det yttersta ansvaret för informationssäkerhetsarbetet. Informationssäkerhetssamordnaren har det övergripande och strategiska ansvaret att leda, utveckla och samordna arbetet.

Informationsägaren har det övergripande och yttersta ansvaret för sin information och avgör vilken information som får hanteras, hur den hanteras och av vem. Ansvaret följer linjeansvaret vilket betyder att cheferna ansvarar för att det finns rutiner som säkerställer en god efterlevnad av kommunens regelverk för informationssäkerhet.

Riktlinjen anger därtill att rollen systemägare har ett övergripande ansvar för respektive system och dess användning. Systemen ska uppfylla informationssäkerhetskraven i förhållande till verksamhetens behov, legala krav och säkerhetskrav.

Användarnas ansvar regleras i riktlinjen genom skrivelsen ”Alla som hanterar informationstillgångar har ett ansvar för att informationssäkerheten upprätthålls”. Detta förtydligas ytterligare i *Checklista för informationssäkerhet för användare,* vilken vi beskrivit ovan.

I *Tjänsteföreskrift för informationssäkerhet* framgår för första gången ansvaret för nämnden där detta formuleras ”Varje nämnd ska se till att allmän säkerhet upprätthålls inom verksamhetsområdet. Informationssäkerhet är en säkerhet liksom andra”. Respektive nämnd utser systemägare och informationsägare för de system och register som är förvaltningsspecifika. För gemensamma system utser kommunstyrelsen system- och informationsägare. Av tjänsteföreskriften framgår ett förtydligande över att informationsägare som grundregel är:

- Fastställda dokument – Den som fastställt dokumentet
- Data i informationssystem – Systemägaren
- All annan information - Utfärdaren

Intervjupersoner beskriver att de roller och ansvar som är angivna i styrande dokument inte har verkställts fullt ut. I intervjuer framkommer att det finns en utsedd informationssäkerhetssamordnare. Uppdraget leds vid sidan om andra huvudsakliga arbetsuppgifter och uppskattningsvis finns ca fem procent av arbetstiden för att arbeta med informationssäkerhetsfrågorna.

Till viss del finns namngivna på olika funktionerna men några uppdrag eller tydliggörande över vad som förväntas har inte skett och inte heller några krav på rapportering och leveranser. Det är inte heller uppdaterat vilka personer som är involverade i arbetet där vissa har slutat och andra uttrycker att de är ett namn på papperet men inte deltar i något praktiskt arbete inom systemförvaltning eller informationssäkerhet. Det formella ansvaret för informationssäkerhet följer linjeansvaret vilket innebär att chefer i förvaltningarna är informationsägare, om inte detta är formellt delegerat till någon annan funktion.

Det uppges finnas ett motstånd att ta till sig det ansvar som åligger informationsägare och initiativ stoppas på grund av okunskap eller bristande engagemang. I nuläget finns inga utsedda representanter i förvaltningarna som på informationsägarens uppdrag kan utföra det praktiska arbetet som behöver göras för att värdera risker och vidta åtgärder för att skydda informationstillgångarna.

I kommunen finns en digitaliseringsenhet sedan början av 2020. Efter att ha varit igång med sitt arbete i närmare ett år gjorde enheten en analys av aktuell situation. I analysen presenterades en lista på förutsättningar som behöver uppfyllas för att kommunen ska kunna bedriva digitaliseringsstödd verksamhetsutveckling. I april 2021 anmäldes ett ärende[4] till kommunstyrelsens arbetsutskott för att beskriva nuläget och de identifierade behov som fanns för att utveckla digitaliseringsarbetet. I det hade även behov inom IT-infrastruktur, säkerhet, systemförvaltning och informationssäkerhet beskrivits då det är viktiga grundpelare för att kunna digitalisera.

I skrivelsen framgår bland annat ”Utan att både den politiska ledningen och förvaltningsledningen har insikt i digitalisering i kombination med informationssäkerhet, avsätts ej heller tillräckliga ekonomiska och personella resurser för att uppnå målsättningar till exempel i perspektivet ”Kramforsbon” där målsättningen är ”en god verksamhet med effektiva processer”. Underlaget påvisar därtill allvarliga sårbarheter avseende IT-drift och säkerhet där risk för intrång anges vara stor. Det framgår också att ”Därför behöver genomtänkt kraft läggas på att systematiskt komma till rätta med problemen”.

Intervjupersoner uppger att ärendet har varit uppe i kommunstyrelsens arbetsutskott och att beslut väntas om uppdrag för att prioritera åtgärder och stärka arbetet inom nämnda områden. Syftet med ärendet var att medvetandegöra de förtroendevalda om de brister som identifierats och ge förslag till en utvecklingsplan med tidsatta åtgärder för att påbörja förbättringsarbetet. Enligt underlaget så fanns en hel del aktiviteter som skulle genomföras under 2021.

Ärendet finns registrerat som nytt ärende på ärendelista i april[5]. Vid en protokollsgenomläsning återfinner vi inte ärendet varpå kontakt tas med registrator vid kommunen. Vid denna förfrågan om protokoll och beslut i frågan meddelades att inga handlingar finns registrerade i ärendet. Vid uppföljning med registrator 2021-09-03 meddelas att ärendet inte tagits upp för behandling i varken kommunstyrelsens arbetsutskott eller i kommunstyrelsen.

4.1.3 Bedömning

Vår bedömning är att det inte finns en ändamålsenlig organisation för kommunens informationssäkerhetsarbete. Det saknas i stora delar resurser och funktioner för att kunna bedriva ett systematiskt informationssäkerhetsarbete. Det behöver säkerställas att informationsägarna är medvetna om sitt ansvar och vidtar de åtgärder som det finns

[4] KS2021/183
[5] Nya ärenden, Kommunstyrelse. Avser perioden: 2021-04-05 till 2021-04-11. Publicerat på kommunens webbsida 2021-04-12.

behov av för att skydda informationen. Vi bedömer därtill att centralt utsedd funktion som informationssäkerhetssamordnare inte ges tillräckliga förutsättningar för att upprätthålla det ansvar som föreskrivs i styrande dokument.

Brister är identifierade och försök har gjorts att medvetandegöra kommunstyrelsen på dessa för att påbörja ett förbättringsarbete. Vi ser allvarligt på att ärendet som anmälts till kommunstyrelsen inte har prioriterats in på agendan på de fem månader sedan det anmäldes. Det underlag som presenterats i ärendet visar på allvarliga brister som skulle kunna utsätta kommunen för både ekonomisk skada och förtroendeskada.

Vår bedömning är att styrande dokument tydliggör ansvar och krav för informationssäkerhetsarbetet. Styrdokumenten är däremot inte implementerade och tillräckligt kända så att det ansvar som finns beskrivet i styrande dokument efterlevs.

Det saknas en beslutad informationssäkerhetspolicy vilket enligt MSB:s rekommendationer bör utgöra den övergripande styrningen för informationssäkerhetsarbetet. Det har tidigare funnits ett övergripande styrdokument i form av en plan vilken har upphävts. Även om den beslutade riktlinjen för informationssäkerhet innehåller delar som vanligen ingår i en policy anser vi att det bör upprättas en plan eller policy som visar den politiska viljeriktningen samt tydliggör syfte och mål med arbetet. Detta bör sedan konkretiseras i riktlinjer och tjänsteföreskrifter.

Det är positivt att det tydliggörs i styrande dokument en gränsdragning mellan den administrativa säkerheten och den tekniska IT-säkerheten vilken endast utgör en del av informationssäkerhetsarbetet. Vi upplever dock att arbetet även i praktiken behöver tydliggöras så att gränsdragningen är känd och accepterad. I nuläget är inte arbetet samordnat och sker därför inte på ett systematiskt sätt.

Ansvaret för medarbetare är tydliggjort genom en checklista. Vi anser att den på ett lättillgängligt och överskådligt sätt tydliggör medarbetarnas ansvar för informationssäkerhet.

4.2 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.

I de fall kommunen har identifierat verksamhet som samhällsviktig ställs ytterligare krav på ett riskbaserat och systematiskt informationssäkerhetsarbete och det så kallade NIS-direktivet gäller för dessa verksamheter. I intervjuer framkommer att kommunen inte har identifierat någon verksamhet som samhällsviktig som därigenom skulle lyda under NIS-direktivet. Däremot så har Inspektionen för Vård och omsorg, som är tillsynsmyndighet för samhällsviktig verksamhet inom hälso- och sjukvård, meddelat att de bedömer att kommunen har samhällsviktig verksamhet som ska anmälas, då över 50 medarbetare arbetar inom vårdrelaterade yrken. Anpassningar för de nya kraven hade vid tiden för granskningen inte hunnit påbörjas.

4.2.1 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.

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 men även åtgärder för att stärka den administrativa säkerheten kan identifieras. Det kan exempelvis vara att förbättra rutiner, besluta om behörighetsnivåer eller andra åtgärder som bedöms nödvändiga för att säkerställa säkerheten för informationstillgångarna.

I *Riktlinje för informationssäkerhet* anges att systemens informationsmängder ska klassificeras. Ansvar för att så sker ligger enligt riktlinjen hos systemägaren. Det framgår dock vad gäller ansvarsfördelning för informationsägare, att den har i uppgift att bedöma vilken information som hanteras, hur den får hanteras och av vem. Detta är ofta delar som ingår vid klassning och riskbedömning samt vid behörighetstilldelning.

I intervjuer framkommer att det inte finns någon beslutad modell för informationsklassning. Det är ett fåtal system som har klassats i kommunen och har främst skett för mer verksamhetskritiska system. Inom välfärdsförvaltningen och bildningsförvaltningen har piloter för klassning genomförts där SKR:s modell KLASSA använts. Intervjupersoner beskriver dock att den upplevs alltför omfattande. I andra klassningar har en förenklad variant genomförts med grund i en blankett som anger fyra perspektiv utifrån tillgänglighet, riktighet, konfidentialitet. Genom det kan ett skyddsvärde fastställas för informationstillgångar i det system som klassas. Även personuppgiftshantering uppges av intervjupersoner ingå i dessa bedömningar.

Erfarenheter i kommunen från klassningar visar på svårigheter att göra bedömning om information är känslig eller inte. Det finns en generell bild att allt ska vara offentligt och transparent. Dessa föreställningar tillsammans med bristande kunskap inom informationssäkerhet upplevs leda till att de bedömningar som är gjorda är svåra att

vidta åtgärder utifrån. Exempelvis ställer känslig information höga krav på tekniska och administrativa åtgärder vilka kan vara kostsamma att införa.

Informationsklassning ska resultera i en kravställning från förvaltningen till IT-avdelningen om bedömning av skyddsvärdet visar att det finns behov av att stärka skyddet för informationstillgångarna. Utan informationsklassning vidtas åtgärder ur ett tekniskt perspektiv och på initiativ från IT-avdelningen. I intervjuer beskrivs det som att detta får ske till viss del tvingande och inte är något som efterfrågas av verksamheten.

Det har vid tiden för intervjuerna inte genomförts några systematiska riskanalyser för informationssäkerhet enligt intervjupersoner. Därtill uppges att det inte finns en fungerande säkerhetsfunktion i kommunen som kan utforma arbetssätt och strukturer för hur verksamheterna behöver arbeta riskbaserat och med ett säkerhetstänk. Arbetet med informationssäkerhet beskrivs vara reaktivt när något händer och inte ske proaktivt för att förebygga och vidta åtgärder för eventuella sårbarheter. Det sker vissa insatser men inte på ett systematiskt vis.

Ett arbete hade påbörjats under ledning av IT-chefen tillsammans med externa konsulter i syfte att genomlysa status på hantering av identiteter och informationssäkerhet för att rätta upp brister och ta tillvara möjligheter som digitaliseringen innebär inom områdena infrastruktur, identitetshantering och informationssäkerhet. Resultatet var tänkt att ge en dokumenterad inventering av identitet och informationssäkerhet inom de mest kritiska verksamheterna och ge en grund för djupare analyser samt generera konkreta åtgärdsförslag som adresserar förbättringsområden. Arbetet hade vid tiden för intervjuer inte slutförts.

I intervju beskrivs att aktiviteter med riskbedömning och informationssäkerhetsklassning skulle kunna inkluderas i arbetet med systemförvaltning. För att tydliggöra uppdrag och ansvar för systemförvaltning beslutades det om en *Tjänsteföreskrift för systemförvaltning* under 2018. I den dokumenterades en ansvarsfördelning men det ser enligt uppgifter i intervjuer mycket olika ut hur ansvaret uppfattats och efterlevs av systemägare och systemförvaltare.

Arbetet utifrån *Tjänsteföreskrift för systemförvaltning* beskrivs i intervjuer ha fått litet genomslag i verksamheten. Arbetssätt och strukturer för att säkra och utveckla system och tjänster och se på den data som hanteras för att upprätthålla ansvar upplevs inte etablerat. Det finns utsedda systemförvaltare som varken har kunskap eller tid för att utföra ett systematiskt arbete så att funktionalitet och säkerhet kan säkerställas i de system som är implementerade.

4.2.2 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.

Det har enligt intervjupersoner genomförts så kallade Nano-utbildningar som är kortare, digitala utbildningssessioner som sänds ut via e-post. Dessa har omfattat både

informationssäkerhet och GDPR. Utskick av utbildningarna skedde till närmare 700 medarbetare och förtroendevalda inför att dataskyddsförordningen skulle träda ikraft 2018. Uppföljning av dessa utbildningsinsatser visar att utbildningen av många sågs som ett störande moment. Ca 75 % tog del av de inledande avsnitten men ju längre utbildningen pågick så minskade intresset och många hade mest ”klickat sig igenom” vilket visade sig genom att titta på genomförandetiden för respektive utbildningstillfälle.

Under 2020 genomfördes ytterligare utbildningstillfällen via nano-learning. Detta skedde i samband med den nationella informationssäkerhetsmånaden som infaller i oktober årligen. Kommuner och andra verksamheter uppmanas då att arrangera aktiviteter i syfte att aktualisera informationssäkerhetsfrågorna och ge information till verksamhetens medarbetare.

Inom välfärdsförvaltningen har en utbildning genomförts i form av en enkät som kan följas upp. Uppföljningen visar att ca 70 % tagit del av utbildningen när den genomfördes 2020. Uppföljande tillfällen är planerade till hösten 2021. Det finns i nuläget ingen rutin för hur nyanställda ska ta del av utbildningen.

4.2.3 Incidenthantering

I *Tjänsteföreskrift för informationssäkerhet* beskrivs att incidenter som upptäcks ska rapporteras till IT Helpdesk för felrapport och åtgärd. IT Helpdesk bedömer om det är en incident och skriver i sådana fall en incidentrapport. Det anges vidare att det inom förvaltningarna finns specifika rutiner för felanmälan i verksamhetssystem.

Personuppgiftsincidenter hanteras i särskild rutin som tydliggörs i *Tjänsteföreskrift för behandling av personuppgifter, behörigheter och behandlingshistorik*. Rapportering av incidenter rörande personuppgifter ska göras i Flexite av den som upptäcker incidenten. En sammanvägd bedömning av incidenten ska ligga till grund för om diarieföring ska göras.

I intervjuer beskrivs även att övrig incidenthantering som exempelvis säkerhetsincidenter och informationssäkerhetsincidenter ska anmälas via Flexite. Det är dock få incidenter som anmäls och mörkertalet uppges av intervjupersoner vara stort. Det finns enligt uppgift i intervjuer en allmän rädsla i kommunen att göra fel vilket leder till att incidenter inte ses som ett lärande för att identifiera förbättringsområden, så att inte incidenter sker igen, utan som en bestraffning.

Systemet för incidenthantering uppges vara trögarbetat och inte så användarvänligt. Incidenter anmäls om de upptäcks i högre grad via e-post än i systemet. Det har funnits en dialog om incidenthanteringen ska ske genom en e-tjänst men det har vid tiden för granskningen inte fattats beslut i frågan. Det framkommer dock från intervjupersoner att det inte är systemet eller rutinen som främst behöver utvecklas utan kunskapen och medvetenheten att upptäcka incidenter. Samt etablera ett synsätt att det är positivt att uppmärksamma incidenter för att kunna vidta åtgärder.

4.2.4 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 arbete med kontinuitet har skett på verksamhetsnivå men inte avseende informationstillgångar för att säkerställa reservrutiner och återgångsrutiner för tillgång information som finns i verksamhetssystem.

I intervjuer uppges att det har genomförts ett arbete under våren 2021 för att upprätta kontinuitetsplaner. De system inom välfärdsförvaltningen som har bedömts som samhällsviktiga har efter detta arbete avtalats om utökad support från IT-avdelningen. Det uppges dock inte har uppstått så många tillfällen när support utanför kontorstid har behövt nyttjats. Tidigare fick systemförvaltare för respektive system ha en form av jour för att lösa problem oavsett det var arbetstid, sjukdom eller semester så det var ändå angeläget att få till en lösning med stöd från IT-avdelningen.

4.2.5 Bedömning

Vår bedömning är att kommunstyrelsen och nämnderna inte har tillsett att det finns ett systematiskt arbete med riskanalyser och informationsklassning för att säkerställa informationens konfidentialitet, riktighet och tillgänglighet. Arbetet med informationsklassning är i en uppstartsfas och endast gjorts för en liten del av den information som hanteras i kommunens informationssystem.

I nuläget saknas därför etablerade arbetssätt för att uppnå god informationssäkerhet. Hot och risker är 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.

Vi noterar att det finns fastställt i styrande dokument hur incidenter ska hanteras men rutinen efterlevs inte och att det finns en stor risk för att incidenter inte rapporteras. Det är av stor vikt att eventuella incidenter upptäcks och dokumenteras på övergripande nivå så att dessa kan följas upp och vara en del i det systematiska förbättringsarbetet.

Det har inte erbjudits utbildning och information i tillräckligt hög grad inom informationssäkerhet för att etablera en grundläggande kunskap och en medvetenhet om frågorna vilket leder till en säkerhetsrisk då oaktsamhet hos enskilda kan utsätta både IT-miljön och kommunens informationstillgångar för sårbarheter. Konsekvensen vid intrång eller hot mot den information som kommunen ansvarar för kan leda till både ekonomisk skada och förtroendeskada.

4.3 Åtkomst- och behörighetshantering

4.3.1 Kommunövergripande rutiner för tilldelning och hantering

I *Tjänsteföreskrift för behandling av personuppgifter, behörigheter och behandlingshistorik* framgår att behörighetshanteringen ska säkerställa att endast de personer som behöver information för att kunna utföra sina arbetsuppgifter ska ges tillgång till informationen. Det är särskilt viktigt när skyddade uppgifter, känsliga personuppgifter, sekretessbelagd information och information om hemförhållanden hanteras. Behörighetshanteringen ska följa organisatorisk tillhörighet och befogenheter i tjänsten. Hantering av tilldelning och kontroll ska ske av ett fåtal utbildade och behöriga systemadministratörer.

Förutom behörighet för användarkonton och specifika verksamhetssystem så finns så kallade ”super users” som har högre behörigheter (särskild behörighet). Det kan vara personal på IT-avdelningen med tillgång till serverhallar och IT-infrastruktur eller systemförvaltare som har i uppdrag att administrera och utveckla system som används i kommunen. Dessa behörigheter tar sig förbi åtkomstspärrar och kan i sina funktioner både tilldela, ändra och radera uppgifter. Det medför en högre risk och särskilda behörigheter behöver därför begränsas, dokumenteras samt löpande följas upp så att de inte nyttjas på ett felaktigt sätt. Enligt styrdokument är det ansvarig systemförvaltare som beslutar om tilldelning av särskild behörighet. Tilldelning av särskilda behörigheter ska alltid ske individuellt.

Kommunens behörigheter utgår från ett Active Directory (AD) där användarkonton administreras. I intervjuer beskrivs tilldelningsprocessen som att konto skapas i personalsystemet efter att chef har beslutat om anställning i WINLAS. HR skickar beställning till IT av e-post-adress samt filåtkomst beroende på organisationstillhörighet. Övriga behörigheter som behövs i förvaltningarnas verksamhetssystem tilldelas genom respektive systemägare eller administratörer för systemen.

Allt arbete sker manuellt vilket anges vara bristfälligt då nuvarande hantering inte har något automatiserat stöd- och kontrollsystem för tilldelning eller hantering av identitet och åtkomst. I intervju framkommer att IT-avdelningen har jobbat med rutinerna i flera år, men kommer inte vidare på grund av resursbrist och avsaknad av styrande beslut.

Det saknas i nuläget en tydlighet i styrande dokument över hur kommunens åtkomsthantering ska fungera. Utveckling av identitetshantering var en av punkterna i det åtgärdsförslag som anmälts till kommunstyrelsen för beslut. Intervjupersoner anser att det finns allvarliga brister i nuvarande hantering med avsaknad av tillräckliga rutiner vilket leder till att det inte finns en säker process för hantering av behörigheter som kan leda till att obehörig åtkomst till information kan förekomma.

4.3.2 Uppföljning av tidigare genomförd granskning av behörighetshantering och loggkontroll

De förtroendevalda revisorerna gav 2017 KPMG i uppdrag att granska hanteringen av behörigheter och åtkomstkontroll i kommunens datoriserade verksamhetsstöd Treserva. Granskningen avsåg biståndsnämnden, arbetsmarknadsnämnden och socialnämnden samt kommunstyrelsen utifrån uppsiktsplikten.

I granskningen lämnade revisionen ett antal rekommendationer efter att förbättringsområden identifierats. Kommunstyrelsen har därefter svarat kommunrevisionen i ett yttrande[6]. Rekommendationer och yttrande ska enligt uppdrag från kommunrevisionen följas upp av KPMG under 2021, vilket görs i samband med den här granskningen av informationssäkerhet.

En uppföljning av tidigare genomförda granskningar är intressant för att få en uppfattning hur rapporten och rekommendationerna i rapporten tagits tillvara av den granskade nämnden. Resultatet av en sådan uppföljning kan i sin tur ligga till grund för kommande riskanalysarbete.

I intervjuer beskrivs av verksamhetsföreträdare att granskningen som genomfördes 2017 varit till stor nytta. De hade inte innan granskningen varit tillräckligt medvetna om det ansvar de hade för behörighetshantering och loggkontroll. Med grund i granskningsrapportens rekommendationer kunde ett omfattande förbättringsarbete påbörjas.

I kommunstyrelsens yttrande över granskningen 2017 framkommer att ett arbete hade påbörjats under ledning av IT-chefen tillsammans med externa konsulter i syfte att genomlysa status på hantering av identiteter och informationssäkerhet för att rätta upp brister och ta tillvara möjligheter som digitaliseringen innebär inom områdena infrastruktur, identitetshantering och informationssäkerhet. Resultatet var tänkt att ge en dokumenterad inventering av identitet och informationssäkerhet inom de mest kritiska verksamheterna och ge en grund för djupare analyser samt generera konkreta åtgärdsförslag som adresserar förbättringsområden. Enligt intervjupersoner har det inte fattats några beslut om åtgärder för att utveckla identitetshanteringen på kommunövergripande nivå. Det arbete som har genomförts som ett resultat av granskningen är enligt intervjupersoner gjorda specifikt inom välfärdsförvaltningen.

Förbättringsarbetet påbörjades genom en kartläggning hur systemen hänger ihop, från personalsystem, AD och verksamhetssystem. En rensning gjordes i systemen för att endast ha aktuell information om tilldelade behörigheter. Det gjordes en sammanställning av alla funktioner och befattningar som sedan ingick i en risk- och konsekvensanalys.

Vid intervjuer framkommer att den centrala tillämpningsföreskriften för behandling av personuppgifter, behörigheter och behandlingshistorik har fastställts sedan granskningen genomfördes, se avsnitt 4.3.1. Denna har därtill kompletterats av

[6] Kommunstyrelsen 2018-01-09.

förvaltningsspecifik rutin för behörigheter i välfärdsförvaltningens verksamhetssystem[7]. Syftet med rutinen är att säkerställa den enskildes integritet genom att begränsa behörigheter och minimera åtkomst av personuppgifter. Det har också tagits fram en blankett för risk- och konsekvensanalys inför tilldelning av behörigheter i Treserva[8]. Vi noterar att riskvärde över nio föranleder att åtgärder måste vidtas för att möta risker. Av de funktioner som finns dokumenterade i riskanalysen är det högsta riskvärdet åtta.

Behörighetstilldelningen inom välfärdsförvaltningen sker i ett system och tilldelningsblanketten diarieförs. Alla behörigheter måste beställas och signeras av ansvarig chef innan tilldelning sker. Innan tilldelning sker även en kontroll att personen finns i personalsystemet och i kommunens AD. Om inte dessa krav kan tillgodoses tilldelas ingen behörighet. För särskilda behörigheter krävs ett beslut och beställning av förvaltningschef och krav om att beslutet ska diarieföras.

Behörigheter rensas eller ändras löpande när chef meddelar och signerar blankett för ändring, exempelvis vid avslut eller förändring i arbetsuppgifter där åtkomst behöver justeras. Det görs även större kontroller med gallring och uppdatering i systemet två gånger per år som enhetschef ansvarar för. Ett sätt att säkerställa kontroll anges i intervjuer ha skett genom att använda tidsbegränsade behörigheter i större utsträckning. Detta för att inte medarbetare ska ha åtkomst till information längre än de har behov av. Det kan i sin tur leda till en ökad administration men anges både i den skriftliga rutinen och bekräftas i intervjuer inte vara en godtagbar anledning att lägga behörigheter på längre tid eller utan tidsgräns.

Det har genomförts utbildningsinsatser i personuppgiftshantering och informationssäkerhet under 2020 som planeras att följas upp med ytterligare tillfällen under hösten 2021. Enligt intervjupersoner så följer behov av utbildningsinsatser den riskbedömning som gjorts, där funktioner som hanterar information med högre riskvärde ska förses med mer kunskap som ett sätt att möta risker till en godtagbar nivå.

Även avvikelse- och incidenthanteringen uppges ha förbättrats genom en högre medvetenhet och tydliggjort ansvar kring behörigheter och åtkomstkontroll. Inledningsvis efter granskningen hade välfärdsnämnden med punkter i internkontrollplanen där kontroller gjordes av behörigheter och loggar. När kontrollerna inte längre visade på avvikelser så togs kontrollmomenten bort och är inte längre en del i nämndens internkontrollplan. Intervjupersoner menar att det finns en god intern kontroll genom de rutiner och arbetssätt som nu är implementerade så det är tillräckligt.

Sedan arbetssätt och rutiner förbättrats sker ett fåtal avvikelser per år. De senaste avvikelserna har handlat om att en medarbetare lånat ut sin inloggning till en kollega eller att en person tillfälligt varit vikarie i två verksamheter. I samband med arbetet skulle medarbetaren då dokumentera något som hänt dagen innan då denne var i tjänst för att utföra annat arbete. Då åtkomst till informationen inte hade med dagens arbetsuppgifter att göra så är det inte tillåtet och därför registrerades detta som en

[7] Fastställd av förvaltningschef 2018-05-16 samt reviderad 2019-11-28.
[8] Fastställd av administrativ chef Välfärdsförvaltningen, 2017-11-20, reviderad 2019 och 2020.

avvikelse. Händelsen fick en rimlig förklaring till att det skedde och inget ont uppsåt fanns. Sådana avvikelser hade inte identifierats innan det förbättringsarbete som genomförts och enligt intervjupersoner visar det på att det nu finns goda rutiner både för den löpande hanteringen, uppföljning och kontroll.

Som uppföljning sker regelbundna loggkontroller. Metod för loggkontroll finns dokumenterad i systemförvaltningsplan för Treserva. Kontrollen genomförs genom att listor med granskningsobjekt dras ut och diarieförs tillsammans med granskningsdokument och loggar. Dessa sekretessbeläggs i diariet då de innehåller personuppgifter och endast ska finnas tillgängliga för ett fåtal. Ärende går sedan till verksamhetschef hanterar ev. avvikelser. Ansvaret för analyser av genomförda kontroller görs av närmaste chef till granskningsobjekt och verksamhetschef.

4.3.3 Bedömning

Vår bedömning är att det bör genomföras ett förbättringsarbete för att säkerställa hanteringen med tilldelning, förändring och avslut av behörigheter på kommunövergripande nivå. I nuläget är processerna alltför personberoende och det är en riskfaktor med den manuella hanteringen då förändringar lätt kan bli fördröjda eller inte uppmärksammas i tillräckligt hög grad.

De kommunövergripande rutinerna påverkar i sin tur hur säker åtkomsten är i respektive förvaltnings verksamhetssystem då användarkonton som finns kvar medger tillgång till information även om personen har slutat sin anställning eller bytt organisatorisk tillhörighet. Vår bedömning är att kommunstyrelsen inte har genomfört de åtgärder som de uttalat i sitt yttrande avseende granskning av behörighetshantering och loggkontroll 2017 avseende förbättrad identitetsstyrning.

Det finns i nuläget ingen uppföljning eller intern kontroll avseende behörigheter och loggar på kommunövergripande nivå. Därtill indikerar de identifierade bristerna inom IT-drift och säkerhet på betydande risk för att obehöriga skulle kunna komma åt kommunens informationstillgångar där intrång skulle kunna medföra att information förloras eller skadas.

Vår bedömning är att välfärdsnämnden har beaktat de rekommendationer som gavs i granskning av behörighetshantering och loggkontroll 2017 och vidtagit ett flertal åtgärder för att möta de brister som granskningen visade. Vi har inga ytterligare rekommendationer avseende välfärdsnämndens arbete med behörighetshantering och loggkontroll.

4.4 Uppföljning

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.

Enligt *Riktlinjer för informationssäkerhet* ska kommunstyrelsen minst en gång per år informera sig om hur arbetet med informationssäkerhet pågår i kommunens förvaltningar. Genomgången görs vid den årliga aktiviteten ”ledningens genomgång”.

Uppföljningen ska baseras på underlag med rekommendationer som tas fram av informationssäkerhetssamordnaren. Resultatet från uppföljningen ska innefatta beslut om åtgärder för att förbättra informationssäkerheten samt tilldelning av resurser.

I intervjuer framkommer att det har genomförts en uppföljning i form av ledningens genomgång 2019 till kommunstyrelsen. 2020-02-17 genomfördes en föredragning för kommunstyrelsens ledningsgrupp. Då informerade informationssäkerhetssamordnaren om informationssäkerhet, krisberedskap, totalförsvar och säkerhetsfrågor. Ett förslag till förenklad modell informationsklassning gavs också vid detta tillfälle. Enligt uppgift så har inga åtgärder vidtagits utifrån informationen då pandemin medförde att andra frågor behövde prioriteras.

4.4.1 Bedömning

Vår bedömning är att det inte sker en systematisk uppföljning i enlighet med interna styrdokument. 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.

Det ärende som anmälts med förbättringsförslag för att rätta upp brister samt ta tillvara de möjligheter som digitaliseringen innebär inom infrastruktur, identitetshantering och informationssäkerhet har inte behandlats inom rimlig tid med hänsyn tagen till den information och riskbild som underlaget påvisar.

5 Slutsats och rekommendationer

5.1 Slutsats

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen 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 är inte etablerat i kommunen. Vi saknar engagemang och prioritering av informationssäkerhetsfrågorna där resurser tilldelas så att en organisation kan etableras för ett mer sammanhållet och strukturerat arbete. På övergripande nivå saknas en mål- och handlingsplan för arbetet som löpande kan följas upp på ett strukturerat sätt.

De styrande dokumenten tydliggör ansvarsfördelning men är inte tillräckligt förankrade så att ansvaret efterlevs. Det är väsentligt att kommunen genomför informationsklassning av sina verksamhetskritiska system så att val av säkerhetsåtgärder utgår från en bedömning över risker och hur skyddsvärd informationen som hanteras är. Regler för behörighetshantering bör upprättas som tydliggör åtkomst för användare och hur ansvarsfördelning för hanteringen ser ut. Kommunen bör i sitt prioriterade förbättringsarbete se över om det går att implementera en mer automatiserad process för tilldelning och kontroll av behörigheter.

Därtill bör utbildningsinsatser erbjudas för att en grundkunskap och medvetenhet finns i verksamheten om var och ens ansvar för hanteringen av information och IT för att minska risken att incidenter sker som kan skada informationstillgångarna. Kommunen behöver även säkerställa att incidenter upptäcks och rapporteras så att åtgärder kan vidtas så att inte incidenter sker igen. Rutiner för detta behöver beslutas i styrande dokument, tydliggöras för verksamheterna så att rutinen efterlevs och att anmälda incidenter samlas ihop och analyseras på kommunövergripande nivå så att förbättringar kan genomföras.

Slutligen anser vi att kommunstyrelsen skyndsamt ska prioritera det anmälda ärendet från april 2021 avseende förbättringsförslag och planera för aktiviteten ledningens genomgång 2021.

5.2 Rekommendationer

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

- Göra en översyn av styrande dokument så att dessa utgör en sammanhållen helhet för styrningen av kommunens informationssäkerhetsarbete.
- Säkerställa att informationsägarna är medvetna om sitt ansvar och vidtar de åtgärder och aktiviteter som krävs för ett systematiskt informationssäkerhetsarbete för den information de ansvarar för.
- Upprätta en årlig handlingsplan med prioriterade åtgärder och aktiviteter för att utveckla informationssäkerhetsarbetet.
- Genomföra informationsklassningar i prioriteringsordning utifrån en bedömning av de system som är mest verksamhetskritiska.
- Säkerställa att rutiner och regler finns för behörighetshantering på kommunövergripande nivå. Rutiner bör om möjligt utvecklas genom en mer automatiserad process som kvalitetssäkrar hantering, uppföljning samt kontroll av tilldelade behörigheter.
- 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.

Kramfors kommun
Granskning informationssäkerhet

2021-11-15

2021-11-15

KPMG AB

Jenny Thörn	Lena Medin
Kommunal revisor	Certifierad kommunal revisor