Vansbro kommun

Kommunrevisorerna *2022-12-12*

Skickas till:
Kommunstyrelsen
Kommunfullmäktige för kännedom

Granskning av kommunens informationssäkerhet

På uppdrag av Vansbro kommuns revisorer har KPMG granskat rutinerna kring kommunens informationssäkerhetsarbete. Uppdraget ingår i revisionsplanen för år 2022.

Kommunens revisorer önskar att kommunstyrelsen lämnar ett yttrande med redovisning av åtgärder baserat på de rekommendationer som lämnas i rapporten senast 2023-02-28. Yttrandet skickas till revisionens biträde, johan.malm@kpmg.se.

För de förtroendevalda revisorerna i Vansbro kommun,

Gösta Lindkvist

Ordförande Vansbro kommuns revisorer

Granskning av kommunens informationssäkerhet

Rapport

Vansbro kommun

KPMG AB

2022-12-05

Antal sidor 20

Vansbro kommun
Granskning av kommunens informationssäkerhet

2022-12-05

Innehållsförteckning

1 Sammanfattning

Vi har av Vansbro kommuns revisorer fått i uppdrag att granska rutinerna kring kommunens informationssäkerhetsarbete. Uppdraget ingår i revisionsplanen för år 2022.

Granskningen har syftat till att bedöma om kommunen har ett ändamålsenligt och systematiskt arbetssätt med sin informationssäkerhet. Vår sammanfattande bedömning utifrån granskningens syfte är att kommunen till stora delar saknar ett ändamålsenligt och systematisk arbetssätt med sin informationssäkerhet.

Kommunen har till viss del upprättat styrande och stödjande dokument, vi ser dock behov av att komplettera dessa, bland annat avseende den tekniska säkerheten samt att formalisera rutinbeskrivning för hantering av incidenter som inte är en personuppgiftsincident.

För att säkerställa att informationssäkerhetsarbetet bedrivs systematiskt och kontinuerligt gör vi bedömningen att kommunstyrelsen bör överväga vilka resurser som krävs för att utveckla arbetet, bland annat utse en informationssäkerhetssamordnare.

Vidare gör vi bedömningen att kommunen har behov av att utveckla riskbedömning och klassning av information samt verksamhetssystem. Vi ser även ett behov av anvisningar för att regelbundet ompröva genomförda riskanalyser och informationsklassningar för att möta nya risker och behov.

I syfte att stärka medvetenhet och kunskap i kommunen angående informationssäkerhet anser vi att kommunen bör genomföra utbildningsinsatser.

Vidare gör vi bedömningen att Vansbro kommun har behov av att upprätta ett systematiskt arbetssätt med IT-säkerhet för central IT-infrastruktur. IT-enheten har vidtagit åtgärder i syfte att säkerställa att kommunens system skyddas från såväl digitala som fysiska intrång, dock ser vi ett behov av att ytterligare åtgärder vidtas.

Det finns även behov av att tydliggöra hur andra incidenter än personuppgiftsincidenter ska anmälas samt följas upp. Med syftet att kunna vidta åtgärder och på så sätt minska risken för att incidenter sker igen bör incidenterna analyseras på en övergripande nivå.

Som en bidragande del i att informationssäkerhetsarbetet upprätthålls samt följs upp bör kommunstyrelsen beakta informationssäkerhet i internkontrollarbetet samt att återkommande återrapportering och uppföljning upprättas.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Säkerställa samt följa upp att implementering av nya informationssäkerhetspolicyn sker.
- Upprätta en handlingsplan/prioriteringsplan över åtgärder som behöver vidtas i syfte att stärka informationssäkerheten i kommunen.
- Upprätta ett styrande dokument som tydliggör IT-avdelningens uppdrag och ansvar samt de krav som ska finnas avseende teknisk säkerhet.
- Upprätta riktlinjer för behörighetshantering och införa kontroller för att tillse att riktlinjerna följs och att behörigheter är aktuella och korrekta.
- Se över nuvarande organisation och utreda behovet av att utse en informationssäkerhetssamordnare för att stärka arbetet.
- Upprätta former för genomförande av riskbedömning samt informationsklassning och säkerställa att dessa moment genomförs.
- Upprätta ett systematiskt arbetssätt med IT-säkerhet för central IT-infrastruktur. Arbetet bör ha sin utgångspunkt i upprättade och dokumenterade riskanalyser.
- Upprätta alternativt tydliggöra former för hantering av incidenter som inte är personuppgiftsincidenter.
- Säkerställa att anmälda incidenter analyseras i syfte att kunna vidta åtgärder för att minska risken att incidenten sker igen.
- Säkerställa att utbildning genomförs löpande för samtliga användare för att etablera medvetenhet och grundläggande kunskap om informationssäkerhet.
- Inkludera informationssäkerhet det riskanalysarbetet som ligger till grund för internkontrollplanen.
- Ställa krav om uppföljning och återrapportering om kommunens samlade informationssäkerhetsarbete så att beslut kan tas om mål och handlingsplan över erforderliga åtgärder för att förbättra informationssäkerheten.

2 Bakgrund

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

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. Myndigheten för samhällsskydd och beredskap har utifrån ISO 27000-standarden ett antal föreskrifter och metodstöd för att etablera ett ledningssystem för informationssäkerhet i kommunerna.

IT-säkerhetsåtgärder ska stå i relation till informationstillgångarnas värde och de risker och behov som ansvariga för informationen har fastställt. Hotbilden med risker för intrång förändras kontinuerligt och säkerhetsarbetet behöver därför vara en ständigt pågående process för att säkerställa att kommunens informationstillgångar har ett tillräckligt skydd. För att kunna hantera det på ett ändamålsenligt sätt krävs att kommunen har ett systematiskt informationssäkerhetsarbete där flera funktioner i kommunen är involverade och rätt organiserade för uppdraget.

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

2.1 Syfte, revisionsfrågor och avgränsning

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

Granskningen avser 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?
- Har tillräckliga utbildnings- och informationsinsatser genomförts för att medarbetare ska ha en grundläggande kunskap och medvetenhet om risker inom informationssäkerhet?
- Finns ett systematiskt arbete med riskanalyser och informationsklassning för att säkerställa informationssäkerheten?
- Har tillräckliga anpassningar och åtgärder för informationssäkerhet vidtagits utifrån gällande regelverk och krav i enlighet med GDPR och NIS-direktivet?
- 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?

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller:

— Kommunallagens 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

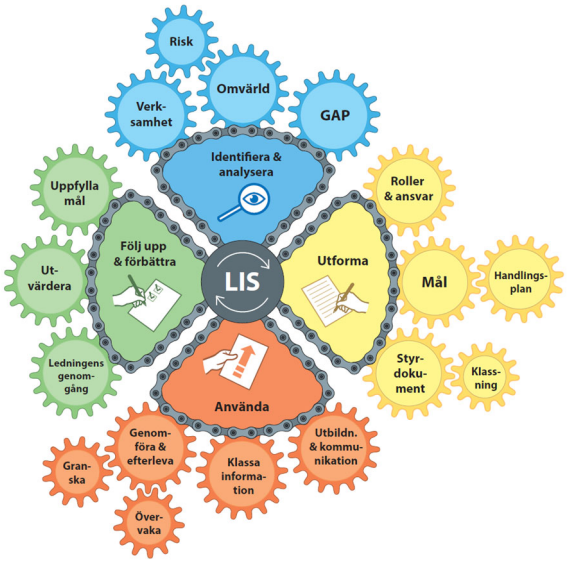
Granskningen har genomförts genom dokumentstudier och intervjuer med berörda tjänstepersoner och politiker.

Samtliga intervjupersoner har getts möjlighet att faktakontrollera rapporten.

2.4 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.



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.

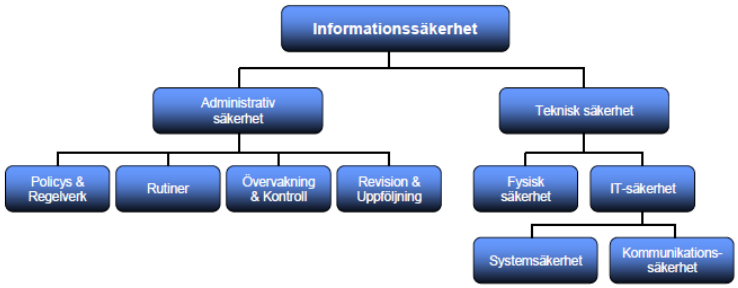
- Genomföra och efterleva de handlingsplaner och styrdokument som avser informationssäkerhetsarbetet
- Utbilda och kommunicera informationssäkerhetsfrågor till organisationens medarbetare. Det är ständigt pågående arbete som är nödvändigt för att skapa ett systematiskt informationssäkerhetsarbete.

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

Informationssäkerhetsbegreppet och dess innehåll kan översiktligt beskrivas i nedanstående skiss:



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

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

Den svenska och internationella standardserien SS-ISO/IEC 27000 visar på ett sådant ledningssystem där säkerhetsnivån tar sin utgångspunkt i en verksamhetsanpassad riskanalys, och där informationssäkerhetsarbetet följer en tydlig process. Tillämpning av standarderna enligt denna serie underlättar arbetet med informationssäkerhet inom organisationer och förbättrar också möjligheterna att externt bedöma säkerhet och revidera denna på ett enhetligt sätt.

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

Det bör finnas en person inom organisationen med ansvar för att samordna informationssäkerhetsarbetet. Grundprincipen är att ansvaret för informationssäkerhetsarbete ska följa det ordinarie verksamhetsansvaret från ledning ner till enskilda medarbetare. Informationssäkerhetssamordnaren har därmed inget formellt ansvar för informationssäkerheten utan ska verka som ett stöd för att den övriga organisationen innefattande ledning, verksamhetschefer och medarbetare tar sitt ansvar för informationssäkerhet i verksamheten.

Det är viktigt att tydligt klargöra informationssäkerhetssamordnarens roll och vilket mandat och rapporteringsplikt som ska ingå i rollen.

Var i organisationen informationssäkerhetssamordnaren eller motsvarande är placerad beror på organisationens struktur men bör generellt vara placerad nära 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 Styrande dokument

Kommunfullmäktige fattade i juni 2022 beslut om ny informationssäkerhetspolicy[1]. Av policyn framgår kommunfullmäktiges mål och viljeriktning, vilket är följande:

- Förhindra att skyddsvärd information hamnar i orätta händer,
- säkerställa att rätt information finns tillgänglig för rätt person vid rätt tillfälle,
- förhindra eller minska effekten av störningar och skador,
- upprätthålla den personliga integriteten och
- upprätthålla ett högt förtroende hos medborgarna.

Kommunfullmäktige antog 2018 en integritetskyddspolicy[2] i syfte att leva upp till dataskyddsförordningen. Policyn syftar till att vara vägledande för behandling av personuppgifter i Vansbro kommun. Av policyn framgår förtydligande om vad en personuppgift är, vad behandling av densamma är samt hur personuppgifter samlas in och varför de behandlas. Utifrån detta ska personuppgiftsansvariga konkretisera policyn i anvisningar på förvaltningsområdesnivå och vidare genom instruktioner på enhetsnivå. Vi har i granskningen tagit del av samtliga förvaltningars anvisningar och intervjupersoner uppger att det även finns instruktioner på enhetsnivå.

På kommunens intranät finns information[3] angående hur en medarbetare på kommunen ska gå till väga vid en personuppgiftsincident. Informationen omfattar vad en personuppgiftsincident är och vart den ska anmälas beroende på allvarlighetsgrad. Om medarbetaren behöver hjälp att bedöma allvarlighetsgraden ska denne kontakta kommunens dataskyddsombud.

Utöver detta har kommunen har även upprättat regler och instruktioner för användandet av e-post[4], rutiner för användande av Teams[5] samt rutiner för loggning[6]. Av rutinerna för Teams framgår att känsliga eller sekretessbelagda uppgifter inte bör delas eller lagras i Teams. Rutinerna för loggning innehåller kortfattad information om loggning som sker i kommunens verksamhetssystem. Där framgår bl.a. vilka aktiviteter som ska loggas, hur loggarna ska hanteras samt bevaras, vilket enligt rutinerna beskrivs i de driftsplaner som upprättats av systemägaren för respektive verksamhetssystem. Av rutinerna framgår även att stickprov kan genomföras i känsliga system för att kontrollera om användare har använt systemen på ett icke korrekt sätt. Det framgår inte av dokumentet vem som genomför stickproven eller hur ofta stickprov ska genomföras. I uppföljning av internkontrollplan för 2021 framgår dock att

[1] Informationssäkerhetspolicy, kommunfullmäktige 2022-06-20
[2] Integritetsskyddspolicy, kommunfullmäktige, 2018-06-28
[3] Information på intranätet, *Vad gör du vid en personuppgiftsincident?* 2022-04-07, senast uppdaterad 2022-05-11
[4] Regler och instruktioner för användandet av e-post i Vansbro, uppdaterad 2018-06-20. Saknar datum för upprättande samt vem som antagit dokumentet.
[5] Information på intranätet, *Vad är Teams?* 2020-04-08, senast uppdaterad 2020-04-09
[6] Information på intranätet, *Loggning,* 2012-12-04, senast uppdaterad 2014-08-19

medicinskt ansvarig sjuksköterska (MAS) är ansvarig för samt har genomfört loggkontroller utifrån Nationell patientöversikt[7] (NPÖ). Enligt uppföljningen har inga brister upptäckts. Utöver detta har MAS tillsammans med en särskilt utsedd handläggare genomfört kontroller av händelseloggning i verksamhetssystemet Treserva. Kontrollen visade bl.a. att en av de chefer som ansvarar för att kontrollera händelseloggar inom sitt verksamhetsområde inte fullföljt kontrollen och att det därför finns en risk för otillbörligt utnyttjande av systemet.

Enligt informationssäkerhetspolicyn sker uppföljning av efterlevnad av styrande dokument inom området informationssäkerhet inom ramen för intern kontroll.

Intervjupersoner uppger att det i tid för granskningen saknas riktlinjer och rutiner avseende hantering av behörigheter och att det pågår ett arbete med att ta fram rutinbeskrivningar för hur verksamheterna ska arbeta med detta.

I intervjuer uppges att sekretariatet i Vansbro kommun utifrån ett eget initiativ samt på uppdrag från kommunchef arbetar för att driva på arbetet med informationssäkerhet utifrån de resurser som de kan avvara. Det uppges i intervjuer att nästa steg i informationssäkerhetsarbetet är att upprätta en prioriteringsordning av de åtgärder som kommunen behöver vidta, däribland upprättande av kompletterande riktlinjer och rutindokument utifrån informationssäkerhetspolicyn.

3.1.2 Roller och ansvar

Av informationssäkerhetspolicyn framgår att det är kommunstyrelsen som ansvarar för samordningen av informationssäkerhetsarbetet i kommunen. I den nya policyn antagen 2022 framgår inte att ansvaret för informationssäkerheten är kopplat till det delegerade verksamhetsansvaret, men intervjupersoner uppger att ansvaret är etablerat hos verksamhetscheferna.

Utöver detta har kommunen ett dataskyddsombud. Funktionen är en extern tjänst som kommunen köper in från ett informations- och kunskapsföretag. Enligt informationssäkerhetspolicyn är det dataskyddsombudets uppgift att kontrollera respektive personuppgiftsansvarigs efterlevnad av gällande dataskyddslagstiftning. Vidare uppges i policyn att dataskyddsombudet har granskande funktion och att denne i tillämpliga delar ska kontrollera efterlevnad av styrande dokument generellt. Intervjupersoner uppger att dataskyddsombudet ska enligt avtal inkomma med en rapport innan årsskiftet.

I övrigt uppges i intervjuer att det vid tid för granskningen saknas en uttalad roll- och ansvarsfördelning inom tjänstepersonsorganisationen avseende informationssäkerhetsarbetet. Som tidigare nämnts har sekretariatets chef gett sina medarbetare i uppdrag att driva arbetet utifrån de resurser de kan avvara.

Intervjupersoner lyfter att det finns en medvetenhet angående det informationssäkerhetsarbete som kommunen har behov av och att det begränsas av resursbrist. Investeringar i den här typen av arbete bortprioriteras då kommunens verksamheter är i behov av resurserna för andra uppgifter.

7

IT-avdelningen består i dagsläget av fem medarbetare inklusive IT-chefen. IT-avdelningen ansvarar för de IT-tekniska åtgärderna i informationssäkerhetsarbetet. Intervjupersoner uppger att finns ett behov av att permanenta organisationen för att få stabilitet i arbetet. Detta utifrån att vissa medarbetare innehar en tidsbegränsad anställning. Vidare uppges att medarbetarna inom IT-avdelningen har en bred kompetens men att avdelningen saknar en tydlig funktionsuppdelning. Det finns även ett behov av att ha IT-enhetens servicefunktioner nära kommunens verksamheter i syfte att finnas till hands vid behov, vilket intervjupersoner uppger att det saknas förutsättningar för i dagsläget. Intervjupersoner uppger att det finns behov av rollförtydligande mellan IT-avdelningen och övriga verksamheter.

Sedan 2021 har IT-avdelningen ett samverkansavtal med MOA[8] som bistår avdelningen med en så kallad första-linjen-support. Syftet med tjänsten är att den ska avlasta IT-avdelningen med att besvara enklare frågor och upprättades under en period när IT-avdelningen hade en låg bemanning på grund av personalomsättning samt sjukfrånvaro. I intervjuer uppges att det vid tiden för granskningen har det inte genomförts någon djupare analys om denna tjänst ska fortgå.

3.1.3 Bedömning

Utifrån det som framkommit i granskningen gör vi bedömningen att Vansbro kommun till viss del har upprättat styrande dokument avseende informationssäkerhet och att dessa är ändamålsenliga. Kommunen saknar styrande dokument avseende krav på IT-säkerhet. Detta innebär att det inte finns någon dokumenterad eller politiskt beslutad uppdragsbeskrivning över den IT-säkerhet som kommunen vill uppnå. Vi gör därför bedömningen att det finns behov av ett styrande dokument som tydliggör IT-avdelningens uppdrag och ansvar samt de krav som ska finns avseende teknisk säkerhet.

Det saknas även ett styrande dokument som reglerar hur anmälan och hantering av incidenter som inte är personuppgiftsincidenter ska ske. Sådana incidenter kan exempelvis vara att en medarbetare klickar på en länk i ett mejl som leder till virus i ett verksamhetssystem.

Vi ser positivt på att ett arbete har påbörjats med att upprätta rutinbeskrivning av behörighetstilldelning, dock ser vi även ett behov av att det upprättas en riktlinje som rutinbeskrivningen kan koppla an mot. Riktlinjen bör som ett övergripande styrdokument innehålla reglering angående exempelvis vem som har rätt att tilldela behörighet, hur ofta uppföljning av tilldelade behörigheter ska ske samt att avsaknad av inloggning efter ett visst antal dagar kräver en ny behörighetstilldelning.

Med anledning av den nya informationssäkerhetspolicyn rekommenderar vi kommunen att prioritera implementering av denna i syfte att informera och medvetandegöra kommunens anställda om policyn så att de i nästa steg kan efterleva policyn.

Vi ser även att det i rutindokumentet för loggkontroller saknas information angående ansvar för att genomföra stickprov på loggning samt med vilken periodicitet detta ska ske. Vi anser därför att rutindokumentet kan utökas med detta.

[8] Samarbete med Mora, Orsa och Älvdalen

Vi gör även bedömningen att upprättande av en prioriteringsplan bör prioriteras så att kommunen får en överblick över vilka åtgärder som är mest kritiska att vidta.

Då det i den nya policyn inte framgår att ansvaret för informationssäkerheten är kopplat till det delegerade verksamhetsansvaret, gör vi bedömningen att policyn bör utökas med detta förtydligande.

Vi gör bedömningen att kommunen har upprättat anpassningar och åtgärder utifrån regelverk och krav i enlighet med GDPR. Bedömningen görs utifrån att kommunen har upprättat styrande dokument avseende personuppgiftshantering och dataskyddsombudets funktion och ansvar, samt att kommunen har säkerställt kontinuitet angående rollen dataskyddsombud genom att köpa in tjänsten externt.

Av det som framkommer i granskningen gör vi bedömningen att det saknas en ändamålsenlig organisation avseende informationssäkerhetsarbete. I syfte att kunna upprätta samt bibehålla ett systematiskt informationssäkerhetsarbete bör kommunen överväga behovet av att utse en informationssäkerhetssamordnare.

3.2 Analys av behov och risker för informationssäkerhet

3.2.1 Riskhantering och informationsklassning

Av informationssäkerhetspolicyn framgår att informationsklassning ska genomföras utifrån säkerhetsaspekterna konfidentialitet, riktighet samt tillgänglighet. Det saknas rutinbeskrivning eller liknande för hur informationsklassning och riskbedömning ska genomföras samt vilken klassningsmodell som kommunen ska använda sig av. I intervjuer uppges att kommunen använder sig av MSB:s klassningsmodell, men att modellen inte är vidare beskriven eller tolkad utifrån kommunens nivå och behov.

Intervjupersoner uppger att kommunen i samband med en revisionsgranskning 2017 påbörjade arbetet med att klassa information samt verksamhetssystem. Dock har inte arbetet fullföljts och det uppges att verksamheterna har kommit olika långt i arbetet. Det pågår ett processkartläggningsarbete i kommunen där klassning av systemen är en del av arbetet.

Som en del i riskhanteringen har kommunen infört tvåfaktorinloggning för vissa system i kommunen. Tvåfaktorinloggning innebär att kommunens anställda behöver komplettera lösenordsinloggning med exempelvis en kod via sms eller en elektronisk tjänstelegitimation.

Då det saknas kommunövergripande riktlinjer samt upprättade rutiner för behörighetstilldelning hanterar verksamheterna detta på olika sätt.

Enligt uppföljningen av internkontrollplanen för 2021 framgår att kommunens verksamheter har upprättat kontinuitetsplaner som syftar till att kunna bibehålla verksamhet vid en eventuell incident. Uppföljningen visar att samtliga verksamheter har upprättat kontinuitetsplaner, dock framgår att planerna behöver standardiseras och göras enhetliga.

Sektor äldreomsorg har bl.a. papperskopior på alla mediciner som kan tas fram av samtliga sjuksköterskor och det finns rutiner och mallar för att följa upp medicinering som genomförts. Ett av kommunens omsorgsboende innehar reservkraft i syfte att kunna trygga elförsörjningen i händelse av elavbrott.

I kontakt med tjänstepersoner från Vansbro kommun framgår att kommunen har gjort bedömningen att de inte bedriver samhällsviktig verksamhet, utifrån de kriterier som finns för att identifieras som samhällsviktig verksamhet/tjänst. Det innebär att Vansbro kommun inte omfattas av regleringen i NIS-direktivet.

I faktakontrollen har synpunkt inkommit att kommunen som bredbandsleverantör är både NIS-pliktig verksamhet och att verksamheten omfattas av säkerhetsskyddslagen. Det ställer högre krav på ett mer systematiskt och riskbaserat informationssäkerhetsarbete för att inom dessa specifika delar uppnå de krav som lagarna ställer. Då synpunkten inkom till oss under faktakontrollen har vi inom ramen för granskningen inte särskilt granskat kommunens ansvar och efterlevnad utifrån dessa lagutrymmen utan det systematiska informationssäkerhetsarbetet för samtliga verksamheter på en övergripande nivå.

3.2.2 Medvetenhet och förståelse

Det uppges i intervjuer att kommunen startade upp ett informationssäkerhetsarbete under 2017, i samband med att kommunens revisorer genomfört en liknande granskning. Som en del i det arbetet genomfördes utbildningar under 2017 och 2018. Sedan dess har kommunen inte genomfört någon kommunövergripande utbildning inom informationssäkerhet. Sekretariatet genomför utbildning för dem som ska få tillgång till det centrala diariet för att det ska finnas en säker informationshantering. Vidare uppges att ledningsgruppen och ett antal utvalda medarbetare har genomgått en webbutbildning för informationssäkerhet samt att IT-avdelningen och sekretariatet har genomfört Försvarshögskolans säkerhetsutbildning. Utöver dessa finns en utbildning avseende GDPR tillgänglig på kommunens intranät. Det uppges inte finnas ett uttalat krav på kommunens medarbetare att genomföra den.

Av intervjuerna framgår det att kommunen har haft ett antal incidenter där den mänskliga faktorn har varit den utlösande faktorn. Det uppges därför finnas ett behov av att informera om vikten av informationssäkerhet i organisationen.

3.2.3 Bedömning

Vi gör bedömningen att kommunen saknar ett systematiskt och ändamålsenligt arbetssätt för att uppnå god informationssäkerhet. Vi ser positivt på att kommunen använder sig av MSB:s klassningsmodell men ser ett behov av att modellen anpassas efter kommunens behov. I övrigt saknas anvisningar och mallar för att genomföra riskbedömning och informationsklassning. Kommunen har påbörjat ett arbete med att klassa verksamhetssystem och information som hanteras, men vi bedömer att arbetet behöver fullföljas. Vi ser även att det saknas rutiner för att regelbundet ompröva genomförda riskanalyser och informationsklassningar för att möta nya risker och behov. Ansvaret för detta behöver etableras hos informationsägarna och rutiner behöver inrättas som en del i säkerställandet av att arbetet genomförs.

Vi bedömer att det finns viss medvetenhet i kommunen angående informationssäkerhet och vilka åtgärder som behöver vidtas. Vi ser ett behov av att genomföra utbildningar löpande för att öka medvetenhet och kunskap om informationssäkerhet hos kommunens anställda för att minska risken för att incidenter uppstår.

3.3 IT-säkerhetsåtgärder

Utifrån MSB:s rekommenderade säkerhetsåtgärder avseende system och IT uppges i intervjuer att kommunen har uppnått vissa punkter. Det finns vissa åtgärder som inte har kunnat genomföras, främst på grund av resursbrist.

I intervjuer framkommer att IT-avdelningen har tilldelats resurser i syfte att byta ut gammal nätverksutrustning, men det uppges ändå finnas ytterligare behov av resurstillsättning för bl.a. nyinvesteringar. Som en del i att skydda den information som hanteras inom kommunen lagras den mesta av informationen på lokala servrar.

Det framgår i intervjuer att kommunen har en viss teknisk övervakningsfunktion i syfte att upptäcka intrång och att kommunen håller sig uppdaterad om tillgängliga sårbarhetsverktyg[9] i syfte att säkerställa att kommunen innehar det verktyg som är bäst lämpat för kommunens behov. Utöver detta finns även fullskaligt överbelastningsskydd, skydd mot nätfiske samt driftövervakning av system.

Då verksamheterna i kommunen inte har fullgjort informationsklassningar har IT-avdelningen inte mottagit någon SLA (Service level agreement). I IT-sammanhang reglerar SLA vanligtvis vilken tillgänglighet ett system ska ha, hur lång tid som högst får passera innan felavhjälpning ska påbörjas, hur snabbt felet ska vara åtgärdat samt hur många gånger ett fel får förekomma under en given tidsperiod. Enligt intervjupersoner finns det upprättade SLA:er på många av de system som driftas av extern leverantör. Avsaknaden av SLA mellan verksamheterna och IT-avdelningen innebär att det i dagsläget inte finns någon dokumenterad prioritering för uppstart av verksamhetssystemen vid ett driftstopp.

Intervjupersoner uppger att kommunen har genomfört sårbarhetsanalyser och att det i dagsläget pågår ett arbete för att kunna genomföra en oberoende övergripande analys av IT-miljön inom kommunen. Vidare framgår det av intervjuerna att det framgent kommer finnas ett behov av att tillsätta en resurs för att kunna arbeta med detta på kontinuerlig basis.

3.3.1 Bedömning

Vår bedömning är att Vansbro kommun till viss del har etablerat ett systematiskt arbetssätt med IT-säkerhet för central IT-infrastruktur. IT-enheten har vidtagit åtgärder i syfte att säkerställa att kommunens system skyddas från digitala som fysiska intrång, dock ser vi ett behov av att ytterligare säkerhetsåtgärder vidtas för att möta hot och risker. Om en allvarlig incident skulle ske i nuläget bedömer vi att det finns en risk att information går förlorad eller skadas.

Vi ser främst att arbetet behöver utvecklas genom en högre grad av systematik, där åtgärder tar sin utgångspunkt i upprättade och dokumenterade riskanalyser. Utifrån dessa kan exempelvis mål- och handlingsplaner upprättas för att säkerställa att rätt prioriteringar görs utifrån sårbarhet och behov över tid. Dokumentationen kan även bidra till att förenkla det uppföljande arbetet.

[9] Exempel på sårbarhetsverktyg är sårbarhetsscanning samt penetrationstest

3.4 Incidenthantering

Som tidigare nämnts har kommunen en rutin avseende personuppgiftsincidenter men saknar en rutinbeskrivning för hur en incident som inte är en personuppgiftsincident ska hanteras i kommunen. Vidare uppges att det upplevs finnas en skev fördelning i kommunens verksamheter över i vilken utsträckning rapportering av personuppgiftsincidenter sker och att det kan bero på kunskapsbrist. Intervjupersoner uppger att anmälda incidenter dokumenteras men att dessa inte analyseras vidare.

Vidare uppges det att det pågår ett arbete med att upprätta ett internt incidenthanteringsdokument för IT-avdelningen. Dokumentet ska tydliggöra roller och ansvarsfördelning vid en eventuell incident. Vidare uppges att dokumentet ska bidra till att medarbetarna vid en långvarig incident växlar mellan roller och ansvar i syfte att minska risken för utmattning.

3.4.1 Bedömning

Vi gör bedömningen att det finns upprättade former för anmälan och hantering av personuppgiftsincidenter. Vi bedömer dock att det finns behov av att informera och uppmärksamma kommunens medarbetare och förtroendevalda om vad en incident är för att säkerställa att en anmälan faktiskt sker vid misstanke eller händelse av incident.

Vidare är vår bedömning att det saknas tydlighet för hantering av andra typer av incidenter. Vår bedömning är att det finns behov av att antingen upprätta former för hantering av incidenter, alternativt tydliggöra att hantering av personuppgiftsincidenter även omfattar incidenter av annan typ.

Vi ser positivt på att IT-avdelningen har för avsikt att upprätta en intern rutinbeskrivning för hur deras medarbetare ska hantera incidenter.

Utöver detta ser vi ett behov av att anmälda incidenter analyseras. Sådana analyser bidrar till att kunna vidta rätt åtgärder och förebygga att incidenten uppstår igen.

3.5 Intern kontroll, uppföljning och rapportering

3.5.1 Intern kontroll

Det framgår i intervjuer att informationssäkerhet inte har beaktats i det riskanalysarbete som ligger till grund för kommunens internkontrollplan 2022.

I internkontrollplanen för 2021 fanns kontrollpunkterna *loggning NPÖ* samt *händelseloggning* i ett verksamhetssystem, där kontrollen bland annat innebar hur riktlinjer för IT-användandet i Vansbro kommun efterlevdes. Som nämndes tidigare visade uppföljningen att en av de chefer som ansvarar för att kontrollera händelseloggar inom sitt verksamhetsområde inte fullföljt kontroll av loggning på grund av saknas behörighet. Det lyfts i uppföljningen att det därmed finns en risk för otillbörligt utnyttjande av systemet.

Som tidigare nämnts fanns även kontrollmomentet att kvalitetssäkra kommunens kontinuitetsplaner i internkontrollplanen för 2021.

3.5.2 Uppföljning och rapportering

Intervjupersoner uppger att det saknas ett tillräckligt uppföljningsarbete i kommunen angående det informationssäkerhetsarbete som bedrivs och de åtgärder som har vidtagits. Det uppges att uppföljning är en del i det arbete som pågår i kommunen med att bygga upp ett systematiskt informationssäkerhetsarbete.

I intervjuer framgår att informationssäkerhet diskuterats på kommunledningens möten där även kommunstyrelsens presidium medverkar. Vidare uppges att det inte sker någon systematisk återrapportering till kommunstyrelsen angående det informationssäkerhetsarbete som bedrivs i kommunen.

3.5.3 Bedömning

Vi konstaterar att kommunstyrelsen under år 2021 uppmärksammade informationssäkerhet i internkontrollplanen. Dock ser vi i internkontrollplanen för 2022 att det saknas kontrollmoment som kan kopplas till granskningsområdet. Vi gör därför bedömningen att kommunstyrelsen bör beakta informationssäkerhet i riskanalysarbetet som ligger till grund för internkontrollplanen.

Det saknas en systematisk uppföljning och återrapportering av det arbete som genomförs avseende informationssäkerheten och de säkerhetsåtgärder som vidtagits i kommunen. Vi bedömer därför att uppföljningsarbetet behöver stärkas inom kommunen. Då en stor del av arbetet som bedrivs i dagsläget genomförs på uppdrag av kommundirektör och sektorchef ser vi behov av att kommunstyrelsen som en del i sin styrning tar del av kommunens utveckling inom området. En återkommande uppföljning bidrar till bättre förutsättningar att identifiera ytterligare åtgärder som behöver vidtas.

4 Slutsats

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunen till stora delar saknar ett ändamålsenligt och systematiskt arbetssätt avseende informationssäkerhet.

Vår bedömning bygger på att det till viss del finns en styrning i arbetet genom styrande dokument, men det saknas en tydlighet i vilka krav som ställs i arbetet och hur ansvaret är fördelat. Det bedrivs ett visst arbete i kommunen, men det saknas i nuläget en systematik för att säkerställa att arbetet är tillräckligt.

Utöver detta ser vi ett behov av att kommunen stärker uppföljningsarbetet genom bl.a. att systematisera uppföljningen för att säkerställa att arbetet sker i enlighet med krav och beslut.

Utifrån kommunstyrelsens övergripande ansvar för informationssäkerhetsarbetet är det vår bedömning att uppföljning och rapportering till styrelsen bör etableras så att beslut om prioriteringar och åtgärder kan göras för att utveckla kommunens informationssäkerhetsarbete.

Då granskningen visar att kommunen i nuläget inte har ett etablerat informationssäkerhetsarbete är vår slutsats att det finns risker för en bristande efterlevnad utifrån krav i NIS-direktivet och säkerhetsskyddslagen.

5 Rekommendationer

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Säkerställa samt följa upp att implementering av nya informationssäkerhetspolicyn sker.
- Upprätta en handlingsplan/prioriteringsplan över åtgärder som behöver vidtas i syfte att stärka informationssäkerheten i kommunen.
- Upprätta ett styrande dokument som tydliggör IT-avdelningens uppdrag och ansvar samt de krav som ska finnas avseende teknisk säkerhet.
- Upprätta riktlinjer för behörighetshantering och införa kontroller för att tillse att riktlinjerna följs och att behörigheter är aktuella och korrekta.
- Se över nuvarande organisation och utreda behovet av att utse en informationssäkerhetssamordnare för att stärka arbetet.
- Upprätta former för genomförande av riskbedömning samt informationsklassning och säkerställa att dessa moment genomförs.
- Upprätta ett systematiskt arbetssätt med IT-säkerhet för central IT-infrastruktur. Arbetet bör ha sin utgångspunkt i upprättade och dokumenterade riskanalyser.
- Upprätta alternativt tydliggöra former för hantering av incidenter som inte är personuppgiftsincidenter.

- Säkerställa att anmälda incidenter analyseras i syfte att kunna vidta åtgärder för att minska risken att incidenten sker igen.
- Säkerställa att utbildning genomförs löpande för samtliga användare för att etablera medvetenhet och grundläggande kunskap om informationssäkerhet.
- Inkludera informationssäkerhet det riskanalysarbetet som ligger till grund för internkontrollplanen.
- Ställa krav om uppföljning och återrapportering om kommunens samlade informationssäkerhetsarbete så att beslut kan tas om mål och handlingsplan över erforderliga åtgärder för att förbättra informationssäkerheten.

Vansbro kommun
Granskning av kommunens informationssäkerhet

2022-12-05

Datum som ovan

KPMG AB

Johan Malm
Kommunal revisor/Kundansvarig

Jenny Thörn
Kommunal revisor

Ida Larsson
Kommunal revisor