Till Kommunfullmäktige i Knivsta kommun

25 oktober 2017

Revisionsrapport, Granskning av IT- och informationssäkerhet inom Samverkansnämnden

I egenskap av förtroendevalda revisorer i Knivsta kommun har vi granskat Samverkansnämnden Knivsta/Heby arbete med IT- och informationssäkerhet. Den övergripande revisionsfrågan är om Samverkansnämnden på en övergripande nivå har ändamålsenliga rutiner och processer för att hantera IT- och informationssäkerhet. I granskningen har vi biträtts av sakkunniga från PwC.

Vår övergripande bedömning är att arbetet kring IT- och informationssäkerhet till viss del uppfyller revisionsfrågans innebörd. Arbete inom informationssäkerhet har påbörjats och medvetenhet om vikten av detta är hög inom ledningen hos både Knivsta och Heby kommun. Det krävs ett antal åtgärder för att säkerställa en god informationssäkerhet varav några behöver verkställas snarast.

- System- och informationsklassning har påbörjats i Knivsta men ej i Heby. Ur informationssäkerhetssynpunkt måste detta finnas på plats för att möjliggöra rätt nivå av säkerhet och skydd av känslig information, speciellt i ljuset av kommande dataskyddsförordning (GDPR), är det av vikt att detta arbete prioriteras och slutförs.

- Det saknas återkommande risk- och sårbarhetsbedömningar ur ett informationssäkerhetsperspektiv. Vi rekommenderar att samverkansnämnden etablerar en process för återkommande riskbedömningar för att möjliggöra upprättande av åtgärdsplaner för de prioriterade riskerna.

- Det saknas tydliga riktlinjer för hur man som medarbetare skall förhålla sig till informationssäkerhet och integritet och hur incidenter skall hanteras. Vi rekommenderar att samverkansnämnden snarast fastställer riktlinjer för informationssäkerhet och incidentrapportering samt en rutin för återkommande utbildning för samtlig personal.

- Det saknas processer för att säkerställa att medarbetare har rätt behörighetsnivå och därmed deras tillgång till skyddsvärd eller känslig information. Ansvaret för behörigheter ligger i dag på enhetscheferna. Vi rekommenderar att samverkansnämnden snarast inför en process för återkommande revision av behörigheter för att säkerställa att medarbetare som bytt tjänst inte har för hög behörighet och att medarbetare som lämnat sin tjänst också avslutas i systemen.

I rapporten lämnas även förslag på andra rekommendationer

Revisorerna överlämnar härmed granskningsrapporten för kännedom och yttrande. **Vi förväntar** oss att yttrandet innehåller en tidplan över vilka åtgärder som planeras att vidtas med anledning av de rekommendationer som lämnas i rapporten. Yttrande från Samverkansnämnden önskas senast den **15 december** 2017.

För Knivsta kommuns revisorer

Eva Enskär
Ordförande

Bilaga: Revisionsrapport "Granskning av IT-och informationssäkerhet inom Samverkansnämnden" PwC.

www.pwc.se

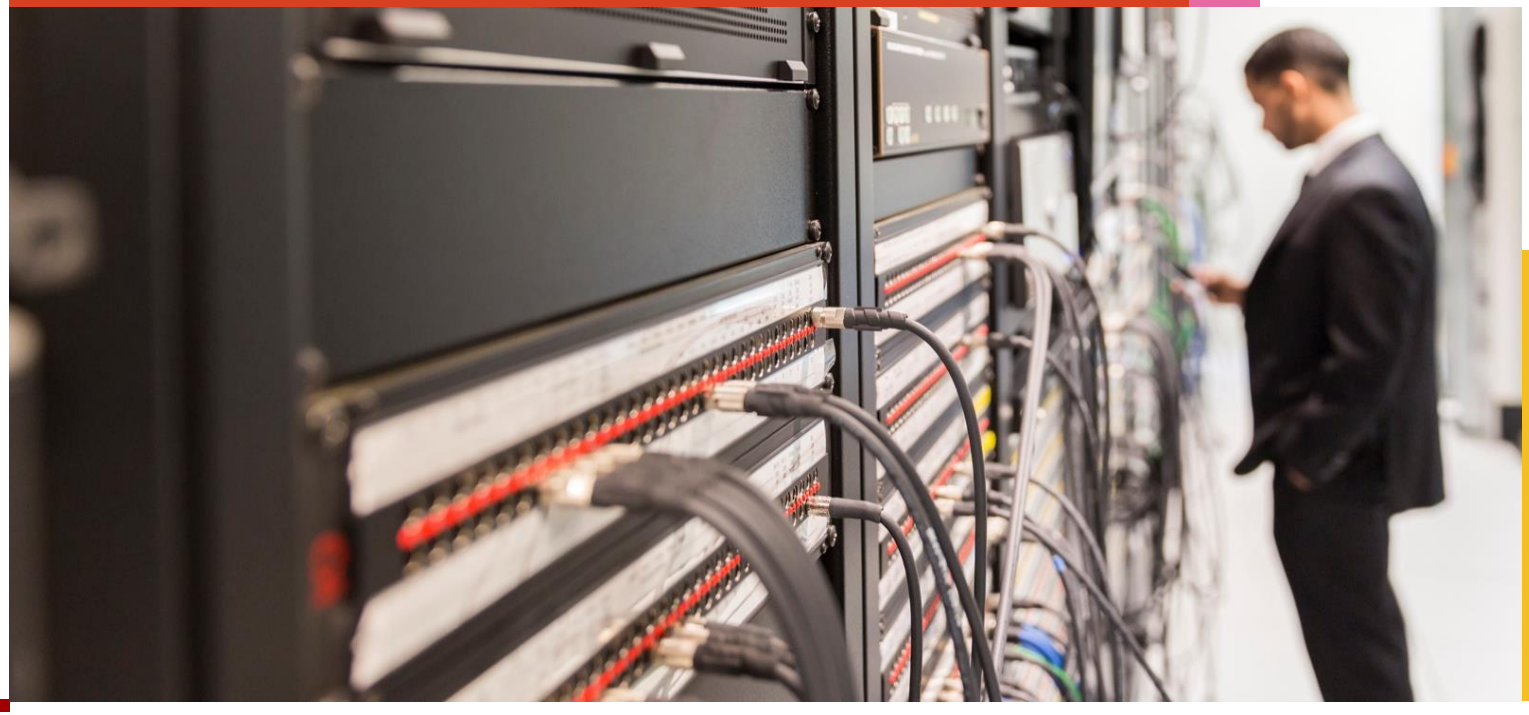
Knivsta och Heby kommun

Granskning av IT- och informations-säkerhet inom Samverkansnämnden Oktober 2017

Knivsta kommun

HEBY KOMMUN

10 oktober 2017



pwc

Innehåll

Sammanfattning

Under perioden augusti till oktober 2017 har PwC på uppdrag av revisorerna i Knivsta och Heby kommuner genomfört en översiktlig granskning av Samverkansnämndens arbete med IT- och informationssäkerhet. *Syftet har varit att granska om Samverkansnämnden på en övergripande nivå har ändamålsenliga rutiner och processer för att hantera IT- och informationssäkerhet.*

Vår övergripande bedömning är att arbetet kring informationssäkerhet till viss del uppfyller revisionsfrågans innebörd. Arbete inom informationssäkerhet har påbörjats och medvetenhet om vikten av detta är hög inom ledningen hos både Knivsta och Heby kommun. Det krävs ett antal åtgärder för att säkerställa en god informationssäkerhet varav några behöver verkställas snarast.

- System- och informationsklassning har påbörjats i Knivsta men ej i Heby. Ur informationssäkerhetssynpunkt måste detta finnas på plats för att möjliggöra rätt nivå av säkerhet och skydd av känslig information, speciellt i ljuset av kommande dataskyddsförordning (GDPR), är det av vikt att detta arbete prioriteras och slutförs.
- Det saknas återkommande risk- och sårbarhetsbedömningar ur ett informationssäkerhetsperspektiv. Vi rekommenderar att samverkansnämnden etablerar en process för återkommande riskbedömningar för att möjliggöra upprättande av åtgärdsplaner för de prioriterade riskerna.
- Det saknas tydliga riktlinjer för hur man som medarbetare skall förhålla sig till informationssäkerhet och integritet och hur incidenter inom området dessa skall hanteras. Vi rekommenderar att samverkansnämnden snarast fastställer riktlinjer för informationssäkerhet och incidentrapportering samt en rutin för återkommande utbildning för samtlig personal.
- Det saknas processer för att säkerställa att medarbetare har rätt behörighetsnivå och därmed deras tillgång till skyddsvärd eller känslig information. Ansvaret för behörigheter ligger i dag på enhetscheferna. Vi rekommenderar att samverkansnämnden snarast inför en process för återkommande revision av behörigheter för att säkerställa att medarbetare som bytt tjänst inte har för hög behörighet och att medarbetare som lämnat sin tjänst också avslutas i systemen.

Bakgrund, syfte och övergripande revisionsfråga

Inledning

Under perioden augusti till oktober 2017 har PwC på uppdrag av revisorerna i Knivsta och Heby kommuner genomfört en översiktlig granskning av Samverkansnämndens arbete med IT- och informationssäkerhet. Granskningen omfattar Samverkansnämndens gemensamma IT-enhet.

Resultatet av granskningen presenteras i denna rapport.

Syfte

Uppdraget innebar att inom ramen för revisionsarbetet inom kommunerna genomföra en övergripande granskning av den gemensamma nämndens arbete med IT- och informationssäkerhet för att förstå och analysera huruvida verksamheten på en övergripande nivå har ändamålsenliga rutiner och processer för att hantera informationssäkerhet. Granskningen har översiktligt fokuserat på; styrning och ledning av IT- och informationssäkerhet, samt rutiner, processer, uppföljning, samt personalaspekter såsom kompetens och bredd.

Syftet med granskningen är att klargöra vilka eventuella områden som Samverkansnämnden behöver utveckla för att uppnå ändamålsenliga rutiner och processer för att hantera IT- och informationssäkerhet på ett för kommunen lämpligt sätt.

Övergripande revisionsfråga

Rapporten avser att belysa följande övergripande revisionsfråga:

Har Samverkansnämnden på en övergripande nivå ändamålsenliga rutiner och processer för att hantera IT- och informationssäkerhet?

För att besvara den övergripande revisionsfrågan har sex områden definierats, bestående av totalt elva delfrågor, se nästa sida.

Revisionsfrågor

Har Samverkansnämnden på en övergripande nivå ändamålsenliga rutiner och processer för att hantera IT- och informationssäkerhet?

Revisionsfrågor delområden:

Styrning av IT

1. Finns det en etablerad styrmodell för IT-verksamheten avseende IT-relaterade prioriteringar inklusive informationssäkerhet?

Styrande dokument

2. Finns beslutade styrande dokument (t.ex. IT-strategi, IT-policy, IT/informationssäkerhetspolicy samt kontinuitetsplan kopplat till informationssäkerhet? Är dessa kommunicerade?)

Informationssäkerhet

3. Har informationssäkerhetsarbetet organiserats på ett ändamålsenligt sätt?
4. Kontrolleras efterlevnaden av riktlinjer för informationssäkerhet?
5. Sker informationsklassning enligt en systematisk metod?
6. Sker utbildning av medarbetare i IT- och informationssäkerhet?
7. Beaktas IT- och informationssäkerhetsrelaterade aspekter vid upphandling/anskaffning av system och applikationer?

IT-Processer

8. Finns det rutiner för rapportering och hantering av säkerhetsbrister och incidenter kopplade till IT och informationssäkerhet?

IT-säkerhet

9. Har risk- och systemsäkerhetsanalyser genomförts för verksamhetskritiska system?
10. Är åtkomstskydd till kritiska system och applikationer (behörighet och lösenord) lämpligt utformat? Genomförs periodisk granskning av tilldelade behörigheter?

IT-drift

11. Är IT-infrastrukturen uppbyggd enligt god praxis och skapar den förutsättningar för ett kvalitativt och säkert IT-stöd (t.ex. finns rutiner och processer för backup och återställning av data)?

Metod

Metod

PwC har baserat granskningen på följande arbetssätt och metodik.

- Intervjuer med identifierade nyckelpersoner i Knivsta och Heby kommuner, (se intervjulista, bilaga 1) samt inläsning och genomgång av tillgänglig dokumentation och styrande dokument.
- Granskningen baseras på PwC:s modell för IT-styrning och IT-mognad (ITM), etablerad god praxis, samt delar av ramverket för informationssäkerhet från National Institute of Standards and Technology (NIST).

Avgränsning

- Erhållet material har granskats på en övergripande nivå.
- PwC har endast granskat den information som tillgängliggjorts för oss.
- Vidare har PwC inte specifikt analyserat Samverkansnämndens externa IT-driftleverantör.
- Verksamhet inom olika kommunala bolag har inte granskats specifikt.

Revisionell bedömning

Övergripande revisionsfråga

Har Samverkansnämnden på en övergripande nivå ändamålsenliga rutiner och processer för att hantera IT- och informationssäkerhet?

Bedömning

Vår övergripande bedömning är att Samverkansnämndens arbete med IT- och informationssäkerhet till viss del uppfyller revisionsfrågans innebörd. Ett strukturerat arbete inom informationssäkerhet har påbörjats och det finns en medvetenhet inom respektive kommun och Samverkansnämnden att det krävs ett antal åtgärder för att optimera arbetet med informationssäkerhet. Vår bedömning är dock att kommunerna kommit olika långt i denna process, där Knivsta kommun uppfattas kommit längre i jämförelse med Heby kommun. Knivsta kommun, till skillnad från Heby kommun, genomför till exempel informationsklassning, har börjat uppdatera befintliga styrdokument kopplade till IT- och informationssäkerhet och utbildar nyanställda chefer inom området. Avseende förberedelse för GDPR, är vår bedömning dock att Heby kommun kommit något längre.

- Det finns en viss diskrepans i uppfattningen inom respektive kommun avseende Samverkansavtalets ansvarsområden och innebörd. Som exempel angavs det under intervjuerna att det tidigare funnits oklarheter kring vilken part som ansvarar för att ta framstyrande dokument.
- Uppdaterade och förnyade styrande dokument i form av IT-strategi, IT-policy, IT/informationssäkerhetspolicy samt kontinuitetsplan med tillhörande riktlinjer, anvisningar och användarvänliga instruktioner bör fastställas och tydligt kommuniceras till användare inom respektive kommun.
- Roller och ansvar kopplade till informationssäkerhet och integritet bör tydliggöras i allmänhet, men särskilt med anledning av kommande dataskyddsförordning (GDPR) som ersätter PUL.
- Kunskapsnivån och medvetenheten avseende IT- och informationssäkerhet varierar bland medarbetarna inom båda kommunerna. De medarbetare som aktivt arbetar med frågor relaterade till IT- och informationssäkerhet bedöms ha en högre grad av kunskap och medvetenhet inom området, i jämförelse med de medarbetare som inte har dessa frågor som primära arbetsområden. Därav är det av vikt att alla medarbetare erbjuds vidare utbildning inom dessa områden och bör ske regelbundet och återkommande.
- Även om respektive kommun är enskilt ansvarig för att tillgodose den egna verksamhetens efterlevnad av lagar, förordningar och regler kopplade till informationssäkerhet, kan detta arbete med fördel samordnas inom Samverkansnämnden. Ett samarbete avseende framtagning av rutiner, processer och dokument kan bland annat leda till högre effektivitet och samsyn avseende avtalets ansvarsområden och innebörd. Vidare bör även en gemensam process för återkommande och regelbundna riskanalyser införas.

Delfråga 1

Finns det en etablerad styrmodell för IT-verksamheten avseende IT-relaterade prioriteringar?

Observationer

- Den strategiska och driftsmässiga ledningen av IT delas mellan Knivsta och Heby. Det finns idag en IT-chef och en IT-driftschef med ansvar för bägge kommunerna.
- Den gemensamma samverkansnämnden för IT ansvarar för de båda kommunernas IT-drift och IT-strategiska frågor. Ansvaret för frågor kring förvaltning och verksamhetsutveckling samt organisation för LIS/informationssäkerhet och hantering av informationssäkerhetsfrågor ligger hos varje kommun. Den gemensamma nämnden kan ges i uppdrag att ta fram olika beslutsunderlag i dessa frågor*.
- Det framkommer under intervjuerna att det inte finns någon ”tydligt etablerad” styrmodell för IT-verksamheten. Det som finns i dagsläget är generella mål för IT (uttryckt i de kommunala målen).
- För löpande styrning & prioritering av IT-relaterade frågor finns i respektive kommun en eStyrgrupp som leds av kommunchefen i Heby kommun och av kanslichefen i Knivsta kommun.

Rekommendationer

- Kommunerna bör ta fram en detaljerad plan och övergripande strategi/styrmodell för sin respektive IT-verksamhet. Denna styrmodell bör utgå från respektive kommuns vision och långsiktiga strategiska mål, samtidigt som Samverkansnämndens gemensamma mål och prioriteringar bör beaktas. Vidare bör den beskriva hur IT ska bidra till att uppfylla dessa mål.
  - Styrmodell bör kompletteras med en handlingsplan med prioriterade aktiviteter. Den bör omfatta både egna och Samverkansnämndens gemensamma prioriteringar.
  - Styrmodellen bör beslutas inom kommunledning och ägas av IT- och informationsansvariga.
  - Arbetet med att planera och ta fram styrmodellerna, kan med fördel samordnas inom Samverkansnämnden för att nå högre effektivitet och transparens.

* Källa: Verksamhetsberättelse och årsbokslut för Samverkansnämnden 2016.

Delfråga 2

Finns beslutade styrande dokument (t.ex. IT-strategi, IT-policy, IT/informationssäkerhetspolicy samt kontinuitetsplan kopplat till informationssäkerhet? Är dessa kommunicerade?

Observationer

- Granskningen visar att det i dagsläget saknas uppdaterade styrdokument gällande IT-strategi, IT-policy samt handlingsplan. Det senast uppdaterade IT-strategidokumentet i Knivsta kommun är daterat 2008-02-28, dock visar intervjuerna att innehållet inte blivit tydligt kommunicerat till berörda medarbetare.
- Utöver ovannämnda dokument saknas aktuell IT-säkerhetspolicy och informationssäkerhetspolicy. I Knivsta kommun finns dock utkast som är under revidering. Planen är att uppdaterade policys ska kommuniceras till verksamheten efter årsskiftet 2017/2018.
- Övergripande kontinuitetsplan för IT-verksamheten saknas, även om det under intervjuerna angavs finnas mer utvecklade kontinuitetsplaner för vissa delar av verksamheten i båda kommunerna (t.ex. Socialförvaltningen).
- Inom Knivsta kommun pågår ett arbete med att uppdatera och komplettera de befintliga styrande dokumenten för informationssäkerhet. I Heby kommun har en medarbetare fått ansvar att påbörja arbetet med att ta fram relevanta styrdokument.

Rekommendationer

- Respektive kommun bör ta fram en plan för att komplettera IT-relaterade styrande dokument, där bland annat följande dokument för IT behöver utvecklas:
  - IT-strategi, IT-policy och handlingsplan.
  - IT-säkerhets- och Informationssäkerhetspolicy, kontinuitetsplan för IT-verksamheten.
  - Arbetet med att planera och ta fram dessa styrdokument, kan med fördel samordnas inom Samverkansnämnden för att nå högre effektivitet och transparens. Samt förbereda för den planerade utvecklingen av samverkansnämnden med fler kommuner.
- Vidare bör respektive kommun ta fram ändamålsenliga, användarvänliga och lättillgängliga riktlinjer, anvisningar och instruktioner kopplade till dessa styrande dokument.

Delfråga 3

Har IT- och informationssäkerhetsarbetet organiserats på ett ändamålsenligt sätt?

Observationer

- Under intervjuerna framkommer det att IT-organisationen har genomgått stora förändringar under senare tid, vilket har påverkat IT-och informationssäkerhetsarbetets framgång.
- Granskningen visar att arbetet med IT-och informationssäkerhet till viss del organiserats och påbörjats, där det under intervjuerna framkommer att t.ex. en person i respektive kommun anställts på heltid för att arbeta med frågor kopplat till dessa områden. Dock är detta arbete i ett initialt skede.
- Det saknas dokumenterade roll- och ansvarsbeskrivningar relaterade till IT-och informationssäkerhetsarbetet samt process för identifiering/tilldelning av informationsägarskap.
- Av intervjuerna framkommer det att det råder en brist i samarbetet och kommunikationen mellan verksamheten och IT. Det upplevs saknas tydliga kontaktpersoner och kommunikationsvägar.
- Vidare framkommer att det saknas tydliga och uppdaterade kontinuitetsplaner kopplade till informationssäkerhets-incidenter. Dock framkommer det att dessa planer är under bearbetning.
- Utifrån intervjuerna bedöms det finnas en medvetenhet bland medarbetarna kring fördelarna samt vikten av att börja av ett välorganiserat IT-och informationssäkerhetsarbete.

Rekommendationer

- Samverkansnämnden bör vidareutveckla den övergripande planen för hur arbetet med informationssäkerhet ska organiseras inom kommunerna. När en sådan plan är upprättad bör den på ett strukturerat sätt kommuniceras till verksamheten, i syfte att skapa en samsyn beträffande informationssäkerhetsarbetet.
- Vidare bör även roll- och ansvarsbeskrivningar fastställas för samtliga roller relaterade till informationssäkerhetsarbetet inom kommunernas verksamheter. Bland dessa roller bör den roll som omfattar ansvaret för att leda arbetet med att anpassa respektive kommuns verksamhet till den nya dataskyddsförordningen (GDPR*) ingå. För denna roll krävs, utöver en tydlig rollbeskrivning, mandat samt erforderlig kompetens då regelverket i den nya förordningen är mer komplext än Personuppgiftslagen (PuL).
- En process för identifiering och tilldelning av informationsägarskap bör tas fram.
- Vidare rekommenderas att kommunerna planerar och genomför återkommande kris- och katastrofövningar kopplade till IT/informationssäkerhet och integritet för att säkerställa en god beredskap för intrång med förlust av t.ex. känsliga persondata samt identifiera och rätta fel i processerna.

***) GDPR** – (General Data Protection Regulation). Ny dataskyddsförordning som är gemensam inom EU och ersätter Personuppgiftslagen. GDPR träder i kraft 25 maj 2018. I Sverige kommer Datainspektionen att vara tillsynsmyndighet

Delfråga 4

Kontrolleras efterlevnaden av riktlinjer för informationssäkerhet?

Observationer

- Granskningen visar att det inte finns några etablerade rutiner, strukturerade processer eller kontroller avseende uppföljning av medarbetarnas efterlevnad av riktlinjer inom IT- och informationssäkerhet eller övriga IT-relaterade styrande dokument.

Rekommendationer

- För att identifiera, hantera och förebygga eventuella incidenter relaterade till IT- och informationssäkerhet är det av vikt att respektive kommun tar fram en strukturerad plan som säkerställer medarbetarnas efterlevnad av policys, riktlinjer, anvisningar och instruktioner. Arbetet med att ta fram en sådan plan kan med fördel samordnas inom Samverkansnämnden för att nå högre effektivitet och transparens.

Delfråga 5

Sker informationsklassning enligt en systematisk metod?

Observationer

- I Knivsta kommun genomförs informationsklassning med hjälp av verktyget *KLASSA**. Dock framkommer det under intervjuerna att detta inte genomförs med regelbundenhet. Vidare framkommer att det saknas en övergripande och gemensam plan avseende vilka system som ska informationsklassificeras och under vilka omständigheter.
- I Heby kommun har arbetet med informationsklassning inte påbörjats i någon större omfattning. Intervjuerna visar dock att det finns en medvetenhet kring fördelarna samt vikten av att börja arbeta med informationsklassning.

Rekommendationer

- Vi rekommenderar respektive kommun att ta fram en strukturerad plan för hur arbetet gällande informationsklassificering ska genomföras. Planen bör innehålla en tydlig beskrivning av målen med informationsklassificeringen samt hur dessa mål ska uppfyllas inom respektive verksamhet.
  - Arbetet med att utveckla denna plan kan med fördel samordnas inom Samverkansnämnden för att nå högre effektivitet och transparens.
- Med bakgrund av den kommande dataskyddsförordningen (GDPR), är det av vikt att Knivsta kommun fortsätter arbetet med informationsklassning på ett mer strukturerat sätt samt att Heby kommun skyndsamt påbörjar arbetet med informationsklassning enligt en systematisk metod.

***) KLASSA** – En metod framtagen av SKL för att hjälpa verksamheten välja rätt åtgärder som skyddar informationen.

Delfråga 6

Sker utbildning av medarbetare i IT- och informationssäkerhet?

Observationer

- Det saknas en fastställd utbildningsplan för utbildning inom IT och informationssäkerhet hos båda kommunerna. Dock framkommer det att en plan är under framtagning inom vilken målet är att varje nyanställd ska få möjlighet att delta i relevanta utbildningar.
- Det finns en webbaserad utbildningsplattform hos båda kommunerna som främst är tillgänglig för nyanställda chefer. Plattformen nämns vara under vidareutveckling.
- I Knivsta kommun genomförs inte strukturerade utbildningar i IT och/eller informationssäkerhet i någon större omfattning, med undantag för nyanställda chefer som genomgår en sådan utbildning. För övriga medarbetare finns ingen motsvarande utbildning.
- I Heby kommun genomgår ingen medarbetare någon utbildning avseende IT- och/eller informationssäkerhet, med undantag för Socialförvaltningen där utbildning av nyanställda sker riktad mot information som skyddas av offentlighets- och sekretesslagen. Arbetet har dock påbörjats inom Heby kommun med att ta fram en kortare introduktionsutbildning, vilken planeras vara färdig under december 2017.
- Kunskapsnivån och medvetenheten avseende IT och informationssäkerhet varierar bland medarbetarna inom båda kommunerna. De medarbetare som aktivt arbetar med frågor relaterade till IT och Informationssäkerhet bedöms ha en högre grad av kunskap och medvetenhet inom området, i jämförelse med de medarbetare som inte har dessa frågor som primära arbetsområden. Det framkommer dock att det inom Socialförvaltningen bedöms föreligga en hög grad av kunskap och medvetenhet avseende information som skyddas av offentlighets- och sekretesslagen.

Rekommendationer

- Kommunerna rekommenderas fortsätta sitt påbörjade arbete med en mer strukturerad utbildningsplan inom IT- och informationssäkerhet. Detta arbete kan med fördel samordnas inom Samverkansnämnden för att nå högre effektivitet och transparens.
  - Utbildningsplanen bör omfatta alla anställda och innehålla information om vilken kunskapsnivå en viss roll kräver, samt vilken typ av kunskapshöjande aktiviteter som bör genomföras.
  - Vidare bör kommunerna tydliggöra ansvaret för att utbildning inom IT- och informationssäkerhet ska ske regelbundet och återkommande, i syfte att öka kunskapen och medvetenheten hos medarbetare inom ämnet. I ett initialt skede skulle detta ansvar kunna ligga på informationssäkerhetssamordnaren.
- För att tillfullo utnyttja de resurser som investerats i respektive kommuns utbildningsplattform, bör kommunerna säkerställa att dessa tillgängliggörs och nyttjas av fler medarbetare än enbart nyanställda chefer.
- Kommunerna bör även skyndsamt säkerställa att utbildning kring regelverket i den nya dataskyddsförordningen (GDPR) genomförs. Denna utbildning bör bland annat omfatta hur det skiljer sig från PUL samt vilka krav det ställer på hantering av personuppgifter.

Delfråga 7

Beaktas IT- och informationssäkerhetsrelaterade aspekter vid upphandling/anskaffning av system och applikationer?

Observationer

- Under intervjuerna framkommer det att upphandling normalt sker med hjälp av Kammarkollegiets ramavtal. Dessa avtal innehåller bland annat rekommendationer över vilka informationssäkerhetsrelaterade aspekter som bör beaktas vid upphandling.
- Granskningen visar dock att ramavtalen inte alltid används som underlag vid upphandling. Som exempel nämns bland annat att anskaffningen av den nya IT-leverantören (Advania) inte granskades i enlighet med ”utökade” informationssäkerhets-relaterade aspekter. Den nya leverantören anges enbart ha granskats i enlighet med de grundläggande krav gällande dataskydd, accesskontroll samt fysisk/logisk tillgång som IT-enheten har.
- Respektive förvaltnings/kontorschef är i dagsläget ansvarig för inköp av verksamhetssystem. Dock framkommer det under intervjuerna att IT inte är involverade i denna process.

Rekommendationer

- För att säkerställa en ändamålsenlig informationssäkerhet och god teknisk IT-säkerhet, är vår rekommendation att upphandling av kritiska system/applikationer/tjänster, ska ske i enlighet med de utökade krav på informationssäkerhet som bland annat ställs i relation till införandet av den nya dataskyddsförordningen.
- Vid upphandling av nya system och applikationer, bör IT användas som en rådgivande stödfunktion i tekniska frågor bland annat relaterade till IT- och informationssäkerhet. Genom detta tillvägagångssätt kan verksamheten få råd kring exempelvis det tilltänkta systemets eller applikationens lämplighet i relation till den nuvarande systemfloran samt kapacitetsplanering.

Delfråga 8

Finns rutiner för rapportering och hantering av säkerhetsbrister och incidenter kopplade till IT- och informationssäkerhet?

Observationer

- Av granskningen framkommer att ändrings-, incident och problemhantering avseende verksamhetskritiska IT-system och applikationer hos båda kommunerna är utlagt på extern leverantör.
- Det framkommer dock av intervjuerna att det saknas generella rutiner för rapportering och hantering av säkerhetsbrister och incidenter kopplade till IT- och informationssäkerhet inom båda kommunerna. Som exempel nämns att det råder en oklarhet bland medarbetarna avseende vem, vad, när och hur en säkerhetsbrist ska rapporteras.
- Dock visar intervjuerna samtidigt på att det inom Socialförvaltningen i respektive kommun finns dokumenterade rutiner och beskrivningar för incidenter avseende information som skyddas av offentlighets- och sekretesslagen.

Rekommendationer

- Rutiner för rapportering och hantering av säkerhetsbrister och incidenter kopplade till IT- och informationssäkerhet bör snarast upprättas, dokumenteras och anpassas till samtliga förvaltningar (kontor), samt kommuniceras och tillgängliggöras till verksamheten inom respektive kommun.

Delfråga 9

Har risk- och systemsäkerhetsanalyser genomförts för verksamhetskritiska system?

Observationer

- Granskningen visar att det i Knivsta kommun främst är en medarbetare som genomför riskanalyser avseende IT- och informationssäkerhet. Enligt intervjuerna finns det dock inte några strukturerade processer och rutiner för detta arbete.
- Avseende Heby kommun visar intervjuerna att det inte genomförs regelbundna riskanalyser avseende IT- och informationssäkerhet. Det saknas även strukturerade processer och rutiner för detta arbete.
- Det framgår av granskningen att det är respektive systemägare som är ansvarig för att genomföra systemsäkerhetsanalyser. Det saknas dock strukturerade processer och rutiner för att säkerställa att sådana analyser genomförs regelbundet.
- Vidare visar intervjuerna att uppdateringen av vissa verksamhetskritiska system varit bristfällig under de senaste åren. I samband med sammanslagningen mellan Knivsta/Heby kommuner har dock fler uppdateringar genomförts, även om det fortfarande uppges finnas ett behov av ytterligare uppdateringar.

Rekommendationer

- Risk- och systemsäkerhetsanalyser är en kritisk del i arbetet med att nå en ändamålsenlig hantering av IT- och informationssäkerhet då dessa bidrar i arbetet med att identifiera risker, som vid allvarliga händelser, kan få väsentlig påverkan på verksamhetskritiska system och processer. Vår rekommendation är därför att kommunerna tar fram tydliga processer och rutiner för att säkerställa att risk- och systemsäkerhetsanalyser genomförs på ett ändamålsenligt sätt. Samverkansnämnden bör samordna detta arbete för att nå en högre effektivitet och samsyn mellan kommunerna.
- För att säkerställa en god tekniskt IT-säkerhet och skydda verksamhetskritisk information, krävs ett aktivt arbete för att upptäcka/motverka intrångsförsök i system och applikationer. Vi rekommenderar därför att respektive kommun tar fram en strukturerad plan med rutiner och processer för vilka system och applikationer som ska uppdateras och med vilka tidsintervall. Samverkansnämnden bör samordna detta arbete för att nå en högre effektivitet och samsyn mellan kommunerna.

Delfråga 10

Är åtkomstskydd till kritiska system och applikationer (t.ex. behörighet och lösenord) lämpligt utformat? Genomförs periodisk granskning av tilldelade behörigheter?

Observationer

- Rent formellt är det respektive förvaltningschef (kontorschef) som är ansvarig att granska, registrera och avsluta medarbetares behörighet och tillgång till diverse verksamhetskritiska system och applikationer. Dock visar intervjuerna att det inte genomförs några strukturerade kontroller för om huruvida medarbetares behörigheter genomförs i enlighet med uppsatta rutiner eller ej.
- Vidare anges det inte finnas några dokumenterade riktlinjer, anvisningar eller instruktioner kopplade till behörighetskontroll (t.ex. upplägg/avslut av medarbetares tillgång till system och applikationer samt beskrivning för när behörigheter ska granskas).
- Av intervjuerna framkommer att tilldelning av behörigheter fungerar väl vid nyanställning. Vid internt byte och avslut av tjänst, upplevs behörighetskontrollen i vissa situationer som bristfällig.

Rekommendationer

- För att säkerställa ett välfungerande åtkomstskydd, behövs uppdaterade och mer organiserade rutiner och processer för respektive kommun avseende upplägg, avslut och granskning av tilldelade behörigheter. Samverkansnämnden kan bidra i detta arbete med syfte att skapa en samsyn mellan kommunerna inom detta område.

Delfråga 11

Är IT-infrastrukturen (kommunens interna nätverks-infrastruktur) uppbyggd enligt god praxis och skapar den förutsättningar för ett kvalitativt och säkert IT-stöd (t.ex. finns rutiner och processer för backup och återställning av data)?

Observationer

- Granskningen visar att Samverkansnämnden ska byta leverantör från Axians till Advania i november 2017. Detta omfattar alla tjänster kopplat till drift, nätinfrastruktur samt backup och återställning av data.
- Vidare ägs IT-plattformen av Samverkansnämnden, där IT-enheten ansvarar för driften av kommunernas interna nätverk.
- Den IT-infrastruktur som är utlagd på extern leverantör antas vara uppbyggd enligt grundläggande förutsättningar som finns för god praxis, dock inkluderas inte Axians/Advanias processer och rutiner avseende dessa områden i denna granskning.
- Den IT-infrastruktur som är kopplad till kommunernas interna nätverk uppfattas i vissa situationer vara av ”för hög säkerhetsnivå”, där medarbetare delger att nivån på säkerhet påverkar nätverkets användarvänlighet negativt. Det noteras dock att det inte har genomförts några återkommande riskanalyser som grund för nätverkets säkerhetsnivå eller några penetrationstester.
- Vidare framkommer det i granskningen att det genomförts återläsning av data vid incidenter (t.ex. om specifik information förlorats). Det har dock inte genomförts några planerade tester av leverantörens förmåga avseende backup- och återställning av data.

Rekommendationer

- För att fastställa ett säkert IT-stöd samt att leverantören uppfyller överenskommet SLA, bör kommunerna framta en rutin för återkommande tester avseende backup och återställning av data (så kallade ”disaster recovery tester”).
- För att säkerställa att leverantören levererar ett ändamålsenligt och säkert IT-stöd, bör Samverkansnämnden begära in styrande dokument relaterade till IT (t.ex. disaster reocvery-plan, kontinuitetsplan) samt karta över deras IT-infrastruktur.
- Vi rekommenderar att kommunerna implementerar en process för genomförande av återkommande riskanalyser och penetrationstester avseende kommunernas interna nätverks-infrastruktur.

Avslutning

Vi vill avslutningsvis ta tillfället i akt och tacka de personer som deltagit i intervjuer och bidragit med underlag till denna översyn för ett vänligt bemötande och ett gott samarbete.

Vid frågor om översynen kan Mikael Carinci eller Anders Gustafson kontaktas.

Stockholm, oktober 2017

Kontakt:

Mikael Carinci

E-post: mikael.carinci@pwc.com

Tel: 072 - 980 90 35

Anders Gustafson

E-post: anders.gustafson@pwc.com

Tel: 070 – 929 42 62

Bilagor

Bilaga 1
Intervjulista

Namn	Roll	Verksamhet
Anders Fredriksson	IT-säkerhetssamordnare	Knivsta kommun
Christina Björses	Samordnare IT	Heby kommun
Emma Burstedt	Kommunchef	Heby kommun
Karin Eljansbo	Administrativ chef	Heby kommun
Lars-Erik Andersson	IT-chef	Samverkansnämnden (Knivsta kommun & Heby kommun)
Lena Fransson	Kommundirektör	Knivsta kommun
Michael Von Essen	IT-driftschef	Samverkansnämnden (Knivsta kommun & Heby kommun)
Rojda Sjöö	Verksamhetsutvecklare	Knivsta kommun
Åsa Franzén	Kanslichef, Biträdande kommundirektör (GDPR)	Knivsta kommun
Åsa Johansson	Förvaltningschef, Vård och Omsorg	Heby kommun

Bilaga 2

Vad innebär en god informationssäkerhet och teknisk IT-säkerhet?

En god informationssäkerhet syftar till att säkra en effektiv informationsförsörjning och att undgå allvarlig fel som påverkar möjligheten att bedriva en ändamålsenlig verksamhet.

En ändamålsenlig informationssäkerhet innebär:

- Vidta preventiva åtgärder för att undvika att information kan förvanskas eller för att förhindra informationsläckage.
- Säkerställa att man alltid har tillgång till den information organisationen behöver för sin dagliga verksamhet, även om kris eller katastrof föreligger.
- Informationssäkerhetsnivån man är helt avhängig den riskaptit man har, samt den bedömda hotbilden.
- En organisation som hanterar mycket känslig information, exempelvis i form av personuppgifter i kundregister, lönelistor eller liknande, kan behöva mer skydd än en organisation som inte hanterar och lagrar liknande information.

En god teknisk IT-säkerhet innebär att organisationen har rutiner, processer och uppsatta kontrollpunkter som löpande följs upp och att organisationen har rutiner för att hålla sig uppdaterad kring omvärldshot och förändringar som kan påverka kritiska resurser.

En god teknisk IT-säkerhet innebär:

- att ha hög tillgänglighet till information och tjänster,
- att säkerställa informationens riktighet genom skydd mot oavsiktlig och avsiktlig förvanskning,
- att ha en behörighetskontroll baserad på klassificering av informationens känslighet, spårbarhet och konfidentialitet, samt möjlighet till skyddad kommunikation,
- ett aktivt arbete för att så tidigt som möjligt upptäcka och åtgärda intrångsförsök och identifiera eventuella sårbarheter i den interna och externa IT-miljön.