Nulägesanalys Informationssäkerhet i Alingsås kommun

Sammanfattning

Alingsås kommuns informations- och IT-säkerhetsarbete är eftersatt och behöver mer aktivt arbetas med. Information finns och hanteras i alla kommunens verksamheter, därtill hanteras stora mängder känslig och skyddsvärd information. Det är av vikt att information behandlas och skyddas på ett lämpligt och korrekt sätt.

Ansvaret för informationssäkerhet är kopplat till verksamhetsansvaret. Det betyder att varje person som är ansvarig för en verksamhet eller får ett delegerat verksamhetsansvar också är ansvarig för informationssäkerheten i denna verksamhet.

Digitalisering är en stor del av vår vardag, såväl privat som i arbetsliv. Alingsås kommun arbetar intensivt med att digitalisera och utveckla verksamheten. Möjligheterna är enorma med digitalisering och den alltmer utbredda användningen av digitala lösningar skapar nya möjligheter att utföra tjänster och dela information. Med dessa möjligheter följer också nya risker och hotbilder, exempelvis genom olika IT-angrepp och skadlig kod. Om kommunens information på något sätt förstörs, förändras eller läcker ut till obehörig genererar det troligtvis minskat förtroende för organisationen och i vissa fall även ekonomiska förluster. Exempel på bristande informationssäkerhetsarbete med tillhörande konsekvenser finns numer relativt gott om (ex Transportstyrelsen, 1177, Svenska kraftnät m.fl.)

Att aktivt jobba med information- och IT-säkerhet hjälper organisationen att hantera och förebygga de risker och ökade hotbilder som uppstår genom den

tekniska utvecklingen. Att ha god kännedom om den information som kommunen hanterar möjliggör och underlättar digitalisering. Verksamheten får då lättare att ställa krav på rätt skyddsnivåer, vilket skapar trygghet vid förändrade arbetssätt.

Arbetet med systematiskt information- och IT-säkerhet ska bedrivas i enlighet med standarder och metoder som finns (Ex ISO 27000-serien). Arbetet behöver bedrivas långsiktigt, först behöver de styrdokument som reglerar verksamheten revideras och aktualiseras. De styrdokument som avses är Policy för Informationssäkerhet och Riktlinjer för Informationssäkerhet.
En handlingsplan ska tas fram där olika insatser sätts in i ett tidsperspektiv(1-5 år). Handlingsplanen består av kortsiktiga mål (1-2 år) och långsiktiga mål (2-5 år) med tillhörande aktiviteter.

1. Bakgrund

Informationssäkerhet handlar om att skapa och upprätthålla lämpligt skydd av information. Ett bra informationssäkerhetsarbete är en förutsättning för effektiv och korrekt informationshantering. Detta skapar förtroende både inom och utanför organisationen.

Sveriges kommuner och landsting har prioriterat informationssäkerhetsområdet utifrån de stora mängder information som finns i kommuner och regioner. Hotbilden, kopplad till informationssäkerhet, har under de senaste åren ökat, exempelvis genom olika IT-angrepp och skadlig kod. Det påpekas att en verksamhets förmåga att hantera och skydda information på ett ändamålsenligt sätt behöver utvecklas i takt med omvärlden.

KPMG har, på uppdrag av dåvarande kommundirektör, genomfört en oberoende granskning av Information- och IT-säkerheten i Alingsås kommun. Granskningen färdigställdes den 6 mars 2018 och överlämnades till kommunen. I rapporten påpekades en rad brister kring både information- och IT-säkerhetsarbetet i kommunen. Några exempel på påpekande är att:

- Kommungemensamma styrdokument saknas eller är föråldrade.
- Organisationen saknar tillräckliga samordningsforum.
- Åtkomsthanteringen behöver stärkas.
- Kontinuitetsplaner behöver revideras och uppdateras.

Alingsås kommun har anslutit sig till VGR:s Informationssäkerhetsprogram 2020. Programmet syftar till att regionens kommuner ska ha infört ett ledningssystem, helt eller påbörjat, för informationssäkerhet(LIS) och genomfört ett systematiskt och likformat informationsklassificeringsarbete. I samarbete med högskolan i Skövde har en 7,5p-kurs i ämnet informationssäkerhet tagits fram, Alingsås kommun har en anställd som går kursen.

”Digital Målbild för Alingsås kommun – öppen och smart” antogs av kommunfullmäktige den 31 oktober 2018. Målbilden är ett styrande dokument som tillser att digitaliseringsprocessen sker i enlighet med Alingsås kommuns mål och vision. Målbilden för arbetet med digitalisering i Alingsås kommun konkretiseras och effektueras i styrdokumentet ”Handlingsplan Digital Målbild för Alingsås kommun – öppen och smart”. Handlingsplanen slår fast att informationsklassning ska genomföras och att en utveckling mot systematiskt informationsarbete ska påbörjas.

Informationssäkerhetsarbetet definieras enligt svensk standard ISO 27000-serien och innehåller en administrativ del samt en teknisk del. Kraven som ställs på information är tillgänglighet, riktighet, konfidentialitet och spårbarhet.

2. Syfte

Nulägesanalysen syftar till att kartlägga Alingsås kommuns status gällande informationssäkerhet. Analysen ska skapa insikt kring vad som eventuellt behöver göras och ge ett underlag för beslut om fortsättning.

3. Avgränsning

Nulägesanalys har genomförts på en kommunövergripande nivå.

4. Tillvägagångssätt

Nulägesanalysen utgörs av tre olika delar:

- Dokumentstudie - befintliga styrdokument har granskats.
- Enkät - en enkät med öppna frågor skickades ut till förvaltningschefer.
- GAP - analys- en GAP-analys är genomförd baserad på intervjuer.

Därtill har KPMG:s rapport ”Granskning av IT- och informationssäkerhet Alingsås kommun” inkluderats i arbetet med att ta fram en lägesbild.

5. Resultat

5.1 Dokumentstudie

Granskade dokument redovisas i bilaga 1. Utifrån dokumentstudien av kommunens befintliga styrdokument rörande informationssäkerhet framkommer att dokumenten behöver aktualiseras. Dokumenten har inte reviderats och uppdaterats i takt med kommunens systembyten och organisatoriska förändringar. Dock ska påpekas att dokumenten mycket väl kan fungera som grund för framtida versioner.

5.2 Enkät

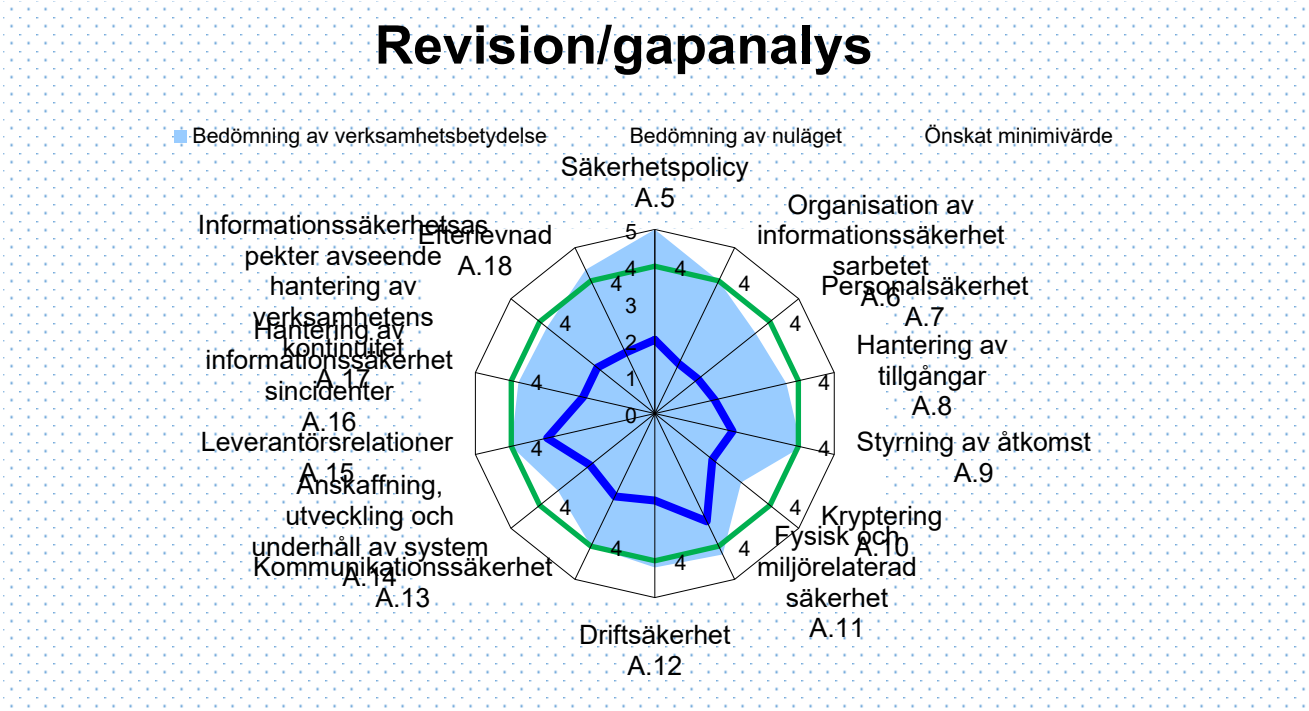
En enkät gällande informationssäkerhet skickades innan sommaren ut till förvaltningschefer. Samtliga förvaltningar har svarat och resultatet presenteras i bilaga 2. Enkäten utgjordes av öppna frågor varför svaren inte redogörs för i sin helhet utan genom en sammanfattning.

Syftet med enkäten var att bredda bilden kring statusen på informationssäkerhetsarbetet i organisationen. Av enkätsvaren framgår att informationssäkerhet är ett känt begrepp i organisationen men att arbetet med

frågan sker i varierande grad. De största bristerna som identifierats genom enkäten är avsaknad av dokumentation, avsaknad av organisation gällande informationssäkerhet, avsaknad av informationsklassning och avsaknad av uppföljning. Positivt är att de flesta anger att de har utsedda systemansvariga.

5.3 Gapanalys

Nulägesanalysen baserat på gapanalys ISO27002:2017 ger vid handen att det största gapet, med hänsyn till verksamhetsbetydelsen, återfinns inom säkerhetspolicy (A.5), organisation av informationssäkerhetsarbetet (A.6), personalsäkerhet (A.7), hantering av tillgångar (A.8) och efterlevnad (A.18).



5.4 Sammanfattning och slutsats av resultat

Resultatet gör inte anspråk på att vara heltäckande i var del av kommunens olika verksamheter utan påvisar generell status. Det är möjligt, till och med troligt, att det finns spetskompetens ute i förvaltningarna.

Resultatet påvisar ändå ett behov av att lyfta upp ämnesområdet informationssäkerhet för att säkerställa och dokumentera att kommunen vidtar administrativa och tekniska åtgärder för att skydda information. Detta är en förväntad status nationellt, vilket SKL har uppmärksammat och påvisat behov av förbättring i kommunerna.

Resultatet av dokumentstudie, enkätundersökning och GAP-analys är relativt lika, utkomsten av respektive datainsamling ger liknande förbättringsområden. Genomgående framgår att:

- Aktuella styrdokument behöver revideras och nya behöver skapas.
- Roller och ansvar behöver klargöras.
- Informationsklassning behöver ske i högre utsträckning.
- Kontinuitetsplanering behöver tas fram/revideras.
- Behörighetsstyrning behöver förbättras.
- Uppföljning för efterlevnad behöver öka.
- Anställdas medvetenhet om informationssäkerhet behöver öka.

6. Rekommendation av framtida arbete

Arbetet med systematiskt information- och IT-säkerhet ska bedrivas i enlighet med standarder och metoder som finns (ISO 27000-serien). Arbetet behöver bedrivas långsiktigt, först behöver de styrdokument som reglerar verksamheten revideras och aktualiseras. De styrdokument som avses är Policy för Informationssäkerhet och Riktlinjer för Informationssäkerhet.
En handlingsplan ska tas fram olika insatser sätts in i ett tidsperspektiv(1-5 år). Handlingsplanen består av kortsiktiga mål (1-2 år) och långsiktiga mål (2-5 år) med tillhörande aktiviteter.

Bilaga 1

Dokumentstudie

Lista över befintliga och granskade dokument:

-IT-policy för Alingsås kommun

-IT-säkerhetsinstruktion Förvaltning

-IT-säkerhetsinstruktion Drift

-IT- och informationssäkerhetsinstruktion för personal i Alingsås kommun

Granskning av dokument består av följande:

-Tid - När gäller styrdokumentet

- Ansvar - Vem ansvarar för dokumentet

- Aktualitet - Hur aktuellt är innehållet, hur giltigt är innehållet, är innehållet anpassat till aktuell lagstiftning/aktuell teknik?

-Relevans- Hur aktuellt och relevant är dokumentet idag?

IT-policy för Alingsås kommun

Tid: Fastställd av kommunfullmäktige 2 september 2009, § 152.

Ansvar: Fullmäktige

Aktualitet: Finns inget slutdatum för giltigheten och någon revidering har inte gjorts.

Innehåll: Policyn definierar övergripande mål, ansvarsfördelning, kostnadsfördelning och säkerhet gällande IT-frågor. Definierar att IT-säkerhetsarbetet ska bedrivas så det blir en integrerad del av den kommunala verksamheten. Tydliggör att systemsäkerhetsplaner ska finnas för kommunens viktigaste system och ska revideras årligen.

Relevans: *Dokumentet bedöms kunna utgöra en grund för en mer aktuell version.*

IT-säkerhetsinstruktion Förvaltning

Tid: Fastställd av kommunstyrelsen 15 oktober 2007, § 236.

Ansvar: Kommunstyrelsen

Aktualitet: Finns inget slutdatum för giltigheten och någon revidering har inte gjorts.

Innehåll: Dokumentet reglerar den interna organisationen för IT-säkerhetsarbetet, ansvar för IT-säkerhetsarbetet, hur arbetet ska bedrivas. Att systemägaren ansvarar för att utarbeta ett IT-program, avtal mot IT-chef med

SLA samt upprätta systemsäkerhetsplaner. Vidare att IT-chef, systemägare för IT-infrastruktur ansvarar för att systemsäkerhetsplan för IT teknisk infra upprättas. Rollen IT-säkerhetssamordnare stödjer arbetet med IT-säkerheten. Rutin för behörighetsadministration definieras generellt, systemförvaltare handlägger respektive system. Årlig revidering av användare ska utföras. Säkerhetskopiering och lagring utförs enligt krav från systemsäkerhetsplaner.

Relevans: *Dokumentet bedöms kunna utgöra en grund för en mer aktuell version.*

IT-säkerhetsinstruktion Drift

Tid: Fastställd av kommunstyrelsen 4 juni 2007, § 164.

Ansvar: Kommunstyrelsen

Aktualitet: Finns inget slutdatum för giltigheten och någon revidering har inte gjorts.

Innehåll: Dokumentet reglerar incidenthantering, säkerhetskopiering och lagring och kontinuitetsplanering.

Relevans: *Dokumentet bedöms kunna utgöra en grund för en mer aktuell version.*

IT- och informationssäkerhet - Instruktion för användare

Tid: Fastställd av kommundirektör 5 december 2019

Ansvar: Ansvaret delegerat till kommundirektör

Aktualitet: Finns inget slutdatum för giltigheten.

Innehåll: Dokumentet vänder sig till anställda i Alingsås kommun. Innehåller information om informationssäkerhet och vilka lagar som styr. Reglerar bland annat hantering av e-post, lagring av information, behörigheter, användning av mobila enheter m.m.

Relevans: *Dokumentet bedöms vara aktuellt och uppdaterat.*

Bilaga 2

Enkätfrågor ställd till förvaltningschefer med sammanfattade svar

1. *-Bedömer du att din förvaltning arbetar aktivt med informationssäkerhet? Om ja, beskriv hur*.

I varierande grad bedömer förvaltningarna att de arbetar med informationssäkerhet. I merparten av svaren framgår att ämnet informationssäkerhet är känt ute i organisationen men att det inte sker något sammanhängande informationssäkerhetsarbete på förvaltningsnivå.

2. *-Finns det en eller flera personer som fått i ansvar att arbeta med informationssäkerhet? Om ja, vilka?*

Merparten av förvaltningarna har ingen utpekad person som jobbar med informationssäkerhet, socialförvaltningen undantaget.

3. *-Finns det lokalt framtagna styrdokument rörande informationssäkerhet?*

Det redogörs för att i vissa fall finns lokala rutiner och andra dokument som reglerar informationssäkerhetsarbetet. Något kommunövergripande styrdokument är inte känt.

4. *-Genomförs informationsklassning på era verksamhetskritiska system och processer? Om ja, hur sker dokumentation*

Det sker ingen sammanhållen informationsklassning på respektive förvaltning, i vissa fall görs det till viss del.

5. *-Genomförs risk- och sårbarhetsanalyser på era verksamhetskritiska system och processer? Om ja, hur sker dokumentation?*

Risk- och sårbarhetsanalyser genomförs till viss del, några förvaltningar jobbar aktivt med detta medans andra inte gör det alls.

6. -Finns det aktuella kontuinitetsplaner för era verksamhetskritiska system och processer? Om ja, när uppdaterades dessa senast?

Till viss del finns kontinuitetsplaner men flera förvaltningar saknar helt kontinuitetsplaner. De som finns är i de flesta fall gamla och behöver aktualiseras.

7. *Finns det utpekad systemansvarig för de system ni är ansvariga för?*

Det finns utpekade systemansvariga på de flesta förvaltningar.

8. *Finns det rutiner kring åtkomsthantering(behörigheter)? Om ja, beskriv hur.*

Rutiner för åtkomsthantering är vanligt förekommande i verksamheter som hanterar känslig information, i något fall saknas dokumentation.

9. *Sker någon uppföljning av informationssäkerhetsarbetet? Om ja, beskriv hur.*

Uppföljning av informationssäkerhetsarbetet är inte vanligt förekommande, vissa delar följs upp men inte på något övergripande sätt.