BROMÖLLA KOMMUN
REVISIONEN

Bromölla den 23 juni 2021

Kommunstyrelsen för svar
Kommunfullmäktige för kännedom

Missiv – Granskning informationssäkerhet

Revisorernas uppdrag av fullmäktige

Revisorerna har fått i uppdrag av fullmäktige att följa upp om verksamheten är ändamålsenlig samt pröva om den interna kontrollen är tillräcklig.

Metod och revisionskriterier

Granskningen har genomförts genom dokumentstudier och intervjuer med: Kommunchef, Säkerhets- och beredskapsansvarig, Kommunikatör, IT-chef (kommunalförbund), IT-strateg (kommunalförbund) och IT-samordnare stöd och omsorg. Samtliga intervjupersoner har erbjudits att faktagranska rapporten.

Granskningen har utgått ifrån om rutinerna uppfyller:

- Kommunallagen 6 kap. 6 §
- MSB:s rekommendationer avseende Ledningssystem för informationssäkerhet
- NIS-direktivet (MSB, Nätverk och InformationsSystem) kartläggning/analys av risker
- Tillämpbara interna regelverk, policys och beslut

Bakgrund

Organisationer i offentlig sektor hanterar ovärderlig information i sina informationssystem. Informationssäkerhet innebär att skydda denna information mot obehörig åtkomst så att vidtagna IT-säkerhetsåtgärderna därefter kan stå i relation till informationstillgångarnas värde, risker och behov.

Ny teknik innebär nya möjligheter men även nya risker som ställer krav på ett fungerande säkerhetsarbete. 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. Brister i hanteringen kan leda till såväl förtroendeskada som ekonomisk skada för organisationen.

För att kunna hantera detta på ett ändamålsenligt sätt krävs att kommunen har ett systematiskt informationssäkerhetsarbete där flera funktioner i kommunen är involverade och rätt organiserade för uppdraget.

Revisorerna i kommunalförbundet (SBKF) har i en tidigare revisionsrapport *Granskning av styrning och ledning av IT-leverans* (2020-02-27), bland annat skrivit att granskningen i förbundet visar vad gäller kontrollmålen på att direktionen inte har ställt krav på kommunen av en tydligare styrning av informationssäkerheten.

Sakkunnigas sammanfattning av genomförd granskning

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

Vi baserar vår bedömning bland annat på följande iakttagelser:

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

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

Revisorerna bedömer och önskar svar

Revisorerna konstaterar i en samlad bedömning att:

- förvaltningen inte uppfyller MSB rekommendationer och direktiv
- informationssäkerheten inte är ändamålsenlig
- den interna kontrollen av informationssäkerheten inte är tillräcklig
- det finns risker för såväl framtida förtroendeskada som ekonomisk skada
- det saknas ett systematiskt informationssäkerhetsarbete i förvaltningen

Revisorerna önskar kommunstyrelsens skriftliga svar senast den 5 september på de rekommendationer som sakkunniga framställt i granskningsrapporten.

På uppdrag av revisionen

Joachim Bengtsson
Ordförande