Huddinge kommun
Kommunrevisorer
Eva-Li Prades Eriksson
Ulrika Wennberg
Lars Blomkvist
Marianne Broman
Fredrik Fischer
Elsa Johansson

Till:
Kommunstyrelsen

För kännedom:
Kommunfullmäktige

2020-12-14

Revisionsrapport: Granskning av informationssäkerhet

Vi har av revisorerna i Huddinge kommun fått i uppdrag att översiktligt granska kommunens rutiner kring informationssäkerhet. Uppdraget ingår i revisionsplanen för år 2020.

Informationssäkerhet är ett begrepp som används om säkerhet för information som hanteras i kommunens IT-system. Allt mer information hanteras idag med olika tekniska lösningar och aldrig förr har offentlig sektor hanterat sådana mängder information som görs idag. Verksamheternas ökade beroende av informationsteknik (IT) innebär ökade risker i form av dataintrång, bedrägerier och spridning av skadlig kod.

Granskningen har syftat till att bedöma om kommunen har ett ändamålsenligt och systematiskt arbetssätt med informationssäkerhet.

Vår sammanfattade bedömning utifrån granskningens syfte är att kommunstyrelsen inte har ett ändamålsenligt och systematiskt arbetssätt avseende informationssäkerhet. Vår bedömning bygger på följande:

- Den organisation som finns är ändamålsenlig men begränsad i sin omfattning. Dessutom finns det otydligheter kring roller och ansvarsfördelning, dels mellan kommunstyrelsens förvaltning och verksamhetsförvaltningarna dels mellan kommunstyrelsens förvaltnings funktioner som är uppdelade på olika sektioner och avdelningar.
- Det finns ett systematiskt och ändamålsenligt arbetssätt dokumenterat genom kommunens styrdokument som behandlar informationssäkerhet. Dock bedömer vi detta arbetssätt inte vara förankrat i kommunens verksamheter.
- Det finns en ansvars- och rollfördelning mellan verksamheterna och den centrala förvaltningen. Dock framstår denna som inte helt tydlig och det framgår av intervjuerna att verksamheterna inte alltid vet vad som förväntas av dem och vilket stöd de kan få. Fördelningen mellan kommunstyrelsens förvaltnings olika sektioner och avdelningar fungerar bra internt, men uppfattas som otydlig ut mot resten av den kommunala organisationen.
- Det huvudsakliga ansvaret för riskidentifiering och riskanalys återfinns hos verksamheterna. Där saknas dock i dagsläget kompetens för att genomföra ändamålsenlig identifiering och analys.
- Verksamheterna identifierar sårbarheter och åtgärder inom ramarna för internkontrollplanen och uppföljningen av systemsäkerhetsanalyser. Dock framkommer det av intervjuerna att sårbarheterna och åtgärderna ofta återkommer vid upprepade tillfällen. Verksamheterna saknar stöd och resurser för att bedriva detta arbete på ett tillfredställande sätt.

Utifrån granskningens resultat rekommenderar vi kommunstyrelsen att:

- Implementera en informationssäkerhetspolicy.
- Implementera en obligatorisk utbildning om informationssäkerhet med kontinuerliga och regelbundna uppföljningsutbildningar.
- Implementera en systematisk och regelbunden rapportering och uppföljning av informationssäkerhetsarbetet till kommunledningen och kommunstyrelsen.

Bilaga: Revisionsrapport: *Granskning av informationssäkerhet*

- Säkerställa att alla verksamheter har tillgång och kännedom om de styrdokument som gäller för verksamheten, samt vilka ansvarsförhållanden som gäller.
- Säkerställa att informationssäkerhetsorganisationen har en tillräcklig omfattning för att möta kommunens behov.
- Ser över möjligheten att implementera nya rutiner för att säkerställa att anställda har rätt behörigheter.
- Implementera en rutin för rapportering av informationssäkerhetsincidenter i ett avvikelserapporteringssystem.
- Säkerställa att det finns en ändamålsenlig organisation för rapportering av incidenter enligt NIS-direktivet.

Revisorerna beslutar att överlämna rapporten till kommunstyrelsen för yttrande senast den 1 april 2021 och för kännedom till kommunfullmäktige.

Eva-Li Prades Eriksson
Ordförande

Ulrika Wennberg
Vice ordförande

Lars Blomkvist

Marianne Broman

Fredrik Fischer

Elsa Johansson

Bilaga: Revisionsrapport: *Granskning av informationssäkerhet*