Revisorerna i Huddinge kommun
Revisionsgrupp 1
Eva-Li Prades Eriksson
Lars Blomkvist
Åke Wickberg
Fredrik Fischer
Elsa Johansson

Till:
Kommunstyrelsen

För kännedom:
Kommunfullmäktige

2022-11-28

Revisionsrapport: Granskning av IT-säkerhet och uppföljning av kommunens informationssäkerhetsarbete

KPMG har av Huddinge kommuns revisorer fått i uppdrag att granska om kommunstyrelsen säkerställer att kommunen har en tillräcklig styrning och intern kontroll vad gäller IT-säkerhet. Uppdraget ingår i revisionsplanen för år 2022. Syftet med granskningen har varit att bedöma om kommunstyrelsen säkerställer att kommunen har en tillräcklig styrning och intern kontroll för sin IT-säkerhet och i samband med granskningen följa upp om de rekommendationer som lämnades i granskningen för 2020 är åtgärdade.

Den sammanfattande bedömningen utifrån granskningens syfte är att kommunstyrelsen inte har säkerställt att kommunen har en tillräcklig styrning och intern kontroll vad gäller IT-säkerheten. Ett flertal av de rekommendationer som lämnades i tidigare granskning har inte åtgärdats. Det bedöms att flertalet av dessa även i vissa delar påverkar förutsättningarna för en god IT-säkerhet.

I avsaknad av beskrivningar av ansvarsförhållanden inom informationssäkerhet avseende den tekniska säkerheten går det i nuläget inte att bedöma om organisationen är ändamålsenlig. Noteras att roller är otydliga och ansvar behöver tydliggöras på olika nivåer avseende informationssäkerhetsarbetet, inklusive den tekniska säkerheten. De nu gällande styrdokumenten saknar hierarkisk ordning och utgör inte en sammanhållen helhet. De är i delar föråldrade och därigenom saknas angivelser till nya lagar, exempelvis GDPR och NIS-direktivet, som hör till informationssäkerhetsarbetet.

Säkerhetsåtgärder vidtas som ett resultat av informationsklassningar. Dessa genomförs emellertid inte med utgångspunkt ifrån verksamhetens egna bedömningar sett till informationens skyddsvärde. Modellen för informationsklassning är därtill att betrakta som föråldrad. Inom IT-avdelningen sker en verksamhetsnära uppföljning av de tekniska säkerhetsåtgärder som är vidtagna. Uppföljning av IT-säkerhetsarbetet på en övergripande nivå, tillika rapportering till kommunstyrelsen är emellertid att betrakta som otillräcklig.

Kommunens IT-avdelning har vissa tekniska verktyg som möjliggör övervakning för att ha en förmåga att upptäcka hot om intrång eller andra incidenter. Det finns en medvetenhet om försök till intrång och kommunen har med hjälp av övervakningsverktyg och övriga säkerhetsåtgärder kunnat stå emot intrångsförsök utan att det hittills har lett till allvarlig konsekvens för verksamheten. Det finns en etablerad organisation och rutiner för att hantera incidenter inom IT-avdelningen men det uppfattas att det finns behov av att tydliggöra incidenthantering generellt i kommunens verksamheter. Kontinuitetsplaner som kan utgöra stöd vid allvarligare störningar finns till viss del i kommunens verksamheter, de planer som finns har dock endast testats i begränsad omfattning.

Efter den senare tidens uppmärksammade attacker mot kommuner runt om i Sverige har information efterfrågats av kommunstyrelsen och kommunledningen. Dock konstateras att den information som rapporterats inte har lett till beslut om särskilda åtgärder för verksamheten att verkställa.

Utifrån uppföljning av tidigare genomförd granskning av informationssäkerhet kvarstår följande rekommendationer till kommunstyrelsen:

- Implementera en informationssäkerhetspolicy.

Bilaga: Revisionsrapport: *Granskning av IT-säkerhet och uppföljning kommunens informationssäkerhetsarbete*

- 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.
- 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.

Utifrån bedömning och slutsats i den fördjupade granskningen av IT-säkerhet rekommenderas kommunstyrelsen att:

- Revidera riktlinjer för informationssäkerhet avseende ansvar för den tekniska säkerheten.
- Se över vilka ytterligare instruktioner och anvisningar som det finns behov av för att etablera en styrning av informations-säkerhetsarbetet.
- Fastställa en ny och uppdaterad modell för riskanalys och informationsklassning.
- Stärka verksamheternas roll i bedömningen av informations skyddsvärde.
- Tillse att de beslut om riskreducerande åtgärder i internkontrollen verkställs och att uppföljning sker av att åtgärder lett till minimerad risk.
- Att genomföra penetrationstester av IT-miljön.
- Fastställa kommunövergripande incidenthanteringsrutiner som tillämpas av alla verksamheter. Samt tillse att nämnder upprättar kompletterande incidenthanteringsrutiner utifrån verksamhetsspecifika krav och lagar.
- Utvärdera befintliga kontinuitetsplaner samt införa tester av de planer som finns för att säkerställa att underlag skulle fungera vid särskilda händelser.

Vi vill poängtera vikten av att rekommendationer åtgärdas. Vi kommer att följa upp granskningens slutsats och rekommendationer i vår revisionsplanering framåt.

Vi beslutar att överlämna rapporten till kommunstyrelsen för yttrande senast den 31 mars 2023 och för kännedom till kommunfullmäktige. Yttrande skickas till ordförande i revisionen Eva-Li.Prades-Eriksson@huddinge.se och Pekka.Poljo@huddinge.se .

.

Eva-Li Prades Eriksson
Ordförande

Lars Blomkvist
Vice ordförande

Åke Wickberg

Elsa Johansson

Fredrik Fischer

Bilaga: Revisionsrapport: *Granskning av IT-säkerhet och uppföljning kommunens informationssäkerhetsarbete*