Revisorerna i Sundbyberg
12/2019

Stadsmiljö- och tekniska nämndens svar på revisionsrapport - Granskning av stadens arbete med informationssäkerhet med fokus på styrning, organisation och incidenthantering

Stadsmiljö- och tekniska nämnden svarar på remissen utifrån sitt ansvarsområde ”ansvara för och förvalta IT-infrastruktur”. Nämnden kommer att bistå kommunstyrelsen i arbetet i enlighet med rekommendationerna.

Rekommendation 4: Otydlig ansvarsfördelning mellan säkerhetsavdelningen och IT-enheten i arbetet med informationssäkerhet.
Nämnden instämmer i revisorernas bedömning att det saknas en tydlig dokumenterad ansvarsfördelning mellan trygghets- och säkerhetsavdelningen och enheten för digitalisering och service. De berörda enheterna är dock överens om att trygghets- och säkerhetsavdelningen ska vara kravställare och enheten för digitalisering och service ska vara rådgivande samt genomföra de systemändringar som kan bli nödvändiga. Utifrån ansvarsfördelningen kommer regelbundna samverkansmöten för fortlöpande arbete samt uppföljning att genomföras.

Rekommendation 7: Avsaknad av övergripande och formaliserad process för åtkomsthantering och Rekommendation 8: Brist på anvisningar för periodiska genomgångar och ändamålsenlig ansvarsfördelning
Nämnden ställer sig bakom ett gemensamt arbete med en stadsövergripande process för åtkomsthantering som även inkluderar periodiska genomgångar. I dagsläget är användar- och behörighetshantering till stadens IT-miljö standardiserad. Information hämtas automatiskt dagligen från personalsystemet, vilket medför att användarkonton är ständigt är uppdaterade under förutsättning att rätt information finns i personalsystemet. Ansvaret för verksamhetssystem ligger enligt stadens systemförvaltarmodell på verksamheterna. I många fall sker tilldelning och borttagning manuellt direkt i verksamhetssystemen. Nämnden anser att en gemensam process tillsammans med en matris kopplad till kritiska IT-system skulle höja IT-säkerheten i staden.

Rekommendation 9: Begränsade definierade rutiner, roller och ansvar för hantering av kritiska incidenter

Nämnden delar revisorernas bedömning att tydligheten kring incidentrapportering behöver öka. I dag skrivs IT- incidentrapporter, större IT-incidenter rapporteras även till Myndigheten för samhällsskydd- och beredskap. Som en del av stadens övriga incidenthanteringsprocess ska processflödet för hantering av kritiska incidenter, inklusive roller, ansvar och rapporteringskrav gemensamt definieras och tydliggöras.

Rekommendation 10: Avsaknad av formaliserad process för programförändringar

Nämnden instämmer i revisorernas bedömning och har därför redan påbörjat arbetet med en formaliserad process gällande hantering av programförändring. Processen har också utökats till att även gälla ändringar i såväl system som stadens IT-miljö som helhet, en så kallad ändringsprocess.

Rekommendation 12: Brist på uppföljning av kontinuitetsplaner för skyddsvärda verksamhetssystem

Nämnden instämmer i revisorernas bedömning. Enheten för digitalisering och service leder sedan försommaren 2019 ett arbete med att identifiera stadens kritiska verksamhetssystem tillsammans med trygghets- och säkerhetsavdelningen. När modellen för att identifiera dessa är fastställd ska samtliga identifierade system grundligt informationsklassificeras och därefter ska det för varje system upprättas kontinuitetsplaner som löpande följs upp och testas.

På stadsmiljö- och tekniska nämndens vägnar

Stefan Bergström (C)
Ordförande i stadsmiljö- och tekniska nämnden