Granskning av IT- och informationssäkerhet

EY har på uppdrag av de förtroendevalda revisorerna i Trollhättans Stad granskat stadens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att bedöma om styrningen och arbetet med IT-och informationssäkerhet bedrivs på ett ändamålsenligt sätt samt om den interna kontrollen är tillräcklig inom området. Granskningen har också följt upp hur staden har åtgärdat de iakttagelser som framkom i Cybersäkerhetsgranskningen under 2017. Granskningen har även inkluderat en jämförelse mot andra kommuners mognadsgrad inom IT- och informationssäkerhet.

Resultat | De tre högst prioriterade iakttagelserna

Granskningen berörde ett antal områden. Nedan listas de viktigaste resultaten från granskningen:

- Trollhättans Stad bedriver ett arbete med att ta fram samt förbättra styrande dokument för stadens arbete avseende IT- och informationssäkerhet. Vid tid för granskning är vissa styrdokument inte ändamålsenliga. Styrdokument för vissa områden saknas.
- Staden har genomfört utbildningar avseende informationssäkerhet och dataskydd, men utbildningar har inte genomförts regelbundet. Avsikten är att fullfölja en upprättad utbildningsplan avseende informationssäkerhet samt genomföra årliga utbildningar inom dataskydd.
- Internkontroll avseende informationssäkerhet genomförs årligen. Uppföljningsarbetet är däremot inte heltäckande då det inte genomförs uppföljning av samtliga områden inom stadens IT- och informationssäkerhetsarbete.

Slutsats | Rekommendationer

Utifrån genomförd granskning rekommenderar vi att Trollhättans Stad arbetar vidare med att:

- Färdigställa och implementera de styrdokument avseende IT- och informationssäkerhet som är under förbättring, samt upprätta de styrdokument som saknas vid tid för granskning.
- Fullfölja den upprättade utbildningsplanen avseende informationssäkerhet, fastställa utbildningsplan avseende dataskydd samt tillse att utbildningsplanerna är tillräckligt robusta för att kunna genomföras även vid oförväntade händelser.
- Tillse att samtliga områden inom stadens IT- och informationssäkerhetsarbete följs upp på en regelbunden basis, samt kontinuerligt rapporteras till kommunstyrelsen.
- Informationssäkerhetskrav på leverantörer följs upp genom att upprätta en gemensam rutin avseende uppföljning av leverantörsavtal.
- Definiera informationssäkerhetsincident samt kommunicera definitionen till berörda parter i verksamheten.
- Upprätta centrala riktlinjer för behörighetshantering och förändringshantering för att säkerställa att samma process gäller för samtliga stadens nämnder och system.
- Tillse att lösenordsinställningarna för samtliga av stadens IT-system lever upp till kraven i lösenordspolicyn.

Slutsats | Samlad bedömning

- Den sammanfattade bedömningen är att Trollhättans Stad bedriver arbetet med IT- och informationssäkerhet på ett delvis ändamålsenligt sätt.
- Trollhättans Stad bedöms ha en något högre mognadsgrad än genomsnittet för jämförbara kommuner. Mognadsgraden är något högre än genomsnittet inom styrning och personuppgiftshantering och något lägre än genomsnittet inom drift.
- Trollhättans Stad har följt upp och åtgärdat iakttagelser och rekommendationer från 2017 års granskning av IT-säkerheten väl.