Kommunrevisorerna informerar

Granskning av IT- och informationssäkerhet

EY har, på uppdrag av de förtroendevalda revisorerna i Umeå, genomfört en granskning av IT- och informationssäkerhet vad gäller policyer, riktlinjer och hantering av säkerhetsfrågor på övergripande nivå i kommunen samt specifikt för två verksamhetskritiska system och hantering av molntjänster. Syftet med granskningen har varit att se på vilket sätt kommunen jobbar för att upprätta en god IT-säkerhet. Granskningen har gjorts mot utvalda delar av Myndigheten för samhällsskydd och beredskaps ramverk för informationssäkerhet, BITS.

Granskningen har visat att Umeå kommun har goda förutsättningar för ett effektivt och ändamålsenligt arbete med informationssäkerhet. Kommunen har interna regelverk och processer som verkar för god säkerhet. Förbättringsområden har identifierats främst inom hantering av tillgångar, styrning av åtkomst, kontinuitetsplanering i verksamheten, efterlevnad och hantering av molntjänster.

Nedan listas våra mest väsentliga rekommendationer. Samtliga rekommendationer återfinns i granskningsrapporten:

- Kommunen har inte genomfört systemsäkerhetsanalys eller klassificering av informationssystem, och dess längsta acceptabla tid för avbrott har ej fastställts. Detta kan innebära problem att prioritera system vid ett avbrott samt en risk att säkerheten ej är tillräcklig då säkerhetskrav inte analyserats. Kommunen bör påbörja ett arbete med att klassificera informationssystem avseende hur kritiska de är samt genomföra systemsäkerhetsanalys för de system som anses kritiska.
- Penetrationstester genomförs inte regelbundet, vilket medför en risk att IT-miljön inte följer satta säkerhetskrav samt att brister inte upptäcks. Kommunen bör periodiskt genomföra penetrationstester.
- Ett antal brister har identifierats i kommunens avtal med leverantörer, vilket kan innebära en risk för att kommunen inte lever upp till gällande lagstiftning, säkerhetsbrister, samt att kommunen tappar kontroll över sin information. Kommunen bör alltid reglera ansvar för informationssäkerhet och informationshantering i avtal med tredjepart.
- Kommunen har inte heller någon rutin för hur leverantörers tjänster följs upp, vilket medför en risk att leverantörer inte lever upp till avtalade nivåer av exempelvis säkerhet och driftstillgänglighet. Kommunen bör införa en rutin för uppföljning av utomstående leverantörer.
- Kommunen har inga formella rutiner för tilldelning av tredjeparts åtkomst till information eller informationssystem, vilket medför en risk att beslut avseende tilldelandet av behörigheter till kommunens system inte utförs på ett kontrollerat och spårbart sätt. Kommunen bör ta fram formella riktlinjer för hur tredjeparts åtkomst/tillträde till information eller informationssystem ska hanteras och dokumenteras.

Av samtliga 71 granskningspunkter är fördelningen av bedömningarna följande:

Kontrollen finns och fungerar tillfredsställande:	66,2%
Kontrollen finns och fungerar delvis:	11,3%
Kontrollen finns ej eller fungerar ej tillfredsställande:	21,1%
Ej tillämplig, kontrollen behövs ej av särskilda skäl:	1,4%

EY:s rapport *”Granskning av IT- och informationssäkerhet” 2015-06-16.*

För ytterligare information, kontakta: Revisionens ordförande Johnny Sandström, tel 070-677 34 89