För yttrande till
Kommunstyrelsen

För kännedom till
Kommunfullmäktige

Granskning av kommunens informationssäkerhetsarbete i praktiken

Lunds kommuns förtroendevalda revisorer har granskat kommunstyrelsen för att bedöma om det finns brister i det praktiska arbetet med IT- och informationssäkerhet. Revisorernas fråga är: finns det risk att en angripare har möjlighet att komma åt kommunens IT-miljöer genom angrepp via e-post? Svaret är ja. Risken är stor och den sammanfattande bedömningen är att arbetet med informationssäkerhet inom kommunen snarast behöver stärkas.

I granskningen genomfördes en simulerad phishingattack för att få information om kunskap och förmåga hos kommunens anställda att hantera ett cyberangrepp. Genom simuleringen kunde revisorerna ta reda på hur många av mottagarna som klickade på länken i det falska e-postmeddelandet och därefter uppgav användarinformation på den förfalskade landningssidan. Därefter utvärderades medvetenheten och kunskapen kring informationssäkerhet genom en enkät som distribuerades efter genomförd övning. Vidare har även dokumentation kring rapporteringsvägar granskats och kontrollerats.

Baserat på genomförd granskning bedöms Lunds kommun ligga på en nivå klart under det revisorerna anser att man kan kräva av kommunen. Bedömningen baseras på den typ av verksamhet som bedrivs samt på känslighetsgraden av den informationen, exempelvis personuppgifter, som kommunen behandlar i sin dagliga verksamhet. Endast miljönämndens förvaltning avviker positivt i sitt resultat.

Revisorerna bedömer vidare att Lunds kommun löper en mycket hög risk att en angripare lyckas fullfölja en så kallad phishingattack. Det finns ett behov av att förbättra utbildning och medvetenhet kring IT- och informationssäkerhet. En stor andel medarbetare är inte medvetna om hotet från en phishingattack, samt saknar kunskapen att kunna identifiera ett falskt e-postmeddelande. Resultaten visar också att det finns brister i kommunens rutiner för rapportering av säkerhetsincidenter vid en phishingattack. Rapporteringsvägarna är inte väl dokumenterade och har inte heller kommunicerats på ett tydligt sätt till alla medarbetare inom kommunen.

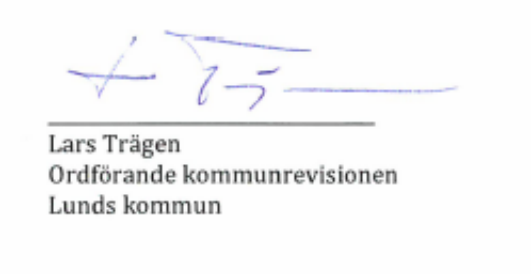
Postadress Box 41 221 00 Lund
Besöksadress Stora Södergatan 47
Telefon växel 046-359 50 00
Internetadress www.lund.se
e-post kommunrevisionen@lund.se

Utifrån granskningsresultatet rekommenderar vi kommunstyrelsen att:

- Snarast stärka informationssäkerheten inom kommunen.
- Utveckla ett strukturerat och regelbundet arbete med utbildningar i informationssäkerhet, särskilt fokuserat på de delar av organisationen som kan vara målgrupper för phishingattacker.
- Genomföra både teoretiska och praktiska övningar inom phishing. Praktiska övningar syftar till att testa kunskapen som behandlats under de teoretiska tillfällena, t.ex. att identifiera ett falskt e-postmeddelande, avsändare eller domän.
- Tydliggöra sina befintliga rapporteringsvägar, säkerställa att dessa är väl kända och tillgängliga för alla medarbetare, samt kommunicera vikten av att samtliga medarbetare rapporterar säkerhetsincidenter.

Revisorerna önskar svar på vilka åtgärder som kommer att vidtas med anledning av vad som framkommit i granskningen och de rekommendationer som lämnas. Svar önskas senast den 31 januari 2022.

På uppdrag av Lunds kommuns revisorer



Lars Trägen
Ordförande kommunrevisionen
Lunds kommun