Handläggare
Kommunstyrelseförvaltningen
Rikard Bauman
Informationssäkerhetssamordnare

rikard.bauman@tyreso.se

Handlingstyp
Tjänsteskrivelse

Sida
1 (3)

Datum
2023-11-08

Diarienummer
2023/KS 0429

Mottagare
Kommunledningsutskottet

Svar på revisionsskrivelse om granskning av informationssäkerhet i praktiken

Kommunstyrelseförvaltningens förslag till kommunledningsutskottet för beslut kommunstyrelsen

- - Kommunstyrelseförvaltningens skrivelse antas som kommunstyrelsens svar på revisionsrapporten av informationssäkerhet i praktiken.

Cynthia Runefjärd
Kommundirektör

Elin Waltersson
Chef stöd- och servicekontoret

Sammanfattning

EY har på uppdrag av de förtroendevalda revisorerna i Tyresö kommun genomfört en granskning av det praktiska arbetet inom IT-och informationssäkerhet i organisationen. Granskningen genomfördes genom att testa medarbetarnas kunskaper och genom att simulera en cyberattack. Resultatet visade på att det finns brister i kunskap och medvetenhet inom området informationssäkerhet och utifrån det lämnades tre övergripande rekommendationer. Förslag är att kommunstyrelseförvaltningen beslutar att genomföra åtgärder utifrån dessa rekommendationer.

Beskrivning av ärendet

EY har på uppdrag av revisorer i Tyresö kommun genomfört en granskning med syftet att bedöma om det finns brister i det praktiska arbetet inom IT-och informationssäkerhet. Detta genom att testa medarbetarnas medvetenhet och

kunskap inom området. Granskningen har också syftat till att bedöma i vilken utsträckning en angripare har möjlighet att komma åt kommunens IT-miljöer genom angrepp via e-postmeddelanden, med fokus på användaren, vanligen kallat nätfiske (eng. Phishing). Den sammanfattande bedömningen är att det finns brister gällande utbildning och medarbetarnas medvetenhet inom informationssäkerhet i Tyresö kommun.

Kommunstyrelsen rekommenderas därför att vidta åtgärder för att förbättra organisationens medvetande, kunskap och förmåga om cyberhot i arbetsvardagen och således minska risken för cyberangrepp, till exempel i form av phishingattacker.

Mot bakgrund av vad som framkommit i granskningen lämnades tre övergripande rekommendationer till kommunstyrelsen:

- Informera om informationssäkerhet och phishing
- Tydliggör och informera om rutiner för rapportering av misstänkta e-postmeddelanden
- Genomför teoretiska och praktiska utbildningar inom phishing

Revisorernas rekommendationer

Revisorerna rekommenderar att Tyresö kommun informerar om informationssäkerhet och phishing

Kommentar

Tyresö kommuns digitala och interaktiva utbildning ”Webbutbildning Trygg Informationssäkerhet” blir obligatorisk och omfattar all verksamhet i Tyresö kommun och dess bolag utan undantag.

Informationssäkerhetssamordnare ansvarar för att innehållet i utbildningen är uppdaterat och relevant.

Verksamhetsansvariga chefer ansvarar för att samtliga anställda har de förutsättningar som krävs för att genomföra utbildningen, både vid nyanställning och kontinuerligt under tjänstgöringen, årsvis eller vid större förändringar i verksamhetens informationshantering.

Samtliga anställda har ett eget ansvar att genomföra utbildningen, både vid nyanställning och kontinuerligt under tjänstgöringen, årsvis eller vid större förändringar i verksamhetens informationshantering.

Revisorerna rekommenderar att Tyresö kommun tydliggör och informera om rutiner för rapportering av misstänkta e-postmeddelanden

Kommentar

Meddelande kopplat till informationen om utbildningen ovan, med en utpekning av phishing och hur detta rapporteras, samt rutinens plats i styrdokumentet ”Instruktion informationssäkerhet användare”.

Informationssäkerhetssamordnare ansvarar för att meddelandet publiceras på intranät så snart som möjligt och senast efter åtgärdspunkten beslutats.

Revisorerna rekommenderar att Tyresö kommun genomför teoretiska och praktiska utbildningar inom phishing

Kommentar

Praktisk och teoretisk utbildning kommer att genomföras med samtliga chefer Tyresö kommun, minst 2024 och 2025, med nytt beslut om utbildningens inriktning 2026, utifrån tydligaste hotet då.

Den praktiska delen grundar sig i synen på hur en angripare tänker när denna designar sitt phishing mail, avsett att vara ett legitimt mail för mottagaren/mottagarna.

Informationssäkerhetssamordnare ansvarar för innehållet i utbildningen och för att leda utbildningstillfället.

Ekonomiska konsekvenser

Förslaget till beslut är att lämna in svar på revisionsskrivelse och det har inga ekonomiska konsekvenser.

Barnens bästa

Ärendet bedöms inte beröra barn varför någon prövning av barnets bästa inte har genomförts.

Motivering till det föreslagna beslutet

Brister i informationssäkerhet kan få allvarliga konsekvenser, både för kommunen och dess invånare. De föreslagna åtgärderna bedöms vara ändamålsenliga och genomförbara.