Malmö stad
Kommunstyrelsen

Datum
2025-03-12
Adress
August Palms Plats 1
Diarienummer
STK-2025-302

Yttrande

Till
Revisorskollegiet

Granskning av IT-säkerhet
SR-2024-38

Sammanfattning
Revisorskollegiet har genom konsulten KPMG granskat stadens IT-säkerhet genom att bedöma om kommunstyrelsen och servicenämnden säkerställt en tillräcklig IT-säkerhet för Malmö stad. Den samlade bedömning är att kommunstyrelsen och servicenämnden inte helt har säkerställt en tillräcklig IT-säkerhet för Malmö stad.

Kommunstyrelsens förslag till yttrande behandlar de rekommendationer som lämnats utifrån genomförd granskning. Kommunstyrelsen instämmer i huvudsak i revisorskollegiets slutsatser. Medvetenhet och utbildning samt uppföljning och utvärdering ingår sedan tidigare i stadskontorets verksamhetsplanering för 2025.

Yttrande
Kommunstyrelsen instämmer i huvudsak i revisorskollegiets slutsatser. Utvecklingsinsatser, för ledningssystemet för informationssäkerhet är redan planerade. Dessa ligger i linje med revisorskollegiets rekommendationer, till exempel vad gäller medvetenhet och utbildning samt uppföljning och utvärdering. Kommunstyrelsen vill betona att det på kort sikt är svårt att se effekterna av vidtagna åtgärder när det handlar om ett långsiktigt systematiskt arbete.

Granskningens avgränsning
Kommunstyrelsen vill betona vikten av tydlighet i språkbruk och avgränsning för granskningar inom informationssäkerhetsområdet. Syftet med granskningen var enligt revisorskollegiet att bedöma om kommunstyrelsen och servicenämnden säkerställer en tillräcklig IT-säkerhet för Malmö stad. IT-säkerhet är del av informationssäkerhet avgränsad till IT-resurser. IT-resurser kan vara nätverk, servrar, hårdvara, mjuk/programvara, mobila enheter, klienter och brandväggar. Kommunstyrelsen anser att granskningen snarare hade ett bredare cybersäkerhetsfokus. Myndigheten för samhällsskydd och beredskap (MSB) definierar i sin termbank cybersäkerhet som ”informationssäkerhet avseende indirekta och direkta, externa beroenden och hot som

finns i ett större och mer komplext digitalt ekosystem än (enbart) inom den egna organisationen eller samhället". MSB anmärker även att "cybersäkerhet" ibland likställs med både "IT-säkerhet" och "informationssäkerhet", men att man ska göra skillnad mellan dessa begrepp och att informationssäkerhet kan ses som en förutsättning för cybersäkerhet.

Rekommendationer och planerade åtgärder

- **Bereda förslag till en informationssäkerhetspolicy eller motsvarande vars innehåll motsvarar de krav som ställs enligt ISO 27000-serien.**

Kommunstyrelsen bedömer att det inte nödvändigtvis är ändamålsenligt att en ny policy tas fram enbart för att öka informationssäkerheten. Kommunstyrelsen ser att det redan finns styrning på området bland annat genom nämndernas reglemente. I samband med översynen av Malmö stads trygghets- och säkerhetspolicy kommer kommunstyrelsen att utreda hur policykraven i ISO 27000-serien skulle kunna omhändertas på ett lämpligt sätt i Malmö stads styrning. Detta förväntas leda till mer ändamålsenlig styrning av Malmö stads informationssäkerhet.

- **Tillse att uppföljning och rapportering av informationssäkerhetsarbetet sker i enlighet med beslut i Riktlinjer för informationssäkerhet samt att kontroll av efterlevnad av riktlinjerna etableras.**

Kommunstyrelsen anser att den systematiska uppföljning som genomförs i hela organisationen med stöd av den nationella uppföljningsstrukturen Cybersäkerhetskollen har en tydlig koppling till Malmö stads riktlinjer och anvisningar för informationssäkerhet. Utöver Cybersäkerhetskollen följs Malmö stads informationssäkerhet upp inom intern kontroll om särskilda riskområden har identifierats. Informationssäkerhetsarbetet kan dessutom komma att följas upp genom externa granskningar (beställda eller genom revisorskollegiet). Sammantaget bedömer därför kommunstyrelsen att ytterligare årlig mätning och uppföljning av Malmö stads efterlevnad av riktlinjerna inte säkert ger önskad effekt eftersom det är samma personella resurser som generellt ansvarar för att genomföra uppföljningarna och leda åtgärdsarbetet.

Kommunstyrelsen instämmer däremot i att den rapportering som gjorts inte är tillräcklig. Kommunstyrelsen kommer därför att utreda vilka områden som med fördel kan ingå i rapportering till kommunstyrelsen och stadens ledningsgrupp, med vilken regelbundenhet rapporteringen ska ske samt hur rapporteringen ska ske. Detta förväntas öka ledningens delaktighet i informationssäkerhetsarbetet och ge bättre förutsättningar för ledningens riskägarskap och beslut om åtgärder.

- **Tillse att rutin för uppföljning av det stadsövergripande informationssäkerhetsarbetet upprättas och etableras i enlighet med Anvisning för informationshantering och säkerhetsprocesser.**

Kommunstyrelsen kommer att ta fram en rutin som tydliggör hur Malmö stad arbetar med uppföljning och utvärdering av informationssäkerhet. Detta förväntas tydliggöra genomförandet för medarbetarna i informationssäkerhetsorganisationen samt höja kvalitén på genomförd uppföljning och utvärdering.

- **Tillse att utbildning och information om IT-säkerhetshot och risker genomförs i hela organisationen för att stärka kunskap och medvetenhet hos användare. Därtill behöver genomförandegraden följas upp och åtgärder vidtas vid bristande genomförande.**

Kommunstyrelsen kommer att införa MSB:s utbildning Digital informationssäkerhetsutbildning för alla (Disa) som grundläggande utbildning för alla medarbetare i Malmö stads nya Learning Management System ”Malmö Lär”. Detta förväntas skapa förutsättningar för kompetenshöjning, uppföljning av genomförda utbildningar och deras effekt samt regelefterlevnad av den cybersäkerhetslag som träder i kraft under 2025.

Eftersom ingen orsaksutredning genomfördes i samband med nätfisketestet menar kommunstyrelsen att det inte säkert går att veta vilka bakomliggande orsaker som låg till grund för testets resultat. Kommunstyrelsen anser därutöver att kunskap och medvetenhet ensamt inte är ett effektivt skydd mot användarrelaterade IT-incidenter. Ett systematiskt och riskbaserat informationssäkerhetsarbete utifrån allriskperspektivet är centralt för att stärka informationssäkerhetskulturen och förebygga och hantera IT-incidenter.

Kommunstyrelsen planerar varje år utvecklingsinsatser utifrån Cybersäkerhetskollen och de förbättringsområden som identifieras där. Kommunstyrelsen ser att fortsatt kombinerat stärka organisation, teknik, personal och fysiskt skydd ger sammantaget goda förutsättningar att undvika allvarliga konsekvenser för Malmö stad.

Kommunstyrelsens bedömning är att samtliga åtgärder förväntas vara genomförda vid tiden för det andra yttrandet 27 februari 2026.

Ordförande [Förnamn Efternamn]

[Fyll i titel] [Förnamn Efternamn]

[Här anger du om det finns reservationer/särskilda yttranden.]