Malmö stad
Stadskontoret

Tjänsteskrivelse

Datum
2025-03-12
Vår referens
Kajsa Thelin
Utvecklingssamordnare
kajsa.thelin@malmo.se

Granskning av IT-säkerhet
STK-2025-302

Sammanfattning
Malmö stadsrevision, revisorskollegiet, har genomfört en granskning av kommunstyrelsens och servicenämndens arbete med IT-säkerhet. Kommunstyrelsen har fått möjlighet att yttra sig över granskningen och dess rekommendationer.

Syftet med granskningen var att bedöma om kommunstyrelsen och servicenämnden säkerställer en tillräcklig IT-säkerhet för Malmö stad. Med tillräcklig IT-säkerhet avsågs i granskningen att den bedrivs i enlighet med lagstiftning, föreskrifter och kommunfullmäktiges beslut. Den samlade bedömningen är att kommunstyrelsen och servicenämnden inte helt har säkerställt en tillräcklig IT-säkerhet för Malmö stad.

Stadskontorets instämmer i huvudsak i revisorskollegiets slutsatser och har sedan tidigare inkluderat medvetenhet och utbildning samt uppföljning och utvärdering i sin verksamhetsplanering för 2025.

Förslag till beslut
Kommunstyrelsen arbetsutskott föreslår kommunstyrelsen besluta

1. Kommunstyrelsen godkänner förslag till yttrande och skickar yttrandet till revisorskollegiet.

Beslutsunderlag
- Granskning av IT-säkerhet Missiv
- Granskning av IT-säkerhet Rapport
- G-Tjänsteskrivelse KSAU 250317 Granskning av IT-säkerhet
- Förslag till yttrande KSAU 250317 - Granskning av IT-säkerhet

Beslutsplanering
Kommunstyrelsens arbetsutskott 2025-03-17
Kommunstyrelsen 2025-04-02

SIGNERAD
2025-03-10

Beslutet skickas till

Revisorskollegiet
Stadskontorets handläggare

Ärendet

Revisorskollegiet har gett servicenämnden och kommunstyrelsen i uppdrag att yttra sig vid två tillfällen med anledning av Malmö stadsrevisions granskning av kommunstyrelsens och servicenämndens arbete med IT-säkerhet. Det första yttrandet ska inkomma senast 31 mars 2025 (servicenämnden) respektive 4 april 2025 (kommunstyrelsen). Det uppföljande yttrandet ska inkomma senast 30 januari 2026 (servicenämnden) respektive 27 februari 2026 (kommunstyrelsen).

Syftet med granskningen var att bedöma om kommunstyrelsen och servicenämnden säkerställer en tillräcklig IT-säkerhet för Malmö stad. Med tillräcklig IT-säkerhet avsågs i granskningen att den bedrivs i enlighet med lagstiftning, föreskrifter och kommunfullmäktiges beslut.

Följande revisionsfrågor ingick i granskningen:

1. Finns styrdokument för arbetet med IT-säkerhet och säkerställs att dessa efterlevs?
2. Förekommer och hanteras IT-säkerhetsincidenter kopplade till medarbetares användning av IT-system?
3. Finns ett arbetssätt för att upptäcka och hantera IT-säkerhetsincidenter?
4. Är roller och ansvarsfördelning tydlig inom IT-organisationen vid IT-säkerhetsincidenter?
5. Genomförs en systematisk uppföljning och rapportering av arbetet med IT-säkerhet?

Revisorskollegiets samlade bedömning är att kommunstyrelsen och servicenämnden inte helt har säkerställt en tillräcklig IT-säkerhet för Malmö stad.

Kommunstyrelsen har genom styrande dokument etablerat en styrning av IT-säkerhetsarbetet men har inte säkerställt en tillräcklig uppföljning och kontroll av arbetet i enlighet med beslutade styrdokument. Genomförda utbildningsinsatser för användare i staden bedöms inte varit tillräckliga för att etablera kunskap och medvetenhet om de IT-säkerhetshot som riktas mot användare. I granskningen har ett test genomförts och utifrån resultatet i testet bedöms att personalsäkerheten är bristfällig och att medarbetarnas användning av IT-system är förenat med risker.

Utifrån resultatet av granskningen rekommenderas kommunstyrelsen att:

- Bereda förslag till en informationssäkerhetspolicy eller motsvarande vars innehåll motsvarar de krav som ställs enligt ISO 27000-serien.
- Tillse att uppföljning och rapportering av informationssäkerhetsarbetet sker i enlighet med beslut i Riktlinjer för informationssäkerhet samt att kontroll av efterlevnad av riktlinjerna etableras.
- Tillse att rutin för uppföljning av det stadsövergripande informationssäkerhetsarbetet upprättas och etableras i enlighet med Anvisning för informationshantering och säkerhetsprocesser.
- 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.

Bakgrund

Kommunstyrelsen beslutade 2022 om Malmö stads riktlinjer för informationssäkerhet (STK-2021-1717). Varje nämnd är ansvarig för informationssäkerheten inom sin förvaltning och ska tillse att riktlinjer och underliggande styrdokument efterlevs. Ansvaret följer det ordinarie verksamhetsansvaret inom nämndsorganisationen. Riktlinjerna gäller för all informationshantering, oberoende av i vilken form eller vilket sammanhang som informationen förekommer. All information som Malmö stad ansvarar för ska behandlas på ett säkert och korrekt sätt. Skyddet ska anpassas efter informationens skyddsvärde, rådande förutsättningar, hot och risker. För att uppnå detta ska informationssäkerhet vara ett integrerat perspektiv och en medveten del av verksamhetens arbetsprocesser. Arbetet ska bedrivas systematiskt, riskbaserat och långsiktigt samt involvera relevanta kompetenser. Som stöd har varje förvaltning informationssäkerhetssamordnare som ingår i ett stadsövergripande nätverk under ledning av stadskontoret.

Kommunstyrelsen har ansvar för det övergripande arbetet med informationssäkerhet och ska leda, samordna och ha uppsikt över området. Detta innebär att utifrån ett helhetsperspektiv leda och samordna stadens övergripande arbete, ta fram stadsövergripande styrdokument och processer samt följa upp att de efterlevs. Stadskontoret har därmed som styrelsens förvaltning ett centralt, stadsövergripande ansvar att sätta ramarna för hur allt arbete med informationssäkerhet i Malmö stad ska bedrivas.

Servicenämnden ansvarar för att leda, utveckla och samordna kommunens gemensamma IT-och digitaliseringsfrågor, informationssystem och digital infrastruktur.

Servicenämnden ansvarar för informationssäkerheten inom sin förvaltning och stadsdirektören har enligt riktlinjerna för informationssäkerhet rätt att delegera fastställande av underliggande dokument till enhetschef säkerhet och beredskap (stadskontoret) samt avdelningschef för IT- och digitaliseringsavdelningen (serviceförvaltningen). Avdelningschef för IT- och digitaliseringsavdelningen har fastställt den stadsgemensamma anvisningen för IT-säkerhet.

Stadskontorets bedömning

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

Stadskontoret bedömer att det inte nödvändigtvis är ändamålsenligt med en policy enbart för informationssäkerhet för att komplettera den styrning som ges genom nämndernas reglemente. Malmö stad har idag en trygghets- och säkerhetspolicy beslutad av kommunfullmäktige den 24 maj 2017. Dessutom är en policy för Malmö stads beredskapsarbete under framtagande. Stadskontoret anser att policystyrningen av trygghets- och säkerhetsarbetet som helhet behöver ses över och att det i samband med det bör utredas hur policykraven i ISO 27000-serien skulle kunna omhändertas på ett lämpligt sätt i Malmö stads styrning.

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

Stadskontoret 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. Mätningens arbetsområden ingår i ett ledningssystem för informationssäkerhet utifrån SS-ISO/IEC 27000-serien, vilket är den standardserie som riktlinjen och underliggande anvisningar, regler och rutiner baseras på.

Cybersäkerhetskollen innehåller även en mätning av Malmö stads IT-säkerhetsmognad, och utökas löpande med nya mätområden. Mätningen har genomförts årligen sedan 2023. 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 stadskontoret 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.

Stadskontoret instämmer däremot i att den rapportering som gjorts till kommunstyrelsen inte är tillräcklig. Det behöver utredas och fastställas hur rapportering av status på Malmö stads informationssäkerhetsarbete hade kunnat genomföras i enlighet med riktlinjerna, det vill säga årlig återkoppling till stadens ledningsgrupp och kommunstyrelsen.

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

Stadskontoret instämmer i att det praktiska genomförandet av uppföljning och utvärdering av informationssäkerhetsarbetet behöver tydliggöras. En rutin som tydliggör hur Malmö stad arbetar med uppföljning och utvärdering av informationssäkerhet kommer därför tas fram.

- **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.**

Stadskontoret delar uppfattningen att utbildning och information om IT-säkerhetshot och risker behöver vara ett återkommande inslag hos Malmö stads medarbetare. Stadskontoret menar dock att utbildning och information i sig inte räcker för att förebygga IT-relaterade säkerhetsincidenter.

Eftersom ingen orsaksutredning genomfördes i samband med nätfisketestet menar stadskontoret att det inte säkert går att veta vilka bakomliggande orsaker som låg till grund för testets resultat. Det är viktigt att verka för att medarbetarna har rätt kunskap och medvetenhet om hot och risker, men kunskap och medvetenhet räcker inte för att bygga en god informationssäkerhetskultur i Malmö stad. Informationssäkerhetskultur kan benämnas som gemensamma tanke-, beteende- och värderingsmönster som uppstår och utvecklas i ett socialt kollektiv genom kommunikativa processer baserade på inre och yttre krav. Dessa gemensamma tanke-, beteende- och värderingsmönster överförs till nya medlemmar och påverkar informationssäkerheten.

I Myndigheten för samhällsskydd och beredskaps (MSB) populärvetenskapliga sammanfattning ”Informationssäkerhetskultur i praktiken” (2023) redogörs för en forskningsstudie där möjligheten att påverka informationssäkerhetskultur undersöktes. Undersökningen baserades på mätningar av kulturen före och efter påverkansförsök i fem organisationer. Mätningarna utfördes genom bland annat en enkät och genom att

studera anställdas reaktioner på simulerade nätfiskemeddelanden. Försöken att påverka kulturen bestod av utbildning av medarbetare och handledning av chefer. Studien visade bland annat att beteende (både självskattat och mätt med nätfiske) tycks vara svårare att påverka genom utbildning och handledning än chefens agerande och gruppens informationssäkerhetsklimat, och att effekterna överlag är små. En medarbetare kan alltså ha ”rätt” kunskap och värderingar, men ändå agera ”fel”. Det beror bland annat på att informationssäkerhetskulturen påverkas av faktorer som ligger utanför själva säkerhetsfältet, såsom hur individens arbetssituation ser ut.

Kompetenshöjande insatser är ett av de områden som ingår i kommunstyrelsens nämndsbudget för 2025. Malmö stad använder sig idag av MSB:s utbildning ”Digital informationssäkerhetsutbildning för alla” (Disa) som grundläggande utbildning för alla medarbetare. Utbildningen kommer att införas i Malmö stads nya Learning Management System ”Malmö Lär” under 2025 för att möjliggöra kompetenshöjning, uppföljning av genomförda utbildningar och deras effekt samt regelefterlevnad av den cybersäkerhetslag som träder i kraft under 2025.

Stadskontoret anser att Malmö stad bör stärka sin informationssäkerhetskultur för att ge medarbetarna bättre förutsättningar att göra säkra val. Exempel på det är prioriterat införande av tekniska säkerhetsåtgärder som gör att vi tidigt kan upptäcka hot, hantering av tekniska sårbarheter som kan utnyttjas av angripare och användning av säkra inloggningsmetoder. Ett systematiskt och riskbaserat informationssäkerhetsarbete utifrån allriskperspektivet är centralt för att stärka informationssäkerhetskulturen och förebygga och hantera IT-incidenter. Stadskontoret planerar varje år utvecklingsinsatser utifrån Cybersäkerhetskollen och de förbättringsområden som identifieras där. Stadskontoret ser att fortsatt kombinerat stärka organisation, teknik, personal och fysiskt skydd ger sammantaget goda förutsättningar att undvika allvarliga konsekvenser för Malmö stad.

Granskningens avgränsning

Då syftet med granskningen var att bedöma om kommunstyrelsen och servicenämnden säkerställer en tillräcklig IT-säkerhet för Malmö stad, vill stadskontoret betona vikten av tydlighet i språkbruk och avgränsning för granskningar inom informationssäkerhetsområdet. IT-säkerhet är del av informationssäkerhet avgränsad till IT-resurser. IT-resurser kan vara nätverk, servrar, hårdvara, mjuk/programvara, mobila enheter, klienter och brandväggar. Stadskontoret 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.

Ansvariga

Agnes Wemme Nämndsekreterare
Per-Erik Ebbeståhl Avdelningschef
Andreas Norbrant Stadsdirektör