Tjänsteskrivelse

Datum
2021-03-18
Vår referens
Josefin Levander
IT-specialist
josefin.levander@malmo.se

Rapport från revisorskollegiet - Granskning av IT-säkerhet
STK-2021-158

Sammanfattning

Revisorskollegiet har genomfört en granskning av Malmö stads IT-säkerhet. Syftet med granskningen är att bedöma om kommunstyrelsen och servicenämnden säkerställer att IT-säkerheten är tillräcklig för att reducera risker för obehörigt intrång. Den sammanfattande bedömningen är att kommunstyrelsen och servicenämnden endast till viss del säkerställer en tillräcklig IT-säkerhet. Ett antal viktiga förbättringsområden har identifierats.

Stadskontoret instämmer i revisorskollegiets iakttagelser av förbättringsområden och redovisar förslag till åtgärder för dessa. Sammanfattningsvis pekar åtgärderna framförallt på tre förbättringsområden:

- Tydlighet i organisation och ansvar för informations- och IT-säkerhet.
- Uppföljning och rapportering av informations- och IT-säkerhet.
- Anpassad information och utbildning inom informations- och IT-säkerhet för tillämpning och efterlevnad.

De föreslagna åtgärderna tar sikte på att utveckla nya former av samverkan, arbetssätt och befintliga riktlinjer. Flera av de identifierade brister som finns beskrivna i rapporten handlar om tillämpning, efterlevnad och uppföljning av redan fattade beslut, det vill säga skapa tydlighet och medvetenhet hos de verksamheter och tjänstepersoner som ansvarar för in-formations- och IT-säkerhet. I de fall stadskontoret bedömer att det behövs beslut om nya uppdrag, föreslås detta i yttrandet. Åtgärderna föreslås hanteras på ett stadsövergripande sätt vilket behöver tas fram gemensamt mellan serviceförvaltningen och stadskontoret.

De nya uppdrag som föreslås av stadskontoret är följande:

- *Kommunstyrelsen föreslås uppdra åt stadskontoret* att i samarbete med serviceförvaltningen utreda och föreslå en tydligare organisation och styrning inom informationssäkerhet och IT-säkerhet med tydligare ansvar och mandat, med anledning av att kommungemensam IT och digitalisering flyttas till servicenämnden, under förutsättning att kommunfullmäktige antar de förslag som lyfts fram i ärende STK-2019-284.

- *Kommunstyrelsen föreslås uppdra åt stadskontoret* att följa upp nämndernas arbete med att dokumentera samtliga informationssystem och tjänster i enlighet med anvisningarna i riktlinjerna för informationssäkerhet.

- *Kommunstyrelsen föreslås uppdra åt stadskontoret* att stötta övriga förvaltningar i att kommunicera behovet av ett systematiskt och fungerande informationssäkerhetsarbete.

- *Kommunstyrelsen föreslås uppdra åt stadskontoret* att ta fram instruktioner och anvisningar för förvaltningarnas utbildning av anställda i informationssäkerhet och IT-användning, som förvaltningarna ansvarar för att genomföra.

- *Kommunstyrelsen föreslås uppdra åt stadskontoret* att hitta lämpliga kompletterande metoder och möjligheter att följa upp det kommunövergripande arbetet med informationssäkerhet.

- *Kommunstyrelsen föreslås uppdra åt stadskontoret* att undersöka hur regelbundet återkommande rapportering av informations- och IT-säkerhetsfrågor till kommunstyrelsen ska kunna ske, samt ta fram en plan för denna. Uppföljningen utgår från beslutade riktlinjer för informationssäkerhet.

Förslag till beslut
Kommunstyrelsens arbetsutskott föreslår kommunstyrelsen besluta

1. Kommunstyrelsen godkänner förslag till yttrande och översänder det till revisorskollegiet.

Beslutsunderlag
- Bilaga – Yttrande till revisorskollegiet
- Missiv
- Granskning av IT-säkerhet
- Förslag till yttrande
- G-Tjänsteskrivelse KSAU 210329 Rapport från revisorskollegiet - Granskning av IT-säkerhet

Beslutsplanering
Kommunstyrelsens arbetsutskott 2021-03-29
Kommunstyrelsen 2021-04-07

Beslutet skickas till
[Här skriver du vem beslutet ska skickas till efter att protokollet är justerat, ange funktion eller organisation. Uppgifterna överförs till protokoll och protokollsutdrag. I fliken expediera till, på ärendekortet, anger du fullständiga uppgifter som exempelvis e-postadress, som en information till nämndsekreteraren . Om beslutet inte ska expedieras, kan denna text och rubrik tas bort.]

Ärendet
Revisorskollegiet har genomfört en granskning av Malmö stads IT-säkerhet. Syftet med granskningen har varit att bedöma om kommunstyrelsen och servicenämnden säkerställer att IT-säkerheten är tillräcklig för att reducera risker för obehörigt intrång.

Syftet har brutits ned i följande revisionsfrågor:

- Finns det en ändamålsenlig organisation med tydlig ansvarsfördelning avseende IT–säkerhetsarbetet?
- Finns det ändamålsenliga styrdokument för IT-säkerhet och säkerställs det att dessa följs?
- Finns det en tillräcklig intern kontroll av IT-säkerheten (t.ex. behörigheter, avslut m.m.)?
- Identifieras och hanteras IT-säkerhetsrisker förknippade med arbete i hemmet och nämndssammanträden på distans?
- Finns det en tillräcklig säkerhet avseende intrång av extern eller intern aktör?
- Hanteras och dokumenteras IT-säkerhetsincidenter på ett ändamålsenligt sätt?
- Finns det dokumenterade och ändamålsenliga kontinuitetsplaner för granskade system?
- Sker det en tillräcklig uppföljning av IT-säkerhetsarbetet och är återrapporteringen till kommunstyrelsen och servicenämnden tillräcklig?

Granskningen har avsett kommunstyrelsen och servicenämnden. Granskningen har genomförts genom dokumentstudier och intervjuer med tjänstepersoner inom stadskontoret och serviceförvaltningen. Vidare har ett penetrationstest genomförts av stadens anslutningsmöjligheter för distansarbete och digitala möten. Testet har genomförts för att bedöma sårbarheter för intrång i stadens informationssystem via de system som finns för fjärråtkomst. Utifrån genomfört penetrationstest har revisorskollegiets bedömning varit att den tekniska säkerhetsrisken i form av hot mot stadens IT-miljö vid distansarbete via de system som finns för fjärranslutning är låg.

Trygghets- och säkerhetsarbetet i Malmö stad är kopplat till det ordinarie verksamhetsansvaret hos respektive förvaltning och följer linjeansvaret för stadens chefer till medarbetarnivån. Arbetet ska utgå från styr- och ledningssystemet vilket ska ge goda förutsättningar för en tydlig koppling mellan mål, insats, uppföljning och utvärdering.

I beslutade riktlinjer och anvisningar för informationssäkerhet framgår att det är nämnderna som är ytterst ansvariga för informationssäkerheten och att de ansvarar för att tillse att krav på verksamhetens informationshantering följs genom intern kontroll samt att resurser avsätts för att möta de hot som kan uppstå i verksamheten.

I Malmö stads IT-strategi från 2007 framgår att styrningen av IT-verksamheten kännetecknas av en tydlig kund och leverantörsrelation med Malmö stads verksamheter som beställare och serviceförvaltningen och andra leverantörer som utförare.

Genom stadens organisering av sitt informations- och IT-säkerhetsarbete finns ett ansvar för detta inom IT-enheten på stadskontoret, enheten för säkerhet och beredskap på stadskontoret, förvaltningarnas eget arbete och IT-service på serviceförvaltningen. Även juridiska enheten på stadskontoret arbetar med frågan utifrån lagstiftning och dataskydd.

I ärendet STK-2019-284, som tas upp i kommunfullmäktige den 31 mars 2021, finns förslag på nya riktlinjer och omorganisering av IT, digitalisering och systemförvaltning. Under förutsättning att kommunfullmäktige fattar beslut enligt förslagen i ärendet, kommer IT-strategin från 2007 att ersättas av riktlinjer för IT och digitalisering samtidigt som organiseringen ändras och ansvaret för bland annat IT-säkerhet flyttas från stadskontoret till servicenämnden. Som en följd av att informations- och IT-säkerhet hamnar under olika nämnder behöver nya former för samverkan och nya arbetssätt etableras mellan stadskontoret och serviceförvaltningen.

Granskningens sammanfattande bedömning
Den sammanfattande bedömningen är att kommunstyrelsen och servicenämnden endast till viss del säkerställer en tillräcklig IT-säkerhet. Ett antal viktiga förbättringsområden har identifierats.

Sammanfattningsvis pekar åtgärderna framförallt på tre förbättringsområden:

- Tydlighet i organisation och ansvar för informations- och IT-säkerhet.
- Uppföljning och rapportering av informations- och IT-säkerhet.
- Anpassad information och utbildning inom informations- och IT-säkerhet för tillämpning och efterlevnad.

Stadskontorets bedömning
Stadskontoret instämmer i revisorskollegiets iakttagelser av förbättringsområden och redovisar förslag till åtgärder för dessa. De föreslagna åtgärderna tar sikte på att utveckla nya former av samverkan, arbetssätt och befintliga riktlinjer. Flera av de identifierade brister som finns beskrivna i rapporten handlar om tillämpning, efterlevnad och uppföljning av redan fattade beslut, det vill säga skapa tydlighet och medvetenhet hos de verksamheter och tjänstepersoner som ansvarar för informations- och IT-säkerhet. I de fall stadskontoret bedömer att det behövs beslut om nya uppdrag, föreslås detta i yttrandet. Åtgärderna föreslås hanteras på ett stadsövergripande sätt vilket behöver tas fram gemensamt mellan serviceförvaltningen och stadskontoret.

Riktlinjer och anvisningar för informationssäkerhet finns framtagna sedan 2013. Stadskontoret har under 2020 påbörjat arbetet med att uppdatera och utveckla riktlinjerna i syfte att förtydliga dess innehåll, ansvar och mandat för att öka riktlinjens tillgänglighetsgrad och underlätta efterlevnaden i stadens förvaltningar. Detta arbete ska även belysa det eventuella behovet av kompletterande anvisningar för IT-säkerhet och förväntas vara klart under 2021.

Det finns redan idag rutiner och IT-verktyg för rapportering av incidenter. Det kan däremot konstateras att implementationen av både rutiner och verktyg inte lyckats såsom förväntat. Det finns mycket arbete att göra när det gäller analys och uppföljning av incidenter. Detta är en fråga som stadskontoret och serviceförvaltningen behöver ha ett gemensamt synsätt kring.

Nedan följer samtliga rekommendationer från revisorskollegiet till kommunstyrelsen, följt av åtgärder samt beskrivning av förväntad effekt av dessa. Samtliga åtgärder ska, såvida inte annat anges, vara genomförda senast vid slutet av 2022 med delredovisning till revisorskollegiet senast den 26 februari 2022, enligt instruktioner i bilagan i ärendet.

Etablera en organisation med tydligt ansvar och mandat för stadens informations- och IT-säkerhetsarbete

Åtgärd
I samband med föreslagen omorganisation och sammanslagning av kommungemensam IT (STK-2019-284), behöver nya former för samverkan mellan IT- och informationssäkerhet etableras mellan stadskontoret och serviceförvaltningen.

Kommunstyrelsen föreslås uppdra åt stadskontoret att i samarbete med serviceförvaltningen utreda och föreslå en tydligare organisation och styrning inom informationssäkerhet och IT-säkerhet med

tydligare ansvar och mandat, med anledning av att kommungemensam IT och digitalisering flyttas till servicenämnden, under förutsättning att kommunfullmäktige antar de förslag som lyfts fram i ärende STK-2019-284.

Förväntad effekt
Tydlighet gällande roller och ansvar för informations- och IT-säkerhet på samtliga förvaltningar skapar förutsättningar för efterlevnad och uppföljning. Fortsatt nära samverkan mellan stadskontoret och serviceförvaltningen för att gemensamt arbeta mot bättre IT- och informationssäkerhet i Malmö stad.

Ta fram policy för informationssäkerhet eller revidera befintlig Trygg- och säkerhetspolicy så att informationssäkerhet är inkluderat. Samt komplettera denna med de riktlinjer och anvisningar som behövs för att styra arbetet

Åtgärd
Stadskontoret har påbörjat arbetet med att uppdatera och utveckla riktlinjerna för informationssäkerhet i syfte att öka tillgänglighetsgraden och efterlevnaden i stadens verksamheter. Det arbetet ska även belysa det eventuella behovet av kompletterande anvisningar för IT-säkerhet. Uppdatering av befintlig trygghets- och säkerhetspolicy är planerat att påbörja inom innevarande år och sker i samverkan mellan säkerhets- och beredskapsenheten samt trygghetsenheten på stadskontoret.

Förväntad effekt
Genom ökad tydlighet i policyn såväl som i befintliga riktlinjer och anvisningar för informationssäkerhet samt komplettering med anvisningar för IT-säkerhet ökas tillgängligheten till denna information. Med ökad tydlighet och bättre tillgänglighet förväntas även möjligheten att styra informations- och IT-säkerhetsarbetet förbättras samt att efterlevnaden ökar.

Ge nämnder och förvaltningar i uppdrag att kartlägga samtliga informationssystem och tjänster och dokumentera dessa i förteckning för att säkerställa att det finns en komplett förteckning som är uppdaterad och kan fungera som informationskälla i hanteringen av IT-säkerhetsåtgärder

Åtgärd
Kommunstyrelsen föreslås uppdra åt stadskontoret att följa upp nämndernas arbete med att dokumentera samtliga informationssystem och tjänster i enlighet med anvisningarna i riktlinjerna för informationssäkerhet. Nämndernas arbete med kartläggning och dokumentation ska förbättras genom utveckling av både metodstöd och IT-verktyg.

Arbete pågår med att revidera och komplettera kravställningarna i samband med klassificering, med målet att IT:s kravbibliotek inarbetas i befintlig process med tillhörande metodstöd för klassificering av information i Malmö stad. Metodstödet förväntas lanseras under våren 2021.

Förväntad effekt
Kommunstyrelsen får ökad kontroll över och insyn i stadens informationssäkerhetsarbete, samtidigt som nämndernas kunskap om området ökar. Ökad tydlighet i befintliga riktlinjer och anvisningar för informationssäkerhet samt uppdatering av befintligt metodstöd förväntas tydliggöra och underlätta Malmö stads efterlevnad av riktlinjen.

Säkerställa att det genomförs risk- och konsekvensanalyser för verksamhetskritiska informationssystem och att det finns tillhörande kontinuitetsplaner för dessa

Åtgärd
Stadskontoret planerar utveckla den kommunövergripande metoden för risk- och konsekvensanalyser på IT-system och digitala tjänster samt ta fram ett dokumentationsstöd för att förenkla uppföljningen av att dessa analyser verkligen genomförts. För identifierade verksamhetskritiska system ska kontinuitetsplaner finnas och vara uppdaterade. Den metod som behövs på systemnivå ska harmonisera med den modell som är framtagen och beslutad för kontinuitetshantering i Malmö stad generellt. En utvecklad kommunövergripande metod ska underlätta för förvaltningarna att identifiera dessa verksamhetskritiska system. Utifrån detta kan kommunstyrelsen följa upp att det finns kontinuitetsplaner för de systemen.

Stadskontoret behöver förtydliga för systemägare och systemförvaltare vad detta innebär för enskilda system.

Förväntad effekt
Ökad följsamhet och tydlighet kring beslutade interna krav och riktlinjer gällande kontinuitetsplanering av samhällsviktiga och verksamhetskritiska processer i Malmö stad.

En kommunövergripande metod förväntas underlätta för den verksamhet som ska utföra riskanalyserna.

Säkerställa att metod för klassning finns som är tillämpbar för dagens informationssystem och tjänstehantering och att klassning genomförs både på system och information som hanteras i förvaltningarna

Åtgärd
Stadskontoret uppdaterar regelbundet metod och metodstöd för klassificering i syfte att förbättra tillämpbarheten på dagens informationssystem och tjänstehantering samt för att följa verksamhetens behov. Översyn av riktlinje och metodstöd ska ske minst en gång per år. Samverkan mellan informationssäkerhet och IT ska tillse att IT:s kravbibliotek integreras i befintlig klassningsprocess. En gemensam framtagning och uppföljning av informations- och IT-säkerhetskrav i samband med klassificering är planerad att påbörjas inom innevarande år

Uppgradering av IT-stödet Ifacts som används av Malmö stad för att klassificera pågår och förväntas gå i skarp drift under Q1 2021.

Kommunstyrelsen föreslås uppdra åt stadskontoret att stötta övriga förvaltningar i att kommunicera behovet av ett systematiskt och fungerande informationssäkerhetsarbete.

Förväntad effekt
Genom kontinuerligt förbättrat metodstöd och ökad samverkan mellan informationssäkerhet, IT och stadens förvaltningar förväntas antalet klassificerade system att öka. Utökad samverkan förväntas leda till ökad förståelse och insikt i processen och ett mer harmoniserat kravbibliotek som tar höjd för både tekniska och organisatoriska krav.

Säkerställa att nyanställda samt befintliga medarbetare får information och utbildning i ansvaret för informationssäkerhet och IT-användning

Åtgärd
Kommunstyrelsen föreslås uppdra åt stadskontoret att ta fram instruktioner och anvisningar för förvaltningarnas utbildning av anställda i informationssäkerhet och IT-användning, som förvaltningarna ansvarar för att genomföra.

Stadskontoret åtar sig att via nätverket för informationssäkerhet informera utpekade samordnare om befintlig utbildning och möjligheten att göra denna utbildning obligatorisk som en del av introduktionen för nyanställda.

Stadskontorets HR-avdelning har påbörjat en utredning om upphandling av en stadsövergripande digital läroplattform. En sådan teknisk lösning möjliggör både e-utbildningar samt uppföljning och kontroll över vilka medarbetare som genomfört och klarat av kunskapsprov inom området.

Förväntad effekt
Medvetenheten kring vikten av säker informationshantering och IT-användning ökar bland anställda. Med en teknisk lösning som på sikt kan leda till en stadsövergripande plattform möjliggörs uppföljning och kontroll över vilka medarbetare som gått vilka utbildningar och därmed uppföljningen av informationssäkerhetsutbildningarna.

Besluta om stadsövergripande rutin för incidenthantering och rapportering där ansvar och eskaleringsvägar finns tydliggjorda samt kommunicera denna till verksamheterna. Det behöver även säkerställas att en uppföljning sker av inträffade incidenter så att detta kan beaktas i förbättringsarbetet

Åtgärd
Arbete pågår på stadskontoret med att utveckla incidentprocessen för IT-säkerhet. För att säkerställa att en kommunövergripande rutin för incidenthantering och rapportering fungerar behöver en mer detaljerad analys genomföras. Denna analys ska ligga till grund för en handlingsplan för utveckling och förbättring av hantering och rapportering av IT-incidenter.

Stadskontoret och serviceförvaltningen behöver tillsammans utveckla nuvarande incidentprocesser för att inkludera information till berörda funktioner med ansvar för informationssäkerhet, IT-säkerhet och ansvar för driftsäkerhet. Serviceförvaltningen har åtagit sig att driva arbetet, som planeras vara slutfört under 2021.

Förväntad effekt
Ansvar för incidenter och eskaleringsvägar tydliggörs. Samtidigt säkerställer stadskontoret tillsammans med serviceförvaltningen att uppföljning av inträffade incidenter sker och kan beaktas i förbättringsarbetet.

Säkerställa genom intern kontroll att det sker ett tillräckligt arbete med informationssäkerhet i

förvaltningarna där efterlevnad av beslutad riktlinje och anvisningar för informationssäkerhet finns

Åtgärd
Malmö stads kommunövergripande system för intern kontroll innefattar ett årligt riskanalysarbete, som resulterar i tre områden som sedan följs upp över hela kommunens verksamheter. Informationssäkerhetskompetens finns med i arbetet med riskanalys. De tre kommunövergripande områdena kan inte omfatta informationssäkerhet varje år, däremot kan stadskontoret rekommendera nämnderna att följa upp informationssäkerhet i deras arbete med intern kontroll av sin verksamhet.

Kommunstyrelsen föreslås uppdra åt stadskontoret att hitta lämpliga kompletterande metoder och möjligheter att följa upp det kommunövergripande arbetet med informationssäkerhet.

Förväntad effekt
Resultatet av den kommunövergripande uppföljningen kan användas för att upptäcka och åtgärda risker i kommunens verksamheter.

Skapa struktur för enhetlig uppföljning av informationssäkerhet inklusive IT-säkerhet och etablera rapporteringsvägar till ledning och styrelse

Åtgärd
Kommunstyrelsen föreslås uppdra åt stadskontoret att undersöka hur regelbundet återkommande rapportering av informations- och IT-säkerhetsfrågor till kommunstyrelsen ska kunna ske, samt ta fram en plan för denna. Uppföljningen utgår från beslutade riktlinjer för informationssäkerhet.

Förväntad effekt
Kommunstyrelsen får ökad kontroll över och insyn i stadens informations- och IT-säkerhetsarbete och tjänstemannaorganisationen får möjlighet att få återkoppling från sin förvaltningsledning.

Ansvariga
Anders Mellberg Kommunikationsdirektör
Magdalena Bondeson Sektionschef
Andreas Norbrant Stadsdirektör