Malmö stad
Servicenämnden

Datum

Adress

Diarienummer
SN-2025-285

Yttrande

Till
Stadsrevisionen

Granskningsrapport Revisionens granskning av IT-säkerhet
SR-2024-38

Servicenämnden har beslutat att lämna följande yttrande:

Sammanfattning
Servicenämnden instämmer i granskningens rekommendationer för incidenthantering och kommunikation och kommer vidta åtgärder. Servicenämnden instämmer inte i granskningens bedömning att det endast delvis genomförs en systematisk uppföljning av IT-säkerhet.

Granskningen utgår ifrån en bedömning där IT-säkerhet och cybersäkerhet är tekniska delar av informationssäkerhet. Bedömningen får en stor påverkan på granskningens utfall.

Granskningen gör bedömningen att servicenämnden delvis har säkerställt en tillräcklig IT-säkerhet för Malmö stad och rekommenderar servicenämnden att vidta åtgärder inom tre områden:

- Uppföljning och rapportering
- Incidenthantering
- Kommunikation

Servicenämnden kommer inledningsvis vidta åtgärder för att möta granskningens rekommendationer för incidenthantering och kommunikation.

Servicenämnden delar inte granskningens sammantagna bedömning att det endast delvis genomförs en systematisk uppföljning. Servicenämndens verksamhet genomför idag en omfattande uppföljning och rapportering som beskrivs i granskningen. Servicenämnden kommer invänta att rutin för uppföljning och rapportering upprättas av kommunstyrelsen i enlighet med den rekommendation som granskningen föreslår.

Yttrande

Servicenämnden som ansvarar för stadens IT-säkerhet tar detta uppdrag på stort allvar och som en del av detta arbete kommer servicenämnden ge serviceförvaltningen i uppdrag att återkomma inför kommande utvecklingsplaner med förslag på aktiviteter för att ytterligare stärka IT-säkerheten i Malmö stad, samt från och med april 2025 kvartalsvis rapportera status för IT-säkerhet, muntligt och skriftligt, för servicenämnden.

Servicenämnden kommer utöver ovan åtgärd i relation till granskningen inledningsvis vidta åtgärder för att möta två av de rekommendationer som granskningen föreslår för servicenämnden:

- Tillse att rutinerna för incidenthantering kompletteras med datering, beslutsinstans samt ansvarig för revidering för att säkerställa dess aktualitet och förankring.
- Komplettera kommunikationsplan vid kritiska incidenter med tydliggjorda eskaleringsvägar och mottagare av information hos samtliga förvaltningar/verksamheter.

Servicenämnden kommer invänta att rutin för uppföljning upprättas av kommunstyrelsen innan förändringar av uppföljning och rapportering genomförs i enlighet med den rekommendation som granskningen föreslår:

- Tillse att uppföljning och rapportering sker i enlighet med beslut i Riktlinjer för informationssäkerhet samt att kontroll av efterlevnad av riktlinjer etableras. Uppföljning och rapportering behöver genomföras dels utifrån nämndens ansvar för egen informationssäkerhet, dels specifikt i relation till nämndens ansvar för kommungemensam IT och tillhörande IT-säkerhet.

Nedan ges fördjupande kommentarer och synpunkter på granskningen. I sitt yttrande redogör servicenämnden för dess verksamhets arbete.

Begreppsdefinition

Servicenämnden konstaterar att granskningen utgår från en definition där IT-säkerhet och cybersäkerhet är den tekniska delen av informationssäkerhet. Servicenämnden konstaterar också att definitionen av de olika begreppen inte alltid är konsekvent inom offentlig förvaltning.

Myndigheten för samhällsskydd oh beredskap (MSB) nyttjar samlingsnamnet cybersäkerhetskollen där de underordnar IT-säkkollen och infosäkkollen som två delmätningar. Sveriges kommuner och regioner (SKR) beskriver att informationssäkerhet och cybersäkerhetsarbete är relaterade till säkerhet och säkert förvar av datorsystem mot datahot och informationsintrång de skriver:

”Konkret handlar informationssäkerhet om att förhindra att information, all data (oavsett form) läcker, förvrängs och förstörs. Det primära är att skydda uppgifternas konfidentialitet, integritet och tillgänglighet. Cybersäkerhet handlar däremot om att

skydda nätverk, enheter, program och data från attacker eller obehörig åtkomst. Det primära är att skydda mot obehörig elektronisk åtkomst till data."[1]

Uppföljning och rapportering

Granskningen beskriver den systematiska uppföljning och rapportering som görs idag av servicenämndens verksamhet genom bland annat penetrationstester, sårbarhetsanalyser, CIS Controls (ett ramverk med fastställda kontrollområden inom IT-säkerhet där regelbunden uppföljning identifierar sårbarheter och förbättringsområden), IT-säkkollen, rapportering till kommunstyrelsen genom "Utvecklingsplan kommungemensam IT och Digitalisering", rapportering till servicenämnden genom årsanalys och även andra revisioner som genomförts av IT-säkerheten inom IT- och digitaliseringsavdelningen (ITD). Utav den sammantaget omfattande uppföljning och rapportering som genomförs gör granskningen bedömningen att det delvis genomförs en systematisk uppföljning av arbetet med IT-säkerhet och att den rapportering som gjorts till servicenämnden inte är tillräcklig. Servicenämnden delar inte granskningens bedömning att det endast delvis genomförs en systematisk uppföljning.

Granskningen slår fast att det saknas tydlighet i hur den samlade årliga uppföljningen ska ske eftersom stadsövergripande rutin saknas.

Servicenämnden välkomnar en ökad tydlighet i hur uppföljning ska ske med den nya rutinen men anser samtidigt att en omfattande uppföljning och rapportering sker redan idag av IT-säkerhet. Servicenämnden kommer invänta att rutinen kommer på plats innan förändring av rapportering och uppföljning kan genomföras. Servicenämnden kommer ta granskningens bedömning i beaktning att även kommunstyrelsen behöver hållas informerad om väsentliga delar av IT-säkerhet.

Incidenthantering

ITD har under lång tid utvecklat den incidentprocess som finns idag för att möta nya behov från staden i takt med en ökad digitalisering som sker i förvaltningarna. Processen har utvecklats till att bli en viktig process för förvaltningarna och ITD arbetat aktivt med att öka effektivitet och kvalitet i processen.

Granskningen gör bedömningen att det inom servicenämnden finns arbetssätt för att upptäcka och hantera IT-säkerhetsincidenter samt att roller och ansvarsfördelning för hantering av dessa är tydliga inom IT- och Digitaliseringsavdelningen.

Granskningen rekommenderar servicenämnden att komplettera rutinerna med datering, beslutsinstans samt ansvarig för revidering. Servicenämndens verksamhet kommer tillse att kompletteringen genomförs under 2025.

Kommunikationsplan

Granskningen gör bedömningen att det inom servicenämnden finns arbetssätt för att upptäcka och hantera IT-säkerhetsincidenter samt att roller och ansvarsfördelning för hantering av dessa är tydliga inom IT- och Digitaliseringsavdelningen.

[1]https://skr.se/skr/naringslivarbetedigitalisering/digitalisering/cyberochinformationssakerhet.24856.html

Servicenämnden delar granskningens bedömning att nuvarande kommunikationsplan vid kritiska incidenter kan utvecklas med tydliggörande av eskaleringsvägar till representanter i övriga förvaltningar såsom föreslagits under granskningens intervjuer.

Under 2025 revideras kriskommunikationsplanen. Kommunikation kring kritiska incidenter kommer vara en del av planen och kommunikation ut till stadens förvaltningar kommer belysas.

Ordförande	Frida Trollmyr (S)
Nämndsekreterare	Jim Johannesson