Malmö stad
Servicenämnden

Datum
2026-08-18
Adress

Diarienummer

Rapport

Till
Servicenämnden

Rapport IT-säkerhet 2026 kvartal 2

Inledning

IT- och digitaliseringsavdelningen bedriver ett kontinuerligt arbete för att stärka skyddet av Malmö stads IT-miljö och minska risken för störningar, informationsförluster och andra konsekvenser till följd av cyberangrepp.

Den digitala hotbilden är fortsatt omfattande och ställer höga krav på kommunens förmåga att förebygga, upptäcka och hantera säkerhetshändelser. Arbetet bedrivs därför både långsiktigt och operativt och omfattar bland annat tekniska säkerhetsåtgärder, kontinuerlig övervakning, sårbarhetshantering, utveckling av incidenthanteringen samt anpassning till nya regulatoriska krav.

Under det andra kvartalet 2026 har arbetet fortsatt enligt plan, med särskilt fokus på att ytterligare stärka den förebyggande förmågan, utveckla skyddet mot e-postrelaterade hot samt förbereda organisationen inför de krav som följer av den nya cybersäkerhetslagstiftningen.

Bakgrund och syfte

Syftet med den kvartalsvisa rapporteringen är att ge Servicenämnden en övergripande bild av utvecklingen inom IT-säkerhetsområdet samt status för de aktiviteter som genomförs för att stärka säkerheten i Malmö stads IT-miljö.

Arbetet utgår från ett riskbaserat förhållningssätt där tekniska, organisatoriska och operativa åtgärder samverkar. Målsättningen är att successivt stärka förmågan att förebygga cyberangrepp, identifiera avvikelser och sårbarheter samt begränsa konsekvenserna om en incident inträffar.

Nuvarande status – kvartal 2 2026

Fortsatt utveckling av sårbarhetshanteringen

Arbetet med att identifiera och hantera tekniska sårbarheter har fortsatt under kvartalet. Den etablerade förmågan för både extern och intern sårbarhetsskanning ger en mer heltäckande bild av möjliga svagheter i IT-miljön och skapar bättre förutsättningar för att prioritera åtgärder utifrån risk.

Detta innebär en förflyttning från ett mer reaktivt arbetssätt till en mer systematisk och förebyggande hantering av sårbarheter. Resultaten från säkerhetskontroller och skanningar används som underlag för fortsatt riskbedömning och förbättring av den tekniska säkerheten.

Övervakning och detektionsförmåga

Den kontinuerliga säkerhetsövervakningen av Malmö stads IT-miljö har fortsatt under kvartalet. Genom säkerhetsövervakningen kan misstänkta aktiviteter och avvikande beteenden identifieras och analyseras för att tidigt upptäcka potentiella säkerhetshändelser.

Arbetet med att successivt förbättra tillgången till relevanta säkerhetsdata och loggar fortsätter. En bredare och mer sammanhållen övervakning förbättrar möjligheten att upptäcka komplexa angrepp och att snabbare skapa en samlad bild vid en säkerhetshändelse.

Den etablerade säkerhetsövervakningen utgör därmed en central del i Malmö stads förmåga att hantera den föränderliga cyberhotbilden.

Förstärkt skydd mot e-postrelaterade hot

E-post är fortsatt en av de vanligaste angreppsvägarna vid cyberangrepp. Under kvartalet har därför arbetet med att utvärdera ett förstärkt e-postskydd fortsatt.

Efter en inledande marknads- och produktutvärdering har två lösningar valts ut för en fördjupad Proof of Concept, Proofpoint och Abnormal Security. Lösningarna utvärderas parallellt och under jämförbara förutsättningar för att bedöma vilket alternativ som ger störst säkerhetsmässigt och operativt mervärde som komplement till det befintliga e-postskyddet.

Utvärderingen omfattar bland annat lösningarnas förmåga att identifiera avancerad nätfiske-e-post, bedrägeriförsök och andra typer av skadlig eller avvikande kommunikation som kan vara svår att upptäcka med traditionella säkerhetsmekanismer.

Resultatet av utvärderingen kommer att ligga till grund för den fortsatta inriktningen av Malmö stads e-postskydd.

Förberedelser inför cybersäkerhetslagen

Under kvartalet har arbetet med att analysera och förbereda IT-verksamheten inför den nya cybersäkerhetslagstiftningen fortsatt.

Arbetet omfattar bland annat en genomgång av befintliga processer, roller och arbetssätt i förhållande till de krav som följer av lagstiftningen. Särskild uppmärksamhet riktas mot områden såsom riskhantering, incidenthantering, kontinuitet, leverantörssäkerhet och uppföljning av säkerhetsåtgärder.

Parallellt med IT- och digitaliseringsavdelningens arbete har enheten för säkerhet och beredskap vid Stadskontoret tillsammans med IT- och digitaliseringsavdelningen tagit fram en gemensam plan för arbetet med den nya cybersäkerhetslagstiftningen.

En översyn av incident- och incidentrapporteringsprocesserna pågår också. Syftet är bland annat att säkerställa tydliga roller, ansvar, informationsflöden och arbetssätt för att kunna möta de krav på rapportering och hantering som följer av den nya lagstiftningen.

Förberedelser inför valåret 2026

Med anledning av det allmänna valet 2026 pågår även ett förstärkt säkerhetsarbete kopplat till den förändrade riskbild som kan uppstå inför och under valperioden.

Arbetet bedrivs riskbaserat och är en del av den samlade säkerhetsplaneringen. Fokus ligger på att säkerställa god beredskap och förmåga att upptäcka och hantera eventuella cyberrelaterade händelser som kan påverka Malmö stads digitala miljö.