Stockholms stad

Ledningens genomgång

2026

start.stockholm

Innehåll

Inledning

Denna rapport utgör Ledningens genomgång 2026 för både det stadsövergripande informationssäkerhetsarbetet och stadsledningskontorets (SLK) interna arbete som förvaltning. Syftet med genomgången är att ge en samlad och aktuell bild av nuläget samt att identifiera behov av förbättringar inför kommande år.

Ledningens genomgång är en central del av stadens ledningssystem för informationssäkerhet (LIS). Genomgången ska säkerställa att LIS är lämpligt, tillräckligt och verksamt i förhållande till stadens uppdrag, risker och omvärld, samt föreslå nödvändiga justeringar.

Enligt stadens tillämpningsanvisning ska genomgången genomföras både på stadsövergripande nivå och på respektive nämnd och bolag. Underlaget bygger på uppföljningar, GDPR-årsrapport, omvärldsbevakning samt inträffade händelser och incidenter.

Resultatet ligger till grund för förslag på övergripande inriktningar inför kommande år. Hur dessa inriktningar omsätts i aktiviteter och resursplanering sker inom ramen för det ordinarie linjearbetet.

Omvärldsbevakning

Stadens informationssäkerhetsarbete påverkas i hög grad av utvecklingen i omvärlden. Nya lagkrav, ett förändrat säkerhetsläge och ett mer komplext tekniskt landskap medför ökade krav på styrning, samordning och förmåga till anpassning. Omvärldsbevakningen visar särskilt på behovet av fortsatt integration mellan informationssäkerhet, beredskap och kontinuitet, samt ett stärkt fokus på det tekniska cybersäkerhetsarbetet.

Skärpta krav på informationssäkerhet

Regeringen har under året presenterat sin proposition om en ny cybersäkerhetslag, som förväntas träda i kraft den 15 januari 2026. Lagen genomför NIS2-direktivet i svensk rätt och innebär att fler verksamheter omfattas av tydligare krav på systematiskt informationssäkerhetsarbete, incidentrapportering och leverantörsstyrning. Det innebär att arbetet med informations-säkerhet behöver stärkas i hela stadens verksamhet, från upphandling av it-tjänster till rekrytering av personal.

Parallellt utvecklas det civila försvaret, där informationssäkerhet är en grundläggande förmåga för att upprätthålla samhällsviktig verksamhet under störningar och kriser. Den nationella cybersäkerhetsstrategi som antogs 2025 betonar högre krav på robusthet, beredskap och uthållighet i samhället.

Sammantaget innebär dessa förändringar att stadens informationssäkerhetsarbete behöver möta nya krav, säkerställa kontinuitet och stärka förmågan att hantera både risker och oönskade störningar.

Förhöjd och mer komplex hotbild

Cyberhoten fortsätter att utvecklas och risken för mer uthålliga och koordinerade angrepp ökar. Angripare utnyttjar i högre grad tekniska brister och digitala beroenden. Ransomware är fortsatt ett framträdande hot, med mer professionella och decentraliserade aktörer som kombinerar tekniska intrång med olika former av utpressning. Parallellt pågår långsiktiga intrångs- och informationsinhämtningskampanjer från aktörer med politiska eller strategiska motiv, ofta riktade mot verksamhetskritiska funktioner och digital infrastruktur.

Nätfiske[1] är fortsatt den vanligaste vägen in i system, och angreppen blir mer trovärdiga genom automatisering och användning av AI. Angripare utnyttjar också i allt högre grad tekniska brister i programvara och tjänster. Samtidigt ökar riskerna kopplade till leverantörskedjor och tredjepartsberoenden, där ett intrång hos en extern part kan få omfattande påverkan. Även mobiltelefoner och andra enheter som används i det dagliga arbetet utgör en växande angreppsyta.

Överbelastningsattacker är ytterligare ett hot där offentlig sektor är särskilt utsatt (ENISA, *Threat Landscape 2025*[2]). Det syftar till att störa stabiliteten och tillgången till olika tjänster samt att påverka opinionen. Parallellt bedrivs mer riktade intrångsförsök av aktörer som söker åtkomst och långsiktig närvaro i it-system.

Sammantaget innebär utvecklingen att arbetet med informationssäkerhet i högre grad behöver fokusera på motståndskraft, tidig upptäckt och kontinuerlig uppföljning. Det handlar om att stärka organisationens förmåga att hantera ett mer långvarigt och sammansatt hotläge, snarare än att enbart förebygga enskilda incidenter.

[1] Nätfiske är en form av social manipulation där bedragare försöker lura mottagare att lämna ut lösenord, kreditkortsnummer eller annan känslig information.

[2] ENISA är EU:s cybersäkerhetsbyrå med uppdrag att bland annat analysera framväxande risker, framför allt på europeisk nivå och bidra till större medvetenhet om informationssäkerhet.

Fortsatt högt tempo i den tekniska utvecklingen

Den tekniska utvecklingen fortsätter att drivas av snabb digitalisering, ökad molnanvändning och mer sammanlänkade systemmiljöer. Det ger nya möjligheter till effektivisering och innovation, men gör det samtidigt svårare att överblicka vilka beroenden som finns. Förändringar sker i allt högre tempo, vilket ställer krav på att säkerhetsaspekter integreras tidigt och konsekvent i utveckling, upphandling och införande av nya it-lösningar.

Användningen av AI ökar snabbt och skapar möjligheter till ökad kapacitet och effektivare arbetsflöden. Samtidigt finns det risker. Om informationen som används i systemen inte är korrekt kan resultaten bli fel. Det kan också vara svårt att förstå hur modellerna fungerar och därför kvalitetssäkra svar. Dessutom ökar risken för att känslig information hanteras eller delas på fel sätt. Den växande tillgängligheten till generativ AI och syntetisk media gör dessutom att bedrägerier och påverkansförsök kan genomföras mer trovärdigt och i större skala. Exempel på detta är förekomst av bluffakturor, falska telefonsamtal eller spridning av bilder med falskt innehåll.

Utvecklingen inom kvantdatorer är fortfarande i ett tidigt skede men kan på sikt påverka dagens kryptografiska skydd. Det kräver att staden följer utvecklingen och långsiktigt planerar för kvanttåliga lösningar.

Säkerhet i leveranskedjan blir allt viktigare

Cyberangrepp sker allt oftare via leverantörer och externa tjänster**.** Genom att angripa en aktör i leveranskedjan kan en angripare få stor effekt och påverka många verksamheter samtidigt. I takt med att staden använder fler molntjänster, externa system och delade digitala plattformar blir beroendena fler och svårare att överblicka, vilket gör att en incident hos en leverantör snabbt kan få konsekvenser för stadens verksamhet och information. Både utvecklingen och den nya cybersäkerhetslagen innebär att informationssäkerhet behöver omfatta hela leveranskedjan – med högre krav på avtal, insyn, uppföljning och samordning än tidigare.

Stadsövergripande genomgång

Det stadsövergripande arbetet med informationssäkerhet vilar på en stabil grund. Staden har ett etablerat ledningssystem för informationssäkerhet (LIS), som har utvecklats stegvis under flera år och som fortsatt anpassas efter nya krav och behov. Jämfört med många andra offentliga organisationer har staden kommit långt.

För att bibehålla och stärka stadens förmåga ytterligare behöver arbetet fortsätta utvecklas. Detta återspeglas även i stadens budget för 2026, där ökade satsningar görs på informations- och cybersäkerhet.

Under 2025 har arbetet med det stadsövergripande informationssäkerhetsarbetet präglats av förberedelser inför cybersäkerhetslagens ikraftträdande, vidareutveckling av it-säkerhetsområdet samt en förstudie kring bättre systemstöd för informationssäkerhetsarbetet i staden. Samtliga delar kommer att fortsätta utvecklas under 2026. Den personuppgiftsincident som drabbade staden och många andra aktörer i Sverige tog stort fokus under framför allt september och visade på stadens förmåga att mobilisera och agera samlat. Som en följd av incidenten har flera riktade insatser inletts 2025 och som fortsätter för att ytterligare stärka säkerhetsarbetet under 2026.

Följande åtgärder föreslås för att säkerställa att LIS är ändamålsenligt, tillräckligt och får verkan i hela staden:

- **Fortsätta anpassningen till cybersäkerhetslagen**
  Stadens LIS behöver anpassas för att uppfylla de krav som följer av den kommande cybersäkerhetslagen. Det innebär bland annat att genomföra åtgärder för att säkerställa ändamålsenligt stöd, ett förstärkt riskbaserat arbetssätt, en höjd teknisk säkerhetsnivå samt tydliga roller, ansvar och rapporteringsvägar.

- **Utveckla och stärka incidenthanteringsprocessen**
  Stadens nuvarande incidenthantering kan stärkas ytterligare. Arbetet innebär att stärka förmågan att upptäcka, hantera och återhämta sig från incidenter på ett mer samordnat och effektivt sätt. Detta omfattar bland annat att tydliggöra roller och ansvar vid störningar som inte kräver förstärkt beredskap eller central krisledning, uppdatera rutiner och eskaleringsvägar samt öka övningsverksamheten.

- **Fortsätta utveckla och stärka it-säkerheten**
  Stadens arbete med att stärka IT-säkerheten behöver fortsätta och fördjupas för att möta ett föränderligt hotlandskap. Arbetet innebär att utveckla styrningen av IT-

säkerhetsarbetet och öka stadens motståndskraft genom ett systematiskt arbete med åtgärder som förebygger cyberangrepp. Detta omfattar bland annat vidareutveckling av IT-säkerhetsarkitekturen och tillhörande ramverk för praktisk tillämpning.

- **Införa systemstöd för informationssäkerhetsarbetet**
  Fortsätta det påbörjade arbetet med utökad användning av ILS för att få ett bättre stöd i arbetet med informationssäkerhet, särskilt vad gäller systematisk och dokumentation av informationsklassning, riskhantering och uppföljning.

- **Utveckla arbetssätt för uppföljning**
  Det finns etablerade arbetssätt för uppföljning av informationssäkerhet i staden, men dessa behöver ses över och vidareutvecklas. Arbetet syftar dels till att utveckla arbetssätt för att utvärdera effektivitet i säkerhetsåtgärder inom cybersäkerhet, dels till att möta ett ökat behov av exempelvis lägesbilder och bättre underlag för styrning, prioriteringar och beslut.

Arbetet genomförs av säkerhetsavdelningen, enheten för säkerhetsskydd och informationssäkerhet. Samarbete sker med andra avdelningar på stadsledningskontoret, S:t Erik Kommunikation och den nyetablerade Computer Emergency Response Team (CERT) samt med övriga förvaltningar och bolag.

Stadsledningskontorets genomgång

Stadsledningskontoret (SLK) ska som kommunstyrelsens förvaltning följa de program, riktlinjer och tillämpningsanvisningar som är beslutade för informationssäkerhet i staden. SLK:s arbete för informationssäkerhet är komplext då det lokala arbetet på stadsledningskontoret ofta innebär ett stadsövergripande perspektiv, inte minst när det kommer till de centrala it-miljöerna.

Med syfte att skapa bättre helhetssyn har stadsledningskontoret omorganiserats, där det lokala och stadsövergripande informationssäkerhetsarbetet har sammanfogats på säkerhetsavdelningen. Genomgången nedan överlappar i vissa delar det stadsövergripande perspektivet, vilket är nödvändigt för att säkerställa att samtliga perspektiv inom SLK omhändertas.

SLK har etablerat en grund för arbetet med informationssäkerhet genom en lokal anvisning för informationssäkerhet som beslutades hösten 2023. Den lokala anvisningen anger roller, ansvar och arbetssätt för informationssäkerhet och har möjliggjort ett mer systematiskt arbete i linjeorganisationen. SLK har genomfört informationsklassningar för sina it-tjänster och har etablerade arbetssätt för uppföljning.

Den personuppgiftsincident som uppstod under hösten 2025 innebar ett stort fokus på incidenthantering under september och har resulterat i flera riktade insatser. Bland annat har ett projekt inletts för att genomlysa personuppgiftshanteringen i samtliga it-tjänster som SLK ansvarar för. SLK har en särskild roll i och med att kontoret förvaltar stadsgemensamma it-tjänster som används av samtliga förvaltningar och bolag. Detta innebär betydande beroenden och ställer krav på transparens, särskilt vad gäller informationsklassning och personuppgiftsansvar.

För att säkerställa att informationssäkerhetsarbetet är ändamålsenligt, tillräckligt och ger effekt i linjeorganisationen föreslås att stadsledningskontoret under 2026 prioriterar följande:

- **Stärka den lokala styrningen av informationssäkerhet**
  Löpande etablera nya arbetssätt mellan säkerhetsavdelningen och övriga avdelningar i informationssäkerhetsarbetet samt uppdatera och utveckla den lokala anvisningen för informationssäkerhet så att den fortsatt är tydlig, aktuell och stödjer ett samordnat arbetssätt inom SLK. Vid behov kan även särskilda rutiner behöva upprättas.

- **Anpassa SLK:s arbete till cybersäkerhetslagen**
  SLK:s arbetssätt behöver förberedas för den kommande cybersäkerhetslagen samt CER-direktivet, med fokus på styrning, rapportering och riskhantering. Områden som särskilt berörs av kraven är inköp och upphandling, personalfrågor, systemutveckling och förvaltning av centrala it-tjänster.

- **Stärka säkerheten i centrala it-tjänster**
  För att säkerställa ett robust och säkert it-stöd behöver säkerheten i de centrala it-tjänsterna höjas. Detta innebär att praktiska säkerhetsåtgärder behöver genomföras och följas upp samordnat inom SLK.

- **Stärka personuppgiftshanteringen inom SLK**
  För att utveckla och stärka dataskyddet behöver både tekniska och organisatoriska säkerhetsåtgärder vidtas. Det innefattar bland annat att registerförteckningen ses över och hålls aktuell, samt att ansvar, instruktioner och rutiner för personuppgiftshanteringen förtydligas och etableras för respektive centralt objekt. Detta skapar förutsättningar för en enhetlig och säker hantering av personuppgifter inom SLK.