Kommunstyrelsen

2026-03-15
TJÄNSTESKRIVELSE
Dnr: KFKS-2026-00063

Medel för cybersäkerhet

Förslag till beslut

Kommunstyrelsens arbetsutskott föreslår att kommunstyrelsen fattar följande beslut.

1. Kommunstyrelsen beslutar att tilldela 1,5 miljoner kronor för insatser inom cybersäkerhet i enlighet med tjänsteskrivelse daterad den 15 mars 2026.

2. Kommunstyrelsen beslutar att kostnaden för insatser inom cybersäkerhet, 1,5 miljoner kronor, finansieras ur kommunstyrelsens budget för oförutsett.

Sammanfattning av ärendet

Den 15 januari 2026 trädde den nya cybersäkerhetslagen (2015:1506) i kraft med syfte att höja cybersäkerheten i samhällskritiska sektorer. För att öka den offentliga förvaltningens motståndskraft mot cybersäkerhetsincidenter och cyberhot har regeringen avsatt 600 miljoner kronor i generella stadsbidrag till Sveriges kommuner över tre år med start 2026.

Nacka kommun har under flera år arbetat strukturerat med att stärka kommunens informations- och cybersäkerhet, men fler insatser behövs under kommande år kopplad till den nya cybersäkerhetslagen och det försämrade omvärldsläget.

De 1,5 miljoner kronor som föreslås tillföras under 2026 avser insatser för att genomföra ett införandeprojekt, ett incidenthanteringsprojekt och implementering av ett säkerhetsobjekt. Det syftar till att ytterligare stärka kommunens informations- och cybersäkerhetsarbete i enlighet med intentionerna i den nya cybersäkerhetslagen.

Ärendet

Bakgrund

Den ökade digitaliseringen i samhället och ett allvarligare omvärldsläge ställer högre krav på säkerhet i verksamhetsutövares digitala miljöer. Viktiga samhällsaktörer såsom myndigheter, kommuner och regioner är en allt större måltavla för cyberangrepp. Flera kommuner har också blivit utsatta och även leverantörer till kommunerna har drabbats av cyberattacker. Attackerna har ibland orsakat stor skada på de utsatta kommunernas förmåga att utföra sitt uppdrag.

Nacka kommun har under flera år arbetat strukturerat med att stärka kommunens informations- och cybersäkerhet. Insatserna tar sin utgångspunkt i kommunens digitaliseringsstrategi, informationssäkerhetsstrategi och utifrån resultatet i Cybersäkerhetskollen[1]. Särskilt har insatser genomförts inom informationsklassning, objektsförvaltning, övergripande samordning av digitala projekt, omvärldsbevakning, systematisk riskhantering, dataövervakning, stöd- och utbildningsinsatser riktad mot kommunens personal, lösenordshantering och skärpta krav vid IT-upphandlingar.

Den 15 januari 2026 trädde den nya cybersäkerhetslagen (2025:1506) i kraft vilken implementerar EU:s NIS2-direktiv med syfte att höja cybersäkerheten i samhällskritiska sektorer genom striktare krav på riskhantering, säkerhetsåtgärder och ledningsansvar. Nästan hela den offentliga sektorn, inklusive kommuner, omfattas nu av skärpta krav på cybersäkerhet för att skydda samhällsviktiga verksamheter.

Lagen ersätter den äldre NIS-lagen (som för Nacka endast omfattade verksamhet med journalföring, till exempel elevhälsan) och skärper kraven på både offentliga och privata aktörer med tydligare skyldigheter för att stärka motståndskraften mot cyberhot, till exempel högre krav på riskanalyser och specifika säkerhetsåtgärder. Länsstyrelsen i Stockholm är tillsynsmyndighet för länets kommuner avseende efterlevnad av den nya lagstiftningen.

Ledningen i en kommun bär enligt nya cybersäkerhetslagen ett tydligt ansvar för cybersäkerhetsarbetet, inklusive utbildning och kontroll av åtgärder. Målet är att säkerställa att digitala system inom äldreomsorg, avfallshantering, skola och annan kommunal service är robusta och inte enkelt slås ut vid cyberattacker eller att känslig information i systemen går förlorad eller blir tillgänglig för obehöriga. Den nya cybersäkerhetslagen innebär att kommuner måste gå från en mer reaktiv hållning till ett proaktivt och systematiskt säkerhetsarbete för att stärka motståndskraften i kritiska digitala infrastrukturer.

Vidare innebär den nya cybersäkerhetslagen att verksamhetsutövare själva ska identifiera om man omfattas av lagen och skyldighet att självmant anmäla detta till aktuell tillsynsmyndighet. Utifrån genomförd analys anmälde Nacka att kommunen omfattas av lagen den 3 februari.

För att öka den offentliga förvaltningens motståndskraft mot cybersäkerhetsincidenter och cyberhot har regeringen avsatt 600 miljoner kronor i generella stadsbidrag till Sveriges kommuner över tre år med start 2026. För Nacka kommun innebär detta cirka 2,1 miljoner kronor i ökade generella stadsbidrag.

[1] Med hjälp av Cybersäkerhetskollen kan organisationer mäta nivån på sitt systematiska cybersäkerhetsarbete samt få stöd för förbättringsarbete. I Cybersäkerhetskollen ingår Infosäkkollen, It-säkkollen, Ot-säkkollen och Leveranskedjekollen. Verktyget har tagits fram mot bakgrund av uppdrag från regeringen och tillhandahålls av Myndigheten för civilt försvar.

Säkerhetsenhetens och digitaliseringsenhetens utredning och bedömning

Den nya svenska cybersäkerhetslagen trädde i kraft den 15 januari 2026 och innebär skärpta krav på att offentlig förvaltning bedriver ett systematiskt informations- och cybersäkerhetsarbete. Kommuner måste nu genomföra grundliga riskanalyser, implementera robusta säkerhetsåtgärder, rapportera incidenter, följa upp arbetet inom cybersäkerhet och utbilda ledning och personal.

Medlen bör användas där de ger störst effekt: att stärka grundskyddet, förbättra incidentberedskapen och förbereda organisationen för krav enligt NIS2 och den nya cybersäkerhetslagen.

Implementering av cybersäkerhetslagen i Nacka kommun

Utifrån den nya lagstiftningen tillsattes i höstas en förstudie med medarbetare från digitaliseringsenheten, säkerhetsenheten och juridik- och kanslienheten. Syftet var att klarlägga hur Nacka kommuns verksamheter kan förberedas för den nya cybersäkerhetslagen som trädde i kraft den 15 januari 2026.

Inom ramen för förstudien har en övergripande gapanalys genomförts som resulterat i ett antal konkreta rekommendationer, en handlingsplan och en utvärderingsplan för kommunens fortsatta arbete med cybersäkerhet, se bilaga 1. Resultatet är ett strukturerat underlag för hur kommunen kan organisera införandet och arbeta för att uppfylla lagkraven, inklusive ett förslag om två parallella projekt: ett införandeprojekt och ett incidenthanteringsprojekt. Totalt kostnad för dessa båda projekt är 1,2 miljoner kronor år 2026, se bilaga 2.

Införandeprojekt

Införandeprojektet syftar till att stärka Nacka kommuns arbete med att uppfylla kraven i den nya cybersäkerhetslagen och NIS2-direktivet. Det innebär att kommunen behöver stärka styrning, uppföljning och dokumentation av sitt systematiska informations- och cybersäkerhetsarbete, tydliggöra roller och ansvar samt införa och formalisera ett antal organisatoriska och tekniska säkerhetsåtgärder.

Arbetet omfattar såväl kommunstyrelsens verksamhet som den samlade kommun-organisationen, eftersom ansvaret enligt lag ligger på kommunen som juridisk person. Om organisationen brister i att uppfylla kraven kan det leda till förelägganden och sanktionsavgifter, det är verksamhetsutövaren som bär det formella ansvaret. Om ledningen brister i sitt utpekade särskilda ansvar gällande ledning och styrning av cybersäkerheten kan sådana brister också bli föremål för ingripanden. Kommunen ansvarar i lagens mening, men ledningen måste aktivt säkerställa att kommunen faktiskt uppfyller kraven.

Genom införandet minskar risken för allvarliga störningar, rättsliga konsekvenser och förtroendeskador, samtidigt som kommunens förmåga att leverera stabil och säker service till Nackaborna stärks även vid störningar eller angrepp.

Införandet omfattar i praktiken att ta fram och besluta nya eller reviderade styrdokument, etablera en tydlig kommunövergripande struktur för riskanalyser och informationsklassning samt genomföra fördjupade analyser av kommunens mest kritiska system och leverantörer. Arbetet innebär även att definiera och formalisera roller och ansvar på ledningsnivå, införa rutiner för uppföljning och intern kontroll samt säkerställa att krav på rapportering och anmälningsplikt kan uppfyllas inom föreskriven tid. Parallellt genomförs kompetenshöjande insatser för chefer och nyckelroller, så att kraven inte bara dokumenteras utan också omsätts i praktiken. Sammantaget leder aktiviteterna till att kommunen går från ett delvis informellt och personberoende arbetssätt till en strukturerad, spårbar och regelbaserad styrning av cybersäkerhetsarbetet.

Incidenthanteringsprojekt

En strukturerad incidenthanteringsprocess är en grundförutsättning för att snabbt kunna upptäcka, rapportera, hantera och följa upp IT- och informationssäkerhetsincidenter. I dag finns delar av detta arbete, men processen behöver bli tydligare, mer sammanhållen och känd i hela organisationen. Genom att införa en gemensam och dokumenterad process med definierade roller, ansvar och rapporteringsvägar säkerställs att incidenter hanteras på ett enhetligt och effektivt sätt. Det minskar risken för konsekvenserna vid intrång eller störningar, förbättrar lärandet över tid och ger ledningen bättre underlag för prioriteringar och riskreducerande åtgärder.

Cybersäkerhetslagen kräver att den första inledande incidentrapporteringen sker inom 24 timmar och därefter ytterligare rapportering efter 72 timmar och 30 dagar. Tydliga processer, rutiner, definierade roller med ansvar och strukturerad dokumentation behövs för att säkerställa efterlevnad. En incidenthanteringsprocess ska även inkludera hantering av krav på incidentrapportering enligt GDPR, Dataskyddslag, Patientdatalag eller liknande. Detta är en blandning av EU-regleringar, svenska lagar och eventuella föreskrifter därav används samlingsbegreppet ”externa regelverk

Arbetet med att införa incidenthanteringsprocessen innebär i praktiken att kartlägga nuvarande arbetssätt, definiera ett gemensamt flöde från upptäckt till avslut, samt fastställa tydliga roller, beslutsvägar och eskaleringsnivåer. Processen ska integreras med befintliga IT- och säkerhetsfunktioner samt kompletteras med stöd för dokumentation, rapportering och analys. Det ingår även att ta fram mallar och stödmaterial, genomföra övningar samt säkerställa att incidenter kan rapporteras till berörda myndigheter inom lagstadgade tidsramar. Genom detta skapas en praktiskt fungerande förmåga att snabbt begränsa skador, återställa verksamhet och dra lärdom av inträffade händelser.

Implementering av säkerhetsobjekt

I nuläget saknas ett objekt för att samla kommunens säkerhetsrelaterade system och lösningar under ett och samma paraply.

För att säkerställa långsiktig, strukturerad och kostnadseffektiv förvaltning av kommunens säkerhetsrelaterade IT-komponenter etableras ett samlat objekt för säkerhet enligt kommunens modell för objektstyrd systemförvaltning. Genom att samla system och tjänster som stödjer informations- och säkerhetsprocesserna i ett gemensamt objekt tydliggörs ansvar, prioriteringar och uppföljning. Det minskar personberoende, stärker leverantörsstyrningen och skapar bättre förutsättningar för kontinuerlig utveckling i takt med förändrade lagkrav och hotbilder.

Objektförvaltningen säkerställer att digitala säkerhetslösningar inte bara införs, utan också hålls aktuella, används rätt och ger avsedd effekt över tid. Införandet av en kommungemensam förvaltningsmodell grundar sig i digitaliseringsstrategin som beslutades av kommunfullmäktige i april 2019 (KFKS 2018/1151). Strategin förespråkar en gemensam och transparent systemförvaltning via objektförvaltning.

Objektsförvaltning är viktig eftersom den:

- **Säkerställer kontinuitet i samhällsservicen** – exempelvis inom skola, äldreomsorg och socialtjänst.
- **Möjliggör långsiktig utveckling** – systemen måste kunna anpassas till förändrade lagkrav, nya arbetssätt och ökade volymer.
- **Minskar sårbarhet och personberoende** – gemensamma arbetssätt och dokumentation gör att verksamheten inte blir beroende av enskilda individer.
- **Bidrar till trygg informationshantering** – korrekt förvaltning är en förutsättning för informations- och IT-säkerhet.

Objektsförvaltning innebär således ett strukturerat och enhetligt arbetssätt för hantering, förvaltning och utveckling av system och informationstillgångar. Exempel på objekt som redan är etablerade i kommunen är ekonomi, ledning och styrning samt personal.

Det finns idag ingen budget för att finansiera etableringen av ett säkerhetsobjekt. Avsaknaden av ett säkerhetsobjekt medför en risk att flera system inom säkerhets-området som införts eller kommer att införas inte omhändertas på ett adekvat sätt. Kostnaden för att etablera ett säkerhetsobjekt på en miniminivå är cirka 300 000 kr. I kostnaden ingår 25% av en heltidstjänst från digitaliseringsenheten i form av rollen som objektledare IT som, i stöd av kommunens metodstöd för objektförvaltning, säkerställer robusthet, tillgänglighet och utveckling av objektets alla IT-system. Det innebär i praktiken prioriterat arbete med IT-säkerhet och informationssäkerhet, leverantörs- och

avtalsuppföljning, framtagandet av förvaltnings- och utvecklingsplan med ekonomiska förutsättningar samt intressentbevakning och kravställning med mera.

Den årliga kostnaden för ett fullt utvecklat arbete med förvaltning av säkerhetsobjektet uppgår till cirka 1 miljon kronor där huvuddelen är interndebiterad tid. Medel för årlig förvaltning av säkerhetsobjektet kommer att föreslås inom ramen för kommunens kommande budgetprocess.

Ekonomiska konsekvenser

Förslag till beslut minskar utrymmet i kommunstyrelsens medel för oförutsett med 1,5 miljoner kronor. Nacka kommun har erhållit generella stadsbidrag för arbetet med cybersäkerhet för att kunna arbeta för att uppnå intentionerna i den nya cybersäkerhetslagen motsvarande cirka 2,1 miljoner kronor. De projekt som medlen avser att finansiera ryms inte inom ordinarie budget.

Konsekvenser för barn

En säker driftsmiljö för kommunens centrala system, särskilt kopplat till skolans värld, är en grundförutsättning för verksamhetens funktionalitet. Vid större driftsavbrott eller cyberattacker kan de kommunala skolorna vara tvungna att övergå till manuella rutiner vilket kan påverka utbildningens kvalitet och elevernas trygghet på ett negativt sätt.

Konsekvenser för klimat och miljö

Beslutet innebär inga särskilda konsekvenser för klimat och miljö.

Handlingar i ärendet

Tjänsteskrivelse daterad den 15 mars 2026
Bilaga 1. Införande av cybersäkerhetslagen och NIS2 i Nacka kommun
Bilaga 2. Estimat över resurs- och finansieringsbehov

Henrik Ahl
Säkerhetsdirektör
Stadsledningskontoret

Henrik Palmblad Wennergren
Digitaliseringsdirektör
Stadsledningskontoret

Beslutet ska skickas till:

- -