

Handläggare
Sonia Siropian
08-508 26 340**Till**
Trafiknämnden
2025-04-24

Transportstyrelsens tillsyn av trafikkontoret avseende säkerhetsåtgärder enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen)

Förslag till beslut

1. Trafiknämnden godkänner trafikkontorets redovisning och uppdrar åt kontoret att redovisa uppföljningen av åtgärdsplanen för nämnden årligen till och med 2027.

Gunilla Glantz
FörvaltningschefPhilip Hall
AvdelningschefPeter Granström
Avdelningschef

Sammanfattning

NIS-direktivet (Network and Information Security Directive) är ett EU-direktiv som syftar till att höja säkerheten för nätverk och informationssystem inom samhällsviktiga sektorer i medlemsstaterna. Transportstyrelsen, som är tillsynsmyndighet inom transportsektorn, inledde i februari 2024 en tillsyn av trafikkontoret enligt den svenska NIS-lagen. Granskningen omfattade säkerhetsåtgärder som bl.a. inventering och förteckning av nätverk och informationssystem, omvärldsbevakning för att identifiera hot, risk- och sårbarhetsanalys samt åtgärdsplan. Transportstyrelsen bedömde att trafikkontoret delvis uppfyller kraven, vilket resulterade i en sanktionsavgift på 1 350 000 kronor samt ett föreläggande om att åtgärda brister.

Trafikkontoret
VerksamhetsstödFleminggatan 4
Box 8311
104 20 Stockholm
Telefon 08-508 26 340
Växel 08-508 27 200
sonia.sirobian@stockholm.se
trafikkontoret@stockholm.se
Org nr 212000-0142
start.stockholm

Trafikkontoret ser allvarligt på de brister som Transportstyrelsens tillsyn har belyst i kontorets arbete och beklagar både de brister som identifierats och den sanktionsavgift som kommer att tas ut. Som svar på tillsynen har trafikkontoret tagit fram en åtgärdsplan som ska genomföras i projektform fram till 2027 med tidsatta åtgärder för att uppfylla kraven. Trafikkontoret har redan påbörjat flera åtgärder och bedömer att planen kommer att stärka informations-säkerheten, förbättra det systematiska arbetet och säkerställa efterlevnad av NIS-direktivet. Kontoret föreslår att nämnden godkänner redovisningen av tillsynen och beslutar om en årlig uppföljning av åtgärdsplanen.

Bakgrund

NIS-direktivet (Network and Information Security Directive) är ett EU-direktiv som syftar till att höja säkerheten för nätverk och informationssystem inom medlemsstaterna. Direktivet ställer krav på kritiska aktörer inom samhällsviktiga sektorer att införa robusta säkerhetsåtgärder och rapportera allvarliga incidenter. Genom detta vill EU stärka cybersäkerheten och öka beredskapen mot cyberhot på europeisk nivå.

Det finns sex tillsynsmyndigheter som utövar tillsyn av NIS-direktivet i Sverige inom sju sektorer. Tjänster som omfattas av NIS-direktivet delas in i samhällsviktiga tjänster och digitala tjänster. Den som inom ramen för NIS-regleringen identifierat sig som en leverantör av en samhällsviktig tjänst ska anmäla det till berörd tillsynsmyndighet. Transportstyrelsen är tillsynsmyndighet inom sektorn transport och trafikkontoret har sedan 2018 anmält sig som leverantör av en samhällsviktig tjänst inom sektorn. I mars 2022 utkom Transportstyrelsen med föreskrifter och allmänna råd om säkerhetsåtgärder för leverantörer av samhällsviktiga tjänster inom transportsektorn.

Transportstyrelsen meddelade den 5 februari 2024 att en tillsyn inleds av trafikkontoret enligt lagen (2018:1174) om informations-säkerhet för samhällsviktiga och digitala tjänster (NIS-lagen) och utgör en del av myndighetens generella tillsyn inom transportsektorn. Syftet med tillsynen är att verifiera att verksamheten bedrivs i enlighet med gällande förordningar, föreskrifter och av organisationen fastställda anvisningar och rutiner.

Tillsynen genomfördes som en revision den 30 maj 2024 och rör säkerhetsåtgärderna 6-11 §§ i Transportstyrelsens föreskrifter och allmänna råd TSFS 2022:14. Dessa paragrafer inkluderar:

Trafikkontoret
Verksamhetsstöd

Fleminggatan 4
Box 8311
104 20 Stockholm
Telefon 08-508 26 340
Växel 08-508 27 200
sonia.sirobian@stockholm.se
trafikkontoret@stockholm.se
Org nr 212000-0142
start.stockholm

- Inventering av nätverk och informationssystem
- Upprättad förteckning över informationstillgångar utifrån genomförd inventering
- Omvärldsbevakning för att identifiera hot och sårbarheter
- Risk- och sårbarhetsanalys som utgår från förteckningen, omvärldsanalysen, identifierade sårbarheter och incidenter
- Åtgärdsplan där det bl.a. framgår vilka nätverk och informationssystem som åtgärderna avser samt vilka risker som motverkas
- Interna regler och arbetssätt för uppföljning och analys av vidtagna säkerhetsåtgärders effektivitet.

Transportstyrelsens sammantagna bedömning är att trafikkontoret delvis uppfyller de grundläggande kraven i Transportstyrelsens föreskrifter om säkerhetsåtgärder. Transportstyrelsen ser positivt på att trafikkontoret har påbörjat ett strukturerat arbete med att omhänderta gällande lagstiftning och har förståelse för utvecklings- och samordningsbehov framåt, dock har trafikkontoret inte fullt ut implementerat de krav som omfattas av tillsynen.

Den 21 oktober 2024 meddelade Transportstyrelsen att myndigheten enligt gällande lagstiftning ska ta ut en sanktionsavgift om 1 350 000 kronor och ett föreläggande med anmodan om att trafikkontoret ska omhänderta identifierade brister och upprätta en åtgärdsplan. I bedömningen tog myndigheten hänsyn till trafikkontorets omsättning samt konstaterade att kontoret inte har några tidigare överträdelser av samma typ. Trafikkontoret svarade Transportstyrelsen den 20 november 2024 med en åtgärdsplan för de åtgärder som kommer att vidtas för att hantera respektive brist, se bilaga 2. Därefter följde en fortsatt dialog med Transportstyrelsen för att utveckla och tydliggöra delar av åtgärdsplanen. Den 28 februari mottog trafikkontoret en underrättelse från Transportstyrelsen med den slutgiltiga bedömningen och myndighetens beslut om sanktionsavgift. Sanktionsavgiften kommer att belasta kontorets driftbudget under 2025 och kontoret har tagit höjd för detta i sin budgetering.

Ärendets beredning

Ärendet har beretts inom trafikkontoret.

Trafikkontorets synpunkter

För att upprätthålla och utveckla de olika funktionerna i stadens offentliga rum krävs många tekniska system som hanterar stora

Trafikkontoret
Verksamhetsstöd

Fleminggatan 4
Box 8311
104 20 Stockholm
Telefon 08-508 26 340
Växel 08-508 27 200
sonia.sirobian@stockholm.se
trafikkontoret@stockholm.se
Org nr 212000-0142
start.stockholm

mängder information. Dessa informationsmängder har vuxit snabbt i takt med den tekniska utvecklingen och med det tillkommer nya utmaningar och risker. För att värna om informationssäkerheten har lagstiftningen skärpts t.ex. genom dataskyddsförordningen och NIS-direktivet.

Sedan NIS-direktivet började gälla har trafikkontoret arbetat med att tolka och implementera lagstiftningen inom ramen för kontorets verksamhet. Kontoret har arbetat för att anpassa och utveckla verksamheten i enlighet med lagstiftningen och kan konstatera att det finns förbättringsområden och att den praktiska tillämpningen av lagen har behövt utvecklas över tid.

Trafikkontoret ser allvarligt på de brister som Transportstyrelsens tillsyn har belyst i kontorets arbete med att uppfylla kraven enligt NIS-direktivet. Kontoret beklagar både de brister som identifierats och den sanktionsavgift som kommer att tas ut. Samtidigt ser kontoret tillsynen som en värdefull möjlighet att tydligt identifiera utvecklingsområden och stärka kontorets arbete med informations- och cybersäkerhet framåt. Genom att åtgärda dessa brister har kontoret möjlighet att inte bara efterleva regelverket, utan också höja säkerheten i verksamheten på ett långsiktigt och hållbart sätt.

Trafikkontoret har tagit fram en åtgärdsplan som Transportstyrelsen har godkänt som svar på genomförd tillsyn. Planen kommer att genomföras i projektform till och med 2027, se kontorets svar på tillsynsrapporten i bilaga 2. Åtgärderna som ska genomföras i projektet är tidsatta och träffar samtliga krav 6-11 §§ och är direkt kopplade till de identifierade bristerna i tillsynen. Kontoret har redan initierat flera åtgärder sedan tillsynen inletts, som exempel har kontoret påbörjat ett utvecklingsarbete av incidenthanteringsprocessen.

Det rådande omvärldsläget ställer högre krav på säkerhet inom alla samhällssektorer och det senaste året har trafikkontoret stärkt sitt arbete, där informationssäkerhet och NIS-direktivet är en viktig del. Kontoret är beroende av information i digitala tjänster varför informationssäkerhet är ett särskilt angeläget utvecklingsområde och Transportstyrelsens tillsyn har aktualiserat frågan ytterligare.

Kontoret bedömer att de tillsatta resurserna i kombination med de planerade åtgärderna kommer att leda till en betydande kunskaps- höjning inom organisationen, ett stärkt systematiskt arbete med informationssäkerhet och efterlevnad av NIS-direktivet.

Mot bakgrund av ovanstående föreslår trafikkontoret att nämnden beslutar att godkänna kontorets redovisning av tillsynen och kontorets svar på den. Kontoret föreslår även att nämnden beslutar om årlig uppföljning av åtgärdsplanen till nämnden.

Slut

Bilagor

1. Tillsynsrapport enligt NIS-lagen (sekretess enligt 18 kap. 8 § offentlighets- och sekretesslagen (2009:400).)
2. Trafikkontorets svar och åtgärdsplan (sekretess enligt 18 kap. 8 § offentlighets- och sekretesslagen (2009:400).)