TJÄNSTEUTLÅTANDE
2019-04-15

Ärende
TN 2019-0313

Infosäkerhetsklass
K1 (Öppen)

Trafiknämnden
2019-05-14, punkt 21

Krister Dackland
08-686 32 69
krister.dackland@sll.se

Svar på skrivelse angående IT-säkerheten inom Trafiknämnden

Ärendebeskrivning

Socialdemokraterna och Vänsterpartiet har ställt frågor om IT-säkerheten inom Trafiknämnden med anledning av de allvarliga brister beträffande skydd för inspelade samtal till vårdtjänsten 1177 som nyligen uppdagades. Bland annat ställs frågor om underleverantörer, riskhantering och geografiskt förläggning av Trafikförvaltningens IT-drift.

Beslutsunderlag

Förvaltningschefens tjänsteutlåtande samt skrivelse från S och V 2019-02-19.

Förslag till beslut

Trafiknämnden föreslås besluta

att anse att skrivelsen är besvarad.

Förslag och motivering

Trafikförvaltningens svar är som följer:

1. *Vilken kunskap har Trafikförvaltningen om förhållandet med underleverantörer på IT området?*

Avtalen stipulerar att trafikförvaltningen på förhand skriftligen ska ge sitt samtycke till eventuell användning av underkonsulter. Den primära leverantören ska ingå skriftligt avtal med underleverantören, bl a i fråga om säkerhet, som minst motsvarar den primära leverantörens skyldigheter.

2. *Finns idag möjlighet för underleverantörer att förlägga drift av IT-verksamheten utomlands, och i så fall i vilka fall?*

Dataskyddsförordningen (GDPR) stipulerar att IT-drift ska ske inom EU/EES-området. Trafikförvaltningen har således förlagt all IT-drift inom EU/EES. Samma krav gäller för underleverantörer. Trafikförvaltningen har utöver lagens krav valt att etablera möjligheten att ordna driftställen inom Sverige. Lokalisering av IT-drift inom Sverige har valts för viss, särskilt skyddsvärd information, bland annat delar av den integritetskänsliga information som nämns i skrivelsen. Trafikförvaltningen med leverantörer och underleverantörer har alltså ingen IT-drift förlagd utanför EU/EES. Inom Trafikförvaltningen förekommer dock användning av några molntjänster för administrativa ändamål. Exempel på sådana är Projectplace och Jira. Dessa tjänster kan ha serverdrift och datalagring förlagd utanför EU/EES-området. Trafikförvaltningen klassificerar information med avseende på sekretess, riktighet och konfidentialitet. Information som bedöms vara skyddsvärd i något av dessa avseenden ska inte hanteras med hjälp av sådana tjänster.

3. *Vilka kontrollmekanismer används för att kontrollera hur IT-säkerhetsavtal efterlevs?*

Ansvarsfördelningen mellan olika funktioner inom Trafikförvaltningen är enligt *Administrativ bestämmelse för intern styrning och kontroll* (TN-S-587888) baserad på principen om tre försvarslinjer. Linjeorganisationen bär i ett första led ansvaret för att avtal tecknas på sådant sätt att uppföljning är möjlig. Likaså bär man ansvar för riskanalyser, granskningar och revisioner som kan ske stickprovsvis eller mer systematiskt. Andra försvarslinjen utgörs av specialister på juridik och informationssäkerhet. Dessa övervakar tillämpningen av verksamhetens riskhantering och regelefterlevnad. Tredje försvarslinjen utgörs av internrevisonsfunktionen. För två år sedan genomförde internrevisionen en omfattande granskning av behörighetshanteingen inom Trafikförvaltningen. Granskningen ledde till en rad åtgärder bland annat inom IT och HR.

4. *Hur ser ansvarsfördelningen ut mellan trafiknämnden, färdtjänstnämnden och andra organ i fråga om rådsansvar och åtgärder med anledning av den förändrade organisationen?*

Av *Reglemente för regionstyrelsen och övriga nämnder* (LS 2018-0731) framgår hur ansvarsfördelningen ser ut inom regionen. Därutöver anges i reglementets inledning (§§1-8) att nämnder inom sitt verksamhetsområde ska följa vad som anges i lag eller annan författning, säkerställa en tydlig,

resurseffektiv och ändamålsenlig organisation samt en tillräcklig intern kontroll. Vidare anges att nämnden är personuppgiftsansvarig för den behandling av personuppgifter som sker i dess verksamhet. Av reglementet följer vidare att färdtjänstnämnden köper förvaltningsstöd av trafiknämnden. Det faktum att förvaltningsstöd tillhandahålls från trafiknämnden påverkar dock inte färdtjänstnämndens ansvar inom sitt verksamhetsområde.

Färdtjänstnämnden respektive trafiknämnden har inom sitt respektive verksamhetsområde fullt och odelat offentligrättsligt ansvar. Eftersom nämnderna har en del integrerad verksamhet, exempelvis kundtjänst och it-system, medför uppdelningen i två nämnder att ansvarsförhållandena måste formaliseras i olika dokument. Det har till stor del skett genom *Reglemente för regionstyrelsen och övriga nämnder*. Ytterligare dokument, exempelvis personuppgiftsbiträdesavtal, kommer att tas fram mellan trafiknämnden och färdtjänstnämnden

5. *Vilka risker anser förvaltningen finns idag inom ramen för de IT system som finns i verksamheten?*

Riskanalyser sker på olika nivåer i Trafikförvaltningens verksamhet. IT-systemen organiseras i tolv förvaltningsobjekt. För varje objekt tas årligen en förvaltningsplan fram och där dokumenteras en genomförd riskbedömning. Inom utvecklingsprojekten gör också riskbedömningar. Riskerna är av olika natur men alltid baserade på bedömningen om huruvida Trafikförvaltningen löper risk att inte nå sina mål. Ingen verksamhet är fri från risk och ledarskap handlar till stor del om att balansera risk mot kostnad. Allvarliga IT-risker ingår som en del av Trafikförvaltningens internkontrollplan vilken redovisas för Trafiknämnden i samband med beslut om den årliga verksamhetsplanen, senast vid nämndens sammanträde den 29 januari 2019.

Caroline Ottosson
Förvaltningschef

Krister Dackland
IT-direktör

Region Stockholm

SKRIVELSE
2019-02-19

Trafiknämnden

Socialdemokraterna
FRAMTIDSPARTIET

VÄNSTERPARTIET

IT-säkerheten inom Trafiknämnden

Igår avslöjade Computer Sweden att ett mycket stort antal samtal till 1177 Vårdguiden på telefon, mottagna av en underleverantör belägen i Thailand, har legat fritt åtkomliga på en icke lösenordskyddad server. Känslig patientdata har därmed funnits lättillgänglig på ett sätt som är ytterst problematiskt ur integritetshänseende. Region Stockholm är en av tre regioner i landet där denna verksamhet outsourcats och vars patienter har drabbats av denna potentiellt enorma integritetskränkning.

I en tid av snabb digitalisering uppstår stora risker såväl som möjligheter. Skandalen kring 1177 riskerar att underminera förtroendet för den viktiga digitaliseringen av hälso- och sjukvården. Avslöjandet kommer kort efter att IT-säkerhetsbrister uppmärksammats även inom Kriminalvården, och riskerar att skada allmänhetens förtroende för hur offentlig sektor hanterar IT.

Avslöjandet borde också vara en larmklocka för dem som aningslöst driver på för outsourcing av verksamhet utan kontroll av underleverantörer i flera led. När denna skrivelse författas vet vi ännu inte omfattningen av skandalen och alla dess orsaker, och ord står mot ord. Representanter för Region Stockholm hävdar att man inte kände till situationen med underleverantörer medan leverantören menar att beställaren, alltså regionen, var informerad.

Bristerna av hanteringen kring IT-säkerheten på ett område i regionen aktualiserar frågor om hur den efterlevs i övriga verksamheter. Även inom Trafiknämndens område finns stora mängder skyddsvärd information. Dels handlar det som på om information som berör den enskildes integritet så som spärr- och biljettinformation, färdtjänstinformation och kamerainformation för säkerhet och övervakning. Därutöver finns viktiga IT-system som är kritiska för trafikdriften så som SNOK (SL-nätets order- och kontrollsystem) och där störningar eller påverkan utifrån skulle kunna få allvarliga konsekvenser både för trafiken och för resenärernas säkerhet.

Region Stockholm

SKRIVELSE
2019-02-19

Trafiknämnden

Socialdemokraterna
FRAMTIDSPARTIET

VÄNSTERPARTIET

IT-säkerheten inom den offentliga sektorn är enormt viktig för att medborgarnas förtroende för det offentliga och för digitaliseringen inte ska skadas. Det är därför av yttersta vikt att gå till botten med dessa frågor.

Därför vill vi skyndsamt ha svar på:

- Vilken kunskap har Trafikförvaltningen om förhållandet med underleverantörer på IT området?
- Finns idag möjlighet för underleverantörer att förlägga drift av IT-verksamheten utomlands, och i så fall i vilka fall?
- Vilka kontrollmekanismer används för att kontrollera hur IT-säkerhetsavtal efterlevs?
- Hur ser ansvarsfördelningen ut mellan trafiknämnden, färdtjänstnämnden och andra organ i fråga om rådsansvar och åtgärder med anledning av den förändrade organisationen?
- Vilka risker anser förvaltningen finns idag inom ramen för de IT system som finns i verksamheten?