Trafikförvaltningen
Ledningsstaben
Juridik

Handläggare
Daniel Angermann
08-686 16 95
daniel.angermann@sll.se

INFORMATION
2020-11-12

Trafiknämnden
2020-12-15, punkt 17

Ärende
TN 2020-1446

Infosäkerhetsklass
K1 (Öppen)

Incidentrapportering inom områdena informationssäkerhet och dataskydd

Ärendebeskrivning

Förvaltningen återkommer med information om nämndens arbete med rutiner för rapportering av incidenter enligt lagen (2018:1174) och förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster samt dataskyddsförordningen[1].

Bakgrund

Trafiknämnden tillhandahåller en modern och hållbar kollektivtrafik, där centrala tjänster och tekniska system i allt större utsträckning är digitaliserade. Digitaliseringen som sådan möjliggör nya, mer avancerade tekniska lösningar och nya tjänster för resenärerna, men den innebär också nya risker i form av t.ex. potentiella intrång i och attacker mot it-miljöer. Dessa risker skapar ett behov av att arbeta systematiskt med informationssäkerhet, bl.a. genom att skapa en samlad bild över olika typer av incidenter som innebär en negativ påverkan på informationssäkerheten.

Informationssäkerheten berör även viktiga frågeställningar kring enskildas integritet, t.ex. när personuppgifter av fel anledning blivit förstörda, gått förlorade på annat sätt eller kommit i orätta händer.

Trafiknämnden har i budget för år 2020 fått i uppdrag att, som ett led i nämndens hantering av skyddsvärd information, utreda beroenden och vid

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG.

behov etablera rutiner för rapportering av incidenter till nämnder med rapporteringsplikt enligt lagen och förordningen om informationssäkerhet för samhällsviktiga och digitala tjänster samt dataskyddsförordningen.

Informationssäkerhet för samhällsviktiga och digitala tjänster

Europaparlamentet och Europeiska unionens råd antog år 2016 det så kallade NIS-direktivet[2] (eng. *Directive on security of network and information systems*). Direktivet syftar till att uppnå en hög gemensam nivå av säkerhet i nätverks- och informationssystem inom hela unionen.

Direktivet innebär att leverantörer av samhällsviktiga och digitala tjänster ska vidta säkerhetsåtgärder i nätverks- och informationssystem samt rapportera s.k. incidenter. Direktivet reglerar den lägsta nivå av informationssäkerhet som ska vara uppfylld, vilket innebär att medlemsländer kan föreskriva en högre nivå än den som följer av direktivet.

Sverige har implementerat NIS-direktivet genom en ny lag, lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Med stöd av bemyndigande i lagen har regeringen meddelat förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster som reglerar ytterligare detaljer samt ytterligare bemyndiganden till myndigheter, bl.a. till Myndigheten för samhällsskydd och beredskap (MSB), att utfärda närmare föreskrifter och allmänna råd.

För att lagen ska vara tillämplig på en verksamhet ska leverantören enligt 3 § vara av det slag som anges i bilaga 2 till NIS-direktivet. Leverantören ska vara etablerad i Sverige och tillhandahålla en samhällsviktig tjänst. Tillhandahållandet av tjänsten ska vidare vara beroende av nätverk och informationssystem, där en s.k. incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten.

I 8 § anges att lagen inte gäller för sådan verksamhet som omfattas av säkerhetsskyddslagen (2018:585). Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster är således subsidiär i förhållande till säkerhetsskyddslagen. Bestämmelsen är av intresse i förevarande sammanhang

[2] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

eftersom vissa delar av tunnelbaneverksamheten omfattas av säkerhetsskyddslagen.

Leverantörer som lyder under lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (fortsättningsvis kallad för lagen) har ett antal skyldigheter, bl.a. ska de enligt 11 § bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete avseende nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. Enligt 12 § ska en riskanalys göras och årligen uppdateras. Analysen ska ligga till grund för val av säkerhetsåtgärder. Om en incident inträffar som har en betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten ska sådan incident enligt 18 § utan onödigt dröjsmål rapporteras till MSB.

Leverantörer av samhällsviktiga tjänster behöver själva identifiera om de uppfyller kriterierna för att omfattas av lagen. Enligt 23 § ska en leverantör som uppfyller kriterierna utan dröjsmål anmäla sig tillsynsmyndigheten. Vid underlåtenhet att inkomma med anmälan kan en sanktionsavgift tas ut som uppgår till lägst 5 000 kronor och högst 10 miljoner kronor.

Trafikförvaltningen inledde under år 2018, inför ikraftträdandet av lagen, ett arbete med att undersöka huruvida verksamheten eller delar av verksamheten omfattas av NIS-direktivet och de krav som följer av lagen. Vissa delar av tunnelbaneverksamheten omfattas per definition inte av lagen eftersom de omfattas av säkerhetsskyddslagen, som har företräde. För övriga delar har frågan varit dels om det är trafiknämnden eller de operatörer som har upphandlats av trafiknämnden som ska anses vara leverantör i lagens mening, dels om de tjänster som levereras i form av kollektivtrafik och tillhandahållande av infrastruktur är samhällsviktiga i den mening som avses i lagen.

I MSB:s föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster, MSBFS 2018:7, har med stöd av 3 och 16 §§ förordningen om samhällsviktiga och digitala tjänster närmare preciserats vilken verksamhet som omfattas av lagen samt kriterier för när en tjänst ska anses vara samhällsviktig.

I föreskriften anges i 1 kap 3 § såsom definition att ”infrastrukturförvaltning och trafikledning järnväg enligt artikel 3.2 i Europaparlamentets och rådets direktiv 2012/34/EU av den 21 november 2012 om inrättande av ett gemensamt europeiskt järnvägsområde” omfattas av lagen. Direktivet gäller enligt art. 1

punkt 2 ”användning av järnvägsinfrastruktur för inrikes och internationell järnvägstrafik.”

Vidare anges i 4 kap 2 § att ”med samhällsviktiga tjänster rörande *järnvägstransport* där incidenter skulle medföra en betydande störning vid tillhandahållandet av tjänsten avses

1. infrastrukturförvaltning eller trafikledning av järnväg, med huvudspår överstigande 200 spårkilometer,
2. persontrafik som trafikerar huvudspår där trafikarbetet årligen överstiger 1 500 000 framförda tågkilometer, eller
3. godstrafik som trafikerar huvudspår där trafikarbetet årligen överstiger 1 500 000 framförda tågkilometer.”

Vid en första kontakt med MSB och Transportstyrelsen år 2018 kommunicerades till förvaltningen att nämndens verksamhet inte var att betrakta som samhällsviktig tjänst i enlighet med kraven i 4 kap. 2 § MSBFS 2018:7.

Vid en uppkommen incident på Roslagsbanan i juni 2019 togs en ny kontakt med de båda myndigheterna. Även då gjordes bedömningen, bl.a. mot bakgrund av en tidigare genomförd utredning[3], att nämndens verksamhet inte omfattas av kraven i NIS-direktivet.

Den principiella dialogen med Transportstyrelsen är alltjämt pågående. I dagsläget har dock inte framkommit något annat än att nämndens verksamhet inte anses omfattas av NIS-direktivet. Några rutiner för rapportering av incidenter enligt lagen och förordningen om informationssäkerhet för samhällsviktiga och digitala tjänster har mot bakgrund av ovanstående inte upprättats.

Dataskyddsförordningen

Sedan den 25 maj 2018 gäller EU:s dataskyddsförordning (*GDPR, eng. General Data Protection Regulation*) inom hela EU. Förordningens regler motsvarar i stora delar de regler som tidigare gällde enligt personuppgiftslagen, vilken upphävdes i samband med förordningens ikraftträdande.

[3] MSB Konsekvensutredning, dat.2018-10-23, dnr 2018-05893.

Trafikförvaltningen
Ledningsstaben
Juridik

INFORMATION
2020-11-12

Ärende
TN 2020-1446

Infosäkerhetsklass
K1 (Öppen)

Dataskyddsförordningen syftar till att stärka och harmonisera dataskyddet för medborgare inom EU. Den primära målsättningen med förordningen är att ge individen bättre kontroll över sina personuppgifter och att förenkla lagstiftningen för internationella företag genom att samordna lagstiftningen inom EU.

Som personuppgift räknas all information relaterad till en identifierad eller identifierbar fysisk levande person. Så kallade känsliga personuppgifter är personuppgifter om exempelvis etniskt ursprung, politisk åskådning, religiös eller filosofisk övertygelse, medlemskap i fackliga organisationer, information om hälsa eller sexliv och sexuell läggning, samt genetiska eller biometriska uppgifter.

För att få behandla personuppgifter om individer krävs alltid en legal grund för behandlingen. Förordningen ställer också stränga krav på transparens, där organisationer som behandlar personuppgifter har omfattande skyldigheter att informera individer om hur deras uppgifter används, varför och på vilken laglig grund samt att dokumentera den behandling som sker.

Dataskyddsförordningen ålägger organisationer att skydda personuppgifter genom organisatoriska och tekniska säkerhetsåtgärder. När skyddet fallerar kan det vara fråga om en så kallad personuppgiftsincident.

Som personuppgiftsincident definieras i förordningen en ”säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats”. Förordningen föreskriver att vissa typer av personuppgiftsincidenter ska rapporteras till den nationella tillsynsmyndigheten – i Sverige är det Datainspektionen – inom 72 timmar efter det att organisationen upptäckt incidenten.

Trafikförvaltningen har etablerat omfattande och noggranna rutiner för dokumentation och rapportering av personuppgiftsincidenter inklusive rapportering till Datainspektionen. Rapporteringen sker genom respektive informationsägare, med stöd av nämndens dataskyddsombud. Dataskyddsombudet utgör Datainspektionens förlängda arm in i organisationen och har som uppgift att övervaka efterlevnaden av dataskyddsförordningens krav.

Trafikförvaltningen
Ledningsstaben
Juridik

INFORMATION
2020-11-12

Ärende
TN 2020-1446

Infosäkerhetsklass
K1 (Öppen)

Utöver den incidentrapportering som sker till Datainspektionen rapporterar dataskyddsombudet månatligen till förvaltningschefen. Under 2020/2021 avser förvaltningen att etablera ytterligare rapporteringsrutiner genom årlig information till trafiknämnden i samband med årsbokslut.

David Lagneholm
Förvaltningschef

Sara Catoni
Stabschef