STOCKHOLMS STADSHUS AB
En del av Stockholms stad

Remissvar

Dnr 2017/3.2.2/103
Sid. 1 (9)
2017-07-06

Handläggare:
Malin Lindvall, 08-508 29 749

Till
Finansroteln

Remiss av "Informationssäkerhet för samhällsviktiga och digitala tjänster" (SOU 2017:36)

Svar på remiss från Finansroteln (dnr 110-972/2017).

Sammanfattning

Det direktiv som betänkandet behandlar innebär bl.a. skyldigheter för vissa leverantörer av samhällsviktiga tjänster och vissa leverantörer av digitala tjänster att vidta säkerhetsåtgärder för att hantera risker samt förebygga och hantera incidenter i nätverk och informationssystem som de är beroende av för att tillhandahålla tjänsterna. Leverantörerna ska också rapportera incidenter som har en betydande respektive avsevärd inverkan på kontinuiteten i tjänsten. För att en leverantör ska anses vara en sådan leverantör av samhällsviktiga tjänster som omfattas av direktivet krävs att leverantören bedriver verksamhet inom någon av de i direktivet särskilt utpekade enheterna. Enheterna finns inom sju angivna sektorer. Sektorerna omfattar bl.a. leverans och distribution av dricksvatten samt digital infrastruktur. Dessutom krävs att den tjänst som tillhandahålls är viktig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet, att tillhandahållandet av tjänsten är beroende av nätverk och informationssystem och att en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten.

Medlemsstaterna är till följd av direktivet bl.a. skyldiga att dels upprätta en förteckning över de tjänster på medlemsstatens territorium som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet, dels identifiera de leverantörer som tillhandahåller sådana tjänster.

Utredningen föreslår en ny lag och en ny förordning som till utformning och innehåll ligger nära direktivet. Enligt utredningens förslag bör Myndigheten för samhällsskydd och beredskap ges i uppdrag att påbörja identifiering och bedömning av samhällsviktiga tjänster så att förteckningen kan meddelas senast den 10 maj 2018, då den nya lagstiftningen föreslås träda ikraft.

Koncernledningen anser att det är angeläget att en förteckning som anger de tjänster som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet och andra relevanta vägledningar tas fram i sådan tid att den möjliggör för leverantörer som kan komma att omfattas av lagstiftningen att vidta nödvändiga åtgärder i syfte att uppfylla

relevanta krav i tid för lagstiftningens ikraftträdande. Koncernledningen har inga synpunkter i övrigt på utredningens förslag.

Ärendet

I juli 2016 antog Europaparlamentet och rådet NIS-direktivet. Direktivet fastställer åtgärder för att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom unionen, i syfte att förbättra den inre marknadens funktion. Direktivet innebär bl.a. skyldigheter för vissa leverantörer av samhällsviktiga tjänster och vissa leverantörer av digitala tjänster att vidta säkerhetsåtgärder för att hantera risker samt förebygga och hantera incidenter i nätverk och informationssystem som de är beroende av för att tillhandahålla tjänsterna. Leverantörerna ska också rapportera incidenter som har en betydande respektive avsevärd inverkan på kontinuiteten i tjänsten. För att en leverantör ska anses vara en sådan leverantör av samhällsviktiga tjänster som omfattas av direktivet krävs att leverantören bedriver verksamhet inom någon av de i direktivet särskilt utpekade enheterna. Enheterna finns inom sju angivna sektorer. Sektorerna omfattar energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt digital infrastruktur. Dessutom krävs att den tjänst som tillhandahålls är viktig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet, att tillhandahållandet av tjänsten är beroende av nätverk och informationssystem och att en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten. Medlemsstaterna är skyldiga att dels upprätta en förteckning över de tjänster på medlemsstatens territorium som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet, dels identifiera de leverantörer som tillhandahåller sådana tjänster. De leverantörer av digitala tjänster som omfattas av direktivet är sådana som tillhandahåller internetbaserade marknadsplatser, internetbaserade sökmotorer eller molntjänster. Medlemsstaterna ska enligt direktivet utse myndigheter med särskilda uppgifter på området, till exempel tillsynsmyndigheter, nationella kontaktpunkter och enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter). Medlemsstaterna ska också säkerställa att tillsynsmyndigheterna har befogenheter och medel för att kontrollera att leverantörerna uppfyller sina skyldigheter samt fastställa regler om sanktioner för överträdelse av de nationella bestämmelserna som antagits enligt direktivet.

Direktivet innehåller vidare en skyldighet för varje medlemsstat att anta en nationell strategi för säkerhet i nätverk och informationssystem. Medlemsstaterna ska senast den 9 maj 2018 anta och offentliggöra de bestämmelser i lagar och andra författningar som är nödvändiga för att följa direktivet. Bestämmelserna ska tillämpas från och med den 10 maj 2018.

Utredningens uppdrag har varit att föreslå hur NIS-direktivet ska genomföras i svensk rätt. Detta har innefattat bl.a. att föreslå hur direktivets krav på utpekande av myndigheter med ansvar för vissa funktioner ska genomföras, hur identifiering av och krav på leverantörer som omfattas av direktivet kan genomföras i ett samlat regelverk, föreslå nödvändiga ändringar i offentlighets- och sekretesslagen (2009:400) för att känslig information i incidentrapporter ska kunna skyddas, och lämna nödvändiga författningsförslag.

Frågan om hur en nationell strategi för säkerhet i nätverk och informationssystem bör utformas har inte omfattats av uppdraget.

Utredningen föreslår en ny lag och en ny förordning som till utformning och innehåll ligger nära NIS-direktivet. Regelverket ska tillämpas endast på sådana leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster som omfattas av direktivet. I den utsträckning det finns bestämmelser om säkerhetskrav eller incidentrapporteringskrav på de aktuella leverantörerna i annan lag som minst motsvarar bestämmelserna i den föreslagna lagen ska emellertid de bestämmelserna tillämpas. Om sådana krav finns i bindande EU-rättsakter (lex specialis) ska den föreslagna lagen inte tillämpas alls.

Vissa företag och leverantörer är uttryckligen undantagna från direktivets tillämpningsområde. Dessa omfattas följaktligen inte heller av den föreslagna lagen. Detta innebär att regelverket inte ska tillämpas på tillhandahållare av ett allmänt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst. I NIS-direktivet anges dock internetknutpunkter uttryckligen som en sådan enhet som ska regleras enligt direktivet. Tillhandahållare av internetknutpunkter omfattas därför av den föreslagna lagen.

För att leverantörer av samhällsviktiga tjänster ska kunna identifieras ska Myndigheten för samhällsskydd och beredskap (MSB) meddela föreskrifter (förteckning) om vilka tjänster som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet (samhällsviktiga tjänster) för varje sektor som omfattas av NIS-direktivet. Det är verksamhetsutövaren som är ansvarig för att avgöra om denne omfattas av lagen. I detta syfte ska den som är ansvarig för en verksamhet som tillhandahåller en samhällsviktig tjänst som finns upptagen i de föreskrifter (förteckning) som MSB ska meddela, undersöka om tillhandahållandet av tjänsten är beroende av nätverk eller informationssystem och om en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten. För att avgöra om en störning är betydande ska verksamhetsutövaren beakta vissa särskilda faktorer, bl.a. det antal användare som är beroende av den aktuella tjänsten. Tillsynsmyndigheten får meddela föreskrifter om vilka sektorspecifika och sektoröverskridande faktorer som ska beaktas vid bedömningen av om en incident skulle medföra en betydande störning.

Såväl leverantörer av samhällsviktiga tjänster som leverantörer av digitala tjänster ska vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i deras nätverk och informationssystem. De ska också vidta lämpliga åtgärder för att förebygga och minimera den inverkan som incidenter som påverkar säkerheten i deras nätverk och informationssystem har på de tjänster som tillhandahålls.

Leverantörer av samhällsviktiga tjänster ska göra en riskanalys som ska ligga till grund för val av säkerhetsåtgärder. Tillsynsmyndigheten får också meddela föreskrifter om utformningen av säkerhetsåtgärderna. Leverantörer av samhällsviktiga tjänster ska också bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete. Både leverantörer

av samhällsviktiga tjänster och leverantörer av digitala tjänster ska utan onödigt dröjsmål rapportera incidenter till CSIRT-enheten (se nedan) vid MSB. Leverantörer av samhällsviktiga tjänster ska rapportera incidenter som har en betydande inverkan på kontinuiteten i tjänsten, medan leverantörer av digitala tjänster ska rapportera incidenter som har en avsevärd inverkan på tillhandahållandet av tjänsten. I lagen anges ett antal faktorer som framför allt ska beaktas vid bedömningen av om incidenten har en sådan inverkan att den ska rapporteras. Tillsynsmyndigheten får meddela närmare föreskrifter om faktorer som ska beaktas vid bedömningen av om en incident har betydande inverkan. MSB får meddela föreskrifter om rapportering av incidenter och om förutsättningarna för frivillig incidentrapportering.

För varje sektor och för de digitala tjänster som omfattas av lagen ska en tillsynsmyndighet ansvara för att övervaka att regelverket följs.

Tillsynsmyndigheten ska försöka få en leverantör som inte följer regelverket att rätta sig. Tillsynsmyndigheten får meddela förelägganden, dels i syfte att få tillgång till viss information som behövs för tillsynen, dels för att få leverantören att följa regelverket. Ett föreläggande får förenas med vite.

Tillsynsmyndigheten ska besluta att sanktionsavgift ska tas ut av den som underlåter att incidentrapportera eller att vidta säkerhetsåtgärder.

För att underlätta gränsöverskridande samarbete och för att möjliggöra ett effektivt genomförande av NIS-direktivet ska det i varje medlemsstat finnas en nationell gemensam kontaktpunkt. Den nationella kontaktpunkten ska ansvara för samordningen av frågor angående nätverk och informationssystem och för gränsöverskridande samarbete på unionsnivå. I varje medlemsstat ska det enligt NIS-direktivet också finnas en eller flera enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter). CSIRT-enheten ska bland annat övervaka incidenter på nationell nivå och tillhandahålla tidiga varningar m.m. till relevanta aktörer om risker och incidenter. Utredningens förslag innebär att MSB ska vara både nationell kontaktpunkt och CSIRT-enhet.

Befintliga bestämmelser om sekretess omfattar uppgifter som ska rapporteras och delas med anledning av incidenter samt tillhandahållas i samband med tillsyn. Det har inte framkommit några exempel på att den nuvarande regleringen är otillräcklig. Det finns därmed inte skäl att införa starkare sekretess för uppgifter som lämnas inom ramen för incidentrapporteringen. Till följd av tillsynen kan tillsynsmyndigheterna emellertid få del av känsliga uppgifter om enskilds affärs- eller driftförhållande. För att sistnämnda uppgifter ska kunna skyddas behöver sekretessförordningen ändras så att sekretess för sådana uppgifter gäller i verksamhet som består i tillsyn enligt det föreslagna regelverket.

Regelverket föreslås träda i kraft den 10 maj 2018.

Ärendets beredning

Finansroteln har remitterat betänkandet *Informationssäkerhet för samhällsviktiga och digitala tjänster*. Stockholms Stadshus AB har i sin tur remitterat betänkandet vidare till dotterbolagen Stockholm Vatten och Avfall AB och AB Stokab. Nedan följer en

redovisning av bolagens remissvar i huvudsak. Remissvaren i sin helhet återfinns i bilagorna.

Underremiss

Stockholm Vatten och Avfall AB:s remissvar har i huvudsak följande lydelse:

Stockholm Vatten och Avfall producerar och tillhandahåller årligen ungefär 150 miljoner m3 dricksvatten, vilket levereras till cirka 1.4 miljoner invånare i regionen.

Stockholm Vatten och Avfall arbetar redan idag med säkerhetshöjande åtgärder kring nätverk och informationssystem för leveransen och distributionen av dricksvatten. Bolaget ställer sig positiva till nationell samordning av kraven för säkerhetshöjande åtgärder inom sektorn i enlighet med förslaget.

Stockholm Vatten och Avfall vill poängtera vikten av att berörda myndigheter ges i uppdrag att skyndsamt påbörja arbetet med vägledande myndighetsföreskrifter mot bakgrund av att regelverket föreslås träda i kraft den 10 maj 2018 *(bilaga 1)*.

AB Stokabs remissvar har i huvudsak följande lydelse:

Tillhandahållare av ett allmänt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst är uttryckligen undantagna från direktivets tillämpningsområde. Detta gäller dock med undantag för s.k. internetknutpunkter, eftersom dessa uttryckligen listas som en sådan enhet som ska regleras enligt direktivet. Stokab tillhandahåller ett allmänt tillgängligt elektroniskt kommunikationsnät i form av svart fiber. Att Stokab endast tillhandahåller ett passivt nät i form av svart fiber innebär rent fysiskt att Stokab inte rår över de elektroniska signaler som går i nätet utan dessa tillhör nyttjaren av nätet. Stokab har således inte någon aktiv utrustning i nätet och tillhandahåller inga aktiva "tjänster", t.ex. Internetknutpunkter. Stokab omfattas således inte av direktivet eller den föreslagna nya lagen.

Stokabs dotterbolag, S:t Erik Kommunikation (STEK), driver och administrerar Stockholms stads interna kommunikationsnät. Vad gäller samhällsviktiga tjänster, tillhandahåller STEK DNS-tjänster i förhållande till t.ex. Stockholms stads webbsida stockholm.se, e-post till staden, internettrafik från staden etc. STEK bedriver därför verksamhet inom en av de s.k. enheter inom vilka vissa tjänster kommer att klassificeras som s.k. samhällsviktiga tjänster, d.v.s. tjänster som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet. Det blir därför upp till STEK att utifrån den av MSB framtagna förteckningen bedöma om STEK:s tillhandahållande av själva DNS-funktionen utgör en samhällsviktig tjänst och om STEK till följd därav omfattas av den föreslagna nya lagen. Vad gäller de tjänster DNS-funktionen stödjer är det däremot upp till respektive verksamhet inom Stockholm stad att, tillsammans med SLK, göra en bedömning av om tillhandahållandet av tjänsten utgör en samhällsviktig tjänst i den nya lagens mening.

Enligt förslaget bör MSB ges i uppdrag att påbörja identifiering och bedömning av samhällsviktiga tjänster så att förteckningen kan meddelas senast den 10 maj 2018, då den nya lagstiftningen föreslås träda ikraft. Stokab anser att det är angeläget att denna förteckning och andra relevanta vägledningar tas fram i sådan tid att den möjliggör för

leverantörer som kan komma att omfattas av lagstiftningen att vidta nödvändiga åtgärder i syfte att uppfylla relevanta krav i tid för lagstiftningens ikraftträdande *(bilaga 2)*.

Koncernledningens synpunkter
Medlemsstaterna är till följd av direktivet bl.a. skyldiga att dels upprätta en förteckning över de tjänster på medlemsstatens territorium som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet, dels identifiera de leverantörer som tillhandahåller sådana tjänster. Enligt utredningens förslag bör MSB ges i uppdrag att påbörja identifiering och bedömning av samhällsviktiga tjänster så att förteckningen kan meddelas senast den 10 maj 2018, då den nya lagstiftningen föreslås träda ikraft.

Koncernledningen delar dotterbolagens uppfattning att det är angeläget att förteckningen och andra relevanta vägledningar tas fram i sådan tid att den möjliggör för leverantörer som kan komma att omfattas av lagstiftningen att vidta nödvändiga åtgärder i syfte att uppfylla relevanta krav i tid för lagstiftningens ikraftträdande.

Koncernledningen har inga synpunkter i övrigt på utredningens förslag.

Jonas Schneider
Vice VD

Bilagor
1. Remissvar Stockholm Vatten och Avfall AB
2. Remissvar AB Stokab

Bilaga 1

STOCKHOLM VATTEN OCH AVFALL

TORBJÖRN LUNDGREN
INFORMATION OCH DOKUMENTHANTERING
TEL 08-522 12582
TORBJORN.LUNDGREN@SVOA.SE

REMISSVAR

Betänkandet informssäkehet för samhällsviktiga och digitala tjänster (SOU 2017:36)

Med anledning av Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen, NIS-direktivet, föreslår Justitiedepartementet en ny lag och en ny förordning som till utformning och innehåll ligger nära NIS-direktivet.

I betänkandet finns det angivet ett antal sektorer vars verksamhet utgör samhällsviktig verksamhet. Stockholm Vatten och Avfall producerar och tillhandahåller årligen ungefär 150 miljoner m^3 dricksvatten vilket levereras till cirka 1.4 miljoner invånare i regionen.

Stockholm Vatten och Avfall arbetar redan idag med säkerhetshöjande åtgärder kring nätverk och informationssystem för leveransen och distributionen av dricksvatten. Bolaget ställer sig positiva till nationell samordning av kraven för säkerhetshöjande åtgärder inom sektorn i enlighet med förslaget.

Stockholm Vatten och Avfall vill poängtera vikten av att berörda myndigheter ges i uppdrag att skyndsamt påbörja arbetet med vägledande myndighetsföreskrifter mot bakgrund av att regelverket föreslås träda i kraft den 10 maj 2018. De vägledande föreskrifterna bör ge anvisningar i förhållande till närliggande reglering.

Med vänliga hälsningar

Stockholm Vatten och Avfall

Krister Schultz
Verkställande direktör

STOKAB

Bilaga 2

Yttrande över betänkandet Informationssäkerhet för samhällsviktiga och digitala tjänster (SOU 2017:36)

Stockholms stad har, genom Stokab, byggt ett operatörsneutralt passivt fibernät som når drygt 90 procent av hushållen och i princip 100 procent av företagen i Stockholm. Stokabs dotterbolag, S:t Erik Kommunikation (STEK), driver och administrerar Stockholms stads interna kommunikationsnät enligt uppdrag av Kommunfullmäktige. Detta nät omfattar alla Stockholms stads verksamheter och bolag, såväl administrativa som tekniska system.

Säkerheten i nätverk och informationssystem är viktig idag, men kommer att bli än mer viktig ju mer välfärdssektorn och digitaliseras.

Det direktiv som betänkandet omfattar medför skyldigheter för bl.a. *vissa leverantörer av samhällsviktiga tjänster* och *vissa leverantörer av digitala tjänster* att vidta säkerhetsåtgärder för att hantera risker samt förebygga och hantera incidenter i nätverk och informationssystem som de är beroende av för att tillhandahålla tjänsterna. Leverantörerna ska också rapportera incidenter som har en betydande respektive avsevärd inverkan på kontinuiteten i tjänsten. De leverantörer av samhällsviktiga tjänster som omfattas inkluderar bl.a. leverantörer inom sektorn digital infrastruktur och de särskilda s.k. enheterna Internetknutpunkter, leverantörer av DNS-tjänster och registreringsenheter för toppdomäner. Med vissa leverantörer av digitala tjänster avses tillhandahållare av internetbaserade marknadsplatser, internetbaserade sökmotorer och molntjänster.

Vissa leverantörer är uttryckligen undantagna från direktivets tillämpningsområde, däribland företag som omfattas av kraven i artiklarna 13a och 13b i direktiv 2002/21/EG, dvs. tillhandahållare av ett allmänt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst. Anledningen till detta är att en sådan leverantör redan är skyldig dels att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att verksamheten uppfyller rimliga krav på driftsäkerhet, dels att utan onödigt dröjsmål rapportera störningar eller avbrott av betydande omfattning. Dessa skyldigheter är implementerade i svensk rätt genom Lagen om elektronisk kommunikation (LEK), 5 kap. 6b och 6c §§. Tillhandahållare av ett allmänt kommunikationsnät omfattas således inte heller av den föreslagna nya lagen. Detta gäller dock med undantag för s.k. internetknutpunkter, eftersom dessa uttryckligen listas som en sådan enhet som ska regleras enligt direktivet. Tillhandahållare av internetknutpunkter omfattas därför av den föreslagna lagen trots att de enligt svensk rätt anses som sådana företag som omfattas av artiklarna 13a och 13b i direktiv 2002/21/EG.

Stokab tillhandahåller ett allmänt tillgängligt elektroniskt kommunikationsnät i form av svart fiber. Bolagets verksamhet omfattas därmed av LEK, däribland skyldigheterna om säkerhetsnivå och rapportering av avbrott och störningar. Att Stokab endast tillhandahåller ett

passivt nät i form av svart fiber innebär rent fysiskt att Stokab inte rår över de elektroniska signaler som går i nätet utan dessa tillhör nyttjaren av nätet. Stokab har således inte någon aktiv utrustning i nätet och tillhandahåller inga aktiva ”tjänster, t.ex. Internetknutpunkter. Stokab omfattas således inte av direktivet eller den föreslagna nya lagen.

STEK driver och administrerar Stockholms stads interna kommunikationsnät. STEK tillhandahåller inte någon av de digitala tjänster som omfattas av direktivet och den föreslagna nya lagen, d.v.s. internetbaserade marknadsplatser, internetbaserade sökmotorer eller molntjänster. Vad gäller samhällsviktiga tjänster, tillhandahåller STEK DNS-tjänster i förhållande till t.ex. Stockholms stads webbsida stockholm.se, e-post till staden, internettrafik från Staden etc. STEK bedriver därför verksamhet inom en av de s.k. enheter inom vilka vissa tjänster kommer att klassificeras som s.k. samhällsviktiga tjänster, d.v.s. tjänster som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet. För att leverantörer av tjänster inom de utpekade enheterna ska kunna identifiera om de tillhandahåller samhällsviktiga tjänster och därför omfattas av den nya lagen och är skyldiga att vidta de säkerhetsåtgärder etc. som föreskrivs, ska Myndigheten för samhällsskydd och beredskap (MSB) upprätta en förteckning över sådana tjänster. Det blir därför upp till STEK att utifrån den av MSB framtagna förteckningen bedöma om STEKs tillhandahållande av själva DNS-funktionen utgör en samhällsviktig tjänst och om STEK till följd därav omfattas av den föreslagna nya lagen. Vad gäller de tjänster DNS-funktionen stödjer är det däremot upp till respektive verksamhet inom Stockholm stad att, tillsammans med SLK, göra en bedömning av om tillhandahållandet av tjänsten utgör en samhällsviktig tjänst i den nya lagens mening.

Enligt förslaget bör MSB ges i uppdrag att påbörja identifiering och bedömning av samhällsviktiga tjänster så att förteckningen kan meddelas senast den 10 maj 2018, då den nya lagstiftningen föreslås träda ikraft. Stokab anser att det är angeläget att denna förteckning och andra relevanta vägledningar tas fram i sådan tid att den möjliggör för leverantörer som kan komma att omfattas av lagstiftningen att vidta nödvändiga åtgärder i syfte att uppfylla relevanta krav i tid för lagstiftningens ikraftträdande.

Med vänlig hälsning

AB Stokab

Niklas Cedstedt
T.f. verkställande direktör