Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av incidenter för leverantörer av samhällsviktiga tjänster

A. Allmänt

Beskrivning av problemet och vad man vill uppnå

Centrala samhällstjänster är i hög utsträckning digitaliserade. Nya sätt att hantera, lagra och kommunicera information medför nya möjligheter men också nya risker. Förekomsten av sårbarheter i nätverk och informationssystem, ökad it-relaterad brottslighet och det förändrade samhällsläget skapar ett stort behov av att arbeta systematiskt med informationssäkerhet samt skapa en samlad bild av inträffade incidenter. Incidenter kan hindra genomförandet av ekonomisk verksamhet, generera omfattande ekonomiska förluster och undergräva användarnas förtroende för tjänsterna. Samhället behöver bli bättre i arbetet med informations- och cybersäkerhet. Detta gäller särskilt för samhällsviktiga tjänster.

I syfte att skapa tillit till digital hantering av information och på det sättet förbättra den inre marknadens funktion antog Europaparlamentet och rådet NIS-direktivet, Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverk och informationssystem i hela unionen.

Genom NIS-direktivet ska en hög gemensam nivå av säkerhet i nätverk och informationssystem inom unionen uppnås. Direktivet innebär att leverantörer av samhällsviktiga och digitala tjänster ska vidta säkerhetsåtgärder i nätverk och informationssystem samt rapportera incidenter. NIS-direktivet reglerar en miniminivå av informationssäkerhet. EU:s medlemsländer kan för leverantörer av samhällsviktiga tjänster anta nya eller behålla befintliga informationssäkerhetskrav som är på samma nivå eller högre än de som NIS-direktivet ställer krav på.

I NIS-direktivet regleras leverantörer av samhällsviktiga tjänster inom sju olika sektorer, energi, transport, bank, finansmarknadsinfrastruktur, hälso- och sjukvård, dricksvatten och digital infrastruktur. Aktör som bedriver

verksamhet inom någon av de i NIS-direktivet angivna sju sektorerna och tillhandahåller en samhällsviktig tjänst är ansvarig för att avgöra om den omfattas av direktivet eller inte.

I Sverige implementeras NIS-direktivet genom en ny lag, lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, förordning (2018: 1175) om informationssäkerhet för samhällsviktiga och digitala tjänster, myndighetsföreskrifter utfärdade av Myndigheten för samhällsskydd och beredskap samt där så behövs sektorsspecifika föreskrifter utfärdade av respektive tillsynsmyndighet avseende säkerhetsåtgärder.

Myndigheten för samhällsskydd och beredskap (MSB) utfärdar närmare föreskrifter och allmänna råd om anmälan och identifiering av leverantörer av samhällsviktiga tjänster, systematiskt och riskbaserat informationssäkerhetsarbete och incidentrapportering för leverantörer av samhällsviktiga tjänster respektive digitala tjänster samt frivillig rapportering av incidenter i tjänster som är viktiga för samhällets funktionalitet.

I denna författning, Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av incidenter för leverantörer av samhällsviktiga tjänster, tydliggörs kraven avseende vad, när och hur incidentrapportering till MSB ska ske.

Beskrivning av alternativa lösningar för det man vill uppnå och vilka effekterna blir om någon reglering inte kommer till stånd

NIS-direktivet ska implementeras i Sverige. Sverige har valt att införa NIS-direktivet genom en ny lag (2018:1174) och en ny förordning (2018:1175) som omfattar alla berörda sektorer. Kraven i lag och förordning kan förtydligas genom myndighetsföreskrifter.

I betänkandet SOU 2017:36 förs ett resonemang rörande möjligheten att implementera NIS-direktivet genom att göra tillägg i respektive sektors reglering. Utredningen konstaterade dock att detta förutsätter ett omfattande kartläggningsarbete samt att regleringen riskerar att bli oöverskådlig och rörig. Utredningen ansåg att fördelarna med ett samlat regelverk bland annat är att det blir tydligt för samtliga berörda vilken reglering som finns avseende samhällsviktiga tjänster och digitala tjänster, lagstiftningen blir heltäckande och ingen tjänst riskerar att bli utan reglering. Beslutad lag och förordning inklusive kommande myndighetsföreskrifter utgör ett sådant samlat regelverk.

Enligt förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster ska MSB årligen till EU:s samarbetsgrupp lämna en sammanfattande rapport om de rapporter som mottagits i enlighet med lag (2018:1174). Samarbetsgruppen består av företrädare för medlemsstaterna, kommissionen och Europeiska unionens byrå för nät- och

informationssäkerhet (ENISA). Den sammanfattande rapporten ska innehålla antalet rapporter, rapporterade incidenters art samt vilka åtgärder som vidtagits. Vidare ska MSB informera andra berörda länder i Europeiska unionen om en incident som rapporterats av en leverantör av samhällsviktiga tjänster har en betydande inverkan på kontinuiteten i samhällsviktiga tjänster i det landet.

Ett system för it-incidentrapportering ska enligt NIS-regleringen kunna användas för att varna andra och därigenom minska konsekvenser av inträffade incidenter. Det ska även utgöra underlag för analyser och bidra till en samlad lägesbild över tid när det gäller informationssäkerhet. Detta ger ökad möjlighet att återkoppla relevant information och stöd till berörda aktörer och inrikta förebyggande insatser. För att systemet ska kunna användas på avsett sätt och för att Sverige ska kunna uppfylla sina skyldigheter gentemot EU behövs en tydlig struktur som klargör vad som ska rapporteras, när och hur. Det är således centralt att kraven blir bindande och tydliggörs i form av myndighetsföreskrifter. Avsaknad av sådana bindande krav bedöms resultera i allt för stor otydlighet om hur en leverantör ska uppfylla rapporteringsplikten, vilket kan leda till en ojämn och sporadisk rapportering där inlämnad information inte kan ligga till grund för utformning av nödvändigt stöd och analyser. Det blir även svårare att säkerställa att skyldigheten att tillhanda information till EU och andra medlemsstater kan uppfyllas. Otydligheten försvårar även tillsynen.

Uppgifter om vilka som berörs av regleringen

Leverantörer av samhällsviktiga tjänster finns inom sektorerna energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt digital infrastruktur och kan vara statliga myndigheter, kommuner, landsting eller företag.

Föreskrifterna om incidentrapportering gäller de leverantörer av samhällsviktiga tjänster som identifieras med stöd av bestämmelserna i Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:xxx) om anmälan och identifiering av leverantörer av samhällsviktiga tjänster.

Bland de som kommer att identifieras som leverantör av samhällsviktiga tjänster finns statliga myndigheter, kommuner, landsting och företag.

Val av kriterier för rapporteringspliktiga incidenter i respektive sektor

I föreskrifterna om incidentrapportering tydliggörs inte bara när och hur rapportering ska ske utan även vilka incidenter som ska anses som rapporteringspliktiga. Leverantörer av samhällsviktiga incidenter är enligt 18 § lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster skyldiga att rapportera incidenter som har en betydande inverkan på kontinuiteten i en samhällsviktig tjänst. Myndigheten för samhällsskydd och

beredskap får, efter att ha gett tillsynsmyndigheterna och Socialstyrelsen tillfälle att yttra sig, meddela föreskrifter om vad som avses med en betydande inverkan.

Vid bedömning om vad som ska avses med betydande inverkan ska enligt förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster särskilt beaktas:

1. det antal användare som påverkas av störningen i den samhällsviktiga tjänsten,
2. hur länge incidenten varar, och
3. hur stort geografiskt område som påverkas av incidenten.

Nedan följer en redogörelse för de överväganden som har skett i arbetet med att närmare tydliggöra innebörden av betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten och därmed vilka incidenter som är rapporteringspliktiga. Utgångspunkten har varit att nyttja samtliga av de tre ovan nämnda kriterierna. Detta har dock för vissa tjänster inte varit fullt ut möjligt. I de fall något eller några av kriterierna antal påverkade användare, tid eller geografiskt område inte omnämnts har de bedömts vara svåra att tillämpa på den aktuella sektorn eller delsektorn och ska därför inte beaktas vid bedömningen av om incidenten är rapporteringspliktig eller inte.

Genomgående har ambitionen varit att beskriva betydande inverkan på ett sådant tydligt sätt att det ska vara förhållandevis enkelt att göra bedömningen om det är en rapporteringspliktig incident eller inte. Ett sätt att uppnå detta har varit att, där så är möjligt, ansluta till befintlig reglering och begreppsanvändning inom respektive sektor och delsektor. Detta har exempelvis resulterat i bedömningen av vilka incidenter som är rapporteringspliktiga inom hälso- och sjukvårdssektorn som kopplas till 3 kap 5 § första stycket patientsäkerhetslagen (2010:659), även kallad lex Maria, istället för påverkade användare, tid eller geografiskt område.

Samtliga kriterier har tagits fram i mycket nära samverkan med respektive tillsynsmyndighet.

Samhällsviktiga tjänster inom Energi

Med betydande inverkan avses i denna bestämmelse

1. leveransavbrott i minst två timmar, eller
2. att styrning och övervakning av stamnätstjänst, regionnätstjänst eller elproduktion inte har kunnat genomföras under minst två timmar.

Nivåerna inom el utgår från tidskriteriet och är baserade på de krav som ställs i Energimarknadsinspektionens föreskrifter (2015:4) om skyldighet att rapportera elavbrott för bedömning av leveranssäkerheten i elnäten samt förda resonemang i Energimyndighetens utredning *Grundläggande säkerhetsnivåer GSN Energi 2012-9068*.

För tydlighetens skull har en uppdelning skett mellan leveransavbrott och styrning och övervakning av eltjänsten. För att leveranskvaliteten av flera tjänster ska kunna garanteras måste styrning och övervakning fungera, även om inget leveransavbrott har skett och energileveransen fungerar som avsett. Kravet att rapportera avbrott i styrning och övervakning har avgränsats till stamnätstjänst, regionnätstjänst och elproduktion.

Motsvarande resonemang har förts inom gas. Med betydande inverkan avses i denna bestämmelse

1. leveransavbrott i minst två timmar, eller
2. att styrning och övervakning inom ramen för systemansvarstjänst inte har kunnat genomföras under minst två timmar.

Tidsramarna på två timmar har valts utifrån Energimyndighetens utredning *Grundläggande säkerhetsnivåer GSN Energi 2012-9068*. Även inom gasområdet har en uppdelning mellan leveransavbrott respektive styrning och övervakning skett för att öka tydligheten.

Motsvarande val rörande uppdelning samt tidsfaktor har gjorts rörande olja och även här har Energimyndighetens utredning *Grundläggande säkerhetsnivåer GSN Energi 2012-9068* legat till grund för de avväganden som gjorts.

Samhällsviktiga tjänster inom transport

Inom sektorn transport kan det finnas ett inbördes beroende inom och mellan olika trafikslag. En infrastrukturförvaltares tillhandahållande av en tjänst utgör en förutsättning för andra leverantörers förmåga att tillhandahålla sina tjänster, till exempel flygplatser och lufttrafikföretag. Likaså kan godstransport på järnväg och mottagande av gods i hamnar vara beroende av varandra för att godstransporten ska fungera.

Genomgående för samtliga trafikslag är att tidsfaktorn är en central aspekt. Därtill kan antalet användare, exempelvis passagerare och hur stort område som påverkas ha betydelse för bedömningen av om en störning kan anses ha en betydande inverkan. En störning i Stockholms tunnelbana bedöms få stora konsekvenser redan efter en timme, i synnerhet med hänsyn till det stora antalet användare. En timme är också ett mått som ofta används i resenärsvillkor gällande ersättning vid resor. En störning kan därtill få stora konsekvenser om trafikledningen slås ut inom ett visst geografiskt område. I dessa fall kan det vara svårt att avgöra antalet användare och området kan då vara en lämpligare faktor.

Störningar som påverkar ≥1000 användare eller ett geografiskt område ≥10 000 km² får anses ha en sådan betydande inverkan på tjänsten att störningen ska rapporteras. Incidenter som drabbar färre antal användare respektive ett mindre geografiskt område ska rapporteras om störningen varar i två timmar eller mer.

Samhällsviktiga tjänster inom bankverksamhet

Inom bankverksamhet relaterar kriterierna till antal transaktioner, antal användare och störningens längd avseende betaltjänster enligt 1 kap. 2 § punkt 1-6 lag (2010:751) om betaltjänster. Kriterierna överensstämmer i stora drag med de incidentrapporteringskrav som ställs i Europaparlamentets och rådets direktiv (EU) 2015/2366 (PSD 2) om betaltjänster på den inre marknaden, om ändring av direktiven 2002/65/EG, 2009/110/EG och 2013/36/EU samt förordning (EU) nr 1093/2010 och om upphävande av direktiv 2007/64/EG (PSD) och dess högre effektnivåer. Vissa avsteg har föreslagits i syfte att tydliggöra att rapporteringskravet enligt NIS-regleringen ligger på en högre nivå än den nivå som är aktuell för att kravet på rapportering av allvarliga incidenter eller säkerhetsincidenter enligt PSD2 ska infinna sig. PSD2:s lägre effektnivåer bedöms inte vara relevanta för NIS-regleringen.

Samhällsviktiga tjänster inom finansmarknadsinfrastruktur

Inom finansmarknadsinfrastruktur relaterar kriterierna till störningens längd, påverkan på konnektivitet och påverkan på andra system av vikt för finansiella infrastrukturföretag. Kriterierna är i linje med CPMI-IOSCO:s principer för finansmarknadsinfrastruktur samt de incidentrapporteringskrav som ställs i EU:s direktiv om värdepappersmarknaden (Mifid 2), vilken har genomförts i svensk rätt, främst i lag (2007:528) om värdepappersmarknaden, och Kommissionens delegerade förordning (EU) 2017/584 av den 14 juli 2016 om komplettering av Europaparlamentets och rådets direktiv 2014/65/EU avseende tekniska tillsynsstandarder som specificerar organisatoriska krav för handelsplatser (Text av betydelse för EES.).

Konnektivitet definieras som förmåga att utbyta information mellan två separata it-system eller datacenter som är uppkopplade genom nätverk. Konnektivitet har stor betydelse för en väl fungerande marknad och finansiell stabilitet. En störning i konnektivitet hos handelsplatser innebär att en ordnad handel i finansiella instrument inte kan genomföras.

Samhällsviktiga tjänster inom hälso- och sjukvård

Det finns ett stort antal aktörer i sektorn, både offentliga och privata. Inom sektorn finns en etablerad rutin för att rapportera avvikelser som leder till allvarliga vårdskador enligt 3 kap 5 § första stycket patientsäkerhetslagen (2010:659), även kallad lex Maria.
De lex Maria-tillbud som beror på att nätverk eller informationssystem inte fungerat tillfredsställande ska enligt kriterierna rapporteras i enlighet med NIS-regleringen, utöver gängse rutiner för lex Maria. Här har fördelarna med att ansluta till existerande rapporteringsrutiner setts överväga alternativet med att formulera nya kriterier utifrån tid, antal användare och geografiskt område.

Samhällsviktiga tjänster inom leverans och distribution av dricksvatten

Med betydande inverkan inom leverans och distribution av dricksvatten avses leveransavbrott i minst två timmar, eller att styrning och övervakning av tjänsten inte har kunnat genomföras under en tidsperiod om minst två timmar. Även här har tidskriteriet setts som det mest tydliga och användbara. Dessutom har en uppdelning skett mellan leveransavbrott respektive styrning och övervakning. Om vatten inte kan levereras under en period som överstiger två timmar ska detta ses som en rapporteringspliktig incident. Leveransavbrott kan exempelvis orsakas av att någon del i styr- och kontrollsystemet eller underliggande utrustning inte fungerar som avsett. De flesta verk går på automatik vid strömbortfall eller datorhaveri, exempelvis avseende reservkraft. Efter två timmar blir det dock nödvändigt att vidta åtgärder för att säkerställa driften eftersom verket då måste få kontroll på nivåer i torn eller ta ut reservel till tryckstegringspumpar m.m.

Punkt två avser funktionen i de industriella styr- och kontrollsystemen, inte leveransen av dricksvatten. I det fall kontrollen har gått förlorad så att det i över två timmar inte har gått att styra och övervaka tjänsten ska detta ses som en rapporteringspliktig incident. Oförmåga att styra och övervaka tjänsten behöver inte samtidigt innebära att dricksvatten inte kan tillhandahållas, åtminstone under en begränsad period. Även här är tidsfaktorn satt till två timmar för att anknyta till regeln om leveransavbrott.

Samhällsviktiga tjänster inom digital infrastruktur

För att ständigt kunna tillhandahålla 100 procent tillgänglighet i en DNS-tjänst, behöver leverantören av DNS-tjänsten bl.a. ha dimensionerat och säkerställt överkapacitet för dels namnservrar, dels för internetanslutningar. DNS-tjänsten kräver en fungerande IP-transportfunktion. Om transportfunktionen utsätts för svåra störningar, t.ex. till följd av överbelastning, resulterar detta ofta i paketförluster och paketfördröjningar, vilket då även drabbar DNS-tjänsten.

När det gäller registreringsenheter för toppdomäner ska incidenter som innebär att en toppdomäns namnservertjänst har en tillgänglighet på mindre än 100 procent rapporteras. Detsamma gäller rekursiva och auktoritativa namnservertjänster om tillgängligheten är mindre än 100 procent under en viss sammanhängande period.

För toppdomänens namnservertjänst och auktoritativa namnservertjänster har det i föreskrifterna satts ett kriterium på 2 500 domännamn då det innebär att 10 procent av domännamnen påverkats för en leverantör. Enligt samma princip är gränsen 10 000 användare för leverantörer av rekursiva namnservertjänster.

MSB bedömer att merparten av de leverantörer som omfattas av kravet inte incidentrapporterar idag.

Uppgifter om de bemyndiganden som myndighetens beslutanderätt grundar sig på

Bemyndigandet grundar sig på 9, 13, 14 §§ förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Uppgifter om vilka kostnadsmässiga och andra konsekvenser regleringen medför och en jämförelse av konsekvenserna för de övervägda regleringsalternativen

Kostnader för leverantörer av samhällsviktiga tjänster bör bedömas i ett helhetsperspektiv tillsammans med Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:xxx) om informationssäkerhet för leverantörer av samhällsviktiga tjänster (se även konsekvensutredning med dnr 2017–11001). Tillsammans med de föreskrifterna kommer leverantörer på längre sikt att minska sin risk för störningar och därmed kunna erbjuda mer stabila leveranser och höja sin konkurrenskraft.

För de leverantörer som inte bedriver ett systematiskt och riskbaserat arbete idag kan krav i föreskrifterna initialt ge obetydligt ökade kostnader. De flesta leverantörer torde dock redan i dag arbeta med informationssäkerhet på något sätt. Kravet på incidentrapportering kan för flertalet leverantörer vara en ny uppgift och därmed ge upphov till nya kostnader. Dessa bedöms infalla främst i det initiala uppbyggnadsskedet i form av administrativa kostnader då anpassning av processer och rutiner kan behöva ske. MSB arbetar med att ta fram ett tekniskt gränssnitt för incidentrapportering. Detta kommer att underlätta för leverantörer att rapportera incidenter.

Statliga myndigheter har sedan 4 april 2016 krav på sig att rapportera it-incidenter enligt Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2016:2) om statliga myndigheters rapportering av it-incidenter. Kraven i föreliggande förslag till föreskrifter skiljer sig något från gällande föreskrifter för statliga myndigheter. Myndigheterna ska dock ha ett upparbetat arbetssätt för att kunna rapportera it-incidenter, vilket kan användas även för att uppfylla kraven på rapportering i föreliggande förslag.

För de leverantörer som utkontrakterar sin informationshantering kan det uppstå vissa initiala kostnader i samband med att processer och rutiner kan behöva anpassas och eventuellt nya avtal skrivas.

Föreskriftskravet att initial notifiering ska ske inom sex timmar efter att leverantören har identifierat en incident som rapporteringspliktig och uppföljande rapportering inom 24 timmar ska inte tolkas som krav på ökad bemanning. Tidsfristen räknas från den tidpunkt då leverantören med stöd av

sina interna processer och rutiner identifierat en incident som rapporteringspliktig. Bedömningen är att incidentrapportering därför sker efter att de första kritiska åtgärderna för att avhjälpa incidenten har vidtagits. Vidare är den mängd information som ska lämnas inom sex timmar och även anvisade kontaktvägar anpassade efter skyndsamhetskravet.

Tidsfristen på sex timmar är framtagen med anledning av möjligheten för CERT-SE (Sveriges Computer Emergency Response Team) att vid behov och när så är möjligt hjälpa leverantören med incidenten. I och med kravet på initial notifiering på sex timmar och sedan uppföljande rapportering inom 24 timmar kan CERT-SE och MSB skapa en samlad lägesbild. Vid inrapporterad incident bedömer CERT-SE om det finns behov av att agera på incidenten. Därefter inleds eventuellt incidenthantering som bland annat kan innebära kontakt med rapporterande leverantör och andra drabbade, sökning bland tillgänglig information och hos CERT-SE:s kontaktnät, informera allmänheten eller samordna åtgärder, informera andra aktörer, såväl nationellt som internationellt. MSB ska, för Sveriges räkning, informera övriga medlemsstater om gränsöverskridande incidenter. Leverantören kan också av MSB få hjälp att vid behov hantera de störningar som incidenten medför i den samhällsviktiga tjänsten. Inkomna rapporter vidarebefordras skyndsamt till berörd tillsynsmyndighet samt avseende incidenter inom sektorn hälso- och sjukvård till Socialstyrelsen. Enligt MSB:s bedömning kommer inte tidskraven att föranleda att leverantörerna drabbas av ökade kostnader i någon större utsträckning annat än i det initiala uppbyggnadsskedet.

Syftet med NIS regleringen är att skapa en hög nivå av säkerhet i nätverk och informationssystem för samhällsviktiga och digitala tjänster. De kriterier som finns i föreskrifterna för rapporteringspliktiga incidenter har utarbetats i samverkan med tillsynsmyndigheterna. Kriterierna ska säkerställa att sådana incidenter som påverkar kontinuiteten i de samhällsviktiga tjänsterna hanteras och i förlängningen kan förebyggas. Även om en incident kan vara allvarlig ur leverantörens perspektiv behöver den inte få en betydande inverkan på en samhällsviktig tjänst. För att använda samhällets resurser på ett effektivt sätt ska inte alla inträffade incidenter rapporteras. Kriterierna ska tydliggöra gränsdragningen.

För samhällsekonomin kommer den ökade tillförlitligheten som ett systematiskt arbete med informationssäkerhet ger de samhällsviktiga tjänsterna vara viktig. Sveriges stora beroende av nätverk och informationssystem gör att brister får större inverkan på samhället och samhällsekonomin. Brister i informationshanteringen, oavsett orsak, kan ge omfattande ekonomisk skada, undergräva användarnas förtroende för tjänsterna och medföra stor samhällspåverkan. Incidentrapporteringen är en åtgärd för att förebygga och minimera verkningar av incidenter för att säkerställa kontinuiteten i de samhällsviktiga tjänsterna.

Bedömning av om regleringen överensstämmer med eller går utöver de skyldigheter som följer av Sveriges anslutning till Europeiska unionen

Bedömningen är att föreskrifterna överensstämmer med de skyldigheter som följer av Sveriges medlemskap i Europeiska unionen.

Bedömning av om särskilda hänsyn behöver tas när det gäller tidpunkten för ikraftträdande och om det finns behov av speciella informationsinsatser

Direktivet börjar gälla från den 10 maj 2018, lag och förordning träder i kraft 1 augusti samma år, föreskrifterna behöver träda ikraft så snart som möjligt efter detta datum. Med hänsyn till remiss och beredningsprocess bedöms ikraftträdande kunna ske under sista kvartalet 2018.

De leverantörer som berörs av föreskrifterna kommer att behöva informeras genom speciella informationsinsatser som koordineras med respektive tillsynsmyndighet.

B. Kommuner och landsting

Markera med x

( ) Regleringen bedöms inte få effekter för kommuner eller landsting.

(X) Regleringen bedöms få effekter för kommuner eller landsting.

Beskrivning av effekter för kommuner eller landsting

Kommuner och landsting som är leverantör av samhällsviktiga tjänster berörs av NIS-regleringen. Det görs ingen åtskillnad mellan offentliga och privata aktörer. Effekterna beskrivs primärt under avsnittet "Uppgifter om vilka kostnadsmässiga och andra konsekvenser regleringen medför och en jämförelse av konsekvenserna för de övervägda regleringsalternativen".

C. Företag

Med företag avses här en juridisk eller en fysisk person som bedriver näringsverksamhet, det vill säga försäljning av varor och/eller tjänster yrkesmässigt och självständigt. Att yrkesmässigt bedriva näringsverksamhet bör tolkas brett.

Markera med x

( ) Regleringen bedöms inte få effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt. Konsekvensutredningen innehåller därför inte någon beskrivning av punkterna i avsnitt C.

(X) Regleringen bedöms få effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt. Konsekvensutredningen innehåller därför en beskrivning av punkterna i avsnitt C.

Beskrivning av antalet företag som berörs, vilka branscher företagen är verksamma i samt storleken på företagen

Leverantörer av samhällsviktiga tjänster finns inom sju sektorer, energi, transporter, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt digital infrastruktur.

I de flesta sektorer behöver företagen vara relativt stora för att falla under de kriterier som gäller för att definieras som leverantör av samhällsviktiga tjänster. Det är i nuläget inte möjligt att uppge antal företag som berörs inom respektive sektor. Antalet berörda företag kommer att variera beroende på sektor. I konsekvensutredningen för Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:xxx) om anmälan och identifiering av leverantörer av samhällsviktiga tjänster med dnr 2018:05893 görs en uppskattning för respektive sektor och delsektor.

Regleringen kan innebära att leverantörer av samhällsviktiga tjänster ställer utifrån lagstiftningen anpassade krav på sina underleverantörer. Sådana krav kan komma att träffa både stora och mindre företag. Grundprincipen är att det är upp till parterna att i avtal reglera fördelning av kostnader och ansvar.

Beskrivning av vilken tidsåtgång regleringen kan föra med sig för företagen och vad regleringen innebär för företagens administrativa kostnader.

Förmåga att identifiera och rapportera incidenter till MSB i enlighet med regleringen på området förutsätter att leverantören av samhällsviktiga tjänster har rutiner för intern incidenthantering. Befintliga arbetsprocesser och rutiner behöver sannolikt anpassas för att stämma överens med föreskrifterna och för att underlätta användning av MSB:s tekniska gränssnitt för rapportering. Tillkommande administrativa kostnader för extern rapportering bedöms inte tillföra några omfattande kostnader. Särskilt då det inte är alla incidenter som ska rapporteras, utan endast de som bedöms ha en betydande inverkan på kontinuiteten i den samhällsviktiga tjänst som de tillhandahåller. De företag som behöver bygga upp sin interna incidenthantering från grunden kommer att behöva tillföra resurser för detta.

Beskrivning av vilka andra kostnader den föreslagna regleringen medför för företagen och vilka förändringar i verksamheten som företagen kan behöva vidta till följd av den föreslagna regleringen

För de leverantörer som inte bedriver ett systematiskt och riskbaserat arbete idag som möjliggör extern rapportering av incidenter kan kraven i föreskrifterna initialt ge obetydligt ökade kostnader då befintliga arbetsprocesser och rutiner sannolikt behöver anpassas för att stämma överens med föreskrifterna och underlätta användning av MSB:s tekniska gränssnitt för rapportering. De flesta leverantörer torde redan i dag arbeta med informationssäkerhet på något sätt.

Beskrivning av i vilken utsträckning regleringen kan komma att påverka konkurrensförhållandena för företagen

Ett av syftena med regleringen är att säkerställa att leverantörer får förutsättningar för att konkurrera på lika villkor genom att alla leverantörer av samhällsviktiga tjänster arbetar utifrån samma krav avseende säkerhet i nätverk och informationssystem och incidentrapportering. Detta motverkar att en leverantör erbjuder en tjänst till lägre pris för att därefter ta ut extra kostnader från sina kunder när leveransen på grund av bristande informationssäkerhet inte fungerar. De leverantörer av samhällsviktiga tjänster som idag arbetar systematiskt och riskbaserat få därmed en mer rättvis konkurrenssituation. Kravet på incidentrapportering är lika för leverantörerna. Leverantörer som drabbas av många incidenter måste naturligtvis i högre grad rapportera till myndigheterna.

Beskrivning av hur regleringen i andra avseenden kan komma att påverka företagen

Rapportering medför att CERT-SE vid behov och när så är möjligt kan hjälpa leverantören med incidenten. Leverantören kan även få hjälp av MSB att vid behov hantera de störningar som incidenten medför i den samhällsviktiga tjänsten. Leverantörer kan också få varningar när andra leverantörer rapporterar om incidenter, som kan få påverkan på andra leverantörer och på så sätt kunna vidta åtgärder i tid.

Den kunskapsbank som MSB kan bygga upp tack vare incidentrapporteringen och analyser som genomförs av informationen ger underlag till utvecklingen av råd och stöd som kan förmedlas till leverantörerna.

Beskrivning av om särskilda hänsyn behöver tas till små företag vid reglernas utformning

Ingen särskild hänsyn har tagits till små företag i föreskrifterna. Dessa bedöms endast i undantagsfall beröras av regleringen.

I de fall små företag berörs är det på grund av att de tjänster de levererar är samhällsviktiga, några särskilda undantag avseende kravställningen ska därför inte göras.

D. Samråd

Beskrivning av ett eventuellt tidigt samråd

I syfte att få underlag till utformningen av regleringen har tillsynsmyndigheterna vid ett flertal tillfällen fått lämna synpunkter på tidiga utkast på föreskrifter och allmänna råd. Tillsynsmyndigheterna har stor kunskap om respektive sektor och har kunnat bidra med värdefulla synpunkter.

Något formellt samråd med direkt berörda leverantörer av samhällsviktiga tjänster har inte genomförts, men vissa tillsynsmyndigheter har informerat inom sin sektor om NIS-direktivet i olika fora och även tagit med synpunkter in i arbetet med MSB.

E. Kontaktpersoner

Ange vem som kan kontaktas vid eventuella frågor

Kontaktperson för konsekvensutredningen gällande föreskrifter om rapportering av incidenter för leverantörer av samhällsviktiga tjänster är Carina Wetzel som lämpligast nås på carina.wetzel@msb.se
eller 010-240 42 62 alternativt 0702-42 16 64