Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster

A. Allmänt

Beskrivning av problemet och vad man vill uppnå

Den ökade digitaliseringen och det förändrade omvärldsläget ökar samhällets behov av att skydda sin information. Nya sätt att hantera, lagra och kommunicera information medför nya risker. De nya riskerna beror på samhällets ökade beroende av olika informationstjänster och på hotet från dem som ser möjligheter med att utnyttja sårbarheter i existerande informationstjänster.

Samhället behöver därför bli bättre i arbetet med informations- och cybersäkerhet.

I strävan efter att förbättra samhällets skydd av information har EU beslutat införa gemensamma krav på skyddsåtgärder i nätverk och informationssystem för leverantörer av speciellt viktiga tjänster. Avsaknaden av gemensamma krav har medfört att konsumenter och företag inom EU har svårt att jämföra olika tjänster som erbjuds i olika europeiska länder. Det blir också svårt för företag att på ett affärsmässigt sätt utveckla it- och nätverkstjänster med tillräckliga säkerhetsåtgärder när det inte finns ett gemensamt sätt för företagen att beskriva sin nivå av säkerhet och för kunderna att förstå vad de betalar för när produkter utvecklas och erbjuds på marknaden, med olika nivåer av säkerhet.

EUs beslut att bättre hantera riskerna i samhällets informationshantering har resulterat i NIS-direktivet. NIS-direktivet sätter bindande miniminivåer för informationssäkerheten och EUs medlemsländer kan välja att lägga sig på samma nivå eller nationellt skärpa kraven jämfört med direktivet.

I Sverige genomförs NIS-direktivet genom en ny lag, lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. I lagförslagets

11§ ställs krav på att leverantörer av samhällsviktiga tjänster ska bedriver ett systematiskt och riskbaserat arbete för att uppnå god informationssäkerhet.

De utifrån direktivet utpekade leverantörerna av samhällsviktiga tjänster ska alla uppnå en hög nivå av informationssäkerhet i sina nätverks- och informationssystem. Genom ett systematiskt och riskbaserat arbete med att införa säkerhetsåtgärder i nätverk- och it-system ökar chansen för att tjänsternas kontinuitet upprätthålls och hela samhällets skydd mot oönskade driftavbrott, oönskad åtkomst och brister i informationens riktighet förbättras.

Leverantörer av samhällsviktiga tjänster kan vara statliga myndigheter, kommuner, landsting eller företag. För statliga myndigheter har reglering om att arbeta systematiskt med informationssäkerhet funnits under en längre tid. Myndigheternas krav på informationssäkerhetsarbete regleras idag föreskriften MSBFS 2016:1. Övriga aktörer arbetar i de allra flesta fall redan idag med informationssäkerhet på något sätt. Arbetet sker ofta utifrån egna identifierade krav eller från branschspecifika regelverk där krav på säker informationshantering antingen är reglerat utifrån lag, överenskommet på annat sätt eller följs på eget initiativ av leverantören.

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

NIS-direktivet är bindande och måste införas i nationell rätt. För de leverantörer som definieras som samhällsviktiga enligt myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018: xxx) om anmälan och identifiering av leverantörer av samhällsviktiga tjänster kan medlemsländerna i EU välja att anta eller behålla existerande bestämmelser som har samma syfte som NIS-direktivet. Medlemsländerna kan också anta eller behålla bestämmelser som ställer krav på en högre nivå av säkerhet i nätverk och informationssystem än de som finns beskrivna i NIS-direktivet.

Sverige har valt att införa NIS-direktivet genom en ny lag, lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster och en ny förordning, förordning (2018:1175) om informationssäkerhet i samhällsviktiga och digitala tjänster.

I 7 § förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster ges myndigheten för samhällsskydd och beredskap bemyndigande att ge ut föreskrifter om ett systematiskt och riskbaserat informationssäkerhetsarbete för leverantörer av samhällsviktiga tjänster.

I 11§ lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster ställs krav på att leverantörer av samhällsviktiga tjänster ska bedriva ett systematiskt och riskbaserat arbetssätt.

I de föreslagna föreskrifterna ställs krav på att det systematiska och riskbaserade informationssäkerhetsarbetet ska bedrivas utifrån internationellt accepterade standarderna SS-EN ISO/IEC 27001 och SS-EN ISO/IEC 27002 vilka bygger på samlade erfarenheter från olika verksamheter och länder för att uppnå ett effektivt sätt arbete med informationssäkerhet. Syftet med standarderna är att hantera risker kopplade till hantering av information inklusive när informationen hanteras i nätverk och it-system. Leverantörernas arbete utifrån standarderna SS-EN ISO/IEC 27001 och SS-EN ISO/IEC 27002 kommer att innebära att de olika sektorerna arbetar på samma sätt för att identifiera de säkerhetsåtgärder som är lämpliga utifrån den enskilde leverantören och sektorn i stort. Genom att utgå från ett gemensamt välkänt arbetssätt kan även tillsyn genomföras på liknande sätt i alla sektorer. Jämförbarheten bidrar till att säkerställa att en hög gemensam nivå av informationssäkerhet uppnås i berörda sektorer.

Ett alternativ skulle vara att i föreskrifterna ställa krav på att leverantörerna certifierar sitt informationssäkerhetsarbete. Ett annat alternativ är att i föreskrifterna införa en mer detaljerad kravställning gällande ett systematiskt och riskbaserat arbetssätt utan stöd av standarder. Båda dessa alternativ bedöms som mer kostsamma för leverantörerna av samhällsviktiga tjänster om än möjliga alternativ. Genom att föreskriva om ett arbetssätt, utifrån beprövad standard, där leverantörerna själva identifierar sitt behov av säkerhetsåtgärder eller att leverantörer tillsammans i de olika sektorerna identifierar säkerhetsåtgärder som behövs för deras verksamhet kommer ett bättre anpassat skydd utifrån leverantörens och sektorns identifierade risker, hot och sårbarheter att införas.

Uppgifter om vilka som berörs av regleringen

Föreskrifterna berör de leverantörer av samhällsviktiga tjänster som definieras i myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:xxx) om anmälan och identifiering av leverantörer av samhällsviktiga tjänster.

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

Uppgifter om de bemyndiganden som myndighetens beslutanderätt grundar sig på

Bemyndigandet grundar sig på 7 § i förordning 2018:1175 om informationssäkerhet för samhällsviktiga och digitala tjänster.

”Myndigheten för samhällsskydd och beredskap får, efter att ha gett tillsynsmyndigheterna och Socialstyrelsen tillfälle att yttra sig, meddela föreskrifter om systematiskt och riskbaserat informationssäkerhetsarbete enligt 11 § lagen (2018:1174) 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 relaterat till föreskriften bör ses ut ett kortare, initialt, och ett längre tidsperspektiv.

Initialt kan föreskriftens krav på att leverantören ska bedriva ett systematiskt och riskbaserat arbetssätt ge obetydligt ökade kostnader för de leverantörer som inte bedriver ett sådant arbete idag. Bedömningen är dock att flertalet av leverantörerna arbetar med informationssäkerhet på något sätt och att leverantörer i flera av de utpekade sektorerna följer andra regelverk som ställer krav på informationssäkerhet på en nivå som helt eller i stora delar uppfyller de krav på säker informationshantering som ställs i föreskrifterna.
I de fall leverantören är en statlig myndighet tillkommer inga extra kostnader då dessa redan ska arbeta systematiskt med sin informationshantering.

På längre sikt kommer föreskrifternas krav att innebära att leverantörerna arbetar kontinuerligt och effektivt för att uppnå tillräcklig säkerhet i sina leveranser. Leverantören kommer därmed att, över tid, minska sin risk för störningar i sina leveranser och därmed erbjuda stabilare leveranser till sina kunder och höja sin konkurrenskraft.

Kunder och konsumenter av de tjänster som leverantörerna erbjuder kan initialt få högre kostnad om leverantören beslutar att ta ut en högre kostnad för tjänsten för att uppnå ställda krav på informationssäkerhet. Kunder till leverantörer som redan har ett systematiskt informationssäkerhetsarbete bör inte få ytterligare kostnader.

För samhällsekonomin kommer den ökade tillförlitligheten som ett systematiskt och riskbaserat arbete med informationssäkerhet ger de samhällsviktiga tjänsterna vara viktig. Sveriges stora beroende av nätverk och informationssystem gör att brister i dessa kan få stor inverkan på samhällets funktionalitet. Brister i informationshanteringen, oavsett orsak, kan ge omfattande ekonomisk skada, undergräva användarnas förtroende för tjänsterna och medföra stor samhällspåverkan. Genom ett systematiskt och riskbaserat informationssäkerhetsarbete ökar tillförlitligheten i nätverk och informationssystem och förutsättningar för att skapa samhällsekonomiska vinster genom fortsatt förtroende för digitaliseringen, på kort och lång sikt.

De övervägda regleringsalternativen är krav på certifiering respektive krav på systematiskt och riskbaserat arbete med informationssäkerheten utan stöd av standarderna, SS-EN ISO/IEC 27001 och SS-EN ISO/IEC 27002.

Kostnader för leverantörerna av samhällsviktiga tjänster att genomgå certifiering bedöms bli betydligt högre än det valda regleringsalternativet. Likaså bedöms konsekvenserna av att inte basera det systematiska och

riskbaserade informationssäkerhetsarbetet på ovan nämna standarderna ger för dåligt stöd till leverantören för hur arbetet ska bedrivas för att nå den effekt som uttrycks genom regleringen. Otillräckligt stöd i arbetet med informationssäkerhet kan ge högre kostnader för leverantörer, konsumenter och samhället i stort då leverantören inte uppnår lämplig nivå av informationssäkerhet.

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

Lag och förordning börjar gälla från den 1 augusti 2018. Föreskrifterna bör träda ikraft så snart som möjligt efter detta datum. Med hänsyn till tid som behövs för remiss och beredningsprocess bedöms ikraftträdandet kunna ske under sista kvartalet 2018.

De sektorer vars leverantörer kommer att beröras av föreskrifterna kommer att behöva informeras om föreskrifterna och tillhörande allmänna råd samt det stöd som finns bland annat på www.informationssakerhet.se för att driva ett systematiskt och riskbaserat informationssäkerhetsarbete.

Informationsinsatser koordineras med tillsynsmyndigheterna.

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 berörs utifrån att de kan vara leverantör av samhällsviktiga tjänster. Kommuner och landsting berörs i så fall på samma sätt som andra leverantörer av samhällsviktiga tjänster. För de kommuner och landsting som idag inte bedriver ett systematiskt och riskbaserat informationssäkerhetsarbete kan en initial kostnad uppkomma men på längre sikt kommer leverantören genom färre problem i sina tjänster få ökat förtroende hos sina kunder och minskade kostnader för avbrott i tjänsterna.

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

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

Företag kan bedriva verksamhet inom alla sektorer. 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. Som underleverantör till leverantör av samhällsviktiga tjänster kan dock mindre företag bli aktuella.

De mindre företagen som är underleverantörer kommer då att beröras av de säkerhetskrav leverantören av samhällsviktiga tjänster ställer på underleverantörer utifrån föreskrifternas krav. Grundprincipen är att det är upp till parterna att regler i avtal de kostnader och det ansvar som faller på underleverantören respektive leverantören för att denne ska kunna leverera den samhällsviktiga tjänsten utifrån ställda legala krav.

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

Ett systematiskt och riskbaserat informationssäkerhetsarbete pågår ständigt och behöver kontinuerligt anpassas till nya förutsättningar. Kostnaden för att arbeta med informationssäkerhet på ett systematiskt och riskbaserat sätt varierar utifrån hur väl arbetet sker hos leverantören idag och den samhällsviktiga verksamhet som företaget bedriver.

För de flesta företag tillkommer ingen kostnad då de redan idag styrs av reglering som motsvarar eller är högre än kommande föreskrifter. För de företag som behöver bygga upp ett systematiskt och riskbaserat informationssäkerhetsarbete från grunden kan omfördelning av de resurser som redan arbetar på annat sätt med att upprätthålla leveranser till viss del ske genom att företagen flyttar fokus från hanterande till förebyggande arbete. En viss initial kostnad, under ett till två år, innan effekten av säkrare leveranser kan hämtas hem kan dock inte uteslutas.

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

Utifrån företagens nuvarande kompetens kan kostnader för utbildning i hur ett systematiskt och riskbaserat arbete, utifrån standarderna SS-EN ISO/IEC 27001 och SS-EN ISO/IEC 27002 eller motsvarande bedrivs, tillkomma.

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. Att en leverantör kan erbjuda en tjänst till lägre pris för att därefter ta ut extra kostnader från sina kunder när leveransen inte fungerar kan inte anses gynna konkurrensförhållandena. De leverantörer av samhällsviktiga tjänster som idag arbetar systematiskt och riskbaserat och genom detta levererar en tillförlitlig tjänst kan få en mer rättvis konkurrenssituation.

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

De företag som påverkas av regleringen kan få fördel vid leverans av andra tjänster än de samhällsviktiga då företaget genom att arbeta systematiskt och riskbaserat med informationssäkerhet får en högre tillförlitlighet och kontroll på sin informationshantering i alla delar av verksamheten. Företaget kan marknadsföra sig som en leverantör som arbetar utifrån de krav som ställs i gällande föreskrifter.

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

Ingen särskild hänsyn har tagits till små företag i föreskrifterna. Det systematiska och riskbaserade informationssäkerhetsarbetet så som det kravställs i föreskrifterna, att arbeta utifrån standarderna, bygger på att arbetet ska anpassas utifrån leverantörens verksamhet vilket innebär att små företag utgår från sina förutsättningar i sitt systematiska och riskbaserade informationssäkerhetsarbete.

I de fall små företag kontrakteras som underleverantör av leverantör av samhällsviktiga tjänster kommer leverantören av samhällsviktiga tjänster att ställa de krav på företagets verksamhet som krävs för att uppfylla lagens intention. Parternas avtal reglerar kostnader.

D. Samråd

Beskrivning av ett eventuellt tidigt samråd

Information till tillsynsmyndigheterna om föreskriftens utformning har givits vid ett flertal tillfällen i samband med de samrådsmöten som MSB genomfört inom ramen för uppdraget att samordna aktiviteter relaterade till införandet av regleringen. Tillsynsmyndigheterna har haft möjlighet att inkomma med synpunkter vilket har varit ett värdefullt bidrag i arbetet.

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 tillbaka till MSB.

E. Kontaktpersoner

Ange vem som kan kontaktas vid eventuella frågor

Kontaktperson för konsekvensutredningen gällande föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster är Tove Wätterstam som lämpligas nås på tove.watterstam@msb.se eller 010-240 4182.