Konsekvensutredning rörande Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälning och identifiering av väsentliga och viktiga verksamhetsutövare

Allmänt

Beskrivning av problemet och vad man vill uppnå

Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS2-direktivet) ska implementeras och börja tillämpas av medlemsstaterna den 18 oktober 2024.

Syftet med NIS2-direktivet är förbättra den inre marknadens funktion genom att fastställa åtgärder för att uppnå en hög gemensam nivå på cybersäkerhet.

Det första NIS-direktivet genomfördes i svensk rätt genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen) och den tillhörande förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-förordningen). Regleringen innebar bland annat att vissa leverantörer av samhällsviktiga respektive digitala tjänster skulle vidta säkerhetsåtgärder för att hantera risker och förebygga incidenter i nätverks- och informationssystem som de använder för att kunna tillhandahålla tjänsterna. Leverantörerna skulle också rapportera incidenter som hade en betydande respektive avsevärd inverkan på kontinuiteten i tjänsterna. NIS-direktivet gällde för leverantörer av samhällsviktiga tjänster inom sju särskilt definierade sektorer: energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt digital infrastruktur. Därutöver gällde direktivet för leverantörer av digitala tjänster.

Det konstateras bland annat i skäl 2 till NIS2-direktivet att NIS-direktivet inneburit att betydande framsteg gjorts med att öka unionens nivå av cyberresiliens, att nationell kapacitet inrättats och att direktivet bidragit till samarbete på unionsnivå. Dock konstateras även att en översyn av NIS-direktivet avslöjat inneboende brister som hindrar det från att effektivt hantera befintliga och framväxande utmaningar på cybersäkerhetsområdet. I skäl 4 och

5 konstateras också att medlemsstaterna gavs stort utrymme för nationella val vid implementeringen av NIS-direktivet. Detta gjorde att krav på säkerhetsåtgärder och incidentrapportering samt genomförande av tillsyn och efterlevnadskontroll kunde skilja sig i hög grad mellan olika medlemsstater. Skillnaderna bidrog till en fragmentering av den inre marknaden och bedöms kunna ha en skadlig inverkan på dess funktion. Det konstateras i skälen att dessa skillnader skulle kunna leda till att vissa medlemsstater är mer sårbara vad gäller cyberhot, med potentiella spridningseffekter i hela unionen.

NIS2-direktivet skiljer sig från NIS-direktivet på flera sätt bland annat genom att regleringen omfattar betydligt fler aktörer och ställer skärpta och tydligare krav på riskanalyser och vilka säkerhetsåtgärder aktörerna ska vidta och hur incidentrapportering ska genomföras. En annan skillnad är att den nya regleringen kommer att gälla all verksamhet hos aktören istället för som i NIS-direktivet endast säkerhet i de nätverk och informationssystem som används för den samhällsviktiga eller digitala tjänsten.

NIS2-direktivet implementeras i första hand genom kommande cybersäkerhetslag och cybersäkerhetsförordning. Lagstiftaren har därutöver pekat ut en rad områden där lagkraven ytterligare behöver konkretiseras i form av myndighetsföreskrifter.

Arbetet med föreskrifter och konsekvensutredningen utgår, i avsaknad av ännu beslutad lag och förordning, från förslaget på cybersäkerhetslag i propositionen Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag (prop. 2025/26:28) (cybersäkerhetslagen) samt regeringens uppdrag till Myndigheten för samhällsskydd och beredskap att förbereda genomförandet av NIS 2-direktivet, Fö2025/01293.

Föreskrifter om anmälan och identifiering

Förslaget till föreskrifter om anmälan och identifiering av väsentliga och viktiga verksamhetsutövare syftar till att förtydliga en verksamhetsutövares anmälningsskyldighet enligt 2 kap 2 § cybersäkerhetslagen samt kriterier vad gäller:

- undantag från storlekskravet för partnerföretag och anknutna företag enligt 1 kap 4 § cybersäkerhetslagen,
- identifiering av huvudsakligt etableringsställe enligt 1 kap 7 § cybersäkerhetslagen, och
- undantag från kravet på att storleksmässigt motsvara eller vara större än ett medelstort företag enligt 1 kap 5 § p 1 3 cybersäkerhetslagen.

Även nuvarande föreskrifter innehåller regler om hur organisationer som omfattas av det första NIS-direktivets tillämpningsområde ska identifiera och anmäla sig och vilken information som ska lämnas. De nya föreskrifterna innehåller något utökade krav på vilken information som ska lämnas i anmälan

för att svara upp mot kraven i NIS2-direktivet samt kommissionens genomförandeförordning C(2024)7151.[1]

I syfte att uppnå ökad harmonisering mellan medlemsstaterna specificerar direktivet vilken information som ska samlas in för att upprätta en sådan förteckning som respektive medlemsstat enligt artikel 3 i NIS2-direktivet ska föra över de aktörer som omfattas av regleringen. Motsvarande detaljreglering fanns inte i NIS1-direktivet.

Även när det gäller tillämpningsområdet innebär NIS2-direktivets krav en betydligt högre grad av harmonisering mellan medlemsstaterna än det första NIS-direktivet. Detta sker genom att EU slår fast huvudregeln att alla organisationer som bedriver verksamhet som omfattas av bilaga 1 eller 2 i NIS2-direktivet samt uppfyller ett visst storlekskrav ska omfattas av regleringen. Även ytterligare aktörer som identifieras enligt kommande CER-reglering omfattas. Huvudregeln innebär att det inte längre finns samma utrymme på nationell nivå att, såsom i nuvarande föreskrifter, närmare specificera vilka typer av verksamhetsutövare som ska omfattas. Syftet med de nya föreskrifterna är istället att specificera några undantag från huvudregelns storlekskrav. Dessutom är syftet att ge verksamhetsutövare inriktning vid bedömningen av vad som utgör deras huvudsakliga etableringsställe enligt NIS2-direktivets mening.

Uppföljning av konsekvenser av föreskrifter och allmänna råd

Enligt 7 § 5 p i förordningen (2024:183) om konsekvensutredningar ska en myndighet följa upp konsekvenser av sina föreskrifter och allmänna råd. En första uppföljning kommer att ske så snart det är möjligt att utvärdera reglernas effekter och därefter regelbundet.

En övergripande uppföljning av hur de nya reglerna påverkar nivån av cybersäkerhet i Sverige kommer att kunna göras genom att följa resultatutvecklingen i Cybersäkerhetskollen[2]. Cybersäkerhetskollen är samlingsnamnet för myndighetens cybersäkerhetsmätningar som mäter nivån på verksamheters systematiska cybersäkerhetsarbete, samt ger stöd för förbättringsarbete. Cybersäkerhetskollen genomförs minst vartannat år.

---

[1] Kommissionens genomförandeförordning C(2024)7151 av den 17.10.2024 om fastställande av regler för tillämpningen av direktiv (EU) 2022/2555 vad gäller tekniska och metodologiska specifikationer för riskhanteringsåtgärder för cybersäkerhet och närmare angivelse av i vilka fall en incident ska anses vara betydande med avseende på leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av utlokaliserade driftstjänster, leverantörer av utlokaliserade säkerhetstjänster, leverantörer av marknadsplatser online, leverantörer av sökmotorer, leverantörer av plattformar för sociala nätverkstjänster och tillhandahållare av betrodda tjänster.

[2] https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/arbeta-systematiskt-med-informationssakerhet-och-cybersakerhet/cybersakerhetskollen/

Vilka som ska omfattas av regleringen är styrt av förordningen, där man kan göra vissa nationella tillägg. Dessa tillägg utgörs av kap 4 i föreskriften. I dialogen med tillsynsmyndigheterna där vissa potentiella ytterligare tillägg har identiferats, översyn av kap 4 kommer att ske löpande utifrån bättre överblick av de aktörer som bedriver de samhällsviktiga verksamheter som omfattas. Därutöver bör en mer grundlig utvärdering av konsekvenserna för både privata och offentliga verksamhetsutövare ske i anslutning den utvärdering av cybersäkerhetslagen som regeringen aviserat ska ske tre år efter den nya lagens ikraftträdande.[3] Utvärderingen bör ske i nära samverkan med utpekade tillsynsmyndigheter för att säkerställa att underlag inhämtas från så många av NIS2-sektorerna som möjligt. Det övergripande syftet med en sådan utvärdering blir att få en bild av hur det nya regelverket påverkat verksamhetsutövarens cybersäkerhetsarbete och cybersäkerhet inklusive ekonomiska konsekvenser. Utvärderingen bör även inkludera ändamålsenligheten av tillhandahållet stöd i form av vägledningar, systemstöd med mera.

Om de grundläggande förutsättningarna för regleringen ändras, exempelvis med hänsyn till nivån på verksamhetsutövarnas cybersäkerhet, teknisk utveckling, hotbild, säkerhetspolitiska förutsättningar, legala grunder med mera kommer reglerna att omprövas och en ny konsekvensutredning göras.

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

Sverige är skyldig att implementera NIS2-direktivet i svensk rätt. Detta görs nu genom den kommande cybersäkerhetslagen (2025:XXX) och cybersäkerhetsförordningen (2025:XXX).

Anmälningsskyldighet

Ett alternativ till att reglera anmälningsskyldigheten i föreskrifter är att ge ut vägledning rörande hur anmälningsskyldigheten uppfylls. Det vill säga vilken information som behöver samlas in för att upprätta den förteckning som Sverige, liksom övriga medlemsstater, är ålagda att hålla över verksamhetsutövare. Avsaknad på legala krav rörande vilken information som ska lämnas vid anmälan bedöms dock öka risken för att verksamhetsutövare lämnar olika och mer eller mindre komplett information. Detta bedöms i sin tur medföra en risk för att Sverige inte kan uppfylla alla NIS2-direktivets krav på förteckningen över verksamhetsutövarna. Avsaknad av föreskriftskrav gör även att eventuella brister i anmälan inte kan åtgärdas genom en tillsyn.

Alternativet att enbart ge vägledning för hur hur anmälningsskyldigheten uppfylls anses inte vara tillräckligt. Däremot är det av stor vikt att det finns vägledning rörande hur föreskrifterna ska tillämpas.

[3] Prop. 2025/26:28 s 226.

I propositionen uttrycks att det inte framstår som ändamålsenligt att i lag reglera vilka uppgifter en anmälan ska innehålla och cybersäkerhetsförordningen innehåller inte heller några sådana regler. Det är därmed påföreskriftsnivå som de detaljerade kraven i artikel 3 p 3 och 4 i NIS2-direktivet bör omhändertas.[4] Vid utformningen av föreskrifterna har även kraven i kommissionens genomförandeförordning C(2024)7151 och övrig inriktning från kommissionen beaktas.[5]

Kravet i föreskrifterna om att i anmälan ange inom vilken sektor och viktig samhällsfunktion aktören bedriver verksamhet bidrar till att säkerställa att uppgifterna i en inkommen anmälan kan vidarebefordras till rätt tillsynsmyndighet. Detta gäller särskilt i sektorn hälsa, sjukvård och omsorg inom vilken det föreslås finnas två tillsynsmyndigheter. Kravet på att ange viktig samhällsfunktion bidrar även till att möta de nationella behoven av att samordna arbetet med cybersäkerhet enligt NIS2-direktivet med det nationella krishanteringsarbetet och arbetet med civilt försvar samt samordning med CER-direktivet[6]. Inhämtad information bedöms komma att ge ett betydelsefullt bidrag till sektorsansvariga myndigheters kunskap om vilka aktörer som utövar verksamhet inom respektive beredskapssektor, och i förlängningen underlätta möjligheterna att etablera samarbeten mellan verksamhetsutövarna inom sektorerna.

Den tydliga inriktningen från EU och behoven vid den nationella samordningen gör att alternativa sätt att reglera anmälningsskyldigheten bedöms vara mindre lämpliga.

Undantag för partnerföretag eller anknutna företag

Av skäl 16 i NIS 2-direktivet framgår att medlemsstater kan meddela undantag från tillämpningsområdet för vissa partnerföretag och anknutna företag om det skulle vara oproportionerligt att partnerföretag eller anknutna företag som inte i sig uppfyller storlekskravet, men gör det genom sin anknytning till en annan verksamhet, omfattas av regleringen.

Av 1 kap 15 § cybersäkerhetslagen framgår att regeringen eller den myndighet som regeringen bestämmer får, om det finns särskilda skäl, i enskilda fall besluta om undantag från skyldigheterna enligt cybersäkerhetslagen för partnerföretag och anknutna företag som omfattas med stöd av 1 kap 4 § cybersäkerhetslagen. Av 1 kap 14 § cybersäkerhetslagen framgår att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om sådana undantag.

---

[4] Prop. 2025/26:28 s 82

[5] MEDDELANDE FRÅN KOMMISSIONEN Kommissionens riktlinjer för tillämpningen av artikel 3.4 i direktiv (EU) 2022/2555 (NIS 2-direktivet), C(2023) 6070 final

[6] EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG.

Ett alternativ till att reglera undantagen i föreskrifter är att ge en beskrivning av möjligheterna för partnerföretag och anknutna företag att beviljas undantag från cybersäkerhetslagen i en vägledning. Avsaknad av rättsligt fastslagna kriterier för när undantag kan beviljas bedöms dock ge verksamhetsutövarna mindre förutsebarhet i när undantag kan och bör beviljas. Det bedöms därför vara mest ändamålsenligt att reglera detta i föreskrifter. Regeringen har även givit MSB i uppdrag att förbereda sådana föreskrifter.[7]

Föreskrifternas utformning av kriterierna för sådana undantag motsvarar skäl 16 i NIS2-direktivet. Även om skälen i sig inte är bindande bedöms det motverka en harmoniserad implementering av direktivet i EU att inte beakta skälen. Brist på harmonisering kan bidra till ökade administrativa kostnader för exempelvis företagskoncerner med partnerföretag i flera olika medlemsstater. Alternativa sätt att reglera möjligheterna till undantag bedöms av den anledningen vara mindre lämpliga.

Huvudsakligt etableringsställe

Vad som ska beaktas vid bedömningen av huvudsakligt etableringsställe framgår av artikel 26.2 i NIS2-direktivet. Av 1 kap 14 § cybersäkerhetslagen får regeringen eller den myndighet som regeringen bestämmer meddela föreskrifter om vad som utgör huvudsakligt etableringsställe enligt 1 kap 7 § cybersäkerhetslagen. Regeringen har givit MSB i uppdrag att förbereda sådana föreskrifter.[8]

Enligt 1 kap 7 § cybersäkerhetslagen är en verksamhetsutövares huvudsakliga etableringställe av grundläggande betydelse för bedömningen för de i paragrafen uppräknade verksamhetsutövare inom digital infrastruktur och förvaltning av IKT-tjänster.

Alternativet att enbart ge vägledning för hur ett huvudsakligt etableringsställe bör bedömas anses inte vara tillräckligt. Berörda verksamhetsutövare bedriver inte sällan verksamhet av gränsöverskridande karaktär. Avsaknad av rättsligt fastslagna kriterier öppnar upp för att verksamhetsutövarna, av olika skäl, väljer att bedöma sitt huvudsakliga etableringsställe på ett sätt som inte går i linje med NIS2-direktivets krav. Det gör också att tillsynsmyndigheterna får svårare att agera. Bristande harmonisering mellan medlemsstaterna vid implementering av artikel 26.2 i NIS2-direktivet vad gäller bedömningen av huvudsakligt etableringsställe kan därför göra det svårare för dessa verksamhetsutövare att bedöma vilken medlemsstats reglering som ska följas. Det bedöms därför som ändamålsenligt att reglera detta i föreskrifter.

Artikel 26.2 i NIS2-direktivet har inriktat utformningen av föreskrifterna och alternativa sätt att reglera vad som ska utgöra huvudsakligt etableringsställe bedöms av den anledningen vara mindre lämpliga. För att förenkla förståelsen har begreppet cybersäkerhetsoperationer ersatts med

[7] Regeringsuppdrag Fö2025/01293
[8] Regeringsuppdrag Fö2025/01293

cybersäkerhetsverksamhet i betydelsen aktiviteter som skyddar information, nätverk och informationssystem från skadliga cyberhot. Det involverar användning av verktyg, arbetssätt och tekniker för att upptäcka, förebygga och svara på cyberincidenter.

Ytterligare verksamhetsutövare

I 1 kap 4 § p 3 cybersäkerhetslagen framgår att lagen gäller verksamhetsutövare som storleksmässigt motsvarar eller är större än ett medelstort företag. Definitionen bygger således på antalet anställda och ekonomisk omsättning. Enligt 1 kap 5 § i cybersäkerhetslagen kan verksamhetsutövare som inte uppfyller storlekskravet 1 kap 4 § cybersäkerhetslagen ändå omfattas om:

1. verksamhetsutövaren är den enda leverantören av en tjänst i Sverige som är väsentlig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet,

2. en störning av den tjänst som verksamhetsutövaren tillhandahåller kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet eller folkhälsa eller kan medföra betydande systemrisker,

3. verksamhetsutövaren har särskild betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst, eller för andra sektorer som är beroende av verksamhetsutövaren.

Detta för att säkerställa att även en mindre aktör som kan bedriva en verksamhet, där en störning kan få en stor påverkan på den inre marknaden, fångas upp. Om dessa aktörer inte omfattas kan det innebära att den inre marknadens funktion inte kan upprätthållas och det blir svårare att uppfylla cybersäkerhetslagens syfte att uppnå en hög nivå av cybersäkerhet i samhället.

MSB har, i samverkan med föreslagna tillsynsmyndigheter, gjort en bedömning av vilka typer av verksamhetsutövare som, mot bakgrund och nationella förutsättningar, borde omfattas av regleringen trots att de inte uppfyller storlekskravet. Alternativet att inte identifiera dessa verksamhetsutövare skulle innebära att nyckelaktörer inte berörs av regleringen och därmed inte åläggs att vidta lämpliga och proportionella säkerhetsåtgärder samt att störningar i deras nätverks- och informationssystem som skulle kunna innebära samhällsstörningar inte på samma sätt fångas upp i den nationella lägesbilden.

I föreskrifterna ingår att peka ut om verksamhetsutövaren är väsentlig eller viktig. Utgångspunkten för bedömningen i föreskrifterna är att det inte är storleken utan den typ av verksamhet som aktören bedriver som ska vara styrande för om den betraktas som väsentlig eller viktig i NIS2-direktivets mening. Av detta följer att de verksamhetsutövare som läggs till genom föreskrifterna och bedriver en sådan verksamhet som omnämns i bilaga 1 i NIS2-direktivet klassificeras som väsentliga och övriga som viktiga.

Alternativa sätt att reglera när cybersäkerhetslagens tillämpningsområde ska utökas till verksamhetsutövare som inte uppfyller storlekskravet samt om de är väsentliga eller viktiga bedöms som mindre lämpliga.

Transporter (väsentliga verksamhetsutövare)

Med hänvisning till 1 kap 5 § p 2 och 3 cybersäkerhetslagen ska alla ledningsenheter för karantänshamnar respektive nödhamnar omfattas av regleringen. Vilka hamnar som utgör karantänshamnar pekas ut av Folkhälsomyndigheten enligt vägledning ”Kapacitet vid karantänshamnar och karantänsflygplatser – vägledning utifrån det internationella hälsoreglementet” och vilka som utgör skyddade platser framgår av Transportstyrelsens beslut om utpekande av skyddade platser i Sverige, bilaga 1 eller 2 (TSS 2019-3262).

Med hänvisning till 1 kap 5 § p 1 och 3 cybersäkerhetslagen ska alla beredskapsflygplatsers ledningsenheter omfattas av regleringen. Vilka flygplatser som utgör beredskapsflygplatser regleras i avtal med Trafikverket.

Med hänvisning till 1 kap 5 § p 3 cybersäkerhetslagen ska alla flygtrafikledningar omfattas av regleringen.

När det gäller karantänshamnar, nödhamnar respektive beredskapsflygplatser har dessa identifierats som särskilt viktiga för krisberedskap och civilt försvar. För flygtrafikledning utgör de oavsett aktörens storlek en nyckelroll lokalt och en del för att få en heltäckande karta.

Dricksvatten (väsentliga verksamhetsutövare)

Med hänvisning till 1 kap 5 § p 2 och 3 cybersäkerhetslagen ska verksamhetsutövare omfattas av regleringen om de levererar dricksvatten till minst 20 000 personer eller är ett akutsjukhus. Med akutsjukhus avses vårdinrättning som är inrättad för slutenvård och som har särskild akutmottagning för den som behöver omedelbar hälso- och sjukvård.

Dricksvattensförsörjningstjänster utgör geografiska monopol med stor betydelse för samhällets funktionalitet, även om de bedrivs av mindre aktörer. Motsvarande bedömning gjordes även i NIS1-regleringen.

Tillverkning, produktion och distribution av kemikalier (viktiga verksamhetsutövare)

Med hänvisning till 1 kap 5 § p 3 cybersäkerhetslagen ska verksamhetsutövare omfattas av regleringen om de tillverkar tillsatser eller insatsvaror överstigande 1 ton/år som är av avgörande betydelse för storskalig kemikalieproduktion inom dricksvattenrening, avloppsrening, industriell tillverkning eller förädling av livsmedel, framställning av gödselmedel eller kväveproduktion, växtskyddsmedel, brandsläckningsmedel, rengöringsmedel för hälso- och sjukvård, eller rengöringsmedel för industriell produktion. Motsvarande förteckning finns i MSBFS 2024:9, föreskrifter om vilka samhällsviktiga verksamheter som omfattas av lagen (2023:560) om granskning av utländska direktinvesteringar.

Till detta kommer kravet att verksamhetsutövaren är registrerad hos European Chemicals Agency (ECHA) enligt REACH förordningen[9]. Detta krav ställs i enlighet med kommissionens inriktning att medlemsstaterna bör identifiera verksamhetsutövare som är registrerade på detta sätt.

Uppgifter om vilka som berörs av regleringen

NIS2-direktivets tillämpningsområde följer av artikel 2. I punkterna 1–5 definieras området för att följas av undantag under punkterna 6–12.

Av artikel 2.1 följer att direktivet är tillämpligt på offentliga eller privata entiteter av den typ som följer av bilaga 1 eller 2.

I bilaga 1 pekas de högkritiska sektorerna ut, totalt 11 till antalet. Dessa är energi, transporter, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvårdssektorn, dricksvatten, avloppsvatten, digital infrastruktur, förvaltning av IKT-tjänster mellan företag, offentlig förvaltning och rymden. Dessa högkritiska sektorer motsvarar i hög grad de som i dag omfattas av lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

I bilaga 2 finns övriga sektorer som omfattas av NIS2-direktivet. Dessa benämns som kritiska sektorer och är 7 till antalet. Det handlar om post- och budtjänster, avfallshantering, tillverkning, produktion och distribution av kemikalier, produktion, bearbetning och distribution av livsmedel, digitala leverantörer och forskning. Bland de kritiska sektorerna ingår också tillverkning. I sektorn tillverkning ingår delsektorerna tillverkning av medicintekniska produkter, datorer, elektronikvaror och optik, elapparater, övriga maskiner, motorfordon, släpfordon och påhängsvagnar och andra transportmedel. I jämförelse med det tidigare NIS-direktivet och NIS-lagen är det i sin helhet nya områden.

Storlekskravet finns i artikel 2.1. Det anges att en verksamhet är av tillräcklig storlek om den minst kan betecknas som ett medelstort företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG.13 Ett vidare krav är att verksamheten tillhandahåller sina tjänster eller bedriver sin verksamhet i unionen. Artikel 2 i bilagan till kommissionens rekommendation definierar mikroföretag samt små och medelstora företag (SMF-kategorin). Av artikeln följer att ett medelstort företag är ett företag som sysselsätter minst 50 personer eller vars omsättning eller balansomslutning överstiger 10 miljoner euro per år.

Vissa sektorer och typer av verksamhetsutövare omfattas av NIS2-direktivet oavsett storlek. Det gäller exempelvis verksamhetsutövare som erbjuder allmänna elektroniska kommunikationsnät, allmänt tillgängliga elektroniska

[9] Europaparlamentets och rådets förordning (EG) nr 1907/2006 av den 18 december 2006 om registrering, utvärdering, godkännande och begränsning av kemikalier.

kommunikationstjänster, betrodda tjänster, registreringsenhet för toppdomäner, DNS-tjänster eller domännamnsregistrering.

Detsamma gäller

1. verksamhet som är väsentlig för att upprätthålla kritiska funktioner i samhället och ekonomiska funktioner,

2. om en störning i verksamheten kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet, folkhälsa eller medföra betydande systemrisker särskilt om det får gränsöverskridande konsekvenser, eller

3. verksamhet som är kritisk på grund av sin särskilda betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst, eller för andra sektorer som är beroende av denna verksamhet.

MSB gör uppskattningen att cirka 600 privata och offentliga aktörer omfattas idag av NIS-direktivets regler. När det gäller NIS2-direktivet med sitt bredare tillämpningsområde uppskattar regeringen att cirka 1500 företag i Sverige med sammanlagt runt 500 000 sysselsatta skulle kunna beröras av den nya lagen och tillhörande föreskrifter. Till detta kommer regioner och kommuner som är sammanlagt 310 stycken om Gotland, som både räknas som kommun och region, endast tas upp en gång. För att en statlig myndighet ska omfattas av regleringen krävs enligt huvudregeln i 1 kap 3 § 1 st p 1 cybersäkerhetslagen att den har befogenhet att fatta beslut som påverkar fysiska eller juridiska personers rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital. Även om det finns viss ledning i propositionen[10] hur detta krav bör tolkas är det inte i alla delar tydligt. Dessutom har regeringen med stöd av 1 kap 3 § st 2 cybersäkerhetslagen möjlighet att bestämma vilka myndigheter som ska läggas till även om de inte har befogenhet att fatta sådana beslut som avses i 1 kap 3 § st 1. Detta sammantaget försvårar uppgiften att på förhand uppskatta hur många statliga myndigheter som kommer att omfattas av cybersäkerhetslagen. Enligt en mycket grov uppskattning, främst utifrån regeringens resonemang i propositionen kring behovet av att inkludera beredskapsmyndigheterna i cybersäkerhetslagen, skulle det kunna vara närmare 100 stycken. Det kan dock vara betydligt fler.

Detta skulle innebära att NIS2-direktivet kommer att beröra runt 1900 privata och offentliga aktörer inom olika områden i Sverige, dvs en utökning med cirka 1300 aktörer jämfört med nuvarande reglering.

En mer exakt siffra kan ges när cybersäkerhetslagen träder ikraft och verksamhetsutövarna anmäler sig till utpekad myndighet.

[10] Prop 25/26:28 s 57ff.

Uppgifter om de bemyndiganden som myndighetens beslutanderätt grundar sig på

Cybersäkerhetslagen planeras att beslutas den 10 december 2025 och träda ikraft den 15 januari 2026. Cybersäkerhetsförordningen bedöms beslutas och träda ikraft i nära anslutning till dessa tidpunkter. Av detta följer att MSB vid tidpunkten för extern remiss i september 2025 ännu inte har något förordningsförordnande att utfärda föreskrifter om anmälningsskyldighet, undantag för partnerföretag och anknutna företag, huvudsakligt etableringsställe samt ytterligare verksamhetsutövare. Myndigheten har i avvaktan på ett sådant förordnande fått i uppdrag av regeringen att förbereda sådana föreskrifter inom ramen för implementeringen av NIS2-direktivet.[11] Regeringsuppdraget ger en bild av hur regeringen avser att fördela föreskriftsmandatet i cybersäkerhetsförordningen. Syftet är att skapa förutsättningar för att nödvändiga myndighetsföreskrifter träder ikraft i så nära anslutning till cybersäkerhetslagens och cybersäkerhetsförordningens ikraftträdande som möjligt. Extern remiss av dessa föreskrifter sker som ett led i arbetet med att utföra nämnda regeringsuppdrag.

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

De kostnadsmässiga och andra konsekvenser som följer av denna reglering bör bedömas utifrån ett helhetsperspektiv tillsammans med MSB:s övriga föreskrifter som utfärdas i enlighet med mandatet i cybersäkerhetsförordningen.

Utredningen om genomförande av NIS2- och CER-direktivens gjorde följande bedömning av kostnaderna i SOU 2024:18[12]. ”För de offentliga verksamhetsutövarna föreslår utredningen att kostnaderna ska finansieras inom befintlig ram. Skälen är att det är rimligt att offentliga verksamhetsutövare vidtar grundläggande säkerhetsåtgärder. Genom förslagen erhåller verksamhetsutövarna också stöd. Vidare kan åtgärder för att förebygga incidenter medföra besparingar.

Förslagen medför även kostnader för enskilda verksamhetsutövare, men även dessa får stöd genom förslagen och det förebyggande arbetet kan medföra besparingar. Som framgått omfattas som huvudregel inte små företag. Kraven kommer att gälla inom hela unionen. Utredningen bedömer därför att regleringen inte får effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt.”

Föreskrifterna om anmälan och identifiering ställer krav på vilken information som ska lämnas vid anmälan, specificerar partnerföretags och anknutna företags möjligheter till undantag från regleringen, hur huvudsakligt

[11] Regeringsuppdrag Fö2025/01293
[12] SOU 2024:18 s 22

etableringsställe ska bedömas samt vilka verksamhetsutövare som trots att de inte uppfyller storlekskravet ändå ska omfattas av cybersäkerhetslagen.

Utvidgningen av cybersäkerhetslagens tillämpningsområde i 4 kap skulle kunna medföra vissa utökade kostnader för verksamhetsutövare som på grund sin betydelse ska omfattas trots att de inte uppfyller storlekskravet. Dessa kostnader följer inte direkt av dessa föreskrifter, däremot blir de en konsekvens av att omfattas av cybersäkerhetslagen övriga krav. Detta gäller exempelvis kostnader för incidentrapportering och vidtagande av vissa säkerhetsåtgärder. För närmare bedömning av dessa kostnader se kommande konsekvensutredning för MSB:s föreskrifter om säkerhetsåtgärder och utbildning respektive MSB:s föreskrifter om incidentrapportering och informationsskyldighet.

Övriga krav bedöms endast ha marginella kostnadsmässiga eller andra konsekvenser givet att nödvändiga vägledningar och systemstöd finns att tillgå.

Alternativa sätt att reglera anmälningsskyldighet, undantag och huvudsakligt etableringsställe har inte bedömts som lämpliga inom ramen för arbetet med att implementera NIS2-direktivet.

Alternativet att inte utvidga tillämpningsområdet till ytterligare verksamhetsutövare i enlighet med kapitel 4 i föreskrifterna innebär att några nyckelaktörer inte berörs av regleringen och därmed inte åläggs att vidta lämpliga och proportionella säkerhetsåtgärder samt att störningar i deras nätverks- och informationssystem som skulle kunna innebära samhällsstörningar inte på samma sätt fångas upp i den nationella lägesbilden.

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

Regleringen utgör en del av implementering av NIS2-direktivet och bedöms överensstämma med de skyldigheter som följer av Sveriges anslutning till 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 planeras att träda ikraft den 15 januari 2026. Eftersom föreskrifterna har som syfte att stödja verksamhetsutövarna genom att konkretisera kraven i lag och förordning och därmed göra det enklare att efterleva dessa behöver föreskrifterna träda ikraft i så nära anslutning som möjligt till detta datum. Med hänsyn till remissförfarande och beredning bedöms föreskrifterna om anmälan och identifiering tidigast kunna träda ikraft den 2 februari 2026.

De som kommer att omfattas av regleringen består av både verksamhetsutövare som tidigare omfattats av NIS-direktivets regler och verksamhetsutövare som inte har någon tidigare erfarenhet av den typen av reglering.

MSB bedömer att det finns behov av att, i samverkan med berörda tillsynsmyndigheter, genomföra särskilda informationsinsatser inför och i samband med att regleringen börjar gälla. Detta för att säkerställa att verksamhetsutövarna ges möjlighet att både få en god bild av sina skyldigheter och rättigheter enligt den nya regleringen. Det är också angeläget att det finns tillgång till relevant stöd i form av vägledningar och tekniska system i samband med att föreskrifterna börjar gälla samt att verksamhetsutövarna ges kunskap om dessa.

Vid utformningen av informationsinsatserna behöver hänsyn tas till om mottagarna sedan tidigare omfattas av lagen om informationssäkerhet i samhällsviktiga tjänster eller inte. Det kommer även att behövas extra information om vad verksamhetsutövarna förväntas göra under perioden mellan att lagen respektive föreskrifterna träder ikraft eftersom det är först i föreskrifterna som det tydliggörs hur anmälan ska göras och vilken information som ska lämnas.

Företag

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

Regeringen har uppskattat att cirka 1500 företag i Sverige med sammanlagt runt 500 000 sysselsatta skulle kunna beröras av den nya lagen och tillhörande föreskrifter. Dessa återfinns inom samtliga sektorer som omfattas av NIS2-direktivet (se ovan) med undantag från offentlig förvaltning.

Med några undantag rör det genomgående företag som klassas som minst medelstora enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG.

Det är endast möjligt att ge en grov uppskattning av hur många verksamhetsutövare som tillkommer med stöd av föreskrifterna om anmälan och identifiering. Sannolikt handlar det inte om fler än 50 och majoriteten inom dricksvattenförsörjning där de som omfattas av befintlig reglering[13] inkluderas..

[13] Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster

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

Givet att nödvändiga vägledningar och systemstöd finns att tillgå bedöms föreskrifterna om anmälan och identifiering i sig endast innebära marginell tidsåtgång och marginellt ökade administrativa kostnader för företagen. I genomsnitt beräknas tiden för att göra en bedömning av om företaget omfattas av cybersäkerhetslagen eller inte uppgå till 2 – 4 timmar vid användning av vägledningar och systemstöd. I detta inräknas även den tid för intern informationsinhämtning om storlek och verksamhet. I de fall företaget behöver göra mer grundlig undersökning, exempelvis rörande möjligheten att tillämpa undantag för anknutna företag eller bedömning av huvudsakligt etableringsställe, krävs mer tid men bedöms ändå endast i undantagsfall överstiga till en eller två dagar. Själva anmälningsförfarandet, dvs att fylla i formuläret, i genomsnitt ta 10 – 15 minuter.

Ett företag behöver endast anmäla sig en gång men är ålagda enligt 2 kap 2 § st 2 cybersäkerhetslagen att vid förändrade förhållanden anmäla detta inom 14 dagar. Att anmäla förändrade förhållanden bedöms inte heller ta mer än 10 – 15 minuter i anspråk. Av de uppgifter som företaget är ålagda att lämna i anmälan torde uppgifter om ip-adresser kunna vara det som oftast förändras och därmed behöva uppdateras. För att underlätta kommer MSB att göra det möjligt att lämna dessa uppgifter genom anslutning till en tjänst hos CSIRT-enheten hos MSB. Genom att uppge ip-adresser i denna tjänst uppfyller inte bara företaget kraven i cybersäkerhetslagen utan erhåller samtidigt automatiska notifieringar av tekniska sårbarheter som kan påverka företagets gränssnitt mot internet.

Även regeringen gör en liknande bedömning och konstaterar följande. ”När det gäller skyldigheten att göra en anmälan bör det, bland annat med hänvisning till vilken arbetstid som kan komma i fråga för att genomföra denna åtgärd, generellt sett endast bli fråga om mindre kostnader för enskilda verksamhetsutövare. Denna engångskostnad kan till exempel begränsas genom att det införs en möjlighet att göra en anmälan via ett centraliserat system. Det analysarbete som krävs för att bedöma om aktören omfattas av lagen, och om en anmälan därmed ska göras, kommer att underlättas genom stöd och tydlig vägledning från berörda myndigheter.”[14]

Bedömningen är att föreskrifterna även kan bidra till minskade kostnader genom att tillhandahålla tydliga rättsliga ramar och därmed bidra till förutsebarhet vid implementeringen av NIS2-direktivet i Sverige. Förslaget bedöms inte påverka intäkterna.

Beskrivning av vilka andra kostnader den föreslagna regleringen medför för företagen och vilka förändringar i verksamheten som

[14] Prop 2025/26:28 s 223.

företagen kan behöva vidta till följd av den föreslagna regleringen

Föreskrifternas regler om anmälningsskyldighet, undantag, huvudsakligt etableringsställe bedöms inte medföra några särskilda kostnader för företagen eller behov av förändringar i verksamheten.

Föreskrifternas regler om ytterligare verksamhetsutövare syftar till att utvidga tillämpningsområdet och får till följd för berörda verksamhetsutövare att dessa verksamhetsutövarna behöver vidta säkerhetsåtgärder och skapa rutiner för incidentanmälan etc för att uppfylla kraven i regleringen. En initial bedömning är att detta endast kommer att beröra ett begränsat antal.

EU-kommissionen uppskattar att utgifterna för de företag som omfattas av NIS2-regelverket kommer att öka med högst 22 procent under de första åren efter införandet av de nya reglerna (se Förslag till Europaparlamentets och rådets direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148, COM(2020) 823 final). För företag som redan omfattas av NIS-direktivet uppskattas kostnaderna öka med 12 procent. Samtidigt understryker kommissionen att det också kan bli fråga om besparingar för berörda företag med hänvisning till att kostnaderna för att hantera cybersäkerhetsincidenter kommer att minska. EU-kommissionen uppskattar att sådana besparingar kommer att motsvara ca 118 miljarder euro under en tioårsperiod.

För en mer detaljerad genomgång av kostnader för de verksamhetsutövare som omfattas hänvisas till kommande konsekvensutredningar för MSB:s NIS2-föreskrifter om säkerhetsåtgärder och utbildning respektive incidentrapportering och informationsskyldighet.

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

Med hänsyn till att NIS2-direktivet kommer att gälla samma typer av företag i hela unionen och förslagen i stor utsträckning är nödvändiga för att genomföra NIS 2-direktivet i nationell rätt bedömer MSB att regleringen i stort inte kommer att påverka konkurrensförhållanden. NIS2-direktivet är ett minimidirektiv men införs i Sverige utan nationell utvidgning vilket gör att den regelbörda som svenska företag får genom cybersäkerhetslagen inte överstiger andra medlemsstaters implementering av direktivet. Det är, som regeringen påpekar i propositionen, ofrånkomligt att direktivet i viss utsträckning kommer att genomföras på olika sätt i olika medlemsstater utifrån de tolkningar och överväganden om behov som görs i de nationella lagstiftningsärendena.[15]

När det gäller föreskrifterna om anmälning och identifiering så är det mest relevant att beröra påverkan på konkurrensförhållandena för företag när det gäller att utvidga regelverkets tillämpningsområde med ytterligare väsentliga

[15] Prop. 25/26:28 s 38

och viktiga verksamhetsutövare i tre sektorer. Detta gäller cirka 50 organisationer som genom föreskrifterna omfattas trots att de inte uppfyller NIS2-direktivets storlekskrav, varav en majoritet redan idag omfattas av NIS-direktivets krav.

Detta aktualiseras i tre sektorer där det identifierats att det finns aktörer som mot bakgrund av att de är

1. den enda leverantören av en tjänst i Sverige som är väsentlig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet,

2. en störning av den tjänst som verksamhetsutövaren tillhandahåller kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet eller folkhälsa eller kan medföra betydande systemrisker, eller

3. verksamhetsutövaren har särskild betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst eller för andra sektorer som är beroende av verksamhetsutövaren,

Myndigheten har gjort uppskattningen att det till antalet sannolikt inte handlar om fler än 50 och majoriteten inom dricksvattenförsörjning. Inom dricksvattenförsörjning inkluderas de som redan omfattas av befintlig reglering. När det gäller både tillagda verksamhetsutövare inom transport och dricksvattenförsörjning agerar dessa på en nationell marknad med lokala monopol, vilket gör att det faktum att de nu omfattas av samma reglering som övriga, något större aktörer, som tillhandahåller samma tjänster snarast bidrar till att säkerställa att konkurrens kan ske på liknande villkor. Påverkan på konkurrensförhållandena bedöms i dessa fall minska genom föreskrifterna.När det gäller verksamhetsutövare inom kemikalier hör de till gruppen viktiga verksamhetsutövare vilket innebär att de omfattas av en mindre betungande tillsyn. De hör dock till en grupp som kan ha en större internationell verksamhet både utanför och innanför EU/EES särskilt då en förutsättning för att omfattas är att verksamhetsutövaren är registrerad hos European Chemicals Agency (ECHA) enligt REACH förordningen[16]. Detta krav är ställt i enlighet med EU-kommissionens rekommendationer för sektorn Tillverkning, produktion och distribution av kemikalier. Bedömningen görs därför att även om marknadsstrukturer mm kan skilja sig så är det sannolikt att de utpekade verksamhetsutövarnas närmaste konkurrenter inom EU/EES också är registrerade hos ECHA och därmed också har att förhålla sig till NIS2 reglering. Vad gäller i förhållande till konkurrenter i tredje land kan det faktum att verksamhetsutövarna genom föreskrifterna nu omfattas av tydligare krav på cybersäkerhet eventuellt komma att påverka konkurrensförhållanden. I detta sammanhang kan noteras att det även på global nivå, efter en rad incidenter med stor påverkan på samhällsfunktioner, sker ett alltmer intensifierat arbete

[16] Europaparlamentets och rådets förordning (EG) nr 1907/2006 av den 18 december 2006 om registrering, utvärdering, godkännande och begränsning av kemikalier.

med att stärka cybersäkerhet hos företag och i leveranskedjor. De nya regelkraven kan därför, såsom regeringen påpekar i propositionen, få en positiv påverkan. ”Högre krav kan förvisso vara resurskrävande och påverka hur mycket resurser en aktör lägger ned på cybersäkerhet jämfört med en konkurrerande verksamhet. Det kan samtidigt stärka en aktörs ställning på marknaden att ha en mer motståndskraftig verksamhet som i mindre utsträckning än andra liknande verksamheter påverkas av incidenter.” [17]

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

MSB bedömer generellt att implementeringen av NIS2-direktivet kommer att bidra till att stärka företagens cybersäkerhet och bidra till att de uppfyller de behov som finns i samhället av att samhällets funktionalitet är cybersäker.

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

Föreskrifterna gäller som huvudregel inte små företag och någon generell hänsyn har därför inte bedömts behövas tas till dessa vid reglernas utformning. De små företag som ändå omfattas gör det på grund av deras vikt för samhällets funktionalitet. Extra stödinsatser kan bli aktuella i det fall det behövs.

Kommuner och regioner

Föreskrifterna bedöms inte innebära några förändringar av kommunala befogenheter eller skyldigheter utöver att en anmälningsskyldighet införs. Föreskrifterna bedöms inte påverka grunderna för kommuners eller regioners organisation eller verksamhetsformer.

Kontaktpersoner

Ange vem som kan kontaktas vid eventuella frågor

Jan-Olof Olsson eller Helena Andersson

[17] Prop 2025/26:28 s 225.