Remissversion: Konsekvensutredning rörande Myndigheten för samhällsskydd och beredskaps föreskrifter om incidentrapportering och informationsskydlighet

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 att 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 att vissa leverantörer av samhällsviktiga och digitala tjänster skulle vidta säkerhetsåtgärder för att hantera risker och förebygga incidenter i de nätverk och informationssystem som används för att tillhandahålla tjänsterna. Leverantörerna skulle även rapportera incidenter som hade en betydande eller avsevärd inverkan på tjänsternas kontinuitet.

Direktivet omfattade leverantörer av samhällsviktiga tjänster inom sju särskilt definierade sektorer: energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt digital infrastruktur. Direktivet gällde dessutom för leverantörer av digitala tjänster.

Det konstateras i skäl 2 till NIS2-direktivet att det tidigare NIS-direktivet har lett till betydande framsteg när det gäller att stärka EU:s cyberresiliens.

Direktivet har bidragit till att nationell kapacitet har byggts upp och till att samarbetet på unionsnivå har utvecklats.

Samtidigt framgår det att en översyn av NIS-direktivet har avslöjat inneboende brister. Dessa brister har hindrat direktivet från att effektivt hantera både befintliga och framväxande utmaningar inom cybersäkerhetsområdet.

I skäl 4 och 5 konstateras att medlemsstaterna fick stort utrymme för nationella val vid implementeringen av NIS-direktivet. Det innebr att krav på säkerhetsåtgärder, incidentrapportering samt genomförande av tillsyn och efterlevnadskontroll kunde skilja sig avsevärt mellan olika medlemsstater.

Skillnaderna har bidragit till en fragmentering av den inre marknaden och bedöms kunna ha en negativ inverkan på dess funktion. Enligt skälen kan dessa skillnader dessutom göra vissa medlemsstater mer sårbara för cyberhot, med potentiella spridningseffekter i hela unionen.

NIS2-direktivet skiljer sig från NIS-direktivet på flera sätt. Regleringen omfattar betydligt fler aktörer och ställer skärpta och tydligare krav på riskanalyser samt vilka säkerhetsåtgärder aktörerna ska vidta. Även kraven på hur incidentrapportering ska genomföras skärps och förtydligas.

Till skillnad från NIS-direktivet gäller den nya regleringen hela verksamheten hos aktören, inte enbart säkerheten 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 i förslaget till cybersäkerhetslag pekat ut en rad områden där lagkraven ytterligare behöver konkretiseras i form av myndighetsföreskrifter.

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

Föreskrifter och allmänna råd om incidentrapportering och informationsskyldighet

Förslaget till föreskrifter och allmänna råd om incidentrapportering och informationsskyldighet syftar till att förtydliga

- vad som utgör en betydande incident enligt 2 kap. 5 § andra stycket cybersäkerhetslagen,
- vilka uppgifter som verksamhetsutövare ska inkomma med vid rapportering av en betydande incident enligt 2 kap. 5-8 §§ cybersäkerhetslagen, och

- hur verksamhetsutövaren ska uppfylla informationsskyldigheten gentemot mottagare av dess tjänster avseende betydande incidenter eller betydande cyberhot i enlighet med 2 kap. 9-10 §§ cybersäkerhetslagen.

Även nuvarande föreskrifter som utfärdats med stöd av den reglering som implementerar det första NIS-direktivet i Sverige innehåller regler om vilka incidenter som anses rapporteringspliktiga för de aktörer som omfattas NIS-direktivets tillämpningsområde samt vilka uppgifter som en rapport ska inkludera.[1] Detsamma gäller de föreskrifter om incidentrapportering som gäller för statliga myndigheter som utfärdats med stöd av beredskapsförordningen.[2]

Jämfört med nu gällande reglering innehåller föreskrifterna om incidentrapportering och informationsskyldighet utökade krav på vad som utgör en betydande incident och därmed omfattas av rapporteringsskyldighet samt vilken information som ska lämnas. Detta för svara upp mot kraven i NIS2-direktivet samt kommissionens genomförandeförordning C(2024)7151.[3] Kraven rörande informationsskyldighet, det vill säga att verksamhetsutövaren åläggs att informera mottagare av påverkade tjänster eller tjänster som kan komma att påverkas negativt av en inträffad betydande incident eller ett betydande cyberhot, har inte något motsvarighet i NIS-regleringen eller kraven som ställs utifrån beredskapsförordningen.

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.

Har de grundläggande förutsättningarna för regleringen ändrats kommer reglerna att omprövas och en ny konsekvensutredning göras.

---

[1] Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster och förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.
[2] Förordning (2022:524) om statliga myndigheters beredskap
[3] 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.

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

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

Vad som utgör en betydande incident

Ett alternativ till att reglera vad som ska utgöra en betydande incident och därmed omfattas av rapporteringsplikt[4] i föreskrifter är att inte ge ut några föreskrifter alternativt endast ge ut vägledning rörande detta.

Av artikel 23 p. 6 i NIS2-direktivet framgår det att Sverige, och övriga medlemsstater ska när så är lämpligt, och särskilt om den betydande incidenten berör två eller flera medlemsstater, och utan onödigt dröjsmål informera andra berörda medlemsstater och ENISA om den betydande incidenten. Av samma artikel p. 9 åläggs medlemsstaterna även att var tredje månad lämna in en sammanfattande rapport till ENISA med anonymiserade och aggregerade uppgifter om betydande incidenter, incidenter, cyberhot och tillbud som rapporterats in. Avsaknad av föreskrifter som konkretiserar vilka incidenter som bedöms vara betydande och därför omfattas av rapporteringsplikt bedöms öka risken för att verksamhetsutövare tolkar kravet på olika sätt vilket i förlängningen försvårar för Sverige att bidra med avsett underlag till ENISA.

Medlemsstater ska därutöver ha vidtagit alla nödvändiga åtgärder för att se till att NIS2-direktivets regler om sanktioner kan tillämpas. Tillsynsmyndigheten ska utöva tillsyn över att cybersäkerhetslagen och föreskrifter som har meddelats i anslutning till lagen följs. I Cybersäkerhetslagen finns bestämmelser om att tillsynsmyndigheten ska ingripa om verksamhetsutövaren åsidosatt sina skyldigheter enligt regleringen. Ett ingripande sker enligt 4 kap. 1 § cybersäkerhetslagen genom beslut om föreläggande, ansökan om förbud att inneha ledningsfunktion, beslut om sanktionsavgift eller, om det inte finns skäl att ingripa mot en överträdelse på något annat sätt, genom anmärkning. En effektiv och rättssäker tillsyn förutsätter att både verksamhetsutövare och tillsynsmyndigheter på ett så enkelt sätt som möjligt ska kunna skilja mellan konkreta krav och vägledning. Avsaknad av föreskrifter som förtydligar kraven lagen bedöms försvåra möjligheterna för både verksamhetsutövare och tillsynsmyndighet att bedöma om verksamhetsutövaren uppfyller lagkraven. Detta får negativ påverkan på rättssäkerheten och försvårar för tillsynsmyndigheterna att bedriva effektiv tillsyn och vid behov ingripa vid en överträdelse. Avvikelser från att följa en vägledning kan inte heller åtgärdas genom tillsyn.

Alternativet att inte utfärda några föreskrifter alls eller enbart ge vägledning för vilka incidenter som ska anses vara betydande och därmed omfattas av

[4] Det vill säga vilka typer av incidenter som motsvarar det som definieras i 2 kap. 5 § andra stycket cybersäkerhetslagen.

rapporteringsskyldighet anses därför inte vara tillräckligt utan medför en risk för att Sverige inte kommer uppfylla NIS2-direktivets krav. Däremot är det av stor vikt att det finns vägledning rörande hur föreskrifterna ska tillämpas.

Av artikel 3 – 14 i Kommissionens genomförandeförordning C(2024)71515 framgår generella och sektorsspecifika krav för vad som ska anses vara betydande incidenter för verksamhetsutövare inom sektorerna digitala leverantörer och digital infrastruktur. Ett alternativ till att ta fram krav för när en incident ska anses betydande för verksamhetsutövare inom resterande sektorer är att använda samma generella kriterier och trösklar som används i genomförandeförordningens artikel 3. Genomförandeförordningen har utgjort en grund vid framtagande av krav i dessa föreskrifter för att säkerställa viss harmonisering mellan alla sektorer som omfattas av NIS2-direktivet. Samtidigt har genomförandeförordningen tagits fram med vissa sektorer i fokus. Det bedöms därför vara nödvändigt att anpassa föreskrifternas krav efter samtliga sektorers behov såväl som rådande svenska förhållanden.

Uppgifter som verksamhetsövaren ska lämna vid incidentrapportering

Ett alternativ till att reglera vilken information som ska lämnas vid incidentrapportering är att ge ut vägledning om det i kombination med tekniskt stöd i form av en rapporteringsportal med formulär som ska fyllas i.

I artikel 23 p. 4 i NIS2-direktivet ställs förhållandevis detaljerade krav på medlemsstaterna vad gäller vilka uppgifter som ska begäras in från verksamhetsutövarna vid respektive rapporteringstillfälle. Till detta kommer att Kommissionen enligt samma artikel p. 11 får anta genomförandeförordningar som närmare anger typen av uppgifter i och formatet och förfarandet för incidentrapportering. Rapportering av betydande incidenter regleras i 2 kap. 5 – 8 §§ cybersäkerhetslagen. I lagen framgår dock endast att verksamhetsutövaren ska lämna olika typer av rapporter vid specificerade tidpunkter och inte vilken information som ska lämnas.

För att Sverige ska kunna säkerställa att verksamhetsutövarna lämnar rätt information vid rätt tillfälle, och på så sätt uppfyller kraven i NIS2-direktivet, bedöms det som otillräckligt att endast tillhandahålla vägledning och en rapporteringsportal. Även om det, särskilt genom rapporteringsportalen, går att underlätta för verksamhetsutövarna att lämna rätt typ av uppgifter, ger en

[5] 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.

sådan lösning inga möjligheter att genom tillsyn åtgärda att verksamhetsutövare att lämnar inkomplett eller missvisande information.

Alternativet att enbart ge vägledning och tillhandahålla en rapporteringsportal som stöd för verksamhetsutövarna när de lämnar uppgifter om inträffade betydande incidenter anses därför inte vara tillräckligt. Däremot bedöms det vara av stor vikt att det finns vägledning och en sådan portal som stöd.

Informationsskyldighet

Ett alternativ till att reglera i föreskrifter vilken information som ska lämnas av verksamhetsutövare till mottagarna av deras tjänster vid betydande incidenter och betydande cyberhot är att inte vidta några åtgärder eller endast ge ut vägledning.

Det framgår av 2 kap. 9 och 10 §§ cybersäkerhetslagen att verksamhetsutövare förväntas informera mottagare av deras tjänster om betydande incidenter och betydande cyberhot. Av författningskommentaren i propositonen framgår att det är flera bedömningar som behöver göras. Det gäller inte bara när sådan informationsskyldighet infinner sig utan även vilka, om inte alla, mottagare av tjänsten som ska informeras och vilken information som ska delas. Skyldigheten att informera omfattas av tillsyn och till detta kommer att tillsynsmyndigheten i enlighet med 4 kap. 4 § cybersäkerhetslagen dessutom får förelägga en verksamhetsutövare att fullgöra informationsskyldigheten.

Att mottagare av en verksamhetsutövares tjänster exempelvis informeras om konsekvenserna för tjänsten och åtgärder som mottagaren kan vidta för att hantera konsekvenser, kan bidra till att begränsa negativ påverkan av en betydande incident. Det är dock, som framgår av propositionen, många bedömningar som verksamhetsutövaren behöver göra rörande hur informationsskyldigheten ska uppfyllas. Stöd för dessa bedömningar kan ges i vägledning men en sådan lösning ger inga möjligheter att genom tillsyn säkerställa att verksamhetsutövare inom samma sektor som drabbas av liknande incidenter väljer att uppfylla informationsskyldigheten på samma sätt. För att så långt möjligt och där så är lämpligt säkerställa att informationsskyldigheten uppfylls på ett så likvärdigt sätt som möjligt bedöms därför det vara mest ändamålsenligt att komplettera lagens krav på informationsskyldighet med föreskrifter om hur informationsskyldigheten ska uppfyllas. Detta minskar risken för att mottagare av samma typ av tjänst ges olika mycket information beroende viken verksamhetsutövare som tillhandahåller tjänsten. Det minskar även risken för att verksamhetsutövare väljer att inte lämna information av konkurrensskäl.

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

Uppgifter om vilka som berörs av regleringen

Genom cybersäkerhetslagen och tillhörande reglering implementeras NIS2-direktivet i Sverige. NIS2-direktivets tillämpningsområde följer av artikel 2. 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 elva högkritiska sektorer ut. 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. Vidare finns det en sektor som heter tillverkning. Där 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.

I artikel 2.1 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 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 idag omfattas 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 och allmänna råd. 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 § första stycket 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 hur detta krav bör tolkas är det inte i alla delar tydligt. Regeringen har med stöd av 1 kap. 3 § andra stycket cybersäkerhetslagen möjlighet att bestämma vilka myndigheter som ska omfattas av lagen även om myndigheterna fattar sådana beslut som avses i 1 kap. 3 § första stycket. Sammantaget gör detta det svårt att i förväg uppskatta hur många statliga myndigheter som kommer att omfattas av cybersäkerhetslagen. Baserat på regeringens resonemang i propositionen kring behovet av att inkludera beredskapsmyndigheterna i cybersäkerhetslagen skulle en preliminär uppskattning kunna vara närmare 100 myndigheter. Det faktiska antalet kan dock vara betydligt högre.

Detta skulle innebära att NIS2-direktivet kommer att beröra runt 1900 privata och offentliga aktörer inom olika områden i Sverige, 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.

Uppgifter om de bemyndiganden som myndighetens beslutanderätt grundar sig på

Cybersäkerhetslagen beslutas sannolikt i början av december 2025 och planeras att 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 oktober 2025 ännu inte har något förordnande att utfärda föreskrifter om incidentrapportering och informationsskyldighet. Myndigheten har i avvaktan på ett sådant förordnande fått i uppdrag av regeringen att förbereda sådana föreskrifter inom ramen för

implementeringen av NIS2-direktivet.[6] Samtidigt erhöll Post- och telestyrelsen ett motsvarande regeringsuppdrag om förberedelser för föreskrifter.[7]

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.

Uppdraget till MSB omfattar att förbereda för att utfärda föreskrifter för verksamhetsutövare i samtliga NIS 2-sektorer med undantag för digital infrastruktur, digitala leverantörer, förvaltning av IKT-tjänster (mellan företag), post- och budtjänster och rymden när det gäller föreskrifter om säkerhetsåtgärder, vad som utgör en betydande incident och informationsskyldighet. Detta fick PTS i uppdrag att förbereda.

De delar av MSB:s föreskrifter om incidentrapportering och informationsskyldighet som avser hur incidentrapportering ska ske gäller samtliga verksamhetsutövare. Kapitel 3-4 i föreskrifterna, som konkretiserar vilka incidenter som ska anses vara betydande samt kapitel 5, som redogör för verksamhetsutövares skydlighet att informera mottagare av tjänster vid betydande incidenter och betydande cyberhot, gäller för samtliga sektorer förutom för de som omfattas av föreskrifter och allmänna råd som ska utfärdas av Post- och telestyrelsen (PTS). Kommissionen har också antagit en genomförandeförordning som närmare specificerar krav avseende säkerhetsåtgärder och vad som avses med betydande incident för sådana verksamhetsutövare som tillhandahåller olika digitala tjänster och infrastrukur.[8]

[6] Uppdrag till Myndigheten för samhällsskydd och beredskap att förbereda genomförandet av NIS 2-direktivet (Fö2025/01293)
[7] Uppdrag till Post- och telestyrelsen att förbereda genomförandet av NIS 2-direktivet (Fi2025/01676)
[8] (EU) 2024/2690 av den 17 oktober 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.

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

Regeringen konstaterar följande i propositionen.[9] ”Det är många faktorer som påverkar kostnaderna för exempelvis incidenthantering, som ingår i lagens krav på säkerhetsåtgärder, såsom störningens art och omfattning, dess konsekvenser för kontinuiteten samt hur snabbt verksamhetsutövaren återhämtar sig från incidenten. En betydande incident kan orsaka både direkta utrednings- och reparationskostnader och indirekta kostnader på grund av exempelvis avbrott i verksamheten eller ett skadat anseende.” 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 cybersäkerhetsförordningen mandat. Tillsammans med kommande föreskrifter om säkerhetsåtgärder och utbildning MCFFS (2026:00) kommer verksamhetsutövare på längre sikt att minska sin risk för att drabbas av incidenter och därmed kunna erbjuda mer stabila leveranser samt höja sin konkurrenskraft.

För de verksamhetsutövare som inte bedriver ett systematiskt och riskbaserat arbete idag kan krav i föreskrifterna om incidentrapportering och informationsskyldighet initialt ge begränsat ökade kostnader. Många verksamhtsutövare bedöms redan idag arbeta med cybersäkerhet och har interna regler och arbetssätt för att upptäcka och hantera incidenter i sina nätverk och informationssystem. Därtill är det idag en självklarhet att en verksamhetsutövare har kostnader för att skydda sina nätverk och informationssystem. I denna kostnad ingår utgifter för system och annat tekniskt stöd för att bedriva verksamheten samt personalkostnader för att upprätthålla en säker informationsbehandling.

Kravet på extern incidentrapportering till den nationella CSIRT-enheten kan för flertalet verksamhetsutövare 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 interna regler och arbetssätt kan behöva ske. MSB arbetar med att ta fram en portal för incidentrapportering med dynamiskt utformade rapporteringsformulär. Denna kommer att underlätta arbetet med incidentrapportering genom att säkerställa att verksamhetsutövaren endast behöver ange sådan information och besvara sådana frågor som är relevant för den aktuella incidenten.

Runt 600 av de verksamhetutövare som kommer att omfattas av den nya regleringen rapporterar redan idag incidenter till den nationella CSIRT-enheten i enlighet med MSB:s föreskrifter om rapportering av incidenter för leverantörer av samhällsviktiga tjänster (MSBFS 2018:9) respektive MSB:s föreskrifter om rapportering av incidenter för leverantörer av digitala tjänster

[9] Prop. 2025/26:28 s 224

(MSBFS 2018:10).[10] Här bedöms den nya regleringen om incidentrapportering därför inte ge upphov till några ökade kostnader. I jämförelse med dessa krav, enligt vilken den första notifieringen till CSIRT-enheten ska lämnas senast sex timmar efter att organisationen har identifierat en rapporteringspliktig incident, utgör den nya regleringen med första krav på rapportering senast 24 timmar efter upptäckt snarare en minskad kravbörda.

Statliga myndigheter har sedan 2016 krav på sig att rapportera it-incidenter.[11] Kraven i föreliggande förslag till föreskrifter skiljer sig något från gällande föreskrifter. Enligt existerande krav ska en första notifering lämnas senast sex timmar efter att myndigheten identifierat incidenten som rapporteringspliktig istället för senast inom 24 timmar i enlighet med den nya regleringen. Den nya regleringen innebära dessutom att rapporteringskrav på statliga myndigheter minskar då det är endast är incidenter som resulterat i eller kan komma att resultera i allvarliga konsekvenser som behöver rapporteras. Detta till skillnad från existerande krav som gör det gällande att påverkan på information eller informationssystem i behov av utökat skydd omfattas av rapporteringsplikt oavsett efterföljande konsekvenser. Enligt existerande krav ska myndigheterna dessutom ha ett upparbetat arbetssätt för att kunna rapportera it-incidenter, vilket kan användas även för att uppfylla kommande krav på rapportering av betydande incidenter. Sammantaget är bedömningen därför att de nya kraven på rapportering snarare minskar än ökar kravbördan.

För de verksamhetsutövare som utkontrakterar sin informationshantering kan det uppstå vissa initiala kostnader i samband med att interna regler och arbetssätt kan behöva anpassas och eventuellt nya avtal skrivas.

Föreskriftskravet att en upplysning ska lämnas inom 24 timmar efter att leverantören har identifierat en incident som rapporteringspliktig och uppföljande rapportering inom 72 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. Detta för att rapporteringen inte ska inverka negativt på arbetet med att avhjälpa incidenten. Vidare är den mängd information som ska lämnas inom 24 timmar och även anvisade kontaktvägar anpassade efter skyndsamhetskravet.

När det gäller informationsplikten handlar eventuellt tillkommande kostnader främst om att etablera nya interna regler och arbetssätt för att kunna tillgodose dessa krav. Föreskrifterna ska i denna del inte tolkas innebära krav på att etablera nya informationskanaler.

[10] Föreskrifterna utgör en del av den svenska implementeringen av NIS-direktivet.
[11] MSBFS 2016:2, senare ersatts med MSBFS 2020:8.

Förslaget bedöms inte generera intäkter för staten, kommuner, regioner, företag och andra enskilda men kan däremot minska kostnader orsakade av incidenter. 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 incidentrapportering och informationsskyldighet tidigast kunna träda ikraft i mitten eller slutet av mars 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.

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 avloppsvattenshantering och dricksvattenförsörjning.

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 samt att interna regler och arbetssätt etablerats i enlighet med MSB:s föreskrifter om säkerhetsåtgärder och utbildning uppskattas tidsåtgången för efterlevnaden av föreskrifterna om incidentrapportering och informationsskyldighet inte överstiga sammanlagt en halv dag per rapporterad betydande incident. Detta bedöms endast innebära begränsade administrativa kostnader för företagen.

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

Föreskrifterna om incidentrapportering och informationsskyldighet bedöms i sig inte medföra några andra särskilda kostnader utöver de som krävs för att etablera adekvata interna regler och arbetssätt för incidentrapportering i enlighet med MSB:s föreskrifter om säkerhetsåtgärder och utbildning.

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 bedömer MSB att regleringen inte kommer att påverka konkurrensförhållanden.

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 definiera cybersäkerhetslagens krav på rapportering av betydande incidenter och informationsskyldighet vid betydande incidenter och cyberhot. Föreskrifterna bedöms inte påverka grunderna för kommuners eller regioners organisation eller verksamhetsformer.

Kontaktpersoner

Ange vem som kan kontaktas vid eventuella frågor

Josefin Andersson