Myndigheten för civilt försvar

Konsekvensutredning

Datum	Ärendenummer
2026-05-13	MCF 2026-13324

Konsekvensutredning för Myndigheten för civilt försvars föreskrifter om incidentrapportering och informationsskyldighet för väsentliga och viktiga verksamhetsutövare

1. Allmänt

1.1 Beskrivning av problemet och vad som ska uppnås

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) skulle ha implementerats av medlemsstaterna den 18 oktober 2024.

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

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 till enheten för hantering av it-säkerhetsincidenter (CSIRT-enheten), det vill säga Myndigheten för samhällsskydd och beredskap – sedan den 1 januari 2026 – Myndigheten för civilt försvar.

NIS-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 även 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 skäl (5) konstateras att medlemsstaterna fick stort utrymme för nationella val vid implementeringen av NIS-direktivet. Det innebär 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 risk för potentiella spridningseffekter i hela unionen.

NIS2-direktivet skiljer sig därför 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. Kraven på hur incidentrapportering ska genomföras har skärpts och förtydligats.

Av skäl (101) i NIS2-direktivet beskrivs syftet med incidentrapporteringen på följande sätt: *I direktivet fastställs en flerstegsstrategi för rapportering av betydande incidenter för att hitta rätt balans mellan, å ena sidan, snabb rapportering som bidrar till att begränsa den potentiella spridningen av betydande incidenter och gör det möjligt för väsentliga och viktiga entiteter att söka bistånd och, å andra sidan, ingående rapportering som drar värdefulla lärdomar av enskilda incidenter och med tiden förbättrar cyberresiliensen hos enskilda entiteter och hela sektorer. I detta avseende bör detta direktiv omfatta rapportering av incidenter som, baserat på en första bedömning som utförts av den berörda entiteten, kan orsaka allvarliga störningar i tjänsterna eller ekonomiska förluster för den berörda entiteten eller påverka andra fysiska eller juridiska personer genom att orsaka betydande materiell eller immateriell skada. En sådan inledande bedömning bör bland annat ta hänsyn till de drabbade nätverks- och informationssystemen, särskilt deras betydelse för tillhandahållandet av entitetens tjänster, allvaret i och de tekniska egenskaperna hos cyberhotet och eventuella underliggande sårbarheter som utnyttjas, samt entitetens erfarenhet av liknande incidenter. Indikatorer såsom i vilken utsträckning tjänstens funktion påverkas, hur länge incidenten pågår eller hur många*

tjänstemottagare som drabbas kan spela en viktig roll när man fastställer om tjänstens driftsstörning är allvarlig.

I skäl (102) i NIS2-direktivet beskrivs incidentrapporteringens upplägg på följande sätt: *Om väsentliga eller viktiga entiteter får kännedom om en betydande incident bör de vara skyldiga att lämna in en tidig varning utan onödigt dröjsmål och under alla omständigheter inom 24 timmar. Denna tidiga varning bör åtföljas av en incidentanmälan. De berörda entiteterna bör lämna in en incidentanmälan utan onödigt dröjsmål och under alla omständigheter inom 72 timmar efter att ha fått kännedom om den betydande incidenten, särskilt i syfte att uppdatera den information som lämnats via den tidiga varningen och göra en inledande bedömning av den betydande incidenten, inbegripet dess allvarlighetsgrad och konsekvenser samt, i förekommande fall, angreppsindikatorer. En slutrapport bör lämnas in senast en månad efter incidentunderrättelsen. Den tidiga varningen bör endast innehålla den information som är nödvändig för att göra CSIRT-enheten, eller i förekommande fall den behöriga myndigheten, medveten om den betydande incidenten och ge den berörda entiteten möjlighet att vid behov söka bistånd. Den tidiga varningen bör i tillämpliga fall ange om den betydande incidenten misstänks vara orsakad av olagliga eller avsiktligt skadliga handlingar och om det är troligt att den kommer att få gränsöverskridande verkningar. Medlemsstaterna bör säkerställa att skyldigheten att lämna in den tidiga varningen, eller den efterföljande incidentunderrättelsen, inte avleder den underrättande entitetens resurser från verksamheter i samband med incidenthantering som bör prioriteras, i syfte att förhindra att skyldigheterna att rapportera incidenter antingen avleder resurser från hantering av betydande incidenter eller på annat sätt undergräver entitetens ansträngningar i detta avseende. I händelse av en pågående incident vid den tidpunkt då slutrapporten lämnas in bör medlemsstaterna säkerställa att berörda entiteter tillhandahåller en lägesrapport vid den tidpunkten och en slutrapport inom en månad efter det att de hanterat den betydande incidenten.*

1.1.1 Cybersäkerhetslagen

NIS2-direktivet införs i svensk rätt genom cybersäkerhetslagen (2025:1506). Av 2 kap. 5–8 §§ cybersäkerhetslagen framgår att de som omfattas av lagens krav, verksamhetsutövare, ska rapportera betydande incidenter i tre skeden efter 24 timmar, efter 72 timmar och efter en månad samt under vissa omständigheter även tillhandahålla en delrapport respektive lägesrapport. I 2 kap. 5 § 2 st. förtydligas när en incident ska vara betydande och därmed rapporteringspliktig:

En incident ska anses vara betydande om den har orsakat eller kan orsaka allvarlig driftsstörning för den erbjudna tjänsten eller ekonomisk skada för den berörda verksamhetsutövaren, eller om den har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande skada.

Av 2 kap. 9 och 10 §§ cybersäkerhetslagen framgår att verksamhetsutövaren under vissa förhållanden har en skyldighet att informera mottagarna av deras tjänster om en betydande incident respektive betydande cyberhot. I 2 kap.10 § 2 st. förtydligas

när ett cyberhot ska anses vara betydande och därmed omfattas av informationsplikt:

Ett cyberhot ska anses vara betydande om det, på grund av dess tekniska egenskaper, kan antas ha potential att ha en allvarlig påverkan på en verksamhetsutövares nätverks- och informationssystem eller användarna av verksamhetsutövarens tjänster genom att vålla betydande skada.

Det specificeras inte närmare i lagen hur incidentrapporterings- och informationsskyldigheten ska fullgöras. Det ges inte heller någon mer detaljerad inriktning och tröskelvärden rörande vad som utgör en betydande incident. Av 2 kap.14 § i lagen framgår att detta får meddelas i föreskrifter.

Av artikel 23 i NIS2-direktivet framgår att incidentrapportering ska ske till enheten för hantering av it-säkerhetsincidenter (CSIRT-enheten) eller behörig myndighet. I artikel 10 och 11 i NIS2-direktivet regleras kraven på CSIRT-enheter. I 31 och 33 §§ cybersäkerhetsförordningen (2025:1507) tydliggörs att Myndigheten för civilt försvar ska vara CSIRT-enhet i enlighet med artikel 10 i NIS 2-direktivet samt att det är CSIRT-enheten som ska ta emot incidentrapporter. I samband med att cybersäkerhetsverksamheten på Myndigheten för civilt försvar den 1 juli 2026 ska föras över till Försvarets radioanstalt kommer även cybersäkerhetsförordningen att uppdateras för att förtydliga att uppgiften som CSIRT-enhet förs över inklusive uppgiften att ta emot incidentrapporter.

1.1.2 Föreskrifter och allmänna råd om incidentrapportering och informationsskyldighet

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

- vilka uppgifter som verksamhetsutövare ska komma in med vid rapportering av en betydande incident enligt 2 kap. 5–8 §§ cybersäkerhetslagen,
- vad som utgör en betydande incident enligt 2 kap. 5 § 2 st. cybersäkerhetslagen för samtliga tillsynsområden förutom de som avses i 37 § cybersäkerhetsförordningen[1], 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.

[1] De tillsynsområden som Post- och telestyrelsen ansvarar för men med undantag för länsstyrelser, det vill säga Digital infrastruktur, Digitala leverantörer, Förvaltning av IKT-tjänster (mellan företag), Post- och budtjänster, Rymden och verksamhetsutövare som erbjuder domännamnsregistreringstjänster.

Samtliga uppgifter bedöms behövas för att säkerställa att syftet med lagen och NIS2-direktivet kan uppfyllas.

Även de föreskrifter som har utfärdats med stöd av den reglering som implementerat det första NIS-direktivet i Sverige innehöll regler om vilka incidenter som anses rapporteringspliktiga för de aktörer som omfattas NIS-direktivets tillämpningsområde samt vilka uppgifter som en rapport skulle inkludera. Både lag och förordning samt föreskrifter upphävdes i samband med cybersäkerhetslagens ikraftträdande.[2] Detsamma gäller de föreskrifter om incidentrapportering som gäller för statliga myndigheter som har utfärdats med stöd av förordningen (2022:524) om statliga myndigheters beredskap (beredskapsförordningen), det vill säga Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:8) om rapportering av it-incidenter för statliga myndigheter.

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 någon motsvarighet i NIS-regleringen eller kraven som ställs utifrån beredskapsförordningen.

[2] Lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster, MSBFS 2018:9 föreskrifter och allmänna råd om rapportering av incidenter för leverantörer av samhällsviktiga tjänster, MSBFS 2018:10 föreskrifter och allmänna råd om rapportering av incidenter för leverantörer av digitala tjänster och MSBFS 2018:11 föreskrifter och allmänna råd om frivillig rapportering av incidenter i tjänster som är viktiga för samhällets funktionalitet.

[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.

2. 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.

Myndigheten för civilt försvar har sedan 2016 enligt sin instruktion[4] i uppgift att årligen rapportera inrapporterade incidenter till regeringen. I årsrapporterna har både sådana incidenter som inrapporterats enligt beredskapsförordningen samt de som rapporteras enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, det vill säga den reglering som genomförde det första NIS-direktivet i Sverige, redovisats. Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster upphörde att gälla den 15 januari 2026 i samband med att cybersäkerhetslagen (2025:1506) trädde ikraft. Årsrapporten för 2026 kommer därför till skillnad från tidigare årsrapporter vara baserad på rapportering enligt beredskapsförordningen och cybersäkerhetslagen. Genom att föreskrifterna som konkretiserar vad och hur som ska rapporteras enligt cybersäkerhetslagen inte kommer att träda ikraft förrän 1 juli 2026 bedöms underlaget för årsrapporten 2026 inte bli helt fullständigt. Årsrapporten för 2027 bedöms dock kunna ge ett heltäckande underlag av inrapporterade incidenter. En första uppföljning av konsekvenserna av föreskrifterna om incidentrapportering avseende möjligheterna att förbättra lägesbilden kommer därför att kunna göras i anknytning till det arbetet och då utifrån en jämförelse mellan årsrapporterna för 2025 respektive 2027.

När det gäller konsekvenser för verksamhetsutövarna rörande krav på själva rapporteringsförfarandet kommer en uppföljning av föreskrifterna göras i samband med uppföljning och vidareutveckling av det systemstöd som nu utvecklas av myndigheten för att omhänderta föreskriftskraven. Identifierade svårigheter för verksamhetsutövarna i samband med incidentrapportering kommer sannolikt i första hand att kunna lösas genom ett vidareutvecklat systemstöd eller ytterligare vägledning men även behov av justeringar på föreskriftsnivå behöver övervägas.

En mer grundlig utvärdering av konsekvenserna för både privata och offentliga verksamhetsutövare sker i anslutning till den utvärdering av cybersäkerhetslagen som regeringen har aviserat ska ske tre år efter den nya lagens ikraftträdande.[5] 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 har påverkat verksamhetsutövarens cybersäkerhetsarbete och

[4] 11 a § st. 2 förordning (2008:1002) med instruktion för Myndigheten för civilt försvar, tidigare Myndigheten för samhällsskydd och beredskap.
[5] Prop. 2025/26:28 s 226.

cybersäkerhet inklusive kostnads- och verksamhetsmässiga konsekvenser. Utvärderingen bör även inkludera ändamålsenligheten av tillhandahållet stöd i form av vägledningar, systemstöd med mera.

Föreskrifter och föreskriftsmandat gällande cybersäkerhetslagen krav på verksamhetsutövares incidentrapportering och informationsskyldighet kommer att flyttas över till Försvarets radioanstalt den 1 juli 2026. Med anledning av detta kommer uppföljningen av konsekvenser ske hos den myndigheten.

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 ansvarig myndighet att ompröva reglerna att omprövas och göra en ny konsekvensutredning.

2.1 Beskrivning av alternativa lösningar för det som ska uppnås 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 (2025:1506) och cybersäkerhetsförordningen (2025:1507) samt genom tillhörande myndighetsföreskrifter. Nedan följer en genomgång av vilka överväganden myndigheten har gjort avseende vad som utgör en betydande incident, uppgifter som ska lämnas vid incidentrapportering och hantering av informationsskyldighet.

2.1.1 Vad som utgör en betydande incident

Ett alternativ till att reglera vad som ska utgöra en betydande incident och därmed omfattas av rapporteringsplikt[6] i föreskrifter är att inte ge ut några föreskrifter alls, alternativt att 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

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

risken för att verksamhetsutövare tolkar kravet på olika sätt vilket i förlängningen försvårar för Sverige att bidra med avsett underlag till ENISA.

Medlemsstaterna 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 har 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 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)71517 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 och 4.

- I artikel 3 p. 1 räknas sju olika kriterier (a – g) upp som var för sig innebär att en incident ska betraktas som betydande och därför vara

[7] 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.

rapporteringspliktig, (f) anger att incidenter som avses artikel 4 är betydande och (g) anger att incidenter som avses i artiklarna 5 – 14 är betydande.

- I artikel 3 p. 2 tydliggörs att planerade avbrott och planerade konsekvenser av planerat underhåll inte ska anses som betydande incidenter.
- I artikel 3 p. 3 ges inriktning hur verksamhetsutövare inom sektorerna digitala leverantörer och digital infrastruktur ska beräkna antalet användare som påverkas av en incident.
- I artikel 4 specificeras vad som krävs för att återkommande incidenter som i sig inte uppfyller kriterierna i artikel 3 ändå ska anses vara betydande.

Artiklarna 5–14 rör specifika krav på när driftstörningar i olika typer av digitala tjänster och digital infrastruktur såsom molntjänster, registreringsenheter för toppdomäner med flera ska anses utgöra en betydande incident.

Genomförandeförordningen skulle kunna användas som förlaga för föreskrifterna både vad gäller struktur och innehåll.

När det gäller *strukturen* rör punkterna i artikel 3 p. 1 inledningsvis ekonomisk skada, sedan skada för annan och därefter allvarlig driftstörning. Definitionen av vad som utgör en betydande incident enligt NIS2-direktivet och cybersäkerhetslagen har dock en delvis annan uppbyggnad, det vill säga en incident som uppfyller en av tre kriterier

- *om den har orsakat eller kan orsaka allvarlig driftsstörning för den erbjudna tjänsten eller*
- *ekonomisk skada för den berörda verksamhetsutövaren,*
- *eller om den har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande skada.*

Eftersom legaldefinitionens struktur så tydligt kan delas in i dessa tre kriterier bedöms det bli enklast för verksamhetsutövarna att även föreskrifterna följer samma struktur framför genomförandeförordningens upplägg att börja med ekonomisk skada och avsluta med allvarlig driftstörning.

När det gäller *innehållet* har genomförandeförordningen till väsentlig del utgjort grund för föreskrifternas krav.

Artikel 3 punkt 1 (a): *Incidenten har orsakat eller kan orsaka en ekonomisk förlust för den berörda entiteten som överstiger 500 000 EUR eller 5 % av den berörda entitetens totala årsomsättning under föregående räkenskapsår, beroende på vilket som är lägst*

Motsvarande krav finns delvis i 3 kap. 2 § i föreskrifterna. När det gäller den fasta summan som en tröskel för rapporteringsskyldighet har den inte lagts in i föreskrifterna. Anledningen är de stora skillnader som finns mellan sektorerna som inte regleras i genomförandeförordningen sammantaget med skillnaderna mellan verksamhetsutövarna inom respektive sektorer. Det bedöms som svårt att på förhand identifiera en summa som får ungefär samma konsekvenser hos berörda verksamhetsutövare. Med anledning av detta beskrivs nivån av förlust i föreskrifterna endast genom en procentsats. Procentsatsen är satt på samma nivå som i genomförandeförordningen. För att omhänderta förhållandena i offentlig sektor har dessutom förtydligats att för denna sektor gäller inte årsomsättning utan anslag eller totala intäkter under föregående räkenskapsår.

För att underlätta verksamhetsutövarens beräkning av den ekonomiska skadan specificeras även i 3 kap. 3 § föreskrifterna vilka typer av direkta och indirekta kostnader som minst ska beaktas vid beräkningen.

Artikel 3 p. 1 (b) *Incidenten har orsakat eller kan orsaka att företagshemligheter enligt artikel 2.1 i direktiv (EU) 2016/943 exfiltreras från den berörda entiteten*

Kriteriet rörande förlust av företagshemligheter är omhändertaget i 3 kap. 1 § p. 2 i föreskrifterna men eftersom företagshemligheter inte är ett vanligt förekommande begrepp i alla sektorer benämns det istället mer generiskt som information som bedöms ha behov av utökat skydd. På detta sätt tydliggörs att förlust av även annan skyddsvärd information, såsom personuppgifter eller sekretessbelagd information kan medföra rapporteringsskyldighet. Mot bakgrund av den incidentrapportering som görs redan idag kan det även konstateras att genomförandeförordningens skrivning om exfiltrering gör att flera huvudorsakerna till att skyddsvärd information förloras eller förvanskas inte omhändertas. För att kunna upprätthålla en rättvisande bild, inte bara gällande resultatet av angrepp, utan även av konsekvenser av mänskliga misstag, systemfel med mera är föreskrifterna neutralt utformade rörande orsaken och tydliggör att det inte bara gäller information som har blivit tillgänglig för obehöriga utan även sådan som av andra anledningar har förvanskats eller förstörts. NIS2-direktivets definitioner av incident, betydande incident, cyberhot och cybersäkerhet tydliggör sammantaget att kriterier för vilka incidenter som är rapporteringspliktiga behöver utgå från ett allriskperspektiv.

Allvarlighetsnivån konkretiseras genom hänvisningen till att det gäller information i behov av utökat skydd som behandlas i sektorskritiska system, det vill säga sådana system som är nödvändiga för att bedriva sådan verksamhet som uttryckligen pekas ut i cybersäkerhetslagen.

Artikel 3 p. 1 (c) *Incidenten har orsakat eller kan orsaka en fysisk persons dödsfall* respektive (d) *Incidenten har orsakat eller kan orsaka betydande skador på en fysisk persons hälsa*

Kravet är omhändertaget i föreskrifternas 3 kap. 4 § p. 3 b–c. Mot bakgrund av det tydliggörs i NIS2-direktivet artikel 23 p. 2 (b) att betydande skada både kan avse materiell och immateriell skada, något som exemplifieras i cybersäkerhetslagens förarbeten som sakskada eller ren förmögenhetsskada bedöms genomförandeförordningens kriterier avseende betydande skada för annan inte vara tillräckligt heltäckande. Föreskrifterna har därför kompletterats med kriterier för rapporteringsskyldighet när skada har uppstått för andra genom informationsförlust och föroreningsskada enligt 10 kap.1 § miljöbalken (1998:808).

Artikel 3 p. 1 (e) *En framgångsrik, misstänkt skadlig och obehörig åtkomst till nätverks- och informationssystem har inträffat och kan orsaka allvarliga driftsstörningar* respektive *(g) Incidenten uppfyller ett eller flera av de kriterier som anges i artiklarna 5–14.*

Genomförandeförordningens kriterium i artikel 3 p. 1 (e) är omhändertaget i föreskrifternas 3 kap. 5 § p. 1. Genomförandeförordningens kriterium i punkten (g) ger en hänvisning till detaljerade kriterier i artikel 5–14 för vilka konsekvenser som ska uppstå på tjänstenivå för att det ska anses som en betydande incident, exempelvis ska en molntjänst vara helt otillgänglig i 30 minuter enligt artikel 7 (a). Motsvarande hänvisning till allvarliga driftstörning för verksamhetsutövaren återfinns i 3 kap. 1 § p. 1 samt 4 kap. 1–9 §§.

Föreskrifternas kriterier för vad som ska anses som en allvarlig driftsstörning ska tillämpas av verksamhetsutövare i rad olika sektorer med olika förutsättningar och behov. Myndigheten för civilt försvar har därför i nära samverkan med utpekade tillsynsmyndigheter både tagit fram generella kriterier som – för att svara upp mot NIS2-direktivets allriskperspektiv och syfte att stärka samhällets funktionalitet genom cybersäkerhet – utformats genom att specificera vilka konsekvenser av en driftstörning som gör att en incident blir rapporteringspliktig. Precis som för de verksamheter som regleras i genomförandeförordningen har ett behov identifierats för vissa sektorer av ytterligare detaljeringsgrad och anpassning till sektorns specifika förhållanden. Detta görs i föreskrifternas kapitel 4 och gäller sektorerna offentlig förvaltning, energi, transporter, dricksvatten, avloppsvatten samt för vårdgivare i sektorn hälso- och sjukvård. Övriga sektorer bedöms ha tillräckligt stöd av de generiska kriterierna på allvarlig driftsstörning. För att säkerställa ett allriskperspektiv har kriterierna genomgående tagit sikte på de konsekvenser incidenten har medfört såsom att sektorsverksamhet endast har kunnat bedrivas i begränsad utsträckning under en viss tid, verksamhetsutövarens personal har blivit tvungna att använda alternativa arbetssätt för att bedriva sektorsverksamhet, skyddsvärd information har förlorats eller förvanskats eller tjänster har inte kunnat tillhandahållas vilket kunnat påverka viktiga samhällsfunktioner.

Artikel 4 *Återkommande incidenter*

Föreskrifterna använder motsvarande kriterier som i genomförandeförordningen i 3 kap. 6 §.

2.1.2 Uppgifter som verksamhetsutövaren ska lämna vid incidentrapportering

Ett alternativ till att reglera vilken information som ska lämnas vid incidentrapportering är att ge ut en 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 sådan lösning inga möjligheter att genom tillsyn åtgärda att verksamhetsutövare 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.

2.1.3 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 alls eller att endast ge ut en 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 propositionen[8] framgår att det

[8] Prop. 2024/25:28 s. 249f

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 en 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 någon information av konkurrensskäl.

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

Informationsskyldighet regleras inte i genomförandeförordningen varför ett sådant alternativ till föreskrifterna inte är aktuellt.

2.2 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 från bestämmelserna 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 elva 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 lagen (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 sju 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, i vilken 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 ytterligare 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.

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.

De verksamhetsutövare som omfattas av cybersäkerhetslagens regler ska anmäla sig till Myndigheten för civilt försvar. I mitten av april 2026 har 2080 företag, 83

statliga myndigheter, 19 regioner, 264 kommuner och 44 kommunalförbund anmält sig. De har angivit att de bedriver verksamhet i en eller flera sektorer fördelat enligt följande: Energi 629 stycken, Transporter 158 stycken, Bankverksamhet 88 stycken, Finansmarknadsinfrastruktur 6 stycken, Hälso- och sjukvård 453 stycken, Dricksvatten 206 stycken, Avloppsvatten 206 stycken, Digital infrastruktur 420 stycken, Förvaltning av IKT-tjänster (mellan företag) 250 stycken, Offentlig förvaltning 404 stycken, Rymden 2 stycken, Post- och budtjänster 18 stycken, Avfallshantering 173 stycken, Tillverkning, produktion och distribution av kemikalier 76 stycken, Produktion, bearbetning och distribution av livsmedel 199 stycken, Digitala leverantörer 14 stycken och Forskning 13 stycken. Antalet förändras givetvis över tid genom nyanmälan och avanmälan i de olika sektorerna.

2.3 Uppgifter om de bemyndiganden som myndighetens beslutanderätt grundar sig på

NIS2-direktivet implementeras genom cybersäkerhetslagen (2025:1506) och cybersäkerhetsförordningen (2025:1507). Av förordningen framgår att Myndigheten för civilt försvar får meddela föreskrifter rörande incidentrapportering enligt 2 kap. 5–8 §§ cybersäkerhetslagen, ytterligare föreskrifter om vad som utgör en betydande incident enligt 2 kap. 5 § samt föreskrifter om informationsskyldighet enligt 2 kap. 9 och 10 §§ samma lag.

Föreskriftsmandatet avseende vad som utgör en betydande incident i 3–4 kap. samt informationsskyldighet vid betydande incidenter och betydande cyberhot omfattar inte sektorsverksamhet inom Digital infrastruktur, Digitala leverantörer, Förvaltning av IKT-tjänster (mellan företag), Post- och budtjänster och Rymden. 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 infrastruktur.[9]

[9] (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.

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

Regeringen konstaterar följande i propositionen.[10] ”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 myndighetens 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 öka 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 verksamhetsutövare 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. Myndigheten för civilt försvar tar också fram en portal för incident-rapportering 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.

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

Runt 600 av de verksamhetsutövare som kommer att omfattas av den nya regleringen har fram till cybersäkerhetslagens ikraftträdande redan omfattats av krav på att rapportera incidenter till den nationella CSIRT-enheten i enlighet med lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster och 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 (MSBFS 2018:10).[11] 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.[12] Kraven i föreliggande förslag till föreskrifter skiljer sig något från gällande föreskrifter. Enligt existerande krav ska en första notifiering lämnas senast sex timmar efter det att myndigheten har identifierat incidenten som rapporteringspliktig istället för senast inom 24 timmar i enlighet med cybersäkerhetslagen. Rapporteringskravet enligt cybersäkerhetslagen omfattar endast incidenter som har resulterat i eller kan komma att resultera i allvarliga konsekvenser. Detta till skillnad från beredskapsförordningens krav som gör det gällande att påverkan på information eller informationssystem i behov av utökat skydd omfattas av rapporteringsplikt oavsett efterföljande konsekvenser. Enligt beredskapsförordningen 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.

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/överenskommelser upprättas.

Föreskriftskravet att en upplysning ska lämnas inom 24 timmar efter det 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 har 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

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

mängd information som ska lämnas inom 24 timmar och även anvisade kontaktvägar anpassade efter skyndsamhetskravet.

När det gäller informationsskyldigheten 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.

2.5 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. NIS2-direktivet är ett minimidirektiv. För ytterligare beskrivning av utrymmet för nationell anpassning se ovan redovisning av alternativa lösningar som har övervägts liksom nedan redovisning om konkurrenspåverkan.

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

Cybersäkerhetslagen och dess förordning trädde ikraft den 15 januari 2026. Eftersom föreskrifterna har som syfte att stödja verksamhetsutövarna genom att konkretisera kraven i lagen och förordningen och därmed göra det enklare att efterleva dessa, behöver föreskrifterna träda ikraft i så nära anslutning som möjligt till detta datum. Fram till dess har verksamhetsutövarna tillgång till begränsad ledning vad gäller vilka incidenter som är rapporteringspliktiga och vilken information som ska lämnas.

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

Myndigheten för civilt försvar 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 få en god bild av sina skyldigheter och rättigheter enligt den nya regleringen.

Vid utformningen av informationsinsatserna behöver hänsyn tas till om mottagarna sedan tidigare omfattas av lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster eller inte.

Det är även angeläget att det finns tillgång till relevant stöd i form av tekniska system för rapportering i så nära samband med att föreskrifterna börjar gälla som möjligt samt att verksamhetsutövarna ges kunskap om dessa. Det systemstöd som Myndigheten för civilt försvar idag tillhandahåller som stöd för nuvarande incidentrapportering kommer att upphöra i samband med att ansvaret för att ta emot incidentrapporter flyttas över från myndigheten till det nationella cybersäkerhetscentret hos Försvarets radioanstalt (FRA) den 1 juli 2026. Efter övergången bedöms systemstöd inte kunna tillhandahållas förrän tidigast i september 2026. I avvaktan på detta används en reservlösning för incidentrapporteringen.

Ambitionen är att så långt möjligt minska antalet tillfälliga lösningar för incidentrapportering som verksamhetsutövarna ska behöva använda. Vid en samlad bedömning av att så snart som möjligt kunna ge ledning till verksamhetsutövarna rörande incidentrapporteringen, att nuvarande systemlösning tas bort den 30 juni 2026 och att det ska finnas tillgång till reservlösningar från den 1 juli 2026 bedöms det som lämpligast att föreskrifterna träder ikraft den 1 juli 2026.

3. Företag

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

I mitten av april 2026 har 2080 företag anmält sig. De är verksamma i samtliga sektorer förutom offentlig förvaltning. Den stora majoriteten av företagen utgör medelstora eller större företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG, dvs sysselsätter minst 50 personer eller vars omsättning eller balansomslutning överstiger 10 miljoner euro per år. Åtminstone cirka 430 stycken uppfyller inte detta storlekskrav, men har ändå anmält sig. Företrädesvis på grund av att de uppfyller kraven i 1 kap. 5 § cybersäkerhetslagen, exempelvis är den enda leverantören av en tjänst i Sverige som är väsentlig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet.

3.2 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 har 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. Om företaget drabbas av fyra rapporteringspliktiga incidenter per år och rapporteringen utförs av en erfaren administratör bedöms tillkommande administrativa kostnader per år uppgå till 8000 kr.[13]

När det gäller intäktspåverkan bedöms, med hänsyn till syfte och begränsad tidsåtgång, inte regleringens krav på att rapportera incidenter påverka företagens produktion och försäljning, verksamhetens kapital, eller möjligheten att få tillgång till stöd och ersättningar. I det fall ett företag bryter mot reglerna i föreskrifterna kan dock en tillsynsmyndighet besluta om sanktionsavgifter enligt cybersäkerhetslagen. Sådana sanktionsavgifter kan påverka företagets ekonomi.

3.3 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 Myndigheten för civilt försvars föreskrifter om säkerhetsåtgärder och utbildning. Användningen av det systemstöd som kommer att tillhandahållas för verksamhetsutövarnas incidentrapportering förutsätter inte att företagen själva anskaffar särskild teknisk utrustning.

[13] En månadslön på 35600 kr uppskattas till, med semesterersättning, arbetsgivaravgifter och overheadkostnader, utgöra en kostnad för företagen på cirka 65500 kr och omvandlat, utifrån 160 timmar i månaden för en helhetstjänst, bli cirka 410 kr i timmen. Tillkommande administrativa kostnader för en incidentrapportering blir då avrundat 2000 kr.

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

För att genomföra NIS2-direktivet i svensk rätt krävs att de krav som ställs i cybersäkerhetslagen konkretiseras i föreskrifter avseende vilka incidenter som är rapporteringspliktiga, vilken information som verksamhetsutövarna ska lämna i respektive rapporteringsskede samt vad som krävs för att uppfylla sin informationsskyldighet. Föreskrifterna om incidentrapportering bedöms såsom ovan redogjorts för att ligga i linje med genomförandeförordningen. I de delar där kraven går utöver genomförandeförordningen handlar det om att svara upp mot NIS2-direktivets skrivningar om vad som är rapporteringspliktigt. Ur ett nationellt perspektiv bedöms det som centralt att anlägga en orsaksneutral hållning till vilka incidenter som är rapporteringspliktiga och fokusera på konsekvenserna. Detta synsätt ligger också i linje med NIS2-direktivets definitioner av incident och betydande incident.

Kommissionen har valt att inte besluta om genomförandeförordningar i andra sektorer än för digitala tjänster och digital infrastruktur. En anledning till det är att andra sektorer inte har en lika gränsöverskridande karaktär och att det bör finnas utrymme för anpassningar till nationella förhållanden. NIS2-direktivet är ett minimidirektiv och detta innebär att medlemsstaterna i viss utsträckning kan komma att ha något divergerande reglering för att kunna omhänderta nationella förhållanden. Syftet är att möjliggöra för trösklar i de sektorer som inte regleras i genomförandeförordningen som, även om de skiljer sig mellan olika medlemsstater, ändå säkerställer en snarlik konsekvensnivå på medlemsstatsnivå. Det handlar exempelvis om att omhänderta skillnader vad gäller konsekvens om 1000 användare påverkas i Luxemburg jämfört med 1000 i Tyskland. När det gäller trösklar för vilka incidenter som är rapporteringspliktiga ger NIS2-direktivet genom sin definition av en betydande incident samt genomförandeförordningens skrivningar tydlig ledning rörande syftet med incidentrapporteringen. Till detta kommer att ett uttalat syfte med att ersätta det tidigare NIS-direktivet med NIS2-direktivet var att ensa medlemsstaternas kravställning, inte minst när det gällde incidentrapporteringen. Detta underlättar medlemsstaternas arbete med att hitta snarlika nivåer för incidentrapportering om än uttryckta på olika sätt.

Mot denna bakgrund görs bedömningen att föreskrifternas konkretisering av NIS2-direktivets och cybersäkerhetslagens krav på incidentrapportering inte i sig bedöms påverka konkurrensförhållanden för företagen på nationell och EU-nivå. Påverkan på global nivå bedöms inte heller, med tanke på att tillkommande kostnader bedöms bli begränsade, vara påtaglig. Snarare kan den förbättrade lägesbild som rapporteringen kommer att ge på EU- och nationell nivå över inträffade betydande incidenter hos företag kunna ge förbättrade möjligheter till att ge både operativt och förebyggande stöd. Som nämnts ovan kan dessa

föreskrifter tillsammans med kommande föreskrifter om säkerhetsåtgärder och utbildning MCFFS (2026:00) på längre sikt även innebära att verksamhetsutövare minskar sin risk för att drabbas av incidenter och därmed kunna erbjuda mer stabila leveranser samt öka sin konkurrenskraft.

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

Myndigheten för civilt försvar bedömer att implementeringen av NIS2-direktivet generellt 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.

3.6 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. Till detta kommer att regleringen är styrd av krav i överordnad EU-rätt vilket begränsar möjligheterna till särskild hänsyn. De små företag som ändå omfattas gör det på grund av deras betydelse för samhällets funktionalitet. Extra stödinsatser kan bli aktuella i det fall det behövs.

4. 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 heller påverka grunderna för kommuners eller regioners organisation eller verksamhetsformer.

5. Kontaktpersoner

Josefin Andersson eller Helena Andersson