Myndigheten för civilt försvar

Konsekvensutredning

Datum	Ärendenummer
2026-04-22	MCF 2026-06325

Konsekvensutredning för Myndigheten för civilt försvars föreskrifter om säkerhetsrevision och säkerhetsskanning

Allmänt

Enligt 3 § förordningen (2024:183) om konsekvensutredningar ska en förvaltningsmyndighet inför att den ska besluta om föreskrifter eller allmänna råd ta fram och dokumentera en konsekvensutredning. Nedan följer en genomgång av de frågor som ska behandlas enligt förordningen.

Det aktuella problemet och vilken förändring som eftersträvas

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 och börjat tillämpas av medlemsstaterna den 18 oktober 2024. Sverige, liksom ett antal andra medlemsstater är försenade med sin implementering. EU-kommissionen har betonat betydelsen av att medlemsstaterna implementerar NIS2-direktivet så snart som möjligt.

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).

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. NIS-direktivet gällde dessutom för leverantörer av digitala tjänster.

Regleringen utifrån NIS-direktivet 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. För att säkerställa att leverantörerna följde regleringen utsågs tillsynsmyndigheter med befogenheter att vidta tillsynsåtgärder när leverantörer uppvisade bristande efterlevnad. Tillsynsmyndigheternas hade enligt regleringen rätt att avkräva leverantörerna information som var relevant för tillsynen, begära tillträde till leverantörernas lokaler och utfärda vite.

I skäl 2 till NIS2-direktivet konstateras 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 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 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 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. Skrivelserna om tillsyn är mer omfattande än innan och kraven på tillsynsmyndigheter har skärpts och förtydligats.

NIS2-direktivet gör en skillnad på viktiga entiteter och väsentliga entiteter, där väsentliga entiteter bör omfattas av en mer utförlig tillsyn än viktiga entiteter. Av skäl 122 i NIS2-direktivet beskrivs tillsynens syfte och upplägg på följande sätt:

För att stärka de tillsynsbefogenheter och tillsynsåtgärder som bidrar till att säkerställa ett effektivt fullgörande av skyldigheter bör detta direktiv innehålla en minimiförteckning över tillsynsåtgärder och tillsynsmedel genom vilka behöriga myndigheter kan utöva tillsyn över väsentliga och viktiga entiteter. Dessutom bör detta direktiv fastställa en differentiering av tillsynssystemet mellan väsentliga och viktiga entiteter i syfte att säkerställa en rättvis balans vad gäller skyldigheterna för dessa entiteter och de behöriga myndigheterna. Väsentliga entiteter bör därför omfattas av ett heltäckande tillsynssystem med förhandstillsyn och efterhandstillsyn, medan viktiga entiteter bör omfattas av enklare tillsyn, endast i efterhand. Viktiga entiteter bör därför inte vara skyldiga att systematiskt dokumentera efterlevnad av riskhanteringsåtgärderna för cybersäkerhet, medan de behöriga myndigheterna bör tillämpa en reaktiv efterhandstillsyn och

därmed inte ha någon allmän skyldighet att utöva tillsyn över dessa entiteter. Efterhandstillsynen av viktiga entiteter kan utlösas av bevis, indikationer eller uppgifter som har kommit till de behöriga myndigheternas kännedom och som enligt dessa myndigheter tyder på potentiella överträdelser av detta direktiv. Sådana bevis, indikationer eller uppgifter kan exempelvis vara av den typ som de behöriga myndigheterna mottar från andra myndigheter, entiteter, medborgare, medier eller andra källor eller offentligt tillgänglig information eller härröra från annan verksamhet som de behöriga myndigheterna bedriver i samband med fullgörandet av sina uppgifter.

Cybersäkerhetslagen

NIS2-direktivet införs i svensk rätt genom cybersäkerhetslagen (2025:1506). I dess 3–5 kap. regleras tillsynsmyndigheternas befogenheter, när och hur de ska ingripa samt processen för överklagande.

Av 3 kap. 5–6 §§ framgår att tillsynsmyndigheter får utföra säkerhetsrevision av väsentliga verksamhetsutövare eller låta ett oberoende organ utföra sådan säkerhetsrevision. Det specificeras inte närmare i lagen hur urvalet av ett oberoende organ ska ske. Det ges inte heller någon inriktning kring hur det oberoende organet ska utföra säkerhetsrevisionen.

Av 3 kap. 7 § framgår att tillsynsmyndigheten får genomföra säkerhetsskanningar hos den som står under tillsyn. En sådan säkerhetsskanning ska ske i samarbete med verksamhetsutövaren. Det specificeras inte närmare i lagen hur säkerhetsskanning ska genomföras eller vad tillsynsmyndigheten ska beakta vid urval av verksamhetsutövare och system för säkerhetsskanning.

Av 3 kap. 10 § i lagen framgår att detta får meddelas i föreskrifter.

Regeringens proposition 2025/26:28 Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag

Av regeringens proposition 2025/26:28 Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag, framgår att lagen inte reglerar vilka krav som bör ställas på oberoende organ som anlitas av tillsynsmyndigheterna för att utföra säkerhetsrevision. Detta ska i stället regleras i föreskrifter och utifrån samordning mellan tillsynsmyndigheterna.[1]

Av propositionen framgår att säkerhetsskanningar avser skanning av verksamhetsutövarens nätverks- och informationssystem i syfte att upptäcka sårbarheter eller osäkert konfigurerade delar av systemet.[2] Regeringen konstaterar i propositionen att säkerhetsskanning inte måste vara icke-inkräktande och en

[1] Prop. 2025/26:28 s. 133–134.
[2] Prop. 2025/26:28 s. 136.

säkerhetsskanning får således påverka de system som skannas negativt. Säkerhetsskanning ska ske i samarbete mellan tillsynsmyndigheten och verksamhetsutövaren. Detta innebär att tillsynsmyndigheten ska involvera verksamhetsutövaren vid utförandet av säkerhetsskanningen, men det betyder inte att det måste finnas en samsyn i hur säkerhetsskanningen ska genomföras.[3]

I propositionen till cybersäkerhetslagen konstateras att NIS2-direktivet inte ger vägledning kring vilka moment som ska innefattas i en säkerhetsskanning. Därtill framgår att säkerhetsskanning kan bestå av olika moment som kan förändras över tid. Därför anses det inte vara lämpligt att reglera innehållet eller omfattningen av säkerhetsskanningar i lag. Det ska i stället regleras i föreskrifter.[4]

Föreskrifter och allmänna råd om säkerhetsrevision och säkerhetsskanning

Förslaget till föreskrifter och allmänna råd om säkerhetsrevision och säkerhetsskanning syftar till att förtydliga:

- hur en tillsynsmyndighets val av oberoende organ vid säkerhetsrevision enligt 3 kap. 5–6 §§ ska ske,
- hur det oberoende organ som anlitas för att genomföra en säkerhetsrevision enligt 3 kap. 5–6 §§ ska genomföra denna, och
- hur en säkerhetsskanning enligt 3 kap. 7 § ska genomföras,

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

Föreskrifterna ska vara ett stöd för både verksamhetsutövare och tillsynsmyndigheter genom att skapa transparens och enighet rörande hur säkerhetsrevision och säkerhetsskanning ska utföras och vad det ska avse.

Säkerhetsrevision

Cybersäkerhetslagen reglerar inte hur en tillsynsmyndighet eller ett oberoende organ som tillsynsmyndigheten anlitar för att genomföra en säkerhetsrevision ska göra detta. Lagen reglerar inte heller hur tillsynsmyndighetens val av ett oberoende organ ska ske.

Utredningen anser inte att det behöver regleras särskilt då tillsynsmyndigheten på egen hand utför säkerhetsrevisioner eftersom det ingår i uppgiften att bedriva tillsyn.[5] Däremot menar regeringen att de krav som ska ställas på ett oberoende

[3] Prop. 2025/26:28 s 137.
[4] Prop. 2025/26:28 s 137.
[5] Prop. 2025/26:28 s 131.

organ som utför säkerhetsrevision på uppdrag av en tillsynsmyndighet ska regleras i föreskrifter.[6] Detta är även av intresse ur ett verksamhetsutövarperspektiv då det finns ett behov av tydlig reglering kring vilka krav som ställs på ett oberoende organ för att säkerställa likvärdig tillsyn. För att säkerställa att tillsyn sker på enhetligt sätt krävs tydlig och konkret reglering kring hur oberoende organ utför säkerhetsrevision. Myndigheten för civilt försvars föreskrifter syftar därför till att tydliggöra hur detta urval ska ske och hur en säkerhetsrevision genomförd av ett oberoende organ ska ske.

Föreskrifternas utformning kan därtill underlätta för verksamhetsutövare som önskar att genomföra en säkerhetsrevision på egen bekostnad. Med tydliga enhetliga krav på ett oberoende organ kan verksamhetsutövaren anlita ett sådant och genomföra en säkerhetsrevision som tillgodoser önskad information. Det finns inte heller något som hindrar att tillsynsmyndigheterna använder föreskrifterna som vägledande vid genomförande av säkerhetsrevision som en del av sin tillsyn.

Säkerhetsskanning

Cybersäkerhetslagen reglerar inte vad som utgör en säkerhetsskanning eller hur den ska ske. Däremot framgår av propositionen till lagen att säkerhetsskanning utgör ett viktigt verktyg som skiljer sig från CSIRT-enhetens icke inkräktande säkerhetsskanning. Det poängteras därtill att det vid en säkerhetsskanning är av vikt att underlåta att orsaka negativ inverkan på verksamhetsutövarens system trots att en sådan får innebära störningar. Vissa störningar kan anses vara acceptabla om de krävs för att uppfylla säkerhetsskanningens syfte. Av denna anledning bör säkerhetsskanning utformas på ett sätt som är lämpligt med hänsyn till bland annat verksamhetsutövarens system.[7]

Säkerhetsskanning är inte en typisk tillsynsåtgärd inom en tillsynsmyndighets kompetens. Därtill kan en säkerhetsskanning bestå av olika moment som kan förändras över tid varför regeringen i propositionen konstaterar att det bör regleras i föreskrifter snarare än i lag.[8] Det är av intresse ur ett verksamhets-utövarperspektiv att genomförandet av säkerhetsskanning regleras för att främja transparens och enhetlighet. Myndigheten för civilt försvars föreskrifter syftar därför till att tydliggöra hur en säkerhetsskanning ska genomföras.

Sammantagen bedömning av vad som ska uppnås med föreskrifterna

[6] Prop. 2025/26:28 s 133–134.
[7] Prop. 2025/26:28 s 137–138.
[8] Prop. 2025/26:28 s 137.

Föreskrifterna stärker sammantaget cybersäkerheten i samhället genom att skapa förutsägbarhet, transparens och enhetlighet. Genom att reglera hur urvalet av oberoende organ ska gå till vid säkerhetsrevision, hur de oberoende organen ska utföra säkerhetsrevisionen, samt reglera hur säkerhetskanning utförs skapas förutsättningar för en god tillsyn som gynnar såväl tillsynsmyndigheter som verksamhetsutövare.

Uppgifter om vilka som berörs av regleringen

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

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

I bilaga 1 pekas de högkritiska sektorerna ut, totalt 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. Det anges att en verksamhet är av tillräcklig storlek om den minst kan betecknas som ett medelstort företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG.13. Ett vidare krav är att verksamheten tillhandahåller sina tjänster eller bedriver sin verksamhet i unionen. Artikel 2 i bilagan till kommissionens rekommendation definierar mikroföretag samt små och medelstora företag (SMF-kategorin). Av artikeln följer att ett medelstort företag är ett företag som sysselsätter minst 50 personer eller vars omsättning eller balansomslutning överstiger 10 miljoner euro per år.

Vissa sektorer och typer av verksamhetsutövare omfattas av NIS2-direktivet oavsett storlek. Det gäller exempelvis verksamhetsutövare som erbjuder allmänna

elektroniska kommunikationsnät, allmänt tillgängliga elektroniska 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 april 2026 hade 2080 företag, 83 statliga myndigheter, 19 regioner, 264 kommuner och 44 kommunalförbund anmält sig. Dessa har angivit att de bedriver verksamhet i en eller flera av följande sektorer; energi 629, transporter 158, bankverksamhet 88, finansmarknadsinfrastruktur 6, hälso- och sjukvårdssektorn 453, dricksvatten 206, avloppsvatten 206, digital infrastruktur 420, förvaltning av IKT-tjänster (mellan företag) 250, offentlig förvaltning 404, rymden 2, post- och budtjänster 18, avfallshantering 173, tillverkning, produktion och distribution av kemikalier 76, produktion, bearbetning och distribution av livsmedel 199, tillverkning 76, digitala leverantörer 14 och forskning 13.

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 cybersäkerhetslagen (2025:1506) och cybersäkerhetsförordningen (2025:1507) samt genom tillhörande myndighetsföreskrifter.

Utredningen SOU 2024:18 föreslog att endast regeringen skulle få meddela föreskrifter om säkerhetsrevision och att inga föreskrifter skulle meddelas om säkerhetsskanning.[9] Regeringen gjorde däremot bedömningen att det behövdes reglering på lägre nivå än lag varpå Myndigheten för civilt försvar gavs föreskriftsmandatet enligt 38 § 7 p. cybersäkerhetsförordningen.

Säkerhetsrevision

Medlemsstaterna ska enligt artikel 31.1 NIS2-direktivet säkerställa att deras behöriga myndigheter på ett ändamålsenligt sätt övervakar och vidtar de åtgärder som krävs för att säkerställa direktivets efterlevnad. Utan att det påverkar de nationella rättsliga och institutionella ramarna ska medlemsstaterna enligt artikel 31.4 NIS2-direktivet säkerställa att de behöriga myndigheterna, vid tillsynen av de offentliga förvaltningsentiteternas efterlevnad av detta direktiv och införandet av efterlevnadskontrollåtgärder vid överträdelser av detta direktiv, har lämpliga befogenheter att utföra dessa uppgifter och är operativt oberoende i förhållande till de offentliga förvaltningsentiteter som övervakas. Medlemsstaterna får besluta att införa lämpliga, proportionerliga och effektiva tillsyns- och efterlevnads-kontrollåtgärder med avseende på dessa entiteter i enlighet med nationella och institutionella ramar. Enligt artikel 32.2 b och c i NIS2-direktivet ska medlemsstaterna säkerställa att behöriga myndigheter, när de utövar sina tillsynsuppgifter avseende väsentliga entiteter, har befogenhet att underställa dessa entiteter säkerhetsrevisioner som utförs av ett oberoende organ eller en behörig myndighet. Vad som avses med ett oberoende organ, eller vilka moment en säkerhetsrevision ska innehålla, framgår dock inte av direktivet. Regeringen konstaterar i propositionen att detta bör regleras i föreskrifter.[10]

Ett alternativ till att reglera säkerhetsrevision vore att inte ge ut några föreskrifter alls och endast ge vägledning om detta. Avsaknaden av legala krav rörande hur tillsynsmyndigheter ska välja vilka oberoende organ som ska anlitas för att genomföra säkerhetsrevision och hur detta ska ske, bedöms medföra en ökad risk att säkerhetsrevisionen sker i varierade former beroende på vem som utför den. Skillnader i utförandet av säkerhetsrevisioner skulle kunna påverka trovärdigheten och ge varierad kvalitet i resultatet på säkerhetsrevisionerna vilket kan påverka myndigheternas möjlighet att bedriva en ändamålsenlig tillsyn. Detta bedöms i sin tur medföra en risk för att Sverige inte kan uppfylla alla NIS2-direktivets krav för tillsyn. Alternativet att enbart ge vägledning kring detta anses därför inte vara tillräckligt.

[9] SOU 2024:18 s. 236–239.
[10] Prop. 2025/26:28 s 133.

Ett ytterligare alternativ vore att reglera i detalj vad en säkerhetsrevision omfattar och hur den ska genomföras, oavsett om det är en tillsynsmyndighet eller ett oberoende organ som genomför den. Tillsynsmyndigheterna har ofta etablerade sätt att arbeta med tillsyn. En alltför detaljerad reglering av deras arbete riskerar att leda till att välfungerande arbetssätt behöver justeras vilket kan generera ökade kostnader för tillsynsmyndigheterna. Däremot skulle en reglering som inkluderar tillsynsmyndigheterna bidra till förenklad tillsynssamordning samt säkerställa att processen för en säkerhetsrevision likställs oberoende av vem som utför den. Detta skulle generera större förutsebarhet och således förenkla för de verksamhetsutövare som är föremål för åtgärden. Det framgår dock av 16 § cybersäkerhetsförordningen att tillsynsmyndigheterna ska komma överens om hur tillsynen ska genomföras. Detta är därmed en uppgift som redan tillfallit tillsynsmyndigheterna och ett behov av reglering i föreskrifter saknas därför i nuläget. Vad som därtill talar emot en reglering av tillsynsmyndigheternas utförande av säkerhetsrevision är det otydliga gränssnittet mellan säkerhetsrevision och övrig tillsyn. Mot bakgrund av detta reglerar föreskrifterna endast säkerhetsrevision som utförs av ett oberoende organ.

Säkerhetsskanning

Enligt artiklarna 32.2 d och 33.2 c i NIS 2-direktivet ska en behörig myndighet ha befogenhet att underställa entiteter säkerhetsskanningar på grundval av objektiva, icke-diskriminerande, rättvisa och transparenta riskbedömningskriterier. Skanningen ska ske i samarbete med den berörd verksamhetsutövare. Direktivet innehåller dock ingen definition av vad som avses med uttrycket säkerhets-skanning eller vilka moment en sådan ska innefatta. Regeringen konstaterar i propositionen att detta bör regleras i föreskrifter. [11]

Ett alternativ till att reglera säkerhetsskanning vore att inte ge ut några föreskrifter alls och endast ge vägledning om detta. Avsaknaden av legala krav rörande vad som utgör en säkerhetsskanning och vilka moment den ska inkludera bedöms medföra en risk att begreppet tolkas olika av olika verksamhetsutövare och tillsynsmyndigheter. Avsaknaden av tydliga ramar av vad säkerhetsskanning betyder och vilka moment en sådan kan inkludera riskerar att generera stor osäkerhet hos verksamhetsutövare då åtgärden saknar förutsebarhet. Alternativet att enbart ge vägledning kring detta anses därför inte ändamålsenligt i förhållande till medlemsstaternas skyldigheter enligt artikel 31 NIS 2-direktivet.

Ett ytterligare alternativ vore att inte reglera säkerhetsskanning i föreskrifter utan endast hänvisa till en etablerad standard för hur detta ska genomföras. En

[11] Prop. 2025/26:28 s 137.

standard anses dock inte ligga på rätt nivå, sett till behovet av flexibilitet i regleringen. Det är därtill möjligt att reglera på detaljnivå i föreskrifterna och redogöra för tekniklösningar. Detta anses dock göra föreskrifterna svårtillgängliga och fördyra processen för utförare såväl som verksamhetsutövare. Mot bakgrund av detta reglerar föreskrifterna säkerhetsskanning på en mer övergripande nivå.

Beskrivning och beräkning av förslagets eller beslutets kostnader och intäkter för staten och företagen

Kostnader för staten

De kostnadsmässiga och andra konsekvenser som följer av denna reglering bör bedömas utifrån ett helhetsperspektiv tillsammans med Myndigheten för civilt försvars övriga föreskrifter som utfärdas i enlighet med mandatet i cybersäkerhets-förordningen.

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

Föreskrifterna om säkerhetsrevision och säkerhetsskanning reglerar säkerhets-revision som utförs av ett oberoende organ samt säkerhetsskanning. Det kan innebära en kostnad för tillsynsmyndigheterna att anpassa sin verksamhet enligt kraven då tillsynsmyndigheten åläggs en rad skyldigheter vid urval av oberoende organ som anlitas för att genomföra säkerhetsrevision. Tillsynsmyndigheten är därtill den som står för kostnaden vid en säkerhetsskanning.

Uteblivna föreskrifter kan få kostsamma konsekvenser för tillsynsmyndigheterna. Utan styrning finns risk att det uppkommer olika tolkningar av hur säkerhetsrevision och säkerhetsskanning ska utföras. Detta kan leda till överimplementerad lagstiftning och att tillsynsmyndigheter vidtar mer kostsamma tillsynsåtgärder än vad som krävs.

Säkerhetsrevision och säkerhetsskanning är inte nya åtgärder och det finns inget som tyder på att tillsynsmyndigheterna kommer initiera flera sådana till följd av

[12] SOU 2024:18 s. 22.

regleringen. Regleringen anses därför inte medföra någon ytterligare kostnad för tillsynsmyndigheterna.

Kostnaden för företagen

Av SOU 2024:18 framgår att ”[f]örslagen medför även kostnader för enskilda verksamhetsutövare, men även dessa får stöd genom förslagen och det förebyggande arbetet kan medföra besparingar. Som framgått omfattas som huvudregel inte små företag. Kraven kommer att gälla inom hela unionen. Utredningen bedömer därför att regleringen inte får effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt.”

Föreskrifterna om säkerhetsrevision och säkerhetsskanning reglerar säkerhetsrevision som utförs av ett oberoende organ samt säkerhetsskanning. En säkerhetsrevision kan vara arbetsam för den verksamhetsutövare som blir föremål för den då det kan ta tid och resurser från denne vilket i sin tur kan påverka dess verksamhet. Dock bör säkerhetsrevision inte vålla större kostnad eller olägenhet än vad som är nödvändigt och får inte i onödan hämma verksamhetsutövarens affärsverksamhet.

Säkerhetsskanningar som utförs av en tillsynsmyndighet eller ett oberoende organ i deras ställe kan påverka verksamhetens kontinuitet och leda till oplanerade störningar, kostnader och förluster samt innebära integritets- och sekretessrisker. Det är däremot tillsynsmyndigheten som står kostnaden för en säkerhetsskanning och kostnaden för utförandet är således inget som belastar verksamhetsutövaren. Vid en säkerhetsskanning ska dock lämpliga åtgärder vidtas för att minska negativ inverkan på funktionaliteten hos systemen och övriga negativa konsekvenser för den berörda verksamhetsutövaren. Tillsynsmyndigheten kan överväga att avstå från att genomföra en säkerhetsskanning om de bedömer risken för störningar för hög.

När en tillsynsmyndighet eller det oberoende organ som denne anlitat utför säkerhetsrevision eller säkerhetsskanning kan driften störas. Exempelvis kan säkerhetsskanning orsaka tillfälliga negativa effekter på de system som skannas. Föreskrifterna har utformats med funktionalitet och kostnadseffektivitet i beaktande och uppmanar tillsynsmyndigheterna att säkerställa minimerade störningar av verksamheten vid genomförandet av säkerhetsrevision och säkerhetsskanning.

Uteblivna föreskrifter kan få kostsamma konsekvenser för verksamhetsutövare. Utan tydlig styrning finns en risk att det uppkommer olika tolkningar av hur säkerhetsrevision och säkerhetsskanning ska utföras. Föreskrifterna syftar därför till att tillhanda tydliga rättsliga ramar vilket skapar ökad förutsebarhet vid

säkerhetsrevision och säkerhetsskanning. Detta gör det möjligt för verksamhetsutövaren att förbereda sin verksamhet för en åtgärd av detta slag redan innan den sker vilket kan generera minskade kostnader för verksamhetsutövaren då en sådan väl genomförs.

Utan reglering i föreskrifter finns därtill en risk att tillsynen inte blir tillräcklig och att sårbarheter respektive cyberhot i verksamhetsutövarnas system inte upptäcks. I förlängningen riskerar verksamhetsutövarnas system att bli mer sårbara för angrepp vilket kan medföra både stora kostnader och störningar i driften.

Regleringen medför en rad krav på det oberoende organ som anlitas av en tillsynsmyndighet för att utföra en säkerhetsrevision. Det oberoende organet behöver vara opartiskt, självständigt och objektivt. Detta skulle kunna innebära att ett oberoende organ, för att kunna åta sig att utföra en säkerhetsrevision på uppdrag av en tillsynsmyndighet, behöver dokumentera vilka verksamhetsutövare det är, eller har varit involverade med på olika sätt för att för att kunna styrka sin opartiskhet, självständighet och objektivitet gentemot verksamhetsutövaren som är föremål för den aktuella säkerhetsrevisionen. Detta kan för vissa oberoende organ antas medföra en viss ökning av administrativa åtgärder och därigenom generera en ökad administrativ kostnad.

Regleringens krav på oberoende, opartiskhet och självständighet medför därtill att ett oberoende organ inte kan anlitas för vilka säkerhetsrevisioner som helst. Inom vissa områden finns det dessutom få oberoende organ som har den expertkunskap som krävs för att kunna utföra en säkerhetsrevision. Detta kan leda till att det uppkommer en brist på kvalificerad personal som kan utföra säkerhetsrevisioner vilket i förlängningen kan leda till ett minskat antal genomförda säkerhetsrevisioner. Detta bedöms dock initialt endast inträffa i enstaka fall.

För de verksamhetsutövare som blir föremål för en säkerhetsrevision eller säkerhetsskanning kan det antas gå resurser till att tillsammans med tillsynsmyndigheten planera och möjliggöra den aktuella åtgärden. De personer i verksamheten som skulle kunna bli aktuella för att genomföra förberedande arbete inför säkerhetsrevisionen skulle behöva ägna ungefär 8–20 timmar åt detta. Ytterligare tid kan behöva läggas utifrån instruktion från tillsynsmyndigheten eller utföraren om någon speciell förberedelse behövs inför revisionen eller skanningen. Därutöver behöver verksamhetens ledning delta vid redovisning av resultatet av aktuell säkerhetsrevision eller säkerhetsskanning. Denna tidsåtgång uppskattas till ungefär mellan 1–4 timmar. Under säkerhetsrevisionens eller säkerhetsskanningens gång finns det dessutom behov av ytterligare personal från verksamhetsutövaren som bistår med olika saker för att möjliggöra åtgärden. Verksamhetsutövaren kan

dessutom efter redovisat resultat av säkerhetsrevisionen eller säkerhetsskanningen behöva genomföra vissa åtgärder. Sådana åtgärder i form av ändringar i konfigurationer eller motsvarande justeringar föranleder en riskbedömning där verksamhetsutövaren bedömer riskerna med ändringarna, planerar och testar lösningar innan de produktionsätts. Denna tidsåtgång uppskattas till ungefär 40 – 200 timmar.

Föreskrifterna antas inte leda till att fler säkerhetsrevisioner eller säkerhetsskanningar utförs än vad som sker idag. Beroende på hur många verksamhetsutövare det är och dess betydelse i sektorn samt sett till relevant tillsynsmyndighets resurser kan intervallet mellan dessa åtgärder för varje enskild verksamhetsutövare variera mellan en gång om året till en gång vart tionde år. Det kan också vara så att tillsynsmyndigheten inte bedömer dessa åtgärder som en lämplig tillsynsåtgärd alls. Med anledning av att dessa åtgärder sker relativt sällan anses de kostnader i administrativa åtgärder och personalkostnader som dem medför ändock proportionerliga.

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

Nedan följer en genomgång hur Myndigheten för civilt försvar bedömer andra konsekvenser än de som nämns ovan kan komma att påverka företagen.

Förstärkning av företagens cybersäkerhet

Myndigheten för civilt försvar 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. Att som verksamhetsutövare ha en hög nivå av cybersäkerhet bidrar till ökad tillförlitlighet på marknaden vilket i sin tur gynnar verksamhetsutövarens verksamhet. Dessa föreskrifter specificerar granskning i form av säkerhetsrevision respektive säkerhetsskanning ska ske. Föreskrifterna bedöms således ge ett ökat incitament för verksamhetsutövare att vidta relevanta åtgärder för att stärka cybersäkerheten i sina system. Detta då sådana åtgärder inte bara bidrar till att stärka verksamhetsutövarens cybersäkerhet och därmed även samhällets samlade cybersäkerhet, utan också skapar en möjlighet för verksamhetsutövaren att uppnå bättre resultat vid en sådan granskning som föreskrifterna reglerar.

Konkurrensen mellan företagen

Med hänsyn till att NIS2-direktivet kommer att gälla samma typer av företag i hela unionen och förslagen i stor utsträckning är nödvändiga för att genomföra NIS 2-direktivet i nationell rätt bedömer Myndigheten för civilt försvar att regleringen i

stort inte kommer att påverka konkurrensförhållanden på marknaden. NIS2-direktivet är ett minimidirektiv men införs i Sverige utan nationell utvidgning. Den regelbörda som svenska företag får genom cybersäkerhetslagen anses således inte överstiga andra medlemsstaters implementering av direktivet i någon betydande utsträckning. Med det sagt är det som regeringen påpekar i propositionen, ofrånkomligt att direktivet i viss utsträckning kommer att genomföras på olika sätt i olika medlemsstater utifrån de tolkningar och överväganden om behov som görs i de nationella lagstiftningsärendena.

Trots detta kan inte uteslutas att företags konkurrensförmåga kan komma att påverkas av regleringen. Det är möjligt att det uppstår skillnader beroende på företagets storlek, dess geografiska belägenhet eller liknande. Regleringen kan komma att påverka företag som endast har ett fåtal anställda med den kompetens som krävs för att utföra en säkerhetsrevision eller säkerhetsskanning. Kraven på oberoende, självständighet och objektivitet gentemot den verksamhetsutövare som blir föremål för åtgärden kan komma att påverka antalet uppdrag som den utförande verksamhetsutövaren kan åta sig. Det kan antas att detta kan ha en viss inverkan på potentiella utförares intresse för att ta på sig sådana uppdrag. Kraven anses ändock behövliga för att i ökad utsträckning främja likvärdig tillsyn varpå de anses vara proportionerliga.

Små och medelstora 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 överliggande EU-rätt vilket begränsar möjligheterna till särskild hänsyn. 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.

Medelstora företag omfattas av regleringen i de fall de tillhör någon av sektorerna. Däremot bedöms ingen särskild insats, utöver det stöd som redan ges till just dessa företag, behövas. I den mån tillsyn utförs i form av säkerhetsrevision och säkerhetsskanning tas därtill hänsyn till företagens storlek.

Bedömning av vilka åtgärder som har vidtagits för att förslaget eller beslutet inte ska medföra mer långtgående kostnader eller begräsningar än vad som bedöms vara nödvändigt för att uppnå dess syfte

NIS2-direktivet syftar enligt skäl 122 till att stärka de tillsynsbefogenheter och tillsynsåtgärder som bidrar till att säkerställa ett effektivt fullgörande av skyldigheter enligt direktivet. Syftet uppfylls genom att reglera utförandet av säkerhetsrevision och säkerhetsskanning. Regleringen ämnar därtill att främja likvärdig tillsyn och skapa tydlighet och förutsebarhet för såväl tillsynsmyndigheter och de verksamhetsutövare som blir föremål för åtgärderna.

Det framgår av föreskrifterna att en säkerhetsrevision ska utformas på ett sådant sätt att den inte vållar större kostnad eller olägenhet än vad som är nödvändigt. Även säkerhetsskanningen har begränsats till att endast genomföras i den omfattning som är nödvändig för tillsynen. Det framgår dessutom att det vid en säkerhetsskanning ska vidtas lämpliga åtgärder för att minska negativ inverkan på funktionaliteten hos systemen och övriga negativa konsekvenser för verksamhetsutövaren. som övriga negativa konsekvenser kan inkluderas ekonomiska sådana.

Dessa skrivningar har inkluderats för att främja kostnadseffektiv tillsyn, både gällande säkerhetsrevision och säkerhetsskanning. De har inkluderats för att säkerställa att tillsynsmyndigheten alltid har verksamhetsutövarens kostnader i åtanke vid genomförande av dessa åtgärder. På detta vis säkerställs att regleringen inte medför mer långtgående kostnader eller begränsningar än vad som bedöms vara nödvändigt för att uppnå dess syfte.

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 lag och förordning och därmed göra det enklare att efterleva dessa, behöver föreskrifterna träda ikraft i så nära anslutning som möjligt till detta datum.

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.

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 både 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.

Hur och när konsekvenserna kan utvärderas

Föreskrifterna om säkerhetsrevision och säkerhetsskanning träder i kraft den 1 oktober 2026. För att möjliggöra en meningsfull inledande uppföljning bör föreskrifterna ha varit i ikraftträdda i minst tolv månader, varpå denna bör genomföras i oktober 2027. Detta då tolv månader anses vara tillräckligt lång tid för att ett flertal tillsynsmyndigheter ska ha utgått från regleringen vid säkerhetsrevision och säkerhetsskanning. Därefter bör uppföljningen ske minst en gång om året.

En första uppföljning kommer att ske så snart det är möjligt att utvärdera reglernas effekter och därefter regelbundet.

Föreskrifterna om säkerhetsrevision och säkerhetsskanning kommer att påverka tillsynsmyndigheter såväl som verksamhetsutövare. Av denna anledning är det i Myndigheten för civilt försvars intresse att följa upp föreskrifternas konsekvenser för både tillsynsmyndigheter som verksamhetsutövare.

Myndigheten för civilt försvar ska enligt 40 § cybersäkerhetsförordningen leda ett samarbetsforum där tillsynsmyndigheterna ingår. Uppföljning av dessa föreskrifter ska således ske inom detta forum. Föreskrifterna om säkerhetsrevision och säkerhetsskanning förväntas också påverka verksamhetsutövare. För att säkerställa en bred och inkluderande uppföljning behöver även deras synpunkter inhämtas. De verksamhetsutövare som omfattas av föreskriften är anmälda och därmed kända av Myndigheten för civilt försvar. Myndigheten kommer därtill kunna få information om vilka verksamhetsutövare som blivit föremål för tillsyn genom samarbetsforumet för tillsynsmyndigheter vilket underlättar uppföljningen. Verksamhetsutövare har därtill möjlighet att kontakta Myndigheten för civilt försvar genom de kontaktvägar som hänvisas till på hemsidan. Föreskrifterna syftar till att främja en transparent och förutsebar tillsyn. Om verksamhetsutövare anser att säkerhetsrevision eller säkerhetsskanning skiljer sig märkbart åt beroende

på vem som utför den bör detta hanteras i första hand i form av vägledning. Även 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 aviserat ska ske tre år efter den nya lagens ikraftträdande. Utvärderingen bör ske i nära samverkan med utpekade tillsynsmyndigheter för att säkerställa att underlag inhämtas från så många av NIS2-sektorerna som möjligt. Det övergripande syftet med en sådan utvärdering blir att få en bild av hur det nya regelverket påverkat verksamhetsutövarens cybersäkerhetsarbete och cybersäkerhet inklusive kostnads- och verksamhetsmässiga konsekvenser. Utvärderingen bör även inkludera ändamålsenligheten av tillhandahållet stöd i form av vägledningar med mera.

Föreskrifter och föreskriftsmandat gällande cybersäkerhetslagens reglering av säkerhetsrevision och säkerhetsskanning kommer att flyttas över till Försvarets radioanstalt den 1 juli 2026. Med anledning av detta kommer uppföljningen av konsekvenser ske hos Försvarets radioanstalt.

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

Bedömning av om förslaget 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 och regleringen går inte utöver miniminivån. För ytterligare om utrymmet för nationell anpassning se ovan redovisning av alternativa lösningar som övervägts liksom nedan redovisning om konkurrenspåverkan.

Uppgifter om de bemyndiganden som myndighetens beslutanderätt grundar sig på

NIS2-direktivet implementeras genom cybersäkerhetslagen (2025:1506) och cybersäkerhetsförordningen (2025:1507). Av 38 § 7 p. cybersäkerhetsförordningen framgår att Myndigheten för civilt försvar får meddela föreskrifter rörande säkerhetsrevision och säkerhetsskanning enligt 3 kap. 5–7 §§ cybersäkerhetslagen.

Datum
2026-04-22

Diarienummer
MCF 2026-06325

Övriga konsekvenser

Föreskrifterna bedöms inte innebära några förändringar av kommunala befogenheter eller skyldigheter utöver att definiera cybersäkerhetslagens reglering om säkerhetsrevision och säkerhetsskanning. Föreskrifterna bedöms inte påverka grunderna för kommuners eller regioners organisation eller verksamhetsformer.

Kontaktpersoner

Ida Sahlin och Helena Andersson