# Remissversion: Konsekvensutredning rörande Myndigheten för samhällsskydd och beredskaps föreskrifter om säkerhetsåtgärder och utbildning

## Allmänt

### Beskrivning av problemet och vad man vill uppnå

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

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

Det första NIS-direktivet genomfördes i svensk rätt genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen) och den tillhörande förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-förordningen).

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

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

Det konstateras i skäl 2 till NIS2-direktivet att det tidigare NIS-direktivet har lett till betydande framsteg när det gäller att stärka EU:s cyberresiliens. Direktivet har bidragit till att nationell kapacitet har byggts upp och till att samarbetet på unionsnivå har utvecklats.

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

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

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

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

Till skillnad från NIS-direktivet gäller den nya regleringen hela verksamheten hos aktören, inte enbart säkerheten i de nätverk och informationssystem som används för den samhällsviktiga eller digitala tjänsten.

NIS2-direktivet implementeras i första hand genom kommande cybersäkerhetslag och cybersäkerhetsförordning. I cybersäkerhetslagen finns det bemyndiganden att utfärda föreskrifter inom en rad områden.

I avsaknad av ännu beslutad lag och förordning utgår arbetet med föreskrifter och allmänna råd samt konsekvensutredning från förslaget på cybersäkerhetslag (cybersäkerhetslagen) i regeringens proposition 2025/26:28 Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag[1] (propositionen) samt regeringens uppdrag till Myndigheten för samhällsskydd och beredskap att förbereda genomförandet av NIS 2-direktivet, Fö2025/01293.

### Föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning

Enligt artikel 21.1 första stycket i NIS2-direktivet ska medlemsstaterna säkerställa att väsentliga och viktiga entiteter vidtar lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder. Syftet är att hantera risker som hotar säkerheten i de nätverk och informationssystem som används i verksamheten eller för att tillhandahålla tjänster.

Åtgärderna ska bidra till att förhindra eller minimera incidenters påverkan på tjänstemottagarna och andra tjänster.

[1] Prop. 2025/26:28 Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag

Av artikel 21.1 framgår bland annat att säkerhetsåtgärderna ska baseras på en allriskansats. Denna ansats ska skydda både nätverk och informationssystem samt deras fysiska miljö från incidenter.

Direktivets krav på säkerhetsåtgärder införs i svensk rätt genom 2 kap. 3 § cybersäkerhetslagen. De åtgärder som listas artikel 21.2 i NIS2-direktivet (och i 2 kap. 3 § 2 stycket cybersäkerhetslagen) utgör en miniminivå. Denna nivå måste minst vara uppfylld för att varje medlemsstat ska kunna bidra till NIS2-direktivets syfte att uppnå en hög gemensam cybersäkerhetsnivå inom unionen.

Enligt artikel 20 punkt 2 i NIS2-direktivet ska medlemsstaterna säkerställa att medlemmarna i entiteters ledningsorgan är skyldiga att genomgå utbildning. Detta krav införs i svensk reglering genom 2 kap. 4 § cybersäkerhetslagen.

Förslaget till föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning avser verksamhetsutövarens skyldighet enligt 2 kap. 3 § cybersäkerhetslagen att vidta säkerhetsåtgärder samt ledningens skyldighet att genomgå utbildning om säkerhetsåtgärder enligt 2 kap. 4 § cybersäkerhetslagen. Föreskrifterna och tillhörande vägledning syftar till att förtydliga cybersäkerhetslagens krav och inrikta verksamhetsutövarnas val och utformning av säkerhetsåtgärder. Målet är att uppnå hög cybersäkerhet i samhället som svarar mot Sveriges behov och uppfyller EU:s krav.

*Cybersäkerhet och civilt försvar*

Regleringen på nationell nivå behöver ta hänsyn till varje medlemsstats förutsättningar och utmaningar. Sverige har en hög grad av digitalt beroende. Mot bakgrund av den nuvarande hotbilden kan bristande cybersäkerhet få påtagliga konsekvenser för samhällets funktionalitet. Detta påverkar i sin tur förutsättningarna för krisberedskap och civilt försvar.

Betydelsen av cybersäkerhet understryks i Försvarsmaktens och Myndigheten för samhällsskydd och beredskaps (MSB) uppdragsredovisning *Utgångspunkter för totalförsvaret 2025 – 2030*. Där konstateras att hotbilden är bred och omfattar konventionella militära angrepp, cyberangrepp, sabotage, informationspåverkan, terrorism och ekonomiska påtryckningar.[2]

Vidare slås fast att säkerhetsläget kräver ett robust, flexibelt och samordnat totalförsvar. Det ska kunna möta flera hot samtidigt, säkerställa viktiga samhällsfunktioner stärka Natos kollektiva säkerhet. För att uppnå detta krävs en samordnad och flexibel planering från både civila och militära aktörer. Civila aktörer har en central roll i att stödja det militära försvaret och

[2] Försvarsmakten och Myndigheten för samhällsskydd och beredskap, Utgångspunkter för totalförsvaret 2025 – 2030, 2025, https://www.msb.se/siteassets/dokument/om-msb/vart-uppdrag/regeringsuppdrag/besvarade-regeringsuppdrag/2025/utgangspunkter-for-totalforsvaret-2025-2030.pdf

upprätthålla viktiga samhällsfunktioner, även under ansträngda förhållanden och krig.[3]

I redovisningens slutsatser betonas behovet av en grundläggande förmåga och motståndskraft hos alla aktörer inom totalförsvaret. Som en lärdom från Rysslands fullskaliga invasion av Ukraina lyfts särskilt vikten av arbete med cybersäkerhet och informationssäkerhet. Organisationer behöver utveckla sin förmåga att identifiera och hantera antagonistiska åtgärder och hybridangrepp inom den egna verksamheten. De behöver också öka förståelsen för hot inom cyberdomänen samt stärka sin förmåga att hantera cyberhot. Cybersäkerhet och informationssäkerhet ska kunna upprätthållas under såväl fred som under höjd beredskap och krig. Detta gäller på alla ledningsnivåer, även inom näringslivet och hos privata aktörer.

En hög cybersäkerhetsnivå i samhället bidrar till en robust grund för det civila försvaret och till ett effektivt cyberförsvar.[4]

*Begreppet cybersäkerhet*

Terminologin på informations- och cybersäkerhetsområdet är under utveckling. I 1 kap. 2 § punkt 5 cybersäkerhetslagen definieras cybersäkerhet som all verksamhet som är nödvändig för att skydda nätverk och informationssystem, användare av dessa system och andra berörda personer mot cyberhot.

Med cyberhot avses en potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka nätverk och informationssystem, deras användare och andra personer.

I NIS 2-direktivet definieras begreppen genom hänvisning till artikel 2.1 respektive 2.8 i EU:s cybersäkerhetsakt.[5] Begreppet cybersäkerhet har i andra sammanhang ibland haft en snävare betydelse med större tekniskt fokus, närmare det som brukar benämnas it-säkerhet. Den legaldefinition som nu fastslagits av EU innebär istället att cybersäkerhet har fått en innebörd som i stort kan likställas med det som traditionellt beskrivs som informationssäkerhet.

Eftersom det kan finnas olika uppfattningar om vad cybersäkerhet innebär, behöver föreskrifterna med tillhörande vägledning bidra till en gemensam

[3] Sid 2, Utgångspunkter för totalförsvaret 2025 – 2030.
[4] Sid 39, Utgångspunkter för totalförsvaret 2025 – 2030.
[5] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2103 (cybersäkerhetsakten).

förståelse för begreppet cybersäkerhet i enlighet med EU:s legalt fastslagna definition.

*Systematiskt och riskbaserat arbete*

Det finns inte något separat krav i cybersäkerhetslagen på att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete. Ett sådant krav finns däremot i lagen om informationssäkerhet för samhällsviktiga och digitala tjänster. I SOU 2024:18 – Genomförande av NIS2- och CER-direktiven föreslog att ett motsvarande krav även skulle finnas i den nya cybersäkerhetslagen. Det framgår dock av propositionen[6] att kravet på att bedriva ett systematiskt och riskbaserat arbete redan bedöms följa av säkerhetskraven som ställs på verksamhetsutövarna enligt artikel 21 punkt 1 i NIS2-direktivet och 2 kap. 3 § cybersäkerhetslagen. Införandet av ett separat krav skulle därför enligt regeringen innebära dubbelreglering. Föreskrifterna och de allmänna råden samt därtill hörande vägledning behöver därför förtydliga att ett systematiskt och riskbaserat arbete med cybersäkerhet i sig utgör en säkerhetsåtgärd.

*Sektorsgemensamma och sektorsspecifika krav*

Organisationer som omfattas av det första NIS-direktivets tillämpningsområde, det vill säga samhällsviktiga och digitala leverantörer omfattas i dag av föreskrifter och allmänna råd från MSB. Dessa regler gäller det systematiska och riskbaserade informationssäkerhetsarbete som leverantörer av samhällsviktiga tjänster ska bedriva enligt 11 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Flera av de utpekade tillsynsmyndigheterna har också utfärdat föreskrifter och allmänna råd med krav på säkerhetsåtgärder enligt 12 – 14 §§ i samma lag. Kraven gäller nätverks- och informationssystem för samhällsviktiga tjänster inom följande sektorerna:

- energi
- transport
- bankverksamhet
- finansmarknadsinfrastruktur
- hälso- och sjukvård
- leverans och distribution av dricksvatten
- digital infrastruktur
- digitala tjänster

Andelen föreskriftskrav som innehåller sektorsunika åtgärder, exempelvis särskilda säkerhetsåtgärder för nätverk och informationssystem inom en viss

[6] Prop. 2025/ s 84 f.

sektor, är i nuvarande NIS-reglering dock begränsad. Samtidigt skiljer sig sektorsföreskrifterna åt i både utformning och struktur.

Tillämpningsområdet för NIS2-direktivet är utökat i förhållande till NIS-direktivet. Redan nu existerande NIS-sektorer kommer att omfatta fler organisationer och ett antal nya sektorer tillkommer när cybersäkerhetslagen börjar gälla. Till detta kommer att kraven på verksamhetsutövare gäller, med några undantag, hela verksamhetsutövarens verksamhet. Inte bara, såsom i nuvarande NIS-reglering, de nätverk och informationssystem som används för att tillhandahålla samhällsviktiga och digitala tjänster.

MSB har av regeringen fått i uppdrag att förbereda för att meddela föreskrifter för säkerhetsåtgärder och utbildning för samtliga sektorer med undantag för säkerhetsåtgärder för sektorerna digital infrastruktur, digitala leverantörer, förvaltning av IKT-tjänster (mellan företag), post- och budtjänster och rymden.[7] Föreskrifterna och de allmänna råden samt därtill hörande vägledning behöver därför utformas för att kunna tillämpas i all verksamhet[8] hos verksamhetsutövarna i samtliga NIS2-sektorer med undantag för sektorerna digital infrastruktur, digitala leverantörer, förvaltning av IKT-tjänster (mellan företag), post- och budtjänster och rymden men vid behov även inkludera sektorsspecifika krav. I detta ligger även att ta höjd för cyberfysiska system och deras särskilda förutsättning.

### Uppföljning av konsekvenser av föreskrifter och allmänna råd

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

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

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

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

*Inga föreskrifter eller endast vägledning*

Ett alternativ till att reglera säkerhetsåtgärder och utbildning i föreskrifter och allmänna råd är att inte vidta några åtgärder alls eller endast ge ut vägledning rörande hur verksamhetsutövarna ska uppfylla kraven i 2 kap. 3 – 4 §§

[7] Uppdrag till Myndigheten för samhällsskydd och beredskap att förbereda genomförandet av NIS 2-direktivet, Fö2025/01293.
[8] Med undantag för säkerhetskänslig och brottsbekämpande verksamhet.

cybersäkerhetslagen. I lagen räknas ett antal säkerhetsåtgärder upp som minst ska vidtas av verksamhetsutövarna. De är samtliga av övergripande karaktär, exempelvis ”strategier för riskanalys och informationssystemens säkerhet”.

Det finns redan idag ett omfattande och fritt tillgängligt stöd för arbete på informations- och cybersäkerhetsområdet. Exempelvis tillhandahåller MSB både metodstöd för arbete med informations- och cybersäkerhet, utbildningar samt vägledningar för hantering av säkerhet i nätverk och informationssystem, upphandling, fysisk säkerhet i it-utrymmen med mera. Tillgängligt stöd kan redan idag hjälpa verksamhetsutövaren att införa sådana säkerhetsåtgärder som nämns i cybersäkerhetslagen. Det krävs endast mindre justeringar och tillägg för att stödet ska bli NIS2-anpassat i sin helhet.

MSB har sedan 2021 regelbundet genomfört cybersäkerhetsmätningar, främst genom Cybersäkerhetskollen, av nivån på verksamhetens systematiska cybersäkerhetsarbete. Mätningarnas omfattning har stegvis utökats och under 2025 mäter Cybersäkerhetskollen nivån på det systematiska arbetet med cybersäkerhet och särskilt it-säkerhet, ot-säkerhet och säkerhet i leveranskedjor. Inskickade svar kommer hittills främst från offentlig förvaltning. Samtliga hittills genomförda mätningar visar på brister i det systematiska cybersäkerhetsarbetet.

Vad gäller verksamhetsutövarna inom sektorn offentlig förvaltning är det endast statliga myndigheter[9] som i sin helhet omfattas av krav som är jämförbara med kraven i cybersäkerhetslagen. De åläggs att uppfylla säkerhetskrav för sina informationshanteringssystem enligt förordning (2022:524) om statliga myndigheters beredskap.[10] Säkerhetskraven för statliga myndigheter förtydligas i MSB:s föreskrifter och allmänna råd om informationssäkerhet för statliga myndigheter (MSBFS 2020:6) och MSB:s föreskrifter och allmänna råd om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7). MSB:s föreskrifter och allmänna råd för statliga myndigheter omfattas inte av tillsyn. Kommuner och regioner (och några enstaka statliga myndigheter) omfattas av NIS-regleringen, dvs lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, men regleringen gäller endast i de delar de tillhandahåller sådana tjänster, exempelvis hälso- och sjukvård eller energi.[11] Till detta kommer reglering som exempelvis rör hantering av viss information eller viss verksamhet. Här kan exempelvis nämnas dataskyddsförordningen[12] som reglerar hanteringen av

[9] Ett antal statliga myndigheter är undantagna från regleringen i enlighet med 3 § förordning (2022:524) om statliga myndigheters beredskap.
[10] Begreppet informationshanteringssystem omfattar sådana nätverk och informationssystem som regleras i NIS2-direktivet.
[11] Utöver detta gäller säkerhetsskyddslagen för säkerhetskänslig verksamhet och hantering av säkerhetsklassificerad information. Hanteringen av vissa typer av information, såsom patientjournaler, kan omfattas av särskild reglering.
[12] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)

personuppgifter och säkerhetsskyddslagen (2018:585) som reglerar arbetet med att skydda säkerhetskänslig verksamhet.

Cybersäkerhetskollen och andra analyser visar på brister trots tillgång till omfattande stöd och även viss reglering rörande både hur ett systematiskt och riskbaserat arbete med cybersäkerhet bedrivs och vilka tekniska och driftrelaterade säkerhetsåtgärder som införts.

MSB gör därför bedömningen att för att uppnå avsedd höjning av cybersäkerheten i samhället är det otillräckligt att inte vidta några åtgärder alls alternativt endast tillhandahålla vägledning för hur lagens krav ska följas.

*Standarder och certifiering*

Ett annat alternativ till att närmare konkretisera innebörden av 2 kap. 3 § cybersäkerhetslagen i föreskrifter är att låta föreskrifterna enbart peka på standarder på området såsom ISO/IEC 27000 och koppla det till krav på certifiering. Standarder och möjligheten till att genomföra certifiering utgör ett viktigt stöd för organisationer. Vissa standarder har en bred tillämpning och andra fokuserar på ett mer begränsat område vilket kan skapa ett behov av att i så fall anvisa verksamhetsutövare att efterleva flera olika standarder för att säkerställa att alla aspekter i cybersäkerhetslagen omhändertas. Standarder uppdateras och utvecklas i enlighet med etablerade format som inte sällan kan ta flera år, vilket också det bör beaktas vid valet om standarder är ett lämpligare format är föreskriftskrav. Certifiering är ofta tidskrävande och kräver särskilt utbildad personal. Ett krav på att upp till två tusen verksamhetsutövare skulle certifiera hela sitt säkerhetsarbete samtidigt bedöms som svårhanterligt utifrån den svenska certifieringsmarknaden. Det finns inget som hindrar att tillsynsmyndigheterna i sin riskbedömning över en verksamhetsutövares cybersäkerhet kan beakta resultatet av genomförda certifieringar.

Till detta kommer att 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. Tillsynsmyndigheten ska utöva tillsyn över att cybersäkerhetslagen och föreskrifter som har meddelats i anslutning till lagen följs. I Cybersäkerhetslagen finns bestämmelser om att tillsynsmyndigheten ska ingripa om verksamhetsutövaren åsidosatt sina skyldigheter enligt regleringen. Ett ingripande sker enligt 4 kap. 1 § cybersäkerhetslagen genom beslut om föreläggande, ansökan om förbud att inneha ledningsfunktion, beslut om sanktionsavgift eller, om det inte finns skäl att ingripa mot en överträdelse på något annat sätt, genom anmärkning. Avsaknad av föreskrifter som förtydligar kraven i 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. Exempelvis behöver storleken på sanktionsavgifter kunna härledas till de konsekvenser bristande

kravuppfyllnad får i förhållande till regleringens syfte. Bristande efterlevnad av en vägledning kan inte åtgärdas genom tillsyn.

MSB gör därför bedömningen att fördelarna med att förtydliga lagkraven i föreskrifter och allmänna råd överväger fördelarna med att enbart hänvisa till standarder och kräva certifiering. Ett samlat regelverk blir enklare att följa än en uppsättning av flera olika standarder, det är enklare att anpassa till svenska förhållanden samt att skyndsamt uppdatera krav för att möta en förändrad hotbild mot Sverige om så behövs. Till detta kommer även en förbättrad möjlighet att hantera inriktning från EU för att på så sätt stärka harmoniseringen och i förlängningen uppnå en hög nivå av cybersäkerhet inom unionen.

*Utformning av föreskrifter och allmänna råd*

När föreskrifter på området utformas bör utgångspunkten vara att nivån på kraven ska läggas så att samhällets behov av cybersäkerhet omhändertas. Samtidigt bör arten och komplexiteten i föreskrifterna, så långt det är möjligt, ligga på en nivå som verksamhetsutövarna själva skulle komma fram till vid en samlad analys. En nivå av säkerhet som sannolikt motsvarar vad en säkerhetsmedveten organisation redan har på plats.

Kraven i sin helhet skapar förutsättningar för verksamhetsutövaren att vidta lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att skydda nätverk och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och systemens fysiska miljö mot incidenter (säkerhetsåtgärder). I detta ingår att skydda nätverkens och informationssystemens fysiska miljö. Incidenter definieras i1 kap. 2 § cybersäkerhetslagen. Säkerhetsåtgärderna ska utgå från ett allriskperspektiv och säkerställa en nivå på säkerheten i nätverk och informationssystemen som är lämplig i förhållande till risken.

*Hur föreskrifterna och de allmänna råden implementerar cybersäkerhetslagens krav på säkerhetsåtgärder*

Av cybersäkerhetslagen framgår att säkerhetsåtgärderna ska utgå från ett allriskperspektiv och säkerställa en nivå på säkerheten i nätverk och informationssystemen som är lämplig i förhållande till risken. Säkerhetsåtgärderna ska åtminstone omhänderta de områden som räknas upp i cybersäkerhetslagen 2 kap. 3 § andra stycket. De uppräknade områdena motsvarar artikel 21 punkt 2 NIS2-direktivet.

Nedan följer en övergripande redovisning av hur lagkraven förtydligats och konkretiserats i föreskrifter och allmänna råd.

Av 2 kap. 3 § första och andra stycket cybersäkerhetslagen framgår att verksamhetsutövare ska vidta lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att skydda nätverk och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och systemens fysiska miljö mot incidenter

(säkerhetsåtgärder).I detta ingår att skydda nätverkens och informationssystemens fysiska miljö. Säkerhetsåtgärderna ska utgå från ett allriskperspektiv och säkerställa en nivå på säkerheten i nätverk och informationssystemen som är lämplig i förhållande till risken

Kraven förtydligas i 2 – 5 kapitlet i föreskrifterna, företrädesvis genom de organisatoriska säkerhetsåtgärderna som ställer krav på ett systematiskt och riskbaserat arbete med cybersäkerhet. Utöver att etablera ett systematiskt och riskbaserat arbete med cybersäkerhet finner verksamhetsutövaren stöd genom de krav som ställs på utformningen av organisatoriska, tekniska, driftrelaterade och fysiska säkerhetsåtgärder. Kraven på respektive säkerhetsåtgärd omhändertar, utifrån risk, samhällets behov av cybersäkerhet i sådan samhällsviktig verksamhet som verksamhetsutövarna bedriver. Föreskrifterna utgör minimikrav när det gäller utformningen av säkerhetsåtgärderna. Vissa föreskriftskrav är mer detaljerade än andra eftersom vissa säkerhetsåtgärder behöver utformas särskilt tydligt för att få avsedd effekt. En verksamhetsutövare behöver alltid göra en egen analys av om de egna behoven och de egna riskerna föranleder att en säkerhetsåtgärd behöver möta ännu högre behov av säkerhet än de krav som anges i föreskrifter och allmänna råd (2 - 5 kap.).

Säkerhetsåtgärderna ska enligt 2 kap. 3 § andra stycket p. 1 – 10 cybersäkerhetslagen åtminstone avse

1. strategier för riskanalys och för nätverk och informationssystemens säkerhet.

   Omhändertas i föreskrifter och allmänna råd främst genom kraven på verksamhetsutövaren avseende riskhantering (2 kap. 14 – 16 §§), informationsklassning (2 kap. 13 §), och omvärldsbevakning (2 kap. 12 §). Gällande strategier för nätverk och informationssystem ger föreskriften i sin helhet stöd för verksamhetsutövarens utformning av det arbetet.

2. incidenthantering,

   Omhändertas i föreskrifter och allmänna råd främst genom kraven på verksamhetsutövaren avseende incidenthantering (2 kap. 17 §), omvärldsbevakning (2 kap. 12 §), driftrelaterad dokumentation (3 kap. 7 – 10 §§) och säkerhetsloggning och logganalys (3 kap. 22 - 27 §§), robust och spårbar tid (3 kap. 28 §).

3. kontinuitetshantering och krishantering,

   Omhändertas i föreskrifter och allmänna råd främst genom kraven på verksamhetsutövaren avseende kontinuitetshantering (2 kap, 18 - 20 §§), krishantering (2 kap. 21 och 22 §§).

4. säkerhet i leveranskedjan,

   Omhändertas i föreskrifter och allmänna råd främst genom kraven på verksamhetsutövaren avseende förvärv, utveckling och underhåll av

system (3 kap. 1 - 6 §§), riskhantering (2 kap. 14-16 §,§, 3 kap. 3 §) och kontinuitetshantering (2 kap. 18 - 20 §§),

5. säkerhet vid förvärv, utveckling och underhåll av nätverk och informationssystem,

Omhändertas i föreskrifter och allmänna råd främst genom kraven på verksamhetsutövaren avseende förvärv, utveckling och underhåll av system (3 kap. 1 - 6 §§) och uppföljning och utvärdering (2 kap. 23 och 24 §§). Övriga krav i föreskriften är underlag för den kravställning som verksamhetsutövaren behöver ställa på säkerhetsåtgärder i den egna organisationen eller som krav på leverantör

6. strategier och förfaranden för att bedöma effektiviteten i säkerhetsåtgärderna,

Omhändertas i föreskrifter och allmänna råd främst genom kraven på verksamhetsutövaren avseende uppföljning och utvärdering (2 kap. 23 och 24 §§) och ledningens arbete med att övervaka genomförandet av säkerhetsåtgärder (2 kap. 8 §) och omvärldsbevakning (2 kap. 12 §).

7. grundläggande praxis för cyberhygien och utbildning i cybersäkerhet,

Omhändertas i föreskrifter och allmänna råd främst genom kraven på verksamhetsutövaren avseende personalsäkerhet rörande kunskap och kompetens (2 kap. 11 §).

8. strategier och förfaranden för användning av kryptografi samt, vid behov, kryptering,

Omhändertas i föreskrifter och allmänna råd främst genom kraven på verksamhetsutövaren avseende kryptering (3 kap. 30 – 33 §§).

9. personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning,

Omhändertas i föreskrifter och allmänna råd främst genom kraven på verksamhetsutövaren avseende personalsäkerhet (2 kap. 10 och 11 §§), segmentering och filtrering (3 kap. 11 – 14 §§), behörighetshantering och autentisering (3 kap. 15 – 21 §§), säkerhetsloggning och logganalys (3 kap. 22 – 27 §§), robust och spårbar tid (3 kap. 28 §), övervakning av system (3 kap. 38 och 39 §§) och driftrelaterad dokumentation (3 kap. 7-10 §§).

10. vid behov användning av lösningar för autentisering, säkrade kommunikationer och säkrade nödkommunikationssystem.

Omhändertas i föreskrifter och allmänna råd främst genom kraven på verksamhetsutövaren avseende behörighetshantering och autentisering (3 kap. 15 – 21 §§), krishantering (2 kap. 21 och 22 §§) och sektorsspecifika säkerhetsåtgärder för offentlig förvaltning (5 kap. 1 och 2 §§).

*Sektorsspecifika krav*

För vissa sektorer kan det finnas anledning att ställa ytterligare krav på säkerhetsåtgärderna de ska införa, exempelvis mot bakgrund av sektorernas uppgifter och samhällets beroende av deras tjänster.

Offentlig förvaltning har särskilda uppgifter i nationell krisberedskap. Dessa uppgifter förutsätter eller underlättas av tillgång till robusta system för kriskommunikation. Av denna anledning har särskilda sektorsspecifika krav riktats mot statliga myndigheter, regioner och kommuner.

### Uppgifter om vilka som berörs av regleringen

NIS2-direktivets tillämpningsområde följer av artikel 2. Av artikel 2 punkt 1 följer att direktivet är tillämpligt på offentliga eller privata entiteter av den typ som följer av bilaga 1 eller 2.

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

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

I artikel 2.1 anges att en verksamhet är av tillräcklig storlek om den minst kan betecknas som ett medelstort företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG.13. Ett 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 behöver enligt NIS2-direktivet inte uppfylla storlekskraven för att omfattas. 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.

Närmare stöd för att identifiera om en verksamhet omfattas av ovan punkt 1 – 3 ges i MSB:s föreskrifter om anmälan och identifiering (MSBFS 2025:XXX).

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

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

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

### Uppgifter om de bemyndiganden som myndighetens beslutanderätt grundar sig på

Cybersäkerhetslagen beslutas sannolikt i början av december 2025 och planeras att träda ikraft den 15 januari 2026. Cybersäkerhetsförordningen bedöms beslutas och träda ikraft i nära anslutning till dessa tidpunkter. Av detta följer att MSB vid tidpunkten för extern remiss i oktober 2025 ännu inte har något förordnande att utfärda föreskrifter om säkerhetsåtgärder och utbildning. Myndigheten har i avvaktan på ett sådant förordnande fått i uppdrag av regeringen att förbereda sådana föreskrifter inom ramen för implementeringen av NIS2-direktivet.[13] Samtidigt erhöll Post- och telestyrelsen (PTS) ett motsvarande regeringsuppdrag rörande förberedelser för föreskrifter.[14]

Regeringsuppdragen ger en bild av hur regeringen avser att fördela föreskriftsmandatet i cybersäkerhetsförordningen. Syftet med regeringsuppdraget är att skapa förutsättningar för att nödvändiga myndighetsföreskrifter träder ikraft i så nära anslutning till cybersäkerhetslagens och cybersäkerhetsförordningens ikraftträdande som möjligt. Extern remiss av MSB:s föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning sker som ett led i arbetet med att utföra nämnda regeringsuppdrag.

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

MSB förbereder därför föreskrifter om säkerhetsåtgärder och föreskrifter om utbildning för samtliga sektorer förutom de som ska omfattas av föreskrifter som ska utfärdas av PTS.

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

En alternativ lösning är att inte utfärda några föreskrifter alls. För och nackdelar med detta alternativ har redovisats i avsnittet om alternativa lösningar. Att inte utfärda några föreskrifter undanröjer inte behovet av att införa säkerhetsåtgärder med anledning av cybersäkerhetslagen. Kostnader för sådana säkerhetsåtgärder blir dock svårare att bedöma med hänsyn till att lagens krav är på en övergripande nivå vilket medför en otydlighet i vilka

[13] Uppdrag till Myndigheten för samhällsskydd och beredskap att förbereda genomförandet av NIS 2-direktivet (Fö2025/01293)
[14] Uppdrag till Post- och telestyrelsen att förbereda genomförandet av NIS 2-direktivet (Fi2025/01676)

investeringar som behöver göras och vad som ger tillräcklig effekt. Otydlighet kan medföra kostnader i samband med att säkerhetsåtgärder både utformas alltför omfattande eller så att de ger ett otillräckligt skydd. Tillgång till och efterlevnad av föreskrifternas krav bedöms minska risk för och konsekvenser av incidenter och tillbud vilket bidrar till minskade kostnader för verksamhetsutövarna.

Den absoluta majoriteten av verksamhetsutövarna som kommer att omfattas av cybersäkerhetslagen utgörs av organisationer som storleksmässigt minst uppfyller kraven på att utgöra ett medelstort företag, det vill säga sysselsätta minst 50 personer eller ha en årsomsättning och balansomslutning som överstiger 10 000 000 euro per år. Till detta kommer att verksamhetsutövarna troligen redan är väl insatta i tjänsternas betydelse för samhällets funktion. Detta gäller särskilt de som bedriver sådan verksamhet som bedöms som väsentlig i NIS2-direktivet. De flesta verksamhetsutövare bedöms därför redan, med hänsyn till sin storlek och den verksamhet de bedriver,

- arbeta med cybersäkerhet utifrån kända hot och identifierade risker
- redan, helt eller delvis, ha implementerat majoriteten av sådana säkerhetsåtgärder som det är allmänt vedertaget att en organisation ska ha och således även majoriteten av de säkerhetsåtgärder som regleras i föreskrifterna.

Regeringen konstaterar följande i propositionen.[15] ” Hur pass stora kostnader som uppstår för en enskild verksamhetsutövare med anledning av skyldigheten att bland annat vidta säkerhetsåtgärder påverkas också av verksamhetens art och omfattning samt antalet och kvaliteten på de system som används i verksamheten. Kostnaderna kan bli högre ju större och mer omfattande företagets verksamhet är. För ett mindre företag som använder endast några få system kan kostnaderna på grund av skyldigheterna enligt lagen bli begränsade. Å andra sidan kan även ett mindre företag drabbas av väsentliga kostnader, om dess affärsverksamhet har särdrag som innebär att verksamheten är förenad med särskilda risker. Det kommer att vara svårt att separera kostnaderna som är hänförliga till lagens införande från övriga kostnader med koppling till cybersäkerhet. Kostnaderna för cybersäkerhet kan inbegripa olika typer av utgifter som utrustning, programvara och datatrafikförbindelser. Andra kostnader som främjar cybersäkerhet kan vara administrativa utgifter, personalutgifter, olika kvalitetsrevisioner och utbildningar. Det kommer till exempel att vara svårt att bedöma vilka kostnader kopplade till systemens fysiska säkerhet som enbart är att hänföra till lagens införande jämfört med vad ett ändamålsenligt verksamhetsskydd rent generellt kräver.”

Idag är det 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.

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

Utöver kostnader för personal som är särskilt utsedd att samordna och leda säkerhetsarbetet måste även ledningen avsätta tid för cybersäkerhetsfrågor. Dessutom behövs personal som handlägger behörighetsadministration, övervakar brandväggar, uppdaterar virusskydd, följer upp säkerheten, tillhandahåller utbildningar med mera. Det är svårt att göra generellt giltiga uppskattningar om hur mycket resurser som krävs för arbetet med cybersäkerhet. En verksamhetsutövare som har utkontrakterat sin it-drift till en extern aktör där kostnader för delar av säkerheten är inkluderad i avtalet kan ha en annan fördelning av kostnaderna än verksamhetsutövare med interna digitala miljöer.

Syftet med konsekvensutredningen är inte att göra en samlad bedömning av kostnaderna för ett systematiskt och riskbaserat arbete med cybersäkerhet inklusive införandet av organisatoriska, tekniska, driftrelaterade och fysiska säkerhetsåtgärder. Istället handlar det om att identifiera vilka kostnader som tillkommer när verksamhetsutövaren ska efterleva föreskrifterna.

För att ge en så konkret bild som möjligt följer nedan en redogörelse för kostnadsuppskattning för säkerhetsåtgärder i respektive kapitel som kan komma att medföra ökade kostnader i form av teknik eller personal. Som stöd för beräkningarna har MSB anlitat externa konsulter som har beräknat den ungefärliga personalkostnaden av att införa och förvalta olika typer av säkerhetsåtgärder i en organisation samt ungefärlig kostnad för inköp/licenser för tekniska säkerhetsåtgärder. Redovisningen innehåller även en kostnadsbild för genomförandet av fysiska säkerhetsåtgärder. Med stöd av underlaget har sedan MSB uppskattat de tillkommande kostnader som följer av föreskriftskraven för en verksamhetsutövare med låg respektive högre mognadsnivå inom cybersäkerhetsområdet.

**2 kap Organisatoriska säkerhetsåtgärder**

Kraven i föreskrifter och allmänna råd när det gäller de organisatoriska säkerhetsåtgärderna kan medföra behov av att vidareutveckla och systematisera redan etablerat arbete med cybersäkerhet. Eftersom det systematiska och riskbaserade arbetet med cybersäkerhet ska integreras med verksamhetsutövarens befintliga sätt att leda och styra organisationen finns det sannolikt även synergier med existerande interna regler och arbetssätt som minskar både arbetsinsats och direkta kostnader. Detta gäller särskilt utformningen av det systematiska arbetet, ledning och styrning, personalsäkerhet, riskhantering, incidenthantering, kontinuitetshantering, krishantering samt uppföljning och utvärdering. När det gäller informationsklassning så utgör det, tillsammans med riskhantering, en förutsättning för att kunna ge information och system ett lämpligt och proportionerligt skydd. Mot denna bakgrund görs bedömningen att verksamhetsutövarna redan bedriver informationsklassning, formen för att värdera information kan givetvis skilja sig från det som ställs krav på genom föreskrifterna. Detsamma gäller omvärldsbevakning. Verksamhetsutövarna

bedöms redan bedriva omvärldsbevakning på något sätt men kraven i föreskrifterna kan komma att innebära ökade krav på struktur och innehåll.

Tillkommande kostnader för de organisatoriska säkerhetsåtgärderna är främst hänförliga till arbetstid för intern och extern personal för att se över och där så behövs uppdatera befintliga interna regler och arbetssätt för att säkerställa att de möter kraven i föreskrifter och allmänna råd. Det bedöms som mindre sannolikt att verksamhetsutövare ska behöva ta fram ett helt nytt regelverk även om det inte går att utesluta att det kan bli aktuellt att ta fram nya regler och arbetssätt på något enstaka område. Omfattningen av arbetet med de organisatoriska säkerhetsåtgärderna beror på vilken mognadsnivå verksamhetsutövaren ligger på när det gäller systematiskt och riskbaserat arbete med cybersäkerhet.

Även om en potentiellt låg mognadsnivå innebär ökade kostnader initialt är möjligheten att på sikt minska kostnader orsakade av incidenter större än för en verksamhetsutövare med ett redan väletablerat systematiskt och riskbaserat arbete. Tillgången till omfattande stöd för hur ett systematiskt och riskbaserat arbete med cybersäkerhet ska etableras och bedrivas bedöms minska kostnaderna. En grov uppskattning av på grund av föreskrifterna tillkommande kostnader för att se över och uppdatera interna regler och arbetssätt så att de möter föreskrifternas krav på organisatoriska säkerhetsåtgärder hos en verksamhetsutövare med låg mognadsgrad uppskattas motsvara kostnaden för tre årsarbetskrafter, för en verksamhetsutövare med högre mognadsgrad bör anpassningen inte motsvara mer än en årsarbetskraft. Verksamhetsutövarens storlek bedöms endast påverka kostnadsberäkningen marginellt men en komplex verksamhet kan behöva lägga mer resurser på att säkerställa efterlevnad av föreskrifterna. När de interna reglerna och arbetssätten för stärkt cybersäkerhet är på plats uppskattas kostnaderna för löpande förvaltning täckas av minskade utgifter för förluster i samband med incidenter.

Några av de organisatoriska säkerhetsåtgärderna bedöms föranleda kostnader som de flesta verksamhetsutövare inte tidigare haft. Det gäller kraven i 2 kap. 9 § på ledningens utbildning, 2 kap. 11 § ökade krav på egen och inhyrd personals kompetens där kompetensutvecklingsbehov inte tillgodoses löpande, 2 kap. 12 § utökad omvärldsbevakning, 2 kap. 15 § bedömning av risker med aggregerad och ackumulerad information, 2 kap 19 § krav på att öva återställning av sektorskritiska system.

*Ledningens utbildning*

Kostnaden består i att ta fram en utbildning utifrån föreskriftskraven som motsvarar ledningens behov i de fall en sådan saknas (40-100 timmar initialt och därtill utveckling av utbildning gällande säkerhetsåtgärder som ledningen uttrycker behov av fördjupning inom 40 timmar per område). Därtill kommer den tid ledningen behöver avsätta för att tillgodogöra sig innehållet i utbildningarna (8-20 timmar initialt och därefter 2-4 timmar per år).

*Kompetensutveckling*

Behovet av kompetenhöjande åtgärder varierar beroende på den informationsbehandling som behövs för verksamhetsutövarens verksamheter, antalet olika verksamheter och komplexiteten i verksamhetsutövarens digitala miljö. En introduktionsutbildning som ger alla medarbetare en grundläggande kunskap om hur de ska hantera verksamhetsutövarens information och system på ett säkert sätt bör redan vara en säkerhetsåtgärd som verksamhetsutövare bedriver. Initial utvecklingskostnad om grundläggande utbildning saknas bedömer vi till 40-100 timmar, översyn och uppdatering av materialet utifrån förändringar i verkamheten och i hotbild mot verksamheten, 20 timmar/år. Formatet på utbildningar kan anpassas till verksamheteutövarens behov. Från föreläsningar med möjlighet till frågor (2-6 timmar) till digitala verktyg som ger stöd i att skicka ut kortare utbildningar med en frekvens som är anpassad till arbetsbelasningen. (15 minuter 10-40 ggr per år). Därtill kommer specifik utbildning för användargrupper som behandlar information där extra kunskap behövs för att skydda informationen eller de system som används.

De utbildningar som tekniker med ansvar för olika system behöver för att hålla sig uppdaterad kring säkerhetsfunktioner varierar beroende på system. Det är inte orimligt att en tekniker behöver avsätta 20-40 timmar per år för att hålla sig uppdaterad.

*Omvärldsbevakning*

Kostnaden för omvärldsbevakning ligger i att utifrån verksamhetutövarens behov värdera den information som källorna i föreskrifterna ställer krav på att bevaka. Vissa av källor tillhandahåller information av betydelse för verksamhetsutövarens strategiska arbete med cybersäkerhet och andra information om sårbarheter där verksamhetutövaren skyndsamt behöver agera för att minska risken för angrepp. Beroende på omfattning och komplexitet i verksamheten uppskattas tiden som bör avsättas för den ytterligare omvärldsbevakning som följer av föreskrifternas krav, exempelvis att löpande bevaka och omhänderta information från det nationella cybersäkerhetscentret och cyberkrishanteringsmyndigheten, variera från 0,5 – 10 timmar per vecka.

*Bedöma risker med aggregerad och ackumelerad information*

Bedömningen är att de flesta verksamhetsutövare inte genomför den här typen av bedömningar i tillräcklig omfattning idag. Här tillkommer därför en kostnad under arbetet med riskanalyser för att identifiera vilken annan information som tillsammans med den informationsbehandling som riskerna bedöms för genererar ytterligare risk (tillägg per riskanalys i tid 0,5 - 3 timmar). Också risken med att behandla en stor mängd av den information som riskanalysen avser behöver bedömas (tillägg per riskanalys 0,2 – 1 timme).

*Öva återställning av sektorskritiska system*

Kostnaden består i att planera och genomföra övningar där de sektorskritiska systemen återställs utifrån scenarier där omfattningen av återställningen varierar. Komplexare digitala miljöer är, högre antal olika sektorskritiska

system och större omfattning av den återställning som ska övas (tex enbart återläsning av data eller återställning av hela systemet från grunden) kräver mer planering (8-40 timmar) och genomförandet av återställningen tar mer resurser. Att öva återställning av ett sektorskritiskt system kan ta ett par timmar för en person (8 arbetstimmar) upp till flera timmar för flera personer (200 arbetstimmar och mer).

### 3 kap Tekniska och driftrelaterade säkerhetsåtgärder

Verksamhetsutövarna som omfattas av cybersäkerhetslagen tillhandahåller sina tjänster i ett digitaliserat samhälle och behöver förhålla sig till olika typer av cyberhot. Även om utformning och omfattning kan skilja sig är det i praktiken idag inte möjligt att bedriva sådan verksamhet som omfattas av NIS 2-direktivet utan att ha skyddat sina system med säkerhetsåtgärder som segmentering, säkerhetsloggning, kryptering, säkerhetskopiering med flera.

Kraven i föreskrifter och allmänna råd kan medföra behov av att vidareutveckla och systematisera verksamhetsutövarens redan etablerade interna regler och arbetssätt som används för utformning och drift av de olika tekniska och driftrelaterade säkerhetsåtgärderna. Till detta kan kostnader tillkomma för att täcka behov av ny eller uppdaterad teknisk utrustning.

Bedömningen av tillkommande kostnader som följer av föreskrifternas krav utgår från antagandet att verksamhetsutövarna inte bara har mer eller mindre heltäckande interna regler och arbetssätt för de tekniska och driftrelaterade säkerhetskraven i föreskrifterna utan även det mesta av nödvändig teknik på plats. Föreskrifterna ställer inte krav på användningen av en specifik teknisk produkt utan på funktionalitet som kan omhändertas med olika tekniska lösningar.

Kostnaderna för de tekniska och driftrelaterade säkerhetsåtgärderna är liksom för de organisatoriska säkerhetsåtgärderna för de flesta verksamhetsutövare främst hänförliga till arbetstid för intern och extern personal för att se över och där så behövs uppdatera befintliga interna regler och arbetssätt för att säkerställa att de möter kraven i föreskrifter och allmänna råd. Detta gäller särskilt kraven på

- förvärv, utveckling och underhåll av system,
- driftrelaterad dokumentation,
- behörighetshantering och autentisering,
- säkerhetsloggning och logganalys,
- kryptering,
- säkerhetskonfigurering,
- säkerhetstester,
- säkerhetskopiering, och

- ändringshantering.

Omfattningen av det arbete som en verksamhetsutövare behöver göra för att uppfylla föreskrifternas krav på tekniska och driftrelaterade säkerhetsåtgärder beror även här på mognadsgraden. Att en lägre mognadsnivå innebär ökade kostnader initialt kompenseras med en större möjlighet att på sikt minska kostnader orsakade av incidenter. En grov uppskattning av tillkommande kostnader för att se över och uppdatera interna regler och arbetssätt så att de möter föreskrifternas krav på de tekniska och driftrelaterade säkerhetsåtgärderna hos en verksamhetsutövare med låg mognadsgrad uppskattas motsvara kostnaden för två årsarbetskrafter, för en verksamhetsutövare med högre mognadsgrad bör anpassningen inte motsvara mer än en årsarbetskraft. Verksamhetsutövarens storlek bedöms endast påverka kostnadsberäkningen marginellt men en komplex verksamhet kan behöva lägga mer resurser på att säkerställa efterlevnad av föreskrifterna. När de interna reglerna och arbetssätten för stärkt cybersäkerhet är på plats uppskattas kostnaderna för löpande förvaltning täckas av minskade utgifter för förluster i samband med incidenter och med den effektivisering av arbetet som ett systematiskt arbete ger. Den relativt sett lägre kostnaden för att få interna regler och arbetssätt på plats avseende de tekniska och driftrelaterade säkerhetsåtgärderna jämfört med de organisatoriska säkerhetsåtgärderna har sin bakgrund i bedömningen att verksamhetsutövarna i större utsträckning förutsätts utföra de tekniska och driftrelaterade säkerhetsåtgärderna på ett sådant sätt som beskrivs i föreskrifterna. Detta har bland annat sin bakgrund i att många organisationer delegerat arbetet med it-säkerhet till it-avdelningen som i sin tur ofta riktat sitt initiala fokus i säkerhetsarbetet på att få olika tekniska och driftrelaterade säkerhetslösningar på plats, såsom intrångsdetektering, kryptering och behörighetshanteringssystem.

Föreskrifternas tekniska och driftrelaterade säkerhetsåtgärder ställer som nämndes ovan även krav på den tekniska miljön och i vissa fall innebär det att det behövs tekniskt stöd för att kunna införa vissa säkerhetsåtgärder. Funktionaliteten kan i vissa fall uppnås med både kostnadsfria open source lösningar och kommersiella lösningar. Det är svårt att uppskatta kostnaderna eftersom licenskostnader ofta beräknas på antalet system eller motsvarande. Det är också vanligt att priserna för licenser för olika system vägs samman och leverantören ger ett gemensamt pris för flera olika system och säkerhetsfunktioner.

De föreskriftskrav som bedöms kunna medföra mest tillkommande kostnader för verksamhetsutövarna som helt eller i stor utsträckning saknar genomtänkta och tidsenliga säkerhetsåtgärder är reglerna om segmentering och filtrering, säkerhetsloggning och logganalys, robust och spårbar tid, säkerhetstester, säkerhetskopiering, övervakning av system samt ändringshantering.

*Segmentering och filtrering*

Kraven på segmentering är omfattande men ger också en förutsättning att minska konsekvenserna av incidenter genom att minska spridningen av skadlig kod mellan olika segment. Att helt förändra en nätverksarkitektur så att den bättre skyddar mot hot, kan byggas ut och klara framtida krav kan vara ett omfattande arbete. Behövs nya centrala brandväggar för att upprätthålla skyddet i vissa segment är kostnaden för en sådan 20 - 60tkr. Vissa verksamheter med höga krav på tillgänglighet och robusthet i sin it-miljö kan behöva mer avancerade brandväggar där en kostnad på flera hundra tusen kronor inte är ovanligt. De flesta system har inbyggda funktioner för att filtera sin trafik. Här består kostnaden i att identfiera verksamhetens behov av trafik och blockera resterande – en kostnad som inkluderas i arbetet med att ta fram och sätta upp systemets säkerhetskonfiguration.

*Säkerhetsloggning och logganalys*

Kraven i föreskrifterna på vad som ska loggas och när kan innebära att verksamhetsutövaren behöver komplettera existerande arbete med säkerhetsloggning och logganalys med ytterligare systemlösningar för att kunna logga rätt händelser, jämföra loggar och utreda problem. Det tillkommande arbetet kan göras per system men för större organisationer där behovet av loggning av användarhändelser och systemhändelser som indikerar tillbud eller incidenter behöver loggar från flera olika system sammanställas för att därefter kunna jämföras. Licenskostnaden för en sådan central lösning som avses i föreskrifternas allmänna råd bedöms uppgå till mellan 150- 500tkr per år.

*Robust och spårbar tid*

Eventuellt tillkommande kostnad när det gäller robust och spårbar tid är främst hänförlig till intern distribution av tiden. En investering i att ändra tidskälla för att få en mer stabil och korrekt tidskälla uppskattas kosta mellan 30 - 200tkr.

*Säkerhetstester*

Bedömningen är att verksamhetsutövaren inte genomför säkerhetstester i tillräckligt stor utsträckning. Säkerhetstester kan genomföras både med verktygsstöd och manuellt. Syftet är att kontrollera att system har den säkerhetskonfiguration som verksamhetsutövaren fastställt. Kostnaderna härrör sig till licenser ( 5 – 100 tkr/år) för verktyg för att verifiera säkerhetskonfigurationer och för att skanna det egna nätverket efter kända sårbarheter. Manuella tester kräver utbildad personal och tar ofta tid att planera och genomföra. Behovet av manuella tester där säkerhetstestaren aktivt, med stöd av olika verktyg, undersöker nätverket för att identifiera sårbarheter genomförs mer sällan och ofta för ett begränsat system men kan vara nödvändiga för att uppfylla föreskrifternas krav.

*Säkerhetskopiering*

Säkerhetskopiering av verksamhetsutövarens information behöver ske utifrån verksamhetsutövarens behov. Att genomföra säkerhetskopiering är en del av varje organisations cybersäkerhetsarbete. Detta medför att programvara för säkerhetskopiering redan finns och tillkommande kostnader utifrån föreskriftskraven är kopplade till verksamhetsutövarens eventuella behov av ytterligare tekniska stödsystem för att skapa och spara säkerhetskopior.

*Övervakning av system*

Kostnaden för övervakningssystem består av licenskostnader för system som sammanställer händelser (80-150 tkr/år) och personalkostnader för att sätta larmgränser och omhänderta händelser där larm utlösts.

Enligt föreskrifterna ska verksamhetsutövaren identifiera och hantera behovet av realtidsövervakning. I händelse av verksamhetsutövaren inte har någon realtidsövervakning tidigare och att ett sådant behov ändå identifieras tillkommer kostnader för extra bemanning för att anlysera behovet av att agera och att personal finns som kan hantera problemet.

*Ändringshantering*

Bedömningen är att verksamhetsutövare genomför ändringshantering men att det inte sällan brister vad gäller systematik och riskhantering. Tillkommande kostnader på grund av föreskrifternas krav består i att förbättra arbetet med att förbereda och planera ändringar så att inte incidenter inträffar. Berörda roller behöver genomföra riskanalys och planera hur ändringen ska genomföras för att minska identifierade risker. Beroende på komplexiteten i systemet varierar kostnaden mellan 0,5 - 20 timmar. Kostnaden för att genomföra ändringen beror också på hur komplex ändringen är.

**4 kap Fysiska säkerhetsåtgärder**

För att förhindra skador på och obehörig åtkomst till it-utrustning, räcker inte organisatoriska, tekniska eller driftrelaterade säkerhetsåtgärder. Ett adekvat skydd förutsätter även fysiska säkerhetsåtgärder. Utgångspunkten är därför att verksamhetsutövaren har ett fysiskt skydd för både lokaler och system. Till detta kommer behovet av att skydda systemen från störningar på grund av avbrott i tekniska försörjningssystem. Vikten av fysiska säkerhetsåtgärder betonas i NIS2-direktivet. [16]

Kraven i föreskrifterna på fysiska säkerhetsåtgärder uppfylls i mindre utsträckning genom justering eller vidareutveckling av verksamhetsutövarens interna regler och arbetssätt. I det fall verksamhetsutövaren inte redan har ett skalskydd för sina lokaler, inte har delat in lokalerna i sektioner samt saknar tillgång till särskilda it-utrymmen och tekniska försörjningssystem med tillräcklig funktion och redundans kan kostnaderna för att uppfylla föreskrifterns krav på fysiska säkerhetsåtgärder bli påtagliga. Bedömningen är dock att majoriteten av verksamhetsutövarna redan, med hänsyn till sin storlek

[16] NIS2-direktivet skäl 79

och den verksamhet de bedriver, redan har uppfyllt stora delar av föreskrifternas krav på fysiska säkerhetsåtgärder.

De krav som bedöms som potentiellt mest kostnadsdrivande på grund av att det är dyrt att få på plats och att många verksamhetsutövare bedöms sannolikt ännu inte uppfylla kraven fullt ut är kraven på att dela in sina lokaler i fysiskt separerade sektioner, säkerställa tillgång till särskilda it-utrymmen med övervakning och larm samt tillräcklig funktion och redundans gällande tekniska försörjningssystem.

*Dela in sina lokaler i fysiskt separerade sektioner*

Det är svårt att uppskatta i vilken omfattning verksamhetsutövarna inte redan delar in sina lokaler i fysiskt separerade sektioner utifrån informationsklassning och riskbedömning. Kravet ställs för att skydda informationsbehandlingen mot att obehöriga får åtkomst till information genom överhörning eller genom att kunna se informationen som behandlas, ska behandlas eller har behandlats i verksamhetuövarens system. Kostnaden för att sätta upp skärmar, bygga rum eller på annat sätt skapa avskilda utrymmen med det skydd som informationsbehandligen kräver beräknas ca 5 - 10 tkr för skärmavskiljare och mellan 10 - 40 tkr per kvadratmeter yta för rum bereonde på behovet av ljudisolering.

*Säkerställa tillgång till särskilda it-utrymmen med övervakning och larm*

Liksom rörande bedömningen om i vilken omfattning verksamhetsutövarna inte redan delar in sina lokaler i fysiskt separerade sektioner är det också svårt att uppskatta om verksamhetsutövarna redan uppfyller föreskrifternas krav på att ha en tillräcklig tillgång till särskilda it-utrymmen med larm och övervakning. De utrymmen där verksamhetutövarens servrar finns behöver skyddas mot direkt åtkomst. Kostnaden för rörelsedetektorer med larmfunktion uppskattas till 10 tkr per detektor. Kodlås med larm uppgår till ca 60 tkr per dörr.

Kostnaden för ett särskilt it-utrymme i form av låst skåp uppskattas till mellan 50- 500tkr beroende på låsfunktion, ventilation och hur väl skåpet skyddar mot avlyssning. För större särskilda it-utrymmen som utrustas med larm, klimatanläggning, brandskydd som inte skadar system är kostnaden att från grunden bygga ett sådant rum (serverhall) 60- 100tkr per kvadratmeter. Föreskrifterna ger verksamhetsutövarna utrymme att utforma det fysiska skyddet utifrån sin bedömning av vilken lösning som är lämpligast. Föreskrifterna ställer inte några krav på att verksamhetsutövarna ska bygga serverhallar.

*Tillräcklig funktion och redundans gällande tekniska försörjningssystem.*

Bedömningen är att de flesta verksamhetsutövare har till stor del hanterat det behov av tillräcklig funktion och redundans gällande tekniska försörjningssystem som beskrivs i föreskrifterna. Behovet av redundans kan lösas på olika sätt, exempelvis genom extra kabeldragning, kontrakt med

ytterligare en leverantör av kommunikationsinfrastruktur eller möjlighet att hyra in elgeneratorer och ventilationssystem om det egna går sönder och reparation tar längre tid.

Redundans för kortare störningar i elförsörjningen löser de flesta med UPS (uninterruptable power supply). Kostnaden för sådan utrustning 30 - 500t kr är beroende av hur många system som behöver hållas igång och under hur lång tid.

**5 kap Sektorsspecifika säkerhetsåtgärder**

*Offentlig förvaltning*

Det är av vikt att ha tillgång till en robust förmåga till kommunikation under en kris eller i övrigt ansträngda förhållanden. Tillkommande kostnader bedöms vara förhållandevis begränsade.

**Intäkter**

Förslaget bedöms inte generera intäkter för staten, kommuner, regioner, företag och andra enskilda men kan däremot minska kostnader orsakade av incidenter.

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

Regleringen utgör en del av implementering av NIS2-direktivet och bedöms överensstämma med de skyldigheter som följer av Sveriges anslutning till Europeiska unionen.

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

Lag och förordning planeras att träda ikraft den 15 januari 2026. Eftersom föreskrifterna har som syfte att stödja verksamhetsutövarna genom att konkretisera kraven i lag och förordning och därmed göra det enklare att efterleva dessa behöver föreskrifterna träda ikraft i så nära anslutning som möjligt till detta datum. Med hänsyn till remissförfarande och beredning bedöms föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning tidigast kunna träda ikraft i mitten eller slutet av mars 2026.

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

MSB bedömer att det finns behov av att genomföra särskilda informationsinsatser inför och i samband med att regleringen börjar gälla. Insatserna bör genomföras i samverkan med berörda tillsynsmyndigheter.

Syftet med informationsinsatserna är att säkerställa att verksamhetsutövarna får en god bild av sina skyldigheter och rättigheter enligt den nya regleringen. Det är också angeläget att det finns tillgång till relevant stöd i form av vägledningar i samband med att föreskrifterna börjar gälla samt att verksamhetsutövarna ges kunskap om både föreskrifter och stöd.

## Företag

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

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

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

Det är endast möjligt att ge en grov uppskattning av hur många verksamhetsutövare som tillkommer med stöd av föreskrifterna om anmälan och identifiering. Sannolikt handlar det inte om fler än 50 och majoriteten inom avloppsvattenshantering och dricksvattenförsörjning.

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

Givet att nödvändiga vägledningar och systemstöd finns att tillgå bedöms föreskrifterna och de allmänna råden om säkerhetsåtgärder och utbildning innebära begränsat ökade administrativa kostnader för företagen i samband med arbetet att etablera de interna regler och arbetssätt som krävs enligt föreskrifterna. Bedömningen är dock att det systematiska och riskbaserade arbetet även kan bidra till minskade kostnader genom att minska risken för kostsamma incidenter.

### 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

Tillkommande kostnader redovisas närmare i avsnittet ovan om vilka kostnadsmässiga och andra konsekvenser regleringen medför och en jämförelse av konsekvenserna för de övervägda regleringsalternativen.

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

Med hänsyn till att NIS2-direktivet kommer att gälla samma typer av företag i hela unionen bedömer MSB att regleringen inte kommer att påverka konkurrensförhållanden.

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

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

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

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

## Kommuner och landsting

Föreskrifterna bedöms i stort inte innebära några förändringar av kommunala befogenheter eller skyldigheter eller påverka grunderna för kommuners eller regioners organisation eller verksamhetsformer. Ett undantag är i det fall föreskrifternas krav på kommunernas lokaler innebär behov av mindre ombyggnationer. En anpassning av lokalerna ska dock alltid ske i syfte att åtgärda ett bristfälligt skydd för information och system som hanteras i lokalerna. Det bedöms därför stärka kommunens möjlighet att utföra sin lagstadgade verksamhet på ett effektivt och rättsäkert sätt.

## Kontaktpersoner

### Ange vem som kan kontaktas vid eventuella frågor

*Tove Wätterstam eller Helena Andersson*