Myndigheten för civilt försvar

Konsekvensutredning

Datum	Ärendenummer
2026-04-29	MCF 2026-04554

Remissversion: Konsekvensutredning rörande Myndigheten för civilt försvars föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning

1. 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.

2. 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 således försenade med sin implementering. EU-kommissionen har betonat betydelsen av att medlemsstaterna implementerar NIS2-direktivet så snart som möjligt.

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, finansmarknads-infrastruktur, 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) i NIS2-direktivet konstateras att medlemsstaterna fick stort utrymme för nationella val vid implementeringen av NIS-direktivet. Det innebar 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 har skärpts och förtydligats.

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.

Av artikel 21.1 i NIS2-direktivet framgår bland annat att säkerhetsåtgärderna ska baseras på en allriskansats. Denna ansats ska skydda både nätverk och informationssystem samt deras fysiska miljö från incidenter.

NIS2-direktivet har implementerats i svensk rätt genom cybersäkerhetslagen (2025:1506) och cybersäkerhetsförordningen (2025:1507) samt genom tillhörande myndighetsföreskrifter. Till skillnad från den tidigare NIS-regleringen gäller cybersäkerhetslagen hela verksamheten hos berörda organisationer, inte enbart säkerheten i de nätverk och informationssystem som används för den samhällsviktiga eller digitala tjänsten.

De som omfattas av regleringen benämns i NIS2-direktivet väsentliga eller viktiga entiteter och i cybersäkerhetslagen väsentliga eller viktiga verksamhetsutövare.

Nedan följer en genomgång av cybersäkerhetslagen i tillämpliga delar samt en fördjupning i ett antal för föreskrifterna centrala utgångspunkter. I avsnitt 3 följer en närmare redovisning rörande hur föreskrifterna om säkerhetsåtgärder och utbildning ska tillgodose cybersäkerhetslagens krav på säkerhetsåtgärder och utbildning.

2.1 Cybersäkerhetslagen

Direktivets krav på säkerhetsåtgärder i artikel 21.2 i NIS2-direktivet införs i svensk rätt genom 2 kap. 3 § cybersäkerhetslagen. De åtgärder som listas 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 p. 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.

Av 2 kap. 3 § cybersäkerhetslagen framgår att verksamhetsutövare ska vidta lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att skydda nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och systemens fysiska miljö mot incidenter (säkerhetsåtgärder), att säkerhetsåtgärderna ska utgå från ett allriskperspektiv och säkerställa en nivå på säkerheten i nätverks- och informationssystemen som är lämplig i förhållande till risken, samt att de åtminstone ska avse:

1. strategier för riskanalys och för nätverks- och informationssystemens säkerhet,
2. incidenthantering,

3. kontinuitetshantering och krishantering,
4. säkerhet i leveranskedjan,
5. säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem,
6. strategier och förfaranden för att bedöma effektiviteten i säkerhetsåtgärderna,
7. grundläggande praxis för cyberhygien och utbildning i cybersäkerhet,
8. strategier och förfaranden för användning av kryptografi samt, vid behov, kryptering,
9. personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning, och
10. vid behov användning av lösningar för säkrade kommunikationer och säkrade nödkommunikationssystem.

Vidare framgår i 2 kap. 4 § cybersäkerhetslagen att de personer som ingår i ledningen för en verksamhetsutövare ska genomgå utbildning om säkerhetsåtgärder.

2.2 Föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning

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. Vägledning kommer att tas fram som ytterligare stöd för tillämpningen av föreskriftskraven. Föreskrifterna och tillhörande vägledning syftar till att förtydliga cybersäkerhetslagens krav och ge stöd för verksamhetsutövarnas val och utformning av säkerhetsåtgärder. Målet är att uppnå hög cybersäkerhet i samhället som svarar mot Sveriges behov och uppfyller EU:s krav.

Eftersom NIS2-direktivet, precis som det första NIS-direktivet, är ett minimidirektiv så har Sverige precis som andra medlemsstater möjlighet att, om så önskas, ställa högre krav än vad EU kräver. Av lagen framgår, precis som i NIS2-direktivet, att uppräkningen av säkerhetsåtgärder inte är uttömmande. Ledning för hur EU har bedömt behovet av att konkretisera kraven på säkerhetsåtgärder ytterligare kan hämtas från EU-kommissionens genomförandeförordning (EU) 2024/2690 av den 17 oktober 2024 om fastställande av regler för tillämpningen av direktiv (EU) 2022/2555 vad gäller *tekniska och metodologiska specifikationer för riskhanteringsåtgärder för cybersäkerhet och närmare angivelse av i vilka fall en incident ska anses vara betydande med avseende på leverantörer av DNS-tjänster, registreringsenheter för*

toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av utlokaliserade driftstjänster, leverantörer av utlokaliserade säkerhetstjänster, leverantörer av marknadsplatser online, leverantörer av sökmotorer, leverantörer av plattformar för sociala nätverkstjänster och tillhandahållare av betrodda tjänster (fortsättningsvis benämnd genomförandeförordningen). I bilagan till genomförandeförordningen ställs en rad förhållandevis detaljerade krav som konkretiserar och kompletterar direktivets skrivningar om säkerhetsåtgärder. Genomförandeförordningen gäller direkt i medlemsstaterna rörande kraven på de omnämnda verksamhetsutövarna vad gäller vilka incidenter som är rapporteringspliktiga och utformningen av säkerhetsåtgärder. Skälet till att dessa omfattas av direkta krav från EU istället för av motsvarande nationell reglering är att deras verksamhet är av en särskild gränsöverskridande karaktär. EU-kommissionen har mandat enligt artikel 21 p. 5 st. 2 i NIS2-direktivet att utfärda genomförandeförordningar även för andra sektorer men har hittills valt att inte göra detta.

Även i den svenska implementeringen av NIS2-direktivet förtydligas som nämnts att uppräkningen av säkerhetsåtgärder i 2 kap. 3 § cybersäkerhetslagen inte är uttömmande när verksamhetsutövaren ska vidta lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att skydda nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och systemens fysiska miljö mot incidenter (säkerhetsåtgärder). Behovet av att närmare konkretisera och komplettera skrivningarna omhändertas genom att ett bemyndigande i 2 kap. 14 § cybersäkerhetslagen om att bland annat meddela ytterligare föreskrifter om säkerhetsåtgärder enligt 2 kap. 3 § samt meddela föreskrifter om utbildning enligt 2 kap. 4 §.

I propositionen konkretiserar regeringen regleringens syfte på följande sätt:[1]

Sveriges cybersäkerhet påverkas av ett antal sårbarheter som kan ha olika ursprung och manifestera sig inom ett antal områden. Dessa sårbarheter kan samlat eller var för sig utgöra strategiska sårbarheter i ett digitaliserat samhälles cybersäkerhetslandskap och riskera att påverka samhällsviktig verksamhet och ytterst Sveriges säkerhet. Den lag som genomför NIS 2-direktivet i Sverige måste ta sin utgångspunkt i denna hotbild och dessa utmaningar. Även om regelverket som genomför NIS 2-direktivet delvis tar sin utgångspunkt i nationella behov kommer det i förlängningen också att bidra till att främja den inre marknaden.

[1] Prop. 2025/26:28 s. 37

2.3 Cybersäkerhet och Sveriges säkerhet

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 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]

2.4 Begreppet cybersäkerhet

Terminologin på informations- och cybersäkerhetsområdet är under utveckling. I 1 kap. 2 § p. 5 cybersäkerhetslagen definieras *cybersäkerhet* som all verksamhet som

[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
[3] Utgångspunkter för totalförsvaret 2025–2030 s. 2.
[4] Utgångspunkter för totalförsvaret 2025–2030 s. 39.

är nödvändig för att skydda nätverk och informationssystem, användare av dessa system och andra berörda personer mot cyberhot.

Med *cyberhot* avses enligt 1 kap. 2 § p. 4 cybersäkerhetslagen 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 har fastslagits av EU innebär istället att cybersäkerhet har fått en innebörd som i stort kan likställas med det som traditionellt beskrivs som informationssäkerhet. Detta understryks även i propositionen där det framgår att regeringen gör bedömningen att uttrycket informationssäkerhet inte tillför något i sak i förhållande till uttrycket cybersäkerhet och att lagen därför bör kallas cybersäkerhetslag, och inte som några remissinstanser föreslår, även inkludera informationssäkerhet i namnet.[6]

Eftersom det kan finnas olika uppfattningar om vad cybersäkerhet innebär, behöver föreskrifterna med tillhörande vägledning bidra till en gemensam förståelse för begreppet cybersäkerhet i enlighet med EU:s legalt fastslagna definition.

2.5 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[7] att kravet på att bedriva ett systematiskt och riskbaserat arbete redan bedöms följa av säkerhetskraven som ställs på verksamhetsutövarna enligt artikel 21 p. 1 i NIS2-direktivet och 2 kap. 3 § cybersäkerhetslagen. Införandet av ett separat krav skulle därför enligt regeringen innebära dubbelreglering eftersom det är ett är en sådan riskhanteringsåtgärd som avses i artikel 21 i NIS 2-direktivet. Föreskrifterna och de allmänna råden samt därtill hörande

[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).
[6] Prop. 2025/26:28 s. 38 ff.
[7] Prop. 2025/26:28 s. 85 med hänvisning till redovisning av remissynpunkt från PTS med flera på s 83.

vägledning behöver därför förtydliga att ett systematiskt och riskbaserat cybersäkerhetsarbete i sig utgör en säkerhetsåtgärd.

2.6 Ledningens ansvar för att godkänna och övervaka säkerhetsåtgärderna

I ett systematiskt och riskbaserat arbete med cybersäkerhet har ledningen en central roll för att arbetet ska kunna bedrivas på avsett sätt. Det kan samtidigt noteras att brister avseende ledningens engagemang i arbetet utgör en sedan länge och ofta påtalad utmaning för, och anledning till, organisationers möjlighet att bedriva ett systematiskt och riskbaserats cybersäkerhetsarbete och därmed ges möjlighet att uppnå en ändamålsenlig cybersäkerhet.[8]

Ledningens betydelse kommer till uttryck både i NIS2-direktivet gällande *att* de har vissa uppgifter och i genomförandeförordningen, närmare om *hur* de säkerhetsåtgärder som involverar ledningen ska utformas.

I artikel 20 p. 1 i NIS2-direktivet tydliggörs att medlemsstaterna *ska säkerställa att väsentliga och viktiga entiteters ledningsorgan godkänner de riskhanteringsåtgärder för cybersäkerhet som dessa entiteter vidtar för att följa artikel 21, övervakar genomförandet av dem och kan ställas till svars för entiteternas överträdelser av den artikeln.* Kraven i artikel 20 har inte någon motsvarighet i cybersäkerhetslagen och av lagens förarbeten framgår att regeringen, bland annat efter referenser till aktiebolagslagen (2005:551), myndighetsförordningen (2007:515) och kommunallagen (2017:725), bedömde att ledningen i enskilda och offentliga verksamhetsutövare ansvarar för att godkänna säkerhetsåtgärder och övervaka genomförandet av dem på sätt som framgår av artikel 20 i direktivet utan särskild reglering och att direktivets krav i denna del därför inte behövde regleras i lagen.[9] Det kan antas att en anledning till att det bedömdes som nödvändigt att i NIS2-direktivet konkretisera att ledningen hos väsentliga och viktiga verksamhetsutövare har ett ansvar för att godkänna och övervaka säkerhetsåtgärder var att det inte var självklart att samtliga medlems-staters nationella reglering redan innefattade ett sådant ansvar. En annan anledning kan utläsas av skäl (137) enligt vilket det framgår att direktivet *bör syfta till att säkerställa en hög ansvarsnivå för riskhanteringsåtgärder för cybersäkerhet och rapporterings-skyldigheter för väsentliga och viktiga entiteter. Därför bör ledningsorganen för väsentliga och viktiga entiteter godkänna riskåtgärderna för cybersäkerhet och övervaka deras genomförande.*

[8] Utmaningarna kring ledningens engagemang utgör exempelvis en återkommande observation i Cybersäkerhetskollen, den mätning som Myndigheten för civilt försvar genomför minst vartannat år. https://rib.msb.se/filer/pdf/31260.pdf Se exempelvis rekommendationer till offentlig förvaltning s. 22.
[9] Prop. 2025/26:28 s 99.

Frågan är då i vilken utsträckning det finns utrymme att i föreskrifter om säkerhetsåtgärder närmare konkretisera hur det ansvar för säkerhetsåtgärder som ledningen har enligt artikel 20 p.1 i NIS2-direktivet respektive aktiebolagslagen, myndighetsförordningen och kommunallagen.

EU-kommissions uppfattning om vad de olika säkerhetsåtgärderna i artikel 21 i NIS2-direktivet, till vilken artikel 20 p. 1 hänvisar, innebär och hur de ska utformas kommer till uttryck i genomförandeförordningen[10]. Där konkretiseras bland annat hur den säkerhetsstrategi som de berörda entiteterna ska ta fram för att implementera artikel 21 p. 2 a) i NIS2-direktivet ska utformas. Av bilagan i förordningen, p.1.1.1, framgår att strategin bland annat ska fastställa mål för arbetet, fastställa roller och ansvarsområden, omfatta ett åtagande om att tillhandahålla tillräckliga resurser, omfatta indikatorer och åtgärder för att övervaka genomförandet och aktuell mognadsnivå hos de berörda entiteterna samt innehålla information om vilket datum som strategin formellt godkändes av de berörda entiteternas ledningsorgan. Ledningsorganens närmare uppgifter vad gäller säkerhetsåtgärderna konkretiseras i genomförandeförordningen även inom ramen för riskhantering p. 2.1.1, övervakning av efterlevnad p. 2.2.1 och 2.2.2, oberoende granskning av nätverks- och informationssäkerhet 2.3.3, cyberhygien och utbildning p. 8.1.1 och 8.1.2 samt personalsäkerhet p. 10.1.2.

Sammantaget kan konstateras att ledningens ansvar och uppgifter beskrivs på två olika nivåer.

- En *övergripande nivå* i artikel 20 p.1, med sin hänvisning till artikel 21, i NIS2-direktivet respektive vad som följer av aktiebolagslagen, myndighetsförordningen och kommunallagen.
- En *detaljerad nivå* i genomförandeförordningen kopplad till utformningen av respektive säkerhetsåtgärd som ska vidtas enligt artikel 21 i NIS2-direktivet och cybersäkerhetslagen 2 kap. 3 §.

Som ovan nämnts har ledningen en ofta avgörande roll för möjligheten att arbeta med cybersäkerhet på ett systematiskt och riskbaserat sätt. Det går inte att utesluta att EU-kommissionens möjlighet att på ett tydligt sätt i genomförande-förordningen konkretisera ledningens uppgifter avseende säkerhetsåtgärder stärktes genom förtydligandet av ledningens ansvar i artikel 20 p. 1 NIS2-direktivet. Motsvarande förtydligande finns, som ovan nämnts, inte i cybersäker-hetslagen men som regeringen uttalar i förarbetena är detta inte för att ett ansvar för ledningen att godkänna och övervaka säkerhetsåtgärder inte ska finnas i

[10] Mandatet att utfärda en genomförandeförordning avseende säkerhetsåtgärder följer av artikel 21 p. 5 i NIS2-direktivet.

Sverige utan för att motsvarande ansvar redan följer av annan lagstiftning. En sammantagen bedömning ger därför att mandatet att utfärda föreskrifter om sådana säkerhetsåtgärder som avses i cybersäkerhetslagen 2 kap. 3 § även inkluderar möjligheten, där så är motiverat, att konkretisera mer i detalj vad ledningens ansvar och uppgifter för att godkänna och övervaka säkerhetsåtgärder innebär kopplat till de respektive säkerhetsåtgärderna. Närmare om vad föreskrifterna reglerar med avseende på detta redovisas i avsnitt 7.2.3 om roller, ansvarsområden och befogenheter.

2.7 Sektorsgemensamma och sektorsspecifika krav

I föreskrifternas krav omfattar en mängd olika typer av verksamhetsutövare inom 18 olika sektorer. Kraven behöver därför utformas på ett sådant sätt att de är flexibla för att möjliggöra för verksamhetsutövare att utforma sitt cybersäkerhets-arbete på ett sätt som passar samtidigt som föreskriftskraven bidrar till att höja nivån av cybersäkerhet i Sverige.

När det gäller de grundläggande sättet på vilket ett systematiskt och riskbaserat arbete med cybersäkerhet utförs skiljer det sig inte på en övergripande nivå mellan olika sektorer. Det kan dock i vissa fall finnas anledning att ställa specifika mer sektorskopplade krav där exempelvis den tekniska miljön förutsätter att vissa åtgärder vidtas för att verksamhetsutövarna inom sektorn ska uppnå en tillräckligt hög nivå av cybersäkerhet. I föreskrifterna samlas den typen av sektorsspecifika krav i kapitel 6. Denna version av föreskrifter innehåller endast krav kopplade till offentlig sektor men det är inte uteslutet att det vid senare uppdateringar tillkommer sektorsspecifika krav även för andra typer av verksamhetsutövare, exempelvis om det inom ramen för tillsynsmyndigheternas verksamhet eller ett förändrat säkerhetspolitiskt läge visas att det finns ett behov av sådana krav.

3. Utformning av föreskrifter och allmänna råd

3.1 En hög nivå av cybersäkerhet och genomförandeförordningen

När föreskrifter på området utformas behöver utgångspunkten vara att nivån på kraven ska läggas så att samhällets behov av cybersäkerhet omhändertas samtidigt som verksamhetsutövarna ges flexibilitet vad avser hur de uppnår avsedd nivå av

cybersäkerhet. Föreskrifterna bör därför innehålla tydliga beskrivningar av vilket syfte och vilken effekt olika säkerhetsåtgärder ska innebära. Krav på hur något ska uppnås ställs när det är centralt för det systembygge som nu sker på cybersäkerhetsområdet, alternativt när det handlar om krav som måste uppfyllas för att kunna garantera samhällets funktionalitet, sådana krav ska då ligga i linje med 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 i 1 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.

Ledning för vad föreskrifterna utifrån EU:s perspektiv behöver innehålla och deras detaljeringsgrad kan som nämnts i avsnitt 2.2 hämtas genom jämförelse med genomförandeförordningen. Eftersom NIS2-direktivet är ett minimidirektiv och EU-kommissionen i nuläget inte har valt att nyttja sitt mandat att anta genomförandeakter även för andra väsentliga och viktiga entiteter än de som regleras i genomförandeförordningen[11] bedöms medlemsstaterna ha ett större nationellt utrymme att utforma säkerhetskrav som tar hänsyn till nationella förutsättningar och förhållanden för övriga sektorer. Inriktning för svensk del kan hämtas från förarbetena där regeringen pekar på att lagen som genomför NIS 2-direktivet i Sverige måste ta sin utgångspunkt i den hotbild och utmaningar som strategiska sårbarheter i ett digitaliserat samhälles cybersäkerhetslandskap och risken att påverka samhällsviktig verksamhet och ytterst Sveriges säkerhet innebär.[12]

[11] Det vill säga leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av utlokaliserade driftstjänster, leverantörer av utlokaliserade säkerhetstjänster, leverantörer av marknadsplatser online, leverantörer av sökmotorer, leverantörer av plattformar för sociala nätverkstjänster och tillhandahållare av betrodda tjänster.
[12] Prop. 2025/26:28 s. 37f.

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

Av cybersäkerhetslagen framgår att säkerhetsåtgärderna ska utgå från ett allriskperspektiv och att de ska 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 p. 2 NIS2-direktivet. Såsom redogjorts för ovan i avsnitt 2 behöver föreskrifterna bland annat utgå från den hotbild och de utmaningar som finns i det svenska cybersäkerhetslandskapet.

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.

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

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

   Gällande strategier för riskanalys och för nätverks och informationssystemens säkerhet ger föreskriften i sin helhet stöd för verksamhetsutövarens utformning av det arbetet. Riskanalys regleras närmare i 3 kap. 12 – 13 §§.

2. incidenthantering,

   Omhändertas i föreskrifter och allmänna råd främst genom kraven på verksamhetsutövaren avseende incidenthantering (3 kap. 15 §), omvärldsbevakning (3 kap. 10 §), driftrelaterad dokumentation (4 kap. 7–9 §§) och övervakning, säkerhetsloggning och logganalys (4 kap. 18–20 §§) samt robust och spårbar tid (4 kap. 21 §).

3. kontinuitetshantering och krishantering,

Omhändertas i föreskrifter och allmänna råd främst genom kraven på verksamhetsutövaren avseende kontinuitetshantering (3 kap. 14 §§), krishantering (3 kap. 16 §).

4. säkerhet i leveranskedjan,

   Omhändertas i föreskrifter och allmänna råd främst genom kraven på verksamhetsutövaren avseende förvärv, utveckling och underhåll av system (4 kap. 1–3 §§), riskhantering (3 kap. 12–13 §§) och kontinuitetshantering (3 kap. 14 §),

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 (4 kap. 1–3 §§) och uppföljning och utvärdering (3 kap. 17 §). 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 (3 kap. 17 §), roller, ansvarsområden och befogenheter (3 kap. 4-8 §§) och omvärldsbevakning (3 kap. 10 §).

7. grundläggande praxis för cyberhygien och utbildning i cybersäkerhet,

   Omhändertas i föreskrifter och allmänna råd främst genom kraven på verksamhetsutövaren avseende personalsäkerhet (3 kap. 9 §).

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 (4 kap. 23-25 §§).

9. personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning,

   Omhändertas i föreskrifter och allmänna råd främst genom kraven på verksamhetsutövaren avseende personalsäkerhet (3 kap. 9 §), segmentering (4 kap. 10–11 §§), behörighetshantering och autentisering (4 kap. 12–17 §§), övervakning, säkerhetsloggning och logganalys (4 kap. 18–20 §§), robust och korrekt tid (4 kap. 21 §) och driftrelaterad dokumentation (4 kap. 7–9 §§).

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 (4 kap. 12–17 §§), krishantering (3 kap. 16 §) och sektorsspecifika säkerhetsåtgärder för offentlig förvaltning (6 kap. 1–2 §§).

För vissa sektorer kan det finnas anledning att ställa ytterligare krav på de säkerhetsåtgärder som de ska införa, exempelvis mot bakgrund av sektorernas uppgifter och samhällets beroende av deras tjänster. Detta har gjorts för offentlig förvaltning. Offentlig förvaltning har särskilda uppgifter i nationell krisberedskap och uppgifterna förutsätter eller underlättas av tillgång till robusta system för kriskommunikation. Av denna anledning har särskilda sektorsspecifika krav riktats mot statliga myndigheter, regioner och kommuner i kap. 6 i föreskrifterna.

Sådana åtgärder som ska vidtas för att skydda systemens fysiska miljö är samlade i kap. 5 i föreskrifterna.

4. 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 och cybersäkerhetsförordningen med tillhörande myndighetsföreskrifter. Nedan redogörs för några *alternativa* lösningar till att konkretisera kraven i cybersäkerhetslagen och cybersäkerhetsförordningen genom myndighetsföreskrifter. Vidare redogörs för konsekvenserna om inga föreskrifter genomförs.

4.1 Inga föreskrifter eller endast vägledning

Det första alternativet 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 §§ cyber-

säkerhetslagen. 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 Myndigheten för civilt försvar både metodstöd för arbete med informations- och cybersäkerhet, utbildningar samt vägledningar för hantering av säkerhet i nätverk och informationssystem, upphandling, fysisk säkerhet i it- och ot-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.

Myndigheten 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[13] som i sin helhet omfattas av krav som är jämförbara med kraven i cybersäkerhetslagen. De åläggs att uppfylla säkerhetskrav för sina informationshanteringssystem enligt förordningen (2022:524) om statliga myndigheters beredskap.[14] Säkerhetskraven för statliga myndigheter förtydligas i myndighetens föreskrifter och allmänna råd om informationssäkerhet för statliga myndigheter (MSBFS 2020:6) och föreskrifter och allmänna råd om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7). Myndighetens 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.[15] Till detta kommer reglering som exempelvis rör hantering av viss information eller viss

[13] Ett antal statliga myndigheter är undantagna från regleringen i enlighet med 3 § förordningen (2022:524) om statliga myndigheters beredskap.
[14] Begreppet informationshanteringssystem omfattar sådana nätverk och informationssystem som regleras i NIS2-direktivet.
[15] 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.

verksamhet. Här kan exempelvis nämnas dataskyddsförordningen[16] som reglerar hanteringen av 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.

Myndigheten för civilt försvar 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.

4.2 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 olika 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 har åsidosatt sina skyldigheter enligt

[16] 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).

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 en negativ påverkan på rättssäkerheten och försvårar för tillsynsmyndigheterna att bedriva en effektiv tillsyn och vid behov ingripa vid en överträdelse. Exempelvis behöver storleken på sanktionsavgifter kunna härledas till de konsekvenser som bristande kravuppfyllnad får i förhållande till regleringens syfte. Bristande efterlevnad av en vägledning kan inte åtgärdas genom tillsyn.

Myndigheten för civilt försvar 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, är enklare att anpassa till svenska förhållanden samt går att mer skyndsamt uppdatera 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. Det bör dock betonas att användningen av standarder på området bedöms bidra till en hög cybersäkerhet och föreskrifterna innehåller ett uttryckligt krav på att verksamhetsutövare ska identifiera och hantera sitt behov av att använda relevanta standarder i sitt cybersäkerhetsarbete.

5. Beskrivning och beräkning av förslagets eller beslutets kostnader och intäkter för staten och företagen samt andra konsekvenser

För att ge en beskrivning av vilka kostnader och intäkter förslagen beräknas ha ges först en beskrivning av vilka som omfattas av förslagen. Därefter följer en beskrivning av kostnaderna och slutligen beskrivs andra konsekvenser för företagen än sådana som avser kostnader.

5.1 Vilka berörs av regleringen

NIS2-direktivets tillämpningsområde följer av artikel 2. I p. 1–5 definieras området för att följas av undantag under p. 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 ytterligare krav är att verksamheten tillhandahåller sina tjänster eller bedriver sin verksamhet i unionen. Artikel 2 i bilagan till kommissionens rekommendation definierar mikroföretag samt små och medelstora företag (SMF-kategorin). Av artikeln följer att ett medelstort företag är ett företag som sysselsätter minst 50 personer eller vars omsättning eller balansomslutning överstiger 10 miljoner euro per år.

Vissa sektorer och typer av verksamhetsutövare omfattas av NIS2-direktivet oavsett storlek. Det gäller exempelvis verksamhetsutövare som erbjuder allmänna elektroniska kommunikationsnät, allmänt tillgängliga elektroniska kommunikationstjänster, betrodda tjänster, registreringsenhet för toppdomäner, DNS-tjänster eller domännamnsregistrering.

Detsamma gäller

1. verksamhet som är väsentlig för att upprätthålla kritiska funktioner i samhället och ekonomiska funktioner,
2. om en störning i verksamheten kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet, folkhälsa eller medföra betydande systemrisker särskilt om det får gränsöverskridande konsekvenser, eller
3. verksamhet som är kritisk på grund av sin särskilda betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst, eller för andra sektorer som är beroende av denna verksamhet.

För att en statlig myndighet ska omfattas av regleringen krävs enligt huvudregeln i 1 kap. 3 § 1 st. p. 1 cybersäkerhetslagen att den har befogenhet att fatta beslut som påverkar fysiska eller juridiska personers rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital.

De verksamhetsutövare som omfattas av cybersäkerhetslagens regler ska anmäla sig till Myndigheten för civilt försvar. I mitten av april 2026 har 2080 företag, 83 statliga myndigheter, 19 regioner, 264 kommuner och 44 kommunalförbund anmält sig. De har angivit att de bedriver verksamhet i en eller flera sektorer fördelat enligt följande: Energi 629 stycken, Transporter 158 stycken, Bankverksamhet 88 stycken, Finansmarknadsinfrastruktur 6 stycken, Hälso- och sjukvård 453 stycken, Dricksvatten 206 stycken, Avloppsvatten 206 stycken, Digital infrastruktur 420 stycken, Förvaltning av IKT-tjänster (mellan företag) 250 stycken, Offentlig förvaltning 404 stycken, Rymden 2 stycken, Post- och budtjänster 18 stycken, Avfallshantering 173 stycken, Tillverkning, produktion och distribution av kemikalier 76 stycken, Produktion, bearbetning och distribution av livsmedel 199 stycken, Digitala leverantörer 14 stycken och Forskning 13 stycken. Antalet förändras givetvis över tid genom nyanmälan och avanmälan i de olika sektorerna.

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, att arbeta med cybersäkerhet utifrån kända hot och

identifierade risker och 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.

5.2 En beskrivning och beräkning av förslagets kostnader och intäkter för företag.

En alternativ lösning är som tidigare har beskrivits 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 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.

Regeringen konstaterar följande i propositionen. [17] *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

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

att upprätthålla en säker informationsbehandling. 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 informationsbehandling 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 myndigheten 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 myndigheten uppskattat de tillkommande kostnader som följer av föreskriftskraven för en verksamhetsutövare med låg respektive högre mognadsnivå inom cybersäkerhetsområdet. Det bör i detta sammanhang även betonas att ett systematiskt och riskbaserat cybersäkerhetsarbete i enlighet med föreskrifterna även kan bidra till minskade kostnader genom att minska risken för kostsamma incidenter.

Förslaget bedöms inte generera intäkter för staten, kommuner, regioner, företag och andra enskilda men kan däremot minska kostnader orsakade av incidenter. I det fall ett företag bryter mot reglerna i föreskrifterna kan dock en tillsynsmyndighet besluta om sanktionsavgifter enligt cybersäkerhetslagen. Sådana sanktionsavgifter kan påverka företagets ekonomi.

5.3 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

För att begränsa kostnaderna för verksamhetsutövarna är kraven utformade så att de slår fast vilken effekt verksamhetsutövaren ska uppnå men ger ett så stort utrymme som möjligt för verksamhetsutövarna att välja på vilket sätt detta ska göras. Detta ger flexibilitet och möjlighet för verksamhetsutövaren att mer i detalj utforma de åtgärder som ska vidtas på ett sätt som ansluter till existerande sätt att arbeta. Myndigheten kommer till detta även att ta fram en vägledning som ger ett konkret stöd i hur kraven kan uppfyllas, exempelvis genom att redovisa bakgrund, olika lösningar samt hänvisningar till fördjupat stöd. Utöver det kommer myndigheten genom sin cybersäkerhetsrådgivningstjänst att erbjuda verksamhets-utövare möjlighet att få individuella svar på olika frågor relaterade till arbetet med cybersäkerhet inklusive hur kraven i regleringen kan uppfyllas.

5.4 Kostnader och konsekvenser avseende 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 som ledningen behöver avsätta för att tillgodogöra sig innehållet i utbildningarna (8-20 timmar initialt och därefter 2-4 timmar per år).

5.5 Kostnader och konsekvenser avseende organisatoriska säkerhetsåtgärder

Kraven i föreskrifter och allmänna råd när det gäller de organisatoriska säkerhets-åtgärderna 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, roller och ansvar, 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 och hanterar risker på ett mer eller mindre samlat sätt. Formen för att värdera information och risker kan dock 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 något ökade krav på 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 har haft. Det gäller kraven i 2 kap. 1 § på ledningens utbildning, 3 kap. 9 § ökade krav på egen och inhyrd personals kompetens där kompetensutvecklingsbehov inte tillgodoses löpande, 3 kap. 10 § utökad omvärldsbevakning, allmänt råd till 3 kap. 12 § bedömning av risker med aggregerad och ackumulerad information, och allmänt råd till 3 kap. 14 § rörande att öva återställning av sektorskritiska system.

5.5.1 Kompetensutveckling

Behovet av kompetenshöjande 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 i de fall grundläggande utbildning saknas bedömer myndigheten till 40-100 timmar, översyn och uppdatering av materialet utifrån förändringar i verksamheten och i hotbild mot verksamheten till 20 timmar/år. Formatet på utbildningar kan anpassas till verksamhetsutövarens 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 arbetsbelastningen (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.

5.5.2 Omvärldsbevakning

Kostnaden för omvärldsbevakning ligger i att utifrån verksamhetsutövarens behov värdera den information som källorna i föreskrifterna ställer krav på att bevaka. Vissa av källorna tillhandahåller information av betydelse för verksamhetsutövarens strategiska arbete med cybersäkerhet och andra information om sårbarheter där verksamhetsutövaren 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 inklusive CSIRT och cyberkrishanteringsmyndighet, variera från 0,5–10 timmar per vecka.

5.5.3 Bedöma risker med aggregerad och ackumulerad information

I det allmänna rådet rörande riskhantering rekommenderas verksamhetsutövaren att bedöma risker med aggregerad och ackumulerad 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).

5.5.4 Öva återställning av sektorskritiska system

I det allmänna rådet rörande kontinuitetshantering rekommenderas verksamhetsutövaren att 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, ett högre antal olika sektorskritiska system och större omfattning av den återställning som ska övas (t.ex. 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 eller fler).

5.6 Kostnader och konsekvenser avseende 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 åt 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 it- och ot-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 av 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 säkerhets-åtgärderna 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.

5.6.1 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 20–60 tkr. 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 filtrera sin trafik. Här består kostnaden i att identifiera

verksamhetens behov av trafik och blockera resterande – en kostnad som inkluderas i arbetet med att ta fram och sätta upp systemets säkerhetskonfiguration.

5.6.2 Säkerhetsloggning och logganalys

Kraven i föreskrifterna på vad som ska loggas och när det ska ske 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. För större organisationer, där behovet av loggning av användarhändelser och systemhändelser som indikerar tillbud eller incidenter är större, 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 150–500 tkr per år.

5.6.3 Robust och spårbar tid

Eventuellt tillkommande kostnader 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 30–200 tkr.

5.6.4 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.

5.6.5 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.

5.6.6 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 realtids-övervakning tidigare och att ett sådant behov ändå identifieras tillkommer kostnader för extra bemanning för att analysera behovet av att agera och att personal finns som kan hantera problemet.

5.6.7 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.

5.7 Kostnader och konsekvenser avseende fysiska säkerhetsåtgärder

För att förhindra skador på och obehörig åtkomst till it- och ot-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. [18]

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- och ot-utrymmen och tekniska försörjningssystem med tillräcklig funktion och redundans kan kostnaderna för att uppfylla föreskriftens krav på fysiska säkerhetsåtgärder bli påtagliga. Bedömningen är dock att majoriteten av

[18] NIS2-direktivet skäl (79)

verksamhetsutövarna redan, med hänsyn till sin storlek 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 de är dyra 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- och ot-utrymmen med övervakning och larm, samt
- tillräcklig funktion och redundans gällande tekniska försörjningssystem.

5.7.1 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 redan behandlas, ska behandlas eller har behandlats i verksamhetsutövarens system. Kostnaden för att sätta upp skärmar, bygga rum eller på annat sätt skapa avskilda utrymmen med det skydd som informationsbehandlingen kräver beräknas ca 5–10 tkr för skärmavskiljare och mellan 10–40 tkr per kvadratmeteryta för rum beroende på behovet av ljudisolering.

5.7.2 Säkerställa tillgång till särskilda it- och ot-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- och ot-utrymmen med larm och övervakning. De utrymmen där verksamhetsutövarens 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- och ot-utrymme i form av låst skåp uppskattas till mellan 50–500 tkr beroende på låsfunktion, ventilation och hur väl skåpet skyddar mot avlyssning. För större särskilda it- och ot-utrymmen som utrustas med larm, klimatanläggning, brandskydd som inte skadar system är kostnaden att från grunden bygga ett sådant rum (serverhall) 60–100 tkr 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.

5.7.3 Tillräcklig funktion och redundans gällande tekniska försörjningssystem.

Bedömningen är att de flesta verksamhetsutövare till stor del har 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 30–500 tkr är beroende av hur många system som behöver hållas igång och under hur lång tid.

5.8 Kostnader och konsekvenser avseende sektorsspecifika säkerhetsåtgärder

5.8.1 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.

5.9 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.

6. Andra relevanta konsekvenser än kostnaderna för företagen

6.1 Konkurrensförhållandena för företagen

För att genomföra NIS2-direktivet i svensk rätt krävs att de krav som ställs i cybersäkerhetslagen konkretiseras i föreskrifter avseende vilka organisatoriska, tekniska, driftrelaterade och fysiska säkerhetsåtgärder verksamhetsutövarna ska vidta för att uppnå en tillräcklig nivå av cybersäkerhet. NIS2-direktivet är som nämnts ett minimidirektiv och ger därmed utrymme för de olika medlemsstaterna att vidta nationella anpassningar. Samtidigt är det, som redovisades inledningsvis i avsnitt 2, betydligt mer detaljerat jämfört med det första NIS-direktivet. Den ökade detaljnivån har haft till uttalat syfte att minska skillnaderna mellan hur olika medlemsstater genomför direktivets krav. Flera medlemsstater, till skillnad från Sverige, har redan regelverk med liknande krav på plats sedan flera år. Detta har möjliggjort för flera medlemsstater att med mindre justeringar implementera NIS2-direktivet krav på säkerhetsåtgärder. Hur regelverket kring cybersäkerhet är strukturerat ser dock olika ut i olika medlemsstater vilket gör det svårt att göra enkla jämförelser. Vissa medlemsstater, exempelvis Finland, har övergripande regelkrav men tillsynar även mot ramverk som i en svensk kontext närmast är att likställas med vägledning.

När det gäller verksamhetsutövare som bedriver en hög grad av gränsöverskridande verksamhet har behovet av ensning mellan medlemsstaterna bedömts som extra högt. Detta omhändertas genom att EU-kommissionen tagit fram en genomförandeförordning för verksamhetsutövare inom sektorerna digitala tjänster och digital infrastruktur. EU-kommissionen har, som nämnts ovan i avsnitt 2.2, även fått mandat att utfärda genomförandeförordningar för andra sektorer som omfattas men ännu inte valt att nyttja detta. Även om genomförandeförordningen endast gäller en begränsad andel av de olika verksamhetsutövare som omfattas av NIS2-direktivet och cybersäkerhetslagen kan den ses som vägledande för hur EU-kommissionen ser på behoven av att ytterligare konkretisera NIS2-direktivets krav på verksamhetsutövares säkerhetsåtgärder. Genomgången nedan i avsnitt 7 av hur föreskrifternas krav förhåller sig till motsvarande krav i genomförandeförordningen visar på en överensstämmelse kring vilka åtgärder som regleras men att föreskrifterna i många fall ger de svenska verksamhetsutövarna en något större flexibilitet i hur åtgärderna ska utformas.

Vad gäller relationen till företag i tredje land kan krav på cybersäkerhet inte bara utgöra en belastning utan även som en tillgång. Regeringen konstaterar i propositionen att högre krav förvisso kan vara resurskrävande och påverka hur mycket resurser en verksamhetsutövare lägger ned på cybersäkerhet jämfört med en konkurrerande verksamhet. Det kan samtidigt stärka en verksamhetsutövarens ställning på marknaden att ha en mer motståndskraftig verksamhet som i mindre utsträckning än andra liknande verksamheter påverkas av incidenter.[19]

Av skäl (3) i NIS2-direktivet framgår att *beredskap och ändamålsenlighet på cybersäkerhetsområdet är därför nu viktigare än någonsin för att den inre marknaden ska fungera väl. Cybersäkerhet är dessutom en viktig förutsättning för att många kritiska sektorer ska kunna tillgodogöra sig den digitala omställningen och fullt ut utnyttja digitaliseringens ekonomiska, sociala och hållbarhetsmässiga fördelar.*

Mot denna bakgrund görs bedömningen att föreskrifternas konkretisering av NIS2-direktivets och cybersäkerhetslagens krav på säkerhetsåtgärder inte bedöms påverka konkurrensförhållanden för företagen på nationell och EU-nivå. Påverkan på global nivå bedöms inte heller, med tanke på vikten av cybersäkerhet för att kunna dra nytta av digitaliseringens fördelar, vara påtaglig. Föreskrifterna om säkerhetsåtgärder och utbildning bedöms medföra att verksamhetsutövare minskar sin risk för att drabbas av incidenter och därmed kunna erbjuda mer stabila leveranser samt öka sin konkurrenskraft.

6.2 Behov av om särskild hänsyn 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.

6.3 Bidrag till samhällets cybersäkerhet

Myndigheten 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.

[19] Prop. 2024/25:28 s. 225

7. 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 föreskrifternas krav bedöms hålla sig inom utrymmet för nationell anpassning. Nedan följer en närmare redogörelse för föreskrifternas utformning i förhållande till med NIS2-direktivet, cybersäkerhetslagen och dess förarbeten samt genomförandeförordningen där genomförandeförordningen som nämnts ovan i avsnitt 2.2 kan betraktas som ett uttryck för vad EU-kommissionen ser som en lämplig nivå av reglering, åtminstone för verksamhetsutövare inom vissa särskilt gränsöverskridande sektorer.

7.1 Ledningens utbildning i kapitel 2

7.1.1 Ledningens utbildning om säkerhetsåtgärder (2 kap. 1 §)

7.1.1.1 Föreskrifterna

Ledningen ska ha den kunskap och den kompetens som krävs för att fastställa mål och inriktning för cybersäkerhet, bedöma vilka säkerhetsåtgärder som verksamhetsutövaren behöver genomföra för att upprätthålla en lämplig nivå av cybersäkerhet utifrån identifierade risker och övervaka genomförandet av säkerhetsåtgärder.

Av de allmänna råden framgår vidare att ledningens utbildning bör omfatta ledningens roll i ett systematiskt och riskbaserat cybersäkerhetsarbete, relevant terminologi och reglering, vilken betydelse cybersäkerheten hos verksamhetsutövaren har för att upprätthålla viktiga samhällsfunktioner, riskhantering och övervakning som ett stöd för att leda och styra arbetet med cybersäkerhet, samt för ledningen relevanta interna regler, arbetssätt och stöd.

7.1.1.2 NIS2-direktivet

Av artikel 20 p. 2 i NIS2-direktivet följer att medlemsstaterna ska säkerställa att *medlemmarna i väsentliga och viktiga entiteters ledningsorgan är skyldiga att genomgå utbildning, och ska uppmuntra väsentliga och viktiga entiteter att regelbundet erbjuda liknande utbildning till sina anställda för att de ska få tillräckligt med kunskap och kompetens för att kunna identifiera risker och bedöma riskhanteringspraxis för cybersäkerhet och deras inverkan på de tjänster som tillhandahålls av entiteten.*

7.1.1.3 Cybersäkerhetslagen

Av cybersäkerhetslagen 2 kap. 4 § framgår att de personer som ingår i ledningen för en verksamhetsutövare ska genomgå utbildning om säkerhetsåtgärder.

Av propositionen framgår att utbildningen enligt artikel 20.2 i direktivet ska *syfta till att den som genomgår utbildningen ska få tillräckligt med kunskap och kompetens för att kunna identifiera risker och bedöma riskhanteringspraxis för cybersäkerhet och deras inverkan på de tjänster som tillhandahålls av entiteten. Eftersom utbildningskravet har en koppling till skyldigheten för ledningen att godkänna och övervaka genomförandet av säkerhetsåtgärder bör utbildningen enligt regering handla om säkerhetsåtgärder. Utbildningen bör alltså därmed bland annat syfta till att ledningen ska ha tillräcklig kompetens för att kunna identifiera risker och kunna bedöma vilka säkerhetsåtgärder som bör vidtas av verksamhetsutövaren.*[20]

7.1.1.4 Genomförandeförordningen

Genomförandeförordningen fastställer i bilagan närmare krav på genomförandet av riskhanteringsåtgärder för cybersäkerhet enligt artikel 21, inte kraven på ledningens utbildning enligt artikel 20 p.2.

Det kan dock nämnas att i p. 8.1. och p. 8.2 ställs närmare krav på kunskap och medvetandehöjande insatser och utbildning, inklusive för personer i verksamhetsutövarens ledning, med anledning av kravet i artikel 21 p.2 g) om grundläggande praxis för cyberhygien och utbildning i cybersäkerhet. Bland annat omnämns behov av medvetenhet om risker, kunskap om cybersäkerhet, införda säkerhetsåtgärder med mera. Krav ställs även på schemaläggning och att ett program för medvetandehöjning och cyberhygien ska fastställas.

7.1.1.5 Sammanfattningsvis

Kraven i föreskrifterna bedöms ligga i linje med uttalanden i förarbetena och har utformats för att motsvara den nivå och omfatta de områden som ledningen behöver för att kunna utföra sina uppgifter att godkänna och övervaka genomförandet av säkerhetsåtgärder. Genom att de mer detaljerade kraven utgör

[20] Prop. 2025/26:28 s. 100

allmänna råd och därmed är bör-krav ges verksamhetsutövaren flexibilitet avseende utformningen av utbildningen.

7.2 Organisatoriska säkerhetsåtgärder i kapitel 3

7.2.1 Ett systematiskt och riskbaserat arbete med cybersäkerhet (3 kap. 1–2 §§)

7.2.1.1 Föreskrifterna

I paragraferna ställs krav på att verksamhetsutövaren ska bedriva ett systematiskt och riskbaserat cybersäkerhetsarbete bestående av stegen analysera krav och behov, utforma och genomföra säkerhetsåtgärder, följa upp vidtagna åtgärder och risker samt förbättra åtgärderna vid behov.

Av föreskrifterna framgår även att verksamhetsutövaren ska identifiera och hantera sitt behov av relevanta standarder i cybersäkerhetsarbetet och av det tillhörande allmänna rådet framgår att verksamhetsutövaren bör använda standarderna ISO 27001 respektive ISO 27002 som stöd för sitt arbete.

Kravet på ett systematiskt och riskbaserat cybersäkerhetsarbete ger uttryck för ett väletablerat sätt att arbeta i enlighet med den så kallade PDCA-cykeln, plan-do-check-act, som utgör en central grund i standarden ISO 270001. Det är en systematisk process för ständiga förbättringar av organisationens informations- och cybersäkerhetsarbete. Krav ställs även på att arbetet ska integreras med befintligt sätt att leda och styra organisationen samt att verksamhetsutövarna ska identifiera och hantera sitt behov av att använda relevanta standarder i cybersäkerhetsarbetet. Ett systematiskt och riskbaserat arbete ger en tydlig och strukturerad styrning i enlighet med ledningens uppsatta mål och externa krav (såsom reglering och avtal med externa parter).

7.2.1.2 NIS2-direktivet

Av artikel 21 p. 1 i NIS2-direktivet framgår att *medlemsstaterna ska säkerställa att väsentliga och viktiga entiteter vidtar lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och för att förhindra eller minimera incidenters påverkan på mottagarna av deras tjänster och på andra tjänster.*

Med beaktande av de senaste, och i tillämpliga fall, relevanta europeiska och internationella standarder samt genomförandekostnaderna, ska de åtgärder som avses i första stycket säkerställa

en nivå på säkerheten i nätverks- och informationssystem som är lämplig i förhållande till den föreliggande risken. Vid bedömningen av dessa åtgärders proportionalitet ska vederbörlig hänsyn tas till entitetens grad av riskexponering, entitetens storlek samt sannolikheten för att incidenter inträffar och deras allvarlighetsgrad, inbegripet deras samhälleliga och ekonomiska konsekvenser.

Av artikel 21 p. 2 a) i NIS2-direktivet framgår att säkerhetsåtgärderna ska utgå från en allriskansats och minst inbegripa *a) strategier för riskanalys och informationssystemens säkerhet,*

7.2.1.3 Cybersäkerhetslagen

Motsvarande krav finns i cybersäkerhetslagens 2 kap. 3 § st. 1 och st. 2 p. 1.

Se ovan avsnitt 2.5 om systematiskt och riskbaserat arbete.

7.2.1.4 Genomförandeförordningen

I p. 1.1.1 i bilagan till genomförandeförordningen ställer EU bland annat krav på att berörda entiteter genom sin strategi för säkerhet i nätverk och informationssystem bland annat ska fastställa sitt tillvägagångssätt för att hantera säkerheten i sina nätverks- och informationssystem, vara lämpliga för och komplettera de berörda entiteternas affärsstrategi och mål, samt omfatta ett åtagande om kontinuerlig förbättring av säkerheten i nätverks- och informationssystem,

Av skäl (3) i genomförandeförordningen omnämns standarderna ISO/IEC 27001 och ISO/IEC 27002 som sådana europeiska och internationella standarder som är relevanta för säkerheten i nätverks- och informationssystem.

7.2.1.5 Sammanfattningsvis

Föreskriftskraven bedöms ligga i linje med genomförandeförordningens krav. Även om genomförandeförordningen inte uttryckligen omnämner PDCA-cykeln utgör den en central del av de standarder som lyfts i genomförandeförordningen och som nämnts vara en väletablerad metod för att på ett systematiskt och riskbaserat sätt kunna välja lämpliga och proportionella säkerhetsåtgärder inklusive garantera kontinuerlig förbättring av säkerheten. Föreskrifternas krav på att arbetet med cybersäkerhet ska integreras i befintligt sätt att leda och styra organisationen motsvaras av genomförandeförordningens krav på att strategin ska vara lämplig för och komplettera de berörda entiteternas affärsstrategi och mål. Av förarbetena till lagen framgår, som ovan redogjorts för på s. 6, att ett systematiskt och riskbaserat arbete med cybersäkersäkerhet ska ses som en sådan säkerhetsåtgärd som avses i artikel 21 NIS2-direktivet.

7.2.2 Interna regler och arbetssätt (3 kap. 3 §)

7.2.2.1 Föreskrifterna

I paragraferna ställs krav på att verksamhetsutövaren ska fastställa de interna regler och arbetssätt som behövs för att vidta lämpliga och proportionella säkerhetsåtgärder utifrån externa krav, interna behov och identifierade risker avseende cybersäkerhet. De interna reglerna och arbetssätten ska uppdateras vid behov och sparas för att man i efterhand kunna värdera om de säkerhetsåtgärder som har vidtagits är ändamålsenliga och effektiva. Verksamhetsutövaren ska identifiera och hantera sitt behov att dokumentera och spara ytterligare information som kan behövas vid uppföljning och tillsyn.

Av de allmänna råden framgår bland annat att verksamhetsutövaren bör utgå från ledningens mål och inriktning för cybersäkerheten när interna regler och arbetssätt utformas, att de interna regler och arbetssätt bör kommuniceras till berörd personal samt innehålla information om vilken säkerhetsåtgärd de avser, vilka som berörs, vilken roll som ska göra vad och hur resultatet ska dokumenteras.

Syftet med att ställa krav på att verksamhetsutövaren har interna regler och arbetssätt är att säkerställa att arbetet med cybersäkerhet blir systematiskt och strukturerat. Genom de interna reglerna och arbetssätten tydliggör verksamhetsutövaren för organisationen vad som ska göras, hur det ska göras och när.

Genom att inte bara dokumentera interna regler och arbetssätt utan även att spara dessa får verksamhetsutövaren stöd för den egna uppföljningen av cybersäkerhetsarbetet. Det ger även tillsynsmyndigheten stöd för sina bedömningar. Genom att gå tillbaka och bedöma hur verksamhetsutövarens cybersäkerhetsarbete har utvecklats över tid kan tillsynsmyndigheten få en förbättrad bild av om verksamhetsutövaren – även om dagens nivå på cybersäkerhet fortfarande är låg – ändå genom ett målmedvetet arbete har stärkt sin cybersäkerhet jämfört med tidigare.

7.2.2.2 NIS2-direktivet

Av artikel 21 p. 1 i NIS2-direktivet framgår att *medlemsstaterna ska säkerställa att väsentliga och viktiga entiteter vidtar lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och för att förhindra eller minimera incidenters påverkan på mottagarna av deras tjänster och på andra tjänster.*

Av artikel 21 p. 2 a) i NIS2-direktivet framgår att säkerhetsåtgärderna ska utgå från en allriskansats och minst inbegripa *a) strategier för riskanalys och informationssystemens säkerhet.*

7.2.2.3 Cybersäkerhetslagen

Motsvarande krav finns i cybersäkerhetslagens 2 kap. 3 § st. 1 och st. 2 p. 1.

Av författningskommentaren anges att *utarbeta rutiner* som exempel på en säkerhetsåtgärd.[21]

7.2.2.4 Genomförandeförordningen

I p. 1.1.1 i bilagan till genomförandeförordningen ställer EU bland annat krav på att verksamhetsutövare genom sin strategi för säkerhet i nätverk och informationssystem ska fastställa sitt tillvägagångssätt för att hantera säkerheten i sina nätverks- och informationssystem, fastställa nätverks- och informationssäkerhetsmål, kommuniceras till och erkännas av berörda anställda och berörda externa parter, förteckna den dokumentation som ska sparas och ange hur länge dokumentationen ska bevaras samt ange det datum då den formellt godkändes av de berörda entiteternas ledningsorgan (ledningsorganen).

Säkerhetsstrategin för nätverks- och informationssystem ska ses över och när så är lämpligt uppdateras av ledningsorganen minst en gång om året samt när betydande incidenter eller betydande förändringar av driften eller riskerna inträffar. Resultatet av översynerna ska dokumenteras.

Dokumentationskrav ställs därutöver i anslutning till p. 2.1 riskhanteringsram, p. 3.1 incidenthanteringsstrategi, p. 3.2 övervakning och loggning, p. 3.5 incidenthantering, p. 3.6 efterhandsgranskning efter incidenter, p. 4.2 hantering av säkerhetskopiering och redundans samt p. 6.1 säkerhet vid förvärv av IKT-tjänster och IKT-produkter med flera.

7.2.2.5 Sammanfattningsvis

Föreskrifternas krav på att interna regler och arbetssätt ska fastställas och göras tillgängliga för organisationen genom att de dokumenteras och delas bedöms inte gå utöver genomförandeförordningens krav. Flera av genomförandeförordningens krav, exempelvis rörande krav på formellt godkännande och kommunikation finns i föreskrifterna endast som allmänna råd – dvs. rekommendationer, inte uttryckliga krav. I dessa delar ger föreskrifterna verksamhetsutövarna mer handlingsfrihet än genomförandeförordningen.

[21] Prop. 2025/26:28 s 244

7.2.3 Roller, ansvarsområden och befogenheter (3 kap. 4–8 §§)

7.2.3.1 Föreskrifterna

För att verksamhetsutövaren ska kunna vidta lämpliga och proportionella säkerhetsåtgärder ska ledningen godkänna och övervaka genomförandet av säkerhetsåtgärder genom att säkerställa att det finns fastställda mål och inriktning för cybersäkerheten, ledningens uppgifter i arbetet med cybersäkerhet är tydliggjorda, det finns resurser för att bedriva ett systematiskt och riskbaserat cybersäkerhetsarbete, de roller och ansvarsområden som arbetet med cybersäkerhet kräver har tilldelats tillräckliga befogenheter och resurser, samt att ledningen, som en del av sin övervakning, vid behov men minst årligen blir informerad om genomförandet av säkerhetsåtgärder och verksamhetsutövarens nivå på cybersäkerhet.

Av de allmänna råden framgår bland annat att ledningen även ge inriktning för exempelvis hur verksamheter ska prioriteras vid återställning och acceptabel förmåga att upprätthålla sektorskritiska system vid samhällsstörningar.

Även om begreppet ledning tydliggörs i förarbetena[22] så kan olika verksamhetsutövare ha utformat sitt systematiska och riskbaserade cybersäkerhetsarbete på lite olika sätt, exempelvis kan ansvarsfördelningen mellan en kommunstyrelse och kommunfullmäktige i vissa kommuner ha en annan utformning än utgångspunkten i förarbetena. För att ge tillräcklig flexibilitet är därför kravet utformat såsom att verksamhetsutövarens ledning ska säkerställa att vissa saker görs, de behöver inte nödvändigtvis göra detta själva.

I föreskrifterna ställs även krav på att verksamhetsutövaren ska fastställa de roller, ansvarsområden och befogenheter som ett systematiskt och riskbaserat cybersäkerhetsarbete arbete kräver. Verksamhetsutövaren ska utse roller eller ansvarsområden för samordning av cybersäkerhetsarbetet (samordnare), informationsbehandling i system (informationsägare) och för säkerheten i system (systemägare). Vilka befogenheter de roller eller ansvarsområden som verksamhetsutövaren utser rörande motsvarande samordnare, informationsägare och systemägare specificeras i efterföljande tre paragrafer.

Kraven innebär inte någon skyldighet för verksamhetsutövaren att benämna roller eller ansvarsområden som samordnare, informationsägare eller systemägare. Nämnda begrepp används snarast av författningstekniska skäl som ett alternativ till att skriva ”den roll eller det ansvarsområde som har i uppgift att samordna

[22] Prop. 2024/25:28 s 99f

cybersäkerhetsarbetet" när en hänvisning till detta behöver göras. Det kan dock noteras att både systemägare och informationsägare är väletablerade begrepp. Vad gäller samordnare motsvarar det närmast en CISO det vill säga Chief Information Security Officer, ofta benämnd informationssäkerhetssamordnare eller informationssäkerhetschef. Att säkerställa att roller, ansvarsområden och tillhörande befogenheter är utsedda möjliggör ledning och styrning av cybersäkerhetsarbetet och därmed en förutsättning att kunna bedriva ett systematiskt och riskbaserat cybersäkerhetsarbete.

7.2.3.2 NIS2-direktivet

Av artikel 21 p 1 i NIS2-direktivet framgår att *medlemsstaterna ska säkerställa att väsentliga och viktiga entiteter vidtar lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och för att förhindra eller minimera incidenters påverkan på mottagarna av deras tjänster och på andra tjänster.*

Av artikel 21 p 2 a) i NIS2-direktivet framgår att säkerhetsåtgärderna ska utgå från en allriskansats och minst inbegripa *a) strategier för riskanalys och informationssystemens säkerhet.*

Av artikel 20 p 1 i NIS2-direktivet framgår att medlemsstaterna *ska säkerställa att väsentliga och viktiga entiteters ledningsorgan godkänner de riskhanteringsåtgärder för cybersäkerhet som dessa entiteter vidtar för att följa artikel 21, övervakar genomförandet av dem och kan ställas till svars för entiteternas överträdelser av den artikeln.*

Av skäl (137) framgår att direktivet *bör syfta till att säkerställa en hög ansvarsnivå för riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter för väsentliga och viktiga entiteter. Därför bör ledningsorganen för väsentliga och viktiga entiteter godkänna riskåtgärderna för cybersäkerhet och övervaka deras genomförande.*

7.2.3.3 Cybersäkerhetslagen

Motsvarande krav finns i cybersäkerhetslagens 2 kap. 3 § st. 1 och st. 2 p. 1.

Av författningskommentaren ges *fördelar ansvar, roller och mandat i organisationen* som exempel på säkerhetsåtgärd.[23]

Cybersäkerhetslagen innehåller inte någon reglering om ledningens ansvar för säkerhetsåtgärder men ställer däremot krav på att verksamhetsutövarna enligt 2 kap.3 § ska vidta säkerhetsåtgärder. Se avsnitt 2.6 för fördjupad analys kring hur detta ska bedömas utifrån mandatfrågan.

[23] Prop. 2025/26:28 s. 244

7.2.3.4 Genomförandeförordningen

I p. 1.2 i bilagan till genomförandeförordningen ställer EU bland annat krav på att verksamhetsutövare genom sin strategi för säkerhet i nätverk och informationssystem ska peka ut roller, ansvarsområden och befogenheter:

(a) Som ett led i sin strategi för säkerheten i nätverks- och informationssystem enligt p. 1.1 ska de berörda entiteterna fastställa ansvarsområden och befogenheter för säkerheten i nätverks- och informationssystem, dela upp dem på roller och fördela dem i enlighet med de berörda entiteternas behov samt kommunicera dem till ledningsorganen.
(b) De berörda entiteterna ska kräva att all personal och alla tredje parter tillämpar säkerheten i nätverks- och informationssystem i enlighet med den fastställda strategin för säkerhet i nätverks- och informationssystem samt med de berörda entiteternas ämnesspecifika strategier och förfaranden.
(c) Åtminstone en person ska rapportera direkt till ledningsorganen om frågor som rör säkerheten i nätverks- och informationssystem.
(d) Beroende på de berörda entiteternas storlek ska säkerheten i nätverks- och informationssystem täckas av särskilda roller eller uppgifter som utförs utöver de befintliga rollerna.
(e) Uppgifter och ansvarsområden som står i strid med varandra ska separeras, om tillämpligt.
(f) Roller, ansvarsområden och befogenheter ska ses över och vid behov uppdateras av ledningsorganen med planerade intervall och när betydande incidenter eller betydande förändringar av driften eller riskerna inträffar.

Av skäl (26) kan utläsas att verksamhetsutövarens tillgångar ska ha ägare och att verksamhetsutövaren på personnivå bör identifiera vem som har ansvar för att skydda tillgången. Det framgår vidare av skäl (24) att tillgångar kan vara både materiella och immateriella. Detta tillsammans med övriga referenser till tillgångar i skälen gör att det ligger närmast till hands att med tillgångar avses inte bara system utan även information. En sådan tolkning ligger i linje med begreppet informationstillgångar med vilket avses information och informationsbehandlande resurser som är av värde för en organisation.[24]

Av skäl (27) framgår att *tilldelningen och organisationen av cybersäkerhetsroller, ansvarsområden och behörigheter bör innebära att en konsekvent struktur inrättas för styrningen och genomförandet av cybersäkerhet inom de berörda entiteterna, vilket bör säkerställa effektiv kommunikation vid incidenter. När ansvaret för vissa roller fastställs och anförtros bör de*

[24] Se exempelvis termbanken för informationssäkerhet https://termbank-informationssakerhet.msb.se/

berörda entiteterna överväga sådana roller som informationssäkerhetschef, informationssäkerhetsansvarig, incidenthanterare och revisor, eller motsvarande.

7.2.3.5 Sammanfattningsvis

De krav som ställs i föreskrifterna rörande ledningens uppgifter bedöms vara mer begränsade än genomförandeförordningen krav på ledningen. Exempelvis ställs i p. 1.2.3 genomförandeförordningen krav på att åtminstone en person ska rapportera direkt till ledningen om frågor som rör säkerheten i nätverks- och informationssystem.

När det gäller övriga krav på roller, ansvarsområden och befogenheter kan konstateras att både föreskrifterna och genomförandeförordningen har krav på att verksamhetsutövaren ska fastställa de roller, ansvarsområden och befogenheter som arbetet med cybersäkerhet kräver. Behovet av att fördela ansvar, roller och mandat i organisationen lyfts även upp i förarbetena till cybersäkerhetslagen. Genomförandeförordningen innehåller en rad krav som inte ställs i föreskrifterna, exempelvis rörande separation av roller, medan föreskrifterna innehåller något mer konkreta krav rörande roller, ansvar och befogenheter kopplade till samordning av cybersäkerhetsarbetet, säkerheten för informationsbehandling i system (informationsägare) och för säkerheten i system. Motsvarigheten till dessa roller och ansvarsområden återfinns dock i genomförandeförordningens skäl i form av informationssäkerhetschef/informationssäkerhetsansvarig samt ägare till olika tillgångar.

Kravet på fördelningen av roller, ansvarsområden och befogenheter i föreskrifterna bedöms ligga i linje med etablerat sätt att arbeta systematiskt och riskbaserat med cybersäkerhet och även med skälen i genomförandeförordningen. Skillnaderna mellan genomförandeförordningen och föreskrifterna bedöms därför i praktiken innebära förhållandevis begränsade konsekvenser för verksamhetsutövarna och inte heller gå utöver det nationella utrymmet för reglering av roller, ansvarsområden och befogenheter för cybersäkerhetsarbetet.

7.2.4 Personalsäkerhet (3 kap. 9 §)

7.2.4.1 Föreskrifterna

I föreskrifterna ställs krav på verksamhetsutövarna att de ska fastställa vilka kontroller av egen och inhyrd personal som ska göras vid rekrytering och förändrade uppgifter samt vilka utbildningar, övningar och andra informationsinsatser avseende cybersäkerhet som ska göras. Enligt de allmänna råden bör kontroller bland annat ske genom referenstagning och identitetskontroll. Informationsinsatser och utbildning bör bland annat anpassas utifrån roller,

ansvarsområden och befogenheter. En utbildningsplan bör upprättas och personal som avslutar sin anställning bör informeras om eventuella begränsningar avseende hur verksamhetsutövarens information får användas.

Syftet med kraven är att så långt möjligt förebygga att incidenter sker på grund av olämplighet eller okunskap hos personal. De allmänna råden konkretiserar kraven som stöd för att hitta rätt nivå. Rekommendationen att tydliggöra begränsningar rörande informationsanvändning efter avslutad anställning eller uppdrag bedöms, liksom övriga av de allmänna råden, utgöra standard hos de flesta organisationer.

7.2.4.2 NIS2-direktivet

I artikel 21 p. 2 g) och i) ställs krav på att säkerhetsåtgärder ska avse *grundläggande praxis för cyberhygien och utbildning i cybersäkerhet* respektive *personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning*.

7.2.4.3 Cybersäkerhetslagen

Motsvarande krav finns i 2 kap. 3 § st. 2 p. 7 och 9 cybersäkerhetslagen.

Av propositionen s. 94 framgår följande: *Syftet med personalsäkerhet är enligt regeringen att förebygga att personal orsakar incidenter på grund av olämplighet eller okunskap. Kravet på personalsäkerhet kan enligt regeringen bland annat innebära att verksamhetsutövaren genomför insatser för att höja kompetensen och kunskapen hos personalen om frågor som rör cybersäkerhet för att motverka mänskliga misstag. En aspekt på personalsäkerhet kan därmed vara utbildning av personal. Det finns ingen vedertagen definition av uttrycket bakgrundskontroller, men personalsäkerhet kan också innebära att olika typer av kontroller genomförs exempelvis i form av verifiering av olika kvalifikationer bland annat för att motverka avsiktligt skadliga handlingar.*

7.2.4.4 Genomförandeförordningen

Genomförandeförordningen ställer flera krav med koppling till personalsäkerhet och utbildning. Bland annat kan nämnas krav i:

- punkt 8 om både medvetandehöjning, cyberhygien och säkerhetsutbildning,
- punkterna 10.1.1 och 10.1.2 a) – c) rörande medvetandehöjning och kunskap. Exempelvis ska verksamhetsutövarna *säkerställa att deras anställda och direkta leverantörer och tjänsteleverantörer, om tillämpligt, förstår och åtar sig att uppfylla de säkerhetsuppgifter som de ansvarar för, på ett sätt som är lämpligt för de erbjudna tjänsterna och arbetet och i enlighet med de berörda entiteternas strategi för säkerheten i nätverks- och informationssystem*,
- punkt 10.1.2 d) på att verksamhetsutövaren ska säkerställa *mekanismer för att anställa personal med rätt kvalifikationer för sina respektive roller, såsom*

referenskontroller, prövningsförfaranden, validering av certifieringar eller skriftliga prov, och

- punkt 10.3.2 vad gäller förfarande vid *avslutad eller ändrad anställning* som bland annat reglerar överenskommelser om ansvar om uppgifter efter avslutad anställning eller avtal, exempelvis konfidentialitetsklausuler.

7.2.4.5 Sammanfattningsvis

Föreskrifternas krav bedöms vara på en mer övergripande nivå än genomförandeförordningens motsvarande krav. I delar är genomförande-förordningen förhållandevis detaljerad och reglerar även fler aspekter än föreskrifterna, exempelvis i p. 10.4 krav på disciplinära förfaranden.

7.2.5 Omvärldsbevakning (3 kap. 10 §)

7.2.5.1 Föreskrifterna

I föreskrifterna ställs krav på att verksamhetsutövarna ska hålla sig uppdaterade om hot, sårbarheter, teknisk utveckling, rättsliga krav och tillgängligt stöd av betydelse för verksamhetsutövarens cybersäkerhet och därför säkerställa omvärldsbevakning av relevant information från leverantörer och det nationella cybersäkerhetscentret (NCSC) hos Försvarets radioanstalt (FRA) inklusive CSIRT-enhet och cyberkrishanteringsmyndigheten.

Verksamhetsutövaren ska även ansluta sig till automatiska notifieringar om tekniska sårbarheter från CSIRT-enheten hos NCSC samt identifiera och hantera behovet av att, om möjligt, ansluta sig till informationsutbytet enligt MISP-konceptet hos CSIRT-enheten.

Av de allmänna råden framgår även att verksamhetsutövaren bland annat bör omvärldsbevaka tillsynsmyndigheterna, Sveriges nationella samordningscenter för forskning och innovation (NCC-SE) hos NCSC samt EU:s cybersäkerhetsbyrå (ENISA).

Ändamålsenlig omvärldsbevakning är en förutsättning för att säkerställa att det finns ett tillräckligt underlag för att kunna värdera risker, ha kunskap om tekniska och andra förutsättningar, externa krav och övrigt stöd som sammantaget ger möjlighet att införa lämpliga och proportionella säkerhetsåtgärder. En grund-läggande åtgärd i ett systematiskt och riskbaserat cybersäkerhetsarbete är att omvärldsbevaka sina leverantörer för att exempelvis snabbt kunna uppdatera sina system med leverantörens lösningar på upptäckta sårbarheter. NCSC hos FRA kommer att ha en nationell portal genom vilken relevant stöd avseende cyber-säkerhet kommer att kanaliseras. I den nationella portalen kommer verksamhets-

utövarna även att kunna fullgöra skyldigheter i form av anmälan och incident-rapportering. Detta bedöms bidra till uppbyggnaden av ett samlat system att arbeta med cybersäkerhet nationellt. Den nationella portalen underlättar både för verksamhetsutövarna att få tillgång till relevant information och för ansvariga myndigheter att, vid behov, skyndsamt kunna nå ut till relevanta organisationer med tidskritisk information.

Genom att ställa krav på att verksamhetsutövarna ansluter sig till tjänsten ANTS säkerställs att de får löpande information om deras externt exponerade system innehåller sårbarheter och därmed kan vidta nödvändiga åtgärder för att åtgärda detta. Deltagande i MISP ger verksamhetsutövare möjlighet att utbyta relevant information om cybersäkerhet som syftar till att förebygga, upptäcka, reagera på eller återhämta sig från incidenter eller begränsa deras inverkan eller höjer cybersäkerhetsnivån.

7.2.5.2 NIS2-direktivet

NIS2-direktivet innehåller inte något samlat och uttalat krav på omvärlds-bevakning utan det framgår indirekt av kraven på att säkerhetsåtgärder enligt artikel 21 p. 2 ska baseras på en allriskansats som ska skydda nätverks- och informationssystem inklusive systemens fysiska miljö från incidenter. Att inhämta information om hot, sårbarheter, teknisk utveckling, rättsliga krav och tillgängligt stöd är en grundförutsättning för samtliga av de säkerhetsåtgärder som omnämns i artikel 21 p. 2, exempelvis *incidenthantering och säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem, inbegripet hantering av sårbarheter och sårbarhetsinformation*.

NIS2-direktivet ställer flera krav på medlemsstaterna vad gäller att tillgodose tillgången till relevant information om hot, sårbarheter och annan information som stärker cybersäkerheten:

- tjänsten ANTS tillhandahålls av CSIRT-enheten som ett led i att stödja verksamhetsutövare med proaktiv, icke inkräktande skanning av väsentliga och viktiga verksamhetsutövare allmänt tillgängliga system enligt art 11 p. 3 b) och 34 § cybersäkerhetsförordningen och
- informationsutbyte med stöd av MISP sker i enlighet med artikel 29 i NIS2-direktivet och tillhandahålls av CSIRT-enheten. Av artikel 29 i NIS2-direktivet framgår att medlemsstaterna ska säkerställa att verksamhetsutövare har möjlighet att utbyta relevant information om cybersäkerhet som syftar till att förebygga, upptäcka, reagera på eller återhämta sig från incidenter eller begränsa deras inverkan eller höjer cybersäkerhetsnivån.

7.2.5.3 Cybersäkerhetslagen

Motsvarande krav på allriskperspektiv, och utifrån det hitta en lämplig nivå av säkerhet, finns i 2 kap. 3 § st. 2 cybersäkerhetslagen.

7.2.5.4 Genomförandeförordningen

Behovet av omvärldsbevakning omhändertas inte samlat i genomförande-förordningen utan det följer bland annat av följande:

- Punkt 2.1.2 e) *analysera riskerna för säkerheten i nätverks- och informationssystem, inklusive hot, sannolikhet, konsekvenser och risknivå, med beaktande av underrättelser om cyberhot och sårbarheter.*
- Punkt 5.1.4 att reglera i avtal med leverantörer och tjänsteleverantörer: (d) *En skyldighet för leverantörer och tjänsteleverantörer att utan onödigt dröjsmål underrätta de berörda entiteterna om incidenter som utgör en risk för säkerheten i dessa entiteters nätverks- och informationssystem.*
- Punkt 6.10.1. *De berörda entiteterna ska inhämta information om tekniska sårbarheter i deras nätverks- och informationssystem, bedöma sin exponering för sårbarheter och vidta ändamålsenliga åtgärder för att hantera sårbarheterna.*
- Punkt 6.10.2. *Vid tillämpning av p. 6.10.1 ska de berörda entiteterna göra följande*:

  (a) *Övervaka information om sårbarheter via lämpliga kanaler, såsom meddelanden från CSIRT-enheter eller behöriga myndigheter eller information som tillhandahålls av leverantörer eller tjänsteleverantörer.*

  (b) *När så är lämpligt, genomföra sårbarhetsskanningar och registrera resultaten av skanningarna, med planerade intervall.*

7.2.5.5 Sammanfattningsvis

Föreskrifternas krav på att verksamhetsutövarna ska bevaka sina leverantörer uttrycks på näraliggande sätt i genomförandeförordningen. Kravet på att bevaka NCSC svarar väl mot skyldigheter i genomförandeförordningen att inhämta sådan information som krävs för att utifrån ett allriskperspektiv kunna upprätthålla lämplig nivå av cybersäkerhet. Det bedöms därför inte vara en belastning utan snarare en förenkling för verksamhetsutövarna att uttryckligen ställa krav på att följa vilken information NCSC tillhandahåller eftersom relevant information på så sätt kan kanaliseras till verksamhetsutövarna på ett samlat sätt.

Föreskrifternas krav på anslutning till ANTS ansluter till motsvarande krav i genomförandeförordningen på att inhämta information om tekniska sårbarheter i sina system. Skillnaden ligger närmast i att det i Sverige finns en utpekad tjänst (ANTS) som tillhandahåller detta. Vad gäller informationsutbyte om hot och

annan information så innebär MISP en plattform för detta och underlättar även den för verksamhetsutövaren. Ett högt antal aktiva deltagare i MISP stärker deltagande verksamhetsutövares tillgång till relevant information.

Skillnaden mellan föreskrifterna och genomförandeförordningens krav på omvärldsbevakning kan sammanfattningsvis främst ses följa av:

- hur de har strukturerats – det vill säga om de samlats som i föreskrifterna eller omhändertagits i samband med specifika säkerhetsåtgärder, och
- förekomsten i Sverige av etablerade och namngivna tjänster för inhämtning av tekniska sårbarheter i system respektive informationsutbyte.

De faktiska skillnaderna i sak bedöms som begränsade.

7.2.6 Informationsklassning (3 kap. 11 §)

7.2.6.1 Föreskrifterna

För att identifiera vilka konsekvenser bristande cybersäkerhet kan få för information som behandlas i system, det vill säga de digitala uppgifter som avses i cybersäkerhetslagen 1 kap. 2 § p. 16 c), ska verksamhetsutövaren säkerställa att informationen värderas utifrån vilken nivå av skydd informationen behöver avseende konfidentialitet, riktighet inklusive autenticitet, och tillgänglighet.

Föreskriftskraven innebär att verksamhetsutövaren behöver analysera vilken typ av skydd och vilken nivå av skydd som informationen som behandlas i system behöver. Den närmare utformningen av hur informationsklassningen ska gå till överlåts till verksamhetsutövaren men av de allmänna råden framgår att verksamhetsutövaren bör arbeta strukturerat med stöd av fastställda kriterier och nivåer. Verksamhetsutövaren bör även säkerställa en nära anknytning till motsvarande arbete med riskhantering.

7.2.6.2 NIS2-direktivet

Medlemsstaterna ska enligt artikel 21 p. 1 st. 1 *säkerställa att väsentliga och viktiga entiteter vidtar lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och för att förhindra eller minimera incidenters påverkan på mottagarna av deras tjänster och på andra tjänster.*

Av st. 2 i samma artikel framgår att detta ska ske *med beaktande av de senaste, och i tillämpliga fall, relevanta europeiska och internationella standarder samt genomförande-kostnaderna, ska de åtgärder som avses i första stycket säkerställa en nivå på säkerheten i nätverks- och informationssystem som är lämplig i förhållande till den föreliggande risken.*

Säkerhetsåtgärderna ska enligt artikel 21 p. 2 i) minst inbegripa *tillgångsförvaltning.*

7.2.6.3 Cybersäkerhetslagen

Enligt cybersäkerhetslagen 2 kap. 3 § *ska verksamhetsutövare vidta lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att skydda nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och systemens fysiska miljö mot incidenter (säkerhetsåtgärder).*

Säkerhetsåtgärderna ska utgå från ett allriskperspektiv och säkerställa en nivå på säkerheten i nätverks- och informationssystemen som är lämplig i förhållande till risken.

Även lagen ställer krav på tillgångsförvaltning men det specificeras inte närmare vad som ingår.

7.2.6.4 Genomförandeförordningen

Genomförandeförordningen konkretiserar kraven på hur artikel 21 p. 2 ska genomföras, det vill säga vilka tekniska, driftsrelaterade, organisatoriska och fysiska säkerhetsåtgärder som minst ska vidtas.

Vad som ska ingå i tillgångsförvaltning specificeras närmare i p. 12 och när det gäller klassificering av tillgångar framgår att de berörda entiteterna ska *fastställa klassificeringsnivåerna för alla tillgångar, inbegripet information, som omfattas av deras nätverks- och informationssystem för den skyddsnivå som krävs.*

Detta konkretiseras ytterligare med krav på att:

(a) Fastställa ett system med klassificeringsnivåer för tillgångar.

(b) Tilldela alla tillgångar en klassificeringsnivå baserat på krav avseende konfidentialitet, riktighet, autenticitet och tillgänglighet, för att ange vilket skydd som krävs mot bakgrund av tillgångarnas känslighet, kritikalitet, risk och affärsvärde.

(c) Anpassa tillgänglighetskraven för tillgångarna till de leverans- och återställningsmål som fastställs i deras driftskontinuitets- och katastrofplaner.

Det framgår även att klassificeringsnivåer ska regelbundet ses över och uppdateras när så är lämpligt.

Vad som närmare avses med tillgångar specificeras inte i genomförandeförordningen men, det inom cybersäkerhetsarbete etablerade begreppet, informationstillgångar brukar beskrivas som organisationens information och de resurser som behandlar informationen, exempelvis genom att ta emot, lagra, bearbeta, visa eller kommunicera den.

7.2.6.5 Sammanfattningsvis

Kunskap om vilka konsekvenser bristande cybersäkerhet avseende konfidentialitet, riktighet inklusive autenticitet, och tillgänglighet kan få för information som behandlas i system utgör en grundförutsättning för att kunna välja och utforma lämpliga och proportionella säkerhetsåtgärder. Ett behov av att kunna garantera en hög grad av tillgänglighet till sådan information kräver andra säkerhetsåtgärder än exempelvis ett grundläggande behov av riktighet. Genom informationsklassningen säkerställs förmåga att identifiera rätt nivå på säkerhetsåtgärderna, det vill säga undvika både för mycket säkerhet (vilket kan bli onödigt kostsamt) och för lite säkerhet (vilket kan innebära ökad risk för incidenter).

Genomförandeförordningens krav på klassificering av tillgångar bedöms som något mer omfattande och detaljerade än motsvarande krav i föreskrifterna.

7.2.7 Riskhantering (3 kap. 12–13 §§)

7.2.7.1 Föreskrifterna

För att identifiera vilka lämpliga och proportionella säkerhetsåtgärder som ska genomföras i den digitala miljön ska verksamhetsutövaren säkerställa att risker identifieras, analyseras och värderas utifrån konsekvens och sannolikhet.

Genom föreskriftskravet på att i detta beakta såväl den digitala miljöns arkitektur som resultatet av informationsklassning och omvärldsbevakning säkerställs att verksamhetsutövaren i sitt arbete med riskhantering omhändertar:

- den digitala miljöns särskilda förutsättningar, exempelvis vad och hur mycket som är utkontrakterat,
- skyddsvärdet hos informationen som behandlas i systemen, samt
- hot, risker, legala krav, tekniska lösningar med mera.

Föreskrifternas krav innebär att verksamhetsutövaren, precis som vid informationsklassning, ska arbeta strukturerat genom att värdera risker utifrån kriterier och nivåer.

Risker ska värderas för all informationsbehandling i system, hela den digitala miljön respektive för både enskilda system och segment i verksamhetsutövarens interna digitala miljö.

Till detta kommer krav att verksamhetsutövaren ska värdera risker inför utkontraktering.

I föreskrifterna ställs även krav på att valet av säkerhetsåtgärder ska utgå från resultatet av riskanalysen och verksamhetsutövarens riskacceptans. Hur risker hanteras med olika säkerhetsåtgärder ska dokumenteras i en åtgärdsplan.

7.2.7.2 NIS2-direktivet

Av artikel 21 p. 2 a) framgår att de åtgärder som ska vidtas ska minst inbegripa strategier för riskanalys och säkerheten i nätverks- och informationssystem.

7.2.7.3 Cybersäkerhetslagen

Motsvarande krav på strategi för riskanalys finns i cybersäkerhetslagens 2 kap. 3 § st. 2 p. 1. Av författningskommentaren framgår att strategierna *kan exempelvis utformas som rutiner. Riskanalysen ska ligga till grund för valet av säkerhetsåtgärder. Verksamhetsutövaren bör bland annat ta hänsyn till att det finns olika modeller för riskanalys och att flera riskanalyser kan vara nödvändiga för att lagens krav ska anses vara uppfyllda.*[25]

7.2.7.4 Genomförandeförordningen

Kravställningen i genomförandeförordningen avseende riskhantering är förhållandevis detaljerad och innehåller bland annat krav på att berörda entiteter ska:

(a) följa en riskhanteringsmetod,
(b) fastställa risktoleransnivån i enlighet med de berörda entiteternas riskbenägenhet,
(c) fastställa och upprätthålla relevanta riskkriterier,
(d) i enlighet med en allriskansats identifiera och dokumentera riskerna för säkerheten i nätverks- och informationssystem, i synnerhet i förhållande till tredje parter och när det gäller risker som kan leda till störningar vad gäller tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten för nätverks- och informationssystemen, inbegripet identifiering av felkritiska systemdelar (SPOF),
(e) analysera riskerna för säkerheten i nätverks- och informationssystem, inklusive hot, sannolikhet, konsekvenser och risknivå, med beaktande av underrättelser om cyberhot och sårbarheter,
(f) bedöma de identifierade riskerna baserat på riskkriterierna,
(g) identifiera och prioritera lämpliga riskhanteringsalternativ och åtgärder,
(h) kontinuerligt övervaka genomförandet av riskhanteringsåtgärderna,
(i) identifiera vem som har ansvaret för riskhanteringsåtgärderna och när dessa bör genomföras,
(j) på ett begripligt sätt dokumentera de valda riskhanteringsåtgärderna i en riskhanteringsplan, liksom skälen till att kvarstående risker godtas.

[25] Prop. 2025/26:28 s. 244

Av genomförandeförordningen framgår att bland annat klassificeringen av tillgångar ska utgöra underlag i arbetet och att riskbedömningen ska uppdateras regelbundet eller efter betydande förändringar av driften eller riskerna.

7.2.7.5 Sammanfattningsvis

Föreskriftskraven bedöms i stort sett ligga i linje med kraven i genomförandeförordningen. Kravet i allmänna råd på att beakta aggregering och ackumulering av information har inte någon direkt motsvarighet i genomförandeförordningen men motiveras av att sådana risker i ett starkt digitaliserat samhälle är centrala att beakta.

7.2.8 Kontinuitetshantering (3 kap. 14 §)

7.2.8.1 Föreskrifterna

Av föreskrifterna framgår rörande *kontinuitetshantering* att för att kunna bedriva sin verksamhet oavsett vilken störning som produktionsmiljön utsätts för ska verksamhetsutövaren fastställa acceptabla tider för nedsatt funktionalitet och otillgänglighet för informationsbehandling och system. Av föreskrifterna framgår även att verksamhetsutövaren ska säkerställa att behovet av redundanta funktioner bedöms och att övning sker.

Verksamhetsutövaren ska även identifiera och hantera sitt behov av att fastställa acceptabla tider för nedsatt funktionalitet och otillgänglighet och övning i sin utvecklings-, test- och utbildningsmiljö.

I de allmänna råden rekommenderas att verksamhetsutövaren bör fastställa hur och när alternativa arbetssätt ska användas respektive hur och när återgång till ordinarie arbetssätt görs. Dessutom regleras när verksamhetsutövaren bör öva återställning av sektorskritiska system.

7.2.8.2 NIS2-direktivet

Av artikel 21 p. 2 c) framgår att de åtgärder som ska vidtas ska minst inbegripa *driftskontinuitet, exempelvis hantering av säkerhetskopiering och katastrofhantering, och krishantering*.

7.2.8.3 Cybersäkerhetslagen

Motsvarande krav finns i cybersäkerhetslagens 2 kap. 3 § st. 2 p. 3 men där formulerat som krav på *kontinuitetshantering och krishantering*. I propositionen konstateras att uttrycket driftskontinuitet bör ersättas med det mer etablerade uttrycket kontinuitetshantering.[26] Av författningskommentaren framgår att

[26] Prop. 2025/26:28 s. 92

verksamhetsutövaren har en skyldighet att *planera för och ha förmåga att upprätthålla sin verksamhet på en tolerabel nivå oavsett vilken störning den utsätts för eller om en kris inträffar. Verksamhetsutövaren bör bland annat överväga vilken säkerhetskopiering som krävs för detta och hur arbetet ska bedrivas för att minska störningen i verksamheten.*[27]

Som ytterligare exempel på sådana konsekvenser av störningar som skulle behöva hanteras inom ramen för kontinuitetshantering och krishantering nämns i förarbetena att personalen inte kan komma till arbetet, att lokalerna inte går att använda, att strömavbrott inträffar eller att leveranser av viktiga varor och tjänster inte når verksamhetsutövaren.[28]

7.2.8.4 Genomförandeförordningen

I p. 4.1 specificeras att de berörda entiteterna ska fastställa och upprätthålla en driftskontinuitets- och katastrofplan att använda vid incidenter. De berörda entiteternas drift ska återställas i enlighet med driftskontinuitets- och katastrofplanen och planen ska baseras på resultaten av den riskbedömning som utförts i enlighet med p. 2.1 i genomförandeförordningen. Planen ska, när så är lämpligt, innehålla

(a) ändamål, tillämpningsområde och målgrupp,
(b) roller och ansvarsområden,
(c) viktiga kontakter och (interna och externa) kommunikationskanaler,
(d) villkor för aktivering och avaktivering av planen,
(e) ordningsföljden för återställande av driften,
(f) återställningsplaner för olika delar av driften, inklusive återställningsmål,
(g) resurser som krävs, inklusive säkerhetskopior och redundans, och.
(h) återläsning och återupptagande av verksamhet från tillfälliga åtgärder.

Det framgår även i p. 4.1.3 att de berörda entiteterna *ska göra en konsekvensanalys för att bedöma de potentiella konsekvenser som allvarliga störningar har för deras verksamhet och, baserat på konsekvensanalysens resultat, fastställa kontinuitetskrav för sina nätverks- och informationssystem.*

Vidare framgår i p. 4.1.4 att övning ska ske. *Driftskontinuitetsplanen och katastrofplanen ska testas, ses över och, när så är lämpligt, uppdateras med planerade intervall och efter betydande incidenter eller betydande ändringar av driften eller riskerna. De berörda entiteterna ska säkerställa att planerna införlivar lärdomarna från sådana tester.*

[27] Prop. 2025/26:28 s. 244
[28] Prop. 2025/26:28 s. 93

Krav på redundant funktionalitet ställs i p. 4.2 där särskilt 4.2.1 och 4.2.4 är av intresse vid en jämförelse med föreskriftskraven.

4.2.1. De berörda entiteterna ska bevara säkerhetskopior av data och *tillhandahålla tillräckliga tillgängliga resurser, inklusive anläggningar, nätverks- och informationssystem och personal, för att säkerställa en lämplig nivå av redundans.*

4.2.4. Baserat på resultaten av den riskbedömning som utförts i enlighet med p. 2.1 och driftskontinuitetsplanen ska de berörda entiteterna säkerställa tillräckliga resurser genom åtminstone partiell redundans på följande områden

(a) nätverks- och informationssystem,
(b) tillgångar, inklusive anläggningar, utrustning och materiel,
(c) personal med det ansvar, de befogenheter och den kompetens som krävs, och
(d) ändamålsenliga kommunikationskanaler.

7.2.8.5 Sammanfattningsvis

Föreskriftskraven ligger i linje med motsvarande krav i genomförande-förordningen. I delar är genomförandeförordningens krav mer detaljerade.

7.2.9 Incidenthantering (3 kap. 15 §)

7.2.9.1 Föreskrifterna

För att minimera konsekvenserna av incidenter och tillbud ska verksamhetsutövaren säkerställa att incidenter kan upptäckas, analyseras och begränsas i omfattning. Verksamhetsutövaren ska kunna återhämta sig från och lära sig av incidenter i den digitala miljön.

Av de allmänna råden i föreskrifterna framgår att verksamhetsutövaren bör göra det enkelt att anmäla incidenter och tillbud, att externa krav på rapportering och informationsskyldighet omhändertas inom incidenthanteringen, att risken för att ytterligare incidenter inträffar beaktas vid valet av åtgärder som ska begränsa omfattning och konsekvenser av en inträffad incident samt att verksamhetsutövaren bör ha kontakt med berörda leverantörer och utreda grundorsaker.

7.2.9.2 NIS2-direktivet

Av artikel 21 p. 2 b) framgår att de åtgärder som ska vidtas ska minst inbegripa *incidenthantering*. Incidenthantering definieras i artikel 6 p. 8 som *alla åtgärder och förfaranden som syftar till att förebygga, upptäcka, analysera, begränsa eller reagera på och återhämta sig från en incident.*

7.2.9.3 Cybersäkerhetslagen

Motsvarande krav på incidenthantering finns i cybersäkerhetslagens 2 kap. 3 § st. 2 p. 2. Begreppet definieras dock inte i lagen utan förklaras istället i författningskommentaren.[29]

7.2.9.4 Genomförandeförordningen

Genomförandeförordningen reglerar incidenthantering närmare i p. 3. Här ingår krav på *incidenthanteringsstrategi* och vad en sådan ska innehålla rörande bland annat roller och ansvarsområden, *övervakning och loggning*, *händelserapportering,* incidenthantering och *efterhandsgranskning efter incidenter*. Kraven är detaljerade i samtliga skeden och reglerar bland annat krav på att i incidenthanteringsstrategin specificera vilka dokument som ska användas i samband med upptäckt och åtgärdande, att införa en enkel mekanism för att förenkla för anställda, leverantörer och kunder att rapportera misstänkta händelser, vilka stadier incidenthanteringsförfaranden ska innehålla och att de ska testa samt krav på att om möjligt identifiera grundorsaker och dokumentera lärdomar.

7.2.9.5 Sammanfattningsvis

Föreskrifterna och genomförandeförordningen reglerar samma områden, det vill säga upptäcka, analysera, begränsa, återhämta sig från och lära sig av incidenter men kraven i genomförandeförordningen är betydligt mer detaljerade.

7.2.10 Krishantering (3 kap. 16)

7.2.10.1 Föreskrifterna

För att minimera konsekvenser av incidenter som inte kan omhändertas genom incidenthantering ska verksamhetsutövaren fastställa hur roller, ansvarsområden och befogenheter fördelas under en kris samt hur kriskommunikation ska genomföras.

Av föreskrifterna framgår även att verksamhetsutövaren ska identifiera och hantera behovet av tillgång till system för intern och extern kriskommunikation.

Enligt de allmänna råden bör verksamhetsutövaren använda etablerad stabsmetodik och struktur samt öva sin krishantering inklusive användning av det webbaserade informationsdelningssystemet WIS som tillhandahålls av Myndigheten för civilt försvar.

[29] Prop. 2025/26:28 s. 244

7.2.10.1 NIS2-direktivet

Av artikel 21 p. 2 c) framgår att de åtgärder som ska vidtas ska minst inbegripa *driftskontinuitet, exempelvis hantering av säkerhetskopiering och katastrofhantering, och krishantering.*

7.2.10.2 Cybersäkerhetslagen

Motsvarande krav finns i cybersäkerhetslagens 2 kap. 3 § st. 2 p. 3 men där formulerat som krav på *kontinuitetshantering och krishantering.* I propositionen konstateras att uttrycket driftskontinuitet bör ersättas med det mer etablerade uttrycket kontinuitetshantering.[30] Av författningskommentaren framgår att verksamhetsutövaren har en skyldighet att *planera för och ha förmåga att upprätthålla sin verksamhet på en tolerabel nivå oavsett vilken störning den utsätts för eller om en kris inträffar. Verksamhetsutövaren bör bland annat överväga vilken säkerhetskopiering som krävs för detta och hur arbetet ska bedrivas för att minska störningen i verksamheten.*[31]

Som ytterligare exempel på sådana konsekvenser av störningar som skulle behöva hanteras inom ramen för kontinuitetshantering och krishantering nämns i förarbetena att personalen inte kan komma till arbetet, att lokalerna inte går att använda, att strömavbrott inträffar eller att leveranser av viktiga varor och tjänster inte når verksamhetsutövaren.[32]

7.2.10.3 Genomförandeförordningen

I p. 4.1 specificeras att de berörda entiteterna ska fastställa och upprätthålla en driftskontinuitets- och katastrofplan att använda vid incidenter. De berörda entiteternas drift ska återställas i enlighet med driftskontinuitets- och katastrofplanen och planen ska baseras på resultaten av den riskbedömning som utförts i enlighet med p. 2.1 i genomförandeförordningen. För mer om driftskontinuitets- och katastrofplanen se ovan avsnitt 7.2.8.

När det gäller krishantering så framgår även av p. 4.3 att de berörda entiteterna ska införa en krishanteringsprocess och att denna process åtminstone omfattar:

(a) Roller och ansvarsområden för personal och, när så är lämpligt, leverantörer och tjänsteleverantörer, där rollfördelningen i krissituationer specificeras, inklusive specifika steg att följa.
(b) Ändamålsenliga kommunikationsmedel mellan de berörda entiteterna och de berörda behöriga myndigheterna.

[30] Prop. 2025/26:28 s. 92
[31] Prop. 2025/26:28 s. 244
[32] Prop. 2025/26:28 s. 93

(c) Tillämpning av ändamålsenliga åtgärder för att säkerställa att säkerheten i nätverks- och informationssystem upprätthålls i krissituationer.

Vid tillämpning av led b ska informationsflödet mellan de berörda entiteterna och de berörda behöriga myndigheterna innefatta både obligatorisk kommunikation, såsom incidentrapporter och tillhörande tidslinjer, och kommunikation som inte är obligatorisk.

7.2.10.4 Sammanfattningsvis

Föreskriftskraven ligger i linje med motsvarande krav i genomförande-förordningen. I delar är genomförandeförordningens krav mer detaljerade.

7.2.11 Uppföljning och utvärdering (3 kap. 17 §)

7.2.11.1 Föreskrifterna

För att kunna bedöma effektiviteten av genomförda säkerhetsåtgärder ska verksamhetsutövaren säkerställa att införda säkerhetsåtgärders lämplighet och proportionalitet i förhållande till externa krav, interna behov och risk, vid behov men minst årligen, följs upp och utvärderas.

Av de allmänna råden framgår att verksamhetsutövaren bör säkerställa att etablerade metoder för uppföljning och utvärdering används och att sådan uppföljning och utvärdering bland annat används vid förändrade hot, en säkerhetsåtgärd införs, vid omorganisation och efter betydande incidenter. Uppföljning och utvärdering av cybersäkerhetsarbetet bör omfatta hur ledningens mål och inriktning efterlevs och om interna regler, arbetssätt och stöd motsvarar behoven. Även brister och oklarheter avseende tilldelade mandat, resurser och arbetsuppgifter samt bristande kompetensförsörjning bör bedömas.

7.2.11.2 NIS2-direktivet

Av artikel 21 p. 2 f) framgår att de åtgärder som ska vidtas ska minst inbegripa *strategier och förfaranden för att bedöma effektiviteten i riskhanteringsåtgärderna för cybersäkerhet.*

7.2.11.3 Cybersäkerhetslagen

Motsvarande krav finns i cybersäkerhetslagens 2 kap. 3 § st. 2 p. 6 om *strategier och förfaranden för att bedöma effektiviteten i säkerhetsåtgärderna*. Av författnings-kommentaren framgår att punkten innebär att *verksamhetsutövaren ska ha strategier och förfaranden för att utvärdera sådana säkerhetsåtgärder som har vidtagits. Detta innebär att verksamhetsutövaren ska vidta åtgärder, i form av exempelvis framtagande av interna regler och arbetssätt, för att följa upp att de åtgärder som har vidtagits är lämpliga och tillräckliga. Det bör*

även vara tydligt vem som ansvarar för att utvärdering sker och på vilket sätt utvärdering ska ske.[33]

7.2.11.4 Genomförandeförordningen

Uppföljning och utvärdering av säkerhetsåtgärder aktualiseras såväl i p. 2 inom ramen för *strategier för riskhantering* som i p. 7 för *strategier och förfaranden för att bedöma effektiviteten i riskhanteringsåtgärder för cybersäkerhet.*

Av p. 2.2 framgår att de berörda entiteterna regelbundet ska granska efterlevnaden av sina strategier för säkerhet i nätverk- och informationssystem och att ledningsorganet regelbundet ska informeras om nivån av säkerhet. Det ska bland annat finnas ett effektivt system för rapportering om efterlevnad. Detta ska *vara ändamålsenligt i förhållande till deras strukturer, driftsförhållanden och hotbilder. Rapporteringssystemet ska kunna ge ledningsorganen en väl underbyggd bild av det rådande läget i fråga om de berörda entiteternas riskhantering.* Övervakningen ska göras med planerade intervall och när betydande incidenter eller betydande förändringar av driften eller riskerna inträffar.

I p. 2.3 regleras när och hur oberoende granskning av nätverks- och informationssäkerheten ska göras. De berörda entiteterna ska *på ett oberoende sätt granska sitt tillvägagångssätt för att hantera säkerheten i nätverks-och informationssystem och sitt genomförande, inbegripet personer, processer och teknik.* Krav ställs bland annat på vilken kometens de som utför granskningen ska ha och hur deras opartiskhet ska garanteras. Vidare framgår att resultaten av de oberoende granskningarna inklusive övervakning och mätning enligt p. 7 ska rapporteras till ledningsorganen samt att korrigerande åtgärder ska vidtas eller kvarstående risk godtas i enlighet med kriterier för riskacceptans. De oberoende granskningarna ska, liksom granskningen av efterlevnaden av strategierna för säkerhet i nätverk- och informationssystem, genomföras med planerade intervall och när betydande incidenter eller betydande förändringar av driften eller riskerna inträffar.

I p. 7.1 framgår att berörda entiteter ska *fastställa, införa och tillämpa en strategi och förfaranden för att bedöma om de riskhanteringsåtgärder för cybersäkerhet som vidtagits av den berörda entiteten genomförs och upprätthålls på ett effektivt sätt.*

Vidare framgår att dessa strategier och förfaranden ska beakta resultaten av riskbedömning och betydande incidenter. Det åligger berörda entiteter att fastställa

(a) vilka riskhanteringsåtgärder för cybersäkerhet som ska övervakas och mätas, inklusive processer och kontroller,

(b) metoderna för övervakning, mätning, analys och utvärdering, såsom tillämpligt, för att säkerställa giltiga resultat,

[33] Prop. 2025/26:28 s. 245

(c) när övervakning och mätning ska utföras,

(d) vem som har ansvaret för övervakning och mätning av effektiviteten i riskhanteringsåtgärderna för cybersäkerhet,

(e) när resultaten från övervakning och mätning ska analyseras och utvärderas, och

(f) vem som ska analysera och utvärdera dessa resultat.

Strategierna och förfarandena ska se över och uppdateras med planerade intervall och när betydande incidenter eller betydande förändringar av driften eller riskerna inträffar.

7.2.11.5 Sammanfattningsvis

Föreskrifternas krav skulle kunna beskrivas som en kombination av p. 2.2, p. 2.3 och p. 7 i genomförandeförordningen men är utformade på en mer övergripande nivå som ger verksamhetsutövarna mer utrymme att själva utforma sitt arbete med att följa upp och utvärdera sina säkerhetsåtgärder.

7.3 Tekniska och driftrelaterade säkerhetsåtgärder i kapitel 4

7.3.1 Förvärv av system och utkontraktering av informationsbehandling (4 kap. 1–3 §§)

7.3.1.1 Föreskrifterna

För att säkerställa att verksamhet kan bedrivas med en tillräcklig nivå av cybersäkerhet ska verksamhetsutövaren innan förvärv av system eller inför utkontraktering av informationsbehandling utvärdera potentiella leverantörer.

I föreskrifterna ställs även krav på att verksamhetsutövaren, innan avtal och överenskommelse tecknas om förvärv och utkontraktering, ska ha bedömt att leverantören kommer att kunna uppfylla ställda krav på cybersäkerhet under hela avtalstiden.

Till detta kommer krav på att identifiera och hantera behovet av att välja certifierade system och tjänster samt att säkerställa att lämpliga och proportionella säkerhetsåtgärder kan genomföras och förvaltas över tid innan system förvärvas eller informationsbehandling utkontrakteras.

I de allmänna råden konkretiseras att verksamhetsutövaren bör säkerställa att informationsklassning är genomförd och risker omhändertagna innan avtal och överenskommelser om utkontraktering av informationsbehandling tecknas. Vidare

att ett avtal om utkontraktering bör reglera sådant som ansvarsfördelning, kompetenskrav, informationsdelning, övning, uppföljning med mera.

7.3.1.2 NIS2-direktivet

Av artikel 21 p.2 d) framgår att de åtgärder som ska vidtas ska minst inbegripa *säkerhet i leveranskedjan* och av samma artikel 21 p. 2 e) följer krav på *säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem, inbegripet hantering av sårbarheter och sårbarhetsinformation.*

7.3.1.3 Cybersäkerhetslagen

Motsvarande krav finns i cybersäkerhetslagens 2 kap. 3 § st. 2 p. 4 om *säkerhet i leveranskedjan* och p. 5 om *säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem.*

Av författningskommentaren till p. 4 framgår att säkerhet i leveranskedjan, bland annat rör förbindelserna mellan verksamhetsutövare och deras direkta leverantörer eller tjänsteleverantörer. *Verksamhetsutövaren bör bland annat beakta sårbarheter kopplade till varje direktleverantör och tjänsteleverantör samt kvaliteten på leverantörernas produkter. Verksamhetsutövaren kan även behöva beakta risker som härrör från leverantörer på andra nivåer för att anses uppfylla lagens krav på säkerhetsåtgärder. Resultatet av samordnade säkerhetsriskbedömningar på unionsnivå av kritiska leveranskedjor bör också beaktas. Det får avgöras i varje enskilt fall om en verksamhetsutövare har vidtagit tillräckliga åtgärder i fråga om säkerhet i leveranskedjan, inbegripet åtgärder för att revidera avtal.* [34]

När det gäller p. 5 om förvärv, utveckling och underhåll av nätverks- och informationssystem bör enligt författningskommentaren verksamhetsutövaren bland annat *ta hänsyn till vilka risker som ett förvärv av nätverks- eller informationssystem innebär. Bestämmelsen innebär även krav på hantering av sårbarheter och sårbarhetsinformation. Att åtgärderna ska avse säkerhet vid utveckling och underhåll av systemen innebär att verksamhetsutövaren behöver vidta åtgärder för att upprätthålla säkerheten även vid exempelvis utkontraktering och licensiering.*[35]

7.3.1.4 Genomförandeförordningen

När det gäller säkerhet i leveranskedjan specificeras i p. 5.1.1 att de berörda entiteterna ska *fastställa, genomföra och tillämpa en strategi för säkerhet i leveranskedjan som styr relationerna med deras direkta leverantörer och tjänsteleverantörer i syfte att minska de identifierade riskerna för säkerheten i nätverks- och informationssystem. I denna strategi ska de berörda entiteterna identifiera sin roll i leveranskedjan och förmedla den till sina direkta leverantörer och tjänsteleverantörer.*

[34] Prop. 2025/26:28 s. 245
[35] Prop. 2025/26:28 s. 245

Strategin för leveranskedjan som ska tas fram ska enligt p 5.1.2 innehålla kriterier för att välja ut och ingå avtal med leverantörer och tjänsteleverantörer. Kriterierna ska inbegripa:

(a) Leverantörernas och tjänsteleverantörernas cybersäkerhetsrutiner, inklusive deras säkra utvecklingsförfaranden.

(b) Leverantörernas och tjänsteleverantörernas förmåga att uppfylla de berörda entiteternas cybersäkerhetsspecifikationer.

(c) IKT-produkternas och IKT-tjänsternas allmänna kvalitet och resiliens samt de riskhanteringsåtgärder för cybersäkerhet som ingår i dem, inklusive IKT-produkternas och IKT-tjänsternas risknivå och klassificeringsnivå.

(d) De berörda entiteternas förmåga att diversifiera leveranskällor och förhindra inlåsningar till enskilda leverantörer, om tillämpligt.

De avtal som berörda entiteter ingår med leverantörer och tjänsteleverantörer ska enligt p. 5.1.4 innehålla följande:

(a) Cybersäkerhetskrav för leverantörerna eller tjänsteleverantörerna, inklusive krav som rör säkerheten vid förvärv av IKT-tjänster eller IKT-produkter enligt p. 6.1.

(b) Krav som rör medvetenhet, kompetens och utbildning och, när så är lämpligt, certifiering, för leverantörens eller tjänsteleverantörens anställda.

(c) Krav som rör kontroll av bakgrunden för leverantörers och tjänsteleverantörers anställda.

(d) En skyldighet för leverantörer och tjänsteleverantörer att utan onödigt dröjsmål underrätta de berörda entiteterna om incidenter som utgör en risk för säkerheten i dessa entiteters nätverks- och informationssystem.

(e) Rätt att göra revisioner eller erhålla revisionsrapporter.

(f) En skyldighet för leverantörer och tjänsteleverantörer att hantera sårbarheter som utgör en risk för säkerheten i de berörda entiteternas nätverks- och informationssystem.

(g) Krav som rör underentreprenader och, om de berörda entiteterna tillåter underentreprenader, cybersäkerhetskrav för underleverantörer i enlighet med de cybersäkerhetskrav som avses i led a.

(h) Skyldigheter för leverantörer och tjänsteleverantörer vid uppsägning av avtalet, såsom insamling och bortskaffande av de uppgifter som leverantörerna och tjänsteleverantörerna erhållit i utövandet av sina uppgifter.

Av 6.1.1 i genomförandeförordningen framgår att de berörda entiteterna ska *fastställa och genomföra processer för att hantera risker till följd av förvärv av IKT-tjänster eller*

IKT-produkter för komponenter som är kritiska för säkerheten i de berörda entiteternas nätverks- och informationssystem, baserat på den riskbedömning som utförts i enlighet med p. 2.1, från leverantörer eller tjänsteleverantörer under hela deras livscykel.

I p. 6.1.2 specificeras att dessa processer ska omfatta:

(a) Säkerhetskrav som ska tillämpas på de IKT-tjänster eller IKT-produkter som förvärvas.

(b) Krav på säkerhetsuppdateringar under hela livslängden för IKT-tjänsterna eller IKT-produkterna eller krav på att de ska ersättas efter stödperiodens utgång.

(c) Information som beskriver de maskinvaru- och programvarukomponenter som används i IKT-tjänsterna eller IKT-produkterna.

(d) Information som beskriver de cybersäkerhetsfunktioner som IKT-tjänsterna eller IKT-produkterna omfattar och den konfiguration som krävs för en säker drift av dem.

(e) Garantier för att IKT-tjänsterna eller IKT-produkterna uppfyller säkerhetskraven enligt led a.

(g) *Metoder för att validera att de levererade IKT-tjänsterna eller IKT-produkterna uppfyller de angivna säkerhetskraven samt dokumentation av valideringsresultaten.*

Av skäl (17) framgår att verksamhetsutövaren bör *hantera risker till följd av förvärv av IKT-produkter eller IKT-tjänster från leverantörer eller tjänsteleverantörer och bör se till att de får garantier för att de IKT-produkter eller IKT-tjänster som förvärvas uppnår en viss cybersäkerhetsskyddsnivå, t.ex. genom europeiska cybersäkerhetscertifikat och EU-försäkran om överensstämmelse för IKT-produkter eller IKT-tjänster som utfärdats inom ramen för ett europeiskt certifieringssystem för cybersäkerhet.*

7.3.1.5 Sammanfattningsvis

Föreskrifternas krav på att utvärdera leverantörer innan förvärv och utkontraktering ställs även i genomförandeförordningen men med ytterligare detaljeringsgrad.

När det gäller kravet på att identifiera och hantera behovet av att kravställa certifiering i föreskrifterna motsvarar det genomförandeförordningens krav i p. 6.1.2 (e) enligt vilken processerna ska innehålla garantier för säkerhetskrav, att sådana garantier kan utgöras av certifiering framgår av skäl (17).

Enligt de allmänna råden bör verksamhetsutövaren säkerställa att avtal eller överenskommelser reglerar vissa aspekter. I genomförandeförordningen är ungefär samma krav obligatoriska.

Sammanfattningsvis reglerar inte föreskrifterna mer än genomförandeförordningen. Däremot är föreskriftskraven på en mer övergripande nivå och lämnar över mer till verksamhetsutövarens att själv utforma än vad genomförandeförordningen gör.

7.3.2 Utveckling, underhåll och avveckling av system (4 kap. 4–6 §§)

7.3.2.1 Föreskrifterna

För att motverka att sårbarheter uppstår vid utveckling och underhåll av den digitala miljön ska verksamhetsutövaren inför och under utveckling säkerställa att

1. informationsägare och systemägare involveras i arbetet för att identifiera och hantera behov av säkerhetsåtgärder,
2. informationsklassning är genomförd och hålls uppdaterad,
3. riskanalys är genomförd och hålls uppdaterad,
4. åtgärdsplanen hålls uppdaterad, och
5. etablerade metoder för säker utveckling följs.

Dessutom innehåller föreskrifterna krav på vad verksamhetsutövaren ska göra innan ett system driftsätts i den digitala miljön och vad som ska göras för att upprätthålla skyddet för information under avveckling av system. Det handlar bland annat om att kontrollera att nödvändig driftdokumentation finns på plats och att granskningar och säkerhetstester genomförts respektive att risker med avvecklingen har omhändertagits och en åtgärdsplan för avvecklingen tagits fram.

7.3.2.2 NIS2-direktivet

Av artikel 21 p.2 e) framgår att de åtgärder som ska vidtas ska minst inbegripa *säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem, inbegripet hantering av sårbarheter och sårbarhetsinformation.*

7.3.2.3 Cybersäkerhetslagen

Motsvarande krav finns i cybersäkerhetslagens 2 kap. 3 § st. 2 p. 5 om *säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem.*

Av författningskommentaren till p. 5 om förvärv, utveckling och underhåll av nätverks- och informationssystem framgår att verksamhetsutövaren bland annat att åtgärderna om *säkerhet vid utveckling och underhåll av systemen innebär att verksamhetsutövaren behöver vidta åtgärder för att upprätthålla säkerheten även vid exempelvis utkontraktering och licensiering.*[36]

[36] Prop. 2025/26:28 s. 245

7.3.2.4 Genomförandeförordningen

I genomförandeförordningen specificeras närmare krav på en säker utvecklingscykel i p. 6.2. Enligt p. 6.2.1 ska de berörda entiteterna, innan de utvecklar ett nätverks- och informationssystem, inklusive programvara, *fastställa reglerna för en säker utveckling av nätverks- och informationssystem och tillämpa dessa regler när de själva utvecklar nätverks- och informationssystem och när utvecklingen läggs ut på entreprenad. Reglerna ska omfatta alla utvecklingsfaser och inbegripa specifikationer, utformning, utveckling, genomförande och testning.*

Av p. 6.2.1 ställs krav på att de berörda entiteterna ska:

(a) Göra en analys av säkerhetskraven i specifikations- och utformningsfaserna för alla utvecklings- eller inköpsprojekt som genomförs av de berörda entiteterna eller på dessa entiteters vägnar.
(b) Tillämpa principerna för konstruktion av säkra system och säker kodning på allt utvecklingsarbete som rör informationssystem, t.ex. främjande av inbyggd cybersäkerhet och nolltillitsarkitektur.
(c) Fastställa säkerhetskrav för utvecklingsmiljöer.
(d) Fastställa och genomföra processer för säkerhetstester under utvecklingscykeln.
(e) På lämpligt sätt välja ut, skydda och förvalta säkerhetstestdata.
(f) Sanera och anonymisera testdata enligt den riskbedömning som utförts i enlighet med p. 2.1.

Av p. 12.2 framgår vilka krav som ställs på hantering av tillgångar. De berörda entiteterna ska enligt 12.2.1 fastställa, införa och tillämpa en strategi för korrekt hantering av tillgångar, inbegripet information, i enlighet med deras strategi för säkerhet i nätverks- och informationssystem och ska kommunicera denna strategi till alla som använder eller hanterar tillgångar. Denna strategi ska enligt p. 12.2.2:

(a) omfatta hela livscykeln för tillgångarna, inklusive förvärv, användning, lagring, transport och bortskaffande,
(b) omfatta regler för säker användning, säker lagring, säker transport och oåterkallelig radering och förstöring av tillgångarna, och
(c) föreskriva att överföringen ska ske på ett säkert sätt, i enlighet med den typ av tillgång som ska överföras.

När det gäller hantering av tillgångar kan även nämnas p. 12.4 enligt vilken det ställs krav på inventering av tillgångar.

7.3.2.5 Sammanfattningsvis

Föreskrifternas och genomförandeförordningens krav är lite olika utformade. De krav som ställs i föreskrifterna 3 kap. 3 § utgörs förenklat av kontroller av att

relevanta ingångsvärden för utveckling, underhåll och avveckling av system som följer av andra paragrafer i föreskrifterna är uppfyllda inför och under utveckling. Ungefär motsvarande krav, exempelvis rörande klassificering av tillgångar eller riskanalys, följer även av genomförandeförordningen även om de inte direkt kopplas till utveckling och underhåll.

Vad gäller föreskriftskraven i 3 kap. 5–6 §§ på vad som ska göras innan beslut om driftsättning respektive innan avveckling finns motsvarigheter i genomförandeförordningen i både p. 6 och p. 12. I delar är dock genomförandeförordningens krav mer detaljerade och tekniska, exempelvis med regler för säker utveckling med bland annat krav på säker kodning och hantering av testdata.

7.3.3 Driftrelaterad dokumentation (4 kap. 7–9 §§)

7.3.3.1 Föreskrifterna

När det gäller driftrelaterad dokumentation ställer föreskrifterna krav på detta i tre nivåer.

- För att kunna upprätthålla den driftsäkerhet som verksamhetsutövaren behöver ska verksamhetsutövaren säkerställa att det finns uppdaterad *dokumentation över arkitekturen för den digitala miljön*.
- För att verksamhetsutövaren skyndsamt ska kunna omhänderta sårbarheter och incidenter i den digitala miljö och bedöma konsekvenserna för verksamheten ska verksamhetsutövaren säkerställa att det finns en *uppdaterad förteckning över relevant information om den digitala miljön*.
- För att kunna upprätthålla säker drift möjliggöra återställning av system i produktionsmiljön ska verksamhetsutövaren säkerställa att det finns *uppdaterad driftdokumentation för systemen*.

I de allmänna råden specificeras närmare vad dokumentationen över arkitekturen, förteckningen respektive driftdokumentation för systemen bör innehålla. När det gäller arkitekturen handlar det bland annat om hur den digitala miljön är indelad, informationsflöden och vilken informationsbehandling som är utkontrakterad. Förteckningen bör enligt de allmänna råden bland annat innehålla relevanta kontaktuppgifter till systemägare och informationsägare, vilka system som används till vad och kontaktuppgifter till berörda leverantörer. Systemens driftdokumentation bör bland annat innehålla uppgifter vad systemen används till, acceptabla tider för nedsatt funktionalitet och otillgänglighet, mjukvara och hårdvara, kontaktuppgifter till systemägare och informationsägare samt hur det återställs.

7.3.3.2 NIS2-direktivet

Av artikel 21 p. 2 i) framgår att de åtgärder som ska vidtas ska minst inbegripa *personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning.*

7.3.3.3 Cybersäkerhetslagen

Motsvarande krav finns i cybersäkerhetslagens 2 kap. 3 § st. 2 p. 9 om *personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning.*

Innebörden av tillgångsförvaltning förklaras inte närmare i propositionen.

7.3.3.4 Genomförandeförordningen

Av p. 12.4 i genomförandeförordningen ställs krav på inventering av tillgångar. Kravet innebär att de berörda entiteterna *ska utveckla och upprätthålla en fullständig, tillförlitlig, uppdaterad och konsekvent inventering av sina tillgångar. De ska registrera ändringar av poster i inventeringen på ett spårbart sätt.*

Detaljnivån i denna inventering ska enligt p. 12.4.2 anpassas till den berörda entitetens behov men omfatta följande:

(a) En förteckning över drift och tjänster och en beskrivning av dessa.
(b) En förteckning över nätverks- och informationssystem och andra tillhörande tillgångar som stöder de berörda entiteternas drift och tjänster.

De berörda entiteterna ska enligt p. 12.4.3. regelbundet se över och uppdatera inventeringen och sina tillgångar och dokumentera ändringshistoriken.

Av p. 5.2 framgår också att den berörda entiteten ska ha en förteckning över leverantörer och tjänsteleverantörer vilket ska omfatta:

(a) Kontaktpunkter för varje direkt leverantör och tjänsteleverantör.
(b) En förteckning över IKT-produkter, IKT-tjänster och IKT-processer som den direkta leverantören eller tjänsteleverantören tillhandahåller den berörda entiteten.

Till detta kan läggas kravet i p. 6.7 om nätverkssäkerhet där de berörda entiteterna enligt p. 6.7.1 *ska vidta ändamålsenliga åtgärder för att skydda sina nätverks- och informationssystem mot cyberhot* och p. 6.7.2 som tydliggör att de berörda entiteterna vid tillämpning av p. 6.7.1 ska *(a) dokumentera nätverkets arkitektur på ett begripligt och uppdaterat sätt.*

7.3.3.5 Sammanfattningsvis

Föreskrifternas krav motsvarar ungefär genomförandeförordningens krav på inventering och förteckning. De allmänna råden konkretiserar visserligen delvis innehållet på en större detaljnivå än i genomförandeförordningen. I och med att

det handlar om bör-krav torde dock inte den ökade detaljnivån utgöra någon större ytterligare börda för berörda verksamhetsutövare.

7.3.4 Segmentering (4 kap. 10–11 §§)

7.3.4.1 Föreskrifterna

För att minimera konsekvenser av incidenter orsakade av angrepp mot och misstag i produktionsmiljön ska verksamhetsutövaren säkerställa att den delas in i segment för att förhindra spridning av incidenten.

I föreskrifterna specificeras vilka system i produktionsmiljön som ska placeras i separata segment. Det handlar om:

1. *system som används för gästnätverk,*
2. *system i den interna digitala miljön som sammankopplas med system hos leverantör,*
3. *system som tillhandahåller externa tjänster, och*
4. *system som innehåller sårbarheter som inte kan omhändertas på ett tillfredställande sätt.*

Till detta kommer krav på att identifiera och hantera behovet av ot-segment och ytterligare segmentering. Liksom att säkerställa utveckling, test och utbildning som kan påverka säkerheten i produktionsmiljöns it-segment bedrivs i en från produktionsmiljön avskild utvecklings-, test- respektive utbildningsmiljö.

I de allmänna råden specificeras ytterligare system som bör placeras i separata segment.

7.3.4.2 NIS2-direktivet

Av artikel 21 p.2 e) framgår att de åtgärder som ska vidtas ska minst inbegripa *säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem, inbegripet hantering av sårbarheter och sårbarhetsinformation*.

7.3.4.3 Cybersäkerhetslagen

Motsvarande krav finns i cybersäkerhetslagens 2 kap. 3 § st. 2 p. 4 om *säkerhet i leveranskedjan* och p. 5 om *säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem*.

7.3.4.4 Genomförandeförordningen

Av p. 6.8.1 framgår att de berörda entiteterna *ska segmentera system i nätverk eller zoner i enlighet med resultaten från den riskbedömning som avses i p. 2.1. De ska segmentera sina system och nätverk från tredje parters system och nätverk.*

I 6.8.2 specificeras ytterligare hur de berörda entiteterna ska segmentera sina system. Det handlar om exempelvis om att

(a) beakta det funktionella, logiska och fysiska förhållandet, inklusive lokalisering, mellan tillförlitliga system och tjänster,

(b) bevilja åtkomst till ett nätverk eller en zon baserat på en bedömning av dess säkerhetskrav,

(c) förvara system som är kritiska för den berörda entitetens drift eller säkerhet i säkrade zoner,

(d) införa en demilitariserad zon inom sina kommunikationsnät för att säkerställa säker kommunikation från eller till sina nätverk,

(e) begränsa åtkomst och kommunikation mellan och inom zoner till vad som är nödvändigt för de berörda entiteternas drift eller för säkerheten,

(f) separera det särskilda nätverket för administration av nätverks- och informationssystem från de berörda entiteternas nätverk för drift,

(g) segregera kanalerna för nätverksadministration från annan nätverkstrafik, och

(h) separera produktionssystemen för den berörda entitetens tjänster från system som används för utveckling och testning, inklusive säkerhetskopior.

7.3.4.5 Sammanfattningsvis

Föreskrifterna ställer mer begränsade krav på segmentering än genomförandeförordningen. Flera av de krav som ställs i genomförandeförordningen finns dock i föreskrifternas allmänna råd som bör-krav.

7.3.5 Behörighetshantering och autentisering (4 kap. 12–17 §§)

7.3.5.1 Föreskrifterna

För att endast behöriga användare och system ska få åtkomst till olika delar av den digitala miljön ska verksamhetsutövaren säkerställa att behörighetshanteringen fastställer hur digitala identiteter, behörigheter och autentiseringsuppgifter utformas, tilldelas, används, förändras, avslutas och skyddas.

I övrigt ställer föreskrifterna krav på när digitala identiteter ska låsas, blockeras och tas bort, att användare och system inte tilldelas mer behörighet än nödvändig, att systemadministrativ behörighet tilldelas restriktivt, när flerfaktorsautentisering ska användas.

Verksamhetsutövaren ska även identifiera och hantera behovet av att mottagare av externa tjänster ska använda e-legitimation samt att andra ska kunna verifiera verksamhetsutövaren identitet vid kontakt via digitala kanaler.

7.3.5.2 NIS2-direktivet

Av artikel 21 p.2 i) framgår att de åtgärder som ska vidtas ska minst inbegripa *personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning* samt i j) *användning inom entiteten, när så är lämpligt, av lösningar för multifaktorautentisering eller kontinuerlig autentisering, säkrade röst-, video- och textkommunikationer och säkrade nödkommunikationssystem.*

7.3.5.3 Cybersäkerhetslagen

Motsvarande krav finns i cybersäkerhetslagens 2 kap. 3 § st. 2 p. 9 om *personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning* men även i p. 10 om, vid behov, *användning av lösningar för autentisering, säkrade kommunikationer och säkrade nödkommunikationssystem.*

Av författningskommentaren till p. 9 framgår att det i uttrycket åtkomstkontroll ingår sådana funktioner om *syftar till att reglera och kontrollera en användares åtkomst till information och resurser. Det rör sig bland annat om behörighetsstyrning i form av tilldelning, återkallande och hantering av behörigheter samt uppföljning av åtkomst till information och resurser, till exempel genom loggar och andra hjälpmedel.*[37]

I författningskommentaren till p. 10 exemplifieras lösningar för autentisering bland annat som kontroller av en uppgiven identitet vid exempelvis inloggning i ett system.

7.3.5.4 Genomförandeförordningen

Åtkomstkontroll regleras i genomförandeförordningens p. 11. Kraven rör i p. 11.1 strategier för åtkomstkontroll, i p. 11.2 hur åtkomsträttigheter ska hanteras, i p. 11.3 krav på privilegierade konton och systemadministrationskonton, i p. 11.4 systemadministration, i p. 11.5 identifiering, i p. 11.6 autentisering och i p. 11.7 flerfaktorsautentisering.

I detta sammanhang kan även nämnas kravet i p. 6.7.2 (k) enligt vilket de berörda entiteterna inom ramen för nätverkssäkerhet ska *anta en genomförandeplan för införande av internationellt överenskomna och interoperabla moderna standarder för e-postkommunikation för att säkra e-postkommunikationen i syfte att begränsa sårbarheter kopplade till e-postrelaterade hot och fastställa åtgärder för att påskynda ett sådant införande.*

Kraven är genomgående detaljerade.

[37] Prop. 2025/26:28 s. 246

7.3.5.5 Sammanfattningsvis

De krav som ställs i föreskrifterna om behörighetshantering och autentisering ställs även i genomförandeförordningen men ofta på en högre detaljnivå. Vissa av kraven i allmänna råden (det vill säga bör-kraven) utgörs av ska-krav i genomförandeförordningen. Sammanfattningsvis ger föreskrifterna verksamhetsutövarna i dessa delar ett större utrymme för att utforma sin behörighethantering och autentisering på egen hand.

Ett undantag från ovan gäller kravet i föreskrifterna på verksamhetsutövarna om att identifiera och hantera behovet av att andra organisationer och enskilda personer kan verifiera verksamhetsutövaren identitet vid kontakt via digitala kanaler. Syftet med kravet är att minska risken för incidenter där användare av verksamhetsutövarens tjänster vilseleds av angripare och därigenom påverkar verksamhetsutövaren verksamhet. Den här typen av angrepp har vuxit och utgör särskilt en problematik i ett högt digitaliserat samhälle som Sverige där både stora delar av samhällets tjänster i det närmaste bygger helt på digitala kontakter och förutsätter en hög nivå av cybersäkerhet. Kravet innebär inte att alla verksamhetsutövare kommer att införa en sådan funktionalitet som avses men att samtliga ska bedöma behovet av det. Mot denna bakgrund bedöms kravet vara proportionerligt utformat och adressera en typ av angrepp som behöver motverkas för att uppnå hög cybersäkerhet i Sverige. Kravet anknyter till kravet i genomförandeförordningens p. 6.7.2 (k) om att vidta åtgärder för att minska sårbarheter kopplade till e-postrelaterade hot.

7.3.6 Övervakning, säkerhetsloggning och logganalys (4 kap. 18–20 §§)

7.3.6.1 Föreskrifterna

För att kunna upptäcka tekniska fel, intrång och andra brister i cybersäkerheten ska verksamhetsutövaren säkerställa att system och informationsflöden övervakas samt att utredning av fel, intrång och andra brister i cybersäkerheten möjliggörs genom säkerhetsloggning. Säkerhetsloggarna ska skyddas mot obehörig åtkomst och sparas så länge de behövs för att kunna genomföra sådan utredning.

Av föreskrifterna följer även att verksamhetsutövaren ska identifiera och hantera behovet av realtidsövervakning i produktionsmiljön samt vad som, om det inte är uppenbart olämpligt, ska säkerhetsloggas. Det handlar om:

1. obehörig åtkomst och försök till obehörig åtkomst,
2. användning av systemadministrativ behörighet,

3. förändring av konfigurationer i centrala säkerhetsfunktioner och sektorskritiska system,
4. förändring av behörighet för användare och system,
5. åtkomst till information i behov av utökat skydd, samt
6. händelser som upptäckts genom övervakning och indikerar brister i cybersäkerheten.

Här nämns exempelvis obehörig åtkomst och försök till obehörig åtkomst, användning av systemadministrativ behörighet samt förändring av konfigurationer i centrala säkerhetsfunktioner och sektorskritiska system.

Avslutningsvis ställs krav på att säkerhetsloggarna analyseras för att upptäcka och utreda fel, obehörig åtkomst och andra brister i cybersäkerheten samt att en sådan analys görs med lämpligt intervall.

Med säkerhetsloggning avses sådan loggning som görs i säkerhetssyfte, den loggning som verksamhetsutövaren gör i syfte att exempelvis övervaka effektiviteten i sin verksamhet regleras inte i föreskrifterna.

7.3.6.2 NIS2-direktivet

I NIS2-direktivet behandlas inte övervakning och loggning som enskild säkerhetsåtgärd.

7.3.6.3 Cybersäkerhetslagen

Inte heller i cybersäkerhetslagen uttrycks övervakning och loggning som en separat säkerhetsåtgärd i 2 kap. 3 § men det framgår av författningskommentarerna till 2 kap. 3 § p. 9 och p. 10 att loggning exempelvis kan användas både som en del i arbetet med åtkomstkontroll och lösningar för autentisering. [38]

7.3.6.4 Genomförandeförordningen

I genomförandeförordningen ställs krav på loggning i flera olika sammanhang. Det handlar om, under rubriken övervakning och loggning, krav i p. 3.2.1 enligt vilken de berörda entiteterna *ska fastställa förfaranden och använda verktyg för att övervaka och logga aktiviteter på sina nätverks- och informationssystem för att upptäcka händelser som skulle kunna anses som incidenter och vidta åtgärder för att begränsa konsekvenserna*.

Det framgår även i p. 3.2.3 att de berörda entiteterna ska upprätthålla, dokumentera och granska loggar. Listan på vad som ska loggas om det är lämpligt utifrån riskbedömning innehåller 12 olika poster såsom *all privilegierad åtkomst till system och applikationer samt aktiviteter som utförts av administratörskonton* respektive

[38] Prop. 2025/26:28 s. 245f

händelseloggar och loggar från säkerhetsverktyg, såsom antivirusprodukter, intrångsdetekterings-system eller brandväggar.

Enligt p. 3.2.5 ska de berörda entiteterna bevara och säkerhetskopiera loggar under en på förhand fastställd tidsperiod och ska skydda dem från obehörig åtkomst eller obehöriga ändringar.

Krav på granskning av loggar ställs även i samband med bedömning och klassificering av händelser där berörda entiteter enligt p. 3.4.1 och p. 3.4.2 ska bedöma misstänkta händelser för att fastställa om de är incidenter och inom ramen för detta *granska lämpliga loggar för bedömning och klassificering av händelser* respektive införa *en process för korrelering och analys av loggar*.

Till detta kommer även krav på loggning i p. 9.2 (c) vid hanteringen av nycklar med koppling till *kryptografi*, i p. 11.2.2 avseende hantering av *åtkomsträttigheter* och i p. 11.5.2 rörande *identitetshantering*.

7.3.6.5 Sammanfattningsvis

Den största skillnaden mellan kraven i föreskrifterna och genomförande-förordningen avseende övervakning, loggning och logganalys torde vara av strukturell karaktär. I föreskrifterna är kraven samlade under en rubrik medan kraven i genomförandeförordningen är placerade under flera olika rubriker och i anslutning till flera olika säkerhetsåtgärder.

Innehållsmässigt är genomförandeförordningen mer detaljerad. Listan i genomförandeförordningen på vad som, om det är lämpligt, ska loggas utifrån riskbedömning är mer omfattande än motsvarande uppräkning i föreskrifterna. Kravet i föreskrifterna på att logga just de poster som nämns är dock något skarpare eftersom det gäller om det inte är uppenbart olämpligt.

Realtidsövervakning omnämns inte uttryckligen i genomförandeförordningen men det är en metod för att genomföra sådan övervakning som omnämns i p. 3.2.1.

Sammanfattningsvis kan konstateras att kraven i föreskrifterna generellt sett är mer övergripande än kraven på övervakning, loggning och logganalys i genomförande-förordningen. Skillnaderna i styrka rörande kravet på vad som ska loggas bedöms i praktiken vara av mindre betydelse eftersom en riskbedömning torde mycket sällan resultera i att det inte skulle vara lämpligt att logga den typen av händelser som omnämns i föreskrifterna.

7.3.7 Robust och korrekt tid (4 kap. 21 §)

7.3.7.1 Föreskrifterna

För att kunna jämföra säkerhetsloggar vid incidenter som involverar andra organisationer ska verksamhetsutövaren säkerställa att robust och korrekt tid som är översättningsbar till den svenska tillämpningen av koordinerad universell tid, UTC (SP) används i produktionsmiljö.

Av föreskrifterna följer även att verksamhetsutövaren ska identifiera och hantera behovet av att använda sådan robust och korrekt tid även i sin utvecklings-, test- och utbildningsmiljö.

Kravet innebär inte att verksamhetsutövaren behöver använda den svenska tillämpningen av UTC (SP) som tidskälla utan endast att den tidskälla som används kan översättas till den svenska tiden.

7.3.7.2 NIS2-direktivet

I NIS2-direktivet behandlas inte robust och korrekt tid som en separat säkerhetsåtgärd.

7.3.7.3 Cybersäkerhetslagen

Inte heller i cybersäkerhetslagen uttrycks robust och korrekt tid som en separat säkerhetsåtgärd i 2 kap. 3 §.

7.3.7.4 Genomförandeförordningen

Krav på tidskällor ställs i genomförandeförordnigen i p. 3.2.6. Där framgår att de berörda entiteterna i den mån det är genomförbart *ska säkerställa att alla system har synkroniserade tidskällor så att det är möjligt att korrelera loggar mellan system för bedömning av händelser.*

7.3.7.5 Sammanfattningsvis

Av både föreskrifterna och genomförandeförordningen följer att verksamhetsutövaren behöver använda tidskällor för sina system på ett sådant sätt att det går att följa ett händelseförlopp via loggar. Det tillkommande kravet i föreskrifterna rörande möjlighet att översätta den interna tiden till den svenska tillämpningen av koordinerad universell tid, UTC (SP), uppfylls enkelt genom att verksamhetsutövaren dokumenterar vilken relation den interna tiden har till den svenska (exempelvis ”tre timmar före”). Denna översättningsbarhet är av stor betydelse vid utredningen av mer omfattande incidenter som involverar flera verksamhetsutövare.

7.3.8 Skydd mot skadlig kod (4 kap. 22 §)

7.3.8.1 Föreskrifterna

För att skydda system i it-segment mot angrepp med skadlig kod ska verksamhetsutövaren använda mjukvara som ger tillräckligt skydd för systemen där sådan mjukvara finns tillgänglig.

Av de allmänna råden framgår att verksamhetsutövaren bör skydda system i ot-segment där sådan mjukvara finns tillgänglig.

Anledningen till att kraven på skydd av system i it-segment respektive ot-segment skiljer sig åt är ot-segment kan i vissa fall ha sådana uppgifter eller vara utformade på ett sådant sätt att oförsiktig implementering av skydd mot skadlig kod kan påverka funktionaliteten negativt.

7.3.8.2 NIS2-direktivet

I NIS2-direktivet behandlas inte skydd mot skadlig kod som en separat säkerhetsåtgärd men kan sägas ingå i artikel 21 p. 2 b) där det framgår att de åtgärder som ska vidtas ska minst inbegripa *incidenthantering.* Incidenthantering definieras i artikel 6 p. 8 som *alla åtgärder och förfaranden som syftar till att förebygga, upptäcka, analysera, begränsa eller reagera på och återhämta sig från en incident*.

Det har även koppling till kravet i artikel 21 p. 2 e) på *säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem, inbegripet hantering av sårbarheter och sårbarhetsinformation.*

7.3.8.3 Cybersäkerhetslagen

Inte heller cybersäkerhetslagen nämner uttryckligen skydd mot skadlig kod men ställer motsvarande krav på incidenthantering och säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem i 2 kap. 3 § 2 st. 2 p. och 5 p.

7.3.8.4 Genomförandeförordningen

Genomförandeförordningen tar upp *skydd mot sabotageprogram och otillåten programvara* i p. 6.9 i anslutning till *säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem.*

Av p. 6.9.1 framgår att de berörda entiteterna *ska skydda sina nätverks- och informationssystem mot sabotageprogram och otillåten programvara*. Kravet konkretiseras ytterligare i p. 6.9.2 enligt vilken de berörda entiteterna ska *i synnerhet vidta åtgärder för upptäckt eller förhindrande av användning av sabotageprogram eller otillåten programvara. De berörda entiteterna ska, när så är lämpligt, säkerställa att deras nätverks- och informationssystem är utrustade med programvara för upptäckt och åtgärdande, som regelbundet*

uppdateras i enlighet med den riskbedömning som utförts i enlighet med p. 2.1 och avtalen med leverantörerna.

Av p. 3.2.3 (g) om övervakning och loggning följer att loggen, när så är lämpligt, ska inkludera händelseloggar och loggar *från säkerhetsverktyg, såsom antivirusprodukter, intrångsdetekteringssystem eller brandväggar.* Av p. 12.3 (b) framgår bland annat att verksamhetsutövarens strategi för flyttbara medier ska föreskriva *att självexekvering ska avaktiveras från sådana medier och att skanning efter skadlig kod ska ske innan de används på de berörda entiteternas system.*

7.3.8.5 Sammanfattningsvis

Föreskrifternas krav går i linje med genomförandeförordningens men ger verksamhetsutövaren mer flexibilitet vad gäller skyddet av system som är placerade i ot-segment.

7.3.9 Kryptering (4 kap. 23–25 §§)

7.3.9.1 Föreskrifterna

För att skydda information i system mot obehörig åtkomst och obehörig förändring vid överföring mellan och lagring i system ska verksamhetsutövaren identifiera och hantera behovet av att kryptera information i den digitala miljön.

Av föreskrifterna följer även krav på att kryptering används för att *skydda säkerhetsloggar och autentiseringsuppgifter vid överföring i den digitala miljön. Säkerhetsloggar, autentiseringsuppgifter och annan information i behov av utökat skydd ska skyddas med kryptering vid överföring till system utanför den digitala miljön.*

Föreskrifterna ställer dessutom krav på att verksamhetsutövaren, i syfte att försvåra angrepp genom manipulation av översättningen mellan domännamn och ip-adresser i domännamnssystemet (DNS), ska säkerställa *användning av Domain Name System Security Extensions (DNSSEC) för domännamn som verksamhetsutövaren registrerat i DNS.*

Av de allmänna råden framgår att verksamhetsutövaren bör ta fram kriterier för *val och godkännande av krypteringsalgoritmer, krypteringsprotokoll och nyckellängder , samt att fastställa när och hur krypteringsnycklar genereras, distribueras, används, återkallas, skyddas och förstörs.*

7.3.9.2 NIS2-direktivet

Av artikel 21 p. 2 h) framgår att de åtgärder som ska vidtas ska minst inbegripa *strategier och förfaranden för användning av kryptografi och, när så är lämpligt, kryptering.*

7.3.9.3 Cybersäkerhetslagen

Motsvarande krav finns i cybersäkerhetslagens 2 kap. 3 § st. 2 p. 8, *strategier och förfaranden för användning av kryptografi och, när så är lämpligt, kryptering.*

Av författningskommentaren till p. 8 framgår att bestämmelsen bland annat innebär att *verksamhetsutövaren ska göra en bedömning av om kryptering krävs för att upprätthålla säkerheten och vid behov ha strategier och förfaranden för användning av sådan.*

7.3.9.4 Genomförandeförordningen

Av genomförandeförordningen p. 9.1 följer att de berörda entiteterna vid tillämpning av artikel 21.2 h ska *fastställa, införa och tillämpa en strategi och förfaranden för kryptografi, för att säkerställa en ändamålsenlig och effektiv användning av kryptografi för att skydda konfidentialiteten, autenticiteten och integriteten för data i enlighet med de berörda entiteternas klassificering av tillgångar och resultaten av den riskbedömning som utförts i enlighet med p. 2.1.*

Den strategi och de förfaranden som tas fram ska i enlighet med p. 9.2 bland annat fastställa

> *(a) I enlighet med de berörda entiteternas klassificering av tillgångar – typ, styrka och kvalitet när det gäller de kryptografiska åtgärder som krävs för att skydda de berörda entiteternas tillgångar, inklusive data i vila och data vid transitering.*
>
> *(b) Baserat på led a, de protokoll eller protokollfamiljer som ska antas, liksom kryptografiska algoritmer, krypteringsstyrka, kryptografiska lösningar och användningspraxis som ska godkännas och krävas för användning i entiteten, med kryptoföljsamhet när så är lämpligt.*

Till detta kommer i p. 9.2 (c) en uppräkning på tolv metoder som de berörda entiteternas nyckelhantering, när så är lämpligt, bör omfatta, exempelvis hur olika nycklar genereras, hur certifikat utfärdas, hur nycklar distribueras och hur de ändras.

Genomförandeförordningen innehåller även specifika krav på när kryptering ska användas:

Av p. 6.7.1 och p. 6.7.2 (i) framgår rörande nätsäkerhet att de berörda entiteterna ska vidta ändamålsenliga åtgärder för att skydda sina nätverks- och informationssystem mot cyberhot och däribland *upprätta kommunikation mellan separata system endast via tillförlitliga kanaler som är isolerade med användning av logisk, kryptografisk eller fysisk separation från andra kommunikationskanaler och tillhandahålla säkrad identifiering av deras ändpunkter och skydd för kanaldata från ändring eller avslöjande.*

Av p. 11.4 (c) framgår att de berörda entiteterna ska *skydda åtkomsten till system för systemadministration genom autentisering och kryptering.*

Av p. 12.3.2 (d) framgår att strategin för flyttbara medier ska *när så är lämpligt, omfatta åtgärder för användning av kryptografisk teknik för att skydda data på flyttbara lagringsmedier.*

Vad gäller säkerhetsåtgärder rörande DNS så framgår av p. 6.7.2 (l) att berörda entiteter ska tillämpa bästa praxis för DNS-säkerhet, dirigeringssäkerhet och dirigeringshygien för trafik från eller till nätverket.

7.3.9.5 Sammanfattningsvis

Föreskrifternas krav bedöms ligga i linje med motsvarande krav i genomförande-förordningen. I delar är genomförandeförordningens krav mer detaljerade.

7.3.10 Säkerhetskonfigurering (4 kap. 26 §)

7.3.10.1 Föreskrifterna

För att försvåra angrepp mot system ska de konfigureras så att obehörig åtkomst försvåras och cybersäkerheten upprätthålls.

Av föreskrifterna följer även att verksamhetsutövaren ska säkerställa att *förinställda autentiseringsuppgifter byts ut och att funktioner i system som inte behövs tas bort, stängs av eller blockeras och att endast godkända informationsflöden tillåts till, från och inom den digitala miljön.* Till detta kommer krav på att *identifiera och hantera behovet av att endast tillåta installation och användning av på förhand godkänd mjukvara,* det vill säga vitlistning av mjukvara.

Av de allmänna råden följer ytterligare inriktning vad gäller konfigurering rörande kommunikationer mellan klienter, inaktiva sessioner, inhämtande av rekommendationer från leverantören och användningen av standarder samt tekniskt systemstöd.

7.3.10.2 NIS2-direktivet

Av skäl (49) som rör riktlinjerna i de nationella strategierna för cybersäkerhet framgår att riktlinjerna *för cyberhygien utgör grunden för att skydda nätverks- och informationssystemens infrastruktur, maskinvara, programvara och säkerhet för onlinetillämpningar samt affärs- eller slutanvändardata som entiteter förlitar sig på. Riktlinjer för cyberhygien som omfattar en gemensam grundläggande uppsättning rutiner, bland annat uppdateringar av programvara och maskinvara, byte av lösenord, hantering av nya installationer, begränsning av användarkonton på administratörsnivå och säkerhetskopiering av data, möjliggör en proaktiv ram för beredskap samt övergripande säkerhet och trygghet i händelse av incidenter eller cyberhot.*

Av skäl (89) framgår att väsentliga och viktiga entiteter *bör anta ett brett spektrum av grundläggande cyberhygienrutiner, såsom nollförtroende-principer, programuppdateringar,*

enhetskonfiguration, nätverkssegmentering, identitets- och åtkomsthantering eller användar-medvetenhet, anordna utbildning för sin personal och öka medvetenheten om cyberhot, nätfiske eller sociala manipuleringstekniker.

Krav på cyberhygien ställs i artikel 21 p. 2 g) i form av att de åtgärder som vidtas ska minst inbegripa *grundläggande praxis för cyberhygien och utbildning i cybersäkerhet.*

7.3.10.3 Cybersäkerhetslagen

Motsvarande krav på cyberhygien ställs i 2 kap. 3 § p. 7 om grundläggande praxis för cyberhygien och utbildning i cybersäkerhet.

Av författningskommentaren framgår att *kravet på grundläggande praxis för cyberhygien innebär att verksamhetsutövaren ska ha rutiner för bibehållande av hög säkerhet inom exempelvis programuppdateringar, åtkomsthantering och användarmedvetenhet.*[39]

7.3.10.4 Genomförandeförordningen

Konfigurationshantering regleras närmare i genomförandeförordningen p. 6.3 inom ramen för säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem. Enligt p. 6.3.1 ska de berörda entiteterna *vidta ändamålsenliga åtgärder för att fastställa, dokumentera, genomföra och övervaka konfigurationer, inklusive säkerhetskonfigurationer av maskinvara, programvara, tjänster och nätverk.* Kravet konkretiseras ytterligare i p. 6.3.2 av vilken följer att de berörda entiteterna ska:

(a) Fastställa och säkerställa säkerheten i konfigurationer för sin maskinvara och programvara och sina tjänster och nätverk.

(b) *Fastställa och genomföra processer och verktyg för att verkställa de fastställda säkerhetskonfigurationerna för maskinvara, programvara, tjänster och nätverk, för nyinstallerade system och för system som är i drift under deras livslängd.*

Krav på konfiguration återfinns på fler ställen i genomförandeförordningen såsom:

- Krav enligt p. 3.2.3 (f) att om lämpligt logga åtkomst eller ändringar av kritiska konfigurations- och säkerhetskopieringsfiler.
- Krav enligt p. 6.7.2 att de berörda entiteterna inom ramen för nätverkssäkerhet:
    - konfigurerar *kontroller för att förhindra åtkomst och nätverkskommunikation som inte krävs för de berörda entiteternas drift.*
    - uttryckligen förbjuder eller avaktiverar *anslutningar och tjänster som inte behövs.*

[39] Prop 2025/26:28 s 245

- Krav enligt p. 11.6.2 (c) att de berörda entiteterna ska *kräva att autentiseringsuppgifterna ändras initialt, med på förhand fastställda intervall och vid misstanke om att uppgifterna har kompromitterats*

7.3.10.5 Sammanfattningsvis

Föreskriftskraven ligger i linje med genomförandeförordningens krav och i delar är genomförandeförordningen mer detaljerad.

7.3.11 Säkerhetstester (4 kap. 27 §)

7.3.11.1 Föreskrifterna

För att identifiera bristande cybersäkerhet i system, segment och den digitala miljön ska verksamhetsutövaren genom säkerhetstester säkerställa att valda tekniska säkerhetsåtgärder är införda och möter identifierat behov av säkerhet.

Av föreskrifterna följer även att säkerhetstester ska används för att kontrollera att systemen är uppdaterade till senaste version, publicerade sårbarheter är omhändertagna, och att valda konfigurationer är införda.

I de allmänna råden specificeras att verksamhetsutövaren bör använda etablerad testmetodik och att inte tidigare publicerade sårbarheter som upptäcks bör rapporteras till den nationella CSIRT-enheten.

7.3.11.2 NIS2-direktivet

I NIS2-direktivet behandlas inte säkerhetstestning som en separat säkerhetsåtgärd men kan sägas ingå i artikel 21 p. 2 e) där det framgår att de åtgärder som ska vidtas ska minst inbegripa *säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem, inbegripet hantering av sårbarheter och sårbarhetsinformation.*

7.3.11.3 Cybersäkerhetslagen

Inte heller cybersäkerhetslagen nämner uttryckligen säkerhetstestning men ställer motsvarande krav på säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem i 2 kap. 3 § st. 2 p. 5.

7.3.11.4 Genomförandeförordningen

I genomförandeförordningen behandlas säkerhetstestning i p. 6.5 som en del av säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem.

De berörda entiteterna ska fastställa och använda strategier och förfaranden för säkerhetstestning enligt p. 6.5.1 och enligt p. 6.5.2 ska de:

(a) baserat på den riskbedömning som utförts i enlighet med p. 2.1 fastställa behov, tillämpningsområde, frekvens och typ när det gäller säkerhetstestning,
(b) genomföra säkerhetstester i enlighet med en dokumenterad testmetod, som omfattar de komponenter som i en riskanalys identifierats som relevanta för säker drift,
(c) dokumentera testernas typ, tillämpningsområde, tidsram och resultat, inklusive en bedömning av kritikalitet och begränsningsåtgärder för varje iakttagelse, och
(d) tillämpa begränsningsåtgärder vid kritiska iakttagelser.

Krav på testning ställs även i genomförandeförordningen avseende bland annat hantering av säkerhetskopiering och redundans i p. 4.2 och säker utvecklingslivscykel i p. 6.2.

Vad gäller hantering av sårbarhetsinformation kan även kravet i p. 6.10.1. nämnas enligt vilket de berörda entiteterna *ska inhämta information om tekniska sårbarheter i deras nätverks- och informationssystem, bedöma sin exponering för sårbarheter och vidta ändamålsenliga åtgärder för att hantera sårbarheterna* och p. 6.10.2 (e) enligt vilket de berörda entiteterna ska fastställa *ett förfarande för information om sårbarheter i enlighet med den tillämpliga nationella policyn för samordnad information om sårbarheter*.

7.3.11.5 Sammanfattningsvis

Föreskrifterna bedöms ligga i linje med motsvarande krav i genomförande-förordningen. I vissa delar är genomförandeförordningen mer detaljerad.

7.3.12 Återställning av förlorad information och säkerhetskopiering (4 kap. 28 §)

7.3.12.1 Föreskrifterna

För att minska konsekvenserna för verksamheten om informationen i system förlorats, förvanskats eller på annat sätt blivit otillgänglig ska verksamhetsutövaren säkerställa att informationen kan återställas inom fastställda acceptabla tider för nedsatt funktionalitet och otillgänglighet.

Av föreskrifterna framgår även att verksamhetsutövaren ska identifiera och hantera behovet av att säkerhetskopiera information.

I de allmänna råden konkretiseras vad som bör fastställas i samband med säkerhetskopiering exempelvis vad som ska säkerhetskopieras, hur ofta och på vilket sätt, hur säkerhetskopior ska skyddas och hur återläsning ska göras. Verksamhetsutövaren bör även skydda minst en säkerhetskopia mot skadlig kod genom att lagra den på hårdvara separerad från det system som informationen hämtats ifrån.

7.3.12.2 NIS2-direktivet

Av artikel 21 p. 2 c) framgår att de åtgärder som ska vidtas ska minst inbegripa *driftskontinuitet, exempelvis hantering av säkerhetskopiering och katastrofhantering, och krishantering.*

7.3.12.3 Cybersäkerhetslagen

Motsvarande krav finns i cybersäkerhetslagens 2 kap. 3 § st. 2 p. 3 men där formulerat som krav på *kontinuitetshantering och krishantering.*

Av författningskommentaren för p. 3 framgår att verksamhetsutövaren har en skyldighet att *planera för och ha förmåga att upprätthålla sin verksamhet på en tolerabel nivå oavsett vilken störning den utsätts för eller om en kris inträffar. Verksamhetsutövaren bör bland annat överväga vilken säkerhetskopiering som krävs för detta och hur arbetet ska bedrivas för att minska störningen i verksamheten.*[40]

7.3.12.4 Genomförandeförordningen

Säkerhetskopiering berörs främst i p. 4.2 Hantering av säkerhetskopiering och redundans. Av p. 4.2.2 framgår att de berörda entiteterna ska fastställa säkerhetskopieringsplaner utifrån genomförd riskbedömning och driftskontinuitetsplan. Säkerhetskopieringsplanerna ska omfatta följande:

(a) Återställningstid.
(b) Säkerställande av att säkerhetskopiorna är fullständiga och korrekta, inklusive konfigurationsdata och data som lagras i molntjänstmiljö.
(c) Lagring av säkerhetskopior (online eller offline) på en eller flera säkra platser, som inte ingår i samma nätverk som systemet och som är på tillräckligt avstånd för att klara sig från eventuella skador från en katastrof vid huvudanläggningen.
(d) Lämplig fysisk och logisk kontroll av åtkomst till säkerhetskopiorna, i enlighet med tillgångens klassificeringsnivå.
(e) Återläsning av data från säkerhetskopior.
(f) Lagringstiden baseras på verksamhetskrav och rättsliga krav.

Av p. 4.2.3 ska de berörda entiteterna utföra regelbundna integritetskontroller av säkerhetskopiorna och enligt p. 4.3.6 ska de regelbundet testa återställningen av säkerhetskopior.

[40] Prop. 2025/26:28 s. 244

7.3.12.5 Sammanfattningsvis

Kraven i föreskrifterna ger verksamhetsutövaren ett större utrymme än genomförandeförordningen att utforma hur återställning av förlorad information ska ske och på vilket sätt säkerhetskopiering ska genomföras.

7.3.13 Intrångsdetektering och intrångsskydd (4 kap. 29 §)

7.3.13.1 Föreskrifterna

För att kunna upptäcka och hindra angrepp mot den digitala miljön ska verksamhetsutövaren säkerställa att intrångsdetektering och intrångsskydd används i produktionsmiljön.

Av föreskrifterna följer även att verksamhetsutövaren ska identifiera och hantera behovet av intrångsdetektering och intrångsskydd i utvecklings-, test- och utbildningsmiljön.

7.3.13.2 NIS2-direktivet

Av artikel 21 p. 2 b) framgår att de åtgärder som ska vidtas ska minst inbegripa *incidenthantering*. Incidenthantering definieras i artikel 6 p. 8 som *alla åtgärder och förfaranden som syftar till att förebygga, upptäcka, analysera, begränsa eller reagera på och återhämta sig från en incident*.

7.3.13.3 Cybersäkerhetslagen

Motsvarande krav på incidenthantering finns i cybersäkerhetslagens 2 kap. 3 § st. 2 p. 2. Begreppet definieras dock inte i lagen utan förklaras istället i författningskommentaren.[41]

7.3.13.4 Genomförandeförordningen

Under rubriken incidentrapportering, p. 3, reglerar genomförandeförordningen i p. 3.2.3 (g) bland annat att när berörda entiteter utformar loggar ska de inkludera händelseloggar och *loggar från säkerhetsverktyg, såsom antivirusprodukter, intrångsdetekteringssystem eller brandväggar*.

Av skäl (19) framgår att bör entiteterna, för att skydda sina nätverk och informationssystem mot sabotageprogram och otillåten programvara, *införa kontroller för att förhindra eller upptäcka användning av otillåten programvara och bör, när så är lämpligt, använda programvara för upptäckt och åtgärdande.*

[41] Prop. 2025/26:28 s. 244

Av p. 6.9.1 framgår att de berörda entiteterna *ska skydda sina nätverks- och informationssystem mot sabotageprogram och otillåten programvara*. Kravet konkretiseras ytterligare i p. 6.9.2 enligt vilken de berörda entiteterna ska *i synnerhet vidta åtgärder för upptäckt eller förhindrande av användning av sabotageprogram eller otillåten programvara. De berörda entiteterna ska, när så är lämpligt, säkerställa att deras nätverks- och informationssystem är utrustade med programvara för upptäckt och åtgärdande, som regelbundet uppdateras i enlighet med den riskbedömning som utförts i enlighet med p. 2.1 och avtalen med leverantörerna.*

7.3.13.5 Sammanfattningsvis

Även om genomförandeförordningen inte nämner intrångsdetekteringssystem mer än kort så får det anses naturligt att åtgärder som syftar till att ge ett skydd mot sabotageprogram eller otillåten programvara. De krav som ställs i föreskrifterna respektive genomförandeförordningen kan sägas ligga på ungefär samma övergripande nivå.

7.3.14 Ändringshantering (4 kap. 30–31 §§)

7.3.14.1 Föreskrifterna

För att minska risken för incidenter och tillbud som kan uppkomma vid ändringar i produktionsmiljön ska verksamhetsutövaren säkerställa att ändringshantering bedrivs på ett strukturerat och spårbart sätt vid införande, uppgradering, uppdatering och avveckling av hård- och mjukvara i produktionsmiljön. Till detta ställer föreskrifterna krav på att verksamhetsutövaren ska identifiera och hantera behovet av att bedriva ändringshantering på ett strukturerat och spårbart sätt i utveckling-, test- och utbildningsmiljö.

För att skydda system i it-segment mot kända sårbarheter ska verksamhetsutövaren enligt föreskrifterna säkerställa att säkerhetsuppdateringar genomförs skyndsamt. Mjukvara som leverantören inte längre tillhandahåller säkerhetsuppdateringar för ska bytas ut eller uppgraderas utan onödigt dröjsmål. Dessutom ska verksamhetsutövaren identifiera och hantera behovet av säkerhetsuppdateringar, uppdateringar och uppgraderingar i ot-segment.

Av de allmänna råden framgår att bland annat att verksamhetsutövaren bör säkerställa att endast godkända ändringar genomförs, att mjukvara uppgraderas till senaste versionen och att arbetet med att införa säkerhetsuppdateringar bör påbörjas senast 72 timmar efter att programvara som ger skydd mot sårbarheten tillgängliggjorts.

7.3.14.2 NIS2-direktivet

Av artikel 21 p. 2 e) följer krav på *säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem, inbegripet hantering av sårbarheter och sårbarhetsinformation.*

7.3.14.3 Cybersäkerhetslagen

Motsvarande krav finns i cybersäkerhetslagens 2 kap. 3 § st. 2 p. 4 om *säkerhet i leveranskedjan* och p. 5 om *säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem*.

7.3.14.4 Genomförandeförordningen

Förändringshantering regleras närmare i genomförandeförordningen p. 6.4 rörande *förändringshantering, reparationer och underhåll* inom ramen för säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem.

Enligt p. 6.4.1 ska de berörda entiteterna *tillämpa förändringshanteringsförfaranden för att kontrollera ändringar av nätverks- och informationssystem. Om tillämpligt ska förfarandena överensstämma med de berörda entiteternas allmänna strategier för förändringshantering.*

Av p. 6.4.2 framgår att de *förfaranden som avses i p. 6.4.1 ska tillämpas på versioner, ändringar och akutanpassningar av programvara och maskinvara som är i drift och på konfigurationsändringar. Förfarandena ska säkerställa att dessa ändringar är dokumenterade och, baserat på den riskbedömning som utförts i enlighet med p. 2.1, testade och bedömda med avseende på de potentiella konsekvenserna innan de genomförs.*

I p. 6.6 regleras hantering av programfix.[42] Enligt p. 6.6.1 ska de berörda entiteterna *specificera och tillämpa förfaranden som överensstämmer med de förändringshanteringsförfaranden som avses i p. 6.4.1 och med sårbarhetshantering, riskhantering och andra relevanta hanteringsförfaranden* för att säkerställa att

(a) programfixar tillämpas inom en rimlig tid från det att de blir tillgängliga,
(b) programfixar testas innan de tillämpas på produktionssystem,
(c) programfixar kommer från tillförlitliga källor och kontrolleras med avseende på integritet, och
(d) kompletterande åtgärder vidtas och kvarstående risker godtas i de fall då en programfix inte är tillgänglig eller inte tillämpas i enlighet med p. 6.6.2.

6.6.2. Genom undantag från p. 6.6.1 a får de berörda entiteterna *välja att inte tillämpa programfixar när nackdelarna med detta inte uppvägs av cybersäkerhetsfördelarna. De berörda entiteterna ska vederbörligen dokumentera och motivera varje sådant beslut.*

[42] I den engelska versionen benämnt Security patch management.

7.3.14.5 Sammanfattningsvis

Föreskrifterna ligger i stort sett i linje med genomförandeförordningen. Föreskrifterna är något tydligare att mjukvara som inte längre uppdateras ska bytas ut eller uppgraderas utan onödigt dröjsmål medan genomförandeförordningen ställer mer detaljerade krav på hur säkerhetsuppdateringar ska hanteras innan de tillämpas.

7.4 Fysiska säkerhetsåtgärder i kapitel 5

7.4.1 Lokaler (5 kap. 1–3 §§)

7.4.1.1 Föreskrifterna

För att undvika obehörig fysisk åtkomst till, förlust av och fysisk skada på system ska verksamhetsutövaren säkerställa att lokaler där information behandlas i system skyddas mot obehörigt tillträde genom tillträdesbegränsning och övervakning. Verksamhetsutövaren ska säkerställa att personals och besökares identitet kontrolleras innan de ges tillträde till sådana lokaler förutom till utpekade besöksutrymmen.

Av föreskrifterna framgår även att verksamhetsutövaren ska säkerställa, om det inte är uppenbart obehövligt, att särskilda it- och ot-utrymmen förses med övervakning och larm samt att åtgärder vidtas vid larm om obehörigt tillträde.

För att undvika förlust av, skada på eller funktionsstörning i system ska verksamhetsutövaren identifiera och hantera behovet av att skydda lokaler mot

1. brand,
2. vattenskador,
3. oacceptabel nivå av luftfuktighet, och
4. oacceptabel temperatur.

Enligt de allmänna råden bör verksamhetsutövaren säkerställa att det finns ett lämpligt skalskydd, att information i behov av utökat skydd behandlas i sektioner skilda ifrån övriga lokaler, samt att tillträde till särskilda it- och ot-utrymmen tilldelas restriktivt och registreras på individnivå. Verksamhetsutövaren bör också placera servrar och nätverksutrustning i särskilda it- och ot-utrymmen. Till detta kommer att verksamhetsutövaren bör säkerställa att övriga lokaler där information behandlas i system finns förses med övervakning och larm samt att åtgärder vitas vid larm om obehörigt tillträde.

7.4.1.2 NIS2-direktivet

Kraven på att skydda nätverks- och informationssystems fysiska miljö från incidenter följer huvudsakligen av artikel 21 p. 2 första meningen men har även koppling till kraven i artikel 21.2 (e) och (i) rörande *säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem* samt *personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning*.

7.4.1.3 Cybersäkerhetslagen

Motsvarande krav ställs i 2 kap. 3 § st.2.

7.4.1.4 Genomförandeförordningen

Kraven i p. 13 rörande miljömässig och fysisk säkerhet i genomförandeförordningen är kopplade till NIS2-direktivets artikel 21.2 (c), (e) och (i) rörande *driftskontinuitet*, *säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem* samt *personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning*.

I p. 13.3 behandlas *perimeterkontroll och kontroll av fysiskt tillträde*. Enligt p. 13.3.1 ska de berörda entiteterna förhindra och övervaka obehörig fysiskt tillträde, skada och interferens i deras nätverks- och informationssystem. Detta ska de berörda entiteterna uppnå enligt p. 13.3.2 genom att:

(a) På grundval av den riskbedömning som utförts i enlighet med p. 2.1 fastställa och använda säkerhetsperimetrar för att skydda områden där nätverks- och informationssystemen och andra tillhörande tillgångar är lokaliserade.
(b) Skydda de områden som avses i led a genom lämpliga inträdeskontroller och tillträdespunkter.
(c) Utforma och genomföra fysisk säkerhet för kontor, rum och anläggningar.
(d) Kontinuerligt övervaka sina lokaler för obehörig fysisk åtkomst.

I detta sammanhang kan även nämnas p. 6.8.2 (c) enligt vilken de berörda entiteterna ska *(c) förvara system som är kritiska för den berörda entitetens drift eller säkerhet i säkrade zoner*.

I p. 13.2 regleras skydd mot *fysiska och miljömässiga hot*. Det framgår av p. 13.2.1 att de berörda entiteterna ska *förhindra eller begränsa konsekvenserna av händelser som härrör från fysiska och miljömässiga hot, såsom naturkatastrofer och andra avsiktliga eller oavsiktliga hot, baserat på resultaten av den riskbedömning som utförts i enlighet med p. 2.1*.

Genomförandeförordningen specificerar också i p. 13.2.2 att de berörda entiteterna, när så är lämpligt, ska

(a) utforma och genomföra skyddsåtgärder mot de fysiska och miljömässiga hoten,
(b) fastställa lägsta och högsta kontrolltrösklar för fysiska och miljömässiga hot, samt
(c) övervaka miljöparametrarna och till behörig intern eller extern personal rapportera händelser utanför de lägsta och högsta kontrolltrösklar som avses i led b.

Av skäl (28) framgår att riskhanteringsåtgärder för cybersäkerhet bör baseras på en allriskansats som syftar till att skydda nätverks- och informationssystem och dessa systems fysiska miljö mot sådana händelser som stöld, brand, översvämning, telekommunikations- eller elavbrott eller obehörig fysiskt tillträde till och skada eller störning på en väsentlig eller viktig entitets information och informations-behandlingsresurser, som kan undergräva tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade data eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem.

7.4.1.5 Sammanfattningsvis

Föreskrifternas krav bedöms ligga i linje med genomförandeförordningens motsvarande krav, även om p. 13 inte konkretiserar lika tydligt som föreskrifterna vilka fysiska och miljömässiga hot som behöver omhändertas så framgår det av skälen till genomförandeförordningen vilka som avses.

7.4.2 Tekniska försörjningssystem (5 kap. 4 §)

7.4.2.1 Föreskrifterna

För att undvika skada på eller störning i system på grund av fel eller avbrott i tekniska försörjningssystem ska verksamhetsutövaren säkerställa tillräcklig funktionalitet i den digitala miljön avseende elförsörjning, elektroniska kommunikationsnät och elektroniska kommunikationstjänster, kyla, värme, och ventilation.

Föreskrifterna ställer även krav på att verksamhetsutövaren ska identifiera och hantera behovet av att övervaka de tekniska försörjningssystemens funktion och säkerställa att larm genereras och åtgärder vidtas vid otillräcklig funktionalitet samt identifiera och hantera behovet av redundanta funktioner för tekniska försörjningssystem.

7.4.2.2 NIS2-direktivet

I likhet med krav på lokaler följer kraven på tekniska försörjningssystem av NIS2-direktivets krav på att skydda nätverks- och informationssystems fysiska miljö från incidenter följer huvudsakligen av artikel 21 p. 2 första meningen men har även koppling till kraven i artikel 21.2 (c) rörande *driftskontinuitet*.

7.4.2.3 Cybersäkerhetslagen

Motsvarande krav ställs i 2 kap. 3 § st.2.

7.4.2.4 Genomförandeförordningen

Av p. 13.1.1 i genomförandeförordningen framgår att de berörda entiteterna vid tillämpning av artikel 21.2 c i NIS2-direktivet ska *förhindra förlust, skada eller kompromettering av nätverks- och informationssystem eller avbrott i driften av dem på grund av fel eller avbrott i försörjningstjänster.*

I samband med detta ska berörda entiteterna enligt 13.1.2 när så är lämpligt

(a) skydda anläggningar från strömavbrott och andra störningar som orsakas av avbrott i försörjningstjänster såsom el, telekommunikation, vattenförsörjning, gas, avlopp, ventilation och luftkonditionering,
(b) överväga användning av redundans i försörjningstjänster,
(c) skydda försörjningstjänster för el och telekommunikation som transporterar data eller används för nätverks- och informationssystem mot avläsning och skada,
(d) övervaka de försörjningstjänster som avses i led c och till behörig intern eller extern personal rapportera händelser utanför de lägsta och högsta kontrolltrösklar som avses i p. 13.2.2 b och som påverkar försörjningstjänsterna,
(e) ingå avtal om nödförsörjning med motsvarande tjänster när det gäller t.ex. bränsle för nödkraftförsörjning, samt
(f) säkerställa kontinuerlig effektivitet och övervaka, underhålla och testa den försörjning som nätverks- och informationssystemen behöver för driften av de tjänster som erbjuds – i synnerhet el, reglering av temperatur och luftfuktighet, telekommunikation och internetanslutning.

Enligt p. 13.1.3 ska de berörda entiteterna *testa, se över och, när så är lämpligt, uppdatera skyddsåtgärderna regelbundet eller efter betydande incidenter eller betydande förändringar av driften eller riskerna.*

7.4.2.5 Sammanfattningsvis

Föreskrifternas krav är generellt sett mer övergripande än motsvarande krav i genomförandeförordningen och lämnar därmed ett större utrymme till verksamhetsutövaren att utforma sina säkerhetsåtgärder.

7.5 Sektorsspecifika säkerhetsåtgärder i kapitel 6

7.5.1 Offentlig förvaltning: System för kriskommunikation (6 kap. 1–2 §§)

7.5.1.1 Föreskrifterna

I kapitel 6 i föreskrifterna har sektorsspecifika säkerhetsåtgärder samlats. Sådana finns i nuläget endast för offentlig förvaltning men det kan inte uteslutas att även andra sektorer vid kommande uppdateringar av föreskrifterna kan komma att få liknande sektorsanpassade tillägg.

När det gäller offentlig förvaltning utgår kravet från att det är av särskild vikt vid olika typer av samhällsstörningar att offentlig förvaltning kan upprätthålla god förmåga att kommunicera vid kriser. Med anledning av detta ställs krav i föreskrifterna på att verksamhetsutövare ska säkerställa att funktionaliteten i system som ska användas för intern och extern kriskommunikation vid kriser kontrolleras.

Det framgår även att verksamhetsutövare ska identifiera och hantera behovet av att använda Rakel (Radiokommunikation för effektiv ledning) eller SWEN (The Swedish Emergency Network) och SGSI (Swedish Government Secure Intranet) för kriskommunikation.

Enligt de allmänna råden bör verksamhetsutövaren var tredje månad kontrollera att kriskommunikationssystem kan användas på avsett sätt.

Såväl Rakel, SWEN och SGSI erbjuds av Myndigheten för civilt försvar och är olika typer av säkra kommunikationer.

7.5.1.2 NIS2-direktivet

Av artikel 21 p. 2 j) följer krav på användning inom entiteten, när så är lämpligt, av lösningar för multifaktorautentisering eller kontinuerlig autentisering, säkrade röst-, video- och textkommunikationer och säkrade nödkommunikationssystem.

7.5.1.3 Cybersäkerhetslagen

Motsvarande krav finns i cybersäkerhetslagen 2 kap. 3 § p. 10, *vid behov användning av lösningar för autentisering, säkrade kommunikationer och säkrade nödkommunikations-system.*

Av författningskommentaren framgår att p. 10 innebär att verksamhetsutövaren *ska bedöma om lösningar för autentisering, säkrade kommunikationer och säkrade nödkommunikationssystem krävs och i så fall vilka.*

Säkrad kommunikation avser röst-, video- och textkommunikation som bland annat är skyddad mot obehörig avlyssning eller upptagning. Säkrad kommunikation ska, om behovet finns, kunna användas både i den dagliga verksamheten och i nödsituationer.[43]

7.5.1.4 Genomförandeförordningen

Genomförandeförordningen specificerar inte närmare användningen av säkrade kommunikationer och säkrade nödkommunikationssystem.

7.5.1.5 Sammanfattningsvis

Även om föreskrifternas krav inte har någon direkt motsvarighet i genomförandeförordningen så ligger de i linje med de uttalanden som finns i cybersäkerhetslagens författningskommentar rörande 2 kap. 3 § p.10. Tillämpligheten har dessutom begränsats i föreskrifterna till att endast gälla verksamhetsutövare i offentlig sektor.

8. Uppgifter om de bemyndiganden som myndighetens beslutanderätt grundar sig på

Av 38 § p. 5 cybersäkerhetsförordningen framgår att Myndigheten för civilt försvar får meddela föreskrifter rörande utbildning enligt 2 kap. 4 § cybersäkerhetslagen samt enligt 39 § p. 1 ytterligare föreskrifter om säkerhetsåtgärder enligt 2 kap. 3 § samma lag.

Föreskriftsmandatet avseende säkerhetsåtgärder enligt 2 kap. 3 § cybersäkerhetslagen omfattar inte sektorerna Digital infrastruktur, Digitala leverantörer, Förvaltning av IKT- tjänster (mellan företag), Post- och budtjänster eller Rymden. För dessa sektorer utfärdar Post- och telestyrelsen motsvarande reglering. Kommissionen har också antagit en genomförandeförordning som närmare specificerar krav avseende säkerhetsåtgärder för sådana verksamhetsutövare som tillhandahåller olika digitala tjänster och infrastruktur.[44]

[43] Prop. 2025/26:28 s. 246
[44] (EU) 2024/2690 av den 17 oktober 2024 om fastställande av regler för tillämpningen av direktiv (EU) 2022/2555 vad gäller tekniska och metodologiska specifikationer för riskhanteringsåtgärder för

9. 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 beslutas i början av juni 2026. När det gäller tidpunkt för ikraftträdande bedömer myndigheten att det är centralt att de verksamhetsutövare som omfattas av regleringen också ges tillgång till stöd i form av vägledning men även möjlighet att ställa frågor och andra informationsinsatser. Mot bakgrund av att det är semesterperiod för många verksamhetsutövare samt att cybersäkerhetsverksamheten vid Myndigheten för civilt försvar kommer att föras över till det nationella cybersäkerhetscentret under ledning av FRA den 1 juli 2026 bedöms det som mindre lämpligt att låta föreskrifterna om säkerhetsåtgärder och utbildning träda i kraft som brukligt är efter fyra veckor från beslutsdatum, det vill säga i början av juli. Myndigheten bedömer istället att det är lämpligast att sätta ikraftträdandedatum till den 1 oktober 2026. Detta ger verksamhetsutövare god tid att förbereda sig samt tillgång till stöd i olika former kan säkerställas på ett helt annat sätt än mitt under en verksamhetsövergång. De resurser som behöver läggas på att arbeta med cybersäkerhetsaspekter rörande valet i september blir även tillgängliga i oktober.

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.

cybersäkerhet och närmare angivelse av i vilka fall en incident ska anses vara betydande med avseende på leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av utlokaliserade driftstjänster, leverantörer av utlokaliserade säkerhetstjänster, leverantörer av marknadsplatser online, leverantörer av sökmotorer, leverantörer av plattformar för sociala nätverkstjänster och tillhandahållare av betrodda tjänster.

Myndigheten för civilt försvar 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.

10. Hur och när konsekvenserna kan utvärderas

En övergripande uppföljning av hur de nya reglerna påverkar nivån av cybersäkerhet i Sverige kommer att kunna göras genom att följa resultatutvecklingen i Cybersäkerhetskollen[45]. Cybersäkerhetskollen är samlingsnamnet för myndighetens cybersäkerhetsmätningar som mäter nivån på verksamheters systematiska cybersäkerhetsarbete, samt ger stöd för förbättringsarbete. Cybersäkerhetskollen genomförs minst vartannat år och ska på regeringens uppdrag riktas till hela den offentliga förvaltningen och de verksamhetsutövare som omfattas av NIS-direktiven.

En mer grundlig utvärdering av konsekvenserna för både privata och offentliga verksamhetsutövare sker i anslutning den utvärdering av cybersäkerhetslagen som regeringen aviserat ska ske tre år efter den nya lagens ikraftträdande.[46] Utvärderingen bör ske i nära samverkan med utpekade tillsynsmyndigheter för att säkerställa att underlag inhämtas från så många av NIS2-sektorerna som möjligt. Det övergripande syftet med en sådan utvärdering blir att få en bild av hur det nya regelverket påverkat verksamhetsutövarens cybersäkerhetsarbete och cybersäkerhet inklusive ekonomiska konsekvenser. Utvärderingen bör även inkludera ändamålsenligheten av tillhandahållet stöd i form av vägledningar, systemstöd med mera.

Föreskrifter och föreskriftsmandat gällande cybersäkerhetslagen krav på verksamhetsutövares säkerhetsåtgärder och utbildning kommer att flyttas över till

[45] https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/arbeta-systematiskt-med-informationssakerhet-och-cybersakerhet/cybersakerhetskollen/
[46] Prop. 2025/26:28 s. 226

FRA den 1 juli 2026. Med anledning av detta kommer uppföljningen av konsekvenser ske hos FRA inom ramen för det nationella cybersäkerhetscentret.

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

11. Övriga konsekvenser

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 rättssäkert sätt.

12. Kontaktpersoner

Tove Wätterstam eller Helena Andersson