Från: Myndigheten för samhällsskydd och beredskap <noreply@msb.se>
Skickat: den 29 oktober 2025 15:39
Till: Regelrådet
Ämne: [extern] Förslag till MSB:s föreskrifter och allmänna råd utifrån kommande cybersäkerhetslag

Uppföljningsflagga: Följ upp
Flagga: Har meddelandeflagga

Kategorier: Björn
AppServerName: public360_prod
DocumentID: RR 2025-344:01
DocumentIsArchived: -1

Du får inte ofta e-post från noreply@msb.se. **Läs om varför det här är viktigt**

Myndigheten för samhällsskydd och beredskap

Ser ditt nyhetsbrev konstigt ut? **Klicka här.**

Oktober, 2025

Förslag till MSB:s föreskrifter och allmänna råd utifrån kommande cybersäkerhetslag

Välkommen att lämna synpunkter på Myndigheten för samhällsskydd och beredskaps förslag till nya föreskrifter samt tillhörande konsekvensanalys om säkerhetsåtgärder och utbildning respektive incidentrapportering och informationsskyldighet enligt NIS2-direktivet. NIS2-direktivet implementeras i Sverige genom kommande cybersäkerhetslag.

Vi ser fram emot er återkoppling senast den 10 december. Var vänlig använd anvisad svarsmall då det underlättar vår beredning av inkomna remissvar.

Underlaget hittar ni via knapparna nedan.

Förslag till nya föreskrifter om säkerhetsåtgärder och utbildning enligt ny cybersäkerhetslag

Förslag till nya föreskrifter om incidentrapportering och informationsskyldighet enligt ny cybersäkerhetslag

Myndigheten för samhällsskydd och beredskap

www.msb.se
651 81 Karlstad
0771-240 240
registrator@msb.se

Skicka vidare | Prenumerera | Avprenumerera

Avdelningen för cybersäkerhet och samhällsviktiga kommunikationer

Enl. sändlista

Remiss avseende förslag till myndighetens för samhällsskydd och beredskaps föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning;

Ärendet

Myndigheten för samhällsskydd och beredskap ber härmed om era synpunkter på förslag till nya föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning enligt kommande cybersäkerhetslag.

Bakgrund

Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS2-direktivet) ska implementeras i Sverige genom cybersäkerhetslagen (2025:XXX). Lagen planeras att börja gälla den 15 januari 2026.

MSB har fått i uppdrag av regeringen att vidta vissa åtgärder för att förbereda genomförandet av NIS2-direktivet.[1] I detta ingår att förbereda för att meddela föreskrifter rörande

1. anmälningsskyldighet,
2. kriterier för när en verksamhetsutövare ska omfattas av regelverket med hänvisning till sin särskilda betydelse i samhället och när sådana verksamhetsutövare ska räknas som väsentliga,
3. vad som utgör huvudsakligt etableringsställe,
4. undantag för partnerföretag och anknutna företag,
5. säkerhetsåtgärder,
6. utbildning,
7. rapporteringsskyldigheter,
8. vad som utgör en betydande incident,
9. skyldighet att informera vid betydande incidenter och betydande cyberhot, och
10. säkerhetsrevisioner och säkerhetsskanningar.

PTS har fått i uppdrag av regeringen att förbereda för att meddela föreskrifter om säkerhetsåtgärder, skyldigheten att föra register om domännamn, vad som utgör en betydande incident och skyldighet att informera vid betydande incidenter och betydande cyberhot för följande sektorer: digital infrastruktur, digitala leverantörer, förvaltning av IKT-tjänster (mellan företag), post- och budtjänster och rymden.[2] Dessa delar omfattas därför inte av MSB:s uppdrag om att förbereda föreskrifter.

[1] . Uppdrag till Myndigheten för samhällsskydd och beredskap att förbereda genomförandet av NIS 2-direktivet, Fö 2025/012893.

[2] Uppdrag till Post och telestyrelsen att förbereda genomförandet av NIS 2-direktivet, Fi 2025/01676.

Uppdraget genomförs i nära samverkan med de myndigheter som föreslås få i uppdrag att utöva tillsyn över tillämpningen av cybersäkerhetslagen och föreskrifter som har meddelas i anslutning till lagen.

Vid årsskiftet 2025/2026 kommer Myndigheten för samhällsskydd och beredskap att byta namn till Myndigheten för civilt försvar vilket kommer att medföra att föreskrifternas grafiska profil justeras.

Föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning

Enligt artikel 21 punkt 1 första stycket i NIS2-direktivet ska medlemsstaterna säkerställa att väsentliga och viktiga entiteter vidtar tekniska, driftsrelaterade och organisatoriska åtgärder som är lämpliga och proportionella. Syftet är att hantera risker som hotar säkerheten i verksamhetsutövarens nätverks- och informationssystem. Åtgärderna ska bidra till att förebygga eller begränsa effekterna av incidenter.

Av artikel 21.2 framgår att säkerhetsåtgärderna ska bygga på en allriskansats. Denna ansats ska skydda både nätverks- och informationssystem och deras fysiska miljö. Direktivets krav på säkerhetsåtgärder föreslås införas i svensk rätt genom 2 kap. 3 § cybersäkerhetslagen.

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

Förslaget till föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning syftar till att förtydliga vilka säkerhetsåtgärder verksamhetsutövarna minst behöver vidta respektive vilken utbildning som behöver genomföras för att uppfylla lagkraven.

Remiss

Remissen utgörs av:

- Förslag till Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning,
- Konsekvensutredning rörande föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning.

https://www.msb.se/sv/regler/remisser-om-foreskrifter-och-allmanna-rad/remiss-forslag-till-nya-foreskrifter-om-sakerhetsatgarder-och-utbildning-enligt-ny-cybersakerhetslag/

(På MSB.se, välj Regler, sedan Remisser om föreskrifter och allmänna råd, därefter Regelförslag till nya MSB:s föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning)

Vi önskar era synpunkter senast 10 december 2025 i anvisad svarsmall inskickad i excelformat (inte skannade kopior) för att underlätta hanteringen av de inkomna svaren.

Svaren skickas till registrator@msb.se, var vänlig och märk ert svar med **MSB 2025-13269.**

Frågor hänvisas till funktionsbrevlådan nis2-cer@msb.se

Vänliga hälsningar
Åke Holmgren
Chef för Avdelningen för cybersäkerhet och samhällsviktiga kommunikationer

Myndigheten för samhällsskydd och beredskap

Postadress: 651 81 Karlstad
Telefon: 0771-240 240
Fax: 010-240 56 00
registrator@msb.se
www.msb.se
Org.nr: 202100-5984

Sändlista

Affärsverket svenska kraftnät
Ale kommun
Alingsås kommun
Alvesta kommun
Amazon Web Services - EMEA SARL Sverige Filial
Aneby kommun
Arbetsförmedlingen
Arbetsgivarverket
Arbetsmiljöverket
Arboga kommun
Arjeplogs kommun
Arvidsjaurs kommun
Arvika kommun
Ascro
Askersunds kommun
Avesta kommun
Bengtsfors kommun
Bergs kommun
Bjurholms kommun
Bjuvs kommun
Blekinge tekniska högskola
Bodens kommun
Bolagsverket
Bollebygds kommun
Bollnäs kommun
Borgholms kommun
Borlänge kommun
Borås stad
Botkyrka kommun
Boxholms kommun
Braathens Regional Airways AB
Bromölla kommun
Brottsförebyggande rådet
Bräcke kommun
BTPOS
Burlövs kommun
Båstads kommun
Centrala studiestödsnämnden
Chalmers tekniska högskola
CMP
Dals-Eds kommun
Danderyds kommun
Degerfors kommun
Domstolsverket
Dorotea kommun
Drivkraft Sverige
Eda kommun
E-hälsomyndigheten

Ekerö kommun
Ekobrottsmyndigheten
Ekonomistyrningsverket
Eksjö kommun
Emmaboda kommun
Energiföretagen
Energigas Sverige
Energimarknadsinspektionen
Enköpings kommun
Epiroc Rock Drills AB
Eskilstuna kommun
Eslövs kommun
Essunga kommun
Fagersta kommun
Falkenbergs kommun
Falköpings kommun
Falu kommun
Filipstads kommun
Finansbolagens förening
Finansinspektionen
Finspångs kommun
Flens kommun
Folkhälsomyndigheten
Forshaga kommun
Fortifikationsverket
Färgelanda kommun
Föreningen för Generiska läkemedel och Biosimilarer
Föreningen Svenskt Flyg Intresse AB
Föreningen Sveriges Järnvägsentreprenörer (FSJ)
Försvarets materielverk
Försvarets radioanstalt
Försvarshögskolan
Försvarsmakten
Försäkringskassan
Gagnefs kommun
Gislaveds kommun
GleSYS AB
Gnesta kommun
Gnosjö kommun
Grums kommun
Grästorps kommun
Gullspångs kommun
Gällivare kommun
Gävle kommun
Göteborgs Hamn AB
Göteborgs stad
Göteborgs universitet
Götene kommun
Habo kommun
Hagfors kommun

Hallsbergs kommun
Hallstahammars kommun
Halmstads kommun
Hammarö kommun
Haninge kommun
Haparanda stad
Havs- och vattenmyndigheten
Heby kommun
Hedemora kommun
Helsingborgs hamn
Helsingborgs stad
Herrljunga kommun
Hjo kommun
Hofors kommun
Hostek AB Huddinge kommun
Hudiksvalls kommun
Hultsfreds kommun
Hylte kommun
Håbo kommun
Hällefors kommun
Härjedalens kommun
Härnösands kommun
Härryda kommun
Hässleholms kommun
Höganäs kommun
Högsby kommun
Högskolan i Skövde
Högskolan i Väst
Hörby kommun
Höörs kommun
IKEM
Innovations- och kemiindustrierna i Sverige
Inspektionen för strategiska produkter
Inspektionen för vård och omsorg
Integritetsskyddsmyndigheten
Jokkmokks kommun
Järfälla kommun
Jönköpings kommun
Kalix kommun
Kalmar kommun
Kammarkollegiet
Karlsborgs kommun
Karlshamns kommun
Karlskoga kommun
Karlskrona kommun
Karlstads kommun
Karlstads universitet
Karolinska institutet
Katrineholms kommun
Kemikalieinspektionen
Kils kommun
Kinda kommun
Kiruna kommun
Klippans kommun
Knivsta kommun

Kommerskollegium
Konkurrensverket
Konsumentverket
Kramfors kommun
Kriminalvården
Kristinehamns kommun
Krokoms kommun
Kronofogdemyndigheten
Kumla kommun
Kungliga tekniska högskolan
Kungsbacka kommun
Kungsörs kommun
Kungälvs kommun
Kustbevakningen
Kävlinge kommun
Köpings kommun
Laholms kommun
Laholmsbuktens VA
Landskrona stad
Lantbrukarnas Riksförbund
Lantmännen
Lantmäteriet
Laxå kommun
Lekebergs kommun
Leksands kommun
Lerums kommun
Lessebo kommun
Lidingö stad
Lidköpings kommun
Lilla Edets kommun
Lindesbergs kommun
Linköpings kommun
Linköpings universitet
Linnéuniversitet
Livsmedelsverket
Ljungby kommun
Ljusdals kommun
Ljusnarsbergs kommun
Logent AB
Lomma kommun
Loopia AB
Ludvika kommun
Luftfartsverket
Luleå kommun
Luleås tekniska högskola
Lunds kommun
Lunds universitet
Lycksele kommun
Lysekils kommun
Läkemedelsverket
Läkemedelsindustriföreningen
Länsstyrelsen i Blekinge län
Länsstyrelsen i Dalarnas län
Länsstyrelsen i Gotlands län
Länsstyrelsen i Gävleborgs län
Länsstyrelsen i Hallands län
Länsstyrelsen i Jämtlands län
Länsstyrelsen i Jönköpings län
Länsstyrelsen i Kalmar län

Länsstyrelsen i Kronoberg län
Länsstyrelsen i Norrbottens län
Länsstyrelsen i Skåne län
Länsstyrelsen i Stockholms län
Länsstyrelsen i Södermanlands län
Länsstyrelsen i Uppsala län
Länsstyrelsen i Värmlands län
Länsstyrelsen i Västerbottens län
Länsstyrelsen i Västernorrlands län
Länsstyrelsen i Västmanlands län
Länsstyrelsen i Västra Götalands län
Länsstyrelsen i Örebro län
Länsstyrelsen i Östergötlands län
Malmö stad
Malmö universitet
Malung-Sälens kommun
Malå kommun
Mariestads kommun
Markaryds kommun
Marks kommun
Mediemyndigheten
Melleruds kommun
Migrationsverket
Mittuniversitetet
Mjölby kommun
Mobility Sweden
Mora kommun
Motala kommun
Mullsjö kommun
Munkedals kommun
Munkfors kommun
Myndigheten för digital förvaltning
Myndigheten för psykologiskt försvar
Myndigheten för totalförsvarsanalys
Myndigheten för yrkeshögskolan
Mölndals kommun
Mönsterås kommun
Mörbylånga kommun
Nacka kommun
Nationellt cybersäkerhetscenter (NCSC)
Naturvårdsverket
Netnod AB
Nobina
Nora kommun
Norbergs kommun
Nordanstigs kommun
Nordmalings kommun
Norrköpings kommun
Norrtälje kommun
Norsjö kommun
Norwegian
Nybro kommun
Nykvarns kommun
Nyköpings kommun
Nynäshamns kommun
Nässjö kommun
Ockelbo kommun
Oderland Webbhotell AB
Olofströms kommun

One.com Group AB
Orsa kommun
Orust kommun
Osby kommun
Oskarshamns kommun
Ovanåkers kommun
Oxelösunds kommun
Pajala kommun
Partille kommun
Pensionsmyndigheten
Perstorps kommun
Piteå kommun
Polismyndigheten
Post – och telestyrelsen
Ragunda kommun
Regelrådet
Region Blekinge
Region Dalarna
Region Gotland
Region Gävleborg
Region Halland
Region Jämtland Härjedalen
Region Jönköpings län
Region Kalmar län
Region Kronoberg
Region Norrbotten
Region Skåne
Region Stockholm
Region Sörmland
Region Uppsala
Region Värmland
Region Västerbotten
Region Västernorrland
Region Västmanland
Region Örebro län
Region Östergötland
Riksantikvarieämbetet
Riksarkivet
Riksbanken
Riksdagsförvaltningen
Riksgäldskontoret
Robertsfors kommun
Ronneby kommun
Rymdstyrelsen
Rättviks kommun
Sala kommun
Salems kommun
SAS Link AB
SCA Logistics AB
Scania
SDATS
Sida
Sigtuna kommun
Simrishamns kommun
Sjöbo kommun
Sjöfartsverket
Skara kommun
Skatteverket
Skellefteå kommun

Skinnskattebergs kommun
Skurups kommun
Skövde kommun
Smedjebackens kommun
Socialstyrelsen
Sollefteå kommun
Sollentuna kommun
Solna kommun
Sorsele kommun
Sotenäs kommun
Staffanstorps kommun
Statens energimyndighet
Statens fastighetsverk
Statens jordbruksverk
Statens servicecenter
Statens skolverk
Statens tjänstepensionsverk
Statens veterinärmedicinska anstalt
Statistiska centralbyrån
Statskontoret
Stenungsunds kommun
Stiftelsen för Internetinfrastruktur
Stockholm Skavsta
Stockholm stad
Stockholms universitet
Stockholm Vatten och Avfall
Stockholms Hamnar
Storfors kommun
Storumans kommun
Strålsäkerhetsmyndigheten
Strängnäs kommun
Strömstads kommun
Strömsunds kommun
Styrelsen för ackreditering och teknisk kontroll
Sundbybergs stad
Sundsvalls kommun
Sunne kommun
Surahammars kommun
Svalövs kommun
Svedala kommun
Svenljunga kommun
Svensk Dagligvaruhandel
Svensk Handel
Svensk Medicinteknisk Förening
Svensk sjöfart
Svenskt näringsliv
Sveriges kommuner och regioner
Sveriges lantbruksuniversitet
Sveriges meteorologiska och hydrologiska institut
Sveriges regionala flygplatser
Swedavia
SwedenBIO
Swedish Labtech
Swedish Medtech
Swedish space corporation
Säffle kommun
Säkerhetspolisen
Säkerhets och försvarsföretagen
Säters kommun

Sävsjö kommun
Söderhamns kommun
Söderköpings kommun
Södertälje kommun
Södertörns högskola
Sölvesborgs kommun
Tanums kommun
TechSverige
Teknikföretagen
Tetra Pak
Tibro kommun
Tidaholms kommun
Tierps kommun
Tillväxtverket
Timrå kommun
Tingsryds kommun
Tjörns kommun
Tomelilla kommun
Torsby kommun
Torsås kommun
Totalförsvarets forskningsinstitut
Trafikförvaltningen Region Stockholm
Trafikverket
Tranemo kommun
Transportföretagen
Transportstyrelsen
Tranås kommun
Trelleborgs kommun
Trollhättans kommun
Trosa kommun
Tullverket
Tyresö kommun
Tågföretagen
Täby kommun
Töreboda kommun
Uddevalla kommun
Ulricehamns kommun
Umeå kommun
Umeå universitet
Upphandlingsmyndigheten
Upplands Väsby kommun
Upplands-Bro kommun
Uppsala kommun
Uppsala universitet
Uppvidinge kommun
Utbetalningsmyndigheten
Vadstena kommun
Vaggeryds kommun
Valdemarsviks kommun
Vallentuna kommun
Valmyndigheten
Vansbro kommun
Vara kommun
Varbergs kommun
Vaxholms stad
Vellinge kommun
Verket för innovationssystem
Vetlanda kommun
Vilhelmina kommun

Vimmerby kommun
Vindelns kommun
Vingåkers kommun
Visita
Volvo Cars
Vårgårda kommun
Vänersborgs kommun
Vännäs kommun
Värmdö kommun
Värnamo kommun
Västerviks kommun
Västerås stad
Västra Götalandsregionen
Växjö kommun
Ydre kommun
Ystads kommun
Åmåls kommun
Ånge kommun
Årjängs kommun
Åsele kommun
Åstorps kommun
Åtvidabergs kommun
Älmhults kommun
Älvdalens kommun
Älvkarleby kommun
Älvsbyns kommun
Ängelholms kommun
Öckerö kommun
Ödeshögs kommun
Örebro kommun
Örebro universitet
Örkelljunga kommun
Örnsköldsviks kommun
Östersunds kommun
Österåkers kommun
Östhammars kommun
Östra Göinge kommun
Överkalix kommun
Övertorneå kommun

Kopia
Försvarsdepartementet

Myndigheten för samhällsskydd och beredskaps författningssamling

Utgivare: Anna Asp, Myndigheten för samhällsskydd och beredskap
ISSN 2000-1886

MSBFS
Remissutgåva
[Fyll i nr]
Utkom från trycket
den [Fyll i datum]

Förslag till Myndighetens för samhällsskydd och beredskaps föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning;

beslutade den [Fyll i datum]

Myndigheten för samhällsskydd och beredskap föreskriver[1] följande med stöd av XX § förordningen (2025:XXX) om cybersäkerhet och beslutar följande allmänna råd.

Allmänna råd har en annan juridisk status än föreskrifter. De är inte tvingande. Deras funktion är att förtydliga innebörden i lag, förordning och föreskrifter och att ge generella rekommendationer om deras tillämpning.

1 kap. Inledande bestämmelser

Tillämpningsområde

1 § Dessa föreskrifter och allmänna råd innehåller bestämmelser om säkerhetsåtgärder och utbildning som avses i 2 kap. 3 och 4 §§ lagen (2025:XX) om cybersäkerhet.

För sektorsverksamhet inom digital infrastruktur, digitala leverantörer, informations- och kommunikationstjänster mellan företag (IKT-tjänster), post- och budtjänster och rymden gäller endast kraven på ledningens utbildning i 2 kap. 9 §.

2 § Om en annan författning innehåller en bestämmelse som ställer högre krav än kraven i dessa föreskrifter tillämpas den bestämmelsen.

Ordförklaring

3 § Termer och uttryck i dessa föreskrifter och allmänna råd har samma betydelse som i lagen (2025:XXX) om cybersäkerhet.

[1] 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).

I dessa föreskrifter och allmänna råd avses med

cybersäkerhetskris	storskalig cybersäkerhetsincident eller kris enligt artikel 9 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),
digital miljö	den samlade mängden system som verksamhetsutövaren ansvarar för. Digital miljö delas in i produktionsmiljö och utvecklings-, test- och utbildningsmiljö,
it-segment	ett nätverkssegment som verksamhetsutövaren har inrättat för andra system än sådana som placeras i ot-segment. Är ett segment i produktionsmiljö och utvecklings-, test- och utbildningsmiljö,
ot-segment	ett nätverkssegment i en del av den digital miljön som verksamhetsutövaren har inrättat för system som används för att styra och övervaka cyberfysiska system, Är ett segment i produktionsmiljö och utvecklings-, test- och utbildningsmiljö,
produktionsmiljö	den av den digitala miljön som verksamhetsutövaren använder för sin produktion eller utförande av sitt uppdrag,
redundant funktion	två eller flera, identiska eller olika, funktioner som oberoende av varandra uppfyller samma syfte,
sektorskritiskt system	system som är nödvändigt för verksamhetsutövarens möjlighet att bedriva sektorsverksamhet,

REMISS

sektorverksamhet	verksamhet som anges i bilaga 1 eller 2 till NIS2-direktivet. Med sektorverksamhet i offentlig förvaltning avses sådan verksamhet som en kommun, region eller statlig myndighet är skyldig att utföra enligt författning,
system	nätverks- och informationssystem enligt 1 kap. 2 § p 19 i cybersäkerhetslag (2025:XX),
systematiskt och riskbaserat arbete	arbete som bedrivs med stöd av interna regler och arbetssätt för att upprätta, genomföra, driva, övervaka, kontrollera, underhålla och utveckla organisationens cybersäkerhet utifrån risk,
säkerhetslogg	registrering av säkerhetsrelaterade händelser,
säkerhetskonfiguration	konfigurationer som påverkar cybersäkerheten,
särskilda it-utrymmen	en lokal eller ett låst skåp som är särskilt utformat för att skydda hårdvara i syfte att säkerställa systemens funktion och behov av fysiskt skydd,
viktig samhällfunktion	en viktig samhällsfunktion är en sådan samhällsfunktion som är nödvändig för samhällets grundläggande behov, värden eller säkerhet.

.

2 kap. Organisatoriska säkerhetsåtgärder

Systematiskt och riskbaserat arbete

1 § Verksamhetsutövarens arbete med cybersäkerhet ska vara systematiskt, riskbaserat och integrerat med befintliga sätt att leda och styra organisationen. Verksamhetsutövaren ska identifiera och hantera behovet av att använda relevanta standarder i arbetet.

Allmänna råd

Som stöd för arbetet bör följande eller motsvarande standarder användas:

REMISS

1. Svensk standard SS-ISO/IEC 27001:2022 Informationssäkerhet - cybersäkerhet och integritetsskydd – Ledningssystem för informationssäkerhet – Krav, och
2. Svensk standard SS-EN ISO/IEC 27002:2022 Informationssäkerhet – cybersäkerhet och integritetsskydd- Informationssäkerhetsåtgärder.

---

2 § Det systematiska och riskbaserade arbetet ska minst omfatta att

1. identifiera och analysera externa krav, interna behov och risker avseende cybersäkerhet,
2. utifrån externa krav, interna behov och risker utforma och införa säkerhetsåtgärder,
3. följa upp och utvärdera risker och säkerhetsåtgärder, samt
4. vid behov förbättra säkerhetsåtgärder.

Interna regler och arbetssätt

3 § Verksamhetsutövaren ska upprätta de interna regler och arbetssätt som behövs för arbetet med att genomföra lämpliga och proportionella säkerhetsåtgärder utifrån ett allriskperspektiv. Interna regler och arbetssätt ska dokumenteras och hållas uppdaterade. De ska

1. utgå från ledningens mål och inriktning,
2. utformas utifrån externa krav, interna behov och risker,
3. vid behov kompletteras med stöd för hur interna regler och arbetssätt ska tillämpas, samt
4. kommuniceras till berörd egen och inhyrd personal.

4 § Interna regler och arbetssätt ska minst innehålla

1. vilken säkerhetsåtgärd som avses,
2. vilken målgruppen är,
3. beslutsdatum samt vilken roll som ansvarar för att dokumentet hålls uppdaterat,
4. hur och när de interna regler och arbetssätt ska följas upp och utvärderas,
5. beskrivning av
   a) vad som ska göras,
   b) när det ska göras,
   c) hur det ska göras,
   d) vilka roller som ska göra vad,
   e) vilka beslut som ska fattas, när och av vilken roll, samt
6. hur resultatet av tillämpningen av interna regler och arbetssätt ska dokumenteras och när det ska följas upp och utvärderas.

Dokumentation av interna regler och arbetssätt ska bevaras i minst 5 år.

Dokumentation av resultatet av tillämpningen av interna regler och arbetssätt ska, om inte särskilda hinder identifierats, bevaras i minst 5 år.

REMISS

Underlag enligt 2 kap. 24 § och de beslut som ledningen fattar med anledning av arbetet med övervakning av genomförandet av säkerhetsåtgärder ska bevaras i minst 5 år.

5 § I interna regler och arbetssätt ska minst följande ingå

1. organisatoriska säkerhetsåtgärder i enlighet med kapitel 2,
2. tekniska och driftrelaterade säkerhetsåtgärder i enlighet med kapitel 3,
3. fysiska säkerhetsåtgärder i enlighet med kapitel 4, och
4. relevanta sektorsspecifika säkerhetsåtgärder i enlighet med kapitel 5.

Ledningens ansvar för säkerhetsåtgärder

6 § Ledningens ansvar att leda och styra arbetet med cybersäkerhet ska minst omfatta att

1. besluta om mål och inriktning,
2. säkerställa att arbetet med att genomföra säkerhetsåtgärder bedrivs systematiskt och riskbaserat med stöd av interna regler och arbetssätt,
3. besluta om arbetsuppgifter och mandat för de roller som arbetet kräver,
4. säkerställa tillgång till kompetens för arbetet,
5. besluta om resurstilldelning,
6. besluta om kriterier för riskacceptans,
7. besluta om acceptabla tider för nedsatt funktionalitet för organisationens verksamheter,
8. besluta om prioriteringsordning för återställning av verksamheter,
9. besluta om vilka system som är sektorskritiska, och
10. övervaka genomförandet av säkerhetsåtgärder.

7 § Ledningen ska minst utse roller motsvarande samordnare, informationsägare och systemägare.

Ledningen ska ge

1. samordnaren mandat att samordna och utvärdera arbetet med säkerhetsåtgärder som stöd för ledningens arbete med cybersäkerhet,
2. informationsägaren ansvar för att information klassas och ges ett tillräckligt skydd och mandat att besluta om att påbörja behandling av information, samt
3. systemägaren ansvar för att system skyddas med lämpliga och proportionella säkerhetsåtgärder och mandat att besluta om driftsättning av system.

Ledningen ska säkerställa att information och system har en informationsägare respektive systemägare. Ledningen ska tydliggöra vilken behandling av information en informationsägare ansvarar för och vilka system som en systemägare ansvarar för.

REMISS

Allmänna råd

Ledningen bör utse systemägare för organisationens olika delar i den digitala miljön.

8 § I ledningens arbete med att övervaka genomförandet av säkerhetsåtgärder ingår att vid behov men minst årligen informera sig om

1. risker som bedöms som allvarliga för cybersäkerheten,
2. status i arbetet med åtgärdsplaner,
3. betydande incidenter,
4. bristande cybersäkerhet hos leverantörer och i leveranskedjor,
5. samordnarens utvärdering enligt 2 kap. 24 §,
6. resultat av intern och extern revision,
7. resultat av genomförd tillsyn, och
8. hinder för att uppnå lämplig nivå av cybersäkerhet.

Ledningens utbildning om säkerhetsåtgärder

9 § Ledningens utbildning om säkerhetsåtgärder ska minst omfatta

1. ledningens roll i arbetet med cybersäkerhet,
2. grundläggande terminologi och relevant reglering,
3. riskhantering och övervakning som ett stöd för att leda och styra arbetet med cybersäkerhet,
4. systematiskt och riskbaserat arbete, samt
5. för ledningen relevanta interna regler, arbetssätt och stöd.

Personalsäkerhet

10 § Verksamhetsutövaren ska säkerställa att egen och inhyrd personal har förutsättningar för att behandla information och system på ett säkert sätt inför och under anställning eller uppdrag. Kontroller ska genomföras i syfte att identifiera risker med åtkomst till information och system. De ska utformas utifrån vilken information och vilka system personalen ska få åtkomst till.

Verksamhetsutövaren ska identifiera och hantera behovet av förnyade kontroller vid förändrade arbetsuppgifter.

Verksamhetsutövaren ska säkerställa att egen och inhyrd personal som avslutar anställning eller uppdrag har informerats om begränsningar av framtida användning av verksamhetsutövarens information.

Allmänna råd

Kontroller bör genomföras genom identitetskontroll, intervju, kontakt med referenser samt verifiering av akademiska, yrkesmässiga och övriga kvalifikationer.

REMISS

11 § Egen och inhyrd personal ska ha relevant och aktuell kunskap och kompetens avseende cybersäkerhet för att kunna omhänderta risker vid åtkomst till information och system.
Interna regler ska minst ange

1. vilka informationsinsatser som egen och inhyrd personal ska ta del av,
2. vilka utbildningar och övningar som olika roller ska genomföra,
3. när och hur informationsinsatser, utbildningar och övningar genomförs, och
4. att tillgängliga och genomförda informationsinsatser, utbildningar och övningar följs upp och utvärderas vid behov men minst årligen.

Omvärldsbevakning
12 § Verksamhetsutövaren ska bedriva omvärldsbevakning för att kunna identifiera omständigheter och risker av betydelse för verksamhetsutövarens cybersäkerhet. I detta ingår att hålla sig uppdaterad om hot, sårbarheter, teknisk utveckling och tillgängligt stöd.

Verksamhetsutövaren ska minst bevaka

1. verksamhetsutövarens nuvarande leverantörer av hård- och mjukvara,
2. den gemensamma kontaktpunkten,
3. den nationella CSIRT-enheten,
4. det nationella cybersäkerhetscentret,
5. den nationella cyberkrishanteringsmyndigheten,
6. relevanta tillsynsmyndigheter,
7. det nationella samordningscentret för forskning och innovation inom cybersäkerhet (NCC-SE), samt
8. Europeiska unionens cybersäkerhetsbyrå (ENISA).

Verksamhetsutövaren ska ansluta sig till automatiska notifieringar av tekniska sårbarheter (ANTS) hos den nationella CSIRT-enheten.

Allmänna råd

Verksamhetsutövaren bör ansluta sig till stöd för informationsutbyte om cybersäkerhet (MISP-SE) hos den nationella CSIRT-enheten.

Informationsklassning
13 § Verksamhetsutövaren ska värdera sin information avseende konfidentialitet, riktighet inklusive autenticitet, och tillgänglighet i olika nivåer utifrån vilka konsekvenser ett bristande skydd kan få.

Interna regler ska minst ange

REMISS

1. att informationsägaren ansvarar för att initiera arbetet med och fastställa resultatet av informationsklassning,
2. vilka kriterier och nivåer som används vid bedömning av konsekvenser,
3. att informationsklassning genomförs innan information behandlas i system, samt
4. att resultatet av informationsklassningen följs upp och utvärderas vid behov men minst årligen.

Allmänna råd

Samma nivåer för bedömning av konsekvenser bör användas som vid värdering av risker.

Kriterier och nivåer bör utformas så att bedömningarna kan jämföras över tid.

Riskhantering

14 § Verksamhetsutövaren ska utifrån ett allriskperspektiv identifiera, analysera och värdera risker för att få underlag för valet av lämpliga och proportionella säkerhetsåtgärder.

Interna regler ska minst ange

1. att riskanalys genomförs
   a) innan information behandlas i system, och
   b) vid förändrade hot och nya sårbarheter ,
2. att uppgiften att initiera arbetet med och fastställa resultatet av riskanalysen utförs av
   a) informationsägaren avseende den information som denne ansvarar för, och
   b) systemägaren avseende de system och de delar av den digitala miljön som denne ansvarar för,
3. att resultatet av informationsklassningen och risker som identifierats genom omvärldsbevakning används som ett ingångsvärde i riskanalysen,
4. vilka kriterier och nivåer som används vid bedömning av konsekvenser och sannolikhet, samt
5. att resultatet av riskanalysen följs upp och utvärderas vid behov men minst årligen.

15 § Risker för system, segment och den digitala miljön ska identifieras, analyseras och värderas. I detta ingår att identifiera risker med

1. aggregering och ackumulering av information,
2. användning av mobila system, och
3. utkontraktering.

REMISS

16 § De säkerhetsåtgärder som väljs för att åtgärda identifierade risker ska dokumenteras i en åtgärdsplan eller motsvarande. I åtgärdsplanen ska minst anges

1. vilket system, segment eller vilken del av den digitala miljön som avses,
2. vilka säkerhetsåtgärder som övervägts respektive valts,
3. motivering av valet av en säkerhetsåtgärd utifrån ledningens kriterier för riskacceptans,
4. vilken risk som en säkerhetsåtgärd avser att reducera,
5. tidpunkt för när en säkerhetsåtgärd ska vara genomförd,
6. vem som ansvarar för att en säkerhetsåtgärd genomförs, och
7. hur stor risken bedöms vara efter att säkerhetsåtgärden är genomförd.

Arbetet med säkerhetsåtgärder enligt åtgärdsplanen ska följas upp utifrån identifierat behov, men minst var tredje månad.

Incidenthantering

17 § Verksamhetsutövaren ska kunna upptäcka och vidta åtgärder för att minimera konsekvenserna av incidenter och tillbud i system.

Interna regler ska minst ange

1. hur information om incidenter och tillbud samlas in,
2. hur konsekvenserna av den inträffade incidenten bedöms,
3. hur konsekvenser av inträffade incidenter minimeras,
4. hur risken för ytterligare incidenter eller tillbud beaktas vid valet av åtgärder,
5. hur behandling av information återställs med stöd av driftsdokumentation,
6. hur åtgärder som vidtagits eller övervägts för att återställa information och system dokumenteras,
7. hur samverkan vid incidenter och tillbud med berörda leverantörer genomförs,
8. när och hur kontakt tas med den nationella CSIRT-enheten för stöd vid incidenter,
9. hur instruktioner från den nationella CSIRT-enheten omhändertas,
10. hur externa krav på rapportering av incidenter och tillbud uppfylls,
11. hur och när berörda målgrupper informeras,
12. hur verksamhetsutövaren ska uppfylla informationsskyldigheten vid betydande incidenter och betydande cyberhot,
13. när och hur inte tidigare publicerade sårbarheter i hårdvara och mjukvara rapporteras till den nationella CSIRT-enheten, samt
14. att och hur en grundorsaksanalys genomförs efter en incident om grundorsaken inte redan är känd.

REMISS

Allmänna råd

Resultatet av informationsklassningen för den information som berörs av incidenten bör användas som ingångsvärde för bedömningen av incidentens konsekvens.

I arbetet med återställning bör vidtagna åtgärder, genomförda riskanalyser, beslut, samt avsteg från interna regler och arbetssätt dokumenteras.

Berörda målgrupper bör skyndsamt informeras om hur de kan agera för att minimera konsekvenser av det inträffade.

Det bör anges när en grundorsaksanalys ska genomföras efter inträffade tillbud.

Kontinuitetshantering

18 § Verksamhetsutövaren ska kunna bedriva sin verksamhet trots nedsatt funktionalitet eller otillgänglighet i system i produktionsmiljön.

Interna regler ska minst ange

1. hur konsekvenser av nedsatt funktionalitet och otillgänglighet hos system bedöms,
2. hur informationsägare ska bedöma behovet av att behandla information under störda förhållanden utifrån vad som är acceptabla tider för nedsatt funktionalitet och otillgänglighet för verksamheten,
3. hur och när alternativa arbetssätt ska användas vid störda förhållanden samt hur och när återgång till normalt arbetssätt ska göras,
4. hur återställning av system ska genomföras utifrån ledningens prioriteringsordning för återställning av verksamhet,
5. hur behov av resurser för att upprätthålla kontinuitet tillgodoses,
6. vilka krav som ska ställas på leverantörer för att tillgodose verksamhetens behov av kontinuitet,
7. hur och när stöd från cyberkrishanteringsmyndigheten ska användas, och
8. hur kontinuitet ska övas.

19 § Verksamhetsutövaren ska

1. identifiera och hantera behovet av redundanta funktioner för system i produktionsmiljön,
2. placera system som skapar redundant funktion i fysiskt åtskilda sektioner, och
3. öva återställning av sektorskritiska system vid behov men minst årligen.

20 § Verksamhetsutövaren ska identifiera och hantera behovet av kontinuitet i utvecklings-, test- och utbildningsmiljö.

REMISS

Krishantering

21 § Verksamhetsutövaren ska minimera konsekvenser vid kriser orsakade av nedsatt funktionalitet i eller otillgänglighet hos system, segment, den digitala miljön eller leveranskedjor.

Interna regler ska minst ange

1. hur roller, mandat och arbetsuppgifter fördelas vid kriser med olika ursprung och konsekvenser för produktionsmiljön,
2. hur samverkan med berörda roller inom incident- och kontinuitetshantering genomförs,
3. fastställa när och hur roller som ska delta i arbetet vid en kris ska kontaktas,
4. hur stöd och instruktioner från cyberkrishanteringsmyndigheten omhändertas, och
5. hur och när arbetssätt för olika kriser ska övas.

Vid en cybersäkerhetskris ska verksamhetsutövaren på begäran av cyberkrishanteringsmyndigheten delta vid samverkanskonferenser och följa instruktionerna om hur konsekvenserna ska begränsas.

Allmänna råd

Vid krishantering bör etablerad stabsmetodik och struktur användas.

22 § Verksamhetsutövaren ska identifiera och hantera behovet av

1. att teckna avtal med leverantörer om stöd före, under och efter en kris,
2. tillgång till system för intern och extern kriskommunikation med höga krav på robusthet och tillgänglighet för informationsdelning och samverkan under kriser, samt
3. använda system för kriskommunikation som stöd för extern informationsdelning och samverkan före, under och efter en kris.

Allmänna råd

I syfte att stärka förmågan till kriskommunikation mellan olika organisationer som kan komma att påverkas vid en samhällsstörning bör verksamhetsutövaren öva att använda det webbaserade informationsdelningssystemet WIS som tillhandahålls av Myndigheten för civilt försvar.

Uppföljning och utvärdering

23 § Verksamhetsutövaren ska vid behov men minst årligen bedöma effektiviteten av införda säkerhetsåtgärder genom att följa upp och utvärdera deras lämplighet och proportionalitet i förhållande till externa krav, interna behov och risk.

REMISS

Allmänna råd

Vid uppföljning och utvärdering av säkerhetsåtgärder bör etablerade metoder användas. Exempel på sådana metoder är egenkontroller, granskningar, tester samt interna och externa revisioner. Uppföljning och utvärdering bör genomföras i samband med att säkerhetsåtgärder införs. Det bör även ske vid förändrade hot eller när nya sårbarheter identifieras.

Verksamhetsutövarens systematiska och riskbaserade arbete med cybersäkerhet bör följas upp och utvärderas. Det bör omfatta hur ledningens mål och inriktning efterlevs och omfatta om interna regler, arbetssätt och stöd motsvarar verksamhetens behov. Vidare bör hinder för arbetet bedömas, till exempel brister i tilldelning av arbetsuppgifter, mandat, kompetensförsörjning eller resurser.

Uppföljning och utvärdering bör även göras vid verksamhetsuppföljning, omorganisation, förändrade rättsliga krav, inför beslut om utkontraktering samt efter betydande incidenter.

24 § Samordnaren ska utvärdera nivån på cybersäkerheten i förhållande till externa krav, interna behov och risk utifrån minst följande underlag

1. ledningens mål och inriktning,
2. genomförda informationsklassningar,
3. genomförda riskanalyser,
4. aktuella åtgärdsplaner,
5. utvärdering av säkerhetsåtgärder,
6. information om inträffade incidenter och tillbud samt genomförda grundorsaksanalyser,
7. utvärdering av cybersäkerhet hos leverantörer och i leveranskedjor, samt
8. genomförda interna och externa revisioner.

3 kap. Tekniska och driftrelaterade säkerhetsåtgärder

Förvärv, utveckling och underhåll av system

1 § Verksamhetsutövaren ska säkerställa att systemen skyddas med lämpliga och proportionella säkerhetsåtgärder genom systemens livslängd.

2 § Verksamhetsutövaren ska identifiera och hantera behovet av att välja system och tjänster som är certifierade i enlighet med europeiska ordningar för cybersäkerhetscertifiering av IKT-produkter, IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster enligt artikel 1, första stycket b, i 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 526/2013 (cybersäkerhetsakten)

REMISS

Allmänna råd

Sektorskritiska system bör vara certifierade enligt EU:s cybersäkerhetsförordning (EU 2019/881).

3 § Innan avtal som innefattar att behandling av information utkontrakteras tecknas med en leverantör ska verksamhetsutövaren

1. genomföra en informationsklassning av den information som ska utkontrakteras,
2. ha åtgärdat de risker utkontrakteringen innebär,
3. säkerställa att informations- och systemägare är utsedda för den informationshantering som utkontrakteras,
4. identifierat de krav på säkerhetsåtgärder som behöver ställas på leverantören,
5. kontrollerat att tilltänkt leverantör uppfyller kraven på säkerhetsåtgärder och bedömt att leverantören kommer att kunna uppfylla kraven under avtalstiden, samt
6. säkerställa att avtalet reglerar

    a) vilka säkerhetsåtgärder leverantören ska vidta,
    b) vilken kompetens avseende cybersäkerhet leverantören behöver
    c) när och hur leverantören ska informera om förändringar i system som kan påverka avtalsefterlevnaden,
    d) hur leverantören ska informera verksamhetsutövaren om misstänkta och inträffade incidenter och tillbud,
    e) i vilken omfattning leverantören ska öva incident-, kontinuitets- och krishantering med verksamhetsutövaren,
    f) hur leverantören ska informera verksamhetsutövaren om identifierade sårbarheter,
    g) hur leverantören ska följa upp sin egen och eventuella underleverantörers efterlevnad av ställda avtalskrav på säkerhetsåtgärder att verksamhetsutövaren har rätt att följa upp efterlevnaden av ställda krav, samt
    h) hur verksamhetsutövarens information ska återlämnas eller förstöras när avtalet upphör.

Innan behandlingen av information hos leverantören påbörjas ska verksamhetsutövarens informationsägare godkänna behandlingen och verksamhetsutövarens systemägare fatta beslut om driftsättning.

4 § Inför och under utveckling av system ska verksamhetsutövaren säkerställa att

1. informationsägare och systemägare involveras i arbetet för att identifiera och hantera behov av säkerhetsåtgärder,

REMISS

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.

5 § Innan ett beslut om att för första gången driftsätta ett system ska fattas, ska systemägaren minst kontrollera att

1. det finns nödvändig dokumentation för drift och förvaltning,
2. säkerhetstester och granskningar genomförts för att säkerställa att valda säkerhetsåtgärder är lämpliga och proportionella,
3. tilldelade resurser för driften av systemet är tillräckliga,
4. informationsägaren har beslutat om att påbörja behandlingen av information, och
5. en riskanalys av identifierade brister avseende punkt 1-4 genomförts och det är dokumenterat hur dessa åtgärdas.

Systemägaren ska genomföra samma kontroller som ovan vid underhåll av system som innebär en förändring som kan påverka säkerheten i verksamhetsutövarens digitala miljöer.

6 § Innan ett beslut om avveckling av ett system fattas, ska systemägaren minst kontrollera att

1. riskanalys rörande avveckling har genomförts,
2. åtgärdsplan för avveckling finns,
3. tilldelade resurser för avveckling av systemet är tillräckliga,
4. informationsägaren beslutat om att avveckla behandlingen av informationen, och
5. en riskanalys av identifierade brister avseende punkt 1-4 genomförts och det är dokumenterat hur dessa åtgärdas.

Driftrelaterad dokumentation

7 § Verksamhetsutövaren ska upprätthålla uppdaterad dokumentation över befintlig arkitektur. Dokumentationen ska minst beskriva

1. hur den digitala miljön är indelad,
2. vad respektive del innhåller avseende

   a) segment
   b) system,
   c) hårdvara,
   d) mjukvara, och

3. aktuella informationsflöden

   e) mellan olika delar i den digitala miljön,
   f) mellan interna system, samt
   g) till och från system hos andra organisationer.

REMISS

Allmänna råd

Tekniskt systemstöd bör användas för att hålla dokumentationen uppdaterad. Arkitekturen bör visualiseras i en systemkarta.

8 § För varje system som används i produktionsmiljön ska det finnas uppdaterad dokumentation över

1. fastställd systemägare,
2. informationsägare vars information behandlas i systemet,
3. resurser som behövs för drift och förvaltning,
4. förekomsten av information som vid informationsklassning bedömts ha behov av utökat skydd,
5. vilken egen verksamhet systemet stödjer,
6. om systemet är sektorskritiskt och på vilket sätt,
7. om systemet är nödvändigt för att upprätthålla viktiga samhällsfunktioner hos andra organisationer och på vilket sätt,
8. acceptabla tider för nedsatt funktionalitet respektive otillgänglighet,
9. vilka behov av cybersäkerhet som systemet behöver uppfylla,
10. om systemet är placerat i it-segment eller ot-segment,
11. vilken hårdvara som används och hur den identifieras samt dess version,
12. vilken mjukvara som används och dess version,
13. hur hård- och mjukvara är konfigurad,
14. hur systemet återställs,
15. aktuell riskanalys,
16. vilka säkerhetsåtgärder som genomförts för att möta identifierat behov av säkerhet, samt
17. risker som inte åtgärdats.

9 § Verksamhetsutövaren ska identifiera och hantera behovet av dokumentation för varje system i utvecklings-, test- och utbildningsmiljö.

Allmänna råd

Dokumentationen av hur hårdvara identifieras bör inkludera mac-adress och ip-adress.

10 § Det ska finnas en uppdaterad förteckning över

1. vilka system som är sektorskritiska,
2. behandling av information som är utkontrakterad och till vilken leverantör, samt
3. kontaktuppgifter till anlitade leverantörer

    a) för utkontraktering, samt

REMISS

b) av hård- och mjukvara.

Verksamhetsutövaren ska identifiera och hantera behovet av att ha kontaktuppgifter till olika funktioner hos leverantören.

Kontaktuppgifter till funktioner hos leverantören som ger stöd vid incidenter ska finnas lättillgängliga för användning vid incidenthantering.

Segmentering och filtrering

11 § Verksamhetsutövaren ska dela in sin produktionsmiljö i segment för att förhindra spridning och minimera konsekvenser av incidenter. I produktionsmiljöns it-segment ska, om inte särskilda hinder identifierats, minst följande placeras i separata segment

1. klienter för användare,
2. klienter för systemadministration,
3. sektorskritiska system,
4. centrala stödfunktioner i form av skrivare, scanner och liknande,
5. centrala säkerhetsfunktioner,
6. trådlösa nätverk,
7. gästnätverk,
8. system som sammankopplas med system hos leverantör,
9. externt åtkomliga tjänster, och
10. system som innehåller sårbarheter som inte kan hanteras.

Allmänna råd

Följande centrala säkerhetsfunktioner bör placeras i separata segment

1. filtrering av extern kommunikation,
2. behörighetskontroll,
3. säkerhetsloggning,
4. säkerhetskopiering, och
5. övervakning av system.

12 § Verksamhetsutövaren ska identifiera och hantera behovet av

1. att placera varje system, ett begränsat antal system eller system med liknande funktion, användning eller skyddsbehov i separata segment, och
2. ot-segment.

Allmänna råd

Varje sektorskritiskt system bör placeras i separata segment.
Varje system i ot-segment bör placeras i separata segment.

REMISS

13 § Trafik mellan segment ska filtreras så att endast godkända informationsflöden förekommer.

Trafik mellan system inom ett it-segment ska filtreras så att endast godkända informationsflöden förekommer.

14 § Utveckling, tester och utbildning som kan påverka säkerheten i produktionsmiljöns it-segment ska ske i en från produktionsmiljön avskild utvecklings-, test- respektive utbildningsmiljö.

Risker med utveckling, tester och utbildning i produktionsmiljöns ot-segment ska identifieras och åtgärdas.

Behörighetshantering och autentisering

15 § Verksamhetsutövaren ska genom behörighetshantering säkerställa att det endast är behöriga användare och system som har åtkomst till system, segment och olika delar av den digitala miljön.

Interna regler ska minst ange

1. vilken information och vilka system som får vara tillgängliga utan behörighetstilldelning,
2. hur användare och system ska identifieras,
3. hur användare och system ska tilldelas digitala identiteter och behörigheter,
4. när en digital identitet ska låsas, blockeras och tas bort,
5. när behörigheter ska ändras eller återkallas,
6. hur autentiseringsuppgifter ska utformas avseende längd och komplexitet, samt
7. hur autentiseringsuppgifter byts, distribueras och skyddas.

Allmänna råd

Interna regler för behörighetshantering bör ange

1. att en digital identitet i produktionsmiljön endast får användas av en användare eller ett system,
2. tidsbegränsningar för tilldelade digitala identiteter och behörigheter,
3. hur många misslyckade inloggningsförsök som tillåts innan en digital identitets ska låsas, och
4. att kontroll av behörighet ska genomföras innan åtkomst ges till centrala stödfunktioner i form av skrivare, scanner och liknande.

16 § Verksamhetsutövaren ska

1. säkerställa att varje digital identitet inte tilldelas behörighet till mer information eller fler system än nödvändigt,
2. säkerställa att digitala identiteter som används i produktionsmiljön inte används i utvecklings-, test- och utbildningsmiljö,
3. vid behov men minst årligen kontrollera om tilldelade digitala identiteter och behörigheter fortfarande ska kunna användas, samt

REMISS

4. identifiera och hantera behovet av att använda tekniska system som stöd för efterlevnad av interna regler och arbetssätt för behörighetshantering och autentisering.

17 § Digitala identiteter som ger systemadministrativ behörighet ska endast användas för systemadministration och inte innehålla andra behörigheter. Dessa identiteter ska tidsbegränsas och tilldelas restriktivt. Systemadministrativa behörigheter som ges till en leverantör ska begränsas gällande omfattning och tid till aktuellt uppdrag. Tilldelning av andra priviligierade behörigheter ska ske restriktivt.

Allmänna råd

En digital identitet med systemadministrativ behörighet bör endast ges åtkomst till en begränsad del av produktionsmiljön.

18 § För att minimera konsekvenserna av obehörig åtkomst till behörigheter ska verksamhetsutövaren identifiera och hantera behovet av att fördela behörigheter i olika kataloger.

Allmänna råd

I produktionsmiljön bör verksamhetsutövaren använda olika kataloger för

1. it-segment,
2. ot-segment, och
3. publika tjänster som kräver inloggning.

Verksamhetsutövaren bör använda olika kataloger för utvecklings-, test- och utbildningsmiljö.

19 § Vid åtkomst till system som behandlar information som vid informationsklassning bedömts ha behov av utökat skydd ska flerfaktorsautentisering användas.

I produktionsmiljön ska flerfaktorsautentisering användas för

1. egen och inhyrd personals åtkomst via externt nätverk,
2. leverantörers åtkomst via externt nätverk, och
3. systemadministrativ åtkomst till system i nätverk.

Verksamhetsutövaren ska identifiera och hantera övrigt behov av flerfaktorsautentisering i sin digitala miljö.

20 § Verksamhetsutövaren ska identifiera och hantera behovet av att andra organisationer och enskilda personer kan verifiera verksamhetsutövaren som avsändare av information.

REMISS

Allmänna råd

I arbetet med att hantera behovet av att kunna verifiera versamhetsutövaren som avsändare av information bör i e-post, sms, telefonsamtal och webbsidor omhändertas.

På sin webbplats bör verksamhetsutövaren tillhandahålla lättillgänglig information om hur andra organisationer och enskilda personer kan verifiera att det är verksamhetsutövaren som avsändare av information.

21 § Verksamhetsutövaren ska identifiera och hantera behovet av att tillhandahålla e-tjänster som kräver inloggning med e-legitimation och säkerställa tillräcklig redundans i sådana tjänster.

Säkerhetsloggning och logganalys

22 § Verksamhetsutövaren ska genom loggning säkerställa att intrång, tekniska fel och brister i cybersäkerheten kan upptäckas och utredas.

Interna regler ska minst ange

1. vilka säkerhetsrelaterade händelser som ska säkerhetsloggas,
2. tidpunkt för när säkerhetsloggning ska genomföras,
3. hur säkerhetsloggar ska utformas och vilka ytterligare uppgifter som säkerhetsloggarna ska innehålla utöver 26 §,
4. hur säkerhetsloggar ska skyddas mot obehörig åtkomst, obehörig förändring och fysisk skada,
5. var säkerhetsloggar ska lagras och hur länge de ska bevaras, samt
6. när och hur säkerhetsloggar ska analyseras och av vem.

Allmänna råd

Ett centralt systemstöd avsett för säkerhetsloggar bör användas för att samla och analysera loggarna.

23 § Försök till obehörig åtkomst och obehörig åtkomst till den digitala miljön ska loggas.

24 § Följande säkerhetsrelaterade händelser i produktionsmiljön ska minst loggas

1. åtkomst till produktionsmiljön som förutsätter tilldelad behörighet,
2. åtkomst till system som förutsätter tilldelad behörighet,
3. försök till obehörig åtkomst och obehörig åtkomst till
   a) produktionsmiljön,
   b) it- och ot-segment,
   c) system i it-segment, och
4. användning av systemadministrativ behörighet,
5. förändring av säkerhetskonfigurationer,

REMISS

6. förändring av behörighet för användare och system,
7. åtkomst till information som vid informationsklassning bedömts ha behov av utökat skydd, samt
8. händelser som upptäckts genom övervakning och indikerar brister i cybersäkerheten.

25 § Verksamhetsutövaren ska identifiera och hantera behovet av säkerhetsloggning i utvecklings-, test- och utbildningsmiljö.

26 § Säkerhetsloggarna ska minst innehålla uppgift om

1. vilken användare eller vilket system som givit upphov till händelsen,
2. vilken händelse som inträffat,
3. vilken information som har påverkats, och
4. vid vilken tidpunkt händelsen inträffade.

Säkerhetsloggarna ska utformas på ett sätt som möjliggör jämförbarhet mellan olika loggar. Loggarna ska vara tillgängliga för analys under fastställd bevarandetid.

27 § Innehållet i säkerhetsloggarna ska analyseras för att upptäcka och utreda brister i cybersäkerheten.

Robust och spårbar tid

28 § Verksamhetsutövare ska använda robust och korrekt tid som är spårbar till den svenska tillämpningen av koordinerad universell tid, UTC (SP), i sin produktionsmiljö för att möjliggöra jämförbarhet av säkerhetsloggar vid incidenter som involverar andra organisationer.

Verksamhetsutövaren ska identifiera och hantera behovet av att använda robust och korrekt tid som är spårbar till den svenska tillämpningen av koordinerad universell tid, UTC (SP) i utvecklings-, test- och utbildningsmiljö.

Allmänna råd

För robust och korrekt tid bör tidstjänsten Swedish Distributed Time Service användas.

Skydd mot skadlig kod

29 § Verksamhetsutövaren ska använda mjukvara som ger skydd mot skadlig kod för system i it-segment där sådan mjukvara finns tillgänglig.

Verksamhetsutövaren ska identifiera och hantera

1. risker om mjukvara som ger skydd mot skadlig kod inte finns tillgänglig, och
2. behovet av att endast tillåta mjukvara som på förhand godkänts för installation eller användning.

REMISS

Allmänna råd

För system i ot-segment bör mjukvara användas som ger skydd mot skadlig kod om sådan mjukvara finns tillgänglig.

Kryptering

30 § Verksamhetsutövaren ska identifiera och hantera behovet av kryptering för att skydda information i system mot obehörig åtkomst och obehörig förändring vid överföring och lagring.

Interna regler ska minst ange

1. hur nationella rekommendationer från det nationella cybersäkerhetscentret (NCSC) gällande kryptering omhändertas,
2. kriterier för val och godkännande av krypteringsalgoritmer, krypteringsprotokoll och nyckellängder, samt
3. när och hur krypteringsnycklar genereras, distribueras, används, återkallas och förstörs.

31 § Kryptering ska användas i verksamhetsutövarens digitala miljö för att minst skydda

1. säkerhetsloggar, och
2. autentiseringsuppgifter.

32 § Information som vid informationsklassning bedömts ha behov av utökat skydd ska skyddas med kryptering vid överföring till system utanför verksamhetsutövarens digitala miljö.

33 § Domain Name System Security Extensions (DNSSEC) ska användas för domännamn som verksamhetsutövaren registrerat i domännamnssystemet (DNS).

Säkerhetskonfigurering

34 § Verksamhetsutövaren ska skydda system mot obehörig åtkomst genom säkerhetskonfigurering. Konfigurationen ska anpassas till det behov av säkerhet som identifierats.

Som minst ska

1. förinställda autentiseringsuppgifter bytas ut, och
2. funktioner som inte behövs tas bort, stängas av eller blockeras.

Allmänna råd

Tekniska systemstöd bör användas för att införa och följa upp valda konfigurationer.

Direktkommunikation mellan klienter bör inte tillåtas ochinaktiva sessioner bör automatiskt avslutas efter en fördefinierad tidsperiod. Säkerhetsfunktioner bör konfigureras så att säkerhet upprätthålls när tekniska fel och brister inträffar.

Vid säkerhetskonfigurering bör leverantörens rekommendationer och relevanta standarder användas.

REMISS

Säkerhetstester

35 § Verksamhetsutövaren ska genomföra säkerhetstester för att identifiera brister i cybersäkerheten.

Säkerhetstester ska användas för att minst kontrollera att

1. systemen är uppdaterade,
2. konfigurationer omhändertar publicerade sårbarheter, samt
3. valda tekniska säkerhetsåtgärder för system, segment och digitala miljö är genomförda och möter identifierade behov av cybersäkerhet.

Allmänna råd

Etablerad testmetodik bör användas för automatiserade respektive manuella säkerhetstester

Upptäcks sårbarheter som inte tidigare publicerats bör dessa rapporteras till den nationella CSIRT-enheten.

Säkerhetskopiering

36 § Verksamhetsutövaren ska kunna återställa information som förlorats eller förvanskats inom fastställda acceptabla tider för nedsatt funktionalitet och otillgänglighet i system.

37 § Verksamhetsutövaren ska identifiera och hantera behovet av säkerhetskopiering.

Interna regler ska minst ange

1. vilken information som ska säkerhetskopieras,
2. hur ofta och på vilket sätt säkerhetskopior ska tas,
3. hur säkerhetskopior ska skyddas och lagras,
4. hur länge säkerhetskopiorna ska bevaras,
5. hur återläsning av säkerhetskopior ska göras, och
6. hur återläsning av säkerhetskopior kontrolleras.

Säkerhetskopiorna ska skyddas mot obehörig åtkomst, obehörig förändring och fysisk skada. Minst en säkerhetskopia ska skyddas mot skadlig kod genom att lagras på hårdvara separerad från det system som informationen hämtats ifrån.

Allmänna råd

Verksamhetsutövaren bör

1. bedöma programvara, konfiguration och information separat avseende vad som ska säkerhetskopieras och hur ofta,
2. använda tekniskt systemstöd för att kontrollera att information på säkerhetskopior är korrekt och komplett, samt

REMISS

3. kontrollera att information kan återställas från säkerhetskopior inom acceptabla tider för nedsatt funktionalitet och otillgänglighet vid större förändringar av produktionsmiljön men minst årligen.

Övervakning av system

38 § Verksamhetsutövaren ska använda intrångsdetektering och intrångsskydd i produktionsmiljön för att upptäcka intrång, tekniska fel, incidenter och tillbud i egna system.

Behovet av intrångsdetektering och intrångsskydd i utvecklings-, test- och utbildningsmiljö ska identifieras och hanteras.

39 § Behovet av realtidsövervakning ska identifieras och hanteras.

Allmänna råd

Realtidsövervakning bör användas i produktionsmiljön för att skyndsamt upptäcka incidenter och tillbud i centrala säkerhetsfunktioner och sektorskritiska system.

Ändringshantering

40 § Verksamhetsutövaren ska genomföra ändringar i produktionsmiljön på ett strukturerat och spårbart sätt för att minska risken för incidenter och tillbud.

Interna regler ska minst ange

1. kriterier för när och hur uppdateringar och uppgraderingar ska genomföras i it- och ot-segment, samt
2. hur beslut om att genomföra ändringar fattas så att endast godkända ändringar genomförs.

Allmänna råd

Kriterier bör fastställas för när och hur uppdateringar och uppgraderingar ska genomföras i utvecklings-, test- och utbildningsmiljö.

---

41 § Verksamhetsutövaren ska identifiera och åtgärda risker för att säkerheten påverkas när

1. system, it-segment, ot-segment och olika delar av den digitala miljön införs, uppgraderas, uppdateras och avvecklas, samt
2. uppdatering eller uppgradering inte kan genomföras i enlighet med fastställda kriterier eller pågående ändring behöver avbrytas.

42 § I it-segment ska säkerhetsuppdateringar genomföras utan onödigt dröjsmål. Mjukvara som leverantören inte längre tillhandahåller

REMISS

säkerhetsuppdateringar för ska bytas ut eller uppgraderas utan onödigt dröjsmål.

Verksamhetsutövaren ska identifiera och hantera behovet av säkerhetsuppdateringar, uppdateringar och uppgraderingar i ot-segment.

Allmänna råd

Arbetet med att godkänna en säkerhetsuppdatering bör inledas senast inom 72 timmar efter att den tillgängliggjorts av leverantören.

Mjukvara bör uppdateras till senaste version utan onödigt dröjsmål.

4 kap. Fysiska säkerhetsåtgärder

Lokaler

1 § Verksamhetsutövaren ska skydda lokaler där information behandlas mot obehörigt tillträde för att undvika obehörig fysisk åtkomst till, förlust av och fysisk skada på system genom att minst

1. ha ett för verksamheten anpassat skalskydd, samt
2. dela in sina lokaler i fysiskt separerade sektioner utifrån resultat av informationsklassning och riskanalys avseende den information som ska behandlas i lokalerna.

2 § Verksamhetsutövaren ska identifiera och hantera behovet av

1. tillträdesbegränsning till lokaler och sektioner,
2. övervakning av lokaler och sektioner samt av att agera på larm vid obehörigt tillträde,
3. att kontrollera egen och inhyrd personals samt besökares identitet innan de ges tillträde till lokaler och sektioner,
4. särskild sektion för besökare,
5. att inrätta sektioner i form av särskilda it-utrymmen, och
6. ytterliga indelning i sektioner inom särskilda it-utrymmen.

3 § Särskilda it-utrymmen ska förses med övervakning och larm. Tillträde till särskilda it-utrymmen ska tilldelas restriktivt och registreras på individnivå.

4 § För att undvika förlust av, skada på eller funktionsavbrott i system ska verksamhetsutövaren identifiera och hantera behov av att minst skydda lokaler mot

1. brand,
2. vattenskador,
3. onormal luftfuktighet, och
4. onormal temperatur.

REMISS

System

5 § Verksamhetsutövaren ska skydda system mot obehörig fysisk åtkomst, förlust och fysisk skada genom att identifiera och hantera behovet av att placera servrar och nätverksutrustning i särskilda it-utrymmen eller låsta skåp.

Servrar som används för att bedriva sektorsverksamhet ska placeras i särskilda it-utrymmen eller i låsta skåp.

Tekniska försörjningssystem

6 § Verksamhetsutövaren ska undvika förlust av eller skada på system eller avbrott i deras funktion på grund av fel eller avbrott i tekniska försörjningssystem.

Verksamhetsutövaren ska säkerställa tillräcklig funktion och redundans i produktionsmiljö avseende

1. elförsörjning,
2. elektroniska kommunikationsnät och elektroniska kommunikationstjänster,
3. kyla,
4. värme, och
5. ventilation.

7 § Verksamhetsutövaren ska identifiera och hantera behovet av att övervaka de tekniska försörjningssystemens funktion och säkerställa att larm genereras vid otillräcklig funktion vid på förhand fastställda nivåer i produktionsmiljön.

8 § Verksamhetsutövaren ska identifiera och hantera behovet av tillräcklig funktion och redundans hos tekniska försörjningssystem i utvecklings-, test- och utbildningsmiljö.

5 kap. Sektorsspecifika säkerhetsåtgärder

Offentlig förvaltning

System för kriskommunikation

1§ Verksamhetsutövaren ska identifiera och hantera behovet av att använda Rakel (Radiokommunikation för effektiv ledning) och SGSI (Swedish Government Secure Intranet) för kriskommunikation.

2 § Verksamhetsutövare ska en gång per kvartal, kontrollera funktionen hos system för intern och extern kriskommunikation.

REMISS

6 kap. Undantag

Myndigheten för samhällsskydd och beredskap får i enskilda fall och om det finns särskilda skäl medge undantag från tillämpningen av dessa föreskrifter.

---

1. Dessa föreskrifter och allmänna råd träder i kraft [Klicka och skriv tidsangivelse].

Myndigheten för samhällsskydd och beredskap

MIKAEL FRISELL

Tove Wätterstam
Avdelningen för cybersäkerhet och samhällsviktiga kommunikationer

REMISS

Beställningsadress:
Norstedts Juridik, 106 47 Stockholm
Telefon: 08-657 95 00
E-post: order@forlagssytem.se
Webbadress: www.nj.se/offentligapublikationer
Beställningsnummer:

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

Allmänt

Beskrivning av problemet och vad man vill uppnå

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

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

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

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

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

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

REMISS

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

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

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

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

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

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

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

Föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning

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

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

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

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

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

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

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

Cybersäkerhet och civilt försvar

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

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

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

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

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

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

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

Begreppet cybersäkerhet

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

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

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

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

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

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

Systematiskt och riskbaserat arbete

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

Sektorsgemensamma och sektorsspecifika krav

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

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

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

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

[6] Prop. 2025/ s 84 f.

REMISS

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

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

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

Uppföljning av konsekvenser av föreskrifter och allmänna råd

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

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

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

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

Inga föreskrifter eller endast vägledning

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

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

REMISS

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

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

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

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

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

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

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

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

Standarder och certifiering

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

Till detta kommer att en effektiv och rättssäker tillsyn förutsätter att både verksamhetsutövare och tillsynsmyndigheter på ett så enkelt sätt som möjligt ska kunna skilja mellan konkreta krav och vägledning. Tillsynsmyndigheten ska utöva tillsyn över att cybersäkerhetslagen och föreskrifter som har meddelats i anslutning till lagen följs. I Cybersäkerhetslagen finns bestämmelser om att tillsynsmyndigheten ska ingripa om verksamhetsutövaren åsidosatt sina skyldigheter enligt regleringen. Ett ingripande sker enligt 4 kap. 1 § cybersäkerhetslagen genom beslut om föreläggande, ansökan om förbud att inneha ledningsfunktion, beslut om sanktionsavgift eller, om det inte finns skäl att ingripa mot en överträdelse på något annat sätt, genom anmärkning. Avsaknad av föreskrifter som förtydligar kraven i lagen bedöms försvåra möjligheterna för både verksamhetsutövare och tillsynsmyndighet att bedöma om verksamhetsutövaren uppfyller lagkraven. Detta får negativ påverkan på rättssäkerheten och försvårar för tillsynsmyndigheterna att bedriva effektiv tillsyn och vid behov ingripa vid en överträdelse. Exempelvis behöver storleken på sanktionsavgifter kunna härledas till de konsekvenser bristande

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

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

Utformning av föreskrifter och allmänna råd

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

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

Hur föreskrifterna och de allmänna råden implementerar cybersäkerhetslagens krav på säkerhetsåtgärder

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

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

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

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

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

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

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

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

2. incidenthantering,

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

3. kontinuitetshantering och krishantering,

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

4. säkerhet i leveranskedjan,

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

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

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

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

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

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

7. grundläggande praxis för cyberhygien och utbildning i cybersäkerhet,

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

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

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

9. personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning,

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

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

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

REMISS

Sektorsspecifika krav

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

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

Uppgifter om vilka som berörs av regleringen

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

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

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

I artikel 2.1 anges att en verksamhet är av tillräcklig storlek om den minst kan betecknas som ett medelstort företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG.13. Ett ytterligare krav är att verksamheten tillhandahåller sina tjänster eller bedriver sin verksamhet i unionen. Artikel 2 i bilagan till kommissionens rekommendation definierar mikroföretag samt små och medelstora företag (SMF-kategorin). Av artikeln följer att ett medelstort företag är ett företag som sysselsätter minst 50 personer eller vars omsättning eller balansomslutning överstiger 10 miljoner euro per år.

Vissa sektorer och typer av verksamhetsutövare behöver enligt NIS2-direktivet inte uppfylla storlekskraven för att omfattas. Det gäller exempelvis verksamhetsutövare som erbjuder allmänna elektroniska kommunikationsnät, allmänt tillgängliga elektroniska kommunikationstjänster, betrodda tjänster,

REMISS

registreringsenhet för toppdomäner, DNS-tjänster eller domännamnsregistrering.

Detsamma gäller

1. verksamhet som är väsentlig för att upprätthålla kritiska funktioner i samhället och ekonomiska funktioner,

2. om en störning i verksamheten kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet, folkhälsa eller medföra betydande systemrisker särskilt om det får gränsöverskridande konsekvenser, eller

3. verksamhet som är kritisk på grund av sin särskilda betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst, eller för andra sektorer som är beroende av denna verksamhet.

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

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

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

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

REMISS

Uppgifter om de bemyndiganden som myndighetens beslutanderätt grundar sig på

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

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

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

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

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

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

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

REMISS

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

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

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

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

Idag är det en självklarhet att en verksamhetsutövare har kostnader för att skydda sina nätverk och informationssystem. I denna kostnad ingår utgifter för system och annat tekniskt stöd för att bedriva verksamheten samt personalkostnader för att upprätthålla en säker informationsbehandling.

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

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

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

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

2 kap Organisatoriska säkerhetsåtgärder

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

REMISS

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

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

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

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

Ledningens utbildning

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

Kompetensutveckling

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

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

Omvärldsbevakning

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

Bedöma risker med aggregerad och ackumelerad information

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

Öva återställning av sektorskritiska system

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

REMISS

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

3 kap Tekniska och driftrelaterade säkerhetsåtgärder

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

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

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

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

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

- ändringshantering.

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

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

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

REMISS

Segmentering och filtrering

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

Säkerhetsloggning och logganalys

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

Robust och spårbar tid

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

Säkerhetstester

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

Säkerhetskopiering

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

Övervakning av system

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

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

Ändringshantering

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

4 kap Fysiska säkerhetsåtgärder

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

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

[16] NIS2-direktivet skäl 79

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

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

Dela in sina lokaler i fysiskt separerade sektioner

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

Säkerställa tillgång till särskilda it-utrymmen med övervakning och larm

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

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

Tillräcklig funktion och redundans gällande tekniska försörjningssystem.

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

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

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

5 kap Sektorsspecifika säkerhetsåtgärder

Offentlig förvaltning

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

Intäkter

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

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

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

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

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

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

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

REMISS

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

Företag

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

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

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

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

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

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

Beskrivning av vilka andra kostnader den föreslagna regleringen medför för företagen och vilka förändringar i verksamheten som företagen kan behöva vidta till följd av den föreslagna regleringen

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

REMISS

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

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

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

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

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

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

Kommuner och landsting

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

Kontaktpersoner

Ange vem som kan kontaktas vid eventuella frågor

Tove Wätterstam eller Helena Andersson

REMISS

Svar på remiss gällande förslag till: **Föreskrifter och allmänna råd om säkerehtsåtgärder och utbildning, Diarienummer MSB 2025-13269**

Svarande organisation:

Intern referens:

För generella kommentarer välj "Generellt" under kolumn Kapitel.
För kommentarer som gäller allmänna råd välj "Allmänna råd" under kolumn annars välj det kapitel du vill lämna synpunter på.
Välj i kolumn Paragraf vilken paragraf du vill lämna synpunkt på
Välj i kolumn Punkt vilken punkt i paragrafen dina kommetarer avser både om de avser paragraf eller allmännt råd.

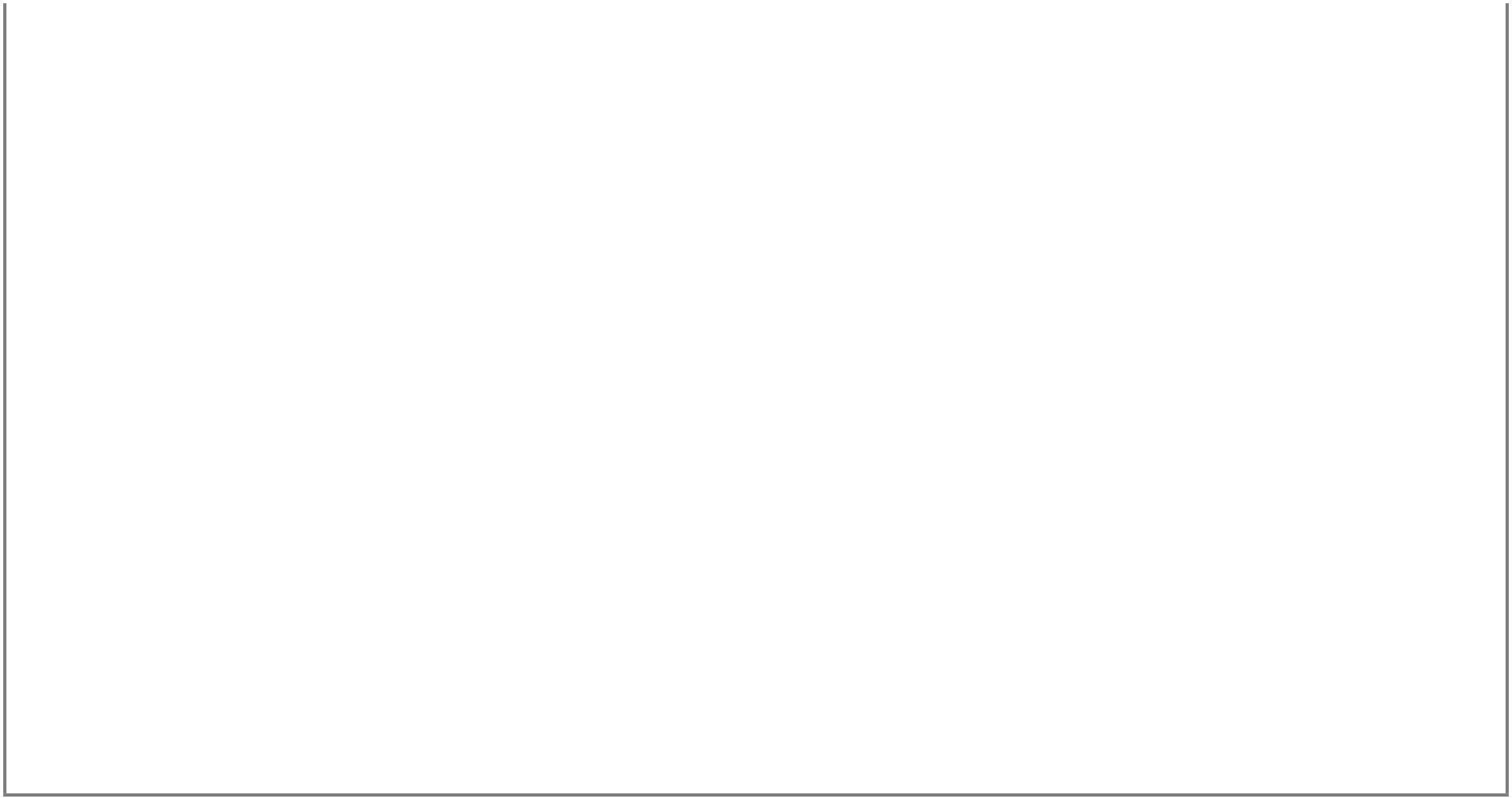
Synpunkter på konsekvensutredningen lämnas på filken Konsekvensutredningen

Vänligen skicka dina svar i excelformat för att underlätta sammanställningen av synpunkter.

Synpunkter föreskrifter och allmänna råd					
Kapitel	**§**	**Punkt**	**Synpunkt**	**Förslag till ändring**	**Kommentar**
Välj	Välj	Välj	Exempel: Saknar mer detaljerade krav	Exempel: Lägg till också krav på X, Y och Z	Exempel: Vi tycker de kraven skulle kunna läggas till i kap 2 paragraf 3,4, eller 7, eller kap 3 paragraf 34.
Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj		

Välj	Välj	Välj			
Välj	Välj	Välj			
Välj	Välj	Välj			

Välj	Välj	Välj			
Välj	Välj	Välj			

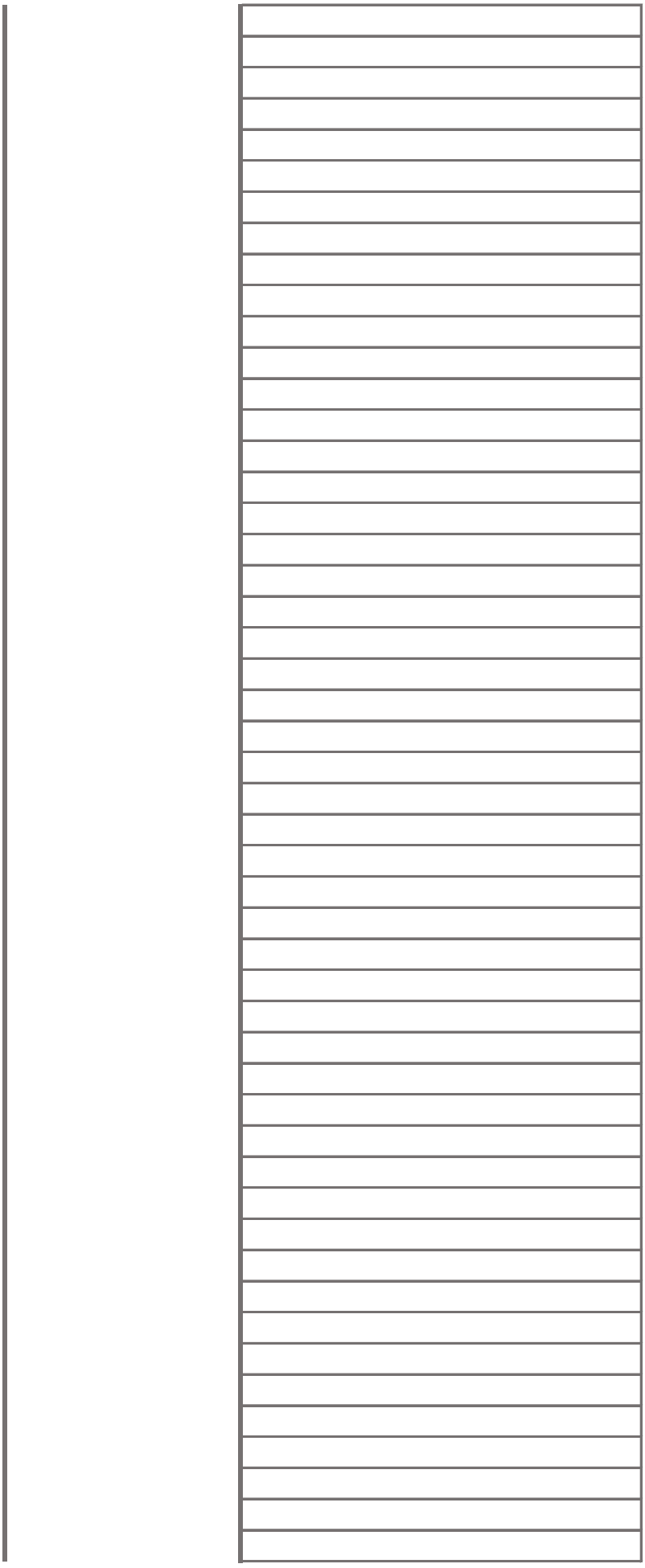


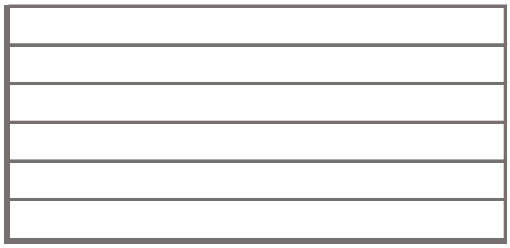
Svar på remiss gällande förslag till:

Svarande organisation:

Intern referens:

Synpunkter Konsekvensutredningen
Rubrik, stycke
Exempel: Rubrik XXXX stycke 4
Exempel: sidan X





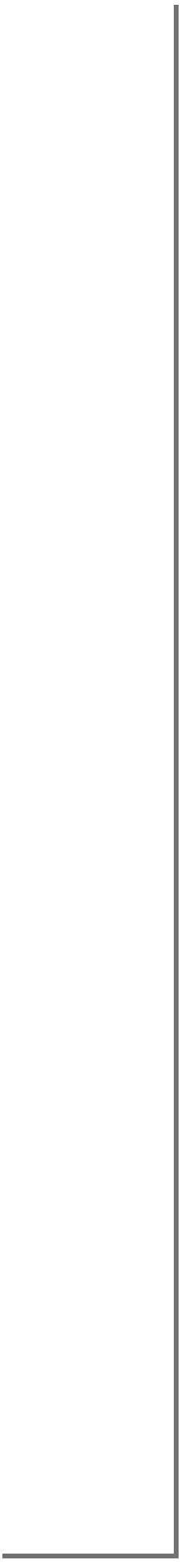
Konsekvensutredning för

Synpunkter
det finns fler exempel
beskrivet spann på kostnaden är x

föreskrifter och allmänna om säkeretsåtgärder och utbildning, Diarienummer MSB 2

Här kan du lämna synpunkter på konsekvensutredningen.

Synpunkter på föreskrifter lämnas på fliken Föreskrifter

Vänligen skicka dina svar i excelformat för att underlätta

Kommentar
komplettera med följande xxxxxx
Vi har följande konstnader för motsvarande xxxxx