Strålsäkerhetsmyndigheten
Swedish Radiation Safety Authority

Regeringskansliet, Försvarsdepartementet, RS
fo.remissvar@regeringskansliet.se

Kopia till:
visnja.raguz@regeringskansliet.se.

Remissvar
Datum: 2024-05-28
Er referens: Fö2024/00496
Diarienr: SSM2024-2339
Dokumentnr: SSM2024-2339-3
Handläggare: Mathias Häggblom
Telefon: 08-799 44 85

Nya regler om cybersäkerhet (SOU 2024:18)

Strålsäkerhetsmyndigheten (SSM) har mottagit en remiss från Försvarsdepartementet av delbetänkandet nya regler om cybersäkerhet (SOU 2024:18). Nedan följer SSM:s remissvar uppdelat på sammanfattande och generella synpunkter, och mer detaljerade synpunkter på utredningens författningsförslag.

Generella synpunkter

SSM anser att regeringen bör överväga att tillsätta en utredning efter att NIS2- och CER-direktiven har införlivats i svensk rätt med uppdrag att se över cybersäkerhets-, säkerhetsskydds- och beredskapsförfattningarna och tydliggöra gränssnitt och relationer mellan dessa. En sådan utredning ges i uppdrag att lämna förslag för att minska fragmenteringen mellan rättsområdena, tydliggöra ansvarsfördelningen mellan myndigheter och om det behövs ytterligare lagstiftning för att skapa en basnivå för it-säkerheten Sverige.

SSM anser att den föreslagna cybersäkerhetslagen bör kompletteras med ett antal revideringar av säkerhetsskyddslagen (2018:585) för att skapa förutsättningar för tillsynsmyndigheter enligt båda lagstiftningar att på ett rationellt och effektivt sätt kunna genomföra sina uppdrag. Utredningen föreslår att krav införs på verksamhetsutövares ledning att genomgå utbildning i riskhanteringsåtgärder inom cybersäkerhet. SSM tillstyrker detta förslag och anser att motsvarande krav på utbildning i riskhanteringsåtgärder bör införas i säkerhetsskyddslagen. SSM tillstyrker även utredningens förslag att tillsynsmyndigheter ska kunna besluta om riktad säkerhetsrevision och säkerhetsskanningar och konstaterar samtidigt att likvärdiga möjligheter för tillsynsmyndigheter bör införas även i säkerhetsskyddslagen. Även den tidigare cybersäkerhetsutredningen (SOU 2021:63) påtalade behovet att stärka just undersökningsbefogenheter i it-system för tillsynsmyndigheter enligt säkerhetsskyddslagen.

SSM konstaterar att utredningens förslag till sanktionsavgifter för enskilda verksamhetsutövare kommer att kunna vara avsevärt högre än motsvarande belopp i säkerhetsskyddslagen. SSM anser att denna asymmetri vad avser sanktionsavgiftsbelopp riskerar att leda till en relativ försvagning av säkerhetsskyddsregelverket, vilket avser att skydda det mest skyddsvärda och att säkerhetsskyddet hos verksamhetsutövare riskerar att missgynnas om dessa istället prioriterar om resurser till förmån för åtgärder enligt cybersäkerhetslagen. SSM anser därför att det finns anledning att se över säkerhetsskyddslagens bestämmelser om sanktionsavgifter.

Utredningens författningsförslag (cybersäkerhetslag och förordning) innehåller begrepp som även finns i säkerhetsskyddsförfattningen, t.ex. begreppet *personalsäkerhet.*

Strålsäkerhetsmyndigheten
Swedish Radiation Safety Authority

SE-171 16 Stockholm
Solna strandväg 96
Tel:+46 8 799 40 00
Fax:+46 8 799 40 10
E-post: registrator@ssm.se
Webb: stralsakerhetsmyndigheten.se

Användandet av det begreppet i två näraliggande författningar kan leda till missuppfattningar vid tillämpningen av författningarna, t.ex. vid tillsyn. SSM anser att det finns behov av att tydligare definiera i cybersäkerhetslagen vad som avses med begreppet och resonera kring eventuella skillnader i betydelse kontra säkerhetsskyddslagen.

SSM anser att det bör utredas om det finns behov av bestämmelse i cybersäkerhetslagen avseende uppgiftsskyldighet myndigheter emellan, samt mellan myndigheter och enskilda verksamhetsutövare. Det bör även utredas huruvida det finns behov av en bestämmelse om tystnadsplikt i cybersäkerhetslagen, likt den som finns i säkerhetsskyddslagen. En sådan utredning bör också se över förutsättningarna för utbyte av uppgifter som omfattas av sekretess med myndigheter och verksamhetsutövare utomlands. Utredningsbehoven avser framförallt förutsättningar för arbetet hos tillsynsmyndigheterna, gemensamma kontaktpunkten, CSIRT-enheten och verksamhetsutövarna vad gäller dataskydd och personuppgiftsbehandling samt delgivning (utbyten) av personuppgifter[1]. Utöver ovan nämnda utredningsbehov finns även behov av att utreda frågor om sekretess och sekretessbrytande bestämmelser vad avser uppgifter om cybersäkerhetsbrister, incidenter, hotinformation, hotaktörsinformation, samt behov av att agera med risk att röja källor, säkerhetsförmågor och kännedom om aktuella sårbarheter.

Synpunkter på förslag till lag om cybersäkerhet

2 kap. 2 §

SSM anser att det bör göras ett tillägg till bestämmelsen som tydliggör gränsdragningen mellan säkerhetsskyddslagen och dess tillämpning och cybersäkerhetslagen. Kraven på verksamhetsutövares anmälan till tillsynsmyndigheten enligt cybersäkerhetslagen bör inte inbegripa de system och den delen av verksamheten som omfattas av säkerhetsskyddslagen.

Förslag till tillägg i den föreslagna bestämmelsen:

2 kap. 2 §
Verksamhetsutövare ska i en anmälan till tillsynsmyndigheten lämna uppgift om identitet, kontaktuppgift, IP-adressintervall, verksamhet och uppgift om i vilka länder verksamheten bedrivs. Gränsöverskridande verksamhetsutövare ska även lämna uppgift om huvudsakligt etableringsställe och i förekommande fall kontaktuppgift till företrädaren.

Ändras uppgifterna ska verksamhetsutövaren anmäla förändringen inom 14 dagar.

Skyldighet att lämna uppgifter i anmälan gäller inte den del av verksamheten som omfattas av säkerhetsskyddslagen (2018:585).

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om uppgifterna.

3 kap.

SSM föreslår att det införs ett krav i cybersäkerhetslagen att verksamhetsutövare ska ha en befattning motsvarande den som finns om kravet på säkerhetsskyddschef i säkerhetsskyddslagen. SSM föreslår därför att krav på inrättande av befattningen *cybersäkerhetschef* införs i cybersäkerhetslagen. SSM anser att denna befattning inte behöver lyda direkt under verksamhetens högsta chef men bör ha tydliga mandat

[1] T.ex. alias, användarnamn, lösenord, digitala certifikat, digitala signaturer, IP-adresser, e-postadresser, domänadresser som inte föregåtts av samtycken, text kopplat till misstänkta hotaktörer och incidenter.

och ha direkt koppling till verksamhetens högsta ledning. En sådan befattning skulle även kunna kombineras med andra befattningar. Cybersäkerhetschefen har till uppgift att leda, samordna och kontrollera cybersäkerheten enligt cybersäkerhetslagen. SSM:s erfarenheter av motsvarande bestämmelser i säkerhetsskyddslagen är att ett samlat funktionsansvar för säkerhetsskyddsarbetet ger stöd till verksamhetsutövaren att leva upp till författningskraven.

Förslag till tillägg i föreslagen cybersäkerhetslag:

3 kap. ny bestämmelse
Vid verksamhet som omfattas av denna lag ska det finnas en cybersäkerhetschef. Cybersäkerhetschefen ska leda och samordna cybersäkerhetsarbetet samt kontrollera att verksamheten bedrivs enligt denna lag och föreskrifter som har meddelats med stöd av denna lag. Detta ansvar kan inte delegeras.

3 kap. 2 §

SSM anser att termen "informationssäkerhetsarbete" i första stycket bör definieras under 1 kap. 2 §. Av definitionen bör framgå att avsett informationssäkerhetsarbete, utöver systemet, även ska omfatta informationen.

3 kap. 5-7 §§

SSM anser att förslaget till cybersäkerhetslag bör innehålla krav på att incidentrapporter även ska meddelas tillsynsmyndigheten, samt att tillsynsmyndigheten får föreskriftsrätt för hur incidentrapportering ska ske till tillsynsmyndigheten. SSM bedömer att denna uppgift inte kommer att innebära någon stor ökning i administrativ börda hos verksamhetsutövare. Om tillsynsmyndigheten anser sig vara i behov av mer information från verksamhets-utövaren bör sådan informationsinhämtning samordnas med CSIRT-enheten för att inte i onödan belasta verksamhetsutövare under pågående incidenthantering. Vid incidenter ska tillsynsmyndigheten utifrån sin kunskap kunna lämna underlag i form av information, operativa råd och vägledning via CSIRT-enheten. Incidentrapporter ska enligt förslaget till cybersäkerhetslag meddelas inom viss tid till CSIRT-enheten vilket SSM tillstyrker då it-incidenter ofta behöver hanteras mycket skyndsamt.

SSM anser att information om it-incidenter är av relevans även för tillsynsmyndigheterna då den är en viktig indikator om cybersäkerhetsstatusen hos verksamhetsutövaren, samt att händelseförloppet utgör relevant underlag för framtida tillsyn. Allvarliga cyberangrepp och bristande cybersäkerhet i kringliggande it-system (som skulle omfattas av cybersäkerhetslagen) är av relevans också för tillsynen av system som omfattas av säkerhetsskyddslagen och kärntekniklagen. Ingången för cyberangrepp mot en verksamhetsutövares system som omfattas av säkerhetsskyddslagen kan antas ofta ske via mindre skyddade it-system och leveranskedjor, som skulle omfattas den föreslagna cybersäkerhetslagen.

Verksamhetsutövarens it-säkerhetskultur är sammanhängande och behöver ses som en helhet utifrån flera författningsområden, inte minst vid kärnkraftverk och reaktoranläggningar.

Förslag till tillägg i föreslagna bestämmelser:

3 kap. 5 §
Verksamhetsutövaren ska som en varning underrätta CSIRT-enheten *och tillsynsmyndigheten* om betydande incidenter inom 24 timmar efter det att

verksamhetsutövaren fått kännedom om den. Det ska anges om att det finns misstanke om incidenten orsakats uppsåtligen och om incidenten kan ha gränsöverskridande effekter.

3 kap. 6 §
Verksamhetsutövaren ska också inom 72 timmar från tidpunkten från kännedom göra en incidentanmälan till CSIRT-enheten *och tillsynsmyndigheten* om betydande incidenter. Den ska innehålla en inledande bedömning av hur allvarlig den betydande incidenten är, konsekvenserna av den och förekomsten av angreppsindikatorer. Vidare ska tidigare varning enligt 5 § uppdateras.
CSIRT-enheten *och tillsynsmyndigheten* får begära ytterligare information av verksamhetsutövaren.

Tillsynsmyndigheten ska innan begäran om ytterligare information ifrån verksamhetsutövaren samverka med CSIRT-enheten.

3 kap. 7 §
Verksamhetsutövaren ska inom en månad från incidentanmälan i 5 § lämna en slutrapport till CSIRT-enheten *och tillsynsmyndigheten***.** Om incidenten fortfarande är pågående ska i stället en lägesrapport lämnas som ska kompletteras med en slutrapport en månad efter det att incidenten har hanterats.

Förslag till tillägg i den föreslagna bestämmelsen och förslag till ny bestämmelse (cybersäkerhetsförordningen):

36 §
Myndigheten för samhällsskydd och beredskap får meddela föreskrifter om vad som utgör en betydande incident enligt 3 kap. 4 § och om incidentrapportering enligt 3 kap. 5–7 §§ lagen om cybersäkerhet. Tillsynsmyndigheten ska ges tillfälle att yttra sig.

Tillsynsmyndigheten får meddela föreskrifter om incidentrapportering till tillsynsmyndigheten enligt 3 kap. 5–7 §§ lagen om cybersäkerhet.
Innan en tillsynsmyndighet meddelar sådana föreskrifter ska myndigheten samråda med Myndigheten för samhällsskydd och beredskap.

Ny bestämmelse.
Tillsynsmyndigheten ska kunna lämna underlag till stöd för CSIRT-enhetens uppgift enligt 29 § 3 punkten.

4 kap. 2 §

SSM anser att tillsynsmyndighetens undersökningsbefogenheter, möjlighet att utföra säkerhetsrevision, säkerhetsskanning samt CSIRT-enhetens uppdrag inte omfattar de informationssystem och den delen av verksamheten som redan omfattas av säkerhetsskyddsförfattningen. Deltagande i säkerhetskänslig verksamhet och möjligheten att ta del av säkerhetsskyddsklassificerade uppgifter är reglerat i säkerhetsskyddslagen och tillsynen enligt säkerhetsskyddslagen följer en indelning av tillsynsobjekt i säkerhetsskyddsförordningen. En sådan indelning motverkar aggregering av säkerhetskänslig verksamhet och säkerhetsskyddsklassificerade uppgifter genom att dela upp den säkerhetskänsliga verksamheten mellan olika tillsynsmyndigheter.

4 kap 3 §

Utredningen föreslår att tillsynsåtgärder för viktiga verksamhetsutövare endast får vidtas när tillsynsmyndigheten har en *befogad anledning* att anta att lagen eller föreskrifter till lagen inte följs. SSM anser att denna begränsning gör det svårt för

tillsynsmyndigheten att arbeta preventivt med regelefterlevnaden hos verksamhetsutövare. Tillsynsmyndigheternas kontrollmöjligheter kommer att vara begränsade till i huvudsak efterhandstillsyn t.ex. i de fall då brister har meddelats tillsynsmyndigheten via t.ex. funktioner för visselblåsare, eller då incidentrapportering gjorts till den föreslagna CSIRT-enheten, samt i de fall denna meddelar tillsynsmyndigheten enligt 3 kap 4-7 §§ i förslaget till cybersäkerhetslag. SSM anser att denna begränsning bör tas bort.

4 kap 8-9 §§

SSM anser att det bör förtydligas att såväl säkerhetsrevision som säkerhetsskanning innebär att tillsynsmyndigheten ska beredas faktisk tillgång till nätverks- och informationssystemen. SSM anser att en sådan tillgång utgör en förutsättning för att kunna genomföra tillsyn, säkerhetsrevision och säkerhetsskanningar.

Synpunkter på förslag till förordning om cybersäkerhet

SSM anser att det bör tydliggöras i förslaget till cybersäkerhetsförordning att CSIRT-enhetens uppgifter inte omfattar de informationssystem och den delen av verksamheten som omfattas av säkerhetsskyddsförfattningen.

Förslag till tillägg i föreslagen cybersäkerhetsförordning:

Ny bestämmelse
CSIRT-enhetens uppgifter i 29-30 §§ avser inte informationssystem och den delen av verksamheten som hos verksamhetsutövaren omfattas av säkerhetsskyddslagen (2018:585).

8 §

Av 8 § framgår att Energimyndigheten är tilltänkt tillsynsmyndighet för energisektorn. SSM anser att Strålsäkerhetsmyndigheten bör utpekas som tillsynsmyndighet för enskilda verksamhetsutövare som bedriver kärnteknisk verksamhet. Detsamma gäller för transport- och/eller avfallsverksamhet som utgör kärnteknisk verksamhet, för dessa bör SSM vara tillsynsmyndighet istället för Transportstyrelsen och länsstyrelserna.

Kärnkraftverken kommer med utredningens förslag att omfattas av informations- och it-säkerhetskrav i säkerhetsskyddslagen, kärntekniklagen och förslaget till cybersäkerhetslag och därigenom ha två tillsynsmyndigheter inom informations- och it-säkerhet (SSM och Energimyndigheten). SSM bedömer att en sådan ordning medför ökad komplexitet för både verksamhetsutövarna och tillsynsmyndigheterna. SSM:s erfarenheter av den tillsyn som myndigheten har bedrivit gentemot verksamhetsutövares system utifrån säkerhetsskyddslagen och kärntekniklagen visar på en redan signifikant administrativ kostnad för regelefterlevnad. Det kommer att vara svårt att praktiskt särskilja säkerhetsskyddsåtgärder och åtgärder inom informations- och it-säkerhet med stöd av kärntekniklagen från cybersäkerhetslagens riskhanteringsåtgärder.

SSM anser att det finns fördelar ur informationssäkerhetssynpunkt om den nya cybersäkerhetsförordningens indelning av tillsynsmyndigheter baseras på säkerhetsskyddsförordningens indelning. En sådan indelning skulle leda till en minskad spridning av skyddsvärd information mellan olika tillsynsmyndigheter, då skyddsvärden som berör informations- och it-säkerhet (cybersäkerhet) hos en verksamhetsutövare hålls samlad inom en tillsynsmyndighet istället för hos flera. Ovan ordning kan ge synergieffekter även för SSM:s beredning av ärenden om tillstånd för ny kärnkraft.

Undersökningsbefogenheterna säkerhetsskanningar, riktade säkerhetsrevisioner, samt föreskriftsrätt och ingripanden inom den kärntekniska verksamheten förutsätter särskild kompetens och helhetsförståelse om nationella och internationella regelverk inom det kärntekniska området.

Förslag till tillägg i den föreslagna bestämmelsen:

8 §
Följande myndigheter ska vara tillsynsmyndighet enligt lagen om cybersäkerhet och denna förordning för angivna tillsynsområden.

Tillsynsmyndighet	**Sektor**
Länsstyrelserna i Norrbottens, Skåne, Stockholms och Västra Götalands län	Avfallshantering, *med undantag för kärnteknisk verksamhet* Forskning Lärosäten med examenstillstånd Offentlig förvaltning Tillverkning, produktion och distribution av kemikalier Tillverkning av datorer, elektronikvaror och optik Tillverkning av elapparatur Tillverkning av övriga maskiner
Statens energimyndighet	Energi, *med undantag för kärnteknisk verksamhet*
Strålsäkerhetsmyndigheten	*Energi, avfallshantering och transporter inom kärnteknisk verksamhet.* *Tillverkning, produktion och distribution av kärnbränsle.*
Transportstyrelsen	Transporter, *med undantag för kärnteknisk verksamhet*. Tillverkning av motorfordon, släpfordon, påhängsvagnar och andra transportmedel.

I detta ärende har generaldirektören Michael Knochenhauer beslutat. Utredaren Mathias Häggblom har varit föredragande. I den slutliga handläggningen har också inspektören Andreas Flygare deltagit.

Beslutet har fattats digitalt och saknar därför underskrifter.

STRÅLSÄKERHETSMYNDIGHETEN

Michael Knochenhauer

Mathias Häggblom