Datum
2024-05-20

Nr FOI-2024-455-1

Er referens: Christina Siwring

Vår handläggare: Anna Wetter Ryde

Delbetänkandet Nya regler om cybersäkerhet, SOU 2024:18

Sammanfattning av FOI:s synpunkter

Totalförsvarets forskningsinstitut (FOI) redogör i det följande – från de utgångspunkter myndigheten har att beakta – för sina synpunkter på delbetänkandet Nya regler om cybersäkerhet.

FOI ser i huvudsak positivt på utredningens arbete och föreslagna cybersäkerhetslag avseende genomförandet av NIS2-direktivet. Utredningen påvisar flertalet viktiga områden som ur ett nationellt och europeiskt perspektiv är nödvändiga att reglera med hänsyn till det försämrade omvärldsläget och de sårbarheter som kan följa av digitaliseringen i samhället. Med ett ökat beroende av externa tjänsteleverantörer samt en allt vidare exponering av såväl infrastruktur som data behöver lagstiftningen bl.a. tydliggöra roll- och ansvarsfördelning nationellt samt krav på skyndsamhet för att tidigt kunna identifiera och motverka hot.

FOI vill också påpeka att svensk cybersäkerhetslagstiftning idag är anpassad efter fredstida tillstånd trots att cyberkrigföringen – som påpekas i Försvarsberedningens slutbetänkande från 26 april 2024 – pågår hela tiden (*Stärkt försvarsförmåga, Sverige som allierad, Ds 2024:6, s. 210*). FOI menar att en konstant lågintensiv offensiv cyberkrigföring riskerar att underlätta för aggressiva aktörer att förbereda sig också för mer storskaliga angrepp. Mot denna bakgrund är FOI positiv till NIS2-direktivets skärpta krav på cyberdomänen i samtliga medlemsstater. Direktivet bidrar enligt FOI:s mening inte bara till att säkerställa att svensk säkerhet stärks genom att andra EU-medlemsstater blir bundna av direktivets bestämmelser, utan även svensk cybersäkerhet tjänar på att genomgås och förstärkas.

FOI avstyrker dock utredningens förslag i den del som handlar om vilka myndigheter som föreslås ansvara för tillsynen av de berörda sektorerna, inklusive uppmanar till tydliggöranden gällande kraven på nationell samordning och ansvarsfördelning

Postadress
FOI
164 90 STOCKHOLM

Besöksadress
Gullfossgatan 6, Kista
Leveransadress
Gullfossgatan 12, Kista

Telefon
08-55 50 30 00

Fax

registrator@foi.se

Orgnr: 202100-5182
www.foi.se

mellan tillsynsområden (punkt 1). I punkt 2 lämnas härutöver ytterligare kommentarer på utredningens förslag som FOI menar stärker svensk cybersäkerhet.

1. **Informationen om cybersäkerheten bör samlas på särskilda aktörer inom staten och den nationella samordningen bör öka**

FOI *avstyrker* utredningens förslag om att bibehålla befintlig ordning för tillsynsansvariga myndigheter för de berörda sektorerna med några kompletteringar. För myndigheternas samlade systematiska informationssäkerhetsarbete utgör idag flertalet lagstiftningar och tillsynsansvariga myndigheter en utmaning inom samtliga aspekter av den egna informationshanteringen såväl som vid utbyte eller samarbete kring information med externa organisationer. I förlängningen riskerar detta leda till att parallella ledningssystem skapas för att inrikta, stödja och följa upp informationshanteringen. Även om det kräver en viss omfördelning i tillsynsansvaret menar FOI att man nu bör ta tillfället i akt och skapa en mer sammanhållen ordning för *var* i staten stöd till verksamhetsutövarna, incidentrapportering samt uppföljning av informationshantering sker. FOI föreslår mot denna bakgrund att tillsynsansvaret för cybersäkerhetslagen hanteras av de sektorsansvariga beredskapsmyndigheterna som enligt förordningen (2022:524) är utsedda beredskapsmyndigheter, eftersom dessa myndigheter innehar ett övergripande ansvar för att minska sårbarheten i samhället samt har ett viktigt uppdrag att samordna mellan myndigheter.

Enligt utredningens förslag är 6 av de 7 utpekade tillsynsmyndigheterna beredskapsmyndigheter, varav 4 av 7 utgör sektorsansvariga beredskapsmyndigheter. Att låta de sektorsansvariga beredskapsmyndigheterna utöva tillsyn över de sektorer som faller under cybersäkerhetslagen har flera fördelar; dels ges de en förbättrad lägesbild av det allmänna säkerhetsläget, dels underlättas deras ansvar att stödja andra myndigheter och att säkerställa att samordning sker med andra aktörer. Att samla ansvaret på ett fåtal myndigheter kan också förbättra förmågan att bedöma cyberincidenters allvar vilket i sin tur underlättar bedömningar om vilka sanktioner som är rimliga. Detta möjliggör vidare en likvärdig tillsyn över verksamhetsutövarna (såväl offentliga som enskilda). Förslaget är således i linje med FOI:s mening att samordningen om incidenter mellan myndigheter bör förbättras för att möjliggöra att information om allvarliga incidenter (inklusive i enskilda ärenden) delas mellan angränsande myndigheter på ett sätt som gör att det går att förebygga liknande händelser. Detta tyder också på att ansvaret ska ligga på de sektorsansvariga beredskapsmyndigheterna. FOI vill dock påpeka att incidentrapportering bör ske mellan myndigheter i ett tidigt skede och inte efter att en tillsynsmyndighet har behövt agera mot aktörer som bryter mot cybersäkerhetslagen. Att informationen om cybersäkerheten samlas inom ett fåtal aktörer med särskilt ansvar bör stimulera till ett bättre erfarenhetsutbyte mellan berörda verksamhetsutövare.

En annan aspekt av behovet av en förstärkt cybersäkerhet är att det saknas konsensus inom branschen om vad som omfattas av cybersäkerhetsaktens breda definition av cybersäkerhet och cyberhot (som författningsförslaget hänvisar till i kap. 1 § 2). Begreppet används ofta synonymt med antingen informationssäkerhet och/eller IT-säkerhet. Cyber används även inom angränsande områden, för att beskriva tjänsteutbud, kommunikation och infrastruktur eller för att beskriva komplexitet i system av system. FOI menar att begreppet cybersäkerhet bör framgå tydligare i den svenska lagen eller ersättas med mer specifika begrepp, särskilt då det används i lagstiftning och med anledning av den otydlighet som omgärdar dess tillämpning och möjliga påverkan i de områden lagstiftningen avser att reglera. Däremot får en precisering av begreppen inte inkräkta på cybersäkerhetsaktens definition, med anledning av EU-rättens krav. Tydliga definitioner är också viktiga i ljuset av aktuell sanktionslagstiftning, vilket följer av både svensk och EU-rättslig lagstiftning.

Även om FOI ser en poäng med att de utpekade länsstyrelserna i nuläget görs ansvariga för cybersäkerheten på regional nivå – eftersom de utgör högsta civila totalförsvarsmyndigheter på länsnivå – bör uppmärksammas att information sprids bortom regionala gränser, varför ett regionalt tillsynsansvar inte bidrar på annat sätt än att länsstyrelser exempelvis har god kännedom och kontakt med det lokala näringslivet. Utifrån FOI:s perspektiv bör dock ansvaret för all cyber- och informationssäkerhet på sikt samlas i en central myndighet.

2. Positivt att fler verksamhetsutövare omfattas av cybersäkerhetslagen

FOI *tillstyrker* förslaget om att fler verksamhetsutövare bör omfattas av cybersäkerhetslagen, än vad NIS2-direktivet uppställer som ett minimikrav. Att de identifierade statliga myndigheterna, regionerna och kommunerna bör omfattas styrks av en FOI-rapport från januari 2024, som pekar på bristfällig incidentrapportering i kommuner och statliga myndigheter samt på hur det delegerade ansvaret för cybersäkerheten till myndigheterna riskerar att leda till urvattnad cybersäkerhet (*Delat ansvar är ingens ansvar?, FOI-R—5546—SE, januari 2024, s. 22)*. Rapportförfattarna kan inte konstatera om det är det delegerade ansvaret eller den bristande styrningen från regeringen som är problemet, utan nöjer sig med att konstatera att det finns brister i hur cybersäkerheten hanteras av svenska myndigheter och kommuner.

Även om NIS2-direktivet ger medlemsländerna en möjlighet att undanta kommuner från direktivets tillämpningsområde delar FOI mot ovan angivna bakgrund utredningens förslag om att kommuner bör omfattas, givet deras ansvar för olika samhällstjänster, däribland dricksvatten och hemtjänst. Den kommunala självstyrelsen är i detta avseende inte ett problem eftersom det rör sig om ett område som kommunerna inte själva kan besluta om (dvs. varken om det frivilliga eller det fakultativa verksamhetsområdet), varpå det står riksdagen – eller EU efter riksdagens maktöverlåtelse – fritt att lagstifta om frågan.

FOI ger även stöd åt utredningens förslag att lärosäten med examenstillstånd bör omfattas av cybersäkerhetslagen och delar i denna del UHR-utredningens syn på riskerna som övergången till ett öppet vetenskapssystem kan medföra. I sin utredning påpekar UHR att övergången till ett öppet vetenskapssystem (där tillgång till forskningsdata ingår) är en strategisk satsning som dock kan medföra risker för stöld, störningar eller oönskad överföring av kunskap och resultat på sätt som forskare och andra aktörer i forsknings- och innovationssystemet inte avser. Olika typer av data är olika känsliga för delning och spridning och det krävs således medvetenhet och noggrannhet i hanteringen så att enbart personer med verkligt behov har tillgång till känsliga data, och att data inte kan spridas på ett otillbörligt sätt eller lämnas öppet för åtkomst via cyberangrepp (*Ansvarsfull internationalisering, UHR, Rapport 2024:1, s. 43)*. FOI anser att utredningens förslag om att tillämpa cybersäkerhetslagen på lärosäten med examenstillstånd är proportionerligt i och med att NIS2-direktivet inte innehåller bestämmelser som inskränker lärosätenas akademiska frihet. En aspekt i denna bedömning är att verksamhetsutövare som åläggs sanktioner med stöd i NIS2-direktivet alltid kan överklaga beslut till domstol. Detta gäller även offentliga verksamhetsutövare.

FOI gör vidare bedömningen att myndigheten själv inte kommer att omfattas av NIS2 (med utgångspunkt kap. 1 § 9 i författningsförslaget, respektive genom förklaring på s. 162 i utredningen). FOI tillstyrker detta förslag, men vill samtidigt påpeka att om regeringen genom sin föreskriftsrätt avser att ändra denna ordning skulle det krävas en än mer tydlig harmonisering med bl.a. säkerhetsskyddslagstiftningen, samt ett utökat samarbete mellan tillsynsansvariga myndigheter för att inte tillföra otydlighet och komplexitet i informationssäkerhetsarbetet.

Detta remissvar har beslutats av generaldirektör Jens Mattsson efter föredragning av forskare Anna Wetter Ryde. I den slutliga handläggningen har även chefsjurist Eva Liljefors och enhetschef Jessica Appelgren deltagit.

Kista, som ovan

…….
Jens Mattsson

……..
Anna Wetter Ryde

Sändlista:

Internt FOI
Registrator
GD-sekreterare
Särskild rådgivare
Chefsjurist
AC FA