Remissvar delbetänkandet SOU 2024:18
Till Försvarsdepartementet: fo.remissvar@regeringskansliet.se
Kopia till: visnja.raguz@regeringskansliet.se

Fö2024/00496

Cybersäkerhetslagen och -förordningen

20240527

Detta remissvar har förberetts av remissrespondenter från små och medelstora företag, samt science park -grupper, och från offentlig sektor, som träffats under två möten för att diskutera SOU 2024:18. Syftet med detta gemensamma svar är att särskilt lyfta lagförslagets effekter utifrån företagsperspektivet, inte minst utifrån förutsättningarna för de små och medelstora företagen att arbeta med cybersäkerhet. Detta torde vara viktigt, i och med NIS2 -direktivet, och dess skäl som lagförslaget hänvisar till, understryker att syftet och ändamålet är att höja och harmonisera den gemensamma marknadens motståndskraft mot cyberrelaterade incidenter, attacker och händelser, samt öka förmågan att mitigera effekterna av dessa så att verksamheterna som ska återfå snabbt och effektivt sin drift vid sådana händelser.

Den gemensamma marknaden inom EU är en central grundbult inom EU och därmed finns det även ett antal viktiga EU-rättsliga principer och praxis som de nationella rättsordningarna förväntas att ta hänsyn till. Detta är särskilt viktigt för företag som har verksamhet samtidigt i olika EU-länder. Den ytterst snabba utvecklingen inom AI-området gör en det än mer angeläget att få en effektiv och träffsäker cybersäkerhetslagstiftning på plats snarast.

Remissrespondenterna är överens om att direktivet EU 2022/2555, så kallade NIS2 och cybersäkerhetslagen behövs och är bra i sin grundmening. Direktivet är en viktig författning som särskilt tillsammans med andra kommande EU-författningarna inom EU:s cybersäkerhetsramverk kommer att höja säkerheten inom EU:s digitala infrastruktur, digitala nätverk och system, samt hos enskilda verksamheter. Vi får dagligen höra om cyberattacker såsom belastningsattacker som får viktiga servrar kollapsa, eller *ransomware* -attacker som är systematiska rån mot verksamheter ofta med stora ekonomiska och immateriella skador som följd, bedrägerier, ideologiska attacker, med mera. Det torde inte vara oklart för någon att cybersäkerhetslagen är helt nödvändig.

I) Remissrespondenterna välkomnar följande innehåll i cybersäkerhetslagen

- Direktivets ansats att inte göra skillnad mellan IT och industriella OT-system, är bra och nödvändigt, då vi ofta upplever att cybersäkerhetsinstruktioner skapas av IT -avdelningar till IT-användare, och kan till och med bli direkt kontraproduktiva inom en industrimiljö som ofta är en unik sammansättning av komponenter och system, och måste skyddas som sådan.

- Även skarpa konsekvenser och ett utbildningskrav för organisationsledningen är positivt, eftersom det bidrar till att ta fram skydds- och åtgärdsplanering som har sin utgångspunkt i förståelsen av den egna organisationen.

- Riskbaserad utgångspunkt är mycket bra eftersom det tvingar organisationer att analysera sina hot och risker konkret, samt utgå från dessa vid åtgärder.

- Att inkludera forskningen och lärosäten med examensrätt upplevs som en viktig punkt eftersom på detta sätt kommer cybersäkerheten in i innovation, produktutvecklingen från början, och inte som ett främmande inslag senare. Vi ser gärna att cybersäkerheten får ett affärsperspektiv i hela värdekedjan.

- Att lägga ett ansvar på verksamheter för att kontrollera och fastställa säkerheten inom leverantörskedjan är en bra princip för att sprida säkerheten i samhället såväl inom den privata och den offentliga sektorn.

II) Remissrespondenterna är kritiska till följande innehåll i cybersäkerhetslagen och föreslår ändringar:

1) Standardneutraliteten kan leda till otydlighet och ineffektivt säkerhetsarbete

SOU 2024:18 tar upp begreppet *teknikneutralitet* ungefär som likvärdigt med *standardneutralitet*. Att inte förespråka någon teknisk säkerhetsstandard (t ex inom ISO-gruppen) anses skapa en frihet och teknikneutralitet som kan vara behjälpligt i och med tekniken utvecklas så snabbt inom fältet. Remissrespondenterna noterar dock att NIS2 -direktivet tar upp möjligheten att arbeta med standarderna i artikel 25.1. som följer:

> *För att främja en enhetlig tillämpning av artikel 21.1 och 21.2* [Riskhanteringsåtgärder för cybersäkerhet] *ska medlemsstaterna, utan att föreskriva eller gynna användning av en viss typ av teknik, uppmuntra användningen av europeiska och internationella standarder och tekniska specifikationer av relevans för säkerheten i nätverks- och informationssystem.*

NIS2 -direktivet fastställer även i artikel 21.5 en styrning via tekniska rekvisit, genom att kommissionen kommer senast den 17 oktober anta genomförandeakter för att fastställa de tekniska och metodologiska specifikationerna för de åtgärder som avses i artikel 21.2 beträffande DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster, leverantörer av marknadsplatser online, sökmotorer och för plattformar för sociala nätverkstjänster samt kvalificerade tillhandahållare av betrodda tjänster.

Det är väsentligt att förstå att rättsinformatik som rättsvetenskapligt område hämtar sitt innehåll från andra discipliner än juridiken; och för att upprätthålla en rättssäkerhet, likabehandling och förutsebarhet (alla viktiga rättsliga principer för en ny författning) krävs det innehåll från teknikämnena. Remissrespondenternas mening är att någon konkret hänvisning till vad som uppfyller lagens krav (rekvisitkrav) krävs för att kunna förstå ledarskaps- och teknikkraven i direktivet och lagen.

Bristen på det ovannämnda i lagförslaget har visat sig skapa en hel del frågor om hur lagen ska tolkas:

a. När det gäller små och medelstora företag (SME), så har många remissrespondenter uttryckt en förvåning och oro inför *hur* man ska kunna uppfylla kraven från lagen och direktivet. Inom deras vardag finns det oftast varken personal eller resurser för att sätta sig in och bli experter inom en ny lag, utan det är genom föreskrifter och branschinstruktioner som man lär sig hantera nya utmaningar. Men i detta nu är branschorganisationer och tillsynsmyndigheter lika ovetande kring vilka konkreta åtgärder (rekvisit) som krävs för att uppfylla de olika paragraferna, och särskilt den viktiga 3 kap, § 1 om allriskhanteringen av cyberhot (motsvarar artikel 21.2)

b. Inom NIS -direktivet och dess implementering i lag och förordning har en tydlig hänvisning gjorts till ISO 27000-serien, samt till OT-standard IEC 62443. I och med NIS2 är en utvidgning av NIS2 finns dessa i grunden och bör enligt vår mening hänvisas till, särskilt som

standardhänvisning finns inom direktivets skäl 78 och 79. För SME är det viktigt att veta vilken ledstång man ska välja och följa den hela vägen, men i den nuvarande formuleringen kan det bli aktuellt att ett mindre företag plockar vissa saker från en viss standard och annat från en annan, vilket kommer att leda till en stor förvirring av vad som krävs för att uppnå en godkänd cybersäkerhetsstandard inom verksamheten.

c. Det finns även nationella standarder som har efterfrågats som grund.

Remissrespondenterna anser att en teknikstandardhänvisning bör finnas med i lagkonstruktionen.

2) Användning av korrekt terminologi är av största vikt

I SOU 2024:18 anförs att begreppen i lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster inte kan användas på grund av den förvirring det skulle åsamka. Direktivets begrepp ska i stället användas. Samtidigt anges att direktivet inte ska införlivas direktivnära utan utformas utifrån den systematik och terminologi som används i svensk rätt, där normalt språkbruk ska eftersträvas. En autonom tolkning av EU-rättsliga begrepp ska ge en tolkning som är enhetlig i EU, oavsett hur Sverige väljer att definiera begreppen.

Till följd av detta ter det sig problematiskt när terminologin tidvis är inkoherent med direktivet och andra författningar. Vidare har uppmärksammats vissa fel i den svenska översättningen av NIS2-direktivet. Om terminologin är inkorrekt riskerar bestämmelserna att reglera mer extensivt eller restriktivt, alternativt helt andra områden än avsett. För att en tekniskt kunnig ska kunna uppnå en fullgod cybersäkerhet erfordras att denne inte missuppfattar kraven på grund av missvisande terminologi.

Exempelvis:

- NIS2: Managed service provider översätts till driftsentreprenad. I cybersäkerhetslagen kallas den hanterade tjänster.

  NIS2: Managed security service provider översätts till leverantör av hanterade säkerhetstjänster. I cybersäkerhetslagen kallas det hanterade säkerhetstjänster.

En inkoherent begreppsanvändning riskerar att skapa tolknings- och tillämpningsproblem. Det är önskvärt att lagen överensstämmer med etablerade definitioner inom de avsedda branscherna.

Remissrespondenterna anser att terminologin och koncept behöver justeras och anpassas så att i praktiken etablerade termer både inom juridiken och tekniken används. Om utredaren avsett en skild tillämpning från direktivet behöver detta förklaras närmare. Det noteras även att lagens namn "cybersäkerhetslagen" kan lätt associeras till Cyber Security Act (EU 2019/881).

3. Aktörsundantagen för offentlig sektor saknar till synes stöd i EU-rätten

Med stöd i direktivet föreslås det i lagförslagets 2 kap 1 § att statliga myndigheter (punkt 1) och kommuner, samt lärosäten (punkt 2) är *väsentliga* entiteter (bilaga 1 till direktivet) och omfattas av den högsta kravnivån. Dessa offentliga aktörer omfattas av lagen enligt 2 kap 3 §.
Ändå noterar remissrespondenterna att det svenska lagförslaget erbjuder i 5 kap 8 § 2 st och 5 kap 9 § 3 st den offentliga sektorns verksamheter undantag som saknas för privata företag, och som inte har något stöd inom EU-direktivet. Detta sker genom att koppla direktiv kravet om ett förbud mot att utöva ledningsfunktion till den svenska lagen om näringsförbud (2014:836).
Denna brist på likabehandling av olika verksamhetsutövare är anmärkningsvärt eftersom EU:s grundläggande rättsliga princip om *en EU-konform tolkning* handlar om att de direktivregler som inarbetas i varje medlemslands nationella rättsordning ska tolkas på samma sätt i alla länder (14/83 von Colson, C-

106/89 Marleasing och C-397/01 Pfeiffer). Denna princip är en del av den grundläggande lojalitetsprincipen inom EU-rätten, som fastställer att medlemsstaterna är förpliktade att lojalt genomföra och tillämpa EU-rätten. Lojalitetsprincipen finns kodifierad i art. 4.3 FEU, som är EU:s primärrätt och har företräde för nationella lagar och regler inom mandatområdet.

Därmed har remissrespondenterna följande synpunkter

d. I och med det svenska lagförslaget gör en skillnad mellan privata och vissa statliga och kommunala aktörer uppstår frågan hur de övriga formerna av verksamhetsutövarna och -ägarna träffas av lagen, t ex stiftelser eller ideella föreningar som kan vara ägare av kritisk samhällsviktig verksamhet. Detta är högst oklart och skapar en osäkerhet hos verksamheterna.

   På sidan 130–136 framgår från utredarens resonemang att begreppet myndighetsutövning är otydligt och ej definierat. Dels anses det att den högsta juridiskt ansvariga nivån på kommuner och regioner – förvaltningen, dvs den politiska ledningen - skulle ej uppfattas av kraven på NIS2, och ska därmed undantas av skyldigheterna, något som skulle helt kasta omkull direktivets krav på den högsta ledningen inom väsentliga samhällskritiska entiteter, eftersom nämndordförandena är den högsta juridiska beslutsnivån och bärare av ansvar.

   Samtidigt resonerar utredaren om myndighetsutövningens kärnuppgift såsom: ”att verksamheten ska ha befogenhet att rikta administrativa eller reglerade beslut till fysiska eller juridiska personer som påverkar deras rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital.” Utredaren tolkar det som om dessa rättigheter kan påverkas bara vid faktiskt gränsöverskridande mellan två länder, och verkar obekant med att EU:s inre marknad alltid beskrivs som gränsöverskridande rörlighet för personer, varor, tjänster och kapital. Men även marknaden inuti i ett medlemsland är en del av den gemensamma marknaden och precis på samma sätt som upphandlings- eller konkurrenslagstiftning gäller inom Sverige gentemot svenska rättssubjekt även om de härleds från EU-rätten, är syftet med NIS2 att förstärka och harmonisera cyberskyddet *inom* medlemsländerna (som en del av den gemensamma marknaden) lika mycket som mellan medlemsländerna.

   Enligt EU-domstolens vägledande dom (Case Law), 188/89 Foster vs. British Gas, som har enligt EU-rätten en primärrättslig rättskraft i medlemsländerna, fastställs det att skyldigheten för allmänna och offentliga verksamheter att uppfylla EU-rättsliga krav gentemot enskilda juridiska och fysiska personer får ej undergrävas av en nationell formalitet såsom organisationsform. Denna princip är viktig för att medlemsländerna ska inte kunna genom krav på organisationsformer kunna undvika sitt EU-rättsliga ansvar. I stället är det själva verksamheten och dess effekt på målgruppen som ska avgöra om den träffas av vissa bestämmelser. Resonemanget om olika organisationsnummer för en kommun och för kommunägd samhällsviktig verksamhet (dricksvattenproduktion, el, värme, energi, fiber, mm.) torde därmed strida den ovannämnda vägledande domen och därigenom EU-rätten.

e. Om cybersäkerhetslagen ställer olika krav till exempel på kommunalägda vattenverk och bolagiserade vattenverk hamnar Sveriges kommuner i en situation där likabehandlingsprinciperna slås ut, vilket är rättsosäkert och emot den gemensamma marknadens principer.

f. Enligt praxis i den svenska förvaltningsmodellen kan myndighetsledare inte avsägas från sitt uppdrag, utan normalt flyttas till andra uppdrag inom staten, (LOA 33 §, 2; paragrafen läses jämte RF 12 kap 5 §). Lagstiftaren har därmed löst detta genom att bygga in en skillnad mellan en företagsledare, dvs. styrelsen samt VD, och en myndighetsledare, dvs. GD, beträffande påföljder, i fall dessa inte lever upp till sitt cybersäkerhetsansvar inom organisationen.

Remissrespondenterna anser dock att det inte finns stöd för en sådan uppdelning och olikbehandling utifrån NIS2 och dess skäl eller utifrån gällande EU-primärrätt. Se mer om detta under punkt 6.

Utredaren har heller ej diskuterat det faktum att för företag finns det inbyggt ansvarskrävande och sanktioner redan i form av att till exempel aktiekursen kan påverkas kraftigt av ledningsbeslut eller underlåtenhet, eller att företaget kan gå i konkurs, i värsta fall. Sådana konsekvenser finns inte för en myndighet, som har varken ägartryck eller konkurrens på ”marknaden” för sin verksamhet. Samtidigt är konsekvensen för en ledare av förvaltningsmyndigheten högst en varning och löneavdrag på 25 % under 30 dagar, enligt LOA. Dessa konsekvensskillnader har lagstiftaren inte vägt in på det sätt som sig bör enligt artikel 34.1 i direktivet som tillskriver staterna ett ska-krav över rättsmedel som är effektiva, proportionella och avskräckande,

g. Vidare har lagstiftaren ansett att förvaltningsmyndigheter inom den offentliga verksamheten kan högst få 10 miljoner SEK i påföljd om verksamhetsutövaren orsakar en betydande skada avsiktligt eller på grund av grov oaktsamhet gällande cybersäkerhet. Motsvarande påföljd inom den privata sektorn är 10 miljoner EUR, dvs tio gånger mer i enlighet med direktivets riktlinjer. Åter konstaterar remissrespondenterna att det inte går finna något stöd i direktivet eller inom dess skäl för en nedsättning av påföljden till den offentliga verksamheten.

   Tvärtom kan det påpekas att det är tveksamt om en administrativ avgift på högst 10 miljoner kronor – kombinerad med reglering som undantar ledningen från personligt ansvar – kan anses vara ett rättsmedel som uppfyller kravet av effektivitet, proportionalitet och avskräckning:

   i) stora myndigheter såsom Trafikverket har en årlig budget på över 2,3 miljarder kronor varav de största posterna är utvecklingsarbetet och vägunderhåll. Det är enligt remissrespondenteran inte troligt att vite på 10 miljoner kronor skulle avskräcka eller styra verket att agera på något sätt, utan beloppet skulle accepteras inom ramen för riskaccpetans, och därmed skulle lagen inte ge någon cyberssäkerhetseffekt.
   ii) Genom att tillsynsmyndigheterna själva kommer att kunna bedöma vite på maximalt 10 miljoner EUR eller 2 % av den årliga omsättningen i en koncern, kommer de inte behöva leva som de lär, om deras egen risknivå är en tiondel av detta. Det krävs en tydlig signal till tillsynsmyndigheter att det förväntas av dem intentioner på samma nivå som det förväntas av privata företag.

Remissrespondenterna anser att den offentliga och privata sektorn ska behandlas lika i fråga om konsekvenserna och ansvaret för cybersäkerhetsincidenter. Vidare anses att i och med inom den svenska förvaltningsmodellen den politiska ledningen inom folkvalda förvaltningar är den högsta ansvarige ska det inte finnas ett undantag för deras ansvar för cybersäkerheten.

4. Cybersäkerhetskompetensen inom fältet för att kunna avgöra vad som gäller

Remissrespondenter är generellt oroliga för bristande kompetens inom cybersäkerhetsfältet, både inom SME, men också inom den statliga förvaltningen och övriga aktörer i samhället. Cybersäkerhetslagförslaget ställer just nu ska-krav endast till ledningen av en verksamhet om utbildning inom cybersäkerhet, trots att direktivet ställer mer omfattande krav på hela organisationen samt även om regelbundna övningar. Remissrespondenterna anser att detta borde vara en miniminivå som ställs på alla, oavsett organisationsformen. Det finns inget som hindrar att ställa högre cybersäkerhetskrav än vad direktivet anger i artikel 20.1. Lagkrav skulle hjälpa organisationer att prioritera det systematiska säkerhetsskyddsarbetet.

Remissrespondenter anser att kravet på utbildning och övning bör gälla verksamhetsutövare i sin helhet med inspiration till exempel från brandsäkerhetskraven, arbetsmiljökraven, eller hållbarhetskraven.

5. *Leverantörskedjans ansvar otydligt*

I det nuvarande lagförslaget och dess förarbete är det otydligt hur leverantörsansvaret ska hanteras. Det fastställs att det ska hanteras, men en djupare konsekvensanalys saknas. Remissrespondenterna vill särskilt fästa uppmärksamheten på följande punkter:

h. Många svenska företag faller för nedre strecket "under 50 anställda" / "under 10 M EUR i omsättning". Men samtidigt finns ett underleverantörsansvar. Detta har skapat en del frågor som cybersäkerhetslagen kan inte svara på:

   - Tidsaspekten och *direkt effekt*; i och med Sverige i sitt lagförslag skjuter upp implementeringen till 1 januari 2025 till synes utan ett giltigt undantag, är frågan huruvida en EU-rättslig *direkt effekt* träder i kraft den 18 oktober 2024, och i så fall hur. Det går inte att läsa från lagförslaget eller förarbetet hur NIS2 -direktivet skulle förhålla sig till NIS-lagen som nationellt antas gälla till slutet av året, dvs. om vertikal direkt effekt gäller. Samtidigt har EU-rätten ett företräde och NIS2 direktivet har redan trätt i kraft över ett år sedan. Lagstiftaren bör förtydliga på vilka grunder medlemsstat Sverige skulle inte behöva beakta NIS2 efter den 18 oktober 2024 och hur påverkar det värdekedjan.

   Om leverantörsansvaret träder i kraft den 18 oktober 2024 för företagen som inte träffas direkt av NIS2, måste deras uppfyllelse av cybersäkerhetskraven hanteras kontraktuellt med verksamhetsutövaren som träffas av direktivet och lagen. Detta kräver ett förtydligande i förhållande till andra lagar, såsom aktiebolagslagstiftningen och informationsreglerna för börsnoterade bolag. Remissrespondenterna uppmanar lagstiftaren genast förtydliga vad som gäller rättsligt för leverantörskedjan som inte *per se* träffas av cybersäkerhetslagen, men som måste uppfylla kraven som leverantörer till verksamheter som är inom *scopet*, inom första led.

h. En fråga som behöver belysning är det faktum att om relationen mellan verksamhetsutövaren och leverantören är kontraktuell – och inte indispositiv såsom till exempel säkerhetsskyddslagens krav inom säkerhetsskyddsavtal är – kommer de eventuella tvister om tolkningen hamna i de allmänna domstolarna eller bli förlikningsavtal? En konsekvensanalys av detta torde visa att på grund av det känsliga innehållet inom cybersäkerhetsarbetet kommer företagen och organisationer dra sig för att ta frågor till en allmän domstol, dvs. tingsrätten, och därigenom kommer vi i Sverige också bli utan en rättsskipning vilket innebär att tolkningen och praxis av reglerna kommer inte att utvecklas som sig bör.

Remissrespondenterna uppmanar lagstiftaren att tydliggöra relationen och ansvaret mellan verksamhetsutövarna och leverantörerna, samt stifta regler om en snabb utveckling av implementationsföreskrifter från tillsynsmyndigheterna, för att ge SME en chans att veta vad de ska göra, samt när och hur för att följa lagen. Remissrespondenterna vill påminna lagstiftaren om att eftersom direktivet och lagförslaget kräver en riskanalys och åtgärder av leverantörer som inte träffas av direktivet och lagen direkt, måste detta regleras kontraktuellt inom avtalsrätten, samt via soft law. Det är troligt att vid tvister kommer parterna ej vilja föra talan vid allmänna domstolar, då saken handlar om känsliga uppgifter inom företagen. Därmed kan det antas att praxis och rättsskipning ej kommer ske snabbt inom detta fält, och behovet av föreskrifterna utan fördröjning ökar därav.

6. *Otydlighet om tillsynsmyndigheterna och om CSIRT*

Enligt det svenska lagförslaget kommer ett betydande antal olika statliga förvaltningsmyndigheter bli sektorsansvariga tillsynsmyndigheter. Flera verksamhetsutövare kommer att få fler tillsynsmyndigheter än en. Precis som MSB har i sitt remissvar den 12 april påpekat, finns det oklarheter i samordningen av dessa tillsynsmyndigheter såsom lagförslaget lyder idag. Särskilt förenar vi oss med punkterna 3 och 8 i Myndigheten för samhällsskydd och beredskaps, MSB, svar;

3. En gemensam tjänst för myndighetskontakter behöver skapas.
8. Tillsynssamordningen behöver stärkas.

Respondenterna vill påminna lagstiftaren om, att i samband med (EU) 2016/1148 dvs. NIS-direktivets genomförande 2018, fick flera tillsynsmyndigheter uppgiften att ta fram föreskrifter utifrån lagen, för att ge sektorerna svaret på ”hur” man ska arbeta med cybersäkerheten. Fem år senare hade en myndighet inte fått fram några föreskrifter alls, medan en annan kom med den första branschspecifika föreskriften inom ett samhällskritiskt område först 2023. Notera, att samtidigt har samma myndigheter fått utöva tillsyn enligt så kallade NIS-lagen, SFS 2018/1174. Från verksamhetsutövarnas perspektiv är detta inte rättssäkert eller effektivt och motverkar direktivets och lagens syfte. I den nuvarande formuleringen av cybersäkerhetslagen finns inga verkliga krav på tillsynsmyndigheter att få fram högkvalitativa föreskrifter effektivt och utan fördröjning, samtidigt som samma myndighet har enligt lagförslaget rätt att agera som tillsynsmyndighet. Denna situation kan bli ohållbar för många branscher, särskilt sådana med många små och medelstora företag.

Enligt § 27 i cybersäkerhetsförordningen föreslås MSB fortsättningsvis vara Sveriges nationella CSIRT - enhet, i enlighet med direktivets artikel 15 och utföra för sektorer flera viktiga uppdrag i enlighet med förordningens § 29. Under denna delbetänkandets remisstid har det dock kommit uttalanden från regeringen om att en annan myndighet skulle bli CSIRT-centrum. Remissrespondenterna beklagar den politiska osäkerheten kring frågan eftersom det skapar osäkerhet och minskar planeringsbarheten för alla inom fältet.

Remissrespondenterna vill också påminna om att det lämpliga med att ett cybersäkerhetscentrum som ska betjäna ändamålen och syften av NIS2, finns hos en sektorsmyndighet som ingår EU:s mandatområde, och därmed är van att arbeta med och för den gemensamma marknaden i EU. Polisiär verksamhet, försvaret och domstolarna ingår inte den gemensamma marknaden, eller EU:s mandat hos medlemsländer. Att förvalta cybersäkerhetslagen och -förordningen utan insikter i EU-rätt som gäller den gemensamma marknaden, där de privata företagen agerar, torde vara en utsträckning av NIS2:s syfte och ändamål som går förbi det nationella tolkningsutrymmet enligt EU-praxis.

En tydlig utvärderingsprocess med kriterier bör fastställas av lagstiftaren i enlighet med direktivets krav.

Remissrespondenterna föreslår att en yttre tidsgräns fastställs för de 11 tillsynsmyndigheterna, som räknas upp i § 11 i förslaget till cybersäkerhetsförordning, för att presentera fullgoda och effektiva föreskrifter inom sina respektive sektorer. Remissrespondenterna föreslår vidare att den nationella CSIRT -verksamheten läggs hos en myndighet som redan arbetar med detta politikområde, som ingår EU:s mandat och är en del av den gemensamma marknaden.

7. *<u>Om straffpåföljderna – straffrättsliga sanktioner saknas</u>*

NIS2 direktivet ger utrymme att införa nationella straffpåföljder på överträdelser av direktivet och dess nationell implementering. Straffrätten är alltid nationell inom EU och därmed kan straffrättslig ansvarskrävande bara genomföras i den nationella lagen. I SOU 2024:18 fastställs att något ansvarskrävande inte är tänkt att ske inom ramen av cybersäkerhetslagen:

> *Det är enligt direktivet upp till medlemsstaterna att avgöra om bestämmelser om straffansvar ska införas för den nationella regleringen. Vid genomförandet av det tidigare NIS-direktivet gjordes bedömningen att överträdelser inte skulle vara straffsanktionerade. Skälen var att kriminalisering som metod bör användas med försiktighet. Vidare skulle straff inte heller vara den effektivaste sanktionen, eftersom de som skulle kunna göra sig skyldiga till överträdelser skulle vara myndigheter, kommuner, landsting och företag. Straff kan enligt svensk rätt endast ådömas en fysisk person. Det saknas enligt regeringen nu skäl att frångå*

den bedömningen. Utredningens inriktning ska därför vara att sanktioner ska vara av administrativt slag. Det handlar då om sanktionsavgifter. En förändring i förhållande till NIS-lagen är att dessa ska ligga på en högre nivå. (s. 75)

Remissrespondenterna kan inte se någon omvärldsanalys som grund till ovanstående. I själva verket skulle en riskanalys visa följande:

- Välfärdsbrottsligheten i Sverige ökar lavinartat, samtidigt som den offentliga sektorn saknar kontroller och tillsyn för att kunna hantera förluster av miljarder kronor årligen som resultat av detta. Detta har gestaltats av bl. a Jens Nylanders AI-genomgång av kommuners ekonomi.

- Brottsligheten som riktar sig mot kritiska samhällsviktiga verksamheter, till exempel avfallshanteringen, har också blivit normalitet i Sverige, t ex fallet med Think Pink. Vinsterna är stora och riskerna små, vilket lockar den organiserade brottsligheten.

- Att påverkansmöjligheter och infiltrering in i den offentliga förvaltningen är lätt och händer ofta, det finns otaliga exempel på kriminalvården, domstolar och polis. Även inom tillsynsmyndigheterna sker detta, såsom inom livsmedelsverket.

- Under de senaste åren har fler kommuner och myndigheter blivit utsatta för omfattande cyberattacker, i form av till exempel *ransomware* och hackerattacker, med stora och dyra skador på verksamheten och för de enskilda medborgarna.

- Sverige är alltmer en integrerad del av EU och NATO, och båda medlemskapen kräver en hög säkerhetsnivå, inklusive förebyggande, samt sanktionerande av cyberbrottslighet.

En materiell analys av vad NIS2 direktivet ger för handen att påförandet av administrativa sanktionsavgifter för väsentliga och viktiga entiteter i artikel konstateras att sanktionerna ska vara effektiva, proportionella och avskräckande. Det är fråga om effektiva rättsmedel:

Artikel 34.1

Medlemsstaterna ska säkerställa att de administrativa sanktionsavgifter som påförs väsentliga och viktiga entiteter enligt denna artikel för överträdelser av detta direktiv är effektiva, proportionella och avskräckande, med beaktande av omständigheterna i varje enskilt fall.

Vidare finns det stöd i NIS2-direktivet till straffpåföljd för personer i ledande funktioner enligt artikel 32.6, 1 stycke, som lyder:

Medlemsstaterna ska säkerställa att varje fysisk person som ansvarar för eller agerar som juridiskt ombud för en väsentlig entitet har befogenhet att säkerställa att entiteten efterlever detta direktiv, på grundval av en befogenhet att företräda entiteten, att fatta beslut på dess vägnar eller att utöva kontroll över entiteten. Medlemsstaterna ska säkerställa att dessa fysiska personer kan hållas ansvariga för överträdelser av sitt uppdrag att säkerställa att detta direktiv efterlevs.

I det andra stycket konstateras:

När det gäller offentliga förvaltningsentiteter påverkar inte denna punkt nationell rätt avseende det ansvar som åligger statligt anställda och valda eller utnämnda tjänstepersoner.

Remissrespondentrenas läsning och förståelse av det andra stycket innebär att denna punkt ej ska påverka befintliga nationella regleringar om tjänstefel och tjänsteansvar. Det betyder inte att tjänstepersoner inom offentlig förvaltning skulle kunna gå utan påföljd vid en överträdelse enligt artikel 32.6 ovan, såsom utredningskommittén har tolkat detta. Det är orimligt eftersom Sverige saknar idag en effektiv reglering av tjänsteansvar. När det gäller tjänstefel och grovt tjänstefel enligt Brottsbalkens 20 kap, 1 §, ska det dels finnas ett uppsåt, dels ska överträdelsen ske i samband med myndighetsutövning – ett begrepp som faktiskt inte finns definierat i en lag.

Cybersäkerhetsöverträdelser kan ske utan uppsåt, men av oaktsamhet, och samtidigt leda till oanade och stora negativa konsekvenser för organisationen och dess kunder, användare och intressenter. De kan också ske utan att det är fråga om myndighetsutövning i något specifikt fall, utan i stället kan det handla om ledningsbeslut och styrning, såsom artikel artikel 20.1. listar:

Medlemsstaterna ska säkerställa att väsentliga och viktiga entiteters ledningsorgan godkänner de riskhanteringsåtgärder för cybersäkerhet som dessa entiteter vidtar för att följa artikel 21, övervakar genomförandet av dem och kan ställas till svars för entiteternas överträdelser av den artikeln.

Remissrespondenterna anser att det är både lämpligt och nödvändigt att införa effektiva rättsmedel, i form av straffrättsliga sanktioner, för dem som avsiktligt eller med grov oaktsamhet orsakar betydande ekonomiska, fysiska eller immateriella skador till juridiska eller fysiska personer genom att underlåta en hög nivå av cybersäkerhet i sina digitala strukturer, nätverk, program och applikationer i enlighet med kraven på NIS2. De administrativa sanktionerna räcker inte för att uppnå direktivets syfte, då de riktas endast mot den högsta ledningen och endast inom näringslivet.

Dataföreningen i Sverige, Leif Häggmark, ordförande

Edvina AB, Olle E. Johansson, medlem i Cybernode.se

Joanna Sjölander, Klusterledare Cyberly, Linköping Science Park - medlem i Cybernode.se

Johanna Parikka Altenstedt, jurist, Samhällssäkerhet, AFRY, medlem i Cybernode.se

Lamm Consulting AB, Hans Thorsen Lamm, medlem i Cybernode.se

Thomas Brül, VD, SSF Stöldskyddsförening, medlem i Cybernode.se

Riktning Rilde AB, Marianne Rilke Björkman, medlem i Cybernode.se

Petter Larsson, Secure by Q, medlem i Cybernode.se

Jan-Olof Andersson, JOA Infosäk AB

Sakarias Strand, Kista Science City AB, medlem i Cybernode.se

Advenica AB, Thomas Carnehult, medlem i Cybernode.se

Oscar Hedlund, VD, Comparo AB

Niclas Swanér, VD, Synkzone AB

Pernilla Rönn, Affärsområdeschef HiQ Stockholm AB

Johannes Collmar, Ekonomi & Säkerhetsskydd, Nordisk Larm & Teleteknik AB, medlem i Cybernode.se

Remissvaret har arbetats fram i en arbetsgrupp inom cybernode.se som letts av Johanna Parikka Altenstedt, Per-Erik Eriksson och Olle E. Johansson.