Försvarsdepartementet
via e-post:
fo.remissvar@regeringskansliet.se
med kopia:
visnja.raguz@regeringskansliet.se

Vår referens/dnr:
2024-45

Er referens/dnr:
Fö2024/00496

2024-05-28

Remissvar

Delbetänkande Nya regler om cybersäkerhet (SOU 2024:18)

Inledning

Ett antal nya regelverk inom datarätt, digitalisering, AI och cybersäkerhet ger företag en stor regel- och kostnadsbörda att hantera. Svenskt Näringsliv noterar att den omfattande regleringsvågen starkt påverkar företagens kostnadsläge, innovation och konkurrenskraft. Verksamhet och investeringar står på vänt tills företagen hunnit överblicka, förstå och finansiera den nya regelbördan. I den mån de nya reglerna består av direktiv är det av stor vikt att svensk implementering ger våra företag den bästa möjliga lagstiftningen utan att reglera mer än vad som ansetts proportionerligt och lämpligt inom övriga EU. Därför utgår vi ifrån att regeringens uppdrag till utredningen att förslagen ska utformas så att regelbördan och administrationen minimeras respekteras och säkerställs av lagstiftaren, särskilt i de delar utredningens förslag inte lever upp till instruktionen.

Att samarbeta och dela kunskap är avgörande för att stärka vår gemensamma cybersäkerhet. Privat-offentligt samarbete utgör en mycket viktig del i cybersäkerhetsarbetet för att förhindra, hantera och följa upp och dra erfarenheter. Betänkandet tar dock inte upp denna aspekt, vilket är beklagligt. Ett närmare samarbete mellan tillsynsmyndigheter och företag inom de sektorer som omfattas av reglerna bör prioriteras. Dessutom är det nödvändigt att ge stöd och vägledning till de verksamheter som tidigare inte har varit föremål för NIS- reglerna, särskilt små och medelstora företag. Mot bakgrund av det stora behovet av stöd och vägledning blir det också viktigt att behöriga myndigheter samarbetar för att säkerställa en enhetlig tolkning, tillämpning och undvika oklarheter för företagen. Det blir särskilt viktigt när företag står under tillsyn av flera myndigheter.

Sammanfattning

Svenskt Näringsliv

- anser att konsekvensanalysen är undermålig vad avser företagens kostnader, tidsåtgång och hur konkurrensförhållanden påverkas
- avstyrker att hela verksamheten som huvudregel ska omfattas av kraven i cybersäkerhetslagen (CSL) då det inte är vår tolkning av NIS2
- tillstyrker att inte civilrättsligt specifikt reglera styrelsens ansvar för riskhanteringsåtgärder, eftersom det redan följer av aktiebolagslagen att styrelsen svarar för bolagets organisation och förvaltningen av dess angelägenheter
- tillstyrker att utbildning för ledningen om riskhanteringsåtgärder följer av direktivet
- avstyrker utredningens förslag att kräva utbildning för anställda eftersom det är en överimplementering av direktivet
- tillstyrker att förbud mot att utöva ledningsfunktion förutsätter allvarliga överträdelser och endast får ske i händelse av uppsåt eller grov oaktsamhet
- avstyrker förslaget att styrelsen ska ingå i den ledningskrets som är relevant för förbud att utöva ledningsfunktion eftersom det är en överimplementering av direktivet och oproportionerligt
- tillstyrker att förbud att utöva ledningsfunktion ska kräva domstolsbeslut och att dessa ärenden ska vara förtursärenden
- avstyrker att förbudsärenden hanteras av förvaltningsdomstol och förespråkar i stället allmän domstol
- anser att verksamhetsutövare och person som ska avregistreras som befattningshavare måste informeras i förväg och att en rimlig tidsfrist införs innan avregistrering sker
- anser att behovet av bakgrundskontroller av personal sannolikhet kommer öka, oavsett om det rör säkerhetskänslig verksamhet, föreslagen CSL eller kommande implementering av CER-direktivet
- avstyrker skyldighet att rapportera potentiella incidenter till myndigheter och kunder
- avstyrker inrapportering av tillbud då det är ett oproportionerligt krav utifrån nytta och administrativ börda
- anser att företagens uppgifter behöver skyddas genom sekretess vid incidentrapportering för att inte hämma incidentrapporteringen eller öka antagonistiska angrepp
- anser att incidentrapportering behöver hanteras enhetligt i medlemsstaterna
- avstyrker den från direktivet avvikande begränsningen att endast myndigheter och andra med offentligrättsliga uppgifter kan vara legitima åtkomstsökare enligt lagen om nationella toppdomäner för Sverige på internet.

Konsekvensanalys

Svenskt Näringsliv konstaterar att önskvärd nivå på konsekvensanalys saknas. Framför allt borde en tydlig analys ha gjorts av förslagets lämplighet och proportionalitet eftersom utredningen lägger förslag som går längre än direktivet.

Utredningen lever inte upp till regeringens direktiv att förslagen skulle utformas så att regelbördan och administrationen minimeras. Vi noterar att utredningen saknat

näringslivsrepresentant i expertgruppen vilket sannolikt kunnat förbättra förståelsen för företagandets villkor och för vad som är en rimlig nivå för praktiskt genomförbart säkerhetsarbete. Utredningen anser att konkurrensförhållandena inte påverkas. Här missar utredningen vad regelbördor får för konsekvenser för olika typer och storlekar av företag i värdekedjan. Konkurrenskraftsperspektivet är styvmoderligt behandlat. Svenskt Näringsliv anser att konsekvensanalysen är undermålig vad avser företagens kostnader, tidsåtgång och hur både konkurrensförhållanden och konkurrenskraft påverkas, och instämmer i Regelrådets slutsats att konsekvensutredningen inte uppfyller kraven i förordningen (2007:1244) om konsekvensbedömning vid regelgivning.

Syftet och begreppet ”hela verksamheten”

NIS2 direktivs syfte (artikel 1) är att uppnå en hög gemensam cybersäkerhetsnivå inom unionen, i syfte att förbättra den inre marknadens funktion. För att stärka den inre marknadens funktion är det av största vikt att medlemsstaterna implementerar direktivet så enhetligt som möjligt. Dessutom är enhetlig implementering central för konkurrens på lika villkor. En fråga som Svenskt Näringsliv reagerat på är utredningens tolkning att hela verksamheten som huvudregel ska omfattas av lagen. Det är inte utgångspunkten när entiteter ”samtidigt kan bedriva viss verksamhet som omfattas av, och viss verksamhet som är undantagen från, detta direktiv”, se skäl 21 i NIS2.

Det är viktigt att företag och koncerner kan arbeta och fatta beslut på ett effektivt sätt, och att information kan delas mellan relevanta verksamheter/entiteter/bolag inom en koncern. Detta är viktigt av såväl säkerhetsskäl, effektivitetsskäl och kostnadsskäl och en implementering som inte går i linje med hur företag arbetar i praktiken riskerar leda till stora administrativa kostnader och pålagor utan att bidra till att stärka säkerheten.

Ledningens ansvar och utbildning (CSL, 3 kap 3§)

Svenskt Näringsliv håller med utredningen om att det för aktiebolag förefaller rimligt att styrelsen och VD ska anses utgöra ”ledningen” enligt direktivet. Svenskt Näringsliv håller också med utredningen om att det redan följer av tillämplig associationsrätt att styrelsen svarar för bolagets organisation och förvaltningen av dess angelägenheter och att det därmed saknas anledning att civilrättsligt specifikt reglera styrelsens ansvar för riskhanteringsåtgärder. Det är bra att regelverk om styrelsens och VD:s ansvar är allmänt hållna och det skulle vara ogörligt och olämpligt att specifikt reglera just detta ansvarsområde. Det förefaller ha blivit vanligare att olika regelverk ställer specifika kompetenskrav på styrelser och reglerar vem som ska ansvara för vad i ett företag. Det är olyckligt. Hur ett företags verksamhet styrs och organiseras måste styrelse och ledning ha utrymme att själva bestämma. Detta gäller även beslut om vilka frågor som ska lyftas till vilken nivå och på vilket sätt.

Även om samma slutsats egentligen gäller utbildning för ledningen om riskhanteringsåtgärder, antar vi att det kan vara svårt att undvika lagstiftning om detta mot bakgrund av hur direktivet är utformat. När det gäller anställda i vidare bemärkelse anser vi dock att det är för långtgående att, som utredningen föreslår i 3 kap 3 §, i allmänhet kräva att anställda ska erbjudas utbildning om riskhanteringsåtgärder. Direktivet föreskriver endast att man ska ”*uppmuntra relevanta entiteter att erbjuda liknande utbildning till anställda”* så det förefaller inte finnas något krav på medlemsstaterna att genom lagstiftning kräva detta. Även

om kunskap om riskhanteringsåtgärder säkert är viktigt för många i en organisation är det inte säkert att det är relevant för alla anställda, och i vart fall saknas anledning att gå längre än direktivet och genom lagstiftning kräva att sådan utbildning erbjuds anställda i vid bemärkelse.

Förbud att utöva ledningsfunktion (CSL, 5 kap 8§)

Om ett föreläggande att uppfylla vissa skyldigheter inte följs, får tillsmyndigheten ansöka om att en individ ska förbjudas att utöva vissa ledningsfunktioner hos en viss verksamhetsutövare. Även om detta är en mer begränsad sanktion än ett näringsförbud är det en ingripande åtgärd mot en enskild individ. Det är därför bra att utredningen poängterar att denna typ av sanktion bör vara synnerligen ovanlig och att den bara kommer att tillgripas i extrema undantagsfall. Det skulle vara välkommet om detta kunde upprepas i författningskommentaren. Det är centralt att denna typ av ingripande förbud tillämpas på ett proportionerligt och rimligt sätt, såväl vad gäller begränsning i tid och omfattning. Svenskt Näringsliv välkomnar att det framgår av den föreslagna lagtexten att ett ingripande förutsätter allvarliga överträdelser och endast får ske i händelse av uppsåt eller grov oaktsamhet.

Utredningen har föreslagit att förbudet ska kunna utfärdas mot samma ledningskrets som omfattas av utbildningskravet, även om begreppen som används i de relevanta artiklarna (artikel 20 och artikel 32.5) skiljer sig åt. Eftersom ett förbud att utöva vissa ledningsfunktioner är en mycket ingripande åtgärd anser Svenskt Näringsliv att det är olämpligt att i den svenska lagen gå längre än vad direktivet föreskriver. Därmed anser Svenskt Näringsliv inte att styrelsen bör omfattas av den relevanta kretsen.

Utredningens förslag innebär att beslut att en person inte ska få vara befattningshavare hos en viss verksamhetsutövare ska fattas av förvaltningsdomstol efter ansökan av tillsynsmyndigheten. Av rättssäkerhetsskäl anser Svenskt Näringsliv att det är bra att domstolsbeslut krävs och att det är bra (och nödvändigt) att denna typ av ärenden ska vara förtursärenden. Eftersom bedömningarna som ska göras av domstolen är av straffrättslig karaktär och innefattar subjektiva rekvisit om uppsåt och/eller grov oaktsamhet, anser Svenskt Näringsliv dock att ärenden av detta slag lämpligen hanteras av allmän domstol istället för av förvaltningsdomstol. Det finns i allmänhet en större vana att bedöma denna typ av rekvisit i allmän domstol och det är också där ärenden om det närbesläktade näringsförbudet i de flesta fall hanteras.

Det föreslås i förslaget till förordning att domstolen ska underrätta Bolagsverket (eller länsstyrelsen) och verksamhetsutövaren när beslut om förbud att utöva ledningsfunktion har vunnit laga kraft (förordningen §§ 40 och 41). Denna informationsskyldighet är förstås central. Bolagsverket (eller länsstyrelsen) ska därefter säkerställa att personen avregistreras som befattningshavare hos verksamhetsutövaren i det aktuella registret. Eftersom en sådan avregistrering – vilket också uppmärksammats av utredningen – kan få långtgående konsekvenser för en verksamhetsutövare och kan leda till att denne snabbt behöver vidta åtgärder för att undvika brister bland registrerade företrädare, är det önskvärt att verksamhetsutövaren – innan en avregistrering sker – får information om den planerade åtgärden. Detta är centralt för att ge verksamhetsutövaren möjlighet att vidta erforderliga åtgärder för att utse en ny individ till den aktuella positionen. Först om verksamhetsutövaren efter en rimlig frist underlåtit att vidta sådana erforderliga åtgärder bör avregistrering kunna ske.

Personalsäkerhet

Kommande slutsatser från CER-utredningen vad avser bakgrundskontroller bör också beaktas i verksamheter som omfattas av förslaget till CSL. Behov kan förekomma att även inom cybersäkerhetsområdet göra bakgrundskontroller. Behovet av bakgrundskontroller av personal kommer med all sannolikhet öka, oavsett om det rör säkerhetskänslig verksamhet, föreslagen CSL eller kommande implementering av CER-direktivet. Det är härvidlag av vikt att denna möjlighet inte inskränks och därmed försvårar möjlighet till bakgrundskontroller. En bakgrundskontroll bör därtill följas upp under den tid som deltagandet i den av NIS2 eller CER reglerade verksamheten pågår. Syftet är att behålla och fördjupa personkännedomen.

Incidentrapportering till tillsynsmyndighet

Rapporteringsskyldigheterna föreslås bli mer långtgående än tidigare. Nytt är att även tillbud och cyberhot som kan orsaka en allvarlig driftsstörning ska rapporteras. Skyldigheten att rapportera potentiella framtida händelser verkar orimlig. Inrapportering av tillbud är oproportionerlig när man ser till administrativ börda. Det är också långt ifrån klart när ett hot blir betydande. Detta ökar företagens omotiverade rapporteringsbörda och kommer att vara rättsosäkert att tillämpa i praktiken.

Det bör bara finnas en skyldighet att informera om betydande tillbud och hot när dessa är väsentliga och konkreta och verksamhetsutövaren på ett vederhäftigt sätt har kunnat bedöma allvarligheten. En vidare informationsskyldighet än så skulle riskera medföra spridning av rena spekulationer, och detta skulle kunna vara mycket skadligt utan att göra någon nytta.

Skyddet av företagens uppgifter och företagshemligheter behöver garanteras vid incidentrapportering med sekretess för att inte hämma incidentrapporteringen och öka antagonistiska angrepp.

För att stärka den inre marknadens funktion och minska företagens administration är det centralt att incidentrapportering hanteras på samma sätt i medlemsstaterna. Här skulle en gemensam EU-mall vara att föredra och rapportering bör alltid kunna ske på engelska för att vara användbar inom hela EU. Dessutom bör ett förenklingsarbete påbörjas för att koordinera och effektivisera incidentrapporteringskraven i olika lagstiftningar som till exempel GDPR och kommande cyberresiliensakten.

Informationsskyldighet till kunder

Även om det kan vara viktigt med transparens om betydande incidenter där det finns en kundpåverkan efterfrågar Svenskt Näringsliv en tydlighet att informationsskyldigheten uppstår först när vederhäftiga bedömningar och slutsatser kring tillbudet eller hotet och dess väsentlighet kunnat dras. Information om eventualiteter bör inte spridas.

Enligt förslaget ska verksamhetsutövaren informera kunder som kan antas påverkas av den betydande incidenten, och detsamma gäller betydande cyberhot (se 3 kap 6§). Värdet av information om en incident som ***kan*** få allvarliga konsekvenser är mycket begränsad. I de fall information om en betydande incident eller hot utgör eller kan komma att utgöra

insiderinformation tillkommer ytterligare komplexitet, då bedömningar i den delen kräver viss konkretion. Spridning av information om eventualiteter kan leda till olämplig spridning av information som kan utgöra en säkerhetsrisk. Dessutom kan spridandet av sådan osäker information leda till spekulationer som (felaktigt) kan leda till oro på börsen.

Förslag till lag om ändring i lagen (2006:24) om nationella toppdomäner för Sverige på internet

Utredningen föreslår att uppgifter i registret ska kunna hämtas utan avgift via internet om den registrerade har samtyckt till detta. Därutöver ska, enligt en föreslagen ändring av § 6 i lagen om nationella toppdomäner för Sverige på internet, uppgifter på begäran lämnas till myndigheter och andra med offentligrättsliga uppgifter inom EES eftersom dessa anses vara ”legitima åtkomstsökare”. Svenskt Näringsliv saknar analys till denna snäva avgränsning. Direktivet gör inte motsvarande avgränsning och det torde finnas betydligt fler legitima åtkomstsökare som skulle kunna ges denna möjlighet att få ut information. Exempelvis skulle rättighetshavare kunna ha ett legitimt intresse att få tillgång till uppgifter som kan ha betydelse vid immaterialrättsintrång.

SVENSKT NÄRINGSLIV

Göran Grén Carolina Brånby