Försvarsdepartementet

Datum
2024-05-27

Diarienummer
Ä 2024-609

Remissvar – SOU 2024:18 Nya regler om cybersäkerhet

Tillväxtverket arbetar för att stärka företagens konkurrenskraft. Det gör myndigheten genom att skapa bättre förutsättningar för företagande och attraktiva regionala miljöer där företag utvecklas. Myndigheten har en särskild roll som ansvarig för regional utvecklings- och samordnad landsbygdspolitik. Tillväxtverket är ansvarig myndighet för riksintresse industriell produktion och för frågor inom turism och besöksnäring. Myndighetens arbete syftar till att stärka sambanden mellan näringslivsutveckling, samhällsplanering och hållbar regional utveckling.

Remissvaret är skrivet utifrån dessa utgångspunkter.

Sammanfattning

- Säkerhetsområdet omfattas av många delvis överlappande regleringar och detta blir ytterligare en lagstiftning med oklar avgränsning till andra regelverk på området såsom Digital operations resilience act (DORA), totalförsvarreglering, säkerhetsskyddslag, nationellt cybersäkerhetscenter, mm.
- Risk för rättsosäkerhet genom otydlig och inkonsekvent använd terminologi.
- Konsekvenserna av de omfattande kraven på verksamhetsutövare som tidigare inte omfattats (både myndigheter och företag) har inte utretts på ett tillfredsställande sätt.
- Fördelarna med att samla ansvaret hos en myndighet för ett tydligare ansvar, mer enhetlig tillsyn samt rättssäkra och enhetliga föreskrifter borde utredas vidare.

Övergripande synpunkter

Tillväxtverket ser vikten av att skydda våra digitala informationsresurser och välkomnar en tydligare reglering på informationssäkerhets-/cybersäkerhetsområdet. Vi ser också ett värde i att fler företag och myndigheter omfattas av sådana regler då säkerheten kräver att så många som möjligt arbetar aktivt med dessa frågor. Som medelstor myndighet har vi erfarenhet av hur

svårt det kan vara att få loss tillräckliga resurser för att kunna bedriva ett systematiskt informationssäkerhetsarbete. Tillväxtverket ser också att det finns ett stort behov av att lära av andra myndigheters erfarenheter på området.

Tillämpningsområde och terminologi

Tillväxtverket delar utredningens förslag om att direktivet inte ska genomföras direktivnära utan anpassas till etablerad terminologi och att ett normalt språkbruk ska eftersträvas. Dock har denna princip inte slagit igenom tillräckligt i utredningens förslag. Begreppet cybersäkerhet i lagens rubrik ersätter (utan förklaring) den tidigare och mer etablerade termen informationssäkerhet. Det råder olika mening om vad termen cybersäkerhet faktiskt omfattar, många olika definitioner förekommer, men i de flesta fall handlar det om en delmängd av informationssäkerhet eller till och med delmängd av IT-säkerhet. Att snäva in begreppet på detta sätt rimmar inte med diskussionen om ”allriskapproach”. Dessutom förekommer begreppet ”informationssäkerhet” parallellt (i lagförslagets 3:2 ”verksamhetsutövare ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete” och i instruktionen till PTS ”verka för ökad nät- och informationssäkerhet”). Detta väcker frågor om vad detta begrepp i så fall ska omfatta; är det bredare eller snävare än lagens huvudtema?

Ytterligare begrepp tas direkt från direktivet och ges ny betydelse eller införs utan att definieras, t. ex. ”incident” och ”allriskperspektiv”, se mer kommentarer om dessa under nästa avsnitt.

För att få en tydlig och lättanvänd reglering av informationssäkerhetsfrågorna och särskilt mot bakgrund av det delvis nya strikta ansvarsutkrävandet är det av stor vikt att terminologin är tydlig.

Risk- och incidenthantering

Utredningen menar att kraven vad gäller praktisk hantering av säkerhetsåtgärder skiljer sig ”i hög grad” från kraven i NIS-direktivet och att man därför behöver införa det nya begreppet ”riskhanteringsåtgärder”. Tillväxtverket delar inte bilden av att kraven skiljer sig åt på ett sätt som skulle göra det otydligt att fortsätta använda begreppet säkerhetsåtgärder. I det nya direktivet specificeras kraven vilket i sak inte avviker från de mer övergripande kraven i NIS-direktivet. Tillväxtverket ser en risk för tillämpningsproblem om det införs en ny oetablerad term för något som det skulle gå att införliva under existerande terminologi.

En annan term där utredningen har valt att använda direktivets terminologi och därmed införa en ny definition i svensk lagstiftning är ”incident”. Vad den nya definitionen som föreslagits i 1 kap 2§ innebär i praktiken förklaras inte av utredningen. Incidenter föreslås rapporteras till CSIRT-enhet hos MSB. Tillväxtverket delar utredningens bedömning att det är lämpligt att rapportering sker till en enda myndighet, men tillsammans med förslaget att dela upp tillsynen på sektorsmyndigheter medför förslaget en risk att tillsynsmyndigheterna inte får tillräcklig kännedom om inträffade incidenter inom deras ansvarsområde.

Riskhanteringsåtgärderna ska utgå från ett ”allriskperspektiv” (lagförslagets 3 kap 1§). Detta begrepp borde förklaras så verksamhetsutövare förstår vad det innebär för de åtgärder de ska vidta och vilka andra risker än informationssäkerhetsrisker som ska beaktas.

En av de riskhanteringsåtgärder som föreslås är i lagförslaget 3 kap 1 § p4 att utvärdera säkerhet vid ”förvärv av utveckling och underhåll av nätverks- och informationssystem”. Skrivningen kommer direkt från direktivets artikel 21 och utredningen gör bedömningen att det är viktigt att hålla fast vid en betydelse som betyder ”övergång av äganderätt”. I denna del menar Tillväxtverket att det blir en omotiverad skillnad mellan köpta system och sådana som

verksamhetsutövare licensierar eller har utkontrakterat och att en bredare term skulle vara mer lämplig, t.ex. ”anskaffning” som MSB föreslagit.

Tillsynsansvar och föreskriftsrätt

Utredningen föreslår att tillsynsansvaret på samma sätt som idag delas upp på olika myndigheter och att dessa myndigheter får föreskriftsrätt. Utredningen framför att det är viktigt att föreskrifterna sektoranpassas och att detta redan kommer att ske med de genomförandeakter kommissionen ska ta fram. Det framförs inga exempel på vad det är hos de olika sektorerna som kräver sådan specialanpassning av föreskrifterna och Tillväxtverket menar att sektorsanpassning riskerar att leda till omotiverade skillnader mellan tillämpningen i olika sektorer.

Genom att behålla tillsynsansvar uppdelat på olika myndigheter, riskerar också tillsynen att skilja sig åt mellan olika sektorer. Den undersökning som MSB gjort och som utredningen hänvisar till, visar att tillämpningen av NIS-lagen redan idag skiljer sig åt mellan sektorer på grund av tillsynsmyndigheternas olika resurser och prioriteringar. Detta är problem som inte enkelt löses med ökad samordning och Tillväxtverket hade gärna sett att alternativet med en övergripande tillsynsmyndighet hade analyserats noggrannare. Utredningens argument att det är en för omfattande uppgift för en myndighet att utöva tillsyn över samtliga verksamhetsutövare som framförs av utredningen framstår som dåligt underbyggt då det ju finns ett antal andra myndigheter som har sektorsövergripande tillsynsansvar.

Mycket talar, enligt Tillväxtverket, på att det skulle bli en ökad enhetlighet och tydlighet om det fanns en enda myndighet som hade det övergripande ansvaret för informationssäkerhetsfrågorna. Det hade varit önskvärt att noggrant överväga detta alternativ, även i konsekvensbedömningen.

CSIRT-enhet hos MSB

Det finns ett stort behov hos myndigheter (och sannolikt också hos företag) att få stöd och hjälp att hantera incidenter. Det handlar om varningar för att få en chans att förebygga att incidenter inträffar, men också att få stöd i hanteringen när incidenter väl inträffar. Det finns idag ett behov av mer omfattande stöd än vad funktionen CERT.se har möjlighet att leverera. Att snabbt kunna få korrekt och relevant information om incidenter och pågående antagonistiska handlingar, samt att ha någon att "hålla i handen" när man hanterar dessa är viktiga och efterfrågade funktioner från Tillväxtverket, och förmodligen även från andra myndigheter

Tillväxtverket ser det som önskvärt att det stöd som ska tillhandahållas vid incidenter specificeras bättre och att det blir mer operativt. Även informationsinsamlingens närmare innebörd borde förtydligas; vilken nivå ska de ”forensiska uppgifterna” analyseras på - handlar det om enskilda klienter, nätverk eller nationell konnektivitetsnivå? Hur ska uppgifterna användas? Vad innebär ”proaktiv skanning”, vad är det som det ska skannas efter?

Sammanfattningsvis ser Tillväxtverket ett behov av att bättre beskriva hur kompetensen och förmågan hos en nationell CSIRT skulle kunna höjas med stärkt hotanalysförmåga och bättre återkoppling och stöd till de rapporterade enheterna.

Konsekvensanalys

Konsekvenserna av utredningens förslag för berörda verksamhetsutövare är inte tillräckligt utredda. Även om det i betänkandet går att utläsa vilka de tillkommande sektorerna är, samtidigt som avgränsningen genom storlekskravet är tydligt, hade Tillväxtverket önskat ett

vidare resonemang kring hur många företag som kan komma att omfattas även om det anges att detta ska utredas av utsedda tillsynsmyndigheter. I samband med denna sammanställning bör också de tillskjutande administrativa kostnaderna av förslaget utredas. För att tillgodose kraven på riskhantering och för att driva ett systematiskt informationssäkerhetsarbete krävs det avsevärda resurser, som för mindre företag och myndigheter kommer att vara krävande att uppnå. Hur det ska gå att hantera detta inom existerande budgetramar framgår inte.

Även uppgiften om vilka sektorer som påverkats hade kunnat göras tydligare. Om beräkningarna som togs fram av kommissionen fortfarande är aktuella skulle det innebära att föreliggande förslag kan komma att medföra ökade utgifter motsvarande 11 procent av de berörda sektorernas IKT-utgifter, vilket skulle motsvara ökade utgifter om 0,63 procent av den totala omsättningen under en period om tre till fyra år.1 I kommissionens konsekvensutredning förs också ett resonemang kring de fördelar och kostnadsbesparingar ett mer proaktivt cybersäkerhetsarbete kan komma och medföra (exempelvis genom färre angrepp och incidenter, minskade kostnader för överträdelser, skydd mot företagsspionage och ett ökat förtroende från kunder). Det är Tillväxtverkets mening att ett utvidgat sådant resonemang relaterat till det svenska genomförandet hade bidragit till en ökad förståelse för nyttan av förslaget samt vilka de sammantagna konsekvenserna hade blivit för de berörda verksamheterna i Sverige.

I och med att en liknande reglering funnit på plats sedan 2018 borde det finnas goda möjligheter att göra en tydlig konsekvensanalys avseende förslagen som lämnas i föreliggande betänkande. Genom ett nedslag i vilka kostnader den tidigare regleringen fört med sig (förslagsvis med utgångspunkt i tillsynsobjekten som listats i tabell 8.1, s. 207) borde det vara möjligt att uppskatta en genomsnittlig tillkommande kostnad per berörd enskild verksamhetsutövare.

Beslut i detta ärende har fattats av rättschefen Tove Kockum.
Pernilla Skantze har varit föredragande.

Tove Kockum

Pernilla Skantze

[1] SWD(2020) 345 final, s. 72.