YTTRANDE ÖVER SOU 2017:36

Justitiedepartementet

103 33 Stockholm

Remissyttrande ”Informationssäkerhet för samhällsviktiga och digitala tjänster”

Sammanfattande synpunkter från SOFF:

SOFF välkomnar utredarens förslag generellt sett. Det är positivt att EU får gemensamma regler för säkerhetsåtgärder inom samhällskritisk nät- och informationsinfrastruktur.

SOFF ser dock en fara med förslaget kommer att innebära ökat krångel och otydlighet vad gäller bl.a. it-incidentrapportering. Eftersom utredaren valt att föreslå en ny lag, istället för att ändra de många befintliga lagar som överlappar direktivet, riskeras bl.a. dubbelarbete och ytterst samhällets säkerhet. Vad som utgör skada och effekt, vad syftet är och vem som står bakom ett angrepp, är ofta inte uppenbart. Därmed är det inte heller uppenbart vilken lag som ska appliceras. Om regeringen väljer utredarens förslag, bör särskilda åtgärder vidtas som syftar till förtydliganden, förenkling och samordning av framför allt vad gäller it-incidentrapportering. Vidare bör rapportering föregå nödvändig analys av säkerhetsskäl och inte fördröjas på grund av oklarheter i regelverket och kring vem som är mottagaren. Införandet kan förenklas om krav och riktlinjer i blir tydliga. Det är också viktigt att det finns tillräckligt höga krav på it-incidentrapportering som berör digitala tjänster som molntjänster och dylikt.

En stor del av den samhällskritiska infrastrukturen hanteras i den privata sektorn. SOFF anser därför att det är av stor vikt att näringslivet blir en aktiv samarbetspartner i genomförande av direktivet, inte minst för att nödvändig kompetens ska tillgodoses. Näringslivet bör bl.a. i lämplig form medverka i det samarbetsforum som föreslås och i andra sammanhang som kan vara relevanta för att tillgodose gemensamma mål om samhällets säkerhet.

Tillräcklig med resurser bör avsättas till genomförandet av den nya lagen. Särskilt åtgärder som syftar till att främja medvetandegraden och kompetensen, exempelvis genom övningsverksamhet, är viktiga i sammanhanget.

Vad gäller detaljer och övriga synpunkter, se nedan.

Bakgrund:

Utredaren har fått i uppgift att föreslå hur EU-direktivet om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (EU 2016/1148) ska genomföras i svensk rätt. Direktivet innebär bland annat skyldigheter för leverantörer av samhällsviktiga tjänster som är beroende av nätverk och informationssystem i ett antal utpekade branscher och vissa leverantörer av digitala tjänster att vidta säkerhetsåtgärder för att hantera risker samt förebygga och hantera incidenter. Rapporteringskraven gäller för leverantörerna oavsett om tjänsterna är utlagda på entreprenad eller inte. De sektorer som identifierats är följande: energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt viss digital infrastruktur. Incidenter som rör Sveriges säkerhet ska inte rapporteras enligt den föreslagna lagen utan omfattas av Säkerhetsskyddsförordningen.

Om det finns bestämmelser i annan lag som minst motsvarar bestämmelserna i den föreslagna lagen, ska de förra bestämmelserna gälla. Vidare är verksamhet som är betydelsefull för Sveriges säkerhet undantagen från tillämpningsområdet.

Utredaren konstaterar att det inte finns några skäl att införa en starkare sekretess för uppgifter som lämnas inom ramen för incidentrapporteringen. Däremot föreslås nya sekretessbestämmelser för enskilds affärs- och driftsförhållande i de fall tillsynsverksamhet bedrivs.

Leverantörerna av samhällsviktiga tjänster ska göra årliga riskanalyser som följs upp av åtgärdsplaner samt bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete.

Myndigheten för samhällsskydd och beredskap (MSB) ges en nyckelroll i samordningen av genomförandet både inom Sverige och i EU-samarbetet. Ett antal myndigheter utpekas som tillsynsmyndigheter på de områden som direktivet omfattar.

Synpunkter:

Allmänna utgångspunkter

Inledningsvis skulle SOFF vilja beskriva utgångspunkterna för våra synpunkter. Denna situationsbeskrivning bör utgöra en grund då statsmakterna beslutar om ett genomförande av NIS-direktivet.

Vårt samhälle står idag inför den allvarligaste hotbilden på flera decennier. Orsakerna är många. Samhället och tekniken har blivit allt mer komplex och dynamisk i sin utveckling samtidigt som den säkerhetspolitiska situationen har försämrats. Vi har en hotbild som är mångfacetterad och inte enbart utgör risk för tydliga störningar och avbrott i exempelvis nät- och informationsnätverk. Det kan t.ex. vara svårt att identifiera om, när och hur ett angrepp genomförts. S.k. hybridhot är en

annan form av angrepp. Det utgörs av en arsenal av olika sätt att pröva samhällets motståndskraft och ofta i kombination med andra metoder som inte avser infrastruktur. En annan försvårande faktor är att det inte heller är tydligt vad, varför och vilka som står bakom olika incidenter och hur stor eventuell inverkan dessa har.

Nationell informationssäkerhetsstrategi

Frågan om en nationell strategi för säkerhet i nätverk och informationssystem, som direktivet föreskrivet i paragraf 2 a), har inte ingått i utredarens uppdrag. SOFF förutsätter att regeringen lägger fram en sådan (med reservation för att detta redan gjorts).

Samarbete med näringslivet

De ökade beroendeförhållandena mellan privat och offentlig sektor är en utveckling som är särskilt viktig att beakta när det gäller frågor som rör samhällets säkerhet. Direktivet avspeglar dessa förhållanden då leverantörer av nät- och informationsnätverk omfattas – vare sig det är verksamhet som drivs av privata företag eller ej. Det är därför viktigt att ha ett nära samarbete mellan privat och offentlig sektor för att kunna skapa ett stabilt och säkert samhälle och för att kunna genomföra den nya lagstiftningen. Det är också näringslivet som driver utveckling och innovation, bl.a. vad gäller metodutveckling, riskanalyser och övningsverksamhet.

Myndigheten för samhällets beredskap (MSB) föreslås leda det samarbetsforum där samtliga tillsynsmyndigheterna ska ingå och bedöma brister i nätverk och informationssystem. För att underlätta samarbetet med leverantörer och för att främja utveckling på området, anser SOFF att det vore lämpligt att företrädare för näringslivet på lämpligt sätt deltar i det nationella samarbetsforumet. Det gäller i alla delar av direktivets genomförande och även i andra relevanta samarbeten.

SOFF välkomnar särskilt utredningens förslag på sidan 237 där man inledningsvis konstaterar att information om incidenter blir allt viktigare för allmänhet och företag, särskilt små och medelstora sådana. Eftersom företagens verksamhet ofta är gränsöverskridande är det bra att ha den i samlad form på unionsnivå och särskilt inriktad på företagens intressen och behov.

Den nya lagens koppling till annan lagstiftning

Utredaren föreslår att direktivet blir en egen separat lag utifrån ett resonemang kring krav i annan styrande lagstiftning på säkerhetsområdet. (s.91) Alternativet skulle ha varit att komplettera direktivets bestämmelser i andra berörda nationella lagar som exempelvis Säkerhetsskyddslagen, Lagen om elektronisk kommunikation, Krisberedskapsförordningen, samt andra lagar som rör specifika sektorer. Utredaren anser att detta alternativ inte är lämpligt, bl.a. på grund av bestämmelser i andra lagstiftningar.

SOFF anser att skapande av en ny lag som ska kopplas till ovan nämnda lagar på området innebär minskad överblick och bristande vägledning för berörda. Denna otydlighet innebär i sig en säkerhetsrisk, då flera regelverk kan beröras vid en och samma incident. De överlappande regelverken innebär för berörda aktörer krångel, otydligheter och eventuellt dubbelarbete vad gäller

exempelvis incidentrapportering, se nedan. I slutändan kan det bli förseningar med att vidta nödvändiga åtgärder när ansvaret är otydligt.

Vidare gör utredaren skillnad på hot inriktat på samhällets säkerhet (som faller under Säkerhetsskyddslagen) och NIS-direktivet. Enligt SOFF:s bestämda mening går det inte att göra denna tydliga skillnad. Vilka som står bakom ett angrepp på samhällskritisk infrastruktur är ofta inte uppenbart. Många försök till it-angrepp har visat sig härröra från statligt styrda aktörer i andra länder via mellanhänder. Här vill vi bl.a. hänvisa till FRA:s årsredovisning. Det är alltså nödvändigt ur ett säkerhetsmässigt perspektiv att det finns en och inte flera definitioner, av vad som utgör ett angrepp på samhällskritisk informationsinfrastruktur som hotar samhällets säkerhet. Detta skulle också tala för en gemensam lagstiftning.

Incidentrapportering

Incidenter som rör Sveriges säkerhet ska inte rapporteras enligt den föreslagna lagen utan enligt Säkerhetsskyddsförordningen. SOFF anser att det går att skilja lagarna åt på detta sätt med tanke på dagens hotbild och hur it-angreppen är beskaffade. Med hänvisning till vad som i ovan stycke anförts, är det viktigt att lagstiftningen ger en enhetlig bild av vad som ska rapporteras och tar tillräcklig hänsyn till samhällets säkerhet och den säkerhetspolitiska situationen.

Denna frågeställning återkommer vad gäller förslagets 17 § som innehåller definitioner av vad som ska utgöra en incident av betydande inverkan. Denna föreslagna definition omfattar enbart fysiska störningar i nät och informationssystem, nämligen antal användare som påverkas, längden på incidenten och hur stort geografiskt område som påverkas. Denna definitionen är enligt SOFF:s mening för begränsad och tar inte hänsyn till andra former av incidenter som exempelvis syftar på intrång, stöld eller påverkan av data. NIS-direktivet har en bredare definition då den nämner ytterligare en faktor, nämligen i vilken utsträckning incidenten inverkar på den ekonomiska och samhälleliga verksamheten. SOFF anser att definitionen av incident av betydande inverkan bör följa NIS-direktivets lista över definitioner. Lagen bör vara tydlig särskilt vad gäller effekter på samhällets vitala funktioner, även om SOFF har förståelse för att tillsynsmyndigheterna får till uppgift att ta fram föreskrifter om vad som ska utgöra en incident som har betydande inverkan.

I det här sammanhanget är det också viktigt att se till att lagen ger tillräcklig inriktning även för tillsynsmyndigheternas arbete, krav på åtgärder, sanktionsavgifter och för förebyggande verksamhet.

De överlappande regelverken som berör incidentrapportering kan bl.a. innebära att flera rapporter ska levereras för samma incident. Det är viktigt att sådant dubbelarbete och annat krångel som rör it-incidentrapportering undviks och att rapportering generellt underlättas. Ett sätt att förtydliga när it-incidentrapportering bör ske är att exempelvis MSB tar fram en vägledning som är sektorsöverskridande och sammanställer befintliga regler på området.

Frivillig incidentrapportering bör underlättas för att främja säkerhet och kompetensuppbyggnad. Även här är det viktigt att MSB snarast utfärdar tydliga riktlinjer för detta enligt utredningens förslag. (s. 294) efter konsultationer med näringslivet och inte enbart uteslutande med tillsynsmyndigheterna. Det gäller också vad som ska utgöra grund för sanktioner och liknande.

SOFF ställer sig också frågande till den skillnad på krav på säkerhetsåtgärder och incidentrapportering som görs mellan leverantörer av digitala tjänster och leverantörer av samhällsviktiga tjänster. Förslaget innebär att leverantörer av digitala tjänster inte får samma grad av krav på sig, och behöver exempelvis bara rapportera en incident om leverantören har tillgång till den information som behövs för att bedöma incidentens inverkan. Även om SOFF har förståelse för utredarens resonemang kring leverantörer av digitala tjänster, innebär detta otydligheter. Stora säkerhetsrisker föreligger bl.a. vid användandet av molntjänster, och likaså kan internetplattformar som marknadsplatser och sökmotorer också vara föremål för cyberangrepp. Enbart den årliga riskanalys med åtgärdsplan som föreslås är inte tillräcklig.

Sanktionsavgifter

SOFF har inga övriga synpunkter på vad utredaren föreslår om sanktionsavgifter, förutom att underlåtelse som hotar samhällets säkerhetsintressen, bör betraktas som särskilt allvarliga.

Övningsverksamhet

Utredaren föreskriver att MSB ska tillse att utbildning och övningar kommer till stånd inom myndighetens ansvarsområde. Enligt SOFF:s mening är åtgärder som främjar kompetens och medvetandehöjning åtgärder centrala för att säkra samhället från sårbarheter och angrepp. Den mänskliga faktorn är här särskilt viktig. Därför bör MSB (s. 236) skyndsamt få tydliga uppdrag och resurser att genomföra exempelvis kampanjer och utbildning samt kvalificerad övningsverksamhet, inte minst sådana som rör EU eller annan internationell samverkan för att höja kompetensnivån.

Resurser

Avslutningsvis vill SOFF betona vikten av att särskilda resurser avsätts för genomförandet och uppföljning av direktivet. Samhällets säkerhet bör utgöra en prioriterad verksamhet. Utredaren föreslår bl.a. följduppdrag till Statskontoret i det hänseendet. SOFF anser att det är av vikt att medvetandehöjande åtgärder och övningsverksamhet (se ovan) kommer till stånd snarast. För aktörerna att öka sin säkerhetsnivå krävs stöd och övning för att skapa en ökad förmåga.

Stockholm 15 augusti 2017

På uppdrag av Säkerhets- och försvarsföretagen,

Robert Limmergård

Generalsekreterare