SVENSKT NÄRINGSLIV

Justitiedepartementet

Enheten för lagstiftning om allmän ordning och säkerhet och samhällets krisberedskap
Dan Leeman

103 33 Stockholm

Vår referens/dnr:
93/2017

Er referens/dnr:
Ju2017/03997/L4

2017-08-15

Remissvar

Betänkandet "Informationssäkerhet för samhällsviktiga och digitala tjänster" (SOU 2017:36)

Svenskt Näringsliv har beretts tillfälle att lämna synpunkter på rubricerande betänkande och vill med anledning därav framföra följande.

NIS-direktivet ställer krav på informationssäkerhetsnivån och incidentanmälningar i ett antal specifika sektorer. Svenskt Näringsliv ser överlag positivt på att informationssäkerheten höjs för samhällsviktiga och digitala tjänster. Cybersäkerhet är en angelägen fråga för näringslivet och det bredare samhället. Vi har dock några synpunkter på betänkandet som presenterats.

Sammanfattning
Svenskt Näringsliv tillstryker utredningens förslag att mikro- och småföretag undantas.
Svenskt näringsliv tillstyrker utredningens förslag till ändringar i offentlighets- och sekretesslagen (2009:400).
Svenskt Näringsliv har synpunkter på introduktion av nya sanktionsavgifter.
Vi framför även att ett enhetligt regelverk inom det digitala området är centralt för företagens regelefterlevnad, att myndigheter behöver öka sin information och rådgivning, att nya lagkrav bör vara förenliga med kommande krav inom ett svenskt totalförsvar samt att informationssäkerheten kan förstärkas genom uppdrag till myndigheter att skydda och stötta näringslivet mot dataintrång och industrispionage.

Generellt vill vi betona vikten av att regelverk är så enkla som möjligt både för att underlätta regelefterlevnad och för att minska företagens regelbörda. Att tillämpningsområdet i betänkandets förlag till lag om informationssäkerhet för vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster, 2 §, undantar mikro- och småföretag är klokt då det är viktigt att minimera regelbördan för mindre företag, något som annars skulle riskera att hämma innovation, start-ups och tillväxt.

För näringslivet är det viktigt att säkerställa en så pass enkel implementering av direktivet som möjligt. All regulatorisk börda innebär en belastning för företag och till detta tillkommer

Svenskt Näringsliv delar Datainspektionens uppfattning i skrivelsen Vissa frågor om sekretess med anledning av EU:s dataskyddsreform, Ju 2017-07-07. Svenskt Näringsliv välkomnar därför utredningens förslag till ändringar i offentlighets- och sekretesslagen (2009:400) för att känslig information i incidentrapporter ska kunna skyddas då det är viktigt att säkerställa att konfidentiell/känslig information inte blir öppet tillgänglig. I detta sammanhang är det också viktigt att den offentliga sektorn tillhandahåller säkra kommunikationskanaler för leverans av information.

Sanktionsavgifterna föreslås kunna variera mellan 5000 kronor och 10 miljoner kronor, 33 §. Proportionalitet och rimlighet är grundläggande krav på sanktionsnivåer vilket framgår av 34 §. Men även om sanktionsavgifterna ska ha en avskräckande påverkan är det av största vikt att ansvarig myndighet informerar om säkerhetsåtgärder och anmälningskrav samt säkerställer att kravbilderna och anmälningsprocesserna är så enkla och klara som möjligt att följa.

I konsekvensanalysen framförs optimistisk att konsekvenserna är ekonomiskt positiva för företagen. Om det fanns en uppenbar ekonomisk uppsida skulle sannolikt de flesta företag redan uppfylla de säkerhetskrav som kommer att ställas. Den ekonomiska vinsten beror nog mycket på rimligheten i kravställningen. Är den för låg blir den meningslös, blir den för hög ställs orimliga (och oekonomiska) krav. Utmaningen är att hitta den rätta balansen.

En utmaning som inte tydligt berörs i betänkandet är hur man skall relatera till hård- eller mjukvaruutvecklare vars produkter har bred spridning i de beröra sektorerna. Dessa (ofta globala) utvecklare av hårdvara eller mjukvara är centrala för utvecklingen av lösningar för att motverka cyberincidenter. Förslagsvis bör Sverige, kanske inom ramen för EU, se över hur kontaktkanaler och samarbetsformer med dessa aktörer ser ut och hur de kan förbättras.

NIS-direktivet ställer krav på informationssäkerhetsnivån och incidentanmälningar i ett antal specifika sektorer. För att ytterligare förbättra säkerhetsnivån på dessa områden lär det inte räcka med en ensidig kravställning mot den privata sektorn. Ett logiskt komplement i sammanhanget skulle vara att våra säkerhetsmyndigheter och sektorspecifika myndigheter fick ett tydligare uppdrag att skydda och stötta näringslivet mot intrång. Här skulle vi gärna se att säkerhetsmyndigheterna också fick en uttalad och proaktiv roll att hjälpa till att skydda de sektorer som är immaterialrättsligt intensiva och utsatta för hård internationell konkurrens och industrispionage.

SVENSKT NÄRINGSLIV

Karl Lallerstedt Carolina Brånby