Till Försvarsdepartementet

Yttrande - Remiss SOU 202418 Delbetänkandet Nya regler om cybersäkerhet

Remissinstansen diarienummer: Fö2024/00496

Övergripande kommentarer

Östersunds kommun ser behovet av en enhetlighet inom cybersäkerhetsområdet både på grund av sårbarheter gentemot aktörsdrivna hot men även på grund av samhällets ökade digitalisering. Att samma regler ska gälla såväl det offentliga som privata och att det inom EU finns en likriktad grundsyn i och med detta direktiv kommer att ge synergier och förenkla för alla berörda och i slutändan för den enskilda medborgaren.

I avsaknad av tydlig lagstiftning för kommuner inom informationssäkerhetsområdet har samverkan och samarbete mellan lokal och regional nivå varit svag med följd att en tillräckligt robust basplatta inom cybersäkerhetsområdet inte kunnat upprättas på kommunal nivå. Att införliva samtliga delar av den offentliga sektorn, inkluderat sådant kommunalt ansvar som ofta bedrivs inom bolagsform är en nödvändighet för att uppnå effekt. Östersunds kommun ställer sig därför positiv till utredarens förslag i sin helhet, med det principiella undantaget att kommunen inte delar utredarens slutsats angående finansieringsprincipen i förhållande till kommunernas ansvar för dess egna verksamhet i och med den kostnad ett införande av en cybersäkerhetslag kommer att innebära, i synnerhet för mindre kommuner.

Kommentarer till specifika delar av remissen

Avsnitt **3.2.12 Rapporteringsskyldigheter**

Det behövs en tydlighet i kommande föreskrifter från MSB vad som ska rapporteras avseende incidenter. Gäller NIS2 enbart cyberattacker avseende rapportering? En driftincident (som inte kan relateras till en specifik händelse kopplat till en hotaktör och cyberattack) kan ju innebära en *denial of service-situation,* d.v.s. att tillgänglighetsperspektivet påverkas.

Avsnitt **3.2.13 Cybersäkerhetscertifiering och standardisering**

Hur ska vi som kommun veta om de åtgärder som gjorts är tillräckliga? Det här är ett faktiskt exempel på kostnadsdrivande effekter (primärt för utökning av antal anställda, utbildning av dessa samt systemstöd), som även belyser behovet av metodik och faktiska verktyg för den enskilda kommunen. Även om det ska finnas en valfrihet så bör CSIRT (eller vilken aktör det nu blir som får ansvaret) kunna ta fram en grundläggande ram för enskilda att nå en tillräcklig nivå av till exempel *open source* - produkter. Detta för att minska kostnader (i avrop/upphandling) samt ge en möjlighet att få till stånd en basnivå avseende säkerhet i de organisationer som omfattas. Dessutom kan kompetensdelning ske på ett enklare sätt om flera har samma systemflora och kan dela erfarenheter uppåt och åt sidan.

Föreskrifter och tillsyn bör även utformas så att det över tid är möjligt att prioritera och rikta tillgängliga resurser (speciellt utifrån förutsättningen att inga ekonomiska medel ska tillskjutas kommuner). Även att börja tillsyn utifrån en rimlig basplatta som sedan utökas över tid (i jämförelse med till exempel CIS Controls). Även om ekonomiska medel skulle tillföras är branschen och arbetsmarknaden så beskaffad att det är extremt svårt att attrahera den kompetens som krävs; dels för att kompetens inom cybersäkerhetsområdet är en global bristvara, dels för att den kompetens som ändå finns lockas till andra som har de monetära musklerna att betala mer än till exempel offentlig verksamhet.

Avsnitt **8.4.2 Tillsynsmyndigheter i Sverige**

Kommunen har inga synpunkter på vem regeringen utser som tillsynsmyndighet men då måste dessa får de faktiska resurser som krävs för att kunna utföra sitt uppdrag med den kvalitet som lagstiftaren nog har tänkt sig.

Ställningstagande

Östersunds kommun ställer sig positiv till utredarens förslag i sin helhet, med beaktande av de förslag som redovisas ovan.

ÖSTERSUNDS KOMMUN

Kommunstyrelsen

Yttrandet skickas till Försvarsdepartementet via e-post till fo.remissvar@regeringskansliet.se och med kopia till visnja.raguz@regeringskansliet.se.