

Försvarsdepartementet

Remissyttrande över remiss från Försvarsdepartementet angående kommissionens cybersäkerhetspaket med förslag om ändringar i cybersäkerhetsakten (EU 2019/881) samt riktade ändringar i NIS 2-direktivet (EU 2022/2555)

Sammanfattning

Livsmedelsverket har beretts tillfälle att yttra sig över Europeiska kommissionens förslag till Europaparlamentets och rådets direktiv om ändring av direktiv (EU) 2022/2555 (NIS2 direktivet) vad gäller förenklingsåtgärder och anpassning till den reviderade cybersäkerhetsakten.

Livsmedelsverket välkomnar kommissionens övergripande inriktning att förenkla och effektivisera det befintliga regelverket. Myndigheten bedömer att förslagen i huvudsak är ändamålsenliga och att de kan bidra till en mer proportionerlig och enhetlig tillämpning av NIS 2-direktivet.

Mot denna bakgrund tillstyrker Livsmedelsverket i allt väsentligt de föreslagna ändringarna. Myndigheten vill dock framföra ett antal synpunkter och överväganden som redogörs för i följande avsnitt.

Synpunkter på förslagen

Nya storlekströsklar för väsentliga verksamhetsutövare

Livsmedelsverket tillstyrker införandet av den nya storlekkategorin “small mid-cap enterprises” som ett led i att skapa en mer nyanserad och proportionerlig reglering.

Samtidigt behöver framhållas att storlek inte alltid är ett bra mått på hur kritisk en verksamhet är för samhällets och marknadens funktion. Detta gäller särskilt inom sektorer såsom dricksvatten och avloppsvatten, där verksamhetsutövare med relativt begränsad storlek kan ha en stor eller avgörande betydelse för samhällsviktiga funktioner.

Mot denna bakgrund är det av central betydelse att medlemsstater även fortsättningsvis ges möjlighet att identifiera ytterligare verksamhetsutövare som väsentliga, utifrån kriterier som speglar verksamhetens faktiska betydelse för samhällets funktionalitet och säkerhet.

Livsmedelsverket bedömer att denna flexibilitet är en förutsättning för att regelverkets tillämpningsområde ska bli ändamålsenligt.

Informationsplikt vid ransomware-attacker

Livsmedelsverket är positiva till förslaget att införa ytterligare möjligheter för CSIRT eller behöriga myndigheter att begära information från verksamhetsutövare om incidenter relaterade till så kallade ransomware-attacker. Detta kan möjliggöra kartläggning och ge en värdefull förståelse för det ekonomiska utfallet och hanteringen av sådana attacker.

Uppgifter om att en ransomware-attack har inträffat kan vara känsliga för det berörda företaget och innebära risk för negativ påverkan på varumärke och kundrelationer. Uppgifter om att en begärd lösensumma har betalats är typiskt sett ännu mer känsliga. För att upprätthålla en hög rapporteringsvilja är det därför av stor vikt att uppgifter som lämnas omfattas av ett starkt skydd.

Bestämmelser om informationsplikten avseende ransomware-attacker föreslås införas i artikel 23, som i övrigt avser incidentrapportering. Det är dock inte självklart att samtliga uppgifter som ska lämnas inom ramen för dessa bestämmelser utgör incidentrapporter i rättslig mening.

Livsmedelsverket anser därför att det är angeläget att den svenska lagstiftningen säkerställer att uppgifter som begärs från verksamhetsutövare med anledning av ransomware-attacker omfattas av samma nivå av sekretess som incidentrapporter.

Certifiering som verktyg och begränsande faktor vid tillsyn

Livsmedelsverket noterar förslaget att i ökad utsträckning använda europeiska cybersäkerhetscertifieringar som ett sätt att redovisa efterlevnad av kraven enligt direktivet. För verksamhetsutövare i de sektorer som myndigheten har tillsynsansvar för bedöms efterfrågan på sådana certifieringar vara begränsad, särskilt för viktiga verksamhetsutövare och för kommunala aktörer.

Samtidigt kan certifiering vara av intresse för vissa större verksamhetsutövare. I detta sammanhang vill Livsmedelsverket framhålla vikten av att certifieringar utformas så att de i praktiken motsvarar de krav som gäller enligt direktivet och i svensk rätt, inklusive föreskrifter om säkerhetsåtgärder och utbildning. Om så inte är fallet finns en risk att certifiering får begränsad relevans som stöd för tillsyn och efterlevnad.

Beslut i detta ärende har fattats av generaldirektör Christina Nordin. I den slutliga handläggningen har deltagit avdelningschef Daniel Karlsson, rättschef Elin Häggqvist, enhetschef Kent Jansson, samt informationssäkerhetsspecialisterna Markus Dörner och Anders Lindström, föredragande.

Christina Nordin

Anders Lindström

Kopia

Landsbygds- och infrastrukturdepartementet