ÖSTHAMMARS KOMMUN
– EN DEL AV ROSLAGEN

Kommunledningskontoret

Datum	Dnr	Sid
2024-04-25	KS-2024-217	1(3)

Försvarsdepartementet
FÖ2024/00496

fo.remissvar@regeringskansliet.se
visnja.raguz@regeringskansliet.se

Remissvar Delbetänkandet 2024:18 Nya regler om cybersäkerhet

Östhammars kommun ställer sig positiv till delbetänkandet. Vi ser värdet av en hög cybersäkerhetsnivå inom hela unionen och att Sverige får en sammanhållen reglering för att höja motståndskraften i samhällsviktig verksamhet. De skärpta kraven för informations- och cybersäkerhet innebär dock ett merarbete och ökade kostnader vid införandet i alla kommuners verksamheter. För att underlätta för kommuner föreslår vi:

- Statliga medel
- Tillsynssamordning
- Övergångsperiod för tillsyn
- Incidentrapportering – samordning och förenkling

Bakgrund

Europaparlamentet och rådet antog den 14 december 2022 två nya EU-direktiv, NIS2- direktivet och CER-direktivet. Utredningen redovisar i delbetänkandet förslag om införlivning av NIS2-direktivet och kommer att i sitt slutbetänkande i september 2024 att lämna förslag om införlivning av CER-direktivet. NIS2-direktivet ställer krav på säkerhet i nätverks- och informationssystem. Det ersätter det tidigare NIS-direktivet från 2016, som genomfördes i svensk rätt genom lagen (2018: 1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.
Utredningen föreslår att NIS2-direktivet i huvudsak införlivas genom en ny lag, cybersäkerhetslagen och att den tidigare lagen upphävs. NIS2-direktivet skärper kraven jämfört med det tidigare direktivet för verksamhetsutövare och innehåller bestämmelser om ett mer långtgående samarbete inom unionen. Syftet är att uppnå en högre cybersäkerhet.

Postadress	Besöksadress/Reg.office	Telefon	Telefax	Organisationsnummer	Bankgiro
Box 66	Stångörsgatan 10	Nat 0173-860 00	Nat 0173-175 37	212000-0290	233-1361
Fakturaadress	742 21Östhammar	Int +46 173 860 00	Int +46 173 175 37	V.A.T. No	
Box 106	www.osthammar.se	E-post		SE212000029001	
742 21 Östhammar		kommunen@osthammar.se			

Östhammars kommuns inställning
Utifrån det rådande omvärldsläget, IT-attacker som förekommer allt oftare och behovet av säkerhet i en snabb digitaliseringstakt ser Östhammars kommun värdet av att höja cybersäkerhetsnivån i hela unionen samt att stärka motståndskraften i samhällsviktig verksamhet. Kommunen har redan lagt grunden för ett systematiserat och riskbaserat arbetssätt med informationssäkerhet och vi gör bedömningen att vi kan möta de skärpta kraven och bidra till en stärkt informations- och cybersäkerhet. Detta genom att uppgradera vårt ledningssystem för informationssäkerhet (LIS) och införliva arbetssättet i samtliga kommunens verksamheter.

Vi bedömer dock att ett brett införande kommer att kräva ett omfattande arbete och utökade resurser för att säkerställa att kommunens informations- och cybersäkerhetsarbete i praktiken möter de skärpta kraven. Då införandet av cybersäkerhetslagen medför finansiella konsekvenser för kommunen ser vi att det är rimligt att det avsätts statliga medel även för kommunerna, på samma sätt som utredaren föreslår medel till tillsynsmyndigheterna.

Statliga medel
Kommuner behöver få möjligheten att ansöka om medel för implementering av direktiven. Beroende på hur långt respektive kommun har kommit i sitt informations- och cybersäkerhetsarbete bör statliga medel kunna ges för åtgärder som att:

- Öva beredskaps-, kris- och kontinuitetsplaner som berör kritiska och samhällsviktiga system och digitala tjänster
- Uppgradera LIS, särskilt de områden som rör styrande dokument och processer/stöd för incidenthantering och kontinuitetshantering
- Säkerställa en ändamålsenlig organisation med roller som kan ta ansvar i alla led
- Genomföra obligatoriska utbildningar, såsom utbildningar för kommunledning och förtroendevalda i riskbaserat arbetssätt
- Höja medvetenheten, stärka säkerhetskulturen och erbjuda utbildningar till alla medarbetare
- Införa specifika kostsamma riskhanteringsåtgärder/säkerhetsåtgärder som kan skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter
- Höja kvalitet i uppföljning, rapportering och kommunikationsprocesser – internt och externt
- Ta fram målgruppsanpassat informations- och stödmaterial, t.ex. rutiner, mallar och checklistor för informationssäkerhetskrav vid upphandling och leverantörsuppföljningar
- Verktyg för incidentrapportering internt/externt – säker hantering av känslig information
- Införa SOC-funktion.

Tillsynssamordning

I utredningen framgår att kommunerna måste förhålla sig till flera tillsynsmyndigheter samtidigt. Dessa tillsynsmyndigheter ska ta fram föreskrifter med krav som kommunerna ska följa, men innan dessa är klara är det svårt att till fullo avgöra vad en tillsyn kommer att innebära och vilka krav som kommer att prioriteras. Vi vet dock att det kan bli höga viten. En kommun måste också vara beredd på att flera tillsynsmyndigheter kan välja att göra en tillsyn samtidigt, men de har inga krav på sig att synkronisera dessa. MSB har heller inget mandat att samordna tillsynsmyndigheters tillsyn. Det är upp till varje tillsynsmyndighet att avgöra hur de vill göra.
För att förenkla för oss kommuner ser vi att det bör finnas någon form av tillsynssamordning. Det vore också önskvärt med ett förtydligande om vad miniminivån för cybersäkerhet ska vara och vad kommunerna kommer att granskas utifrån.

Övergångsperiod för tillsyn

I och med att konkreta krav saknas ser vi att det kan bli svårt att granska efterlevnaden på ett rättvist sätt. Beroende på vilka krav som kommer att ställas på kommunerna kan det också ta tid att införa ändamålsenliga åtgärder i samtliga verksamheter. Det bör därför vara en övergångsperiod mellan det att de nya lagarna och regelverken kommer på plats och tillsynsarbetet startar. Detta skulle ge kommunerna bättre förutsättningar att i praktiken kunna svara mot de skärpta kraven förbereda sig inför en tillsyn.

Incidentrapportering - samordning och förenkling

Av utredningen framgår att incidenter ska rapporteras till flera myndigheter och inom en viss tid. Parallellt ska andra myndigheter informeras. Det borde finnas någon sammanhållande myndighet för incidentrapportering och informationsdelning som förenklar för såväl kommuner som andra aktörer och erbjuder en samlad väg in. Den sammanhållande myndigheten skulle kunna uppdras att informera om och rapportera vidare de incidenter som fler myndigheter har rapporteringskrav på, detta enligt fastställda rutiner och processer och säker informationsdelning via säkra kanaler.
Ett annat alternativ som skulle underlätta för kommuner är införandet av ett integrerat incident-rapporteringsverktyg med synkroniserade rapporteringsflöden och mallar som kan användas då incidenter ska rapporteras och skickas på ett säkert sätt till - och mellan - olika myndigheter. Incidenthanteringsverktyget skulle även kunna erbjudas för intern användning inom kommunerna.

Maria Sverredal Langen
Informationssäkerhetsamordnare