Tjänsteutlåtande
Utfärdat 2024-04-19
Ärendenummer SLK-2024-00295

Handläggare
Magnus Junsäter, Linda Larsson, Sara Linderup
Telefon: 031-368 02 27
E-post: fornamn.efternamn@stadshuset.goteborg.se

Remiss från Försvarsdepartementet - Delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18)

Förslag till beslut

I kommunstyrelsen:

Yttrande över delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18), i enlighet med bilaga 2 till stadsledningskontorets tjänsteutlåtande, översänds till Försvarsdepartementet.

Sammanfattning

Remiss för delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18) inkom till Göteborg Stad den 6 mars 2024. Göteborgs Stads yttrande ska vara Försvarsdepartementet tillhanda senast den 28 maj 2024.

Europaparlamentet och EU-rådet antog den 14 december 2022 två nya EU-direktiv, NIS2-direktivet (NIS2) och CER-direktivet. I delbetänkandet redogörs för förslag om införlivning av NIS2 i svensk rätt. I slutbetänkandet, som planeras vara färdigställt i september 2024, kommer även förslag om införlivning av CER-direktivet att lämnas. Utredningen föreslår i huvudsak att följa de skyldigheter som krävs enligt NIS2.

Cybersäkerhet omfattar all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användarna av dessa system och andra berörda personer mot cyberhot. I samband med att Göteborgs Stads riktlinje för informationssäkerhet senast reviderades togs hänsyn till det kommande NIS2. Verksamheter inom Göteborgs Stad ska bedriva sitt informationssäkerhetsarbete utifrån ett riskbaserat arbetssätt i enlighet med riktlinjen. Detta ligger i linje med intentionerna i NIS2 samt den svenska implementeringen av direktivet i form av ny lag om cybersäkerhet (fortsättningsvis cybersäkerhetslagen). Även om staden i sin styrning tagit viss höjd för NIS2 innebär den föreslagna regleringen högre krav på stadens verksamheter. Det handlar exempelvis om hantering av incidenter samt central samordning av cybersäkerhetsarbetet i staden.

Stadsledningskontoret instämmer i huvudsak i delbetänkandets förslag och bedömningar. Det finns dock vissa områden där stadsledningskontoret ser skäl att yttra sig. Det gäller till exempel kommunen som verksamhetsutövare, tolkning av undantag från regleringen, hantering av incidenter, vägledningar i myndighetsföreskrifter och utmaningen med flera tillsynsmyndigheter.

Bedömning ur ekonomisk dimension

I delbetänkandet görs bedömning att kostnaderna för offentliga verksamhetsutövare ska finansieras inom befintlig budgetram.

Den gällande lagstiftningen, NIS-direktivet och lagen (2018:1174) om samhällsviktiga och digitala tjänster, omfattar endast ett fåtal verksamheter och delar av verksamheter. I förslaget till ny lagstiftning omfattas kommunerna i sin helhet, med undantag för kommunfullmäktige. Även bolagen omfattas beroende på vilken verksamhet som bedrivs.

Verksamhetsutövaren ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete enligt krav i NIS2 och i föreslagen cybersäkerhetslag. Det ställs även krav på att verksamhetens ledning ska vara delaktig i riskhanteringen och genomgå utbildning. Utöver detta ska anställda erbjudas utbildning. Med verksamhetsutövare menas juridisk eller fysisk person som bedriver verksamhet. Enligt Göteborgs Stad riktlinje för informationssäkerhet ska stadens verksamheter bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete. I riktlinjen är utgångspunkten att ansvaret för informationssäkerheten är inom ordinarie verksamhetsansvar. I NIS2 är ansvaret kopplat till verksamhetsutövarens juridiska person vilket för nämndernas verksamheter kommer innebära kommunstyrelsen. Förutsatt att en sådan ordning behöver tillämpas kommer det att krävas en mer omfattande central styrning från stadsledningskontoret. Det kan innebära behov av utökade resurser på stadsledningskontoret för att arbeta med informationssäkerhet och implementering av det nya lagkravet i staden.

Det finns en risk att föreslagen lagstiftning kommer att öka stadens kostnader kopplade till IT-drift, riskhantering, incidentrapportering och höga sanktionsavgifter om staden inte når upp till de krav som ställs. Vilka ekonomiska konsekvenser lagen i övrigt medför är svårbedömt fram tills dess framtida tillsynsmyndigheter har utarbetat föreskrifter och definierat former för samordning mellan olika tillsynsmyndigheter.

Bedömning ur ekologisk dimension

Stadsledningskontoret har inte funnit några särskilda aspekter på frågan utifrån denna dimension.

Bedömning ur social dimension

Syftet med implementeringen av NIS2 genom den föreslagna cybersäkerhetslagen är att uppnå en högre cybersäkerhet. Ett utökat regelverk avseende cybersäkerhet möjliggör bättre säkerhet och ett större ansvarstagande vid hantering av medborgardata mellan myndigheter och andra aktörer. Genom att implementera och följa kraven i cybersäkerhetslagen kan medborgarna känna sig ännu tryggare med hur deras information skyddas och används. Detta ökar förtroendet för den offentliga sektorn och stärker det sociala kontraktet mellan medborgare och myndigheter.

Bilagor

1. Sammanfattning delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18)
2. Förslag till Göteborgs Stads yttrande över remiss Nya regler om cybersäkerhet

Ärendet

Remiss för delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18) inkom till Göteborg Stad den 6 mars 2024. Göteborgs Stads yttrande ska vara Försvarsdepartementet tillhanda senast den 28 maj 2024.

Beskrivning av ärendet

Europaparlamentet och EU-rådet antog den 14 december 2022 två nya EU-direktiv, NIS2-direktivet och CER-direktivet. I delbetänkandet redogörs för förslag om införlivning av NIS2-direktivet i svensk rätt. I slutbetänkandet, som planeras vara färdigställt i september 2024, kommer även att lämnas förslag om införlivning av CER-direktivet. Utredningen föreslår i huvudsak att följa de skyldigheter som krävs enligt NIS2-direktivet.

NIS2-direktivet

NIS2-direktivet (NIS2) syftar till att stärka den övergripande cybersäkerheten i EU och skapa en mer enhetlig och robust säkerhetsstruktur över medlemsstaterna. Cybersäkerhet omfattar all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användarna av dessa system och andra berörda personer mot cyberhot enligt EU:s cybersäkerhetsakt 2019/881. NIS2 ersätter det tidigare NIS-direktivet (NIS) och utvidgar antalet sektorer som omfattas i nuvarande NIS från sju till 18 sektorer. I sektorerna inkluderas bland annat energi, transport, hälso- och sjukvård, digital infrastruktur och offentlig förvaltning. Direktivet gäller för både offentliga och enskilda verksamhetsutövare. Då NIS2 benämner offentlig förvaltning som en egen sektor innebär detta att nästan hela den offentliga sektorn omfattas av lagens krav.

I grunden innebär NIS2 att verksamhetsutövare måste arbeta systematiskt och riskbaserat med cyber- och informationssäkerhet för att skydda sin verksamhet, system, IT-användare och andra berörda personer mot cyberhot. Det ställs krav på riskhantering, incidentrapportering till utpekad myndighet inom 24 timmar och utbildning av ledning. Dessutom ska verksamhetsutövaren vidta tekniska, driftrelaterade och organisatoriska riskhanteringsåtgärder för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter.

Det finns en utpekad tillsynsmyndighet för varje sektor (offentlig förvaltning, energi, transport, dricksvatten, avlopp, hälso- och sjukvård, digital infrastruktur, avfallshantering med flera). Det gör att en verksamhet kan få tillsyn av flera tillsynsmyndigheter. Tillsynsmyndigheterna ska utöva tillsyn över hur de verksamheter som omfattas av cybersäkerhetslagen följer de regleringar och föreskrifter som meddelats. Tillsynsmyndigheternas möjligheter att ingripa beror på vilken skyldighet som har överträtts, men består av förelägganden som kan förenas med vite eller sanktionsavgifter.

CER-direktivet

CER-direktivet syftar till att stärka motståndskraften hos kritiska verksamhetsutövare och ersätter det europeiska direktivet om kritisk infrastruktur (ECI-direktivet). CER-direktivet ligger nära NIS och förslag på hur CER-direktivet kommer införlivas i svensk rätt kommer finnas med i slutbetänkandet som planeras vara färdigställt i september 2024.

Förslag och bedömningar i korthet

Delbetänkandet föreslår att införa en ny cybersäkerhetslag och en förordning om cybersäkerhet samt förändringar i ett antal befintliga lagar och förordningar.

Omfattning av lagen om cybersäkerhet

Den nya cybersäkerhetslagen omfattar fler sektorer och aktörer jämfört med nu gällande lagstiftning. Huvudskillnaderna i den föreslagna regleringen jämfört med gällande lagstiftning är att antalet sektorer utökas från sju till 18 och att kraven kommer att gälla för hela verksamheten, inte bara för samhällsviktiga och digitala tjänster.

Cyberssäkerhetslagen är tillämplig på både offentliga och enskilda verksamhetsutövare inom de utpekade sektorerna. Huvudregeln är att alla verksamhetsutövare som är etablerade i Sverige och uppfyller kriterierna för ett medelstort företag omfattas av lagen. Ett medelstort företag är ett företag som sysselsätter minst 50 personer eller har en årsomsättning som överstiger 10 miljoner euro. Vissa utpekade verksamhetsutövare omfattas dock oavsett storlek. Det är Myndigheten för samhällsskydd och beredskap (MSB) som har möjlighet att peka ut vissa särskilt kritiska mindre verksamheter som också ska inkluderas.

För vissa offentliga verksamhetsutövare föreslås en särreglering. Det gäller verksamhetsutövare som bedriver viss säkerhetskänslig verksamhet eller brottsbekämpning, men där detta inte är en övervägande del, exempelvis kommuner. Det innebär att den säkerhetskänsliga delen av verksamheten och den del som avser brottsbekämpning endast kommer att omfattas av informationskrav och eventuell tillsyn och sanktioner. När det gäller säkerhetskänslig verksamhet kommer det att finnas ett undantag från skyldigheter att lämna uppgifter som är säkerhetsskyddsklassificerade.

Väsentliga verksamhetsutövare och viktiga verksamhetsutövare

I NIS2 och den nya cybersäkerhetslagen görs det skillnad på väsentliga verksamhetsutövare och viktiga verksamhetsutövare. För väsentliga verksamhetsutövare finns det en högre sanktionsavgift samt ett mer omfattande tillsynssystem jämfört med viktiga verksamhetsutövare. Tillsyn för väsentliga verksamhetsutövare kan vara förhandstillsyn och efterhandstillsyn. För viktiga verksamheter ska tillsyn genomföras endast om det finns en befogad anledning att anta att cybersäkerhetslagen eller de föreskrifter som har meddelats i anslutning till lagen inte följs.

Enligt delbetänkandet kommer merparten av den verksamhet som bedrivs av nämnder i en kommun ses som väsentlig verksamhet. När det gäller kommunala bolag är det verksamhetens innehåll som avgör om det är väsentlig eller viktig verksamhet.

Tillsyn

Tillsynen enligt den nya cybersäkerhetslagen involverar ett system där tillsynsmyndigheter är utsedda för respektive sektor. Tillsynsmyndigheterna ska säkerställa att riskhanteringsåtgärder, incidentrapportering och andra centrala krav i cybersäkerhetslagen efterlevs. För de sektorer som är nya enligt regleringen har antingen befintliga tillsynsmyndigheter fått utökade ansvarsområden eller nya tillsynsmyndigheter tillkommit. Förslag på tillkommande tillsynsmyndigheter är exempelvis länsstyrelserna i Stockholm, Skåne, Västra Götaland och Norrbottens län samt Läkemedelsverket.

Tillsynsmyndigheternas uppdrag är att bedöma hur verksamhetsutövare lever upp till kraven i cybersäkerhetslagen och tillhörande föreskrifter. Till sitt förfogande har de olika undersökningsbefogenheter som till exempel att begära information och få tillträde till relevanta lokaler (med undantag för bostäder). Tillsynsmyndigheterna får även ålägga verksamhetsutövare att genomgå säkerhetsrevision eller låta genomföra säkerhetsscanningar hos verksamhetsutövare.

För att främja samarbete och effektivitet i tillsynsarbetet föreslås MSB leda ett samarbetsforum där tillsynsmyndigheterna ingår. Detta forum syftar till att underlätta samordningen mellan de olika tillsynsmyndigheterna och bidra till en enhetlig tillsynspraxis.

Ingripanden och sanktioner
Den nya cybersäkerhetslagen ger tillsynsmyndigheterna befogenhet att ingripa mot överträdelser genom en rad olika sanktioner, inklusive förelägganden, förbud mot att utöva ledningsfunktion, sanktionsavgifter och anmärkningar. Dessa sanktioner är tänkta att vara effektiva, proportionella och tillräckligt kraftfulla för att verksamheter ska efterfölja de krav som regleringen innebär.

Sanktionsavgifterna har höjts genom NIS2 och bestäms utifrån överträdelsens allvar. För offentlig verksamhet ligger maximinivåerna för sanktionsavgifter på 10 miljoner kronor. För kommunala bolag, som är enskilda juridiska personer och ofta verkar i konkurrensutsatta miljöer, tillämpas sanktionsavgifter på ett liknande sätt som för privata företag. Detta innebär en maximinivå för sanktionsavgifter på upp till 10 miljoner euro eller 2 procent av den totala globala årsomsättningen för föregående räkenskapsår. För mindre allvarliga överträdelser kan lägre sanktionsavgifter tillämpas.

Leveranskedjan
Av NIS2 framgår att säkerhet i leveranskedjan i ett led är ett minimikrav. Enligt direktivet inbegriper säkerhet i leveranskedja säkerhetsaspekter som rör förbindelserna mellan varje verksamhetsutövare och dess direkta leverantörer eller tjänsteleverantörer. I delbetänkandet görs tolkningen att varje verksamhetsutövare behöver kravställa och vidta riskhanteringsåtgärder endast i förhållande till sin leverantör. Närmare bestämmelser om leveranskedjan kommer framgå i kommande föreskrifter.

Gemensam kontaktpunkt, CSIRT-enhet och cyberkrishanteringsmyndighet
I cybersäkerhetslagen har MSB tilldelats tre roller för att hantera och koordinera cybersäkerhetsfrågor i Sverige: Gemensam kontaktpunkt, CSIRT-enhet (Computer Security Incident Response Team) och cyberkrishanteringsmyndighet.

Aktuell styrning inom området i Göteborgs Stad
Göteborgs Stad har styrdokument som reglerar styrning inom informationssäkerhet, där det redan idag ställs krav likt de som föreslås i cybersäkerhetslagen.

Riktlinje för informationssäkerhet
Göteborgs Stads riktlinje för informationssäkerhet skapar förutsättningar för ett systematiskt, riskbaserat och långsiktigt informationssäkerhetsarbete.

Informationssäkerhet innebär skydd av informationstillgångar avseende:

- Konfidentialitet (att information inte tillgängliggörs eller avslöjas för obehöriga)
- riktighet (att informationen skyddas mot oönskad förändring, att information är korrekt och inte manipulerad eller förstörd)
- tillgänglighet (att information är tillgänglig och användbar när den behövs).

För att uppnå rätt skydd ska informationsägaren genomföra en informationsklassificering och en riskanalys för att därefter vidta lämpliga organisatoriska, personrelaterade, fysiska och tekniska säkerhetsåtgärder. I enlighet med vad som gäller för övrig verksamhet, är ansvaret för informationssäkerheten kopplat till ordinarie verksamhetsansvar.

Det innebär att ansvarig nämnd/styrelse för en verksamhet också är ansvarig för att informationssäkerheten upprätthålls och efterföljs i denna verksamhet.

De skärpta kraven i kommande lagstiftning finns sedan ett år tillbaka i Göteborgs Stads riktlinje för informationssäkerhet.

Göteborgs Stads regel för IT-användare

Göteborgs Stads regel för IT-användare fastställer ansvar och åtagande för IT-användare i Göteborgs Stad samt hur dessa får använda stadens IT-resurser såsom persondator, nätverk, servrar, mobiltelefoni, programvaror, internet och så vidare. Med IT-användare i Göteborgs Stad avses anställda, entreprenörer, inhyrd personal, konsulter och leverantörer som arbetar i eller med stadens IT-resurser. IT-användare har personligt ansvar att följa säkerhetsrutiner och skydda lösenord samt rapportera säkerhetsavvikelser. Det pågår för närvarande en revidering av regeln som planeras att tas upp till kommunstyrelsens sammanträde 2024-05-15, ärendenummer SLK-2024-00392.

Göteborgs Stads riktlinje för säkerhetsskydd

Säkerhetsskydd innebär i korthet förebyggande åtgärder för att skydda Sveriges säkerhet mot antagonistiska angrepp såsom spionerі, sabotage, terroristbrott och andra brott mot landets säkerhet. Av riktlinjen framgår att den som till någon del bedriver säkerhetskänslig verksamhet ska utreda behovet av säkerhetsskydd i en säkerhetsskyddsanalys. Verksamhetsutövaren är ansvarig för att vidta sådana åtgärder som lag, förordning och föreskrifter kräver.

Inhämtande av synpunkter från stadens verksamheter

Med anledning av kort svarstid har det inte varit möjligt att inhämta synpunkter genom nämnd- eller styrelseremiss. Stadsledningskontoret har därmed skickat ut ärendet på förvaltnings- och bolagsremiss för inhämtande av synpunkter. De verksamheter som valts ut är sådana som idag omfattas av befintlig lagstiftning, det vill säga NIS och lagen om samhällsviktiga och digitala tjänster. Grundskoleförvaltningen, Göteborgs Hamn AB, Intraservice, kretslopp och vattenförvaltningen, stadsmiljöförvaltningen och äldre samt vård- och omsorgsförvaltningen har inkommit med synpunkter. Göteborgs Energi AB har tillfrågats men inte inkommit med synpunkter.

Nedan redovisas sammandrag av inkomna remissvar. Svaren i sin helhet finns registrerade på stadsledningskontoret.

Grundskoleförvaltningen

Grundskoleförvaltningen ställer sig positiv till de skärpta kraven på säkerhet i nätverk och informationssystem. Förvaltningen ser att förslagen kan öka belastningen på personalresurser, främst utifrån utökat säkerhetsarbete och incidentrapportering. Definitionen av en betydande incident anses vara för bred vilket kan leda till överrapportering och ökade kostnader. Förvaltningen efterlyser därmed klarare riktlinjer och exemplifieringar kring vad som utgör en betydande incident. Tidskraven för underrättelse om incidenter kan komma att kräva utökad bemanning, även under helger och ledigheter.

Grundskoleförvaltningen ser även att det finns risker kopplade till hur information och register ska överlämnas till tillsynsmyndigheten på ett säkert sätt och hur dessa i sin tur kommer att hanteras.

Göteborgs Hamn AB

Göteborgs Hamn anser att delbetänkandet i betydande grad hänvisar till att detaljer kommer att specificeras i framtida myndighetsföreskrifter. För att Göteborgs Hamn effektivt ska kunna förbereda och säkerställa cybersäkerhet för kritisk infrastruktur krävs specificerad och praktiskt tillämpbar vägledning i de slutgiltiga myndighetsföreskrifterna. I dessa behöver bland annat områden som säkerhet i leveranskedjan, klassificering av kritiska system och data, incidentrapportering och sektoröverskridande samarbete och informationsdelning bli tydligare.

Bolaget har erfarenhet från nuvarande NIS med flera tillsynsmyndigheter och har tydligt sett hur tillsynsmyndigheterna har tolkat direktivet olika. För att adressera dessa utmaningar och säkerställa effektiv implementering av åtgärder krävs att både befintliga och framtida regelverksutmaningar adresseras på ett sätt som är genomförbart och tydligare definierat.

Intraservice

Intraservice ställer sig i stort bakom utredningens förslag. Synpunkter rör bland annat utredningens förslag rörande definition av verksamhetsutövare. Nämligen att enbart kommunstyrelsen ska kunna företräda kommunerna och inte de förvaltningar som i andra motsvarande sammanhang är egna myndigheter och tillsynsobjekt. Intraservice uppmärksammar också otydligheter i utredningen kring fördelningen av ansvar och krav på samordning mellan tillsynsmyndigheter i de olika sektorer som omfattas av lagen. Förvaltningen ser utmaningar och potentiella konflikter när flera myndigheter ska utöva tillsyn av samma verksamhetsutövare. När det gäller gränsöverskridande verksamhetsutövare, exempelvis datacentraltjänster, ser Intraservice ett värde i att det inom EU finns ett likvärdigt regelverk för samtliga sådana verksamhetsutövare.

Intraservice ser att anmälningsskyldigheter och tillsynsmyndigheternas undersökningsbefogenheter behöver förtydligas, eftersom det nuvarande förslaget riskerar att skapa merarbete och ökade kostnader för kommuner. Ett samarbetsforum under ledning av MSB ses positivt för att främja samordning, men förvaltningen efterfrågar tydligare ansvar för deltagarna.

Kretslopp och vatten

Kretslopp och vatten beskriver att de har en verksamhet som i betänkandet pekas ut som antingen högkritisk eller kritisk. Förvaltningen ser därmed att gränsdragningen gentemot säkerhetsskyddslagen (2018:585) blir viktig och utifrån de nya reglerna kan det finnas behov av förtydliganden. Kretslopp och vatten ser även att det finns osäkerheter kopplat till tillsynsansvar, där utredningen pekar på att verksamheter inte bör vara under tillsyn av mer än en tillsynsmyndighet. Det behöver tas större hänsyn till kommuners breda verksamhetsområden. Osäkerhet råder även kring informationsutbyte mellan de myndigheter som kan komma att utöva tillsyn.

Förvaltningen ser även att Göteborgs Stad behöver hitta gemensamma vägar för att möta de krav som framgår av ny reglering. Exempelvis behöver staden säkerställa gemensamma arbetssätt för att identifiera rätt skyddsåtgärder vid informationsklassning samt för att utbilda ledning och medarbetare.

Stadsmiljöförvaltningen
Stadsmiljöförvaltningen instämmer i huvudsak i utredningens förslag till nya regler om cybersäkerhet.

Förvaltningen ser att det finns en risk att verksamhetsutövare får flera tillsynsmyndigheter som kommer att utöva tillsyn gentemot dem gällande delvis samma frågor. Det finns även en risk att det i olika föreskrifter kommer att finnas motsägelsefulla bestämmelser, vilket kan innebära problem med tillämpningen. Utredningen menar att tillsynsmyndigheterna ska samarbeta gällande tillsynen av de verksamhetsutövare som tillhör flera sektorer, men enligt förvaltningen är detta inte är tillräckligt. Det behöver konkretiseras hur tillsynen ska avgränsas. Ett alternativ som stadsmiljöförvaltningen förespråkar är att ha en central tillsynsmyndighet, förslagsvis MSB, i stället för ett antal sektorsspecifika tillsynsmyndigheter. Stadsmiljöförvaltningen ser också ett behov av att det förtydligas vad som avses med betydande incident. På så sätt blir det klart för verksamhetsutövarna vad som ska rapporteras till CSIRT-enheten MSB.

Äldre- samt vård och omsorgsförvaltningen
Äldre- samt vård och omsorgsförvaltningen lyfter att det behöver framgå tydligare hur offentliga aktörer ska hantera den nya lagstiftningen, särskilt givet dess omfattning och det faktum att inte all verksamhet är samhällsviktig. Förvaltningen betonar att det är orimligt att ställa lika höga krav på icke-samhällsviktiga system som på kritiska system, exempelvis journalsystemet. Samtidigt är det viktigt att alla system uppfyller grundläggande säkerhetskrav.

Förvaltningen ser en risk att tillsynen kommer bli inkonsekvent om flera kontrollmyndigheter involveras, vilket kan leda till felaktiga prioriteringar och otydligheter i ansvarsområden. Det är viktigt med en fungerande samordning mellan kontrollmyndigheter för att undvika dubbelarbete och säkerställa effektivitet. Äldre- samt vård och omsorgsförvaltningen pekar även på behovet av samverkan och stöd i upphandlingsfrågor. Västra Götalandsregionen och Sveriges Kommuner och Regioner (SKR) är viktiga samarbetspartners för att hantera framtida utmaningar relaterade till cybersäkerhet inom vården.

Stadsledningskontorets bedömning
Cybersäkerhet omfattar all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användarna av dessa system och andra berörda personer mot cyberhot enligt EU:s cybersäkerhetsakt 2019/881. Samhällets digitala utveckling och de hot som finns inom cyber- och informationssäkerhetsområdet innebär att cybersäkerhet är en prioriterad fråga som berör merparten av stadens verksamheter. I den senaste revideringen av Göteborgs Stads riktlinje för informationssäkerhet, beslutad av kommunfullmäktige 2023-05-25 § 7, togs hänsyn till det kommande NIS2. Verksamheter inom Göteborgs Stad ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete i enlighet med riktlinjen. Detta ligger i linje med intentionerna i NIS2 samt den svenska implementeringen av direktivet i form av ny cybersäkerhetslag.

Det pågår också en översyn av Göteborgs Stads regler för IT-användare som kommunstyrelsen ska besluta om 2024-05-15. I förslag till revidering har hänsyn tagits för att efterleva eventuella krav som uppstår utifrån den nya cybersäkerhetslagen.

Även om staden i sin styrning tagit viss höjd för NIS2 innebär den föreslagna regleringen att det ändå kommer ställas högre krav på stadens verksamheter. Det handlar exempelvis om hantering av incidenter samt central ledning och samordning av cybersäkerhetsarbetet i staden.

Stadsledningskontoret instämmer i huvudsak i delbetänkandets förslag och bedömningar. Det finns dock vissa områden där stadsledningskontoret ser skäl att yttra sig vilka beskrivs nedan.

Kommunen som verksamhetsutövare

Ett centralt begrepp i förslaget till ny lagstiftning är verksamhetsutövare. Utredningen har dragit slutsatsen att en verksamhetsutövare enligt NIS2 är en fysisk eller juridisk person som bedriver verksamhet. SKR har framfört att det inte nödvändigtvis är kommunen som ska betraktas som en verksamhetsutövare. Det skulle vara möjligt att se en nämnd inom kommunen som en särskild enhet, även om den inte utgör en egen juridisk person. Utredningen delar dock inte den uppfattningen. Bedömningen är att de flesta kommuner redan omfattas i sin helhet av kraven i NIS2 genom att de bedriver hemsjukvård. Dessutom bör alla kommuner omfattas för fullständighetens skull. I förslaget till cybersäkerhetslag anges att definitionen av en verksamhetsutövare ska vara en juridisk eller fysisk person som bedriver verksamhet. Offentliga verksamhetsutövare ska bland annat vara kommuner, med undantag för kommunfullmäktige.

En kommun är en sådan aktör som bedriver verksamhet inom flera av de sektorer som NIS2 och förslaget till cybersäkerhetslag omfattar. Även om kommunen är en juridisk person innebär den kommunala nämndorganisationen att en kommun består av flera olika myndigheter som i sig har ett självständigt ansvar för olika delar av kommunens verksamhet. Utifrån det menar stadsledningskontoret att det vore önskvärt med vägledning för den föreslagna lagen. Hur kommer ansvarsfördelningen se ut i den kommunala nämndorganisationen? Vilka möjligheter kommer en kommun ha att fördela ansvar för cybersäkerhet i kommunens verksamheter? En annan fråga som bör belysas är hur ansvaret som verksamhetsutövare ska hanteras när kommuner bedriver verksamhet i gemensam nämnd enligt 3 kap. 9 § kommunallagen (2017:725).

I utredningen anges att det är svårt att tolka direktivet på annat sätt än att den fysiska eller juridiska personens verksamhet omfattas i sin helhet. Det framstår också att incidenter inom en del kan påverka en annan del eftersom nätverks- och informationssystem många gånger är sammankopplade inom hela verksamheten. Detta kan leda till gränsdragningsproblem i försök att dela upp verksamheten. En av de utpekade sektorerna är offentlig förvaltning. Problemet inom denna sektor är att det inte framgår tydligt om offentlig förvaltning avser all verksamhet i en kommun eller endast vissa områden. Stadsledningskontoret anser att det finns behov av förtydliganden av vad som avses med offentlig förvaltning i cybersäkerhetslagen.

Registrering av uppgifter

Utredningen föreslår att verksamhetsutövare ska anmäla sig till respektive tillsynsmyndighet och till dem uppge ett antal obligatoriska uppgifter. Tillsynsmyndigheterna ska sedan lämna uppgifterna till den gemensamma kontaktpunkten, vilket enligt utredningens förslag är MSB.

För att en verksamhetsutövare ska kunna uppfylla sin skyldighet på registrering, bör det förtydligas vilken eller vilka sektorer en kommun anses tillhöra. Detta då anmälan ska ske till olika tillsynsmyndigheter beroende på sektorstillhörighet.

Tolkningen av undantag från regleringen

I delbetänkandet föreslås en särreglering för offentliga verksamhetsutövare som bedriver säkerhetskänslig verksamhet eller brottsbekämpning men där detta inte är en övervägande del. Kommuner omfattas av särregleringen. Enligt förslaget bör den säkerhetskänsliga verksamheten och brottsbekämpningen undantas från flera av kraven i cybersäkerhetslagen.

Kommunerna har ett ansvar att på olika sätt bedriva ett brottsförebyggande arbete och detta utgör en del i samhällets samlade insatser för att förbygga brott. Kommunernas brottsförebyggande arbete bedrivs på olika nivåer och i relation till olika målgrupper. Stadsledningskontoret anser att det finns behov av förtydliganden. Vad avses med brottsbekämpning i det här sammanhanget? Hur ska undantaget för verksamhet som avser brottsbekämpning förstås och avgränsas i en kommunal kontext?

Vägledningar i myndighetsföreskrifter

Utredningen föreslår att föreskriftsrätten ska vara delad mellan MSB och respektive tillsynsmyndighet. Tillsynsmyndigheterna får meddela föreskrifter om till exempel riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning om riskhanteringsåtgärder inom sitt tillsynsområde. MSB har föreskriftsrätten när det gäller till exempel incidentrapportering.

Enligt delbetänkandet pekar MSB på en risk för att kraven tillämpas olika om olika myndigheter får meddela föreskrifter. Göteborgs Stad delar bilden av de risker som detta innebär, bland annat utifrån erfarenheten från nuvarande direktiv. Enligt utredningens uppfattning är det dock viktigt att föreskrifterna kan anpassas utifrån respektive sektor och att den myndighet som har tillsyn också har föreskriftsrätten. Göteborgs Stad delar MSB:s uppfattning att det framstår som ändamålsenligt att MSB får meddela föreskrifter med grundläggande krav på säkerhet. De olika tillsynsmyndigheterna kan vid behov komplettera MSB:s föreskrifter med egna särskilda krav på utökad säkerhet för sin sektor

Mot bakgrund av att utredningen gör en annan bedömning och ett annat vägval menar Göteborgs Stad att det är av stor vikt att det sker en samordning mellan de myndigheter som kommer ha föreskriftsrätt. Detta framstår som särskilt angeläget för kommunerna som ska förhålla sig till krav och tolkningar från flera olika tillsynsmyndigheter. Utredningens förslag att regeringen bör ge MSB i uppdrag att skyndsamt utarbeta en vägledning om riskhanteringsåtgärder till stöd för tillsynsmyndighetens föreskriftsarbete kan bidra till enhetliga krav från tillsynsmyndigheter inom respektive sektor.

Utmaning med flera tillsynsmyndigheter

Utredningens förslag innebär att kommuner som minst kommer att ha två tillsynsmyndigheter. Länsstyrelsen blir tillsynsmyndighet för kommuner som offentlig förvaltning och för sektorn avfallshantering. Eftersom utredningen utgår från att de flesta kommuner kommer att ingå i sektor hälsa och sjukvård kommer också Inspektionen för vård och omsorg utgöra tillsynsmyndighet. Därutöver tillkommer i många fall Livsmedelsverket för sektorerna dricksvatten, avloppsvatten och produktion samt bearbetning och distribution av livsmedel.

Ytterligare tillsynsmyndighet är Transportstyrelsen för sektorn transport. Flera andra kan tillkomma beroende på vilken verksamhet kommunen valt att bedriva själv.

Stadsledningskontoret ser utmaningar gällande tillsynen över verksamhetsutövare som står under flera tillsynsmyndigheter. Den nu rådande tillsynsstrukturen utifrån NIS, där flera myndigheter utövar tillsyn över samma verksamhetsutövare, upplevs svår då regelverk har tolkats olika beroende på tillsynsmyndighet.

Flera tillsynsmyndigheter innebär även en potentiell risk att strukturerna för tillsynsarbetet medför dubbelarbete eller svåra avvägningar och prioriteringar. I förlängningen blir det kostnadsdrivande, såväl för de som granskar som de som granskas. En central fråga är därmed behovet av en tydlig avgränsning och reglering av tillsynsmyndigheternas ansvarsområden.

Tillsynsvägledning

Utredningen lämnar inget förslag på lösning för det fall tillsynsmyndigheter som har tillsyn över samma verksamhetsutövare ger motstridiga besked i respektive vägledning. Enligt utredningen ska respektive tillsynsmyndighet inte utöva tillsyn på den del av verksamheten som är en annan tillsynsmyndighets tillsynsområde. Göteborgs Stad anser att det borde fördelas ett tydligt övergripande ansvar för tillsynsvägledning samt för uppföljning av arbetet.

Definition och hantering av betydande incidenter

Av förslaget till cybersäkerhetslag framgår att ”med betydande incident avses a. en incident som orsakat eller kan orsaka allvarlig driftsstörning för den erbjudna tjänsten eller ekonomisk skada för den berörda verksamhetsutövaren, eller b. en incident som har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada.”. Stadsledningskontoret bedömer att förslagets definition är för bred i sin utformning. Därmed kan en väldigt stor del av de incidenter som kan uppstå definieras som betydande incident, vilket troligen inte är meningen. Det är därmed mycket angeläget att MSB så snart som möjligt meddelar föreskrifter som närmare redogör för betydelsen av ”betydande incident”. Föreskrifterna måste vara mycket tydliga för att undvika felaktig inrapportering av incidenter.

I definitionen av betydande incident anges allvarliga driftstörningar och ekonomisk skada som grund för bedömningen. Incidenter av denna typ kan uppkomma även i verksamheter som inte är samhällsviktiga eller som är helt och hållet frivilliga att tillhandahålla. Underlåtelse att anmäla incidenter enligt delbetänkandets förslag utgör grund för sanktion. Stadsledningskontoret anser att det är av vikt att det förtydligas vad som utgör en anmälningspliktig incident.

I delbetänkandet föreslås att incidenter som är betydande ska anmälas till CSIRT-enheten, det vill säga MSB. Anmälan ska först ske genom en tidig varning inom 24 timmar från det att verksamhetsutövaren fått kännedom om händelsen. Sedan ska ytterligare information lämnas inom 72 timmar och slutrapport inom en månad. Stadsledningskontoret har inga invändningar mot att rapportering ska ske skyndsamt. Dock kan angiven intervall från tidig varning till rapportering med ytterligare information bli svår att hantera, speciellt för verksamheter som idag inte har beredskap utanför kontorstid. En annan utmaning är att verksamhetsutövaren anses vara kommunen som helhet och inte de enskilda kommunala myndigheterna. Det leder till att kontaktleden kan bli många, vilket också gör att tidsramen mellan de två första tidsintervallen blir snäv.

Informationsutbyte och återrapportering

Enligt förslaget om rapporteringsskyldighet ska CSIRT-enheten eller den behöriga myndigheten utan onödigt dröjsmål och om möjligt inom 24 timmar från mottagandet av en tidig varning lämna ett svar till den rapporterande verksamhetsutövaren. Detta svar ska innehålla en initial återkoppling om incidenten och, på verksamhetsutövarens begäran, vägledning eller operativa råd om genomförandet av möjliga begränsande åtgärder.

Det står inget om fortsatt återrapportering tillbaka till verksamhetsutövaren utöver detta. Det bör förtydligas hur återrapportering från CSIRT-enhet till verksamhetsutövare ska ske.

Det bedöms även viktigt att förtydliga hur inrapporterade uppgifter ska användas på regional och unionsnivå. Det bör ske en återkoppling till inrapporterad verksamhet kring vad informationen används till med tillhörande respons från de informerade.

Säkerhet i leveranskedjan

I delbetänkandet framgår att verksamhetsutövare måste bedöma sårbarheten hos leverantörer och deras produkter. Detta kan ställa krav på specifika åtgärder och uppföljningsmekanismer i avtal med leverantörer. Stadsledningskontoret ser att det bör framgå, om inte i slutbetänkandet så åtminstone i kommande föreskrifter, om detta krav kommer att gälla för alla leverantörer, inklusive befintliga avtalsförhållanden, eller enbart för nya avtal framöver.

Medskick till slutbetänkandet

Utredningen kommer i sitt slutbetänkande återkomma med överväganden om ändringar i offentlighets- och sekretesslagen (2009:400). Utan att föregå de slutsatser som utredningen kan tänkas lägga fram önskar stadsledningskontoret i sammanhanget betona de rättsliga förutsättningar som gäller för exempelvis informationsutbytet inom en kommun som ur ett sekretessperspektiv består av flera olika självständiga myndigheter.

Jonas Kinnander	Eva Hessman
Direktör Ärende och utredning	Stadsdirektör

Sammanfattning

Direktivet

Europaparlamentet och rådet antog den 14 december 2022 två nya EU-direktiv, NIS2-direktivet, se bilaga 3 och CER-direktivet. Utredningen redovisar i detta delbetänkande 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. Det är ett minimidirektiv med innebörd att den svenska lagstiftningen skulle kunna innehålla längre gående skyldigheter. Utredningen föreslår med något undantag inte några skyldigheter utöver vad som följer av direktivet.

Vem omfattas av cybersäkerhetsregleringen?

Det finns två viktiga skillnader mellan gällande lagstiftning och förslaget till cybersäkerhetsreglering. Den första är att cybersäkerhetslagen föreslås omfatta betydligt fler aktörer, eftersom antalet sektorer utökas från sju till 18. Den andra viktiga skillnaden är att kraven kommer att gälla för hela verksamheten inte bara för samhällsviktiga och digitala tjänster.

De sektorer som kommer att omfattas är:

- Energi
- Transporter
- Bankverksamhet
- Finansmarknadsinfrastruktur
- Hälso- och sjukvårdssektorn
- Dricksvatten
- Avloppsvatten
- Digital infrastruktur
- Förvaltning av IKT-tjänster (mellan företag)
- Offentlig förvaltning
- Rymden
- Post- och budtjänster
- Avfallshantering
- Tillverkning, produktion och distribution av kemikalier
- Produktion, bearbetning och distribution av livsmedel
- Tillverkning
- Digitala leverantörer
- Forskning

Innebörden är att den som bedriver verksamhet inom någon av sektorerna som utgångspunkt omfattas av kraven i cybersäkerhetsregleringen. Det gäller för såväl offentliga som enskilda verksamhetsutövare.

Som framgår av uppräkningen av sektorer är offentlig förvaltning en egen sektor. Det får till följd att nästan hela den offentliga sektorn omfattas av lagens krav. Utredningen föreslår att cybersäkerhetslagen ska gälla för de flesta statliga myndigheter i Sverige. De som är undantagna är regeringen, Regeringskansliet, myndigheter som lyder under Riksdagen, och domstolar. Detsamma gäller för sammanlagt

16 myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet eller brottsbekämpning.

Vidare omfattas samtliga regioner och kommuner av lagens krav. Undantag gäller enbart för region- eller kommunfullmäktige. Utredningen föreslår också att lärosäten med examenstillstånd ska omfattas av regleringen.

För enskilda verksamhetsutövare gäller som huvudregel ett storlekskrav med innebörd att verksamheten måste sysselsätta minst 50 personer eller ha en årsomsättning som överstiger 10 miljoner euro för att omfattas av lagen. Det betyder att små företag som utgångspunkt inte kommer att beröras. Vissa särskilt utpekade enskilda verksamhetsutövare omfattas dock oavsett storlek. Myndigheten för samhällsskydd och beredskap (MSB) kommer också att ha möjlighet att peka ut vissa särskilt kritiska mindre verksamheter. Enskilda verksamhetsutövare som enbart bedriver säkerhetskänslig verksamhet, brottsbekämpning eller erbjuder tjänster till myndigheter som gör det, är undantagna.

Därutöver kommer lagen att gälla i begränsad utsträckning för offentliga verksamhetsutövare som bedriver säkerhetskänslig verksamhet eller brottsbekämpning, men där den delen inte utgör en väsentlig andel. Motsvarande kommer att gälla för enskilda verksamhetsutövare som bedriver annan verksamhet tillsammans med säkerhetskänslig verksamhet eller brottsbekämpning. För den säkerhetskänsliga delen av verksamheten eller den delen av verksamheten som avser brottsbekämpning kommer det endast att gälla en anmälnings- och uppgiftsskyldighet. Detsamma gäller för verksamheter som redan omfattas av skyldigheter med motsvarande verkan som kraven i cybersäkerhetslagen. Så kommer vara fallet för exempelvis finansiella verksamhetsutövare som omfattas av Dora-förordningen.

Kraven i direktivet

Den nya regleringen ställer krav på verksamhetsutövarna. En verksamhetsutövare som omfattas av lagen ska anmäla sig till sin tillsynsmyndighet och lämna uppgifter om bland annat identitet, kontaktuppgift och verksamhet.

Därutöver ska verksamhetsutövare vidta riskhanteringsåtgärder för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter. Åtgärderna ska utgå från en riskanalys, vara proportionella i förhållande till risken och de ska utvärderas. Det ställs också krav på att verksamhetsutövaren ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete samt krav på att verksamhetens ledning ska genomgå utbildning och att anställda ska erbjudas utbildning.

Slutligen gäller en skyldighet för verksamhetsutövare att rapportera betydande incidenter till MSB i egenskap av CSIRT-enhet (se nedan) inom bestämda tidsgränser. Det betyder att en varning ska lämnas inom 24 timmar efter det att verksamhetsutövaren fått kännedom om den betydande incidenten. Vidare ska en incidentanmälan göras inom 72 timmar och en slutrapport inom en månad.

De uppgifter verksamhetsutövarna lämnar till sin tillsynsmyndighet ovan ska myndigheten använda för att klassificera verksamhetsutövarna som väsentliga eller viktiga och registrera dem.

Det ska också finnas ett särskilt register för gränsöverskridande verksamhetsutövare. Registret ska sedan vidarebefordras till MSB i egenskap av gemensam kontaktpunkt (se nedan) som i sin tur ska informera kommissionen.

Tillsyn

I kommittédirektivet anges att systemet för tillsyn bör utgå från den struktur som finns enligt dagens regelverk. Enligt den nu gällande NIS-lagen finns det för varje sektor och för de digitala tjänster som omfattas av lagen en utpekad tillsynsmyndighet som utövar tillsyn över att regelverket följs. Utredningen föreslår att det även fortsatt ska finnas en tillsynsmyndighet för varje sektor. I de sektorer som är oförändrade i förhållande till det första NIS-direktivet är utredningens förslag att befintliga tillsynsmyndigheter fortsätter att ansvara för dessa. Den kompetens som finns hos befintliga tillsynsmyndigheter bör så långt möjligt även nyttjas för de nya sektorer som omfattas av reglering. Flera tillsynsmyndigheter föreslås därför få utökade ansvarsområden. Utredningen föreslår också fem nya tillsynsmyndigheter. Dessa är länsstyrelserna i Stockholms, Skåne, Västra Götalands och Norrbottens län samt Läkemedelsverket.

Tillsynsmyndigheten ska utöva tillsyn över att cybersäkerhetslagen och föreskrifter som meddelats i anslutning till lagen följs. Tillsynsåtgärder för viktiga verksamhetsutövare får vidtas endast när tillsynsmyndigheten har befogad anledning att anta att regleringen inte följs.

Verksamhetsutövarna ska tillhandahålla tillsynsmyndigheten den information som behövs för tillsynen. Tillsynsmyndigheten får om det finns särskilda skäl ålägga en verksamhetsutövare att på egen bekostnad låta ett oberoende organ utföra en riktad säkerhetsrevision och att redovisa resultatet för tillsynsmyndigheten. Tillsynsmyndigheten får också låta genomföra säkerhetsskanningar hos verksamhetsutövare som omfattas av cybersäkerhetslagen.

MSB ska även fortsättningsvis leda ett samarbetsforum där tillsynsmyndigheterna ingår. Syftet med forumet ska vara att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn.

Gemensam kontaktpunkt, CSIRT-enhet och cyberkrishanteringsmyndighet

För att säkerställa gränsöverskridande samarbete ska varje medlemsstat utse en gemensam kontaktpunkt. Den gemensamma kontaktpunkten ska utöva en sambandsfunktion och bland annat lämna sammanfattande rapporter om betydande incidenter, cyberhot och tillbud till Enisa samt underrätta kommissionen och samarbetsgruppen om antalet verksamhetsutövare i Sverige.

Mot bakgrund av att MSB i dag fullgör de uppgifter som följer av att vara gemensam kontaktpunkt samt myndighetens uppgift att stödja och samordna arbetet med samhällets informationssäkerhet anser utredningen att MSB även fortsatt ska vara gemensam kontaktpunkt i Sverige.

Varje medlemsstat ska också utse eller inrätta en eller flera CSIRT-enheter (Computer Security Incident Response Team). CSIRT-enheten ska bland annat övervaka och analysera cyberhot, sårbarheter och incidenter på nationell nivå och tillhandahålla varningar och information. Vidare ska varje medlemsstat utse eller inrätta en eller flera myndigheter med ansvar för hanteringen av storskaliga cybersäkerhetsincidenter och kriser (cyberkrishanteringsmyndigheter).

Mot bakgrund av de uppdrag MSB har i dag och den kompetens som finns inom myndigheten bedömer utredningen att MSB även fortsatt ska vara CSIRT-enhet samt vara cyberkrishanteringsmyndighet i Sverige.

Varje medlemsstat ska anta en nationell plan för hanteringen av storskaliga cybersäkerhetsincidenter och kriser. Planen ska bland annat innehålla cyberkrishanteringsmyndighetens uppgifter och ansvarsområden. Utformningen av den nationella planen ingår inte i utredningens uppdrag.

Ingripanden och sanktioner

Nuvarande ingripanden och sanktioner

Enligt NIS-lagen får en tillsynsmyndighet ingripa mot överträdelser av vissa skyldigheter i lagen. Tillsynsmyndighetens möjligheter att ingripa beror på vilken skyldighet som har överträtts, men består av förelägganden som kan förenas med vite, eller sanktionsavgifter. Sanktionsavgifterna ska bestämmas till lägst 5 000 kronor och högst 10 000 000 kronor. Tillsynsmyndigheten ska ta särskild hänsyn till vissa omständigheter vid bestämmandet av sanktionsavgiftens storlek.

De nuvarande ingripandena och sanktionerna behålls och kompletteras

Tillsynsmyndighetens möjligheter att besluta om förelägganden (vid vite) och sanktionsavgifter behålls. Tillsynsmyndigheten ska även kunna förelägga en verksamhetsutövare att (1) offentliggöra information om överträdelser av lagens bestämmelser, och att (2) informera användare som kan påverkas av ett betydande cyberhot.

Vidare föreslås tillsynsmyndigheten få ansöka hos allmän förvaltningsdomstol om att en person med ledningsansvar hos en väsentlig verksamhetsutövare ska förbjudas att utöva ledningsfunktioner där. Det krävs särskilda omständigheter för att sådant förbud ska kunna meddelas.

Anmärkning införs som sanktion och ska alltid beslutas vid överträdelser om ingen annan sanktion har använts av tillsynsmyndigheten.

Sanktionsavgifternas maximinivå ska höjas

Lägstanivåerna för sanktionsavgifter behålls på 5 000 kronor. Högstanivåerna höjs väsentligt i jämförelse med gällande nivåer och uppgår:

För väsentliga verksamhetsutövare till det högsta av:

1. Två procent av den väsentliga verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller
2. 10 000 000 euro.

För viktiga verksamhetsutövare till det högsta av:

1. 1,4 procent av verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller
2. 7 000 000 euro.

För offentliga verksamhetsutövare till 10 000 000 kronor.

Tillsynsmyndigheten ska ingripa mot alla överträdelser och beakta fler omständigheter vid val och utformning av sanktioner

Utredningen föreslår att tillsynsmyndigheten ska ingripa mot alla överträdelser av lagen. Den ska i vissa särskilda fall ha möjlighet att avstå från att ingripa, till exempel för att inte bryta mot det s.k. dubbelprövningsförbudet.

Om tillsynsmyndigheten inte avstår från att ingripa ska den åtminstone meddela en anmärkning. Om den ingriper med någon annan sanktion behöver den inte meddela anmärkning.

När tillsynsmyndigheten ingriper ska den alltid beakta alla relevanta omständigheter, men fler omständigheter görs obligatoriska att beakta än vad som tidigare gällt.

Ekonomiska konsekvenser

Utredningens förslag medför ekonomiska konsekvenser för tillsynsmyndigheterna, MSB och verksamhetsutövarna. För tillsynsmyndigheterna handlar det om att betydligt fler verksamhetsutövare kommer att omfattas av lagen. Tillsynsmyndigheterna är enligt utredningens

förslag elva. Sex av dem bedriver redan tillsyn enligt gällande lagstiftning, men fem myndigheter är som framgår ovan nya. Utredningen har som underlag för konsekvensanalysen inhämtat en rapport från Sweco Aktiebolag, som intervjuat de föreslagna tillsynsmyndigheterna och MSB. Av rapporten följer att det varit förenat med svårigheter för myndigheterna att uppskatta de framtida kostnaderna.

Utredningen föreslår att de tillsynsmyndigheter som redan bedriver tillsyn med undantag av Finansinspektionen får ett förstärkt anslag med två miljoner kronor vardera för 2025 avseende löpande kostnader. Skälet är att tillsynsmyndigheterna bör ha utökade resurser för att kunna identifiera vilka verksamhetsutövare som omfattas av den nya lagen, utfärda nya föreskrifter och nya vägledningar utan att samtidigt behöva minska ambitionen med tillsyn. Även MSB bör tillföras motsvarande belopp. De myndigheter som inte redan har tillsynsuppdrag bör få ett förstärkt anslag med fem miljoner kronor vardera för 2025 för att bygga upp tillsynsverksamheten.

Samtidigt föreslår utredningen att regeringen ger Statskontoret i uppdrag att vidare utreda de ekonomiska konsekvenserna för tillsynsmyndigheterna och MSB samt att det för de första åren införs ett återrapporteringskrav för myndigheterna.

För de offentliga verksamhetsutövarna föreslår utredningen att kostnaderna ska finansieras inom befintlig ram. Skälen är att det är rimligt att offentliga verksamhetsutövare vidtar grundläggande säkerhetsåtgärder. Genom förslagen erhåller verksamhetsutövarna också stöd. Vidare kan åtgärder för att förebygga incidenter medföra besparingar.

Förslagen medför även kostnader för enskilda verksamhetsutövare, men även dessa får stöd genom förslagen och det förebyggande arbetet kan medföra besparingar. Som framgått omfattas som huvudregel inte små företag. Kraven kommer att gälla inom hela unionen. Utredningen bedömer därför att regleringen inte får effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt.

Ikraftträdande

Utredningen föreslår att förslagen ska träda i kraft den 1 januari 2025.

Göteborgs Stad

Datum 2024-04-16

Ärendenummer: SLK-2024-00295

Försvarsdepartementet
Diarienummer Fö2024/00496
fo.remissvar@regeringskansliet.se,
visnja.raguz@regeringskansliet.se

Göteborgs Stads yttrande över remiss Nya regler om cybersäkerhet SOU 2024:18

Göteborgs Stad har givits tillfälle att yttra sig över remiss från Nya regler om cybersäkerhet SOU 2024:18. Göteborgs Stad instämmer i huvudsak med delbetänkandets förslag och bedömningar. Det finns dock vissa områden där Göteborgs Stad ser skäl att yttra sig och det är i följande delar:

Kommunen som verksamhetsutövare

Förslag som berörs: 5.2.2 Verksamhetsutövare, 5.2.10 Kommuner, 5.3.1 Jurisdiktion för offentliga verksamhetsutövare.

Ett centralt begrepp i förslaget till ny lagstiftning är verksamhetsutövare. Utredningen har dragit slutsatsen att en verksamhetsutövare enligt NIS2 är en fysisk eller juridisk person som bedriver verksamhet. SKR har framfört att det inte nödvändigtvis är kommunen som ska betraktas som en verksamhetsutövare. Det skulle vara möjligt att se en nämnd inom kommunen som en särskild enhet, även om den inte utgör en egen juridisk person. Utredningen delar dock inte den uppfattningen. Bedömningen är att de flesta kommuner redan omfattas i sin helhet av kraven i NIS2 genom att de bedriver hemsjukvård. Dessutom bör alla kommuner omfattas för fullständighetens skull. I förslaget till cybersäkerhetslag anges att definitionen av en verksamhetsutövare ska vara en juridisk eller fysisk person som bedriver verksamhet. Offentliga verksamhetsutövare ska bland annat vara kommuner, med undantag för kommunfullmäktige.

En kommun är en sådan aktör som bedriver verksamhet inom flera av de sektorer som NIS2 och förslaget till cybersäkerhetslag omfattar. Även om kommunen är en juridisk person innebär den kommunala nämndorganisationen att en kommun består av flera olika myndigheter som i sig har ett självständigt ansvar för olika delar av kommunens verksamhet. Utifrån det menar Göteborgs Stad att det vore önskvärt med vägledning för den föreslagna lagen. Hur kommer ansvarsfördelningen se ut i den kommunala nämndorganisationen? Vilka möjligheter kommer en kommun ha att fördela ansvar för cybersäkerhet i kommunens verksamheter?

En annan fråga som bör belysas är hur ansvaret som verksamhetsutövare ska hanteras när kommuner bedriver verksamhet i gemensam nämnd enligt 3 kap. 9 § kommunallagen (2017:725).

I utredningen anges att det är svårt att tolka direktivet på annat sätt än att den fysiska eller juridiska personens verksamhet omfattas i sin helhet. Det framstår också att incidenter inom en del kan påverka en annan del eftersom nätverks- och informationssystem många gånger är sammankopplade inom hela verksamheten. Detta kan leda till gränsdragningsproblem i försök att dela upp verksamheten. En av de utpekade sektorerna är offentlig förvaltning. Problemet inom denna sektor är att det inte framgår tydligt om offentlig förvaltning avser all verksamhet i en kommun eller endast vissa områden. Göteborgs Stad anser att det finns behov av förtydliganden av vad som avses med offentlig förvaltning i cybersäkerhetslagen.

Registrering av uppgifter

Förslag som berörs: 6.2 Register över väsentliga och viktiga verksamhetsutövare

Utredningen föreslår att verksamhetsutövare ska anmäla sig till respektive tillsynsmyndighet och till dem uppge ett antal obligatoriska uppgifter. Tillsynsmyndigheterna ska sedan lämna uppgifterna till den gemensamma kontaktpunkten, vilket enligt utredningens förslag är MSB. För att en verksamhetsutövare ska kunna uppfylla sin skyldighet på registrering, bör det förtydligas vilken eller vilka sektorer en kommun anses tillhöra. Detta då anmälan ska ske till olika tillsynsmyndigheter beroende på sektorstillhörighet.

Tolkningen av undantag från regleringen

Förslag som berörs: 5.5.3 Undantag för säkerhetsskyddsklassificerade uppgifter, 5.5.4 Undantag för offentliga verksamhetsutövare

I delbetänkandet föreslås en särreglering för offentliga verksamhetsutövare som bedriver säkerhetskänslig verksamhet eller brottsbekämpning men där detta inte är en övervägande del. Kommuner omfattas av särregleringen. Enligt förslaget bör den säkerhetskänsliga verksamheten och brottsbekämpningen undantas från flera av kraven i cybersäkerhetslagen.

Kommunerna har ett ansvar att på olika sätt bedriva ett brottsförebyggande arbete och detta utgör en del i samhällets samlade insatser för att förbygga brott. Kommunernas brottsförebyggande arbete bedrivs på olika nivåer och i relation till olika målgrupper. Göteborgs Stad anser att det finns behov av förtydliganden. Vad avses med brottsbekämpning i det här sammanhanget? Hur ska undantaget för verksamhet som avser brottsbekämpning förstås och avgränsas i en kommunal kontext?

Vägledningar i myndighetsföreskrifter

Förslag som berörs: 7.1 Övergripande lagreglering om riskhanteringsåtgärder, 7.1.2 Riskhanteringsåtgärder, 7.1.3 Systematiskt informationssäkerhetsarbete, 7.2 Ansvar och utbildning – riskhanteringsåtgärder

Utredningen föreslår att föreskriftsrätten ska vara delad mellan MSB och respektive tillsynsmyndighet. Tillsynsmyndigheterna får meddela föreskrifter om till exempel riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning om riskhanteringsåtgärder inom sitt tillsynsområde. MSB har föreskriftsrätten när det gäller till exempel incidentrapportering.

Enligt delbetänkandet pekar MSB på en risk för att kraven tillämpas olika om olika myndigheter får meddela föreskrifter. Göteborgs Stad delar bilden av de risker som detta innebär, bland annat utifrån erfarenheten från nuvarande direktiv. Enligt utredningens uppfattning är det dock viktigt att föreskrifterna kan anpassas utifrån respektive sektor och att den myndighet som har tillsyn också har föreskriftsrätten. Göteborgs Stad delar MSB:s uppfattning att det framstår som ändamålsenligt att MSB får meddela föreskrifter med grundläggande krav på säkerhet. De olika tillsynsmyndigheterna kan vid behov komplettera MSB:s föreskrifter med egna särskilda krav på utökad säkerhet för sin sektor

Mot bakgrund av att utredningen gör en annan bedömning och ett annat vägval menar Göteborgs Stad att det är av stor vikt att det sker en samordning mellan de myndigheter som kommer ha föreskriftsrätt. Detta framstår som särskilt angeläget för kommunerna som ska förhålla sig till krav och tolkningar från flera olika tillsynsmyndigheter. Utredningens förslag att regeringen bör ge MSB i uppdrag att skyndsamt utarbeta en vägledning om riskhanteringsåtgärder till stöd för tillsynsmyndighetens föreskriftsarbete kan bidra till enhetliga krav från tillsynsmyndigheter inom respektive sektor.

Utmaning med flera tillsynsmyndigheter

Förslag som berörs: 8.4.1 System för tillsyn, 8.4.2 Tillsynsmyndigheter i Sverige, 8.4.3 Tillsynsmyndighetens uppdrag, 8.4.4 Tillsyn över viktiga verksamhetsutövare, 8.4.5 Föreskrifter, 8.4.7 Samordning och informationsutbyte

Utredningens förslag innebär att kommuner som minst kommer att ha två tillsynsmyndigheter. Länsstyrelsen blir tillsynsmyndighet för kommuner som offentlig förvaltning och för sektorn avfallshantering. Eftersom utredningen utgår från att de flesta kommuner kommer att ingå i sektor hälsa och sjukvård kommer också Inspektionen för vård och omsorg utgöra tillsynsmyndighet. Därutöver tillkommer i många fall Livsmedelsverket för sektorerna dricksvatten, avloppsvatten och produktion samt bearbetning och distribution av livsmedel. Ytterligare tillsynsmyndighet är Transportstyrelsen för sektorn transport. Flera andra kan tillkomma beroende på vilken verksamhet kommunen valt att bedriva själv.

Göteborgs Stad ser utmaningar gällande tillsynen över verksamhetsutövare som står under flera tillsynsmyndigheter. Den nu rådande tillsynsstrukturen utifrån NIS, där flera myndigheter utövar tillsyn över samma verksamhetsutövare, upplevs svår då regelverk har tolkats olika beroende på tillsynsmyndighet. Flera tillsynsmyndigheter innebär även en potentiell risk att strukturerna för tillsynsarbetet medför dubbelarbete eller svåra avvägningar och prioriteringar. I förlängningen blir det kostnadsdrivande, såväl för de som granskar som de som granskas. En central fråga är därmed behovet av en tydlig avgränsning och reglering av tillsynsmyndigheternas ansvarsområden.

Tillsynsvägledning

Förslag som berörs: 8.4.2 Tillsynsmyndigheter i Sverige

Utredningen lämnar inget förslag på lösning för det fall tillsynsmyndigheter som har tillsyn över samma verksamhetsutövare ger motstridiga besked i respektive vägledning. Enligt utredningen ska respektive tillsynsmyndighet inte utöva tillsyn på den del av verksamheten som är en annan tillsynsmyndighets tillsynsområde. Göteborgs Stad anser att det borde fördelas ett tydligt övergripande ansvar för tillsynsvägledning samt för uppföljning av arbetet.

Definition och hantering av betydande incidenter

Förslag som berörs: 7.3 Incidentrapportering, 8.4.5 Föreskrifter

Av förslaget till cybersäkerhetslag framgår att ”med betydande incident avses a. en incident som orsakat eller kan orsaka allvarlig driftsstörning för den erbjudna tjänsten eller ekonomisk skada för den berörda verksamhetsutövaren, eller b. en incident som har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada.”. Göteborgs Stad bedömer att förslagets definition är för bred i sin utformning. Därmed kan en väldigt stor del av de incidenter som kan uppstå definieras som betydande incident, vilket troligen inte är meningen. Det är därmed mycket angeläget att MSB så snart som möjligt meddelar föreskrifter som närmare redogör för betydelsen av ”betydande incident”. Föreskrifterna måste vara mycket tydliga för att undvika felaktig inrapportering av incidenter.

I definitionen av betydande incident anges allvarliga driftstörningar och ekonomisk skada som grund för bedömningen. Incidenter av denna typ kan uppkomma även i verksamheter som inte är samhällsviktiga eller som är helt och hållet frivilliga att tillhandahålla. Underlåtelse att anmäla incidenter enligt delbetänkandets förslag utgör grund för sanktion. Göteborgs Stad anser att det är av vikt att det förtydligas vad som utgör en anmälningspliktig incident.

I delbetänkandet föreslås att incidenter som är betydande ska anmälas till CSIRT-enheten, det vill säga MSB. Anmälan ska först ske genom en tidig varning inom 24 timmar från det att verksamhetsutövaren fått kännedom om händelsen. Sedan ska ytterligare information lämnas inom 72 timmar och slutrapport inom en månad.

Göteborgs Stad har inga invändningar mot att rapportering ska ske skyndsamt. Dock kan angiven intervall från tidig varning till rapportering med ytterligare information bli svår att hantera, speciellt för verksamheter som idag inte har beredskap utanför kontorstid. En annan utmaning är att verksamhetsutövaren anses vara kommunen som helhet och inte de enskilda kommunala myndigheterna. Det leder till att kontaktleden kan bli många, vilket också gör att tidsramen mellan de två första tidsintervallen blir snäv.

Informationsutbyte och återrapportering

Förslag som berörs: 3.2.12 Rapporteringsskyldigheter, 7.3 Incidentrapportering

Enligt förslaget om rapporteringsskyldighet ska CSIRT-enheten eller den behöriga myndigheten utan onödigt dröjsmål och om möjligt inom 24 timmar från mottagandet av en tidig varning lämna ett svar till den rapporterande verksamhetsutövaren. Detta svar ska innehålla en initial återkoppling om incidenten och, på verksamhetsutövarens begäran, vägledning eller operativa råd om genomförandet av möjliga begränsande åtgärder. Det står inget om fortsatt återrapportering tillbaka till verksamhetsutövaren utöver detta. Det bör förtydligas hur återrapportering från CSIRT-enhet till verksamhetsutövare ska ske.

Det bedöms även viktigt att förtydliga hur inrapporterade uppgifter ska användas på regional och unionsnivå. Det bör ske en återkoppling till inrapporterad verksamhet kring vad informationen används till med tillhörande respons från de informerade.

Säkerhet i leveranskedjan

Förslag som berörs: 7.1.2 Riskhanteringsåtgärder

I delbetänkandet framgår att verksamhetsutövare måste bedöma sårbarheten hos leverantörer och deras produkter. Detta kan ställa krav på specifika åtgärder och uppföljningsmekanismer i avtal med leverantörer. Göteborgs Stad ser att det bör framgå, om inte i slutbetänkandet så åtminstone i kommande föreskrifter, om detta krav kommer att gälla för alla leverantörer, inklusive befintliga avtalsförhållanden, eller enbart för nya avtal framöver.

Medskick till slutbetänkandet

Förslag som berörs: 7.3 Incidentrapportering

Utredningen kommer i sitt slutbetänkande återkomma med överväganden om ändringar i offentlighets- och sekretesslagen (2009:400). Utan att föregå de slutsatser som utredningen kan tänkas lägga fram önskar Göteborgs Stad i sammanhanget betona de rättsliga förutsättningar som gäller för exempelvis informationsutbytet inom en kommun som ur ett sekretessperspektiv består av flera olika självständiga myndigheter.

För Göteborgs kommunstyrelse