Göteborgs Stad

Datum: 2024-05-15
Ärendenummer: SLK-2024-00295

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

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.

Vid behandling av ärendet i kommunstyrelsen antecknade Jörgen Fogelklou (SD) som yttrande en skrivelse från den 15 maj 2024, se bilaga.

Göteborg den 15 maj 2024

Göteborgs kommunstyrelse

Jonas Attenius

Mathias Sköld

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

Sverigedemokraterna har vid upprepade tillfällen yrkat på att Intraservice i Göteborgs Stad bör införa en spärr gällande nedladdning av appen TikTok på stadens mobiltelefoner och surfplattor. Vi har även föreslagit att kommunen ska se över om det finns fler appar som bör begränsas av cybersäkerhetsperspektiv på stadens mobiltelefoner och surfplattor samt att förbud av dessa kommuniceras tydligt i Göteborgs Stads regler för IT-användare. I Sveriges kommuner och regioner delas årligen flertalet mobiler och surfplattor ut som tekniskt hjälpmedel för anställda. Dessa har som huvudsyfte att användas parallellt med en privat mobil enhet, men detta är inte alltid verkligheten för många anställda. Även om det görs uppmaningar i hänseende till vilka appar som ska laddas ner på offentligt finansierade mobila enheter anser vi att tydligare gränsdragningar bör kommuniceras. Ur ett cybersäkerhetsperspektiv finns det flera skäl till att en kommun kan överväga att förbjuda nedladdningar av appen TikTok på offentligt köpta mobiltelefoner.

Flera länder och nyligen EU-parlamentet har beslutat att förbjuda offentligt anställd personal från att ha appen på sina mobiltelefoner av säkerhetsskäl. I USA har Vita huset beslutat att den ska bort från federala enheter inom 30 dagar. I november uppmanade Regeringskansliet sin personal att radera appen.

TikTok har kopplats till flera fall av skadlig programvara och spionprogram. I december 2020 upptäckte forskare en sårbarhet i TikTok-appen som gjorde det möjligt för hackare att komma åt användarnas konton och personliga data. I en annan incident visade det sig att TikTok tyst samlade in användarnas urklippsdata, inklusive känslig information som lösenord och ekonomiska data. Genom att förbjuda TikTok på offentligt köpta mobiltelefoner kan kommunen skydda sina medborgare från liknande cyberattacker.

TikTok kan vara en grogrund för nätfiskeattacker. Hackare kan enkelt skapa falska TikTok-konton och använda för att locka användare att klicka på skadliga länkar eller ladda ner skadliga filer. Sådana attacker kan äventyra säkerheten för användarens enhet och potentiellt leda till datastöld eller ekonomisk förlust.

TikTok har mött flera anklagelser om dataintegritetsbrott. 2020 förbjöds TikTok i Indien på grund av datasekretessproblem, och USA övervägde också att förbjuda appen av liknande skäl. TikToks moderbolag, ByteDance, har anklagats för att dela användardata med den kinesiska regeringen. Genom att förbjuda TikTok på offentligt köpta mobiltelefoner kan kommuner och regioner förhindra eventuella dataintrång och skydda medborgarnas integritet.

Sammantaget kan ett förbud mot TikTok på offentligt köpta mobiltelefoner hjälpa till att mildra flera cybersäkerhetsrisker och skydda kommuners medborgare från potentiella cyberattacker, det vore viktigt eftersom denna typ av attacker förväntas bli allt vanligare. Genom ett proaktivt förhållningssätt till cybersäkerhet kan Sveriges kommuner och regioner garantera säkerheten för sina medborgares personliga och känsliga information.