Kommunstyrelsen

2021-12-08
TJÄNSTESKRIVELSE
Dnr: KFKS 2021/953

Sveriges säkerhet – Behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63)

Yttrande över remiss från Regeringskansliet

Förslag till beslut

Kommunstyrelsens arbetsutskott föreslår att kommunstyrelsen antar förslag på yttrande i enlighet med bilaga 2 till tjänsteskrivelsen daterad den 8 december 2021.

Sammanfattning

Remissen beskriver de allvarliga risker och hot som föreligger i dagens samhälle, med hänsyn till en allt ökande grad av digitalisering av offentlig sektor, där kompetens och resurser kring IT-säkerhet, säkra system och IT-tjänster inte ökar i paritet. Bakgrunden till förslagen är att harmoniera EU:s cybersäkerhetslag med svensk säkerhetsskydds-lagstiftning och att implementera denna. Förslagen innebär bland annat att det införs särskilda krav på nätverks- och informationssystem som hanterar säkerhetskänslig verksamhet, att Försvarets materielverk får i uppdrag att utveckla formerna för införandet av nationella krav på IKT-produkter och att det införs ett utvidgat samrådsförfarande och utökade befogenheter för centrala myndigheter genom ett antal ändringar i säkerhetsskyddslagen. Av det föreslagna yttrandet över remissen lyfts att kommunen instämmer i utredningens problembeskrivning men att utredningens förslag inte tar hänsyn till kommunernas behov, resurser och finansiering.

Ärendet

Utredningens uppdrag

I direktiven till utredningen framhåller regeringen att det finns anledning att nu överväga om ytterligare nationella krav bör införas för att säkerställa att nätverks- och informationssystem som ska användas i säkerhetskänslig verksamhet uppfyller de krav som behövs för att upprätthålla skyddet av sådana verksamheter. Utredningens uppdrag innefattar därför att bedöma om det finns anledning att införa nationella särskilda krav på att IKT-produkter[1], som ingår i ett nätverks- och informationssystem som ska användas i säkerhetskänslig verksamhet, ska vara **certifierade** enligt en nationell särskilt anpassad certifieringsordning utformad för säkerhetskänslig verksamhet. I uppdraget ingår även att

[1] IKT – informations- och kommunikationsteknik

överväga om det finns anledning att införa **krav på godkännande** från en myndighet för att sådana IKT-produkter, -tjänster och -processer ska få tas i drift i viss eller all säkerhetskänslig verksamhet. I uppdraget ingår att göra en internationell jämförelse av lagstiftning som innebär särskilda krav med anledning av nationell säkerhet för IKT-produkter, -tjänster och -processer som ingår i ett nätverks- eller informationssystem i de länder som bedöms vara av intresse.

Utredningens förslag i korthet

Utredningen konstaterar att på samma sätt som den digitala utvecklingen, bland annat i form av 5G-system, molntjänster, artificiell intelligens och kvantdatorer, kan effektivisera samhällsviktiga verksamheter, medför den också nya eller förändrade hot, sårbarheter och risker. Detta påverkar säkerheten i bland annat nätverks- och informationssystem hos många olika verksamhetsutövare, flera med höga skyddsvärden. Informations- och cybersäkerheten utvecklas inte i samma takt som den snabba digitala utvecklingen, vilket medför att riskerna för att drabbas av cyberangrepp eller andra IT-incidenter hela tiden ökar. Hoten kommer främst från främmande statliga aktörer som i olika syften genomför cyberangrepp, men även från kriminella eller ideellt motiverade aktörer.

Flertalet offentliga utredningar och myndighetsrapporter visar att det finns allvarliga brister i informations- och cybersäkerheten hos många myndigheter och andra offentliga aktörer, vilket kan få allvarliga konsekvenser för hela eller delar av den samhällsviktiga verksamheten. Därmed finns det ett behov av att skyndsamt vidta olika åtgärder för att stärka informations- och cybersäkerheten i bland annat säkerhetskänsliga verksamheter. Med anledning av ovan kan utredningens förslag sammanfattas enligt följande.

(1) Berörda myndigheter och övriga aktörer behöver, i större utsträckning än vad som nu sker, samverka och samråda i frågor som avser informations- och cybersäkerhet.
(2) Därtill föreslås att Försvarets materielverk (FMV) får i uppdrag att, i samråd och samverkan med främst de myndigheter som ingår i det nationella cybersäkerhetscentret, utveckla formerna för hur gemensamt framtagna hot-, sårbarhets- och riskbedömningar samt skyddsprofiler kan tas fram till stöd för kravställning på IKT-produkter, -tjänster och -processer som ska användas i nätverks- och informationssystem i säkerhetskänslig verksamhet.
(3) Slutligen föreslås ett utvidgat samrådsförfarande och utökade befogenheter för centrala myndigheter genom ett antal ändringar i säkerhetsskyddslagen.

(1) Behov av ökad styrning och samordning

Behovet av att stärka styrningen och samordningen av digitaliseringen har lyfts av flera offentliga utredningar och rapporter. Det särskilt när det gäller utbyggnad av infrastruktur och samordning av arbete med informations- och cybersäkerhet. Den svenska marknaden utgör en avreglerad marknad med olika skikt av infrastruktur-

producenter, operatörer och tjänsteutvecklare. I ett nationellt perspektiv är Sverige i en situation där nästan alla grundläggande samhällsfunktioner förutsätter och bygger på en fungerande digital infrastruktur. Det saknas dock regler och systematik för och samordning av den digitala utvecklingen och utbyggnaden. Mot bakgrund av mängden offentliga aktörer är detta en uppgift av betydande omfattning då frågan berör bland annat fler än 200 statliga förvaltningsmyndigheter, 21 länsstyrelser, 20 regioner, 290 kommuner, 80 domstolar, 37 lärosäten, och 40 helägda statliga bolag. Det är en omfattande förvaltning som kompliceras av stora skillnader mellan verksamheterna vad gäller uppdrag, storlek, finansiella resurser och kompetens.

Till detta kommer näringslivets verksamheter och alla företag som på något sätt utvecklar, driver och förvaltar samhällets digitala infrastruktur. Motsvarande gäller det övergripande arbetet med att stärka informations- och cybersäkerheten i samhället i stort men även inom säkerhetskänslig och annan samhällsviktig verksamhet. Varje verksamhetsutövare har ansvar för sin egen informations- och cybersäkerhet, bland annat vad avser säkerhet i nätverks- och informationssystem. Det saknas emellertid i dag tillsyn över såväl statliga myndigheters verksamhet som regioners och kommuners verksamhet avseende nätverks- och informationssystem, utom såvitt avser säkerhetskänslig verksamhet och verksamhet som avser vissa samhällsviktiga och digitala tjänster. Ansvaret för tillsynsverksamhet av informations- och cybersäkerhet på dessa reglerade områden utövas dock av flera olika samråds- och tillsynsmyndigheter med i vissa fall tillämpning av olika regelsystem.

Ansvaret för informations- och cybersäkerhet finns således hos många olika aktörer och styrningen och samordningen brister på både statlig, regional och kommunal nivå. Bristen på styrning och samordning medför ökade sårbarheter och risker i nätverks- och informationssystem i säkerhetskänsliga och andra samhällsviktiga verksamheter. Utredningen bedömer att det bland annat finns behov av nationell styrning och samordning vid framtagande av en gemensam hot-, sårbarhets- och riskbedömning till stöd i arbetet med informations- och cybersäkerhet. Berörda myndigheter och övriga aktörer behöver därför i större utsträckning än vad som nu sker samverka och samråda i frågor som avser informations- och cybersäkerhet.

(2) Bristande förutsättningar för en nationell certifieringsordning för nätverks- och informationssystem i säkerhetskänslig verksamhet

En nationell särskilt anpassad certifieringsordning för IKT-produkter kan, när vissa förutsättningar är uppfyllda, vara en åtgärd som kan stärka säkerheten i dessa system. Utredningen bedömer att bestämmelserna i säkerhetsskyddslagen och säkerhetsskyddsförordningen redan ger berörda myndigheter möjlighet att föreskriva att certifierade IKT-produkter, -tjänster och -processer, som uppfyller vissa säkerhetskrav,

ska användas i nätverks- och informationssystem i säkerhetskänslig och även medge undantag från en sådan skyldighet.

En nationell särskilt anpassad ordning för säkerhetskänslig verksamhet ställer krav på att det finns en nationellt framtagen gemensam hot-, sårbarhets- och riskbedömning som kan ligga till grund för säkerhetskrav och framtagande av så kallade skyddsprofiler för olika IKT-produkter, -tjänster och -processer i dessa system. En sådan bedömning är också en förutsättning för inriktning av det nationella arbetet med det europeiska ramverket för cybersäkerhetscertifiering. I dag saknas emellertid nationell organisation och verksamhet som ansvarar för och tar fram en sådan nationell hot-, sårbarhets- och riskbedömning.

Sammantaget gör utredningen bedömningen att det för närvarande inte föreligger tillräckliga skäl att föreslå att det införs en nationell särskilt anpassad certifieringsordning för IKT-produkter, -tjänster och -processer som används i nätverks- och informationssystem i säkerhetskänslig verksamhet.

Det finns dock behov av att berörda myndigheter gemensamt tar fram hot-, sårbarhets- och riskbedömningar samt skyddsprofiler för olika IKT-produkter, -tjänster och -processer som ska användas i nätverks- och informationssystem i säkerhetskänslig verksamhet. Utredningen föreslår därför att regeringen ger Försvarets materielverk (FMV) i uppdrag att, i samråd och samverkan med främst de myndigheter som ingår i det nationella cybersäkerhetscentret, utveckla formerna för hur gemensamt framtagna hot-, sårbarhets- och riskbedömningar samt skyddsprofiler kan tas fram till stöd för kravställning på IKT-produkter, -tjänster och -processer som ska användas i nätverks- och informationssystem i säkerhetskänslig verksamhet. En sådan nationellt framtagen bedömning med åtföljande kravställning kan även till del utgöra underlag i det nationella arbetet inom ramen för det europeiska ramverket för cybersäkerhetscertifiering.

Utredningen bedömer vidare att informations- och cybersäkerheten i statliga myndigheters verksamhet i övrigt behöver stärkas. Åtgärder bör därför vidtas som bidrar till att myndigheterna använder certifierade IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i verksamheten om inte detta framstår som olämpligt eller omöjligt att genomföra. Myndigheten för samhällsskydd och beredskap (MSB) bedöms redan i dag ha bemyndigande att i föreskrifter ange sådant krav på statliga myndigheter. En sådan ordning kan även bidra med kunskap och erfarenheter om behov och användning av certifierade IKT-produkter, -tjänster och -processer i nätverks- och informationssystem i statlig verksamhet och även ligga till grund för det nationella arbetet med hot-, sårbarhets- och riskbedömningar, som utredningen föreslår ska genomföras.

(3) Ett utvidgat samrådsförfarande och utökade befogenheter

För att göra användningen av ett informationssystem i säkerhetskänslig verksamhet säkrare och därmed stärka skyddet för Sveriges säkerhet, föreslår utredningen ändringar i säkerhetsskyddslagen. Föreslagna ändringar innebär bland annat följande åtgärder.

- Befintligt krav på verksamhetsutövare att göra en särskild säkerhetsskyddsbedömning utvidgas till att även omfatta planerade väsentliga förändringar av informationssystem som kan ha betydelse för säkerhetskänslig verksamhet.
- Verksamhetsutövare ska pröva lämpligheten av en planerad driftsättning eller väsentlig förändring av informationssystem som har betydelse för säkerhetskänslig verksamhet. Om lämplighetsprövningen leder till bedömningen att det planerade förfarandet är olämpligt från säkerhetsskyddssynpunkt ska det inte inledas.
- I fall verksamhetsutövarens lämplighetsprövning leder till bedömningen att det planerade förfarandet inte är olämpligt från säkerhetsskyddssynpunkt ska verksamhetsutövaren – om övriga rekvisit för samråd är uppfyllda – samråda med samrådsmyndigheten (Säkerhetspolisen eller Försvarsmakten).
- Verksamhetsutövares skyldighet att, inför driftsättning eller väsentlig förändring av vissa informationssystem, samråda med Säkerhetspolisen eller Försvarsmakten ska inte begränsas till att ske i form av en skriftlig process.
- Säkerhetspolisen och Försvarsmakten ska, i egenskap av samrådsmyndigheter enligt säkerhetsskyddslagen, få inleda samråd och inom ramen för ett samråd besluta åtgärdsföreläggande mot verksamhetsutövaren att vidta en säkerhetsskyddsåtgärd i berört informationssystem.
- Samrådsmyndigheterna ska även få möjlighet att förbjuda en ur säkerhetsskyddssynpunkt olämplig driftsättning eller förändring av informationssystem och besluta sanktionsavgift mot den som åsidosätter samrådsskyldigheten eller agerar i strid med meddelat förbud.
- Tillsynsmyndigheterna får en ny undersökningsbefogenhet genom möjligheten att, vid äventyr av vite, få tillgång till verksamhetsutövares informationssystem.

Juridik- och kanslistaben samlade bedömning och förslag på yttrande

Juridik- och kanslistaben har tillställt remissen till ledningsstaben och digitaliseringsenheten som inkommit med synpunkter över utredningens förslag.

Juridik- och kanslistaben (kansliet) instämmer i det av utredningen identifierade behovet av ett nationellt arbete kring användandet av IKT-produkter i säkerhetskänsliga sammanhang. Kommunal verksamhet behöver resurser för att ta till sig den nya teknikens fördelar för att kunna upprätthålla god kommunal service i takt med den ökande befolkningstillväxten samt ökade krav på funktion och service. Ökat användande

av nya tekniker som AI, robotisering, sensorer och 5G är i sig en stor utmaning där IT- och verksamhetskompetens sträcks till sitt yttersta för att uppnå främsta effektivitet och funktionalitet.

Att säkerhetsskyddslagstiftningen, likt exempelvis dataskyddsförordningen och NIS-direktivet, förutsätter att varje myndighet ska göra en egen utredning och bedömning samt uppfinna en egen lösning, är inte en genomförbar lösning. Det med hänsyn till att erforderliga resurser saknas i kommunerna. Kopplat till just säkerhetskänslig verksamhet försvåras detta avsevärt utifrån att innehållet i och erfarenheten av denna verksamhet inte låter sig diskuteras och delas med andra aktörer mot bakgrund av den sekretess som rådet inom området.

Kansliet konstaterar att den befintliga teknikskulden, blir en utmaning för kommunerna. Kommuner har flertalet diversifierade verksamheter där det inte uppenbart går att använda samma IT-lösningar, vilket leder till att arbetet med cybersäkerhet i säkerhetskänslig verksamhet kommer att ianspråkta betydande tid för att nå önskvärd omfattning. När de kommunala verksamheterna väl kommer igång med detta arbete finns det också risk för att det är svårt att tillse tillgång på kompetens på området cybersäkerhet för säkerhetskänsliga verksamheter.

Avseende förslaget om utökade befogenheter för tillsynsmyndigheterna konstaterar kansliet att exempelvis införandet av viten för brister i säkerhetsskyddsarbetet sannolikt utgör ett direkt kontraproduktivt förslag, för det fall ändamålet är att öka digitaliseringstakten i samhället och samtidigt höja säkerhetsnivån. Det bedöms som mer angeläget att staten fokuserar på att bistå med säkra digitala lösningar och bidrar till en samordning på lokal, regional och statlig nivå för att gemensamt höja säkerhetsnivån bland myndigheter. Viten riskerar att försvåra för kommuner att göra de nödvändiga digitaliseringskliven. I det avseendet förespråkar kansliet att staten tar ett betydligt större ansvar genom att tillföra de resurser som krävs för att stötta kommunerna i arbetet.

Ekonomiska konsekvenser

Ett genomförande av förslagen kommer sannolikt att medföra ökade kostnader för kommunen, både direkta sådana och indirekta, inte minst kopplat till förslaget om viten. Kansliets bedömer att utredningen presterat en bristande och till viss del ofullständig analys avseende konsekvenserna för kommunerna. Det kan konstateras att det föreligger en omfattande förbättringspotential kopplat till den ekonomiska aspekten av förslagen.

Konsekvenser för barn

Förslaget i sig innebär inte några direkta konsekvenser för barn men kan i sin förlängning innebära att möjligheten att satsa resurser till förskola, skola och fritidsverksamheter till barn minskar.

Bilagor

1. Utdrag från SOU 2021:63 – Sammanfattning och författningsförslag
2. Förslag på yttrande

Engin Ceylan
Kanslichef
Juridik- och kanslistaben

Brita Rösblad Molavi
Digitaliseringschef
Digitaliseringsenheten

Henrik Ahl
Stabschef
Stadsledningskontorets stab