Stockholms stad

PM Rotel I (Dnr KS 2021/1167)

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

Remiss från Försvarsdepartementet
Remisstid den 10 januari 2022

Borgarrådsberedningen föreslår att kommunstyrelsen beslutar följande.
Remissen besvaras med hänvisning till vad som sägs i denna promemoria.

Föredragande borgarrådet Anna König Jerlmyr anför följande.

Ärendet

Den digitala utvecklingen i samhället går snabbt. Digitaliseringen innebär nya och förändrade hot, sårbarheter och risker som medför högre krav på informations- och cybersäkerhet.

För nätverks- och informationssystem som används i eller har betydelse för säkerhetskänslig verksamhet finns i dag särskilda krav i säkerhetsskyddslagen (2018:585) och säkerhetsskyddsförordningen (2018:658).

Enligt regeringen finns det anledning att 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 skydda sådan verksamhet. Regeringen har därför tillsatt en utredning, som tagit sig namnet Cybersäkerhetsutredningen, med uppdraget att bland annat överväga om det finns anledning att:

- Införa en nationell särskilt anpassad certifieringsordning för informations- och kommunikationsteknik—produkter (IKT-produkter), tjänster och processer i nätverks- och informationssystem i säkerhetskänslig verksamhet.
- Införa krav på godkännande av en myndighet innan sådana IKT-produkter, tjänster och processer i nätverks- och informationssystem får driftsättas.

Försvarsdepartementet har remitterat utredningens slutbetänkande till staden för yttrande.

Beredning

Ärendet har remitterats till stadsledningskontoret.

Stadsledningskontoret delar utredningens bedömning om att nationella krav på utformning av skyddsåtgärder i informationssystem bör prioriteras men beklagar att arbetet med nationellt godkända underlag inte kommit längre. Utöver detta förslår kontoret viss förändring av de förslag som utredningen presenterar exempelvis

rörande en ny författningsbestämmelse som kräver samråd inför driftsättning eller väsentligt förändring av andra informationssystem.

Mina synpunkter

Digitaliseringens möjligheter är många, men likt beskrivet i utredningen från Försvarsdepartementet måste nya och förändrade hot, sårbarheter och risker hanteras. I stadens budget för 2022 tar vi höjd för detta med riktade satsningar för en förstärkt funktion rörande incidenthanteringsförmåga inom it- och informationssäkerhet.

Likt stadsledningskontoret påpekar är nationella riktlinjer rörande skyddsåtgärder i informationssystem något som bör prioriteras. Det är samtidigt beklagligt att arbetet med godkända underlag inte kommit länge. I övrigt vill jag hänvisa till stadsledningskontorets synpunkter i deras tjänsteutlåtande.

Jag föreslår att borgarrådsberedningen föreslår att kommunstyrelsen beslutar följande.

Remissen besvaras med hänvisning till vad som sägs i denna promemoria.

Stockholm den 8 december 2021

ANNA KÖNIG JERLMYR

Bilaga

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

Borgarrådsberedningen tillstyrker föredragande borgarrådets förslag.

Remissammanställning

Ärendet

Den digitala utvecklingen går snabbt. Digitaliseringen innebär nya och förändrade hot, sårbarheter och risker som medför högre krav på informations- och cybersäkerhet. Regeringen har därför tillsatt en utredning som övervägt om det behöver införas ytterligare åtgärder för att nätverks- och informationssystem som används i säkerhetskänslig verksamhet ska uppfylla de krav som behövs för att skydda verksamheten.

Utredningen anser att det finns skäl att stärka skyddet i nätverks- och informationssystem som har betydelse för säkerhetskänslig verksamhet. Utredningen föreslår därför bland annat flera ändringar i säkerhetsskyddslagen (2018:585) och säkerhetsskyddsförordningen (2018:658) för att förbättra skyddet för Sveriges säkerhet.

Några av de föreslagna ändringar som framför allt bedöms påverka Stockholms stad är följande. Verksamhetsutövare som bedriver säkerhetskänslig verksamhet ska göra en särskild säkerhetsskyddsbedömning och lämplighetsprövning inför driftsättning eller en väsentlig förändring av ett informationssystem som kan ha betydelse för den säkerhetskänsliga verksamheten. Om driftsättningen eller förändringen bedöms vara olämplig ur säkerhetssynpunkt ska den inte inledas. I annat fall ska verksamhetsutövaren, om vissa rekvisit är uppfyllda, samråda med en statlig samrådsmyndighet inför beslutet om driftsättning eller förändring av informationssystemet. Samrådsmyndigheten får också inleda samrådet samt besluta åtgärdsföreläggande mot verksamhetsutövaren att vidta nödvändiga säkerhetsskyddsåtgärder. Vidare får samrådsmyndigheten förbjuda driftsättning eller förändring om förfarandet kan vara olämpligt ur säkerhetsskyddssynpunkt, samt besluta sanktionsavgift mot den verksamhetsutövare som åsidosätter samrådsskyldigheten eller agerar i strid med meddelat förbud. Utredningen föreslår även att tillsynsmyndigheterna får en ny undersökningsbefogenhet och att verksamhetsutövare ska ge tillsynsmyndigheten tillgång till informationssystem och uppgifter som är nödvändiga för tillsynen.

Beredning

Ärendet har remitterats till stadsledningskontoret.

Stadsledningskontoret

Stadsledningskontorets tjänsteutlåtande daterat den 17 november 2021 har i huvudsak följande lydelse.

Stadsledningskontoret delar utredningens syn om behovet att öka informations- och cybersäkerheten i samhället i stort och i säkerhetskänslig verksamhet i synnerhet. Stadsledningskontoret välkomnar därför flera av de förslag till åtgärder och författningsändringar som föreslås i betänkandet, men ser också saker i förslaget som kan tydliggöras eller där ytterligare överväganden behöver göras.

Stadsledningskontoret vill därför lämna följande synpunkter på utredningens förslag.

Stadsledningskontorets generella synpunkter

Stadsledningskontoret delar utredningens bedömning att arbetet med att ta fram nationellt godkända underlag som kan ligga till grund för krav på och utformning av skyddsåtgärder i informationssystem bör prioriteras. Enligt stadsledningskontoret bör detta arbete fullgöras innan det är aktuellt att överväga att införa nya krav på de verksamhetsutövare som bedriver säkerhetskänslig verksamhet.

De brister som utredningen lyfter fram har varit välkända i många år och belyses bland annat i den *nationella strategin för samhällets informations- och cybersäkerhet* som regeringen beslutade år 2017.

Flera av de prioriterade åtgärderna i strategin syftar till att komma till rätta med just dessa brister. Stadsledningskontoret anser att det är beklagligt att arbetet med att ta fram nationellt godkända underlag inte kommit längre, särskilt mot bakgrund av den försämrade omvärldssituationen, den ökade hotbilden mot Sverige och den återupptagna totalförsvarsplaneringen.

Stadsledningskontoret anser att det finns stort behov av nationellt godkända bedömningsunderlag och eventuellt även av certifierade produkter. Det skulle ge verksamhetsutövare av säkerhetskänslig verksamhet ett konkret och välkommet stöd i arbetet med att skydda informationssystem som kan ha påverkan på säkerhetskänslig verksamhet. Nationellt framtagna bedömningsunderlag skulle bidra till att minska flera av de svåra och komplexa frågor och de tekniska och kompetensmässiga utmaningar som verksamhetsutövare behöver hantera när det kommer till att införskaffa eller utveckla säkra informationssystem.

Det går enligt stadsledningskontorets mening inte att bortse från att den nuvarande ordningen – där var och en av alla hundra- eller tusentals verksamhetsutövare som bedriver säkerhetskänslig verksamhet på egen hand behöver ”uppfinna hjulet” med att ta fram hot- och särskilda säkerhetsskyddsanalyser, bedömningsunderlag och att införskaffa säkra informationssystem – sannolikt varit och fortsatt är en stark bidragande orsak till många av de brister och sårbarheter som finns inom informationssäkerhetsområdet. En annan bidragande orsak till den nuvarande situationen bedöms vara att de flesta verksamhetsutövare har mycket begränsad tillgång till personal med rätt kompetens inom informations- och cybersäkerhetsområdet. Kompetensbristen medför också risk att uppgifter och informationssystem av betydelse för Sveriges säkerhet ges olika säkerhetsskydd hos olika verksamhetsutövare, då personal med rätt kompetens och erfarenhet är en förutsättning för att förstå vilka skyddsmekanismer och andra åtgärder som behöver omgärda de informationssystem som har påverkan på säkerhetskänslig verksamhet. De flesta verksamhetsutövare saknar dock tillgång till kvalificerade hotbilder, underrättelser samt de statliga expertmyndigheternas kompetens inom informations- och cybersäkerhetsområdet.

Stadsledningskontoret menar att detta faktum och de brister det medför endast delvis kommer kunna hanteras genom utredningens förslag om att införa ytterligare krav på verksamhetsutövare som bedriver säkerhetskänslig verksamhet. Stadsledningskontoret anser att det går att ifrågasätta vilken reell säkerhetshöjande effekt som sådana krav skulle innebära i praktiken, innan det tagits fram nationella gemensamma hot-, sårbarhets- och riskbedömningar samt godkända kravbilder på säkerhetsnivåer och skyddsprofiler som kan ligga till grund både för kraven och efterföljande skyddsåtgärder. Stadsledningskontoret gör bedömningen att en nationellt samordnad ansats med att ta fram gemensamma beslutsunderlag skulle vara ett betydligt mer kompetens-, resurs- och kostnadseffektivt sätt att stärka informationssäkerheten i säkerhetskänsliga informationssystem. Det skulle också vara ett sätt att få ökad samhällsnytta av de förmågor och kompetenser som de statliga expertmyndigheterna besitter inom informations- och cybersäkerhetsområdet. Stadsledningskontoret anser således att det inte är ändamålsenligt att ställa ytterligare krav på verksamhetsutövare som bedriver säkerhetskänslig verksamhet inom detta område, innan det finns förutsättningar och nödvändigt stöd för verksamhetsutövarna att omhänderta kraven.

Stadsledningskontoret vill framföra vikten av att det i eventuella fortsatta överväganden om att införa en nationellt särskild anpassad ordning för certifiering av IKT-produkter, tjänster och processer även utreds vilka risker det kan medföra för Sveriges säkerhet om en majoritet av landets samhällsviktiga och säkerhetskänsliga verksamheter använder produkter från ett fåtal tillverkare eller leverantörer i sina informationssystem. Ett certifieringsförfarande kan innebära en invecklad och kostsam certifieringsprocess som

endast ett fåtal tillverkare och leverantörer anser att det är motiverat att delta i. Krav på verksamhetsutövare att endast använda sådana nationellt godkända produkter kan innebära en begränsning i utbudet tillgången av verksamhetskritiska produkter, tjänster och processer. Tillgången till sådana produkter kan tänkas bli än mer begränsad om det uppstår en nationell eller internationell bristsituation. Ett sådant krav medför också att samma sorts produkter, tjänster och processer används i ett stort antal samhällsviktiga och säkerhetskänsliga verksamheters informationssystem. Det kan innebära en högre hotbild mot produkterna, inte minst eftersom sårbarheter i dessa därmed kan utnyttjas av en antagonist för att påverka ett stort antal kritiska samhällsfunktioner, vilket kan ge omfattande och svåröverblickbara konsekvenser för Sveriges säkerhet.

Stadsledningskontoret vill också lyfta fram att det kan finnas behov av förtydligande gällande när samråds- och tillsynsmyndigheterna får dela säkerhetsskyddsklassificerade uppgifter som rör eller har lämnats av verksamhetsutövaren mellan varandra.

Stadsledningskontorets synpunkter på förlaget om ändringar i säkerhetsskyddslagen och säkerhetsskyddsförordningen

Stadsledningskontoret avstyrker utredningens förslag till ny författningsbestämmelse som säger att verksamhetsutövaren ska vara skyldig att samråda med samrådsmyndigheten innan informationssystem som kan förutses komma att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen *konfidentiell* eller högre tas i drift, eller i väsentliga avseenden förändras (3 a kap. 2 § säkerhetsskyddslagen). Stadsledningskontoret anser att det vore olämpligt att införa krav på samråd inför en potentiellt mindre riskfylld situation, samtidigt som det inte krävs samråd inför situationer som kan innebära större risk ur säkerhetsskyddshänseende. Den samrådsskyldighet som utredningen föreslår kommer bland annat gälla för en bärbar dator som en enskild medarbetare ska använda för att hantera ett fåtal handlingar i säkerhetsskyddsklassen konfidentiell – även om medarbetaren är säkerhetsprövad av verksamhetsutövaren, datorn kommer förvaras inlåst i verksamhetsutövarens lokaler när den inte används och verksamhetsutövaren kommer ha kontroll över datorn och dess säkerhetsskydd under datorns hela livscykel. Samtidigt finns det inte någon samrådsskyldighet inför ett förfarande som innebär säkerhetsskyddsavtal och där verksamhetsutövare kommer överlämna uppgifter i motsvarande säkerhetsskyddsklass (dvs. konfidentiell) till den externa aktören – trots att ett sådant förfarande kan innebära större exponering av uppgifterna och att verksamhetsutövaren kommer sakna full rådighet över säkerhetsskyddet och hur den andra aktören kommer hanterar uppgifterna. Samrådsskyldigheten i en sådan situation gäller endast för uppgifter i säkerhetsskyddsklassen hemlig eller högre. Samråd är en åtgärd som syftar till att stärka skyddet för Sveriges säkerhet. Om det skiljer sig mellan för vilka situationer det krävs samråd så kommer uppgifter i samma säkerhetsskyddsklass ges olika skydd. Stadsledningskontoret anser att förslaget om samråd för uppgifter i säkerhetsskyddsklassen konfidentiell går emot säkerhetsskyddets grundläggande princip om att skapa ett balanserat och jämnt skydd för säkerhetskyddsklassificerade uppgifter oavsett var, hur eller av vem sådana uppgifter behandlas. Stadsledningskontoret föreslår därför att samrådskravet med samordningsmyndigheten endast ska gälla inför driftsättning eller en väsentlig förändring av ett informationssystem som är avsett att behandla uppgifter i säkerhetsskyddsklassen *hemlig* eller högre. Ett sådant krav harmoniserar bättre med den bestämmelse som införs i säkerhetsskyddslagen den 1 december 2021 om samråd innan en extern aktör får tillgång till uppgifter i säkerhetsskyddsklassen *hemlig* eller högre i samband med en upphandlings-, samarbets- eller samverkanssituation.

Stadsledningskontoret föreslår en ändring av utredningens förslag till ny författningsbestämmelse som säger att det ska krävas samrådsskyldighet innan en väsentlig förändring av ett informationssystem införs (3 a kap. 2 § säkerhetsskyddslagen). Stadsledningskontoret anser att det bör införas ett undantag som gör det möjligt för en verksamhetsutövare som ansvarar för informationssystemets säkerhetsskydd att få genomföra vissa säkerhetshöjande åtgärder innan samråd genomförts, även om det kan innebär en väsentlig förändring av informationssystemet. Verksamhetsutövaren bör dock vara skyldig att samråda med samrådsmyndigheten i ett senare skede. Undantagen kan exempelvis gälla vid en tidskritisk händelse där det är nödvändigt att vidta skyndsamma åtgärder för att upprätthålla säkerheten i informationssystemet eller för att begränsa konsekvensen av ett

pågående angrepp, liksom om det uppstår behov av bortforsling eller förstöring av informations- och kommunikationsutrustning i samband med höjd beredskap eller krig. Enligt utredningens nuvarande förslag kommer även sådana säkerhetshöjande åtgärder behöva samrådas innan de genomförs, vilket kan leda till försening och därmed ett försämrat skydd för Sveriges säkerhet.

Stadsledningskontoret önskar ett förtydligande kring utredningens förslag till ny författningsbestämmelse som säger att det ska krävas samrådsskyldighet innan en väsentlig förändring av ett informationssystem införs (3 a kap. 2 § säkerhetsskyddslagen).

Stadsledningskontoret önskar att det förtydligas att det med *väsentlig förändring* inte avses krav på samråd inför avveckling av ett informationssystem som används i säkerhetskänslig verksamhet. Krav på samråd även inför avveckling kan riskera att försena avvecklingsprocessen, vilket kan leda till ökade kostnader för verksamhetsutövaren. En sådan försening kan även påverka Sveriges säkerhet då informationssystemet behöver kvarstå i drift, och därmed exponeras för en antagonist, under längre tid än vad som är nödvändigt för den säkerhetskänsliga verksamhetens behov. Det får förutsättas att verksamhetsutövaren endast avvecklar ett informationssystem om verksamheten inte längre har behov av informationssystemet eller av de uppgifter som behandlas i informationssystemet, eller i de fall som informationssystemet bedöms för osäkert för att försätta vara driftsatt. Enligt stadsledningskontorets mening kommer avvecklingsbeslut som fattas på saklig grund inte påverka informationssäkerheten för informationssystemet eller uppgifterna, utan snarare stärka verksamhetsutövarens säkerhetsskydd. Avvecklingsbeslut bör därför inte behöva samrådas med samrådsmyndigheten.

Stadsledningskontoret föreslår en ändring av utredningens förslag till ny författningsbestämmelse som säger att det ska krävas samråd inför driftsättning eller en väsentlig förändring av andra informationssystem, om *obehörig åtkomst* till informationssystemen kan medföra skada för Sveriges säkerhet som inte är obetydlig (3 a kap. 2 § säkerhetsskyddslagen). Informationssystem som används i säkerhetskänslig verksamhet i övrigt (exempelvis styr- och reglersystem inom dricksvattenförsörjningen) är främst skyddsvärda ur *tillgänglighets*- och *riktighetsperspektiv.* Stadsledningskontoret anser att det kan uppstå en otydlighet när samrådskravet ska gälla för sådana informationssystem – eftersom den skada som kan uppstå i samband med obehörig åtkomst främst utgår från ett *konfidentialitetsperspektiv*, dvs. att någon som inte är behörig får tillgång till informationssystemet eller de uppgifter som behandlas i systemet. Stadsledningskontoret anser därför att författningskravet bör ändras till att gälla om obehörig påverkan på informationssystemet kan påverka informationssystemets *tillgänglighet* eller *riktighet* och om konsekvenserna kan medföra skada för Sveriges säkerhet som inte är obetydlig.

Stadsledningskontoret föreslår en ändring av utredningens förslag till ny författningsbestämmelse som säger att samrådsmyndigheten under vissa förutsättningar får förbjuda driftsättning eller förändring av en verksamhetsutövares informationssystem (3 a kap. 5 § säkerhetsskyddslagen). Enligt stadsledningskontoret kan ett sådant förbud påverka verksamhetsutövarens möjlighet att bedriva den säkerhetskänsliga verksamheten och därmed medföra konsekvenser för Sverige säkerhet. Ett förbud kan begränsa verksamhetsutövarens möjlighet att bedriva den säkerhetskänsliga verksamheten på ett ändamålsenligt, säkert och resurs- och tidseffektivt sätt. Verksamhetsutövaren kan som följd av ett sådant beslut behöva avbryta den säkerhetskänsliga verksamheten eller införa kompensatoriska åtgärder för att kunna upprätthålla den. Manuella åtgärder ger sannolikt sämre spårbarhet i hanteringen av uppgifter jämfört med vid digital hantering, vilket kan medföra brister i säkerhetsskyddet. Alternativa metoder kan också inverka menligt på verksamhetens robusthet eller tillgänglighet. Enligt stadsledningskontoret kan ett förbud vara nödvändigt för att inte äventyra Sveriges säkerhet, men det kan också medföra andra konsekvenser för Sverige säkerhet än de som samrådsmyndigheten haft för avsikt att förhindra med beslutet. Stadsledningskontoret föreslår därför att samrådsmyndigheten även bör få till uppgift att beakta de hot och sårbarheter samt andra konsekvenser som ett förbud mot driftsättning eller väsentlig förändring av ett informationssystem kan medföra för den säkerhetskänsliga verksamheten och Sveriges säkerhet i övrigt, och väga in dessa aspekter i den proportionalitetsbedömning som myndigheten är ålagd att göra inför ett sådant beslut.

Stadsledningskontoret önskar ett förtydligande kring utredningens förslag till nya författningsbestämmelser som säger att en verksamhetsutövare som står under tillsyn ska ge

tillsynsmyndigheten tillgång till dennas informationssystem i den omfattning som krävs för tillsynen (6 kap. 3 och 4 §§ säkerhetsskyddslagen). Det bör förtydligas att tillsynsmyndigheten endast har rätt att ta del av de delar av informationssystemet och få tillgång till de uppgifter som har betydelse för tillsynen, och inte till hela informationssystemet eller alla säkerhetsskyddsklassificerade uppgifter som förekommer i systemet. Stadsledningskontoret anser också att det kan vara lämpligt att förtydliga att verksamhetsutövaren även i samband med tillsyn är skyldig att vidta åtgärder för att upprätthålla informationssäkerheten för informationssystemet och de säkerhetsskyddsklassificerade uppgifter som förekommer i systemet. Det bör inbegripa att begränsa tillsynsmyndighetens tillgång till och möjlighet att påverka informationssystemet och de uppgifter som inte är nödvändiga för tillsynen.

Stadsledningskontoret avstyrker utredningens förslag till ny författningsbestämmelse som säger att samrådsmyndigheten ska ha rätt att ta ut sanktionsavgift av en verksamhetsutövare (7 kap. 2 a § säkerhetsskyddslagen). Stadsledningskontoret bedömer att frågor om när avgiften ska tas ut, hur sanktionsavgiften ska bestämmas, vilka omständigheter som samrådsmyndigheten ska ta hänsyn till i samband med bestämmandet och vilka konsekvenser det kan innebära att många olika tillsyns- och samrådsmyndigheter ska få rätt att ta ut sanktionsavgift inte har utretts i tillräcklig omfattning för att ge en förutsebar rättstillämpning. Stadsledningskontoret anser därför att förslaget om sanktionsavgift bör utredas närmare. Stadsledningskontoret föreslår en ändring av utredningens förslag till ny författningsbestämmelse som säger att Säkerhetspolisen och Försvarsmakten ska vara samordningsmyndigheter inom sina respektive *tillsynsområden* (3 kap. 1 § säkerhetsskyddsförordningen). Den statliga tillsynsstrukturen inom säkerhetsskyddsområdet kommer att ändras till följd av den nya säkerhetsskyddsförordningen (2021:955) som träder i kraft den 1 december 2021. Säkerhetspolisens och Försvarsmaktens ansvarsområden inom tillsynsverksamheten kommer då avgränsas jämfört med i dag. Stadsledningskontoret anser därför att det vore lämpligare om myndigheternas samrådsansvar speglar de ansvarsområden myndigheterna kommer ha i egenskap av samordningsmyndighet, istället för att samrådsansvaret ska vara begränsat till myndigheternas respektive tillsynsansvarsområde.