FÖRSVARSMAKTEN Säkerhetspolisen

220401 **Bilaga B2**

Inriktning för samråd med Post- och telestyrelsen (PTS) inför tilldelning av frekvenstillstånd

Inledning

PTS ska samråda med Säkerhetspolisen och Försvarsmakten i ärenden som rör tillstånd att använda radiosändare i syfte att klarlägga om en tillståndsansökan kan antas komma att orsaka skada för Sveriges säkerhet.

Säkerhetspolisen och Försvarsmakten (härefter *samrådsmyndigheterna*) kommer i sin bedömning bland annat beakta de styrande principer som presenteras nedan. Samrådsmyndigheterna kommer vidare att göra en riskbedömning där man beaktar icke-tekniska sårbarheter och andra eventuella risker hos operatörer och leverantörer.

Följande dokument redogör på en mer detaljerad nivå för de tekniska krav som är kopplade till respektive princip samt även beroendeförhållanden mellan principerna. Vidare redogörs för de kriterier som samrådsmyndigheterna kommer att beakta i förhållande till riskbedömning av aktörer.

Bestämmelserna i lagen (2003:389) om elektronisk kommunikation (LEK) om skydd av Sveriges säkerhet vid radioanvändning gäller för alla typer av tillståndspliktig användning av radiosändare. Följande dokument redogör dock framförallt för krav och bedömningsunderlag som samrådsmyndigheterna kommer att beakta vid samråd av ansökningar inom ramen för *Allmän inbjudan del 1 till ansökan om tillstånd att använda radiosändare i 900 MHz-, 2,1GHz- och 2,6GHz-banden.*

För det fall de svar och redogörelser som operatörerna inkommer med innehåller säkerhetsskyddsklassificerade uppgifter ska dessa hanteras enligt gällande lagstiftning.

Principer för elektroniska kommunikationsnät som är vitala för Sveriges säkerhet och för leverantörer av sådana nät

De styrande principerna utgör ett underlag för hur samrådsmyndigheterna anser att leverantörer av vitala elektroniska kommunikationsnät ska utforma sina nät för att beakta det skydd som är nödvändigt för Sveriges säkerhet. I detta sammanhang avses främst nätens övergripande funktionalitet och av operatören tillhandahållna kommunikationstjänster till slutanvändare.

De första elva principerna rör primärt tekniska och procedurella krav medan de övriga fem beskriver hur operatörerna ska möta krav på insyn, kontroll och övergripande säkerhetslösningar inklusive säkerhetsskyddsåtgärder.

I förhållande till nätens övergripande funktionalitet ställer respektive princip unika krav samtidigt som uppfyllandet av vissa principer är en förutsättning för uppfyllandet av andra. I den övergripande beskrivningen av systemarkitektur som efterfrågas i Bilaga B1 till Allmän inbjudan del 1 ska det därför framgå hur respektive princip uppfylls. Nedan redogörs för vad som kommer att beaktas när samrådsmyndigheterna gör sin bedömning. Ansökan ska innehålla en

redovisning för hur respektive princip kommer att uppfyllas. I de fall principen helt eller delvis uppfylls med hjälp av internationella standarder ska informationen åtföljas av hänvisning till relevant standard.

Operatörerna förutsätts tillämpa principerna i dialog och kravställning mot leverantörer och underleverantörer av hårdvara/mjukvara samt drift och underhåll.

Med centrala funktioner avses funktioner i bland annat radioaccessnät, kärnnät, transmissionsnät, drift- och underhållsnät som är nödvändiga för att upprätthålla nätens övergripande funktionalitet och av operatören tillhandahållna kommunikationstjänster till slutanvändare samt regulatoriska tjänster (såsom exempelvis 112).

1. Ska fungera även om anslutningar till utlandet bryts

Beskrivning:

Operatören ska visa att centrala funktioner kontinuerligt fungerar inom Sverige och inte är beroende av anslutningar till utlandet.

Principen är övergripande relaterad till tillgänglighet som i detalj beskrivs under princip 3.

Operatören ska ha en tydlig planering för hur nätet ska fungera om störningar i förhållande till produkter och leverantörer uppstår samt att säkerhetsincidenter kan hanteras från Sverige och att system- och användardata lagras i Sverige.

2. Ska tillhandahålla funktioner som medger att förbindelser till och från utlandet enkelt, snabbt och selektivt kan brytas

Beskrivning:

Operatören ska redogöra för anslutningspunkter mot utlandet, deras funktion samt hur brytning av förbindelse (anslutning) går till.

Principen är beroende av bland annat princip 1, då brytning av förbindelser till utlandet annars skulle få nätet att gå ner eller avsevärt begränsa dess funktionalitet.

Operatören ska ha en tydlig planering av hur nätet ska fungera vid störningar eller cyberangrepp från utlandet. Vidare ska operatören ange hur utländsk påverkan förhindras, till exempel genom att tillgång till verktyg för övervakning och granskning av nätverkstrafik inte medges från utlandet.

3. Ska tillhandahålla hög tillgänglighet och sekretess

Beskrivning:

Operatören ska inkomma med specifikation av vilka funktioner som anses vara av vikt för tillgänglighet och sekretess samt vilka skyddsåtgärder som vidtas för att upprätthålla dessa.

Denna princip är delvis beroende av princip 4, eftersom kraven i princip 3 inte kan uppfyllas utan att operatören har ”erforderlig kontroll”.

Operatören ska redogöra för hur nätverk för till exempel administration, behörighetshantering, drift, underhåll, operation, styrning och miljöhantering samt data relaterat till dessa skyddas och separeras från andra nätverk såsom exempelvis internet, operatörens trafikplan och företagsnät samt andra nätverk med kopplingar till internet.

Operatören ska visa hur risker kopplade till kontroll- och signaleringsplanen hanteras.

Operatören ska redovisa att virtualiseringsskiktet kommer att realiseras på ett sätt som säkerställer tillgänglighet och sekretess i hela nätverket inklusive men inte begränsat till konfigurering och livscykelhantering.

4. Ska medge erforderlig insyn och kontroll

Beskrivning:

Operatören ska redogöra för hur systemarkitektur och processer minimerar risken för att nätverkskomponenter kan användas för kartläggning och manipulation. I detta ingår bland annat redovisning av verktyg och processer för kartläggning och identifiering av nätverkstrafik samt gränssnitt mot administrativa funktioner (såväl fysiska som logiska).

Vidare ska operatören redovisa hur insyn och kontroll tillämpas i förhållande till leverantörer och dess underleverantörer.

Denna princip är delvis beroende av princip 5 eftersom operatören inte kan anses ha ”erforderlig kontroll” om inte ”otillåten styrning” förhindras, dessutom beroende av princip 9 eftersom behörighetskontroll är nödvändig för att uppnå denna princip.

5. Ska utformas så att otillåten styrning eller manipulering förhindras

Beskrivning:

Operatören ska redogöra för vilka åtgärder som vidtas för att skydda centrala funktioner i nätet mot otillåten styrning och manipulering, exempelvis genom separering av administration och signalering samt användning av trafikskydd.

Vidare ska operatören redovisa hur ovanstående tillämpas i förhållande till leverantörer och dess underleverantörer.

Denna princip är primärt beroende av princip 3 (tillgänglighet) och princip 4 (erforderlig kontroll).

6. Ska utformas så att styrning eller manipulering från utlandet förhindras

Beskrivning:

Denna princip ska ses som ytterligare krav utöver princip 5. Operatören ska, liksom under princip 1, visa att centrala funktioner för nätet finns inom Sverige och inte är tillgängliga för styrning och manipulation från utlandet.

7. Ska utformas så att otillåten kartläggning av tjänster, kapacitet, lokalisering eller användare förhindras

Beskrivning:

Med tjänster avses såväl tjänster i nätets centrala funktioner som av operatören tillhandahållna kommunikationstjänster till slutanvändare och regulatoriska tjänster (såsom exempelvis 112).

Operatören ska redogöra för hur både fysisk och virtualiserad infrastruktur konfigureras för att dels säkerställa säkerheten i nätet, dels motverka otillåten inhämtning (t.ex. spionage eller annan underrättelseverksamhet) mot nätets centrala funktioner och användardata. I detta ingår också skydd av databaser där det finns användardata inklusive lokaliseringsuppgifter och uppgifter om använda tjänster och kapacitet.

Vidare ska operatören redovisa hur ovanstående tillämpas i förhållande till leverantörer och dess underleverantörer.

Det som beskrivs under denna princip utgör ytterligare krav i förhållande till övriga principer.

8. ***Ska utformas så att otillåtna angrepp (såsom elektroniska attacker) förebyggs och där så inte är möjligt ska dessa upptäckas och förhindras***

Beskrivning:

Operatören ska redovisa åtgärder för att säkerställa funktioner för att: identifiera, skydda, upptäcka och agera mot cyberangrepp eller andra elektroniska attacker samt återställa funktionalitet.

Vidare ska operatören redovisa hur ovanstående tillämpas i förhållande till leverantörer och dess underleverantörer.

Det som beskrivs under denna princip utgör ytterligare krav i förhållande till övriga principer.

9. ***Ska ha behörighetskontrollsystem för de funktioner som kan påverka sekretess, tillgänglighet, insyn och kontroll***

Beskrivning:

Operatören ska redogöra för behörighetskontrollsystem avseende de centrala funktionerna. I detta ingår bland annat att beskriva hur behörigheter utformas och implementeras i den virtuella infrastrukturen samt rutiner för utfärdande och livscykelhantering av behörigheter. Operatören förutsätts ha rutiner som säkerställer att behörighetskontrollsystemen är kontinuerligt i drift och utvecklas i takt med nätet.

Vidare ska operatören redovisa hur ovanstående tillämpas i förhållande till leverantörer och dess underleverantörer. Policys för behörigheter ska särskilt beakta risker i förhållande till extern åtkomst från tredje part och hanteras för att minimera dessa risker.

Denna princip är primärt beroende av princip 5 (otillåten styrning förhindras).

10. ***Ska ha spårbarhet för funktioner som kan påverka sekretess, tillgänglighet, insyn eller kontroll***

Beskrivning:

Operatören ska redogöra för utrustning (fysisk och virtuell) kopplad till centrala funktioner i nätet samt beskriva system och rutiner för loggning, logganalys och säkerhetsgranskning. Detta avser också aktiviteter från tredje part.

Denna princip är primärt beroende av princip 9 (behörighetskontroll-system).

11. ***Ska utformas så att utrustning där det finns risk för otillåten insyn, kontroll eller manipulation genom fysisk åtkomst ska förläggas på svenskt territorium så att svensk lagstiftning blir tillämplig***

Beskrivning:

Operatören ska visa att centrala funktioner för nätet finns lokaliserade i Sverige (se princip 1). Vidare krävs att säkerhetsincidenter kan hanteras från Sverige och att system- och användardata lagras i Sverige.

12. ***Operatören ska kontinuerligt lämna information till utsedda mottagare hos sektorsansvarig myndighet rörande åtgärder, som vidtas i kommunikationsnäten, vilka kan påverka sekretess, robusthet, tillgänglighet, insyn eller kontroll***

13. Operatören ska lämna information i så god tid att sektorsansvarig myndighet kan avgöra vilka risker sådana åtgärder som vidtas i kommunikationsnäten innebär och om åtgärder behövs

14. Operatören ska aktivt underlätta sektorsansvarig myndighets insyn och kontroll

Beskrivning av princip 12, 13 och 14:

Operatören ska beskriva en modell och rutin för informationsdelgivning avseende centrala funktioner till tillsynsmyndigheter.

Vidare ska operatören redovisa hur ovanstående tillämpas i förhållande till leverantörer och dess underleverantörer.

15. Operatören ska ta fram, implementera, drifta samt underhålla adekvata säkerhetsskyddsåtgärder

Beskrivning:

Principen är av övergripande karaktär där en sammantagen bedömning görs av operatörens säkerhetslösning inklusive säkerhetsskyddsåtgärder.

Operatören ska redogöra för sin övergripande säkerhetsarkitektur inklusive grad av nätverksintegration, flexibilitet och automatisering samt administrativa säkerhetsåtgärder i förhållande till olika säkerhetslösningar. Koppling till respektive princip (1-11) ska tydligt framgå.

Vidare ska operatören redovisa hur ovanstående tillämpas i förhållande till leverantörer och dess underleverantörer.

16. Operatören ska se till att personal, som får tillgång till uppgifter vilka kan påverka konfidentialitet, riktighet, robusthet och tillgänglighet, är godkänd och utbildad i säkerhetsskydd samt medvetna om uppgifternas sekretess

Beskrivning:

Principen är av övergripande karaktär där en sammantagen bedömning görs av operatörens säkerhetskyddsåtgärder i förhållande till personal- och informationssäkerhet.

Kriterier för bedömning av aktörer

Vid bedömningen kommer samrådsmyndigheterna, utöver de principer som presenteras ovan, också att beakta icke-tekniska sårbarheter och eventuella andra risker hos operatörer, leverantörer och underleverantörer (jfr vad som följer av den s.k. EU Toolbox[1]).

Samrådsmyndigheterna kommer att beakta bl.a. följande kriterier:

- Sannolikheten för att operatören eller leverantören utsätts för påverkan/påtryckningar. Sådan påverkan/påtryckning kan understödjas av, men är inte begränsat till, förekomsten av följande faktorer:
    - Koppling, bl.a. ägarförhållanden men även andra kopplingar, till regering eller myndigheter i tredje land (icke EU-land).
    - Tredje lands lagstiftning, särskilt i de fall där rättsliga eller demokratiska principer saknas eller där inga överenskommelser om säkerhet eller dataskydd kan tillämpas.
    - Kopplingar till länder eller organisationer som bedriver offensiva cyberoperationer eller annan antagonistisk verksamhet mot Sverige.
    - Övriga möjligheter för tredje land att utöva påtryckningar, bland annat i relation till geografisk placering av produktionstillgångar.

- Leverantörens förmåga att säkerställa leverans av kritiska produkter.

[1] NIS Cooperation Group. CG Publication 01/2020. *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*