EUROPEISKA KOMMISSIONENS SVAR PÅ EUROPEISKA REVISIONSRÄTTENS SÄRSKILDA RAPPORT:

”UTBYGGNADEN AV 5G I EU: FÖRSENINGAR I UTBYGGNADEN AV NÄT OCH SÄKERHETSPROBLEM SOM FORTFARANDE ÄR OLÖSTA”

SAMMANFATTNING

Inledande anmärkningar från kommissionen

I. En snabb och säker utbyggnad av 5G-nät är en viktig prioritering för Europeiska kommissionen. Att skydda 5G-nätverk mot it-hot handlar om att bedöma och minska hot och risker. Medlemsstaterna har gemensamt identifierat och bedömt dessa hot och risker med stöd av kommissionen och Enisa. På grundval av detta arbete har sedan en rad omfattande åtgärder fastställts för att minska riskerna. Även om arbetet fortfarande pågår i vissa medlemsstater har de allra flesta medlemsstaterna redan förstärkt säkerhetskraven för 5G-nät med hjälp av EU:s verktygslåda, eller håller på att göra det.

EU:s verktygslåda är en erkänd och omfattande ram för hantering av 5G-säkerhetsrisker.

Den samordnade insatsen för 5G-säkerhet på EU-nivå och EU:s verktygslåda ingår i en bredare europeisk ram för skydd av elektroniska kommunikationsnät och annan kritisk infrastruktur, och kompletterar befintliga åtgärder såsom den europeiska kodexen för elektronisk kommunikation, telekomramen, cybersäkerhetsakten och nätverks- och informationssäkerhetsdirektivet (NIS-direktivet) och, i förekommande fall, de regler om fri rörlighet som fastställs i fördraget och i EU-stadgan om de grundläggande rättigheterna.

III. 5G kommer att spela en nyckelroll i vår digitala ekonomi och vårt digitala samhälle under de kommande åren. Vi måste se till att våra 5G-nät är säkra och kan stå emot ökande it-hot och it-incidenter. Därför har kommissionen och medlemsstaterna inrättat en samordningsprocess, vars syfte är att fastställa och genomföra en omfattande säkerhetsram för 5G som består av en verktygslåda med de riskreducerande åtgärder som man enades om i januari 2020. Med hjälp av verktygslådan kan de stora risker som 5G-nät utsätts för, däribland kriminell hackning, spionerі och sabotage, hanteras på ett ändamålsenligt och samordnat sätt. Även om arbetet fortfarande pågår i vissa medlemsstater har de allra flesta medlemsstaterna redan förstärkt säkerhetskraven för 5G-nät med hjälp av EU:s verktygslåda, eller håller på att göra det.

VII. EU:s verktygslåda utgör en ram som främjar enhetlighet på den inre marknaden, samtidigt som medlemsstaternas ansvar för den nationella säkerheten respekteras.

När det gäller medlemsstaternas strategi för högriskleverantörer anser kommissionen att det inte går att göra en slutlig bedömning förrän mer information är tillgänglig.

Under genomförandets gång samarbetar kommissionen med medlemsstaterna i samarbetsgruppen för nät- och informationssäkerhet för att främja anpassning och konvergens mellan nationella strategier.

IX. Första strecksatsen – Kommissionen godtar rekommendationen.

Andra strecksatsen – Kommissionen godtar rekommendationen.

Tredje strecksatsen – Kommissionen godtar rekommendationen.

Kommissionen kommer att genomföra bedömningen med beaktande av nationella befogenheter.

INLEDNING

04. Kommissionen erkänner att det finns säkerhetsrisker med 5G, men påpekar att 5G-nätteknik och 5G-standarder också kan medföra säkerhetsförbättringar jämfört med tidigare nätgenerationer.

IAKTTAGELSER

30. Även om 4G redan kan hantera ett brett tjänsteutbud bör 5G utgöra ett ”språng framåt”, dvs. en stor förändring jämfört med 4G. Den största utmaningen är därför övergången från 4G till 5G i hela EU. Risken för en digital klyfta finns alltid, men avsikten är att prioritera hanteringen av denna risk i policyprogrammet *En färdväg för det digitala decenniet* vad gäller utvecklingskurvan mot 5G-målet om 100 % täckning av alla befolkade områden senast 2030 och därigenom stödja medlemsstaternas åtgärder på detta område, särskilt när det gäller tillgången på landsbygden.

32. Observationsorganet *5G Observatory* har varit en tillförlitlig källa att använda för övervakning av utbyggnaden av 5G både i och utanför EU, även om informationen varit bristfällig i vissa fall. Kommissionens avdelningar förväntar sig att ha mer aktuell information tillgänglig med den nya uppdragstagaren.

Kommissionens gemensamma svar på punkterna 48 och 49:

Kommissionen anser att valet av instrument (rekommendation) och strategin att samarbeta med medlemsstaterna för att identifiera risker och riskreducerande åtgärder är det lämpligaste sättet att hantera 5G-säkerhetsrisker på ett snabbt, ändamålsenligt och samordnat sätt.

Anledningen till att kommissionen valde en rekommendation och att samarbeta med medlemsstaterna för att identifiera risker och riskreducerande åtgärder var att detta är ett komplext ämne som omfattar både medlemsstaternas och EU:s behörighetsområden och har en betydande nationell säkerhetsdimension. Dessutom beaktade kommissionen att medlemsstaterna har mycket olika nationella omständigheter (marknadsstruktur, cybersäkerhetskapacitet, underrättelser om hot osv.).

EU:s verktygslåda är ett flexibelt riskbaserat instrument för att hantera säkerhetsutmaningar, som gjorde det möjligt att i tid hantera 5G-säkerhetsfrågor på ett effektivt sätt.

I sitt meddelande *Säker 5G-utbyggnad i EU – Genomförande av EU:s verktygslåda* från januari 2020 angav kommissionen att den skulle stödja genomförandet av verktygslådans åtgärder med avseende på säkerhetskraven, i synnerhet vad gäller relevanta föreskrifter inom de europeiska bestämmelserna om elektronisk kommunikation, och ta ställning till mervärdet av eventuella genomförandeakter med tekniska och organisatoriska säkerhetsåtgärder som kompletterar de nationella bestämmelserna och gör de säkerhetsåtgärder som åläggs operatörerna mer ändamålsenliga och konsekventa.

Kommissionens gemensamma svar på punkterna 51 och 52:

I samband med översynen av kommissionens rekommendation i december 2020 intervjuade kommissionen behöriga myndigheter i alla medlemsstater. De beskrev Europas samordnade åtgärder för 5G-säkerhet som lägliga, ändamålsenliga och proportionella. Samarbetet mellan nationella myndigheter, kommissionen, Enisa och andra relevanta intressenter ansågs vara ett lämpligt sätt att hantera denna komplexa fråga. Strategin ansågs göra det möjligt att i tid fastställa gemensamma mål och metoder, samtidigt som medlemsstaterna kunde anpassa åtgärderna till sina nationella förhållanden.

I EU:s verktygslåda och den lägesrapport som offentliggjordes av samarbetsgruppen för nät- och informationssäkerhet i juli 2020 rekommenderas att man fastställer genomförandeplaner och/eller övergångsperioder för de operatörer som för närvarande använder utrustning från högriskleverantörer eller redan hade ingått avtal med högriskleverantörer innan EU:s verktygslåda antogs (t.ex. genom beaktande av cyklerna för uppgradering av utrustning, i synnerhet migreringen från nät som inte är självständiga 5G-nät till självständiga sådana).

55. Kommissionen noterar revisionsrättens iakttagelser.

I syfte att främja deras tillämpning har de kriterier i verktygslådan som används för att bedöma högriskleverantörer varit föremål för talrika utbyten mellan behöriga nationella myndigheter i samarbetsgruppen för nät- och informationssäkerhet sedan man enades om EU:s verktygslåda.

56. I EU:s verktygslåda rekommenderas att de riskfaktorer som anges i EU:s samordnade riskbedömning samt landsspecifik information (t.ex. hotbedömningar från nationella säkerhetstjänster) beaktas vid bedömningen av leverantörers riskprofil.

61. Leverantörens förmåga att säkerställa tillgången är ett av de kriterier som rekommenderas i EU:s verktygslåda för att bedöma leverantörernas riskprofil. Förmågan att säkerställa tillgången skulle också kunna påverkas av eventuella handelssanktioner mot en viss leverantör, vilket nämns i riskscenariot om ”beroende” i EU:s samordnade riskbedömning.

Kommissionens gemensamma svar på punkterna 70 och 73:

Kommissionen och medlemsstaterna utbyter detaljerad information om genomförandet av verktygslådan på nationell nivå inom samarbetsgruppen för nät- och informationssäkerhet. Offentliggörande av icke-offentlig information är medlemsstaternas ansvar.

Kommissionens gemensamma svar på punkterna 74–76 samt ruta 5:

EU:s verktygslåda utgör en ram som främjar enhetlighet på den inre marknaden, samtidigt som medlemsstaternas ansvar för den nationella säkerheten respekteras.

När det gäller medlemsstaternas strategi för högriskleverantörer anser kommissionen att det inte går att göra en slutlig bedömning förrän mer information är tillgänglig.

Under genomförandets gång samarbetar kommissionen med medlemsstaterna i samarbetsgruppen för nät- och informationssäkerhet för att främja anpassning och konvergens mellan nationella strategier.

SLUTSATSER OCH REKOMMENDATIONER

81. En snabb och säker utbyggnad av 5G-nät är en viktig prioritering för kommissionen. Att skydda 5G-nätverk mot it-hot handlar om att bedöma och minska hot och risker. Medlemsstaterna har gemensamt identifierat och bedömt dessa hot och risker med stöd av kommissionen och Enisa. På grundval av detta arbete har sedan en rad omfattande åtgärder fastställts för att minska riskerna. Även om arbetet fortfarande pågår i vissa medlemsstater har de allra flesta medlemsstaterna redan förstärkt säkerhetskraven för 5G-nät med hjälp av EU:s verktygslåda, eller håller på att göra det.

EU:s verktygslåda utgör en omfattande ram för hantering av 5G-säkerhetsrisker.

83. 5G utgör ett ”språng framåt”, dvs. en stor förändring jämfört med 4G. Den största chansen att undvika den digitala klyftan ligger därför i övergången från 4G till 5G i hela EU.

5G-specifikationer omfattar en hel rad prestationsindikatorer, särskilt i fråga om vertikala användningsfall. De kan bland annat omfatta pålitlighetskrav, instansiering av tjänsternas hastighet, flexibilitet i genomförandet och säkerhetsnivåer.

Rekommendation 1 – Främja en jämn och snabb utbyggnad av 5G-näten inom EU

a) Kommissionen godtar rekommendationen.

Kommissionen ska tillsammans med medlemsstaterna utveckla en gemensam definition av den förväntade tjänstekvaliteten för 5G-näten. Inom ramen för det digitala decenniet och enligt förslaget till beslut om inrättande av 2030-policyprogrammet ”En färdväg för det digitala decenniet” har kommissionen för avsikt att samarbeta med medlemsstaterna om en gemensam strategi för kvaliteten på 5G-tjänster i EU, bland annat vad gäller jämförbarheten av mätningar och övervakningsdata.

Tjänstekvalitet omfattar inte bara hastighet och latens, utan även många andra prestationsindikatorer, främst sådana som rör vertikala användningsfall.

Kommissionen har för avsikt att samarbeta med medlemsstaterna för att fastställa sådana mätningar samt årligen genomföra kontroller och rekommendera policyer, åtgärder och insatser för att uppnå full 5G-täckning senast 2030.

Under det digitala policyprogrammet kommer det att etableras stabila styrformer i form av en mekanism för uppföljning och samarbete som säkerställer framsteg mot policyprogrammets mål, inklusive utbyggnad av 5G-nät, och rekommenderar medlemsstaterna korrigerande åtgärder.

b) Kommissionen godtar rekommendationen.

c) Kommissionen godtar rekommendationen.

Rekommendation 2 – Främja en samordnad strategi för 5G-säkerhet bland medlemsstaterna

a) Kommissionen godtar rekommendationen.

Kommissionen kommer att tillsammans med medlemsstaterna bedöma behovet av ytterligare insatser eller stöd, till exempel i form av vägledning om vissa aspekter av EU:s verktygslåda.

b) Kommissionen godtar rekommendationen.

Övervakningen och rapporteringen kommer att utföras av kommissionen i nära samarbete med medlemsstaterna och Enisa.

c) Kommissionen godtar rekommendationen.

Rekommendation 3 – Övervaka medlemsstaternas strategier för 5G-säkerhet och bedöma hur skillnaderna påverkar den inre marknadens funktion

a) Kommissionen godtar rekommendationen.

b) Kommissionen godtar rekommendationen.

Kommissionen kommer att genomföra bedömningen med beaktande av nationella befogenheter.

Enligt EU:s verktygslåda är det medlemsstaterna som beslutar om den exakta omfattningen av relevanta begränsningar och/eller uteslutningar när så krävs när det gäller nyckeltillgångar som definieras som kritiska och känsliga i EU:s samordnade riskbedömning (t.ex. stomnätsfunktioner, nätförvaltnings- och orkestreringsfunktioner samt accessnätsfunktioner) i syfte att effektivt minska de identifierade riskerna. I besluten beaktas även de nationella underrättelsetjänsternas hotbedömningar. Medlemsstaterna har rätt att vidta åtgärder som rör nationell säkerhet, inbegripet att tillämpa begränsningar på eller utesluta högriskleverantörer.