Kriterierna för att fastställa högriskleverantörer

Kriterierna för att fastställa högriskleverantörer verkställer den strategiska åtgärden (SM03) i EU:s 5G-verktygslåda: "Bedömning av leverantörers riskprofil och begränsningar som tillämpas på leverantörer som anses utgöra hög risk – inklusive nödvändig exkludering för att effektivt reducera riskerna – när det gäller nyckeltillgångar".

Detta kriterium stöder 244 a § i gällande lag om tjänster inom elektronisk kommunikation, där det föreskrivs om utrustning som används i kommunikationsnätets kritiska delar. Syftet med paragrafen är att säkerställa att det inte finns utrustning i kommunikationsnätets kritiska delar som äventyrar den nationella säkerheten eller försvaret. Bedömningen av om den nationella säkerheten och försvaret äventyras baseras på bedömningar från inrikes-, utrikes- och försvarsförvaltningen. Kriterierna för tillverkare med hög risk stöder en eventuell bedömning av om den nationella säkerheten och försvaret äventyras.

I samarbetet mellan säkerhetsmyndigheterna (Traficom, Försvarsmakten, Skyddspolisen) har man bedömt att tillverkare med hög risk i Finland kan anses vara sådana aktörer för vilka följande kriterier framträder, vilka även har identifierats i EU:s gemensamma riskbedömning och av Finlands centrala referensländer:

- Risk som gäller tillverkarens hemland och reglering:
  - Lagstiftningen i tillverkarens hemland, det vill säga ett tredjeland (utanför Nato/EU/EES-området), eller företagets huvudsakliga etableringsställe, följer inte de rättsliga och demokratiska principer som antagits inom EU, och i landet kan man inte tillämpa principer för informationssäkerhets- och dataskyddslagstiftning på motsvarande sätt som inom EU.
  - I tillverkarens hemland och på grund av den lagstiftning som gäller där kan man inte tillämpa säkerhets-, informationssäkerhets-, dataskydds- eller utlämningsavtal.
  - Tillverkaren (inklusive personalen) kan utsättas för påtryckningar från ett sådant tredjeland eller exponeras för extern påverkan.
  - Tillverkaren, inklusive ägarstrukturen, har nära kopplingar till sådana tredjeländers (icke-EU-länders) regeringar, myndigheter eller statligt ägda företag.
- Risk för fientliga cyberoperationer eller åtgärder som äventyrar den nationella säkerheten mot Finland eller dess allierade:
  - Tillverkaren har nära kopplingar till stater eller organisationer som utför fientliga cyberoperationer, informationspåverkan eller andra åtgärder som äventyrar den nationella säkerheten mot Finland eller dess allierade.
- Risk som gäller tillverkarens leveranssäkerhet och leveranskedja:
  - Tillverkarens förmåga att leverera utrustning eller tjänster som uppfyller standarder vid förändringar i verksamhetsmiljön.
  - Tillverkarens transparens i cybersäkerhetspraxis samt tidigare historik när det gäller att åtgärda kända sårbarheter och fel.
  - Tillverkarens förmåga och vilja att hantera risker i sin leveranskedja eller logistiska kedja vid förändringar i verksamhetsmiljön tillsammans med underleverantörer.

Utöver de nämnda kriterierna kan identifieringen av en tillverkare med hög risk även omfatta andra kriterier som kan framträda särskilt i bedömningar av äventyrande av nationell säkerhet i andra fall än de som gäller kommunikationsnätens säkerhet.