NESAS: een belangrijke stap richting veilige ICT-netwerken

[intro]
NESAS (Network Equipment Security Assurance Scheme) is een gestandaardiseerd beoordelingsmechanisme voor cyberbeveiliging dat is ontwikkeld door GSMA, het internationale samenwerkingsverband van de mobiele industrie, en telecomkoepel 3GPP. NESAS biedt een gestandaardiseerde veiligheidsbeoordeling van de apparatuur. De nieuwe, uniforme beveiligingseisen zijn belangrijk bij de uitrol van 5G.

[broodtekst]
Op 14 oktober 2020 vond het door BTG georganiseerde webinar “Veiligheid van ICT-netwerken waarborgen via certificeringsmodel NESAS” plaats. Petra Claessen, ceo BTG/TGG deed de aftrap en gaf vervolgens het woord aan de moderator van het webinar Peter Rake, 5Groningen. Jon France is namens GSMA de openingsspreker. Hij vertelt dat de beveiligingstesten van 3GPP zijn gebruikt om de veiligheid te beoordelen. De twee belangrijkste uitgangspunten voor het NESAS-certificeringsmodel zijn een ‘process audit’, die fabrikanten handvatten bieden voor het ontwikkelen van veilige producten en ‘process evolutions.’ Deze laatste zien erop toe dat producten daadwerkelijk aan de gestelde veiligheidseisen voldoen. De producten worden zowel beoordeeld door een auditteam als door testlabs.

Veiligheidsnormen
De aanleiding om een uniforme beveiligingsstandaard te ontwikkelen is veelzijdig, constateert France. Ten eerste de technische ontwikkelingen. “De complexiteit van en het aantal netwerkfuncties neemt hand-over-hand toe. Cybersecurity staat in de spotlights. Toezichthouders en overheden maken zich zorgen over het beveiligingsniveau van netwerken. Het NESAS-model kan worden gebruikt voor het objectief definiëren van veiligheidseisen.” Vanuit de industrie is behoefte aan een consistent pakket van eisen qua veiligheidsnormen en aan een wereldwijd toepasbare standaard. Fabrikanten kunnen deze meenemen bij de ontwikkeling van nieuwe producten. Voor netwerkbeheerders en andere afnemers biedt de NESAS-norm een handvat bij de beoordeling van producten, als onderdeel van de producteisen.

Gegarandeerd startniveau
Het verhaal van Jaap Meijer, Cyber Security Officer van Huawei Nederland focust op het belang van NESAS voor netwerkleveranciers en sluit naadloos aan bij het betoog van France. “NESAS geeft inzicht hoe we producten moeten ontwikkelen en welke belangrijke veiligheidsvereisten aan het systeem worden gesteld. Het probleem met algemene veiligheidscriteria, die niet zijn toegesneden op de telecommarkt, is dat ze innovaties vertragen. NESAS verkort de time-to-market van nieuwe producten met drie tot zes maanden en de ontwikkelkosten zijn lager.”

NESAS omvat 20 beoordelingscategorieën, definieert beveiligingseisen en een toetsingskader voor 5G-productontwikkeling en productlevenscyclusprocessen. Bovendien gebruikt het beveiligingstesten van 3GPP om de veiligheid van netwerkapparatuur te beoordelen.

De vereisten zijn op maat afgestemd op het telecomnetwerk, constateert Meijer. “Er ontstaat een certificeringsmechanisme. Het is een universele standaard die voor de hele industrie geldt. Dat maakt het makkelijker om het beveiligingsniveau van aanbieders te vergelijken. Klanten hebben een gegarandeerd startniveau qua beveiliging van de producten. Er is sprake van een universele standaard die meetbaar, zichtbaar en vergelijkbaar is.” NESAS verkleint het veiligheidsrisico van producten voor klanten. “Het is een gezamenlijk veiligheidsraamwerk waar alle partijen uit de telecomindustrie bij betrokken zijn geweest.

Security by design
Jacob Groote, directeur 5G bij KPN juicht de introductie van NESAS toe. “Voor KPN is veiligheid hét belangrijkste aspect van het eigen telecomnetwerk. Iedereen moet ons netwerk kunnen vertrouwen. We volgen de richtlijnen van de overheid en zijn transparant over ons veiligheidsbeleid. Dit veiligheidsbeleid is vastgelegd in de KPN Security Policy en is een openbaar document dat voor eenieder toegankelijk is. NESAS is belangrijk voor overheden, netwerkbeheerders, leveranciers en het grote publiek. Het biedt de zekerheid dat het veiligheidsniveau van het netwerk op orde is.” KPN doet er alles aan om het telecomnetwerk zo betrouwbaar mogelijk te maken. Ook qua veiligheid. Bij 5G is veiligheid nadrukkelijk onderdeel van het ontwerp. “Het is veel meer security by design, maar je bent nooit klaar, zo voegt hij hier direct ook een belangrijke waarschuwing aan toe: “Certificering is één. De juiste procedures volgen hoort daarbovenop. De risico’s vinden ook plaats in de operationele procedures. Hoe ga je om met beveiligingsbugs en het onderhoud?”

Samenwerken
Toezichthouders willen goed beveiligde telecomnetwerken. In Nederland heeft het ministerie van Economische Zaken en Klimaat in juli 2020 een voorlopige versie van de uitvoeringswet cyberbeveiligingsverordening ter consultatie gepubliceerd. Joris den Bruinen, directeur van The Hague Security Delta benadrukt dat veiligheidscertificaten, toezicht en standaarden in lijn moeten zijn met de cybersecurityvereisten. NESAS is geen garantie dat netwerken geen kwetsbaarheden meer vertonen. Het is geen aanpak voor een eind-tot-eind veiligheid of een vervanging van de veiligheidseisen van netwerkproviders of overheden. “Beveiliging is niet een eenmalig, maar voortdurend proces” en BTG geeft aan om vanuit haar rol de contacten hiervoor leggen naar de gebruikers en naar de solutions partners. “Juist in co-creatie en volgens het triple helix model, kunnen we samen ook succesvol in dit traject zijn” aldus Claessen namens BTG.

Jon France van GSMA benadrukt in zijn reactie dat NESAS vooral een van de bouwstenen is in de cybersecuritymuur. Jaap Meijer van Huawei wijst erop dat ook aan de operationele kant ‘checks & balances’ nodig zijn. “Ook op dat vlak kunnen fouten plaatsvinden.” Jacob Groote van KPN benadrukt dat je als industrie moet samenwerken. “Je moet vooruitdenken: wat zijn de risico’s van de toekomst?” Hij wijst ook naar de gebruikers en maakt een vergelijking met de Covid-19-pandemie. “Als iedereen zich aan de afspraken houdt, wordt het moeilijk voor het virus om zich te verspreiden. Hetzelfde geldt voor virussen in de cyberwereld. We waarschuwen klanten dat hun apparatuur kwetsbaar is. Je kunt communiceren, maar de klant moet ook acteren.”

[streamer]

“Het NESAS-model kan worden gebruikt voor het objectief definiëren van veiligheidseisen”