Nota van inlichtingen 3

Aanbesteding: I&D Persoonsgebonden Telefonie (DIG-18628)
Datum: 18 augustus 2026

Vraag nr.	Betreft	Vraag	Antwoord
1.	Beschikbaarheids norm koppeling centrale telefonieplatform – PSTN (Bijlage 9 eis 3 en 4 & Bijlage 12 7.1))	Wij begrijpen het belang dat de aanbestedende dienst waarde hecht aan een hoge (technische) beschikbaarheid en continuïteit van de telefoniedienst. Voor de volledige end-to-end dienstverlening, inclusief de onderliggende componenten en onze eigen infrastructuur, kunnen wij contractueel een beschikbaarheid van 99,90% op jaarbasis garanderen. De technische beschikbaarheid wordt daarnaast geborgd door een redundante inrichting van onze infrastructuur. De Direct Routing-koppeling is redundant en active-active uitgevoerd. Bij uitval van een component wordt het verkeer waar de redundante inrichting daarin voorziet automatisch via de beschikbare infrastructuur afgehandeld. Hierdoor leidt een verstoring van een afzonderlijke component niet zonder meer tot onbeschikbaarheid van de telefoniedienst en kan herstel plaatsvinden terwijl de dienstverlening actief blijft. Daarnaast monitoren wij onze infrastructuur en dienstverlening proactief, zodat verstoringen vroegtijdig worden gedetecteerd en herstel direct kan worden ingezet. Gelet op deze technische en operationele borging van de beschikbaarheid verzoeken wij de aanbestedende dienst de in eis 3 en 4 gevraagde beschikbaarheid van 99,95% te wijzigen naar 99,90%.	Opdrachtgever gaat akkoord met beschikbaarheidspercentage van 99,90%. Essentie van de eis is de gegarandeerde beschikbaarheid van een actieve fall-back voorziening (redundante verbinding) bij uitval van een component in de primaire keten.
2.	Pen-test	Wij begrijpen en onderschrijven de doelstelling van Opdrachtgever om digitale weerbaarheid en kwetsbaarheidsbeheer adequaat te borgen. Als aanbieder van elektronische communicatienetwerken en -diensten dragen wij op grond van artikel 11a.1 van de Telecommunicatiewet een eigen verantwoordelijkheid voor de beveiliging en continuïteit van onze netwerken en diensten. Onze dienstverlening maakt gebruik van infrastructuur en platformcomponenten die niet uitsluitend voor Opdrachtgever worden ingezet. Actieve penetratietests kunnen, afhankelijk van scope en testmethodiek, gevolgen hebben voor de integriteit, beveiliging en beschikbaarheid van deze infrastructuur en daarmee ook voor andere klantomgevingen. Vanuit onze verantwoordelijkheid dienen dergelijke tests daarom gecontroleerd en binnen vooraf vastgestelde technische en operationele kaders plaats te vinden. Dit sluit aan bij de NCSC-richtlijnen voor het uitvoeren van securitytests, waarin onder meer het vooraf bepalen van doel, scope, testmethodiek en testomgeving en het voorkomen van ongewenste verstoring centraal staan. Ons verzoek blijft daarom om aan te sluiten bij de reeds opgenomen verplichting dat Opdrachtnemer minimaal jaarlijks penetratietests en kwetsbaarheidsscans laat uitvoeren door daartoe door Opdrachtnemer geselecteerde externe, deskundige partijen. Opdrachtnemer verstrekt Opdrachtgever daarbij op verzoek een samenvatting van de relevante resultaten van de uitgevoerde penetratietest(s). Om die reden achten wij het niet mogelijk dat Opdrachtgever zelfstandig of door een door haar ingeschakelde derde, actieve penetratietests laat uitvoeren op de door Opdrachtnemer gebruikte infrastructuur, platformen en voorzieningen. Partijen stemmen tijdens de contractering tussen de securityafdelingen van Opdrachtgever en Opdrachtnemer nader af over de wijze waarop invulling wordt gegeven aan de informatiebehoefte en de wijze waarop inzicht wordt geboden in de beveiliging van de dienstverlening. Deze afstemming vindt plaats binnen de voor de dienstverlening geldende beveiligings-, continuïteits- en operationele uitgangspunten van Opdrachtnemer. Kan Opdrachtgever bevestigen dat zij hiermee instemt en de betreffende eis dienovereenkomstig aanpassen? Indien Opdrachtgever hier niet mee instemt, verzoeken wij Opdrachtgever gemotiveerd toe te lichten waarom deze binnen de sector gebruikelijke werkwijze voor het uitvoeren van penetratietests niet toereikend wordt geacht.	Opdrachtgever heeft begrip voor het standpunt van gegadigde. Opdrachtgever wil echter de mogelijkheid behouden om, indien daar aanleiding toe is, zelfstandig onafhankelijk onderzoek of een pentest uit te (laten) voeren op de dienstverlening die door opdrachtnemer aan opdrachtgever wordt geleverd. Reden hiertoe is o.a. dat telefonie steeds meer deel uitmaakt van het IT-landschap waardoor het aanvalsoppervlak wordt vergroot. Recht op onafhankelijk onderzoek is volgens opdrachtgever daarom goed verdedigbaar. Opdrachtgever gaat wel akkoord met aan het onderzoek voorafgaande afstemming met opdrachtnemer over scope, planning en methode. De scope van het onderzoek wordt daarbij beperkt tot de dienstverlening die voor opdrachtgever van toepassing is en het onderzoek mag geen verstoring veroorzaken voor andere klanten van opdrachtnemer en/of gedeelde infrastructuur.