Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Minimale eisen continuïteitsplan

Als aanbieder van openbare telecommunicatienetwerken en/of –diensten in Nederland moet u zorgen voor de continuïteit en beschikbaarheid van uw dienstverlening. Dit is in uw eigen belang, maar ook in het belang van uw klanten. Zij rekenen op het ongestoord gebruik van uw diensten. U moet maatregelen nemen om de continuïteit hiervan te waarborgen. Mocht zich ondanks de genomen maatregelen onverhoopt binnen uw organisatie een incident voordoen waardoor uw diensten toch onderbroken worden, dan bent u verplicht dit te melden aan Agentschap Telecom. Hiervoor is het loket Meldplicht Telecomwet ingericht.

Beide verplichtingen zijn vastgelegd in hoofdstuk 11a Continuïteit van de Telecommunicatiewet (Tw) en gelden voor alle aanbieders van openbare telecommunicatienetwerken en/of -diensten. Aanbieders zijn verplicht zich ter registratie aan te melden bij de ACM. Ook aanbieders die dit hebben nagelaten, vallen binnen de scope van de wet. Biedt u uw diensten alleen binnen een besloten groep aan, dan gelden deze verplichtingen niet voor u. Ook in dat geval heeft u echter de morele verplichting aangaande de continuïteit in relatie met de maatschappelijke en/of economische impact van de besloten dienstverlening.

Wetgeving
De zorg- en meldplicht is gespecificeerd in hoofdstuk 11a Continuïteit Tw, te weten de artikelen 11a.1 en 11a.2.

Meldplicht continuïteit
In artikel 11a.2 is de meldplicht continuïteit vastgelegd. Deze meldplicht verplicht aanbieders van openbare telecommunicatienetwerken en -diensten om: een inbreuk op de veiligheid en/of een verlies van integriteit, waardoor de continuïteit van openbare telecommunicatienetwerken en/of –diensten in belangrijke mate werd onderbroken, te melden bij het loket Meldplicht Telecomwet.

Toezicht op hoofdstuk 11a Tw
Naast het loket Meldplicht Telecomwet heeft Agentschap Telecom een toezichthoudende taak waar het de naleving van hoofdstuk 11a betreft. Naast correctief toezicht op naleving van de meldplicht gaat het hierbij ook om preventief toezicht op de zorgplicht continuïteit. Met zorgplicht continuïteit wordt uw plicht om te zorgen voor continuïteit van openbare telecommunicatienetwerken en/of -diensten bedoeld.

Overzicht van maatregelen
In principe is de zorgplicht continuïteit een eigen aangelegenheid van de aanbieder. Toch heeft de wetgever een minimumniveau van continuïteitsmaatregelen voorgeschreven. Zo verwacht de wetgever in het kader van de zorgplicht continuïteit dat u een continuïteitsplan opstelt. Agentschap Telecom kan dit plan ter inzage opvragen. Hierin geeft u een overzicht van de door u genomen maatregelen om de continuïteit van uw dienstverlening te waarborgen. Het minimumniveau is vastgelegd in het besluit: ’continuïteit openbare elektronische communicatienetwerken en -diensten’ en in hoofdstuk 11a Tw.

Passende en noodzakelijke maatregelen
Om ervoor te zorgen dat uw netwerken continu beschikbaar zijn en blijven en om risico's voor de veiligheid en de integriteit van uw netwerken en diensten op een adequate en kwalitatief juiste wijze te beheersen, is het noodzakelijk dat u passende maatregelen neemt. Het betreft hier maatregelen die aansluiten bij de, in de markt, algemeen aanvaarde standaarden c.q. normen ten behoeve van continuïteit management. Agentschap Telecom hanteert bij het toezicht op de Europese wet- en regelgeving internationale kwaliteitstandaarden: de NEN-ISO normen. Deze worden hieronder toegelicht. Deze passende preventieve maatregelen dienen in ieder geval die maatregelen te zijn welke in hieronder "Concrete minimale eisen continuïteitsplan" worden genoemd.

Bent u aanbieder van openbare telefoniediensten, dan geldt de verplichting om in het geval van een technische storing of uitval van het elektriciteitsnetwerk alle noodzakelijke maatregelen te treffen. Dit zijn alle maatregelen die getroffen worden om de beschikbaarheid van de openbare telefoondiensten over de openbare telecommunicatienetwerken, in geval van een technische storing of uitval van het elektriciteitsnetwerk zo volledig mogelijk te waarborgen.

Zowel de passende als de noodzakelijke maatregelen moeten zijn opgenomen in een continuïteitsplan. Het vastgestelde en procedureel ingerichte continuïteitsplan dient ten minste alle hieronder genoemde onderwerpen te bevatten.
Om tot een concrete interpretatie van deze begrippen en verplichtingen te komen zal Agentschap Telecom met de markt de dialoog zoeken.

De genomen continuïteitsmaatregelen door de aanbieder moeten voldoen aan ten minste het minimumniveau en moeten worden beschreven in een continuïteitsplan. Per onderwerp geeft u aan welke daadwerkelijke passende technische en organisatorische maatregels zijn getroffen. Zo vraagt het agentschap u de risico's met betrekking tot de veiligheid en integriteit van uw netwerken en diensten met regelmaat te evalueren en ook de op basis daarvan genomen maatregelen te verwerken in het continuïteitsplan. Ook vragen wij u een persoon aan te stellen die verantwoordelijk is voor continuïteit van uw openbare telecommunicatienetwerken en/of diensten. Deze medewerker zal fungeren als contactpersoon voor Agentschap Telecom bij toezichtcontacten en in geval van eventuele incidenten.

Concrete minimale eisen continuïteitsplan

I Continuïteitseisen algemeen

- Aanbieders beschrijven in het continuïteitsplan welke 'passende' technische en organisatorische maatregelen zij hebben genomen om de risico's voor de veiligheid en integriteit van hun netwerken en diensten te beheersen.
- Aanbieders van openbare telefoondiensten en aanbieders van openbare elektronische communicatie netwerken waarover openbare telefoondiensten worden aangeboden beschrijven in het continuïteitsplan welke 'noodzakelijke' maatregelen zij kunnen nemen om, in geval van een technische storing of uitval van het elektriciteitsnetwerk, de beschikbaarheid van hun telefoondienst te garanderen.
- Aanbieders beschrijven in het continuïteitsplan hoe men het systeem van voortdurende verbetering van de continuïteit beheert en beheerst en licht dit toe.

Binnen deze systematiek worden alle 'passende en noodzakelijke' technische en organisatorische maatregelen als bedoeld in de continuïteitswetgeving in het plan geadresseerd, uitgevoerd, gecontroleerd en geëvalueerd.

II Continuïteitseisen t.a.v. personeel

- De aanbieder dient te vermelden welke kundige functionaris binnen de organisatie verantwoordelijk is voor het beheren en beheersen van het systeem, waarbij gestreefd wordt naar voortdurende verbetering van de continuïteit.
- De aanbieder noteert in het continuïteitsplan de contactgegevens van deze functionaris(en).

III Fysieke beveiliging en beveiliging van de omgeving

- De aanbieder legt bevoegde personen, betrokken bij, de voor de veiligheid en integriteit van het netwerk relevante processen, een geheimhoudingsverplichting op. Aanbieders lichten dit proces inclusief de selectiecriteria toe in het continuïteitsplan.
- De aanbieder licht in het continuïteitsplan toe op welke manier hij zorg draagt voor een deugdelijke beveiliging van zijn netwerk of dienst waardoor er slechts toegang wordt verschaft aan daartoe gemachtigde personen. Met name waar het:
    1. de fysieke toegang tot gebouwen of faciliteiten betreft en
    2. de logische toegang tot informatie en informatie verwerkende systemen betreft die van belang zijn voor de veiligheid of integriteit van netwerk of dienst.
- De aanbieder dient in het continuïteitsplan te beschrijven dat slechts de daartoe bevoegde personen op de hoogte zijn van de inhoud van het continuïteitsplan en/of toegang hebben tot het continuïteitsplan.

IV Melden van een inbreuk op de veiligheid of een verlies van integriteit

- De aanbieder dient in het continuïteitsplan te beschrijven welke functionaris, in geval van een inbreuk op de veiligheid of een verlies van integriteit, verantwoordelijk is voor het doen van een melding. Deze, in Nederland gevestigde, functionaris treedt tevens op als eerste aanspreekpunt van de aanbieder voor het meldpunt.
- De aanbieder dient het proces van melding van een incident in het continuïteitsplan te beschrijven. Vooralsnog betekent dit dat de melding in ieder geval: het tijdstip van aanvang van het incident; de aard en de omvang van het incident; op welk netwerk en/of bij welke dienst het incident heeft plaatsgevonden en een prognose van de hersteltijd moet bevatten.

V Risicobeheer voor de veiligheid en de integriteit

- De aanbieder inventariseert, beoordeelt en evalueert regelmatig de risico´s voor de veiligheid en de integriteit van zijn netwerken en diensten. Hij verwerkt de resultaten hiervan in het continuïteitsplan.
- Majeure incidenten worden in een apart hoofdstuk binnen het continuïteitsplan beschreven. Deze beschrijving bevat in ieder geval: het tijdstip van aanvang van het incident; de aard en de omvang van het incident; op welk netwerk en bij welke dienst het incident heeft plaatsgevonden en de hersteltijd van het onderhavige incident. De beschrijving van het incident wordt aangevuld met het pakket aan maatregelen dat de aanbieder heeft genomen om het risico op herhaling te minimaliseren.

Internationale standaarden: leidraad voor kwaliteitsverbetering continuïteit
Agentschap Telecom hanteert bij het uitoefenen van het toezicht op de zorgplicht continuïteit een normenkader, dat is gebaseerd op verschillende internationale kwaliteitsstandaarden, met als doelen:

- het verbeteren van de continuïteit van uw bedrijf;
- het borgen van de continuïteit van uw openbare telecommunicatienetwerken en/of diensten;
- een betere voorbereiding op calamiteiten en incidenten waar het uw ICT kapitaal betreft.

Ook willen we hiermee bereiken dat u oog heeft voor een steeds betere beheersing van de risico's die eventueel afbreuk kunnen doen aan de continuïteit van uw telecommunicatienetwerk en/of dienst.

Tot slot verwachten wij dat u zorg draagt voor continue verbetering van uw beheerfunctie in relatie tot zowel uw communicatienetwerk als -dienst. In dit licht kunt u achtereenvolgens de volgende internationale kwaliteitstandaarden, de NEN-ISO normen, als leidraad voor kwaliteit hanteren:

1. Corporate governance of information technology (CGIT)
2. Business Continuity Management Systems (BCMS)
3. Risk Management (RM)
4. ICT readiness for Business Continuity (IRBC) en
5. ICT Service Management System (SMS)

- De NEN-ISO 38500 norm (CGIT) geeft concrete aanbevelingen voor goed bestuur van ICT (Informatie Communicatie Technologie).
- De NEN-ISO 22301 norm (BCMS) geeft concrete aanbevelingen om uw continuïteit in algemene zin te adresseren en steeds verder te verbeteren.
- De NEN-ISO 31000 norm (RM) geeft concrete aanbevelingen met betrekking tot het beheren van risico´s welke eventueel afbreuk kunnen doen aan de continuïteit van uw communicatienetwerk en/of -dienst en het beheer steeds verder te verbeteren.
- De NEN-ISO 27031 norm (IRBC) geeft concrete aanbevelingen om uw ICT kapitaal in gereedheid te brengen zodat de continuïteit van uw communicatie netwerk en –dienst steeds beter voorbereid is waar het incidenten en calamiteiten betreft.
- De NEN-ISO 20000 norm (SMS) geeft concrete aanbevelingen voor de inrichting van kwalitatief goed beheer van uw ICT, inclusief incident– en problem management zodat de continuïteit van uw communicatienetwerk en –dienst steeds verder verbetert.

Consistente keuze
Het spreekt voor zich dat het u vrij staat te kiezen voor ongeacht welk kwaliteit- en/of managementsysteem of norm bij de inrichting van de zorgplicht continuïteit. Echter, is het wel zaak dat u een eenduidige keuze maakt en deze keuze op consistente wijze gestalte geeft.