Enterprise Business Unit Solutions

Contractuele dienstbeschrijving Cloud Mail Security-dienst

Datum 06/09/2018
Sensitivity **Unrestricted**

Inhoud

1. Inleiding

Cloud Mail Security (hierna 'de Dienst') beschermt SMTP-compatibele e-mailsystemen tegen interne en externe veiligheidsrisico's zoals in dit document beschreven. De Dienst wordt 'in de cloud' aangeboden, wat betekent dat de Klant geen forse hardware- of software-investeringen hoeft te doen. Alle inkomende e-mailverkeer of mailboxen binnen het kader van deze Overeenkomst wordt gestuurd naar een op internet gebaseerd beveiligingsplatform, dankzij een verandering in het MX-record van het Klantdomein. Daar wordt het gecleand volgens vooraf gedefinieerde parameters vooraleer het e-mailverkeer op de infrastructuur van de Klant toekomt. Eventueel kan ook uitgaande e-mail naar het internetgebaseerde veiligheidsplatform worden doorgestuurd, waar het kan worden geanalyseerd om te zien of het strookt met de geconfigureerde veiligheidspolicy. Hiertoe moet de Dienst het verzendende IP-adres of de gehoste e-maildienst laten registreren. De basisfuncties van de Dienst hebben als doel de organisatie van de Klant te beschermen tegen spam en malware, de Klant de mogelijkheid te bieden zijn e-mailverkeer te versleutelen en de Klant rapporteringstools ter beschikking te stellen. Afhankelijk van de gekozen functionele opties kan de Klant dit aanvullen met diverse geavanceerde functies.

De Dienst is beschikbaar in twee Formules: Reactive Care en Full Care. Ze verschillen in termen van het aantal activiteiten die Proximus uitvoert in de domeinen on-lineadministratie, configuratie en ondersteuning. De Full Care-formule is beschikbaar vanaf 25 mailboxen.

De Dienst is gebaseerd op de volgende infrastructuurelementen, Oplossingselementen genaamd.

- Platform
- Administration Portal
- Spam Quarantine Portal
- Synchronisatietool

Het hoofdstuk 'Overzicht van de Dienst' beschrijft de functionaliteit en supportactiviteitstypes die in de Dienst kunnen zijn begrepen en specificeert de inhoud van elke supportactiviteit die Proximus per Oplossingselement levert.

De werking van de Dienst is in detail beschreven in het hoofdstuk 'Functionele dienstbeschrijving', terwijl de supportdiensten (Assist and Care Services) geleverd aan de Klant tijdens de implementatie- en operationele fasen respectievelijk beschreven zijn in de hoofdstukken 'Implementatiefase' en 'Operationele fase'.

2. Overzicht van de Dienst

De tabellen hieronder geven de functionaliteiten en activiteitstypes weer die in de Dienst kunnen zijn begrepen (ook Dienstcomponenten genoemd). De Dienstcomponenten zijn:

- ofwel standaard in de Dienst opgenomen ('STD');
- ofwel optioneel ('OPT') en moeten door de Klant worden geselecteerd;
- ofwel het voorwerp van een afzonderlijk contract ('AC').

Zodra de Dienstcomponenten zijn geselecteerd via de Bestelbon, wordt het toepassingsveld van deze Overeenkomst gedefinieerd. In geval van toevoeging of wijziging van Dienstcomponenten wordt een nieuwe Overeenkomst opgemaakt.

2.1 Functionele Dienst

In de tabel hieronder wordt een overzicht gegeven van de functionaliteiten die in de basisdienst en in de opties zijn begrepen. Verdere uitleg van deze details wordt gegeven in het hoofdstuk 'Functionele dienstbeschrijving'.

Dienstcomponenten	Detail	Reactive Care	Full Care
Basic-dienst	Antimalware Antispam Opportunistische TLS-versleuteling Adresregistratie Traceren van berichten Rapportering Spam Quarantine Portal voor de eindgebruiker en meldingen Disclaimer management	STD	STD
Voorkomen van gegevensverlies (Data Loss Prevention, DLP)	Bescherming van e-mailgegevens Controleren van afbeeldingen in de e-mail Geforceerde TLS-versleuteling Op de Basic Policy gebaseerde versleuteling Controles voor impersonatie van e-mails	OPT	OPT
Geavanceerde bescherming tegen bedreigingen (ATP)	Op de cloud gebaseerde sandboxing Bescherming van de kliktijd van de URL Gedetailleerde malwarerapportering	OPT	OPT
Add-On: integratie van Active Directory	Synchronisatie van Active Directory-gebruikers en groepen	OPT	OPT

2.2 Assist and Care Services

De support geleverd door Proximus tijdens de implementatie- en operationele fase is van toepassing op de Oplossingselementen die per type activiteit in de onderstaande tabel zijn opgelijst. De Dienst omvat geen activiteiten met betrekking tot andere Oplossingselementen.

Dienstcomponent	Betrokken Oplossingselementen	Reactive Care	Full Care
Assist			
Assist-dienst	Platform Spam Quarantine Portal Synchronisatietool Administration Portal	STD	STD
Optionele Assist-dienst	Platform	OPT	
Toegang tot de Service Desk	Alle oplossingselementen	STD	STD
Behandeling van Incidenten			
Diagnose op afstand	Alle Oplossingselementen	STD	STD
Interventie op afstand	Alle Oplossingselementen	STD	STD
Herstelling van de configuratie	Administration Portal Spam Quarantine Portal	STD	N.v.t.
Configuratiebeheer			
Configuratiebeheer met leesrechten voor de Klant	Administration Portal	N.v.t.	STD
Configuratiebeheer met specifieke toegangsrechten	Spam Quarantine Portal Synchronisatietool	N.v.t.	OPT
Configuratiebeheer zonder toegangsrechten	Platform	N.v.t.	STD/OPT
Back-up van de configuratie	Administration Portal Spam Quarantine Portal	STD	STD
Wijzigingsbeheer			

Koning Albert II-laan 27, B-1030 Brussel, België,
BTW BE 0202.239.951, RPR Brussel, BE50 0001 7100 3118 BPOTBEB1.

Standaardwijzigingen	Administration Portal Spam Quarantine Portal	N.v.t.	AO
Gepersonaliseerde wijzigingen	Administration Portal Spam Quarantine Portal	N.v.t.	AO
Updates en Upgrades	Alle Oplossingselementen	STD	STD
Monitoring			
Monitoring van de Dienstbeschikbaarheid	Alle Oplossingselementen	N.v.t.	STD
Rapportering			
Rapportering van de Dienstbeschikbaarheid	Platform Administration Portal Spam Quarantine Portal	N.v.t.	STD

3. Functionele dienstbeschrijving

De Dienst is gebaseerd op een gehost beveiligingsplatform (ook 'Platform' genoemd), dat inkomende en eventueel uitgaande e-mailberichten van de e-mailadressen in het kader van de Overeenkomst (d.w.z. de e-mailadressen die zijn vermeld in de Valideringslijst hieronder) filtert om de infrastructuur van de Klant te helpen beschermen tegen veiligheidsrisico's zoals beschreven in dit document.

De parameters van de functionaliteiten van de Dienst worden geconfigureerd via de Administration Portal die ter beschikking van de Klant wordt gesteld. In het geval van de Reactive Care-dienstformule configureert de Klant deze parameters zelf in de Administration Portal, terwijl in het geval van de Full Care-dienstformule Proximus deze parameters configureert in de Administration Portal voor de Klant op basis van het formulier 'Vereisten voor de technische configuratie' en de bijhorende vragen van de Klant. De Klant erkent en stemt ermee in dat hij als enige verantwoordelijk is om de configuratie te kiezen en dat de keuze gebeurt conform zijn policy's en procedures.

De Dienst ondersteunt e-maildiensten van meerdere leveranciers, zoals Microsoft Exchange, Office 365, Google Apps, enz. De lijst met compatibiliteiten is beschikbaar op verzoek.

Dit hoofdstuk beschrijft de verschillende functionaliteiten die in de Dienst kunnen zijn begrepen, ongeacht de gekozen Dienstformule.

3.1 Basic-dienst

Koning Albert II-laan 27, B-1030 Brussel, België,
BTW BE 0202.239.951, RPR Brussel, BE50 0001 7100 3118 BPOTBEB1.

3.1.1 Antimalware

Deze functionaliteit is bedoeld om de Klant bescherming te bieden tegen gekende en ongekende malware die wordt verdeeld via URL's of bestanden en eventueel via de mailboxen van de Valideringslijst. De bescherming is een combinatie van verschillende technologieën, zoals heuristiek en reputation- en signature-based systemen.

De Administration Portal wordt gebruikt om de parameters van deze functionaliteit te configureren, die onder meer toelaat om:

- geïnfecteerde e-mails te verwijderen
- verdachte virussen proactief in quarantaine te plaatsen tot een signatuur/oplossing wordt vrijgegeven.
- automatische alarmen als melding naar de administrator en/of de Eindgebruikers te sturen
- e-mails vrij te maken naar het eerste adres van de oorspronkelijke lijst van ontvangers, naar een voorgedefinieerd e-mailadres of naar een alternatief adres dat de Klant had gevraagd.
- banners voor virussen te creëren om Eindgebruikers te informeren over het scannen van e-mails
- maximumvolumes voor e-mails vast te stellen

E-mails die standaard als malware worden beschouwd, worden in quarantaine geplaatst en daar gedurende 30 kalenderdagen bijgehouden. Bij de verstrijking van deze periode wordt de e-mail automatisch gewist.

3.1.2 Antispam

Deze functionaliteit biedt de Klant bescherming tegen spam, d.w.z. ongevraagde commerciële e-mail door inkomend en eventueel uitgaand e-mailverkeer van de mailboxen van de Valideringslijst te scannen.

Er wordt een multilaagbenadering toegepast, wat betekent dat de volgende technieken worden toegepast, zoals:

- Een privélijst van goedgekeurde verzenders samengesteld door de Klant of (met de goedkeuring van de Klant) zijn individuele Eindgebruikers.
- Een privélijst van geblokkeerde verzenders samengesteld door de Klant of (met de goedkeuring van de Klant) zijn individuele Eindgebruikers.
- Een aantal lijsten met publieke geblokkeerde verzenders.
- Een signature-based systeem.
- Symantec.clouds' SkepticTM heuristische detectie

E-mails die verdacht worden spam te zijn, kunnen het voorwerp zijn van diverse acties, naargelang de configuratie in de Administration Portal. Acties die worden gedefinieerd als het resultaat van een signature-based of heuristische detectie komen hierbij in de plaats van alle eventuele minder strenge acties die voordien werden toegewezen door een van de vorige methodes. Mogelijke acties zijn:

- e-mails afkomstig van verdachte zenders uitschakelen met behulp van reputatiefilters
- e-mails afkomstig van verdachte zenders in quarantaine plaatsen met behulp van reputatiefilters
- e-mails afkomstig van geïdentificeerde spam uitschakelen
- e-mails afkomstig van geïdentificeerde spam in quarantaine plaatsen
- verdachte e-mails taggen in de 'subject'-lijn
- verdachte e-mails taggen in de header
- e-mail uit Spam Quarantine vrijgeven door de administrators
- e-mail uit Spam Quarantine vrijgeven door de Eindgebruikers

E-mails die ervan worden verdacht spam te zijn en die in quarantaine worden geplaatst, worden gewist zoals beschreven in de Spam Quarantine Portal en de rubriek 'meldingen' hieronder.

3.1.3 Opportunistische TLS-versleuteling

Deze functionaliteit is bedoeld om de Klant toe te laten op veilige wijze e-mails buiten zijn organisatie uit te wisselen d.m.v. het SMTP over TLS-versleutelingsprotocol, d.w.z. via een versleuteld kanaal. De partnerorganisatie(s) waarmee de Klant e-mails over een versleuteld kanaal wil versturen, worden geïdentificeerd in de Administration Portal. Met deze partnerorganisaties wordt een veilig privé-e-mailnetwerk opgezet, dat gebruikmaakt van de authenticatiecertificaten die volledig door de Klant worden beheerd. Dit is enkel mogelijk als de mailserver van de partnerorganisatie TLS ondersteunt. In andere gevallen zal de e-mail in gewone tekst worden afgeleverd.

Daarnaast kan de Klant versleutelde e-mailcommunicatie ontvangen die opportunistisch wordt verstuurd door organisaties met mailservers die TLS ondersteunen.

Proximus vestigt de aandacht van de Klant op het feit dat met deze functionaliteit, de e-mail zelf niet wordt versleuteld, maar alleen het kanaal wordt versleuteld. Dit in tegenstelling tot de functionaliteit 'Versleuteling gebaseerd op de Basic Policy'.

3.1.4 Adresregistratie

Dankzij deze functionaliteit kan de Klant in de Administration Portal een lijst met geldige e-mailadressen van Eindgebruikers in de organsiatie uploaden. E-mails die naar niet-geregistreerde Eindgebruikers worden gestuurd, worden geblokkeerd. De zender zal een foutmelding '550 invalid recipient' ontvangen indien de e-mail geldig was, maar het adres incorrect was gevormd of verkeerd was gespeld.

De Klant aanvaardt om een lijst op te geven en bij te houden van geldige e-mailadressen die de Dienst mogen ontvangen (de 'Valideringslijst'). De Klant is verantwoordelijk om de Valideringslijst te controleren vooraleer de Dienst beschikbaar wordt en dit gedurende de looptijd van de Overeenkomst.

De Klant aanvaardt dat de Service Levels niet van toepassing zijn op e-mails die naar ongeldige adressen worden gestuurd of niet in de Valideringslijst zijn vermeld.

Voor alle duidelijkheid moeten Klanten die het Spam Quarantine-systeem gebruiken, een Valideringslijst bijhouden en de adresregistratiefunctie hebben geactiveerd. Indien de Klant deze Valideringslijst niet kan voorleggen en vraagt dat de adresregistratiefunctie wordt gedesactiveerd, zal Proximus elk van deze aanvragen geval per geval bekijken en behoudt het zich, geheel naar eigen goeddunken, het recht voor om vragen af te wijzen.

3.1.5 Traceren van berichten

Via de Track and Trace-zoekfunctie van de Administration Portal kan de Klant nagaan hoe specifieke e-mails door het Platform werden verwerkt. Deze functie versterkt details over de verschillende verwerkingsstappen, zoals de ontvangst van e-mail door het Platform, de acties die worden ondernomen m.b.t. de e-mail, de aflevering van de e-mail, enz. Er worden geen kopieën van de e-mails opgeslagen.

De Track and Trace-zoekfunctie is ideaal om individuele e-mails op te sporen, daar ze de Klant toelaat om een berg e-mails te doorzoeken om een specifieke e-mail te vinden. Enkel de e-mails die de voorbije 30 kalenderdagen werden behandeld, kunnen worden opgespoord.

De Track and Trace-functionaliteit is toegankelijk voor de Administrator, dit is Proximus in geval van de Full Care-formule en de Klant in geval van de Reactive Care-formule. Zo nodig kunnen bijkomende Eindgebruikers leesrechten krijgen i.v.m. de Track and Trace-functie.

3.1.6 Rapportering

Reporting dashboards zijn beschikbaar in de Administration Portal. De Dashboards tonen een selectie van statistische gegevens, zoals, maar niet beperkt tot:

- het aantal gescande mails
- het aantal e-mails dat als spam werd geïdentificeerd
- het aantal keer dat de policy inzake gegevensbescherming in werking werd gesteld (ingeval de optie DLP wordt besteld).

De statistische gegevens in deze dashboards kunnen worden getoond per domein of voor alle domeinen.

Daarnaast laat de Administration Portal de Klant toe om rapporten in de vorm van documenten op te vragen. De rapporten in documentformaat kunnen worden gegenereerd voor alle domeinen van de Klant of per individueel domein, maar niet per individuele mailbox. De rapporten zijn beschikbaar in verschillende formaten en kunnen zo worden gepland dat ze ook naar een aantal voorafbepaalde bestemmelingen worden gemaild. Specifiek zijn de volgende formaten beschikbaar:

- Grafische dashboards

- Samenvattende rapporten in .pdf, die grafieken, lijsten en tabellen omvatten, en ten hoogste één jaar teruggaan.

- Gedetailleerde rapporten in .csv, beperkt tot 500.000 rijen. Deze bieden een gedetailleerde loglijst van alle dienstactiviteit voor alle domeinen. De rapporteringsgevens hebben enkel betrekking op de laatste 30 kalenderdagen.

De rapporteringsgegevens blijven 12 maanden beschikbaar.

3.1.7 Spam Quarantine Portal voor de Eindgebruikers en meldingen

De Spam Quarantine Portal is een portaal waar geïntercepteerde e-mails die door de Dienst worden geïdentificeerd als spam of e-mails die gegevens of afbeeldingen bevatten die de Complianceregels van de Klant schenden, in quarantaine worden geplaatst.

In deze Spam Quarantine Portal voor de Eindgebruikers kan de Administrator van de organisatie van de Klant in quarantaine geplaatste mails bekijken, vrijgeven of wissen, geblokkeerde en gemachtigde zenders beheren, en instellingen en voorkeuren specificeren. De Administrator kan dit recht ook aan (sommige) Eindgebruikers verlenen voor de e-mails die naar het e-mailadres van de Eindgebruiker in kwestie worden gestuurd.

Afhankelijk van de configuratie kunnen Eindgebruikers een melding krijgen wanneer een e-mail in quarantaine is geplaatst.

E-mails worden gedurende 14 dagen in de Quarantine Portal bijgehouden, tenzij ze eerder worden gewist.

3.1.8 Disclaimer management

Een e-mail disclaimer is de tekst in de footer van een inkomende of uitgaande e-mail die via de Dienst passeert. Dankzij deze functionaliteit kunnen disclaimers worden geconfigureerd door middel van een combinatie van standaard en gepersonaliseerde e-maildisclaimers, voor inkomende en eventueel uitgaande e-mails van de e-mailaddressen van de Valideringslijst, op globaal, domein- en groepsniveau.

Proximus behoudt zich het recht voor om uitgaande e-mails te scannen als de Klant de Dienst configureert voor uitgaande e-mails. Er zal een standaard disclaimerboodschap worden toegepast op de e-mails die door de Dienst worden gescand vanaf het ogenblik dat de Dienst wordt geleverd.

Proximus behoudt zich het recht voor de standaard disclaimerboodschap te allen tijde te updaten. Dit mag niet worden beschouwd als een wijziging van de Overeenkomst.

3.2 Data Loss Prevention (preventie van dataverlies)

Wanneer ze wordt geselecteerd, biedt de Data Loss Prevention-optie de volgende functionaliteiten die bedoeld zijn om het risico op gegevensverlies te verminderen:

3.2.1 Bescherming van e-mailgegevens

Deze functionaliteit stelt de Klant in staat om een reeks regels te creëren, op basis waarvan inkomende en uitgaande e-mail wordt gefilterd op basis van de inhoud van de e-mail. Elke regel identificeert een specifiek formaat van e-mails (of bijlagen: Microsoft Office-documenten, pdf-documenten of tekstbestanden), waarvoor een voorgeschreven procedure moet worden gevolgd.

De Administration Portal wordt gebruikt om de toepasselijke regels en bijhorende acties die moeten worden genomen i.v.m. inkomende en eventueel uitgaande e-mails te configureren of aan te passen. Mogelijke acties zijn:

- verdachte e-mails blokkeren en wissen;
- (de header van) verdachte inkomende e-mail taggen
- een verdachte e-mail naar een gespecificeerde administrator doorsturen of kopiëren;
- bijlagen bij e-mails comprimeren;
- enkel inloggen op de statistieken van de management portal;
- de 'subject'-regel taggen.

3.2.2 Controleren van afbeeldingen in de e-mail

Deze functionaliteit biedt de Klant de mogelijkheid om ongepaste afbeeldingen in e-mails of bijlagen (Word-, Excel- en PowerPoint-bijlagen, met uitzondering van inhoud die onder de uitsluitende controle van de zender valt, zoals met een wachtwoord beschermde of versleutelde bestanden). Ze scant inkomende en uitgaande e-mail door gebruik te maken van methodes zoals:

- Lijsten met goedgekeurde zenders en ontvangers.

- Goedgekeurde handtekeningen voor afbeeldingen in een database van de Klant.
- De database van de globale Image Control community.
- De engine voor de Image Composition Analysis (ICA).

De Administration Portal wordt gebruikt om acties te configureren die moeten worden genomen op inkomende en eventueel uitgaande e-mails wanneer ongepaste afbeeldingen worden gedetecteerd. Mogelijke acties zijn:

- verdachte e-mail loggen;
- verdachte inkomende e-mails taggen in de header
- verdachte e-mail doorsturen of kopiëren naar een voorgedefinieerd e-mailadres;
- verdachte e-mail wissen;
- verdachte e-mails taggen in de 'subject'-lijn
- alarmmeldingen naar de zender/bedoelde ontvanger sturen

Deze functionaliteit heeft als doel ongepaste afbeeldingen, en in het bijzonder pornografische afbeeldingen, te detecteren. Merk op dat een 100%-detectiegraad van pornografische afbeeldingen niet verzekerd is en dat de definitie van wat al dan niet onder 'pornografische afbeelding' valt, subjectief is.

3.2.3 Geforceerde TLS-versleuteling

Met deze functionaliteit kunnen organisaties veilige links met hun businesspartners en/of met de Dienst creëren, waardoor alle onderling uitgewisselde e-mail kan worden versleuteld zonder bijkomende actie door de verzender. De inhoud van de boodschap blijft transparant voor zowel verzender als recipiënt.

Merk op dat, in tegenstelling tot opportunistische TLS-versleuteling, -e-mail niet wordt afgeleverd wanneer de mailserver van de business partner TLS niet ondersteunt, of indien de Dienst geen authenticatie verleent voor het certificaat dat de derde-ontvanger toont wanneer het domein gebruikmaakt van Sterke Validering. Niet-afgeleverde e-mail wordt teruggestuurd.

3.2.4 Op de Basic Policy gebaseerde versleuteling

Deze functionaliteit dient om e-mails en bijlagen te scannen en is bedoeld om automatisch de berichten zelf te versleutelen die zijn geïdentificeerd als gevoelige informatie bevattend. De versleuteling gebeurt vanaf het ogenblik dat het bericht door de Dienst passeert.

Dankzij deze Dienst kan de ontvanger zijn e-mail ontvangen via zijn mailbox of via een dedicated secure webportaal (dat niet tot de Administration Portal behoort). Deze veilige webportal kan door de ontvangers worden gebruikt om hun antwoorden te versturen of (optioneel) om nieuwe e-mails naar de Eindgebruikers te sturen.

Deze functionaliteit is onderworpen aan de volgende beperkingen:

• Het maximumaantal beveiligde uitgaande e-mails per Eindgebruiker per maand is 300 voor deze functionaliteit. Bij verzending naar meerdere ontvangers zal elk uniek adres worden geteld als een afzonderlijke beveiligde uitgaande e-mail. Als de Klant het toegestane aantal veilige uitgaande e-mails in

een bepaalde kalendermaand overtreft, behoudt Proximus zich het recht voor om de Klant voor het werkelijke verbruik te factureren.

- E-mails die via deze functionaliteit worden gerouteerd, zijn beperkt tot een maximumvolume van vijftig megabyte (50 MB), anders worden ze niet versleuteld.

- Indien wordt gebruikgemaakt van de Pull-encryptie met de functionaliteit Policy Based Encryption (Z) zullen e-mails standaard gedurende 90 kalenderdagen worden opgeslagen in de dedicated, veilige webportal vooraleer ze worden gewist. Deze e-mails kunnen worden geëxporteerd om door de Eindgebruiker lokaal te worden opgeslagen.

- De beschikbaarheid en de Latency Service Levels zijn niet van toepassing op de Policy Based Encryption.

3.2.4.1 E-Mail Impersonation Control (EIC)

Deze functionaliteit is bedoeld om de Klant te beschermen tegen frauduleuze e-mail en spearphishingberichten EIC checkt e-mails die binnenkomen op e-mailadressen van de Valideringslijst voor impersonatie met gebruikersnamen, beter bekend als 'spoofing'. In het bijzonder controleert EIC de legitimiteit van inkomende e-mail die kennelijk wordt verstuurd vanaf de domeinen van de organisatie van de Klant of vanaf de Eindgebruikers.

De Administration Portal wordt gebruikt om de acties te configureren die m.b.t. de e-mail worden genomen wanneer een verdachte impersonatie wordt vastgesteld. Mogelijke acties zijn:

- loggen
- de 'subject'-regel taggen
- in quarantaine plaatsen
- doorsturen naar Admin
- blokkeren en wissen

3.3 Advanced Threat Protection (ATP) (Geavanceerde bescherming tegen bedreigingen)

Wanneer ze wordt geselecteerd, biedt de optie Advanced Threat Protection de hieronder beschreven functionaliteiten;

3.3.1 Op de cloud gebaseerde sandboxing

Om te trachten de eigenschappen van potentiële malware in een onbekend bestand te detecteren, wordt een kopie van het bestand in een op de cloud gebaseerde sandbox gelanceerd. Daarna wordt typisch gedrag van Eindgebruikers binnen verschillende besturingssysteemomgevingen nagebootst. Indien nodig verschuift de sandbox de uitvoering van een virtuele naar een fysieke omgeving om malware bloot te leggen die 'virtual-machine-aware' is. Indien de verdachte malware inactief blijft in de sandboxomgeving, zal de sandbox ze blijven monitoren. Op die manier kan nadien worden vastgesteld of de malware later binnen de omgeving tracht te bewegen of met een controleserver of andere computer tracht te communiceren. De sandbox correleert de gegevens met de gegevens van het Symantec Global Intelligence Network om te bepalen of de bestanden kwaadaardig zijn. De Administrator Portal wordt

gebruikt om te bepalen hoe lang de e-mail wordt bijgehouden alvorens die te versturen, met een maximum van 20 minuten. Indien verdere analyse uitwijst dat een gedownload bestand malware bevat, kunnen maximaal vijf opgegeven e-mailadressen worden gemeld. Specifiek voor klanten die gebruikmaken van Office 365 is het in staat om e-mails die als kwaadaardig worden geïdentificeerd, na aflevering terug te sturen.

3.3.2 Click-Time URL Protection

Deze functionaliteit kan sommige URL's in e-mails die worden afgeleverd aan e-mailadressen van de Valideringslijst 'herschrijven' en er controles op uitvoeren. Het herschrijfproces stelt de Dienst in staat de toegang tot de URL te beheren om te verzekeren dat de bestemming onschadelijk is.

Elke URL die door Click-time URL Protection wordt herschreven wordt gecontroleerd telkens een Eindgebruiker erop klikt, om te verzekeren dat de URL-bestemming geen malware, phishing of spambedreigingen host. Heel wat herschreven URL's kunnen zo worden gecontroleerd en als vrij van bedreigingen worden geïdentificeerd. Een URL die voorheen was toegestaan, kan op een later tijdstip beginnen met malware, phishing of spam te hosten. Op dat ogenblik blokkeert de Click-time URL Protection-functie de toegang tot de URL en krijgt de Administration Portal een melding hierover.

3.3.3 Gedetaileerde rapportering van malware

Deze functionaliteit biedt de Klant een granulaire rapportering over binnenkomende veilige en kwaadaardige e-mails in de organisatie van de Klant. Deze rapporten zijn beschikbaar via de Administration Portal.

De verschafte rapporten omvatten 60+ datapunten, zoals:

- de bron-URL's van een aanval
- informatie i.v.m. een gerichte aanval
- de categorisering van de malware
- informatie i.v.m. verzender en ontvanger
- de detectiemethode
- gedetailleerde informatie i.v.m. file hashes
- de categorie van bedreiging
- de ernstgraad

De rapporteringsgegevens blijven 12 maanden beschikbaar.

3.4 Active Directory Synchronization

Wanneer ze wordt geselecteerd, biedt de Synchroniseringsoptie de Klant een tool om hem te helpen zijn directorybronnen gesynchroniseerd te houden met het Platform. De tool maakt een combinatie van de volgende synchronisatietypes mogelijk:

- Mailsynchronisatie om e-mailadressen te synchroniseren.
- Synchronisatie van Eindgebruikers om de identiteiten van Eindgebruikers, e-mailadressen of het lidmaatschap van een groep te synchroniseren,
- Groepsynchronisatie om de identiteiten van een groep te synchroniseren.

De synchronisatietool gidst de Klant doorheen een configuratieproces om de vereiste gegevens uit zijn directorysysteem te extraheren. Zodra het correct is geconfigureerd, kan het synchronisatieproces ofwel van de synchronisatietoolinterface of van de commandolijn worden gerund. Het proces kan zo worden gepland dat het automatisch opereert. De synchronisatietool kan ook e-mailmeldingen sturen om zijn resultaat te rapporteren telkens hij erom wordt gevraagd.

4. Implementatiefase

4.1 Bestelling

De Klant bestelt de Dienst door de desbetreffende Bestelbon behoorlijk ingevuld en ondertekend aan Proximus te bezorgen. Op deze Bestelbon dient de Klant onder andere het volgende te specificeren:

- De gekozen Dienstformule
- De gekozen opties
- Het aantal mailboxen dat moet worden beschermd
- Technische informatie (bv. IP-adres van mailservers, e-maildomein)
- Informatie i.v.m. het gevraagde quarantainemodel

Het document 'Vereisten voor de technische configuratie', dat van toepassing is op de Full Care-dienstformule, is bijgevoegd bij de Bestelbon.

Voor Wijzigingen waarbij een aanpassing van de Dienstvergoeding komt kijken, moet een nieuwe Bestelbon of een Addendum worden opgemaakt.

4.2 Activering en Assistentiediensten voor de Reactive Care-dienstformule

4.2.1 Activering

Zodra Proximus de behoorlijk ingevulde en ondertekende Bestelbon (met inbegrip van de bijlagen) heeft ontvangen, zal het met de implementatie van de Dienst starten.

Alleen Proximus (of zijn onderaannemers) mag de onderstaande implementatieactiviteiten uitvoeren. Alle implementatieactiviteiten worden uitgevoerd tijdens de Kantooruren, na de activering en conform de 'best practice'-policy. Proximus voert bij de implementatie van de Dienst de volgende activiteiten uit:

Standaard bestaat de implementatie van de Dienst uit:

- Activering van het Platform voor de bestelde domeinen met een maximum van 5, de antivirus- en antispamomgevingen worden standaard geactiveerd.
- Configuratie van de inkomende en, indien besteld, uitgaande e-mailroutes op het Platform;
- Aanmaak van 1 account op de Administration Portal en bezorgen van de relevante inloggevens aan de Klant;
- Overhandiging van de documentatie en de handleidingen i.v.m. de Dienst;
- Aanmaak van 1 administrator account op de Spam Quarantine Portal (indien geselecteerd op de Bestelbon). De juiste inloggegevens worden ter beschikking gesteld.
- Back-up van de configuratie van het Platform.
- Activering van de Dienst en terbeschikkingstelling van de Portal(s)

Zodra de Dienst is geactiveerd en aan de Klant de Portals i.v.m. de Dienst op het Platform zijn geleverd voor de e-maildomeinen die de Klant had gevraagd, zal de Dienst worden beschouwd als ter beschikking gesteld van de Klant.
Om alle misverstanden te vermijden, wijst Proximus de Klant erop dat de volgende activiteiten niet zijn inbegrepen bij de implementatie van de Dienst door Proximus, behalve indien uitdrukkelijk overeengekomen en gespecificeerd op de Bestelbon:

- Activering van het Platform voor meer dan 5 domeinnamen
- Configuratie van het platform De Klant is verantwoordelijk voor de configuratie van het Platform via de Administration Portal. Proximus vestigt de aandacht van de Klant op het feit dat het Service Level alleen van toepassing is wanneer de volgende 'best practices'-instellingen door de Klant zijn gedefinieerd:
    - de beide goedgekeurde-verzenderopties activeren en het aantal entry's op de lijst zo laag mogelijk houden
    - Spoofed sender detection activeren met SPF – Voor inkomende en uitgaande e-mail
    - DMARC activeren - voor inkomende en uitgaande e-mails
    - de beide geblokkeerde-verzenderlijsten activeren
    - gebruikmaken van de dynamische IP-blokkeringslijst
    - het ondertekeningssysteem activeren
    - 'skeptic heuristics' - predictive spam detection activeren
    - uitbreiding van de newsletter filter activeren
    - spoofed sender detection activeren met SPF – voor uitgaande e-mails
    - DMARC activeren - voor uitgaande e-mails
- De administrator kan zelf andere accounts voor zijn organisatie creëren en fijn afgestemde rollen aan deze andere accounts in de Administration Portal toewijzen.
- Opleiding
- Creatie van een veiligheidspolicy voor de Klant
- Zodra de administrator account aan de technisch contactpersoon van de Klant is overhandigd, is het de verantwoordelijkheid van de Klant om het wachtwoord te veranderen.
- Installatie en configuratie van de Active Directory Synchronization-tool, indien besteld.

4.2.2 Assistentiediensten

Indien de Klant de Assistentieoptie heeft besteld, zal Proximus de volgende implementatieactiviteiten uitvoeren, naast de implementatieactiviteiten die standaard zijn begrepen in de Reactive Care-dienstformule:

- Configuratie van de Administration Portal van de Klant waaronder, indien van toepassing, de DLP-, ATP- en/or AD-synchronisatiepolicy, Spam Manager, in overeenstemming met de veiligheidspolicy van de Klant;
- Proximus configureert het Platform niet alleen in overeenstemming met de veiligheidspolicy van de Klant, die hij heeft gecommuniceerd, maar ook met de volgende 'best practice'-instellingen:
  - de beide goedgekeurde-verzenderopties activeren en het aantal entry's op de lijst zo laag mogelijk houden
  - DMARC activeren - Enkel voor inkomende mails
  - de beide geblokkeerde-verzenderlijsten activeren
  - gebruikmaken van de dynamische IP-blokkeringslijst
  - het ondertekeningssysteem activeren
  - 'skeptic heuristics' - predictive spam detection activeren
  - uitbreiding van de newsletter filter activeren

Voor alle duidelijkheid: ook al heeft de Klant op deze optie ingetekend, toch blijft hij verantwoordelijk om de volgende 'best practice'-instellingen aan zijn kant te configureren (het Service Level is niet van toepassing als ze niet door de Klant zijn geconfigureerd):

- spoofed sender detection activeren met SPF – voor uitgaande e-mails
- DMARC activeren - voor uitgaande e-mails

4.3 Activering en Assistentiediensten voor de Full Care-dienstformule

Zodra Proximus de behoorlijk ingevulde en ondertekende Bestelbon (met inbegrip van de bijlagen) heeft ontvangen, zal het met de implementatie van de Dienst starten.

Alleen Proximus (of zijn onderaannemers) mag de onderstaande implementatieactiviteiten uitvoeren. Alle implementatieactiviteiten worden uitgevoerd tijdens de Kantooruren, na de activering en conform de 'best practice'-policy. Proximus voert bij de implementatie van de Dienst de volgende activiteiten uit:

De implementatie van de Dienst omvat:

- De activering van het Platform voor de bestelde domeinen met een maximum van 5. Proximus configureert het Platform in overeenstemming met de Technische configuratievereisten die bij de Bestelbon zijn gevoegd, de veiligheidspolicy van de Klant die tijdig aan de Klant wordt gecommuniceerd, en de volgende best practice-instellingen:
  - de beide goedgekeurde-verzenderopties activeren en het aantal entry's op de lijst zo laag mogelijk houden
  - DMARC activeren - Enkel voor inkomende mails
  - de beide geblokkeerde-verzenderlijsten activeren
  - gebruikmaken van de dynamische IP-blokkeringslijst
  - het ondertekeningssysteem activeren

- 'skeptic heuristics' - predictive spam detection activeren
- uitbreiding van de newsletter filter activeren
- Configuratie van de inkomende en, indien besteld, uitgaande e-mailroutes op het Platform;

- Aanmaak van 1 read-only account op de Administration Portal en bezorgen van de relevante inloggevens aan de Klant;

- Configuratie van de Administration Portal van de Klant waaronder, indien van toepassing, de DLP-, ATP- en/of AD-synchronisatiepolicy, Spam Manager, in overeenstemming met de veiligheidspolicy van de Klant;

- Overhandiging van de documentatie en de handleidingen i.v.m. de Dienst;
- Aanmaak van 1 administrator account op de Spam Quarantine Portal (indien geselecteerd op de Bestelbon). De juiste inloggegevens worden ter beschikking gesteld.
- Back-up van de configuratie van het Platform.
- De activering van de Dienst en terbeschikkingstelling van de Portal(s).

Zodra de Dienst is geactiveerd en aan de Klant de Portals i.v.m. de Dienst op het Platform zijn geleverd voor de e-maildomeinen die de Klant had gevraagd, zal de Dienst worden beschouwd als ter beschikking gesteld van de Klant.

Om alle misverstanden te vermijden, wijst Proximus de Klant erop dat de volgende activiteiten niet zijn inbegrepen bij de implementatie van de Dienst door Proximus, behalve indien uitdrukkelijk overeengekomen en gespecificeerd op de Bestelbon:

- De activering van het Platform voor meer dan 5 domeinnamen De activering en configuratie van bijkomende domeinen kan worden gevraagd via change credits.

- De configuratie van de volgende best practices-instellingen op het Platform (het Service Level is pas van toepassing zodra het door de Klant is geconfigureerd):
  - Spoofed sender detection activeren met SPF – Voor inkomende en uitgaande e-mail
  - DMARC activeren - uitgaande mail

- Opleiding
- Creatie van een veiligheidspolicy voor de Klant
- Zodra de administrator account aan de technisch contactpersoon van de Klant is overhandigd, is het de verantwoordelijkheid van de Klant om het wachtwoord te veranderen.

4.4 Aanvaarding

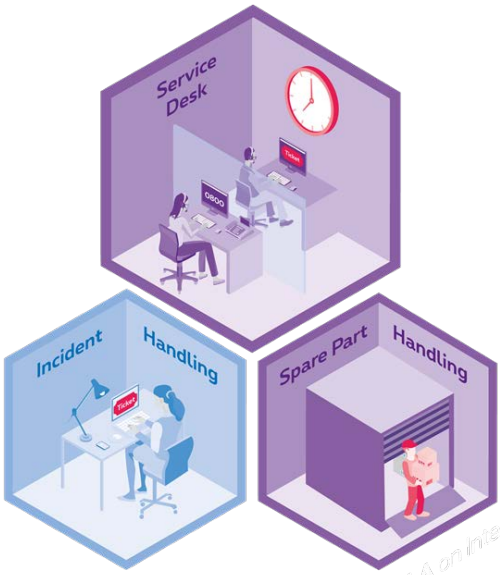
Aan het einde van de implementeringsfase zal Proximus de Klant verzoeken om de configuratie van het Platform te aanvaarden. In dit verband kan de Klant de configuratie van de implementatie checken via de Administration Portal.

De aanvaardingsprocedure staat beschreven in de Algemene voorwaarden voor professionele klanten (zie rubriek 'Configuratie en installatie').

5. Operationele fase

In dit hoofdstuk wordt de ondersteuning beschreven die Proximus verleent van bij de aanvaarding van de Dienst tot aan het einde van de Overeenkomst.

5.1 Reactive Care-dienstformule



Dit onderdeel is van toepassing wanneer de Klant de Reactive Care-dienstformule heeft gekozen. In het kader van deze Dienstformule geniet de Klant **Reactive Care**-ondersteuning, wat betekent dat Proximus de Klant reactieve ondersteuning biedt om de duur van Incidenten in te korten door middel van interventies en vervangingen.

5.1.1 Toegang tot de Service Desk

De Service Desk vormt de interface tussen de Klant en Proximus voor alle aspecten van de Dienst, inclusief ontvangst, opname, registratie en escalatie van Incidenten en andere aanvragen. De Service Desk kent de resources toe (eerste lijn, tweede lijn, experts) en communiceert regelmatig met de Klant.

Proximus verschaft de Klant gecentraliseerde toegang tot de Service Desk via de telefoon of een portal. De Service Desk is enkel toegankelijk voor gemachtigde vertegenwoordigers van de Klant (24x7), elke dag van het jaar, via:

Toegang tot de Service Desk	
Telefoonnummer:	0800 14888

Portal	https://www.proximus.be/login

De Klant stelt de Service Desk met het relevante referentienummer van de Overeenkomst in kwestie ter beschikking.

De Klant wordt op de hoogte gebracht van het feit dat oproepen van of naar de Service Desk van Proximus kunnen worden opgenomen om als bewijs te dienen bij de betwisting van een commerciële transactie. De Klant aanvaardt dat en geeft hiervoor zijn toestemming. Oproepen naar of van de Klantendienst mogen eveneens worden beluisterd of opgenomen met het oog op kwaliteitscontrole.

5.1.2 Behandeling van Incidenten

De activiteiten die Proximus in verband met Incidentbeheer uitvoert, hebben als doel om de gevolgen van een Incident op te lossen of te verminderen binnen het overeengekomen Service Level.

Activiteiten op afstand verwijst naar activiteiten die Proximus niet op de Site van de Klant uitvoert.

5.1.2.1 Diagnose op afstand

Het belangrijkste doel van de Diagnose op afstand is om de oorzaak na te gaan en de impact van het gerapporteerde Incident te valideren, via telefoon of e-mail. De Klant analyseert het Incident alvorens Proximus te contacteren.

Proximus zal de Klant helpen om om een aantal elementaire troubleshootingacties uit te voeren. In bepaalde gevallen zal aan de Klant worden gevraagd Proximus bijkomende informatie te verschaffen. Incidenten te wijten aan de configuratie van het Oplossingselement (zelfs van het betrokken Oplossingselement voor deze Dienstcomponent) worden door Proximus niet ondersteund.

Diagnose op afstand laat Proximus toe te bepalen welke acties nodig zijn om het Incident op te lossen.

5.1.2.2 Interventie op afstand

Indien een diagnose op afstand een Softwareprobleem op de Synchronisatietool te zien geeft, wordt een Interventie op afstand gestart, en wordt tegelijk met de leverancier nagegaan of er patches/updates beschikbaar zijn, die aan de Klant zullen worden aangeraden. De Klant staat in voor de installatie van de patches/Updates. De installatie van een patch/update is niet in de Dienstvergoeding begrepen. Incidenten te wijten aan de configuratie van de Oplossingselementen (zelfs van het betrokken Oplossingselement voor deze Dienstcomponent) worden door Proximus niet ondersteund.

Indien de Diagnose op afstand een probleem op het Platform en/of de Administration Portal en/of - de Spam Quarantine Portal te zien geeft, zal Proximus interventies op deze Oplossingelementen uitvoeren.

5.1.2.3 Herstelling van de configuratie

Naast de interventies op afstand zal Proximus, indien vereist voor het herstellen van de Dienst, trachten de Configuratie van het betrokken Oplossingselement te herstellen, op basis van de laatst beschikbare configuratieback-up die de Klant heeft uitgevoerd.

Proximus zal in dit verband alle redelijke inspanningen doen om regelmatig back-ups te maken van de configuratie van het betrokken Oplossingselement, en ze ter beschikking houden voor herstellingsdoeleinden in geval van een Incident. De eerste back-up wordt gemaakt tijdens de implementatiefase.

Tenzij schriftelijk anders overeengekomen tussen de Partijen wordt de uitvoering van de back-ups dagelijks ('s nachts) gepland. De back-up van de configuratie bestaat uit logs van configuratieveranderingen sinds de implementatiefase, metadata die beschikbaar zijn via de Administration tool en e-mails in quarantaine. De back-up van de configuratie die Proximus uitvoert omvat geen back-up van eender welke andere gegevens van de Klant.

5.1.3 Updates en Upgrades

Alleen Proximus bepaalt welke technische middelen noodzakelijk zijn voor de levering van de Dienst conform de Overeenkomst.

Proximus beslist om Updates/Upgrades naar eigen goeddunken te implementeren. Proximus is niet verplicht om elke Upgrade en Update die de leverancier ter beschikking stelt, te implementeren, of om het betrokken Oplossingselement uit te breiden. Gelet op het feit dat de Dienst is gebaseerd op een Cloud Platform, kan de Klant deze Updates/Upgrades niet weigeren.

5.1.4 Back-up van de configuratie

Proximus zal alle redelijke inspanningen doen om back-ups te maken van de configuratie van het betrokken Oplossingselement, en ze ter beschikking houden voor herstellingsdoeleinden in geval van een Incident.

De eerste back-up wordt gemaakt tijdens de implementatiefase.

Tenzij schriftelijk anders overeengekomen tussen de Partijen wordt de uitvoering van de back-ups dagelijks ('s nachts) gepland. De back-up van de configuratie bestaat uit logs van configuratieveranderingen sinds de implementatiefase, de data die beschikbaar zijn via de message tracing-functionaliteit en de e-mails in quarantaine.

De back-up van de configuratie die Proximus uitvoert omvat geen back-up van eender welke andere gegevens van de Klant.

5.2 Full Care-dienstformule

Dit onderdeel is van toepassing wanneer de Klant de Full Care-dienstformule heeft gekozen. De Klant geniet krachtens deze Dienstformule **Full Care**-ondersteuning, wat betekent dat Proximus de Klant reactieve ondersteuning biedt om de duur van Incidenten in te korten door middel van interventies, vervanging en beheer, monitoring en rapportering van de configuratie van de betrokken Oplossingselementen.

5.2.1 Toegang tot de Service Desk

De Service Desk vormt de interface tussen de Klant en Proximus voor alle aspecten van de Dienst, inclusief ontvangst, opname, registratie en escalatie van Incidenten en andere aanvragen. De Service Desk kent de resources toe (eerste lijn, tweede lijn, experts) en communiceert regelmatig met de Klant.

Proximus verschaft de Klant gecentraliseerde toegang tot de Service Desk via de telefoon of een portal. De Service Desk is enkel toegankelijk voor gemachtigde vertegenwoordigers van de Klant (24x7), elke dag van het jaar, via:

Toegang tot de Service Desk	
Telefoonnummer*	0800 14888
Portal	https://www.proximus.be/login

De Klant wordt op de hoogte gebracht van het feit dat oproepen van of naar de Service Desk van Proximus kunnen worden opgenomen om als bewijs te dienen bij de betwisting van een commerciële transactie. De Klant aanvaardt dat en geeft hiervoor zijn toestemming. Oproepen naar of van de Klantendienst mogen eveneens worden beluisterd of opgenomen met het oog op kwaliteitscontrole.

.

Koning Albert II-laan 27, B-1030 Brussel, België,
BTW BE 0202.239.951, RPR Brussel, BE50 0001 7100 3118 BPOTBEB1.

5.2.2 Behandeling van Incidenten

De activiteiten die Proximus in verband met Incidentbeheer uitvoert, hebben als doel om de gevolgen van een Incident op te lossen of te verminderen binnen het overeengekomen Service Level.

'Activiteiten op afstand' verwijst naar activiteiten die Proximus niet op de Site van de Klant uitvoert.

5.2.2.1 Diagnose op afstand

De hoofddoelstelling van Diagnose op afstand is het gemelde Incident te evalueren en analyseren, de oorzaak van het Incident te bepalen en de impact ervan te valideren - hetzij mondeling, hetzij door middel van toegang tot de omgeving van de Klant via een verbinding op afstand.

Proximus zal al het nodige doen om de oorzaak van de fout en de locatie van de falende component te bepalen. Dat omvat de identificatie van problemen met configuratiebestanden en performantieproblemen.

Diagnose op afstand laat Proximus toe te bepalen welke acties nodig zijn om het Incident op te lossen.

5.2.2.2 Interventie op afstand

Indien een alternatieve of permanente oplossing gevonden werd en op voorwaarde dat het incident op afstand kan worden opgelost, zal Proximus in nauwe samenwerking met de Klant een Interventie opstarten. De Klant wordt op regelmatige tijdstippen geïnformeerd over de vooruitgang.

Proximus herstelt de configuratie van het betrokken Oplossingselement op basis van de recentste beschikbare back-up.

5.2.3 Configuratiebeheer

De Configuratiebeheersactiviteiten die Proximus krachtens de Overeenkomst uitvoert, hebben, binnen de beperkingen opgesomd onder deze rubriek, de volgende doelstellingen:

- De configuratie van de betrokken Oplossingselementen beheren
- Een back-up maken van de configuratie van het betrokken Oplossingselement.
- Wijzigingen aan de configuratie van de betrokken Oplossingselementen implementeren
- De betrokken Software up-to-date houden

5.2.3.1 Toegangs- en configuratiebeheer

Deze rubriek bepaalt de toegangsbeheersrechten van Proximus en de Klant voor het betrokken Oplossingselement van deze Dienstcomponent.

Koning Albert II-laan 27, B-1030 Brussel, België,
BTW BE 0202.239.951, RPR Brussel, BE50 0001 7100 3118 BPOTBEB1.

5.2.3.1.1 Configuratiebeheer met leesrechten voor de Klant

Proximus verzamelt en documenteert up-to-date informatie over het Oplossingselement en maakt gebruik van geplande en in sommige gevallen automatische processen om het Oplossingselement up-to-date te houden.

Proximus voert acties uit om de goede werking van het Oplossingselement te verzekeren. Proximus gebruikt hiertoe een beveiligd centraal beheersplatform met toegangsrechten. Alle platformactiviteiten worden opgenomen om een snellere troubleshooting toe te laten.

Proximus is houder van alle beheersrechten voor het Oplossingselement in naam van de Klant, zelfs indien dit Oplossingselement eigendom is van de Klant. De Klant heeft Read Access-rechten voor de betrokken Oplossingselementen. De gemachtigde vertegenwoordigers van de Klant hebben toegang tot deze configuratie van het Oplossingselement via hetzelfde beveiligde en centrale beheersplatform met leesrechten.

5.2.3.1.2 Configuratiebeheer met specifieke toegangsrechten

Proximus verzamelt en documenteert up-to-date informatie over het Oplossingselement en maakt gebruik van geplande en in sommige gevallen automatische processen om het Oplossingselement up-to-date te houden.

Proximus voert acties uit om de goede werking van het betrokken Oplossingselement te verzekeren. Proximus gebruikt hiertoe een beveiligd centraal beheersplatform met toegangsrechten. Alle platformactiviteiten worden opgenomen om een snellere troubleshooting toe te laten.

Proximus is, in naam van de Klant, houder van alle administratorrechten op het betrokken Oplossingselement, ook indien de Klant eigenaar is van het Oplossingselement. De Klant heeft specifieke toegangsrechten om beperkte wijzigingen door te voeren. De gemachtigde vertegenwoordigers van de Klant hebben toegang tot deze configuratie van het Oplossingselement via hetzelfde beveiligde en centrale beheersplatform met beperkte rechten.

De Klant heeft het recht uitsluitend de volgende wijzigingen door te voeren in de betrokken Oplossingselementen:

- Accounts aanmaken
- Accountgroepen aanmaken
- Aliassen aanmaken
- Toegang krijgen tot de verschillende accounts
- Accounts wissen

Proximus kan niet aansprakelijk worden gesteld voor de gevolgen van wijzigingen die werden aangebracht door de Klant of door derden.

5.2.3.1.3 Configuratiebeheer zonder toegangsrechten

Proximus verzamelt en documenteert up-to-date informatie over het betrokken Oplossingselement en maakt gebruik van geplande en in sommige gevallen automatische processen om het Oplossingselement up-to-date te houden.

Proximus voert acties uit om de goede werking van het betrokken Oplossingselement te verzekeren. Proximus gebruikt hiertoe een beveiligd centraal beheersplatform met toegangsrechten. Alle platformactiviteiten worden opgenomen om een snellere troubleshooting toe te laten.

Proximus is houder van alle beheersrechten voor het betrokken Oplossingselement in naam van de Klant, zelfs indien dit Oplossingselement eigendom is van de Klant. De Klant heeft geen toegangsrechten noch beheersrechten en is niet gemachtigd om Wijzigingen aan te brengen aan het Oplossingselement of de interfaces.

5.2.3.2 Back-up van de configuratie

Proximus zal alle redelijke inspanningen doen om back-ups te maken van de configuratie van het betrokken Oplossingselement, en ze ter beschikking houden voor herstellingsdoeleinden in geval van een Incident.

De eerste back-up wordt gemaakt tijdens de implementatiefase.

Tenzij schriftelijk anders overeengekomen tussen de Partijen wordt de uitvoering van de back-ups dagelijks ('s nachts) gepland. De back-up van de configuratie bestaat uit logs van configuratieveranderingen sinds de implementatiefase, de data die beschikbaar zijn via de message tracing-functionaliteit en de e-mails in quarantaine.

De back-up van de configuratie die Proximus uitvoert omvat geen back-up van eender welke andere gegevens van de Klant.

5.2.3.3 Wijzigingsbeheer

Wijzigingsbeheer geeft de Klant de mogelijkheid om wijzigingen aan de configuratie van het Oplossingselement aan te vragen tijdens de Overeenkomst. Deze wijzigingen hebben geen impact op de terugkerende Dienstvergoeding.

Er zijn twee types wijzigingen: Standaardwijzigingen (Standard Changes) en Gepersonaliseerde wijzigingen (Custom Changes). Om deze wijzigingen aan te vragen moet de Klant over een afzonderlijke Overeenkomst voor Wijzigingsbeheer beschikken.

Voor veranderingen waarbij een aanpassing van de Dienstvergoeding komt kijken, moet een nieuwe Bestelbon of een Bijlage worden opgemaakt.

5.2.3.4 Updates en Upgrades

Alleen Proximus bepaalt welke technische middelen noodzakelijk zijn voor de levering van de Dienst conform de Overeenkomst.

Proximus beslist om Updates/Upgrades naar eigen goeddunken te implementeren. Proximus is niet verplicht om elke Upgrade en Update die de leverancier ter beschikking stelt, te implementeren, of om het betrokken Oplossingselement uit te breiden. Gelet op het feit dat de Dienst is gebaseerd op een Cloud Platform, kan de Klant deze Updates/Upgrades niet weigeren.

5.2.4 Monitoring

De monitoringactiviteiten die Proximus krachtens deze Overeenkomst uitvoert, laten Proximus toe de klok rond statusinformatie over de betrokken Oplossingselementen te verzamelen. Wanneer zich een relevant evenement (zoals hieronder beschreven) voordoet, zal Proximus de Incidentbeheersactiviteiten opstarten. Klanten worden op de hoogte gebracht door de creatie van een Incidentticket.

Proximus voert krachtens de Overeenkomst de volgende monitoringactiviteiten uit.

5.2.4.1 Monitoring van de Dienstbeschikbaarheid

Het centrale monitoringplatform controleert de beschikbaarheid van de betrokken Dienst. De controles van de beschikbaarheid van de Dienst bestaan onder meer uit een controle of de desbetreffende applicaties of processen operationeel zijn.

Als problemen met de Dienstbeschikbaarheid worden gedetecteerd, worden Incidentbeheersactiviteiten opgestart.

5.2.5 Rapportering

Proximus verschaft de Klant rapporten op basis van de informatie verzameld via de uitgevoerde monitoringactiviteiten in het kader van deze Overeenkomst. De Klant kan de status van de relevante parameters bekijken via de link vermeld in de documentatie van de Dienst.

Proximus verschaft de volgende rapporten in het kader van de Overeenkomst:

5.2.5.1 Rapportering van de Dienstbeschikbaarheid

Dit biedt een rapportering op basis van de Monitoring van de Dienstbeschikbaarheid.

6. Service Levels (dienstverleningsniveaus)

Dit onderdeel beschrijft de toepasselijke Service Levels. De Service Levels omvatten Service Level Objectives (SLO) en Service Level Agreements (SLA). Ze worden beschreven in de onderstaande tabellen.

6.1 Toepassingsgebied

Deze Service Levels zijn toepasselijk indien de Dienst werd geactiveerd en de inloggegevens werden ontvangen, binnen de ondervermelde Dienstroosters.

De Service Levels zullen enkel van toepassing zijn op de Dienst beschreven in dit document en op Incidenten waarvoor Proximus verantwoordelijk is.

Zijn ook uitgesloten van de berekening van het Service Level (toepassing van het 'stop clock'-principe):

- Incidenten, vertragingen of voorvallen die Proximus beletten om de Dienst te leveren door een fout van de Klant, gevallen van overmacht, of een fout van een derde;
- de tijd buiten het Dienstrooster, en
- e-mails die niet door de Dienst zijn gekomen als de Klant niet de nodige stappen heeft ondernomen om te verzekeren dat hij enkel uitgaande e-mail van de Dienst zal aanvaarden, en
- inkomende of uitgaande e-mails die initieel werden gestuurd naar de Dienst die meer dan 500 ontvangers per SMTP-sessie bevat, en
- geplande werken (waaronder onderbrekingen voor onderhoud).
- Klanten die bediend worden op gelijk welke Tower die als Bulk Cluster Tower wordt aangeduid (d.w.z. twee of meer load balanced servers in twee of meer locaties);
- alle eventuele inkomende of uitgaande e-mails voor e-mailadressen die niet in de Valideringslijst zijn begrepen, en
- Indien de best practices-instellingen, die door de Klant moeten worden geïmplementeerd zoals gedefinieerd in het hoofdstuk Implementatiefase, niet werden gedefinieerd of niet werden aangehouden gedurende de looptijd van de Overeenkomst (zie ook Bijlage 1). Dit geldt voor alle elementen van het Service Level.

Er zijn geen Service Levels van toepassing voor Support op aanvraag.

6.2 SLO en SLA

De SLO definieert een middelenverbintenis. Een inbreuk op deze SLO kan daarom niet worden beschouwd als een ernstige inbreuk. In geval van een inbreuk kan geen aanspraak worden gemaakt op Dienstkredieten.

De SLA definieert een resultaatsverbintenis. In geval van een inbreuk heeft de Klant recht op de in de onderstaande tabel opgenomen Dienstkredieten van Proximus. Tenzij de Klant een Dienstbeheersovereenkomst heeft ondertekend moet de Klant deze Dienstkredieten zelf opvragen aangezien ze niet proactief door Proximus worden toegekend.

Om een Dienstkrediet te ontvangen moet de Klant de inbreuk op het Service Level schriftelijk aan Proximus melden binnen vijf werkdagen volgend op het einde van de kalendermaand waarin de vermeende inbreuk op het Service Level zich heeft voorgedaan. Deze Dienstkredieten zijn het enige verhaal van de Klant indien een SLA niet wordt nageleefd.

De Klant komt niet in aanmerking voor Dienstkredieten als (1) de Klant nalaat om zijn Proximus-facturen i.v.m. deze Overeenkomst of een ander contract te betalen of als (2) de Klant in overtreding is met de Overeenkomst gedurende de tijd van het Incident of het voorval. Als de Overeenkomst verstrijkt of wordt beëindigd vóór het uitgeven van het Dienstkrediet, zal het Dienstkrediet nietig worden op de datum van verstrijking of beëindiging van de Overeenkomst.

6.3 Dienstroosters

Service Levels zijn van toepassing binnen het volgende Dienstrooster.

Het Dienstrooster is het tijdskader waarbinnen Incidentbeheersactiviteiten worden uitgevoerd.

Naam Dienstrooster	*Afkorting*	*Van toepassing op*	*Dienstroosteruren*
24*7	*24*7*	*Alle Oplossingselementen*	*24*7*

6.3.1 Implementatievenster voor Standaardwijzigingen

Het Implementatievenster voor Standaardwijzigingen is het rooster waarbinnen Standaardwijzigingen in het kader van deze Dienst zullen worden geïmplementeerd. Het Implementatievenster voor Standaardwijzigingen is:

Standaarddiensturen	SDU	*Maandag-vrijdag 8 u - 18 u*

6.4 Incidentprioriteit

Als de Klant een Incident detecteert, kan hij de Service Desk contacteren. De Service Desk zal de Incidentprioriteit toekennen op basis van de impact van het Incident.

Prioriteitsgraden	
P1*	Dienst volledig onderbroken (*)

Koning Albert II-laan 27, B-1030 Brussel, België,
BTW BE 0202.239.951, RPR Brussel, BE50 0001 7100 3118 BPOTBEB1.

P2	Dienst ernstig verstoord (kritieke bedrijfsfuncties) of back-up actief
P3	Beperkte impact (bedrijfsprocessen blijven functioneren)
P4	Geen impact/aanvraag voor informatie

Indien na de diagnose blijkt dat de impact van het Incident niet overeenstemt met de impact opgegeven door de Klant bij de aanmaak van het ticket, zal Proximus de toegekende Incidentprioriteit corrigeren.

*P1-incidenten kunnen uitsluitend gelogd worden door telefonisch contact op te nemen met de Service Desk.

6.5 Beschrijving van de Service Levels

6.5.1 Reactive Care-dienstformule

SLA KPI	Definitie	Van toepassing op	Richtcijfer	Geldig voor	Dienst-kredieten
Reactietijd bij Incidenten	De tijd binnen het overeengekomen Dienstrooster tussen de aanmaak van het ticket en de start van de troubleshooting door Proximus, min alle tijd als gevolg van een voorval waarop het 'stop clock'-principe van toepassing is.	Diagnose op afstand voor alle Oplossingselementen	30 min.	P1-inciden-ten	10% van de maandelijk-se vergoeding voor elk gevalideerd P1-incident met SLA-inbreuk en met een maximum van 25% van de maandelijk-se vergoeding
Efficiëntie antispam	Het Service Level komt overeen met het aandeel tegengehouden Spam als percentage van alle e-	Administration Portal Spam Quarantine Portal	>99%	N.v.t.	98%> X ≥ 99%: 5% 97%> X ≥98%: 10%

Koning Albert II-laan 27, B-1030 Brussel, België,
BTW BE 0202.239.951, RPR Brussel, BE50 0001 7100 3118 BPOTBEB1.

	mailverkeer, verstuurd als geldig e-mailadres van de Valideringslijst. Deze SLA zal enkel van toepassing zijn als de Klant de Antispam Best Practice-instellingen, zoals beschreven in Bijlage 1, heeft geïmplementeerd en gehandhaafd.				96%> X ≥97%: 15% 96%> X: 20% van de maandelijkse vergoeding
Accuraatheid van de anti-spam	Deze Service Level definieert het maximumpercentage Vals-Positieve Spam als percentage van alle e-mailverkeer naar en indien geconfigureerd van een geldig e-mailadres van de Valideringslijst. Deze SLA zal enkel van toepassing zijn indien de Klant de Best Practice-instellingen, zoals opgenomen als Bijlage 1, heeft geïmplementeerd en gehandhaafd. De volgende e-mails worden niet beschouwd als e-mails met Vals-Positieve Spam in het kader van dit Service Level: a) E-mails die geen legitieme business-e-mail zijn; b) E-mails met meer dan 20 bestemmelingen; c) E-mails waarbij de verzender van de e-	Administration Portal Spam Quarantine Portal	≤0.0003%	N.v.t.	0,0003%< X ≤ 0,003%: 5% 0,003%< X ≤ 0,03%: 10% 0,03%< X ≤ 0,3%: 15% 0,3%< X: 20% van de maandelijkse vergoeding

	mail op de lijst van de Klant met geblokkeerde verzenders staat, zoals onder meer, die gedefinieerd door: de individuele gebruiker, als de Klant de instellingen op het niveau van de gebruiker heeft geactiveerd; d) E-mails die vanaf een aangetast toestel worden verstuurd; e) E-mails die worden verstuurd vanaf een toestel dat op een lijst met blokkering van derden staat; f) E-mails geïntercepteerd door uitgaande Spam scanning				
Efficiëntie van het antivirus	Aantal geregistreerde virusinfecties die via de Dienst zijn binnengekomen en door Proximus werden bevestigd.	Administration Portal Platform	0 per kalendermaand of ingeval een virus wordt verstuurd via e-mail als bijlage en dit wordt gedetecteerd en niet gestopt, wordt de Klant voldoende op de hoogte gesteld om de geïnfecteerde e-mail te identificeren en te deleten.	N.v.t.	100% van de maandelijkse vergoeding met een maximum van 5.000 EUR
Accuraatheid van het antivirus	Dit Service Level definieert het maximumpercentage e-mails met Vals-Positieve Virussen als percentage van alle e-mailverkeer naar, en indien geconfigureerd, van	Administration Portal Platform	≤0.0001%	N.v.t.	0,0001%< X ≤ 0,001%: 5% 0,001%< X ≤ 0,01%: 10% 0,01< X ≤ 0,1%: 15%

	de geldige e-mailadressen van de Valideringslijst.				0,1> X ≥ 20% van de maandelijkse vergoeding
E-maillatentie	Het Service Level voor de e-maillatentie wordt gedefinieerd door de gemiddelde round trip time, zoals gemeten door de Symantec.cloud Tracker, voor e-mails die elke vijf (5) minuten van en naar de Dienst worden gestuurd.	Administration Portal Platform	Gemiddelde round trip time van 60 seconden per kalendermaand	N.v.t.	60 seconden< X ≤ 90 seconden: 5% 90 seconden< X ≤ 120 seconden: 10% 120 seconden< X ≤ 150 seconden: 15% 150 seconden< X: 20% van de maandelijkse vergoeding

Het totale bedrag van de Dienstkredieten die krachtens deze Overeenkomst m.b.t. tot eender welke SLA in eender welke kalendermaand aan de Klant worden toegekend, mag niet hoger zijn dan de maandelijkse vergoedingen die de Klant voor de Dienst betaalt, tenzij anders is gespecificeerd.

SLO KPI	Definitie	Van toepassing op	Richtcijfer	
Aanmaaktijd Incidentticket	De tijd tussen de notificatie van het Incident (via de Dienst) en de aanmaak van een Incidentticket in het ticketingsysteem.	Toegang tot de Service Desk voor alle Oplossingselementen	15 minuten	P1- en P2-incidenten
Reactietijd bij Incidenten	De tijd binnen het overeengekomen Dienstrooster tussen de aanmaak van het ticket en	Diagnose op afstand voor alle Oplossingselementen	1 uur	P2-incidenten

	de start van de troubleshooting door Proximus, min alle tijd als gevolg van een voorval waarop het 'stop clock'-principe van toepassing is.			

Koning Albert II-laan 27, B-1030 Brussel, België,
BTW BE 0202.239.951, RPR Brussel, BE50 0001 7100 3118 BPOTBEB1.

6.5.2 Full Care-dienstformule

SLA KPI	Definitie	Van toepassing op	Richtcijfer	Geldig voor	Dienstkredieten
Reactietijd bij Incidenten	De tijd binnen het overeengekomen Dienstrooster tussen de aanmaak van het ticket en de start van de troubleshooting door Proximus, min alle tijd als gevolg van een voorval waarop het 'stop clock'-principe van toepassing is.	Diagnose op afstand voor alle Oplossingselementen	30 min.	P1-incidenten	10% van de maandelijkse vergoeding voor elk gevalideerd P1-incident met SLA-inbreuk en met een maximum van 25% van de vergoeding
Dienstherstellingstijd	De Dienstherstellingstijd wordt gedefinieerd als de tijd tussen het ontstaan en de oplossing van een Incident op het Oplossingselement, binnen het overeengekomen Dienstrooster en minus alle tijd als gevolg van een voorval waarop het 'stop clock'-principe van toepassing is.	Interventie op afstand voor alle Oplossingselementen	4 uur	P1-incidenten	25% van de maandelijkse vergoeding voor elk gevalideerd P1-incident met SLA-inbreuk en met een maximum van 50% van de maandelijkse vergoeding
Jaarlijkse Dienstbeschikbaarheid	De Dienstbeschikbaarheid wordt berekend als volgt: 100*(1 – Nettodowntime/Totale tijd (24x7)) = % Dienstbeschikbaarheid waarbij de Nettodowntime de tijd is gedurende welke een Oplossingselement niet beschikbaar is tijdens het	Dienstbeschikbaarheid voor het Platform	99,95%	P1-incidenten	25% van de maandelijkse vergoeding voor elk gevalideerd P1-incident met SLA-inbreuk en met een maximum van 50% van de maandelijkse vergoeding

	Dienstrooster wegens een P1-incident, min alle tijd als gevolg van een voorval waarop het 'stop clock'-principe van toepassing is, en waarbij de Totale tijd de periode is waarvoor de Beschikbaarheid wordt berekend. Voor deze Dienst wordt de Dienstbeschikbaarheid gedefinieerd als het vermogen om een SMTP-sessie op te zetten op poort 25 van de MTA naar de Dienstinfrastructuur, conform RFC5321. Dit service level is niet van toepassing indien de Klant de Dienst incorrect heeft geconfigureerd (cf. de best practices-instelling in Bijlage 1).				
Implementatietijd voor Standaardwijzigingen	Tijd voor de implementatie van een Standaardwijziging, berekend vanaf de registratie van de aanvraag van een Standaardwijziging (tijdstip waarop het changeticket gecreëerd wordt) tot de volledige uitvoering ervan door Proximus (afsluiting van het changeticket).	Standaardwijzigingen	> 95% uitgevoerd binnen 3 Werkdagen	N.v.t.	95> X ≥ 90%: 5% 90> X ≥ 80%: 10% 80% > X: 25% van het maandelijkse vergoedingsforfait voor de Wijzigingskredieten
Efficiëntie antispam	Het Service Level komt overeen met het aandeel tegengehouden spam als percentage van het totale e-mailverkeer, verstuurd naar een geldig e-mailadres. Deze SLA	Administration Portal Spam Quarantine Portal	>99%	N.v.t.	98%> X ≥ 99%: 5% 97%> X ≥98%: 10% 96%> X ≥97%: 15% 96%> X: 20% van de maandelijkse vergoeding

	is enkel van toepassing indien de Klant de best practice-instellingen, zoals opgenomen als Bijlage 1, toepast en handhaaft.				
Accuraatheid antispam	Dit Service Level definieert het maximumpercentage Vals-Positieve Spam als percentage van alle e-mailverkeer. Dit SLA is enkel van toepassing indien de Klant de best practice-instellingen, zoals opgenomen als Bijlage 1, toepast en handhaaft. De volgende e-mails vormen geen e-mails met Vals-Positieve Spam in het kader van dit service level: a) E-mails die geen legitieme business-e-mail zijn; b) E-mails met meer dan 20 bestemmelingen; c) E-mails waarbij de verzender van de e-mail op de lijst van de Klant met geblokkeerde verzenders staat, zoals onder meer, die gedefinieerd door: de individuele gebruiker, als de Klant de instellingen op het niveau van de gebruiker heeft geactiveerd; d) E-mails die vanaf een aangetast toestel worden verstuurd;	Administration Portal Spam Quarantine Portal	≤0.0003%	N.v.t.	0,0003%< X ≤ 0,003%: 5% 0,003%< X ≤ 0,03%: 10% 0,03%< X ≤ 0,3%: 15% 0,3%< X: 20% van de maandelijkse vergoeding

	e) E-mails die worden verstuurd vanaf een toestel dat op een blokkeringslijst van derden staat; f) E-mails geïntercepteerd door uitgaande Spam scanning				
Efficiëntie van het antivirus	Aantal geregistreerde virusinfecties die via de Cloud Mail Security-dienst zijn binnengekomen en door Proximus werden bevestigd.	Administration Portal	0 per kalendermaand of indien een virus wordt verstuurd als bijlage bij een e-mail en dit wordt gedetecteerd en niet gestopt, wordt de Klant op afdoende wijze op de hoogte gesteld om de geïnfecteerde e-mail te identificeren en te wissen.	N.v.t.	100% van de maandelijkse vergoeding met een maximum van 5.000 EUR
Accuraatheid van het antivirus	Dit Service Level definieert het maximale onderscheppingspercentage Vals-Positieve Virussen als percentage van alle e-mailverkeer.	Administration Portal	≤0.0001%	N.v.t.	0,0001%< X ≤ 0,001%: 5% 0,001%< X ≤ 0,01%: 10% 0,01< X ≤ 0,1%: 15% 0,1> X ≥ 20% van de maandelijkse vergoeding
Aflevering van e-mails	Het Service Level voor de aflevering van e-mails wordt gedefinieerd door het percentage van alle e-mails dan van of	Administration Portal Platform	100%	N.v.t.	De Klant kan de Dienst opzeggen, mits hij dat vooraf schriftelijk laat weten.

	naar de Klant wordt verstuurd, rekening houdend met de volgende voorwaarden: a) De e-mail moet door de Dienst zijn ontvangen; en b) De e-mail mag geen Malware, Spam of andere content bevatten die de oorzaak ervan is dat hij door de Dienst wordt onderschept.				
E-maillatentie	Het Service Level voor de e-maillatentie wordt gedefinieerd door de gemiddelde round trip time, zoals gemeten door de Symantec.cloud Tracker, voor e-mails die elke vijf (5) minuten van en naar de Dienst worden gestuurd.	Administration Portal Platform	Gemiddelde round trip time van 60 seconden per kalendermaand	N.v.t.	60 seconden< X ≤ 90 seconden: 5% 90 seconden< X ≤ 120 seconden: 10% 120 seconden< X ≤ 150 seconden: 15% 150 seconden< X: 20% van de maandelijkse vergoeding

Het totale bedrag van de Dienstkredieten die krachtens deze Overeenkomst m.b.t. tot eender welke SLA in eender welke kalendermaand aan de Klant worden toegekend, mag niet hoger zijn dan de periodieke vergoedingen die de Klant voor de Dienst betaalt.

SLO KPI	Definitie	Van toepassing op	Richtcijfer	Geldig voor	Dienstkredieten
Aanmaaktijd Incidentticket	De tijd tussen de notificatie van het Incident (via de Dienst) en de aanmaak van een Incidentticket in het ticketingsysteem.	Toegang tot de Service Desk voor alle Oplossingselementen	15 minuten	P1- en P2-incidenten	Geen
Reactietijd bij Incidenten	De tijd binnen het overeengekomen Dienstrooster tussen de aanmaak van het ticket en de start van de troubleshooting door Proximus, min alle tijd als	Diagnose op afstand voor alle Oplossingselementen	30 min.	P2-incidenten	Geen

	gevolg van een voorval waarop het 'stop clock'-principe van toepassing is.				
Dienstherstellingstijd	De Dienstherstellingstijd wordt gedefinieerd als de tijd tussen het ontstaan en de oplossing van een Incident op het Oplossingselement, binnen het overeengekomen Dienstrooster en minus alle tijd als gevolg van een voorval waarop het 'stop clock'-principe van toepassing is.	Interventie op afstand Alle Oplossingselementen	6 uur	P2-incidenten	Geen

7. Specifieke voorwaarden

7.1 Algemene informatie

7.1.1. De Specifieke voorwaarden vormen een aanvulling bij de Algemene voorwaarden voor professionele klanten en deze Contractuele dienstbeschrijving. Zij beschrijven de rechten en verplichtingen van Proximus en de Klant met betrekking tot de levering van de Dienst die in dit document wordt beschreven.

7.1.2. De Dienst is enkel beschikbaar voor een Klant die zijn eigen domeinnaam heeft en in staat is om de MX-records en/of DNS voor die domeinnaam te configureren.

7.2 Contractuele procedure

7.2.1 Duur

In afwijking van de Algemene voorwaarden wordt de Overeenkomst vanaf de activering van de Dienst voor onbepaalde tijd gesloten.

7.2.2 Beëindiging en de gevolgen ervan

7.2.2.1 In afwijking van de Algemene voorwaarden kan de Klant het Contract op elk ogenblik schriftelijk beëindigen. Indien Proximus deze kennisgeving ten laatste op de vijftiende van de lopende maand ontvangt, treedt de beëindiging van de Overeenkomst in werking op de laatste kalenderdag van de lopende maand. Indien Proximus deze kennisgeving na de vijftiende van de lopende maand ontvangt, treedt de beëindiging van de Overeenkomst in werking op de laatste dag van de eerstvolgende maand. Proximus heeft het recht om, tot de opzeggingsdatum, de geleverde Dienst aan te rekenen en ervoor te worden betaald.

7.2.2.2. Op aanbeveling van deze Overeenkomst, desactiveert Proximus de Dienst en gelijk welke account die in het kader van de Dienst ter beschikking wordt gesteld. De configuratiewijzigingen die worden aangebracht voor de levering van de Dienst worden ongedaan gemaakt. Bij de beëindiging van de Overeenkomst moet de Klant het gebruik van de Dienst stopzetten en alle van Proximus ontvangen documentatie, samen met eventuele kopieën, inclusief gedeeltelijke kopieën, van de Software die hem in het kader van de Dienst ter beschikking werd gesteld, vernietigen. De Klant moet verklaren dat de Software uit alle toestellen, computergeheugens en opslagapparatuur waarover hij controle heeft, werd verwijderd en de documentatie vernietigd. De Klant dient de noodzakelijke configuratiewijzigingen door te voeren om de omgeving in zijn oorspronkelijke staat te herstellen.

7.2.2.3. De content die door Proximus wordt gehost in het kader van deze Dienst (d.w.z. e-mails in quarantaine, data beschikbaar via de message tracing-functie en het loggen van de configuratie) zal niet langer beschikbaar zijn nadat de Dienst is opgezegd, ongeacht de reden daarvoor. Bijgevolg dient de Klant, vooraleer hij de Overeenkomst opzegt, de nodige maatregelen te nemen om zijn content via de Administration Portal te exporteren (op specifiek verzoek aan Proximus kan malware worden geëxporteerd).

7.2.3 Schorsing

7.2.3.1. Ingeval de Dienst wordt opgeschort, zal de Klant toch de standaardvergoeding moeten betalen. Daarnaast zal Proximus het recht hebben een wederindienststellingsvergoeding te vragen.

7.2.3.2. Indien de Dienst om gelijk welke reden zou worden opgeschort, zal de Dienst niet worden toegepast op inkomende e-mails (en uitgaande e-mails, indien daartoe opdracht wordt gegeven) van de Klant. Deze e-mails zullen niet via het Platform worden gerouteerd. De Klant is verantwoordelijk om zijn e-mails tijdens de opschorting door te sturen, en te bevestigen dat alle configuraties accuraat zijn indien de Dienst wordt hersteld.

7.2.4 Upsize en downsize

7.2.4.1. De Klant mag gelijk wanneer gedurende de looptijd van de Overeenkomst het aantal e-mailadressen in het kader van de Overeenkomst verhogen. Elk schriftelijk verzoek van de Klant om het aantal e-mailadressen uit te breiden, zal worden ingewilligd op en gefactureerd vanaf de datum waarop het verzoek door Proximus geregistreerd wordt.

7.2.4.2. De Klant mag gelijk wanneer gedurende de looptijd van de Overeenkomst het aantal e-mailadressen in het kader van de Overeenkomst verhogen. Onverminderd de vereiste minimumaantallen van de e-mailadressen vermeld in de Overeenkomst, zullen schriftelijke verzoeken om het aantal mailboxen te verminderen, worden geïmplementeerd en gefactureerd vanaf de eerste dag van de volgende maand, op voorwaarde dat Proximus de aanvraag uiterlijk de vijftiende van de lopende maand registreert. Indien Proximus het verzoek na de vijftiende van de lopende maand registreert, zal het worden uitgevoerd en gefactureerd vanaf de eerste dag van de eerstvolgende maand.

7.2.4.3 Indien er bepaalde specifieke maatregelen vereist zijn om de upsize en/of downsize te kunnen uitvoeren, zal Proximus de Klant daarvan op de hoogte stellen. De Klant verbindt zich ertoe dergelijke maatregelen te treffen binnen het tijdsbestek bepaald door Proximus. De Klant aanvaardt dat, indien hij nalaat dergelijke maatregelen te treffen, Proximus niet in staat zal zijn op zijn verzoek in te gaan. De facturatie voor de betrokken maand zal dan volgens de voorheen geldende regels gebeuren.

7.3 Recht van gebruik

7.3.1. In overeenstemming met de voorwaarden van deze Overeenkomst en mits de Klant de vergoeding voor de Dienst vereffent, kent Proximus vanaf de datum van activering van de Dienst aan de Klant een niet-overdraagbaar, niet-sublicentieerbaar, niet-eeuwigdurend en niet-exclusief recht toe van toegang tot en gebruik van de Dienst gedurende de looptijd.

7.3.2. De Klant gebruikt de Dienst in overeenstemming met de Overeenkomst en de acceptable use policy gepubliceerd door de leverancier van Proximus (Symantec) op de volgende link https://www.symantec.com/content/dam/symantec/docs/eulas/policy/online-services-acceptable-use-policy-v6-en.pdf (of gelijk welke link die achteraf wordt toegevoegd) en tot het maximumaantal waarvoor het werd besteld. Het niet-naleven of schenden van de acceptable use policy vormt een inbreuk op de Overeenkomst. Proximus behoudt zich hetzelfde recht voor als zijn leverancier.

7.3.3. Het is de Klant verboden het geheel of een deel van de Dienst te kopiëren of te gebruiken (en derden, onder wie Eindgebruikers, daartoe machtiging of toelating te verlenen), behalve indien dat uitdrukkelijk door deze Overeenkomst wordt toegestaan; de Dienst te gebruiken op niet-toegelaten apparatuur of producten; de Dienst te gebruiken op een manier die de werking van de Dienst kan schaden, storen of onmogelijk maken; de Dienst te wijzigen of afgeleide werken te vertalen of creëren op basis van de Dienst, hem te reverse-engineeren of decompileren, decoderen, disassembleren, of de Dienst terug te brengen tot een door mensen leesbare vorm, tenzij dit bij wet wordt toegestaan; bedrijfseigen vermeldingen of opschriften in of op de Dienst te wijzigen of te verwijderen; de Dienst te gebruiken in strijd met de rechten van andere partijen. De Dienst omvat gelijk welke Portal en Software die in het kader van de Overeenkomst ter beschikking werd gesteld van de Klant.

7.4 Wijzigingen aan de Overeenkomst

7.4.1. Proximus mag de Dienst en de Overeenkomst te allen tijde herzien, zonder voorafgaande kennisgeving om de volgende redenen: (i) het wordt noodzakelijk door de toepasselijke wet of sectornormen; (ii) het wordt nodig om technologische redenen wanneer een verandering wordt aangebracht zonder dat de functionaliteit van de Dienst er wezenlijk door wordt aangetast; (iii) het wordt nodig om de werking van de Dienst in stand te houden zonder dat de functionaliteit van de Dienst er wezenlijk door wordt aangetast; of (iv) wijzigingen ten gunste van de Klant. Door de Dienst te blijven gebruiken, verklaart de Klant zich met deze wijzigingen akkoord.

7.4.2. In andere gevallen zal de procedure beschreven in de Algemene voorwaarden voor professionele klanten van toepassing zijn.

7.5 Rechten en verplichtingen van de klant

7.5.1. De Klant dient een of meer personen aan te stellen met de geschikte vaardigheden, kennis en/of ervaring om toe te zien op de Dienst, om de efficiëntie en de resultaten van de Dienst te beoordelen en om de verantwoordelijkheid voor de resultaten van de Dienst op zich te nemen.

7.5.2. De Klant waakt erover dat enkel gemachtigde personen toegang krijgen tot de Dienst en tot de veilige portals die hij in het kader van deze Overeenkomst ter beschikking heeft. Onverminderd de Algemene voorwaarden voor Professionele klanten, dient de Klant alle veiligheids- of technische normen die Proximus van tijd tot tijd voorschrijft, na te leven om gebruik te maken van de Dienst. Proximus kan niet controleren of aanvragen voor toegang tot en het gebruik van de Dienst wettig zijn en wijst elke aansprakelijkheid voor de gevolgen van frauduleuze of foutieve toegang en frauduleus of foutief gebruik af. De Klant dient Proximus onmiddellijk schriftelijk in kennis te stellen van elke wijziging van de identificatiegegevens van de gemachtigde personen.

7.5.3. De Klant verbindt zich ertoe Proximus onmiddellijk en naar behoren in kennis te stellen van elk Incident betreffende de Dienst en van elke technische of operationele verandering die de levering van de Dienst door Proximus zou kunnen beïnvloeden. Hij dient er zich echter van te vergewissen dat het Incident niet door hemzelf, zijn medewerkers of zijn eigen apparatuur veroorzaakt wordt.

7.5.4. De Klant waakt erover dat zijn systemen (1) niet fungeren als een Open Relay (d.w.z. een e-mailserver die wordt geconfigureerd om e-mail van een niet gekende of niet gemachtigde derde te ontvangen en om de e-mail door te sturen naar een of meer bestemmelingen die niet de gebruiker zijn van het e-mailsysteem waarmee de e-mailserver is verbonden), (2) niet fungeren als Open Proxy (d.w.z. een proxyserver die wordt geconfigureerd om niet gekende of niet gemachtigde derden toe te laten DNS, webpagina's of andere data voor de Dienst te raadplegen, op te slaan of door te sturen), (3) geen Spam (d.w.z. ongevraagde commerciële e-mail) versturen, (4) geen bulk e-mail (d.w.z. een groep van meer dan vijfduizend (5.000) e-mailberichten met in wezen dezelfde inhoud die wordt verstuurd of ontvangen in één operatie of een reeks gerelateerde operaties) verzenden of ontvangen, of (5) de veiligheid van de Dienst niet in het gedrang brengen (onder meer via pogingen tot hacking, 'denial of service'-aanvallen, mail bombs of andere kwaadwilllige activiteiten die ofwel gericht zijn op of afkomstig zijn van het domein van de Klant). Proximus behoudt zich het recht voor om te allen tijde na te gaan of de Klant zich aan dit artikel houdt. Dergelijke handelingen zullen worden beschouwd als de integriteit en de goede werking van de Dienst en de onderliggende infrastructuur ervan in het gedrang brengend. Dit geldt ook als de e-mailsystemen van de Klant op de zwarte lijst staan of indien de Klant er de oorzaak van is dat de systemen van Proximus (of van diens Leverancier) op de zwarte lijst terechtkomen door het versturen van spam. Onverminderd de Algemene voorwaarden voor Professionele Klanten, behoudt Proximus zich het recht voor om de Klant alle eventuele nodige herstellingswerken aan te rekenen tegen de toepasselijke tarieven.

7.5.6. De Klant stelt gedurende de looptijd van de Overeenkomst een correcte, accurate en exhaustieve lijst van alle e-mailadressen (waaronder aliassen) ter beschikking en werkt ze bij om de Dienst te ontvangen (de 'Valideringslijst'). Deze e-mailadressen moeten worden gelinkt aan het domein dat op de Bestelbon is vermeld. Inkomende en uitgaande e-mail verstuurd naar of afkomstig van e-mailadressen die niet zijn gespecificeerd in de Valideringslijst of op onjuiste wijze zijn ingevoerd, zullen automatisch worden geblokkeerd. Proximus erkent geen aansprakelijkheid indien deze e-mail niet kan worden afgeleverd als gevolg van fouten in of het ontbreken van e-mailadressen. De Service Levels zullen niet worden toegepast op ongeldige e-mailadressen. In het geval van de Reactive Care-dienstformule voert de Klant zelf de Valideringslijst in de Administration Portal in, terwijl in het geval van de Full Care-dienstformule de Klant de Valideringslijst bezorgt aan Proximus, dat ze in de Administration Portal zal invoeren.

7.5.7. De Klant erkent uitdrukkelijk van Proximus alle redelijkerwijs te verwachten informatie te hebben gekregen om vóór het aangaan van de Overeenkomst te kunnen nagaan of de Dienst aan zijn noden en vereisten voldoet.

7.5.8. De Klant erkent en aanvaardt dat Proximus zijn prijzen heeft vastgesteld en deze Overeenkomst is aangegaan op basis van de hierin gestipuleerde afstand van waarborg en beperking van aansprakelijkheid, dat deze een verdeling van risico tussen de Partijen weergeven en dat zij een essentiële basis van het akkoord tussen de Partijen vormen.

7.5.9. De Klant gaat ermee akkoord om de Dienst niet te gebruiken met het oog op het ontwikkelen van een concurrentieel product of een concurrentiële dienst of om de functies of de gebruikersinterface ervan te kopiëren, evaluaties van de Dienst of andere vergelijkende analyses uit te voeren gericht op publicatie buiten de organisatie van de Klant zonder de voorafgaande schriftelijke toestemming van Proximus.

7.5.10. De Klant erkent en aanvaardt dat de Dienst (en de toepasselijke oplossingselementen) en alle eventuele bijhorende downloads of technologieën ('Gecontroleerde technologie') kunnen worden onderworpen aan toepasselijke wetten, regelgevingen regels en licenties m.b.t. exportcontroles en handelssancties, en dat de Klant op de hoogte is van de informatie die de leverancier van Proximus (Symantec) heeft gepubliceerd op http://www.symantec.com/about/profile/ policies/legal.jsp (of de website die in de plaats ervan komt), en dient in orde te zijn met het voorgaande en met deze verdere exportbeperkingen die van toepassing kunnen zijn op de Dienst.

7.6 Rechten en verplichtingen van Proximus

7.6.1. De Klant erkent en aanvaardt dat de Dienst een standaarddienst is die niet werd ontworpen om uitdrukkelijk aan zijn specifieke businessbehoeften of -verwachtingen te voldoen. Proximus kan dan ook niet aansprakelijk worden gesteld voor het niet halen van doelstellingen die de Klant met betrekking tot de Dienst zou hebben bepaald. Bovendien erkent en aanvaardt de Klant dat Proximus geen andere verplichtingen heeft dan die welke volledig worden opgesomd in deze Overeenkomst.

7.6.2. Er is geen Dienst die een 100% opsporing van malware of ongewenste content kan waarborgen (zoals spam, pornografische afbeeldingen, content die specifieke voorafbepaalde woorden bevat, geblokkeerde URL, enz.) of een 100% bescherming tegen ongeoorloofde toegang door derden. Hoewel de Dienst speciaal is ontworpen om het netwerk en het internetverkeer van de Klant te beschermen tegen deze veiligheidsrisico's of ongewenste content, biedt Proximus geen waarborgen omtrent het vermogen van de Dienst om al deze ongewenste inhoud, onrechtmatige toegang door derden en veiligheidsrisico's te detecteren, te corrigeren of bescherming ertegen te bieden. Proximus wijst elke aansprakelijkheid af voor schade of verlies die rechtstreeks of onrechtstreeks het gevolg is van het feit dat de Dienst niet in staat is om deze veiligheidsrisico's of ongewenste content te detecteren of dat de Dienst een e-mail ten onrechte als verdacht heeft geïdentificeerd, zoals achteraf bleek, of niet in staat is om onrechtmatige toegang door derden te voorkomen. In overeenstemming met de Algemene voorwaarden is Proximus in dit verband tot een middelenverbintenis gehouden. Daarnaast waarborgt Proximus, onverminderd de toepassing van het Service Level-hoofdstuk, geen ononderbroken Dienst.

7.6.3 De onderhoudsactiviteiten die onder deze Overeenkomst vallen, worden beschreven in het hoofdstuk 'Operationele fase'. De vervanging of herstelling van het betrokken Oplossingselement, of elke andere interventie van Proximus, is niet inbegrepen bij de Dienst (en indien een dergelijke interventie wordt uitgevoerd, behoudt Proximus zich het recht voor ze afzonderlijk aan te rekenen tegen het

toepasselijke tarief) indien (i) het Incident te wijten is aan gebruik of voorvallen buiten de normale werkingsvoorwaarden van het betrokken Oplossingselement, (ii) ondersteuning op aanvraag wordt verstrekt; (III) supportactiviteiten i.v.m. de Software en/of Hardware niet langer door de fabrikant worden ondersteund, (iv) het Incident te wijten is aan:

a. externe oorzaken, met inbegrip van, maar niet beperkt tot weersomstandigheden, afsluiting of onderbreking van communicatielijnen die niet bij de Dienst inbegrepen zijn, defecten van de klimaatregeling, slecht werkende contactdozen, storm, blikseminslag, overstroming en alle andere oorzaken die niet aan het Oplossingselement gerelateerd zijn, ongeschikte omgevingsfactoren zoals een te hoge vochtigheid, abnormale temperaturen of een abnormaal hoog stofgehalte;
b. gebruik van het betrokken Oplossingselement dat niet is toegelaten krachtens de Overeenkomst en eventuele voorschriften verstrekt door Proximus;
c. het gebruik of de aansluiting van het betrokken Oplossingselement met of op items die niet door Proximus werden goedgekeurd of de abnormale werking van het item waarop het Oplossingselement wordt aangesloten;
d. de uitvoering (of poging daartoe) van onderhoud, een verplaatsing, herstelling, aanpassing of wijzigingen van het betrokken Oplossingselement door andere personen dan Proximus of andere dan door Proximus gemachtigde personen zonder voorafgaande schriftelijke goedkeuring van Proximus;
e. onachtzaamheid of fout (door een handeling of nalatigheid) van de Klant of derden bij het gebruik of opzetten van een Oplossingselement;
f. het in gebreke blijven van de Klant met betrekking tot de naleving van zijn verplichtingen die in deze Overeenkomst gestipuleerd worden.

7.6.4. In afwijking van de Algemene voorwaarden en indien Proximus aansprakelijk wordt gesteld voor het verlies van of schade aan de gehoste data van de Klant, zal de aansprakelijkheid van Proximus, naar eigen goeddunken, per schadegeval beperkt blijven tot het herstellen van de data vanaf de laatst beschikbare back-ups die Proximus in het kader van de Dienst heeft gemaakt of tot het bedrag dat de Klant (met uitsluiting van alle eenmalige vergoedingen) aan Proximus voor de Dienst heeft betaald tijdens de maand die aan de oorzaak van de schade voorafgaat.

7.6.5. Proximus wijst alle aansprakelijkheid van de hand voor schade, verlies of (on)kosten die de Klant of een derde kunnen lijden als gevolg van (i) het vrijgeven door de Klant (of door Proximus in opdracht van de Klant) van een met een virus geïnfecteerde e-mail die in quarantaine is geplaatst, (ii) het wissen door de Klant van een e-mail die in quarantaine is geplaatst, (iii) de slechte werking van de Dienst ingevolge de opzettelijke of onopzettelijke wijziging door de Klant of een derde, of (iv) een inbraak in het veiligheidssysteem (frauduleuze operatie of aanval) door gelijk wie (met uitzondering van Proximus-medewerkers). Bij fout of nalatigheid van de Klant dient de Klant Proximus te vrijwaren tegen vorderingen, klachten of acties door derden (met inbegrip van de eigen klanten, Eindgebruikers of leveranciers van de Klant) in dit verband.

7.6.6. Proximus kan niet aansprakelijk worden gehouden voor schade, onderbrekingen of fouten in het e-mailverkeer van de Klant door of te wijten aan de levering, de opschorting of de beëindiging van de Dienst of te wijten aan overmacht.

7.7 Betaling en facturatie

7.7.1 De Dienst zal maandelijks worden gefactureerd en op dezelfde factuur verschijnen als de eventuele Proximus-telecomdiensten waarop de Klant heeft ingetekend (exclusief mobiele diensten). Al deze

telecomdiensten zullen maandelijks worden gefactureerd, ongeacht de datum waarop voor deze diensten werd ingetekend. De Klant erkent en aanvaardt dat de bestelling van de Dienst een impact kan hebben op de periodiciteit van zijn facturatiecyclus en de datum van uitgifte van zijn facturen voor de telecomdiensten van Proximus.

7.7.2. De terugkerende vergoeding voor de Dienst wordt de Klant vooraf aangerekend (behalve voor de eerste facturatiecyclus), conform de prijstabel vermeld in de Bestelbon en afhankelijk van de e-mailadressen in het kader van de Overeenkomst.

Alle andere vergoedingen (zonder exhaustief te zijn: activering van de lijsten, installatie, configuratie, gebruik (voor pay-as-you-use), deactivering, reactivering, specifieke support, enz.) worden achteraf gefactureerd.

De Klant erkent en aanvaardt dat zijn facturen gebaseerd zijn op de metingen die de systemen van Proximus (of zijn leveranciers) voor de betrokken facturatiecyclus hebben uitgevoerd.

7.73. De facturatie start op het ogenblik dat Proximus de identificatiecodes (wachtwoord, gebruikersnaam, enz.) aan de Klant meedeelt, ongeacht de activeringsdatum van de Dienst.

7.74. Tenzij anders gespecificeerd zijn de prijzen exclusief alle eventuele kosten van de apparatuur die nodig zijn om de Dienst te gebruiken, en exclusief alle eventuele internettoegangskosten of kosten voor datatransmissie. De Klant is verantwoordelijk voor al deze bijkomende kosten en eventuele belastingen, en is wettelijk verplicht ze te betalen.

7.8 Rapportage

Alle rapporten die door Proximus in het kader van de Dienst worden voorbereid, worden te goeder trouw opgemaakt op basis van de informatie die op dat ogenblik beschikbaar is. Ze zijn enkel bedoeld voor intern gebruik door de Klant. Derden mogen ze niet gebruiken of er een beroep op doen zonder de voorafgaande schriftelijke toestemming van Proximus. Proximus wijst ten overstaan van alle Partijen, behalve de Klant, elke verantwoordelijkheid of aansprakelijkheid af met betrekking tot eventuele rapporten of documenten die het in het kader van de Dienst heeft voorbereid.

7.9 Bescherming van persoonsgegevens

7.9.1. Proximus treedt op als gegevensverwerker voor de persoonsgegevens die zijn begrepen (1) in de configuratiegegevens van de oplossingselementen (2) in e-mails die worden verwerkt in het kader van deze Overeenkomst, (3) gegevens beschikbaar via de Administration tool. Proximus treedt op als verwerkingsverantwoordelijke voor alle andere persoonsgegevens die door Proximus in het kader van deze Overeenkomst worden verwerkt.

7.9.2. Indien voor de uitvoering van de Dienst door Proximus de toestemming, goedkeuring of bevoegdheid van een andere persoon dan de Klant vereist is, garandeert de Klant dat hij deze toestemming, goedkeuring of bevoegdheid zal hebben verkregen vooraleer Proximus begint met de levering van dat deel van de Dienst waarvoor de toestemming, goedkeuring of bevoegdheid is vereist.

7.9.3. Proximus erkent en bevestigt dat de inhoud die door de Dienst naar de Klant wordt verstuurd of van de Klant wordt ontvangen, vertrouwelijk is. Proximus (en zijn leverancier) hebben geen toegang tot de e-mails, de bijlagen erbij, of tot de ermee verband houdende content, noch zullen ze die lezen of kopiëren, behalve via de elektronische methodes ten behoeve van de levering van de Dienst. Weliswaar behouden Proximus (en zijn leverancier) zich het recht voor om de malware- en spamgerelateerde inhoud van deze e-mails, de bijlagen erbij en de gerelateerde inhoud enkel te gebruiken met het oog op:

- het in stand houden en verbeteren van de Dienst,
- het naleven van gerechtelijke bevelen en alle regelgevende, wetgevende of contractuele vereisten, en
- het beschikbaar maken aan de leverancier van gelijk welke informatie die via de Dienst loopt en die interessant kan zijn voor de leverancier, enkel met het doel om de Dienst verder te ontwikkelen en te verbeteren.

7.10 Overmacht

In het kader van deze Dienst wordt een geval van overmacht gedefinieerd als feiten of omstandigheden die onafhankelijk zijn van zijn wil, onvoorzienbaar of onvermijdelijk zijn, zoals oorlog, opstanden, onlusten, burgeroproer, handelingen van burgerlijke of militaire instanties, embargo's, ontploffingen, faillissement van een licentiegever of leverancier, stakingen of arbeidsconflicten (met inbegrip van die waarbij zijn personeel betrokken is), kabelbreuken, stroomonderbrekingen (met inbegrip van die welke voortvloeien uit de toepassing van een door de overheid opgelegd afschakelplan), een tekort aan resources, overstromingen, aanhoudende vorst, brand of onweer.

Door de specifieke aard van de Dienst wordt de mogelijkheid van beëindiging door overmacht beschreven in de Algemene voorwaarden toegekend aan de beide Partijen indien het geval van overmacht meer dan 30 dagen aanhoudt.

7.11 Beperkingen van de Dienst

De volgende beperkingen zijn van toepassing op de Dienst

- Het maximumaantal inkomende en uitgaande boodschappen, per Gebruiker per kalendermaand is 10.000. In dit aantal is niet de eventuele Spam en Malware begrepen die aan de Klant zijn gericht.
- Mits hij de Klant daarvan in kennis stelt, behoudt Proximus zich het recht voor om de Klant te factureren voor bijkomende Gebruikers, voor de resterende maanden van het contract waar het verbruik het maximumaantal boodschappen overtreft.
- Er zal gedurende 7 kalenderdagen worden getracht om inkomende en uitgaande mail opnieuw te versturen.
- Standaard bedraagt de maximumgrootte van een e-mail 50 MB. De Klant kan gelijk welk maximum voor de e-mailgrootte instellen tot 1000 MB. Alle door de Dienst ontvangen e-mails boven de aangegeven limiet zullen worden geblokkeerd en gewist, en er zal een kennisgevingse-mail worden gestuurd naar de verzender, de bedoelde bestemmeling en een Administrator.

7.12 Specifieke voorwaarden van de Dienst

- De Klanten dienen hun inkomende e-mail via de Dienst te routeren via de routeringsinformatie die Proximus levert en mogen e-mail niet naar een andere bestemming routeren.
- De Klant dient inkomende e-mail van alle vereiste IP-vorken te aanvaarden om de continuïteit van de dienst te verzekeren indien een gedeelte van de Infrastructuur niet beschikbaar is.
- De Klant dient het (de) IP-adres(sen) of de hostnaam (namen) van de mailserver te specificeren voor de levering van inkomende e-mails naar hun organisatie.
- De Klant dient erover te waken dat alle domeinen (inclusief subdomeinen) waarvoor de Dienst vereist is, worden geleverd. De Klant aanvaardt dat functionaliteiten van de Dienst mogelijk niet correct werken en dat de aflevering van e-mails mogelijk onbeschikbaar zal zijn voor domeinen die niet ter beschikking worden gesteld.

Bijlage 1: best practice-instellingen voor Anti-Spam

Merk op dat de SL enkel van toepassing is indien de volgende best practice-instellingen door de Klant worden geconfigureerd. De Klant blijft verantwoordelijk voor de configuratie voor gelijk welke dienstformule.

7.13 Voor de Reactive Care-dienstformule

7.13.1 Te configureren door de Klant

- De beide goedgekeurde-verzenderopties activeren en het aantal entry's op de lijst zo laag mogelijk houden
- Spoofed sender detection met SPF activeren - aanbevolen wanneer er een probleem is met spoofed spam mails – Enkel voor inkomende mails
- DMARC (Domain-based Message Authentication, Reporting, and Conformance) activeren helpt phishingpogingen, die kunnen leiden tot beveiligingsinbreuken, afblokken door het detecteren van spoofing van de e-mailverzender – enkel voor inkomende e-mails
- De beide lijsten met geblokkeerde verzenders activeren - Aanbevolen actie voor beide is 'blokkeren en wissen'.
- De dynamische IP-bloklijst gebruiken - Aanbevolen actie is 'blokkeren en wissen', omdat dit een lijst van dynamische IP ranges bevat waarvan e-mail niet afkomstig mag zijn.
- Het Signature System activeren - Aanbevolen actie is 'blokkeren en wissen', aangezien dit werkt op de eigenschappen van gekende spam.
- Skeptic Heuristics - Predictive Spam detection activeren - De aanbevolen actie is de subject line te taggen en e-mail laten doorkomen, omdat dit kan worden ingesteld via Outlook-rules voor de eindgebruikers. Dit is ook aanbevolen, omdat deze rule set, ook al is hij heel accuraat, potentieel meer vals-positieven kan opleveren, omdat het een voorspellend systeem is. Anders dient 'e-mail in quarantaine plaatsen' te worden gebruikt als het is geactiveerd.
- Activeer indien nodig de newsletter filter uitbreiding - dit is een heel agressieve blokkering van newsletters, die alle gewilde en ongewilde newsletters tegenhoudt. In de regel bevelen we aan dat dit wordt geactiveerd en dat uitzonderingen geval per geval worden toegestaan, afhankelijk van de omgeving waarin je uitrolt.
- Spoofed sender detection activeren met SPF – voor uitgaande e-mails
- DMARC (Domain-based Message Authentication, Reporting, and Conformance) activeren helpt phishingpogingen, die kunnen leiden tot beveiligingsinbreuken, afblokken door spoofing van de e-mail van de verzender te detecteren – voor uitgaande e-mails

7.14 Voor Reactive Care met Assistentie of Full Care-dienstformule

7.14.1 Te configureren door de Klant

- Spoofed sender detection activeren met SPF – voor uitgaande e-mails
- DMARC (Domain-based Message Authentication, Reporting, and Conformance) activeren helpt phishingpogingen, die kunnen leiden tot beveiligingsinbreuken, afblokken door spoofing van de e-mail van de verzender te detecteren – voor uitgaande e-mails

8. Bijlage 2: Technische vereisten

De Klant dient erover te waken dat zijn e-mailsysteem in overeenstemming is met SMTP.

De Klant dient de volgende configuratie-instellingen voor zijn ICT-infrastuctuur te implementeren en in stand te houden om de correcte ondersteuning van de Dienst mogelijk te maken:

- Een sleutel aan de DNS van de Klant toevoegen. Proximus zal deze sleutel meedelen zodra het order is bevestigd.
- Plaats de IP-adressen van de Dienst op de witte lijst om toegang te krijgen tot de omgeving van de Klant, waar de e-mailserver wordt gehost. Proximus zal deze IP-adressen meedelen zodra het order is bevestigd.
- MX-records wijzigen. Proximus zal de details hiervan meedelen zodra het order is bevestigd.