Bastion 365

WHITE PAPER

NTA 7516 compliant

met Microsoft 365 en Bastion 365

Versie 3.5

04-07-2022

INHOUD

INLEIDING

In dit White Paper geven we u een overzicht van de benodigde technische configuratie van uw domein en hoe Bastion 365 past binnen uw architectuur. Houd er rekening mee dat Bastion 365 de beveiligingsinstellingen voor uw domein (-en) niet configureert of onderhoudt maar deze wel nodig heeft om correct te werken. Deze technische gids legt de basisconcepten van de beveiligde e-mailconfiguratie uit en verwijst u waar nodig naar meer informatie.

Deze white paper is geschreven op basis van de nieuwe release van Bastion 365 (R2).

Mocht u vragen of opmerkingen hebben, raadpleeg onze kennisbank op bastion365.nl of neem contact op met onze Supportafdeling via support@bastion365.nl.

WAAROM GEWONE E-MAIL NIET VEILIG IS

Hoewel e-mail een van de oudste vormen van communicatie op internet is en overal in applicaties op diverse apparaten is geïntegreerd, waren veiligheid en privacy nooit onderdeel van het ontwerp. Zorgen over privacy hebben een tijdje geduurd om serieus te worden genomen door wetgevers en er is eindelijk wetgeving geïmplementeerd in 2018 om de veiligheid van onze privacy te waarborgen. Strenge definities en hoge boetes voor niet-naleving hebben nu de aandacht van organisaties getrokken en e-mail is nu geïdentificeerd als een groot probleem en (hoogstwaarschijnlijk) grootste privacy lek in hun proces.

In principe is het artikel 32 van de Algemene Verordening Gegevensbescherming (AVG) die eist dat er zorgzamer om wordt gegaan met persoonsgegevens:

*"De verantwoordelijke legt passende **technische** en **organisatorische** maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een **passend beveiligingsniveau** gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen."*

Op Europees niveau is er een norm ontwikkeld voor wat er minimaal moet gebeuren bij digitale identificatie. Dit is de Europese eIDAS norm. De NEN – het Nederlandse orgaan voor het opstellen van normen en certificaties – heeft specifiek voor de zorgsector o.a. de NEN 7510 norm ontwikkeld voor informatiebeveiliging in de Zorg en ook de mate waarin acties moeten worden gelogd, de NEN 7513.

Om aan al deze eisen te voldoen is de norm voor veilig e-mailen in de zorg-sector geformuleerd: de NTA 7516.

HOE WERKT NTA 7516?

NTA 7516 heeft de vijf veilige e-mail standaarden als technische basis en voegt daaraan toe dat de twee NTA 7516 compliant partijen ook een NTA 7516 record moeten hebben in hun DNS. Hiermee declareren de zender en ontvanger te voldoen aan NTA 7516 en definiëren ze de mailserver die NTA 7516 berichten kan verzenden of ontvangen.

Indien beide partijen voldoen, kan de e-mail veilig worden afgeleverd in de inbox van de ontvanger. Het bericht is dan voorzien van een NTA 7516 header die het bericht herkenbaar maakt als zodanig.

Aangezien beiden partijen declareren aan NTA 7516 te voldoen, moeten beide organisaties ook multi-factor authenticatie hebben toegepast op de werkplek.

Als de e-mail niet conform NTA 7516 kan worden verstuurd, dan moet er een alternatieve methode zijn om het bericht af te leveren. Deze moet ook gebruikmaken van een geldige multi-factor authenticatie, maar moet ook zo gebruiksvriendelijk mogelijk blijven.

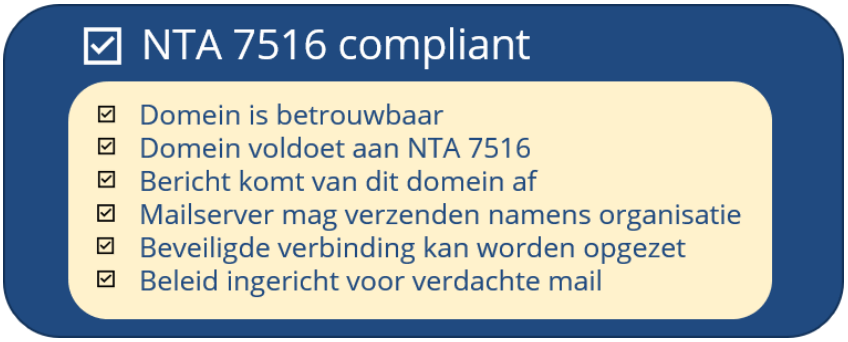
De NTA 7516 richt zich op de volgende doelgroepen:

Doelgroep	Mailprovider	
Professionals die voldoen aan NTA 7516	zivver, zorgmail, SMARTLOCKR, PINEWOOD, E-Zorg, Bastion 365, Cryptshare, SecuMailer	Ontvangen de mail in hun inbox
Professionals die niet voldoen aan NTA 7516	Exchange	Ontvangen de mail via MFA portaal
Patiënten en mantelzorgers	Gmail, yahoo!, Outlook.com	Ontvangen de mail via MFA portaal

1.) De zorgprofessionals die voldoen aan NTA 7516. Deze hebben een NTA 7516 gecertificeerde mailprovider en ontvangen de NTA 7516 berichten in hun e-mail inbox
2.) De zorgprofessionals die (nog) niet voldoen aan NTA 7516. Deze hebben nog geen NTA 7516 gecertificeerde mailprovider of voldoen om een andere reden (nog) niet aan NTA 7516. Deze hebben in ieder geval Microsoft Exchange als mailprovider. Zij kunnen de persoonsgebonden berichten niet direct in hun mailbox ontvangen en moeten eerst via MFA geauthentiseerd worden.
3.) Patiënten kunnen niet voldoen aan NTA 7516 en hebben vaak een mailaccount bij een gratis mailprovider zoals Gmail, Hotmail or Outlook of Yahoo!. Zijn moeten ook eerst via MFA worden geauthentiseerd voordat zij het bericht met persoonsgebonden informatie kunnen lezen.

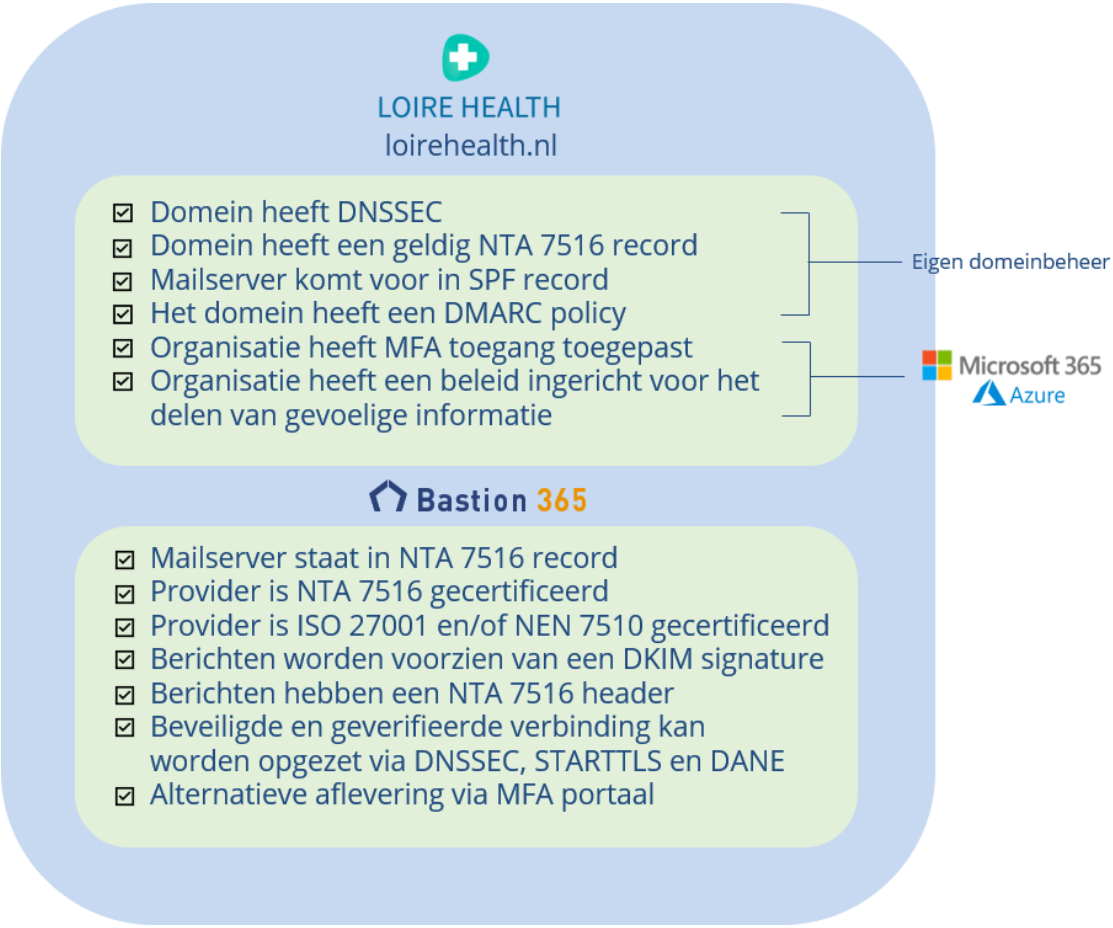
HOE WORD JE NTA 7516 COMPLIANT?

Een NTA 7516 compliant domein voldoet aan de volgende voorwaarden:



In ons voorbeeld moet de zorgorganisatie *Loirehealth* op het eigen domein een aantal zaken inrichten. Dit moet men zelf doen of via een geautoriseerde partner, omdat de mailprovider over het algemeen geen toegang heeft tot het hoofddomein.

Naast het inrichten van de veilige e-mail standaarden, moet men ook MFA toegang tot de werkplek hebben geregeld. De zorgorganisatie moet ook een beleid hebben ingericht voor toegang en delen van gevoelige informatie.



De mailprovider van de zorgprofessional moet NTA 7516 zijn gecertificeerd en heeft daarvoor ook als basis een ISO 27001 en/of of NEN 7510 certificaat nodig om aan te tonen dat hij zijn informatie beveiliging goed op orde heeft. De provider zal de DKIM handtekening plaatsen en het bericht van een NTA 7516 header voorzien, zodat het als zodanig kan worden verstuurd. De provider moet ervoor zorgen dat de beveiligde en geverifieerde verbinding kan worden opgezet.

We willen voorkomen dat berichten niet worden verzonden als de ontvangende partij niet aan NTA 7516 voldoet. Daarom moet er een alternatieve aflevermethode zijn in de vorm van een portaal die voorzien is van MFA.

Dat gaat nu per SMS, omdat dit op dit moment de meest veilige methode is voor iedereen. Vrijwel iedereen heeft een mobiele telefoon en kan SMS berichten ontvangen. Dit portaal moet eenvoudig en gebruiksvriendelijk zijn. Wat daarmee met name wordt bedoeld, is dat de gebruiker naast de multi-factor authenticatie niet nog andere handelingen moet verrichten om bij het bericht te kunnen in het portaal, zoals een aparte login of installatie van plug-ins.

WAT DOET BASTION 365?

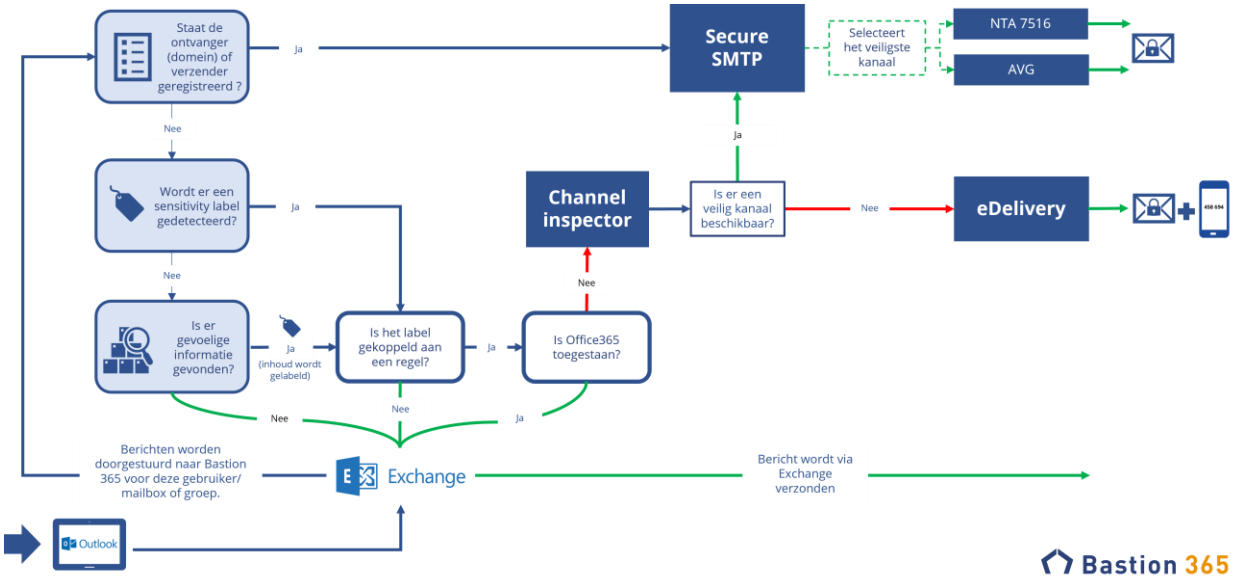
Bastion 365 zorgt ervoor dat het berichtenverkeer dat het ontvangt, wordt geanalyseerd op basis van geadresserden, labels en inhoud. Afhankelijk van het in Bastion 365 ingerichte beleid kan bepaald worden via welke route berichten verstuurd moeten worden.

Het is zeer aangeraden om gebruikers de mogelijkheid te geven om zelf aan te kunnen geven dat een bericht veilig verzonden moet worden. Dit kan door middel van sensitivity labels in Microsoft 365.

In de onderstaande opzet zijn de volgende 3 classificatie stappen ingericht:

1. Op basis van verzender of ontvanger wordt bepaald of een bericht veilig verstuurd moet worden.
2. Op basis van een sensitivity label in bericht of bijlage wordt bepaald of een bericht wel of niet veilig verzonden moet worden.
3. Op basis van een combinatie van classificaties worden het bericht en eventuele bijlagen gescanned op wat door uw organisatie is gedefinieerd als gevoelige inhoud (bijvoorbeeld de combinatie van medische- en persoonlijke informatie).

Als geen van de 3 van toepassing zijn, kan ingericht worden dat het bericht weer via Exchange wordt verstuurd.



INRICHTING

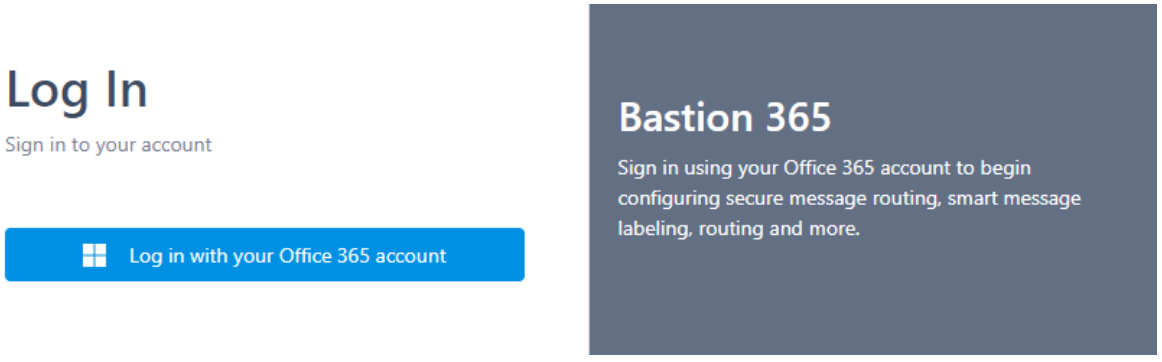
DNS	Microsoft 365			Bastion 365		
	Azure	Outlook	Exchange	**Inrichting**	**Inspector**	**MFA portaal**
Domein is DNSSEC	MFA toegang op de werkplek	Gebruiker heeft toegang tot e-mail	Connectors	Profiel Dataopslag Gebruikers	Berichtlabels - Inrichten bericht classificaties - Inrichten personal identifiers - Inrichten termen - Eigen classificaties	Bewaartermijn Beantwoorden toestaan - met bijlagen - toegestaane bijlagen SMS - provider - naam afzender - bericht
NTA 7516 TXT record aanmaken	Beleid voor toegang tot gevoelige informatie	Gebruiker mag gevoelige informatie delen	Mail flow rules	Beheerders toevoegen / verwijderen	Bericht regels	Portal huisstijl en teksten
Bastion 365 toevoegen in SPF	Sensitivity labels inrichten voor de organisatie	Gebruiker kan sensitivity label op bericht zetten of bijlage kan label bevatten		Domeinen inrichten en valideren	Beveiligde kanalen	Notificaties huisstijl en teksten
DKIM selectors aanmaken				Scripts for connectors en mailflow rules genereren		Mail forms
DMARC policy inrichten						

Eigen DNS

In het configuratieportaal van Bastion 365 richt u uw domein(-en) in voor het zenden en ontvangen van veilige mail, bepaalt u de settings van de eDelivery mailberichten en kunt u de transactie logs bekijken.

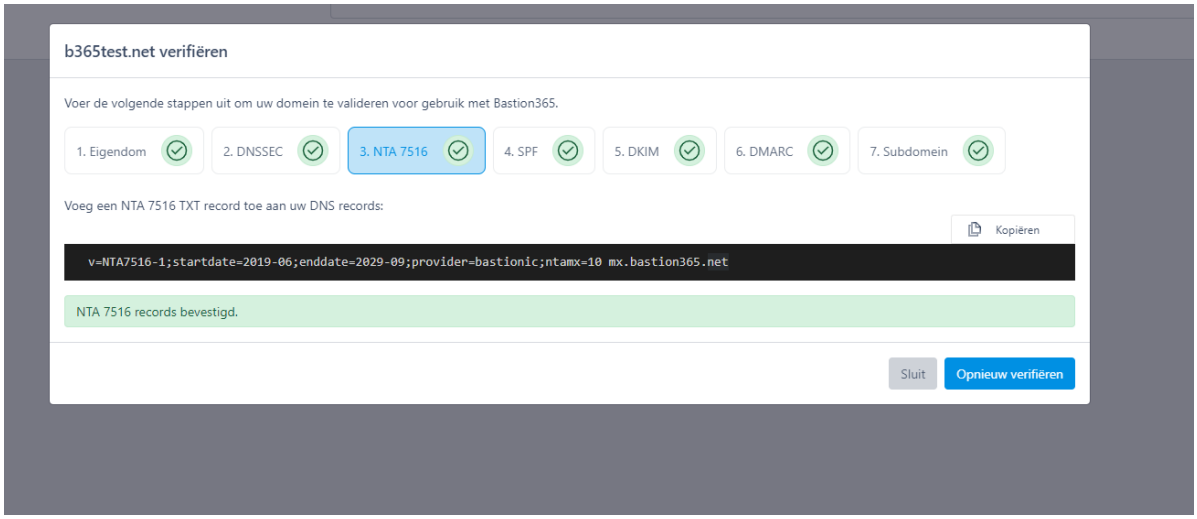
Na activatie van uw organisatie voor het werken met Bastion 365, bereikt u het portaal via uw webbrowser: *r2portal.bastion365.com*

Nadat u bij ons bent geregistreerd kunt u via single sign-on inloggen met uw Microsoft 365 account.



Voor elk domein moet u valideren of deze voldoet aan de veiligheidseisen en -normen van NTA 7516. U wordt ook geholpen met voorbeelden van hoe de DNS records juist geconfigureerd

moeten worden en u hoeft deze alleen te kopieren naar uw DNS records.



Meer informatie over de veilige email standaarden vindt u in Bijlage A: Veilige e-mail standaarden

DNSSEC
Uw hoofddomein moet beveiligd zijn met DNSSEC zodat informatie die verkregen vanaf uw DNS gevalideerd kan worden.DNSSEC wordt over het algemeen ondersteund door de DNS providers, maar moet misschien wel worden aangevraagd.

Alhoewel het beveiligen van het domein met DNSSEC zeer wenselijk is, heeft de NTA 7516 er tevens in voorzien dat organisaties (tijdelijk) ook zonder DNSSEC NTA 7516 berichten kunnen versturen (bijlage B in de NTA 7516). De DNSSEC verificatie in Bastion 365 is daarom geen vereiste om te starten met het versturen van NTA 7516 berichten.

NTA 7516 record
Om te voldoen aan de NTA 7516 en om herkenbaar te zijn als NTA 7516 compliant verzender en ontvanger moet u een NTA 7516 TXT record aanmaken met de volgende inhoud:

v=NTA7516-1;startdate=2019-06;enddate=2024-09;provider=bastionic;ntamx=10 mx.bastion365.net

Voor naar uw domein verzendende domeinen geeft de ntamx in dit record aan wat de mailserver is waar NTA 7516 berichten moeten worden geleverd. Dit is de mailserver van Bastion 365.

SPF
Om een consistent beleid te garanderen, moet SPF worden geïmplementeerd op alle domeinen en alle ontvangende e-mailservers die met Bastion 365 worden gebruikt.

SPF wordt toegepast op alle relevante domeinnamen (inclusief domeinen waarmee niet wordt gemaild), én op alle ontvangende e-mailservers (meer precies: op elk domein met een A-record of een MX-record). Het SPF-record moet de domeinnaam + ip-adres(sen) van de verzendende server(s) en de string «-all» bevatten.

Het SPF-record dient de volgende elementen te bevatten:

- *de e-mailservers voor uw domein*
- *de lijst van servers van Bastion 365, middels de volgende include:* ***include:_spf.mail.services.bastion365.net***
- *eindigen op -all*

het resultaat ziet er dan zo uit:

v=spf1 <uw mail-servers> include:_spf.mail.services.bastion365.net -all

DKIM
Bastion 365 plaatst een DKIM-handtekening op het bericht wanneer het wordt verzonden. Hierdoor is het voor de ontvanger verifieerbaar dat het bericht vanuit uw organisatie is verzonden.

Om dit te doen, moet u twee nieuwe CNAME- records aanmaken voor elk domein dat door Bastion 365 zal worden gebruikt om de uitgaande berichten te ondertekenen.

Als u DKIM-handtekeningen in Exchange Online gebruikt, heeft u al twee CNAME-records (selector1 en selector2) voor Microsoft in uw DNS staan. **Laat deze alstublieft ongewijzigd.**

Uw CNAME-records moeten er als volgt uitzien:

Host = fen-selector-1._domainkey. {formattedDomainName}.mail.services.bastion365.net
Host = fen-selector-2._domainkey. {formattedDomainName}.mail.services.bastion365.net

DMARC
DMARC staat voor Domain-based Message Authentication, Reporting and Conformance. Het is een DNS TXT-record dat in uw domein is gepubliceerd. Hiermee kunt u specificeren welk authenticatiemechanisme wordt gebruikt bij het verzenden van e-mails vanuit uw domein (DKIM, SPF of beide) en wat uw beleid is als de authenticatie mislukt:

p=quarantine
'Quarantine' laat de e-mailontvangers weten dat u wilt dat e-mails met extra voorzichtigheid moeten behandelen wanneer die de DMARC-verificatiecontrole niet doorstaan.

De e-mails worden nog steeds geaccepteerd door de ontvanger, maar de ontvanger beslist welk quarantainebeleid hij wil implementeren.

p=reject
Met 'Reject' zorgt u ervoor dat alle schadelijke e-mail worden gestopt. De ontvanger van de kwaadaardig bedoelde e-mail zal niet op de hoogte worden gebracht van de e-mail, omdat deze nooit naar een spam- of quarantainemap wordt gestuurd. Doordat zij volledig worden

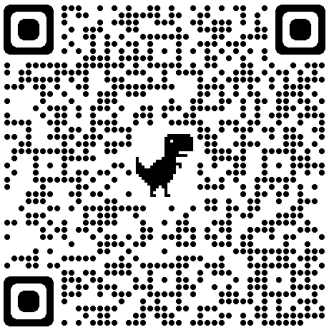
geblokkeerd, worden deze e-mails nooit afgeleverd en kunnen eindgebruikers niet worden misleid om op een kwaadaardige link te klikken of een gevaarlijke bijlage te openen.

Microsoft 365

Azure

De multi-factor authenticatie op de werkplek moet u inrichten in Azure. Dit kan voor alle medewerkers, bepaalde gebruikers of groepen. Met betrekking tot NTA 7516 is het van belang dat iedere medewerker die toegang heeft tot persoonlijke gezondheidsinformatie zich op de werkplek aanmeldt met MFA authenticatie.

Aangezien Bastion 365 geen aparte aanmelding van gebruikers vereist en deze hun berichten via hun normale Outlook client kunnen versturen, zijn er verder geen aanvullende maatregelen nodig.

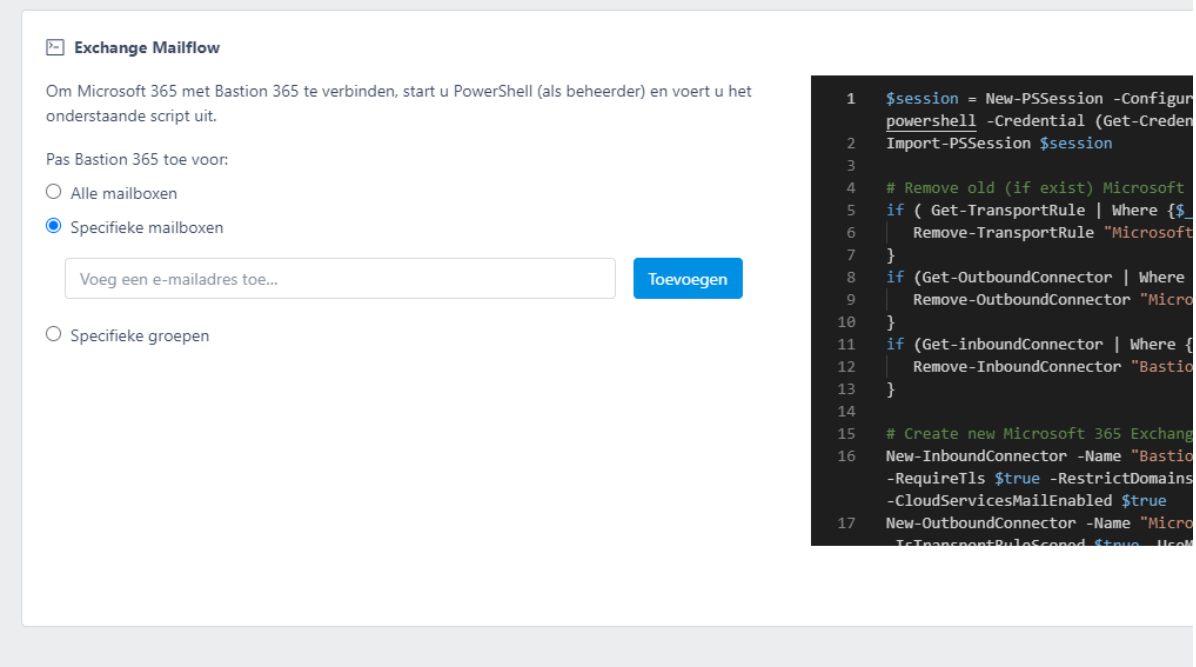


Scan of klik op de QR code hierboven voor meer informatie over MFA in Azure.

Exchange

In Exchange bepaalt u welke berichten via Bastion 365 moeten worden verstuurd, zodat deze conform NTA 7516 kunnen worden bezorgd.

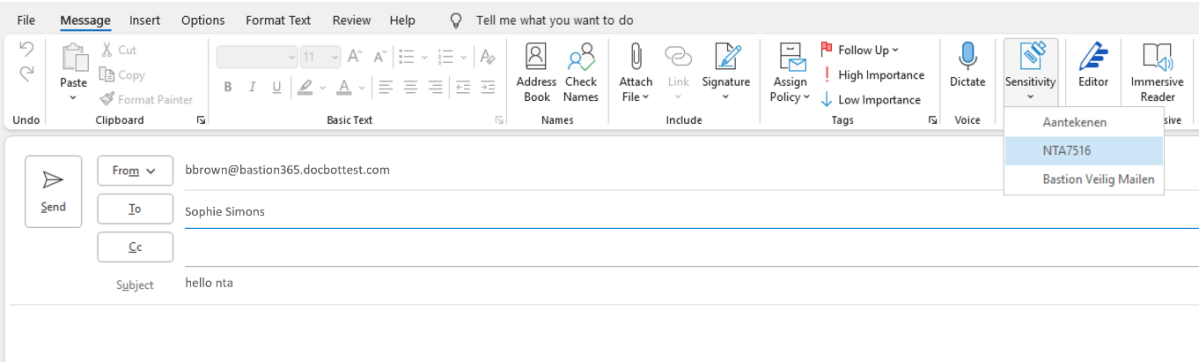
Het is mogelijk om het berichtenverkeer dat via Bastion 365 moet gaan lopen te beperken tot enkele specifieke gebruikers of groepen. Dit wordt ingericht in Exchange. Bastion 365 vereenvoudigt de inrichting met een script generator. U hoeft slechts de gewenste gebruikers, mailboxen of groepen toe te voegen en het script op Exchange uit te voeren.



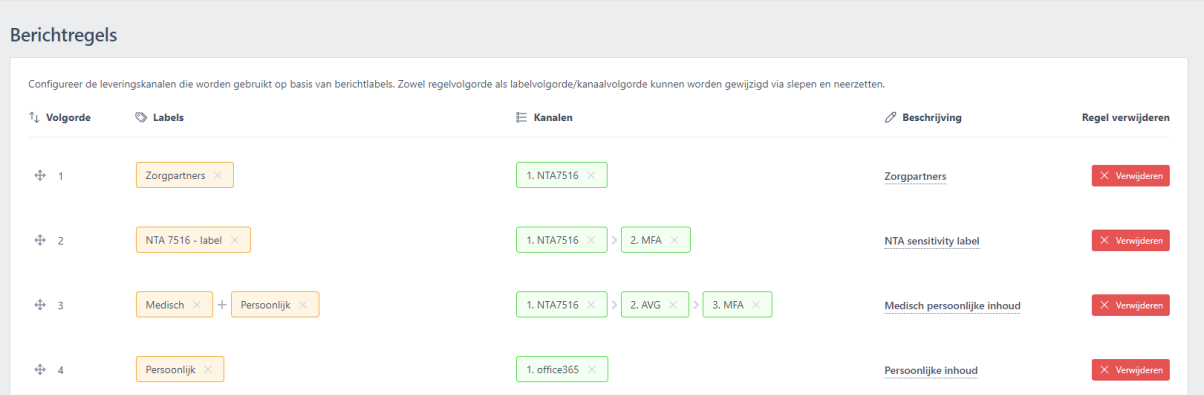
Het script maakt ook de nodige connectors aan, waarmee Bastion 365 en Exchange berichten kunnen uitwisselen met elkaar.

Outlook

In principe hoeft er in de Outlook client niet iets ingericht te worden voor de gebruiker om gebruik te kunnen maken van Bastion 365. Het is echter wel sterk aangeraden om gebruik te maken van sensitivity labels en om deze detecteerbaar te maken in Bastion 365. Hiermee hebben gebruikers de mogelijkheid om in Outlook zelf een veilig bericht te initiëren. Zie Sensitivity labels.



Indien de gebruiker het bericht niet voorziet van een sensitivity label, maar wel een bijlage toevoegt die het label bevat, zal Bastion 365 het label herkennen en de ingerichte veilige routering van het bericht toepassen.



Scan of klik op de QR code hierboven voor meer informatie over sensitivity labels in Microsoft 365.

VEILIGE KANALEN IN BASTION 365

In Bastion 365 zijn er drie standaard veilige kanalen:

NTA 7516

Dit kanaal onderzoekt of het ontvangende domein voldoet aan de NTA 7516. Hierbij worden alle in de NTA 7516 beschreven opties ondersteund:

1. Opzoeken in het met DNSSEC beveiligde domein wie de gecertificeerde provider is en de ntamx (mailserver voor NTA 7516 berichten) in het NTA 7516 record en vervolgens daarheen versturen via DANE (zorgt voor een validatie van de mailserver).

Het is hierbij ook mogelijk om de ntamx server in het NTA 7516 record leeg te laten. Dan moet de MX server van het domein worden gebruikt, mits deze voldoet.

2. *Bijlage B:* het ontvangende domein heeft geen DNSSEC, maar wel een NTA 7516 record waaruit de (gecertificeerde) provider kan worden achterhaald. Berichten worden dan verstuurd naar de bekende mailserver van de provider.

3. *Bijlage C:* het ontvangende domein heeft wel DNSSEC en kan dus gevalideerd worden, maar de ntamx mailserver ondersteunt geen DANE. Berichten worden dan verstuurd naar de MX server van het domein, mits deze voldoet aan de veiligheidseisen.

In alle gevallen moet de MX server in EU/EER grondgebied staan.

AVG

Het AVG kanaal kan optioneel worden gebruikt als alternatief voor NTA 7516. Het verschil met NTA 7516 is dat er geen sprake is van een NTA 7516 record. Bastion 365 kijkt dan naar de mailserver(-s) van het ontvangende domein. Indien deze voldoet met verder dezelfde veiligheidsinstellingen als de NTA 7516 (inclusief de twee variaties) kan het bericht veilig worden verstuurd en moet dus bijvoorbeeld ook de mailserver op EU/EER grondgebied staan.

Kortom, wat bij het AVG kanaal ontbreekt ten opzichte van de NTA 7516 is de declaratie dat er MFA op de werkplek is geïmplementeerd middels het NTA 7516 record.

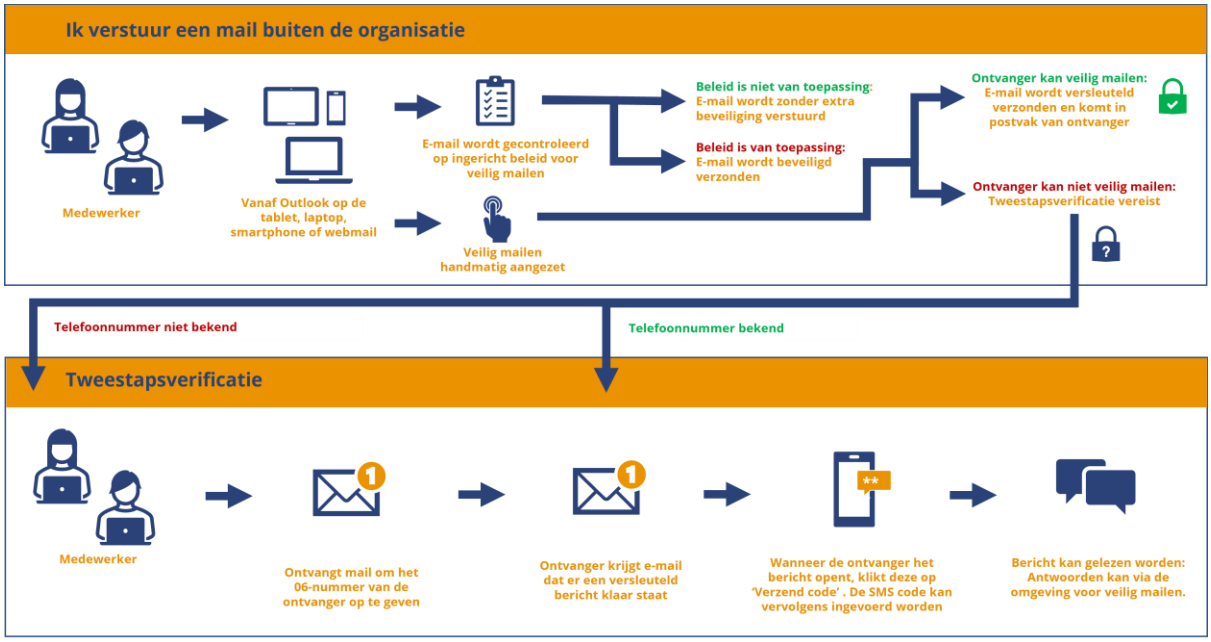
Het voordeel van dit kanaal is dat er minder gevraagd wordt om telefoonnummers. Indien het domein van de ontvanger een technisch valide mailserver heeft kan het bericht veilig worden verstuurd.

eDelivery

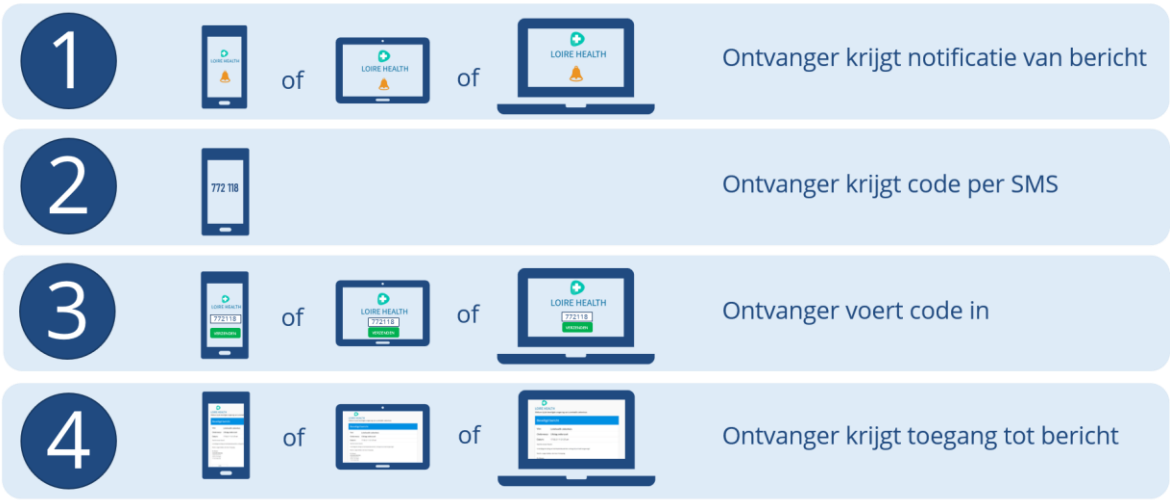
eDelivery is het MFA portaal van Bastion 365. Dit wordt gebruikt als de mailserver van de ontvanger niet voldoet aan de veiligheidseisen en als de mailserver zich bijvoorbeeld ook buiten de EU/EER zone kan bevinden.

Om toegang te geven tot het bericht in een portaal, is het nodig om een mobiel nummer op te geven waarnaar een SMS code kan worden gestuurd. De verzender zal in dat geval een verzoek krijgen om een telefoonnummer op te geven voor de ontvanger.

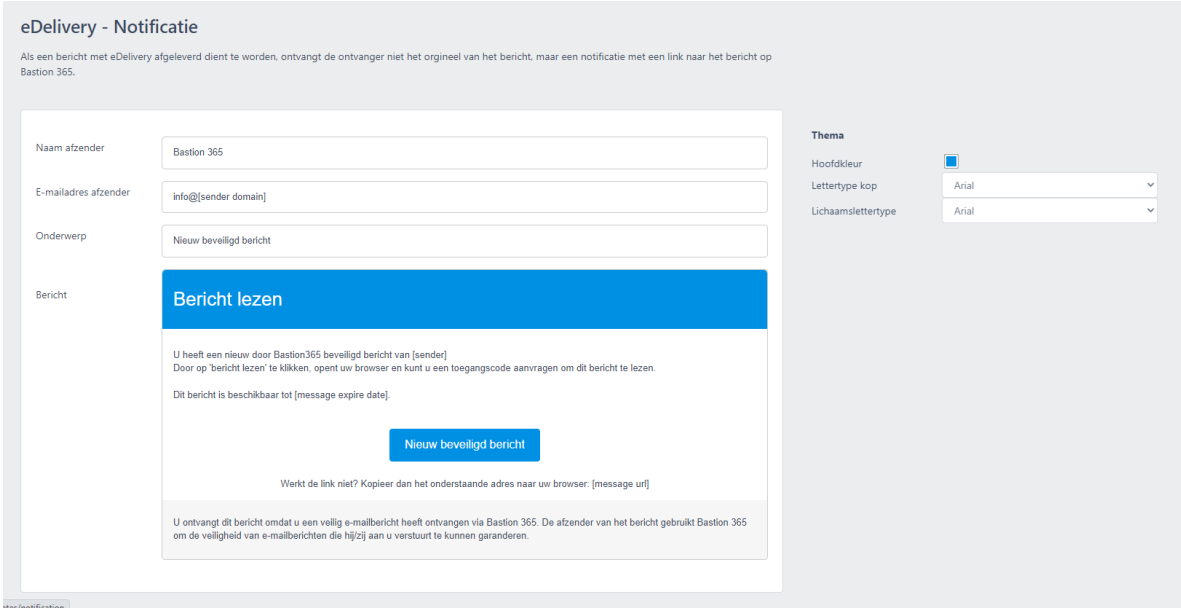
De ontvanger krijgt dan een notifcatie e-mail dat er een veilig bericht klaarstaat in het portaal met een link daarnaartoe. Via deze link kan hij een toegangscode aanvragen die dan per SMS wordt toegestuurd. Na ingave van de toegangscode in het portaal krijgt de ontvanger toegang tot het mailbericht.



De ontvanger heeft verder geen speciale inrichting nodig en de oplossing is niet afhankelijk van de mail-client of mailprovider die de verzender gebruikt.



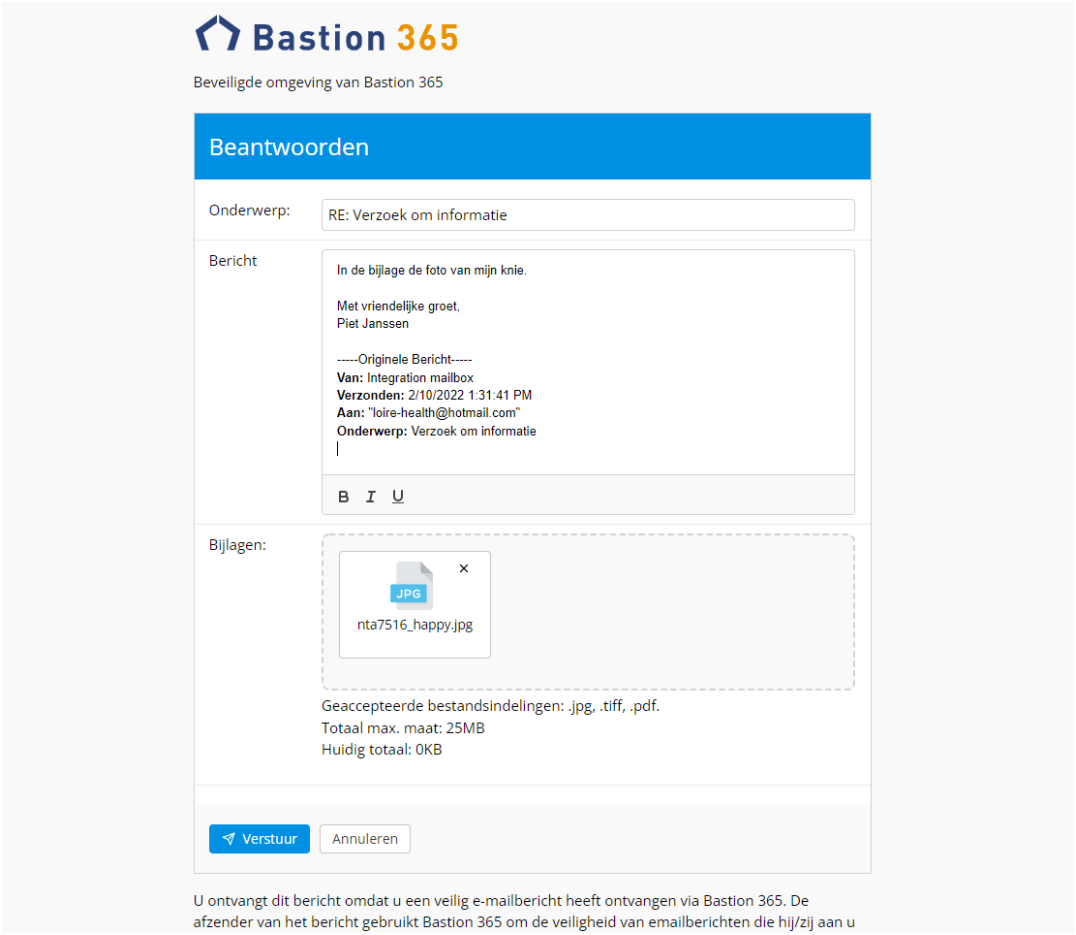
Het eDelivery portaal en de notificaties naar de ontvanger zijn in Bastion 365 in hoge mate inrichtbaar, zodat u deze kunt afstemmen op uw behoeftes.



Ook de notificaties naar uw medewerkers, zoals de vraag om telefoonnummers, de leesbevestiging, ingetrokken berichten of dat de ontvanger aangeeft dat het telefoonnummer niet klopt, kunt u aanpassen door ze bijvoorbeeld te voorzien van extra instructies die gelden voor uw organisatie.

U kunt ook inrichten hoe lang berichten die via eDelivery zijn afgeleverd, moeten worden bewaard. Het minimum is 30 dagen en het maximum is 90 dagen.

Het is tevens inrichtbaar of u wilt toestaan dat de ontvangers ook veilig een antwoord kunnen terugsturen en of zij het antwoord kunnen voorzien van een bijlage.

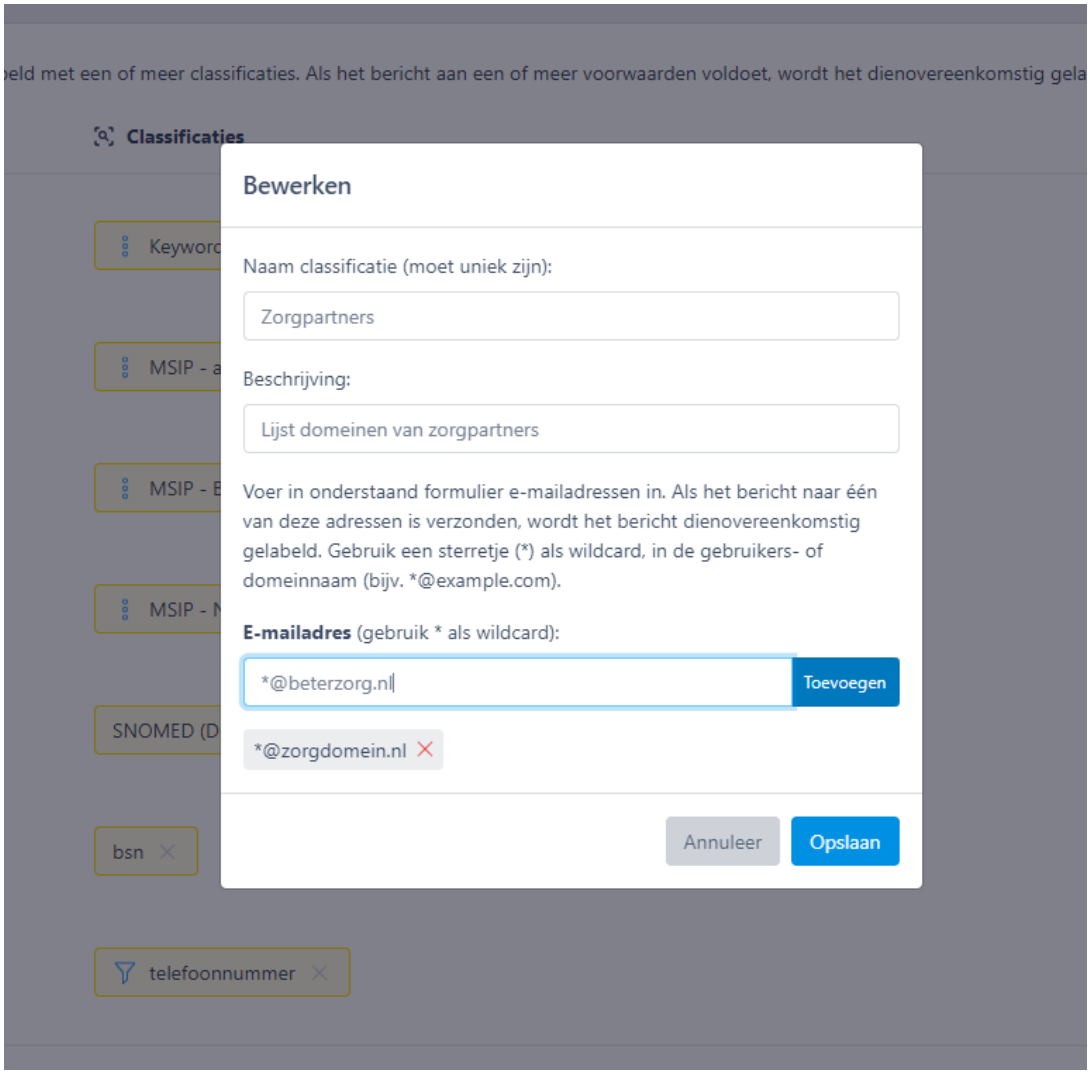

Bastion 365
Beveiligde omgeving van Bastion 365
Beantwoorden
Onderwerp:
RE: Verzoek om informatie
Bericht
In de bijlage de foto van mijn knie.
Met vriendelijke groet,
Piet Janssen
-----Originele Bericht-----
Van: Integration mailbox
Verzonden: 2/10/2022 1:31:41 PM
Aan: "loire-health@hotmail.com"
Onderwerp: Verzoek om informatie
Bijlagen:
JPG
nta7516_happy.jpg
Geaccepteerde bestandsindelingen: .jpg, .tiff, .pdf.
Totaal max. maat: 25MB
Huidig totaal: 0KB
Verstuur
Annuleren
U ontvangt dit bericht omdat u een veilig e-mailbericht heeft ontvangen via Bastion 365. De
afzender van het bericht gebruikt Bastion 365 om de veiligheid van emailberichten die hij/zij aan u

WELKE E-MAILBERICHTEN WORDEN VIA NTA 7516 VERZONDEN?

In Bastion 365 kan ingericht worden welke e-mailberichten via een veilige route moeten worden verstuurd. Hierbij heeft men diverse mogelijkheden om te bepalen welke berichten geclassificeerd kunnen worden als berichten met gevoelige informatie.

Bepaalde ontvangers

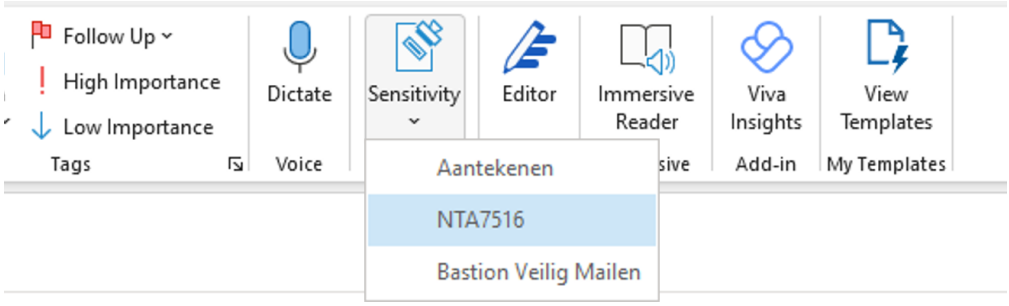
Als u weet dat e-mailberichten naar bepaalde ontvangende domeinen altijd veilig moeten worden verstuurd, kunt u gebruikmaken van de TO classifier in Inspector.



U kunt vervolgens aangeven wat de gewenste veilige route is voor deze domeinen.

Sensitivity labels

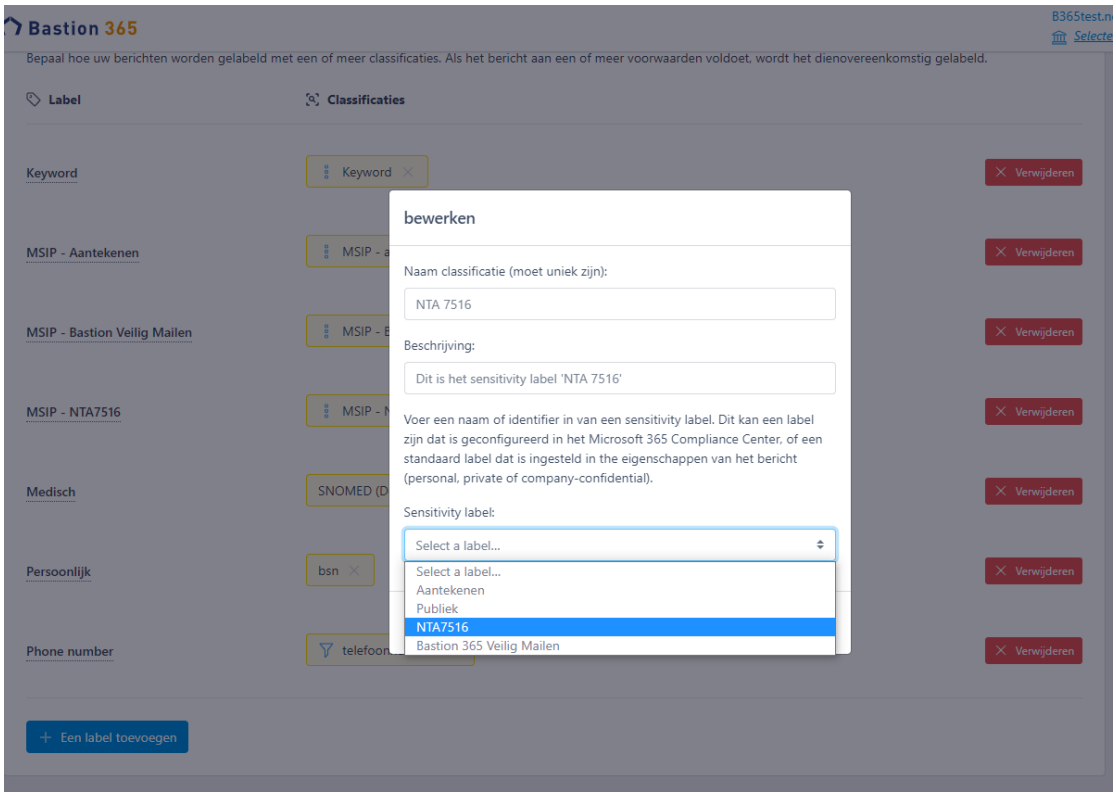
Om ervoor te zorgen dat gebruikers in staat zijn om zelf in Outlook een veilig bericht te initiëren moet u sensitivity labels activeren in Microsoft 365. Welke dit moeten zijn, is iets wat uw organisatie zelf moet bepalen. Het is echter aangeraden om de lijst met mogelijkheden te beperken tot wat er echt nodig is om gebruikers niet te verwarren.



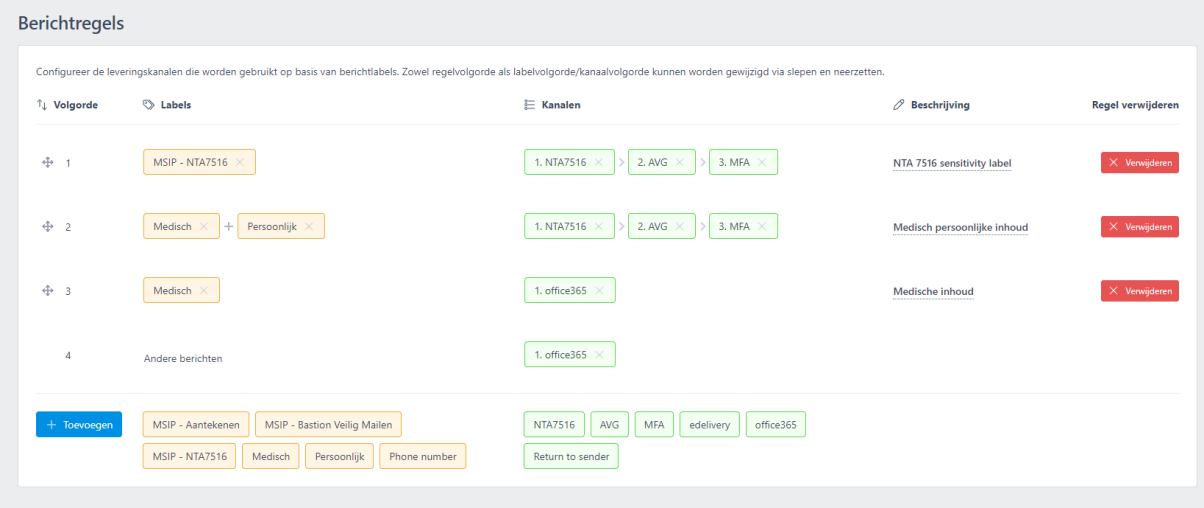
Als de gebruiker dit sensitivity label zet of wanneer er een bijlage wordt gekoppeld die dit label bevat, zal het bericht conform NTA 7516 worden verstuurd.

Zie voor het inrichten onze handleiding ***Sensitivity labels inrichten in Microsoft 365.***

In Bastion 365 kan men vervolgens het sensitivity label koppelen.



Nu het label is ingericht, kan er bepaald worden welke kanalen van toepassing zijn.

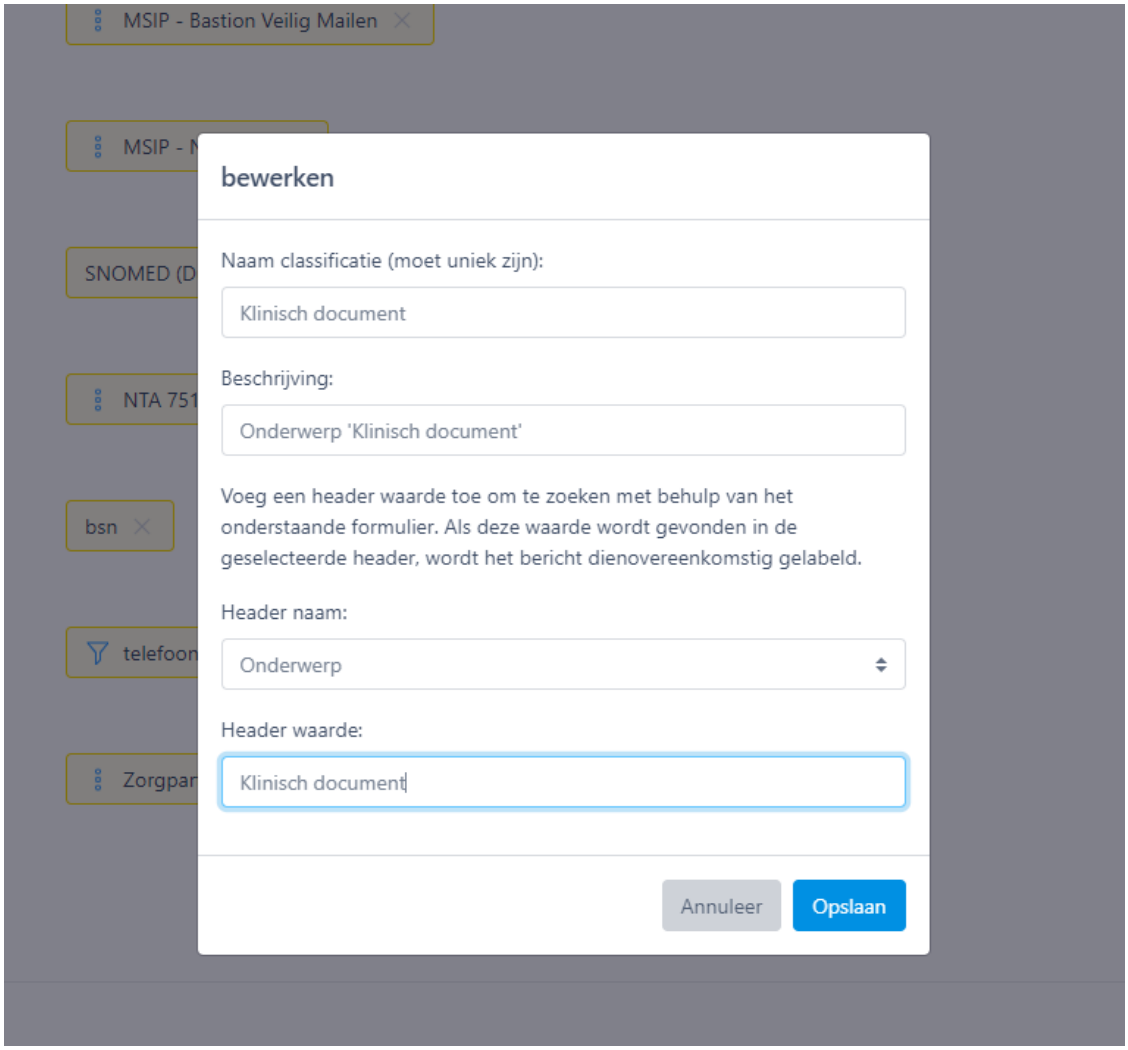


In het bovenstaande voorbeeld wordt als eerste gekeken in Bastion 365 of het NTA 7516 sensitivity label is gezet in het bericht. Deze berichten zullen dan via NTA 7516, AVG compliant (optioneel) of via MFA verstuurd afhankelijk van waar de ontvanger aan voldoet.

Scan of klik op de QR code hierboven voor meer informatie over sensitivity labels toewijzen aan Microsoft 365 groepen in Azure Active Directory

Berichtkopregels

U kunt ook op basis van de kopregels van een e-mailbericht detecteren of een bericht veilig verzonden moet worden. Het gaat dan om kopregels als verzender, ontvanger, onderwerp of andere kopregels die in uw organisatie gebruikt worden.



Berichtinhoud

Bastion 365 heeft diverse mogelijkheden voor het detecteren van gevoelige inhoud in berichten en bijlagen. Deze kunnen worden gebruikt om te bepalen wat voor soort informatie onder gevoelige inhoud valt.

Woordenboeken
In Bastion 365 beschikt u over zorgsector specifieke woordenboeken, zoals de Nederlandstalige SNOMED bibliotheek of de DSM-5 voor termen in de geestelijke gezondheidszorg.

Trefwoorden
Naast de woordenboeken kunt u ook eenvoudig zelf een lijst met in uw organisatie gebruikte trefwoorden samenstellen of importeren.

Personal identifiers

Om te bepalen of het bericht ook persoonsgebonden informatie bevat, kunt u gebruikmaken van een aantal identificatie classifiers.

Adres
Bestaande Nederlandse straatnaam (zoals in de BAG opgevoerd) gevolgd door een huisnummer.

BSN (Burgerservicenummer)
Detecteert het Nederlandse burgerservicenummer. Een cijfer van een lengte van 8 of 9 dat de ‘elfproef’ validatie doorstaat.

ID of paspoort nummer
Detecteert de termen 'paspoort', 'identiteitskaart', 'identiteitsbewijs', 'id-kaart', 'legitimatie', 'verblijfsvergunning', 'w-document', gevolgd door 6 cijfers gevolgd door een cijfer. De letter ‘O’ wordt niet gebruikt.

Detecteert ook de termen 'rijbewijs' of 'rijvaardigheidsbewijs' gevolgd, door een rijbewijsnummer van 10 cijfers.

Phonenumber
Detecteert .een mogelijk telefoonnummer. Hierbij wordt gebruik gemaakt van de Google telefoonnummer functie om vast te stellen dat het om een telefoonnummer gaat.

Postal code (Dutch)
Detecteert het als er een combinatie is van 4 cijfers en twee letters.

Bijlagen

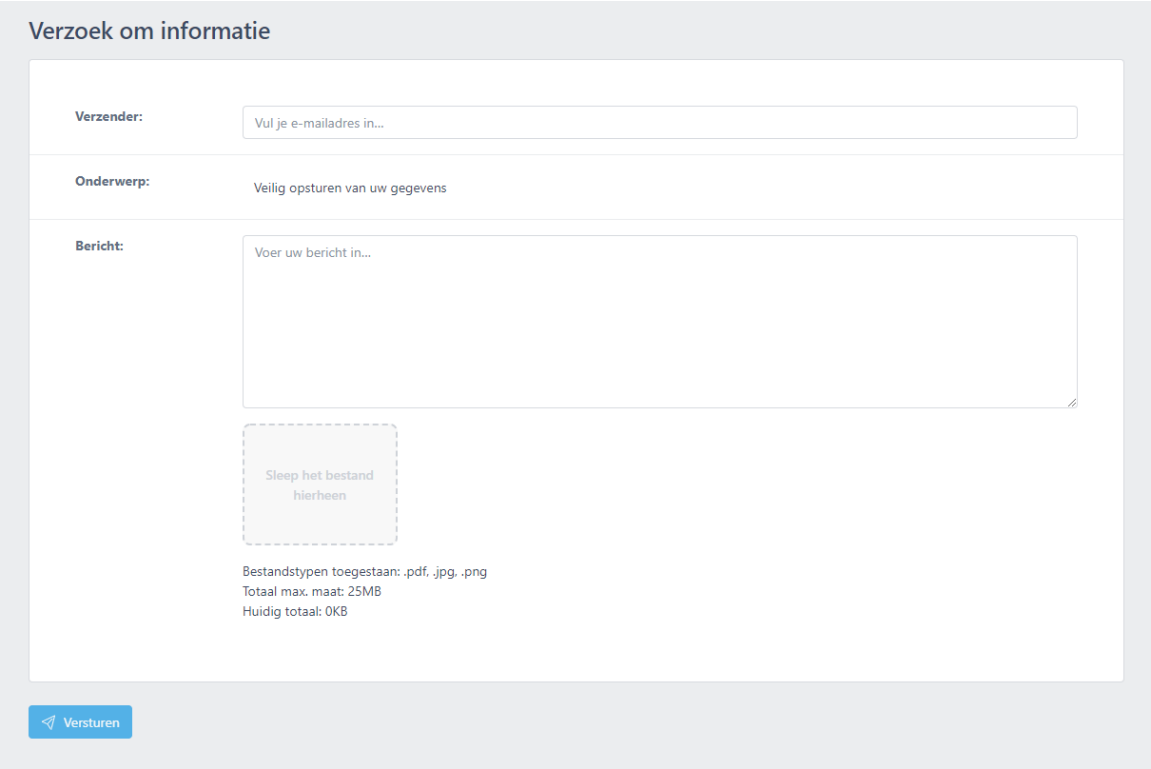
Bastion 365 kan ook bijlagen detecteren die in de zorgsector vaak worden gebruikt, zoals DICOM, Edifact, Fhir en HL7 bestanden.

Met een wachtwoord versleutelde bijlagen
Het kan wenselijk zijn om voor bijlagen die met een wachtwoord zijn beveiligd extra (of juist minder) maatregelen te treffen voor de beveiliging. Met deze classifier worden alle PDF of Office documenten die met een wachtwoord zijn beveiligd gedetecteerd.

Onleesbare bijlagen
Het kan om uiteenlopende redenen zo zijn dat een bijlage niet door Bastion 365's Inspector kan worden gescand, als wachtwoord beveiliging niet de reden is waarom het bestand niet kan worden geinspecteerd. Naast dat Bastion 365 dan niets kan zeggen over de inhoud van het bestand, kan het zo zijn dat het misschien onwenselijk is om bijvoorbeeld een encrypted bestand te delen.

VEILIG E-MAILS ONTVANGEN VAN CLIËNTEN EN MANTELZORGERS

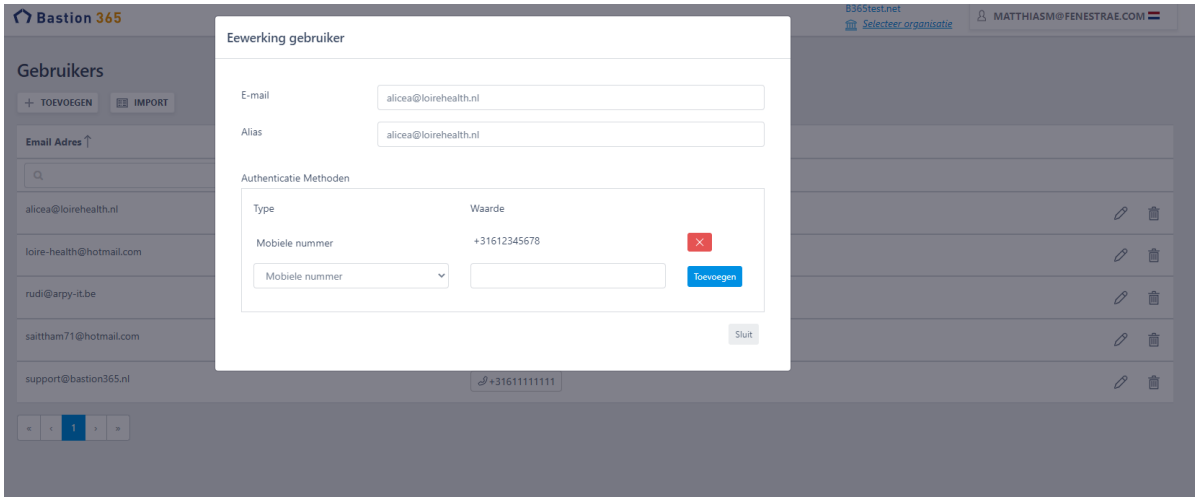
Om ervoor te zorgen dat cliënten en mantelzorgers ook veilig e-mails kunnen sturen naar uw organisatie, kunt u in Bastion 365 een berichtenformulier inrichten dat u vervolgens op uw website kunt plaatsen.



Hiermee kunnen cliënten en mantelzorgers ook bijlagen meesturen. U kunt inrichten in welke mailbox van uw organisatie de berichten veilig moeten worden afgeleverd.

ADRESSENBEHEER

Voor alle ontvangers van eDelivery berichten wordt de combinatie e-mailadres en telefoonnummer (-s) centraal opgeslagen.



U kunt in het configuratieportaal van Bastion 365 telefoonnummers bij een e-mailadres verwijderen of juist meerdere toevoegen of importeren.

Indien er meerdere telefoonnummers zijn ingevoerd bij een e-mailadres, kan de ontvanger kiezen op welk telefoonnummer de toegangscode per SMS ontvangen kan worden.

BIJLAGE A: VERKLARING VAN IN- EN UITSLUITINGEN NTA 7516 VOOR BASTION 365

Criterium	Van toepassing (Ja/Nee)	Toelichting (optioneel)
6.1.2 Minimale beschikbaarheid	Ja	• Bastion 365 heeft een beschikbaarheid van minimaal 99,8% per jaar, voor wat betreft het ontvangen en verwerken van berichten. • Uitval van Bastion 365 of een van zijn componenten zal niet leiden tot een andere - onveilige - methode van het versturen van een e-mail.
6.1.3 Maximale uitvalduur	Ja	• De maximale uitvaltijd van Bastion 365 bedraagt 24 uur, gerekend vanaf het moment van versturen vanuit de aangesloten (Exchange) server.
6.1.4 Maximaal gegevensverlies	Ja	• Bastion 365 zal niet bijdragen aan gegevensverlies vanaf het moment dat een bericht is ontvangen.
6.1.5 Herkomstbevestiging	Ja	• Bastion 365 voorziet het bericht van een DKIM signature en toont daarmee aan dat het bericht is verstuurd vanuit een beveiligd domein. • Door DMARC juist te implementeren en te verifiëren, is misbruik van domeinnamen bij het e-mailbericht uitgesloten. • Binnen Microsoft 365 zijn er meerdere mogelijkheden voor multi-factor authenticatie voor de client. Dit moet door de beheerder van de professional worden ingericht.

6.1.6 Data-integriteit	Ja	• Er worden geen aanpassingen of toevoegingen gedaan aan de inhoud van het originele bericht door Bastion 365. Bastion 365 voorziet het e-mailbericht van een NTA 7516 header en ondertekent het bericht vóór het versturen, conform de richtlijnen van NTA 7516. • Het transport van het e-mailbericht is beveiligd via TLS.
6.1.7 Onweerlegbaarheid verzender	Ja	• SPF wordt toegepast op alle relevante domeinnamen én op alle ontvangende e-mailservers conform de NTA 7516 richtlijnen. Hiermee wordt bevestigd dat het e-mailbericht wordt verstuurd door een legitieme mailserver. • Bastion 365 voorziet het bericht van een DKIM signature en toont daarmee aan dat het bericht is verstuurd vanuit een beveiligd domein. • Door DMARC juist te implementeren en te verifiëren, is misbruik van domeinnamen bij het e-mailbericht uitgesloten. • De inrichting van de verzender wordt via Microsoft 365 gedaan. Hierbij moet sprake zijn van multi-factor authenticatie. Dit moet door de beheerder van de professional worden ingericht.
6.1.8 Autorisatie verzender	Ja	• Autorisatie van de verzendende medewerkers vindt plaats in Microsoft 365/Azure.

6.1.9 Gegevensvertrouwelijkheid	Ja	• Door een combinatie van technische implementaties (zoals gespecificeerd in NTA 7516) wordt gegarandeerd dat veilig verkeer tussen Bastion 365 en de ontvangende mailserver kan plaatsvinden. • Tijdens het transport worden berichten versleuteld via TLS. • Binnen Bastion 365 worden berichten versleuteld opgeslagen en alleen bewaard zolang nodig is voor het bezorgen van het e-mailbericht.
6.1.10 Toegangsvertrouwelijkheid	Deels	• De inrichting van de ontvangende client wordt via Microsoft 365 gedaan. Hierbij moet sprake zijn van multi-factor authenticatie. Dit moet door de beheerder van de professional worden ingericht. • Ontvangers die niet voldoen aan NTA 7516 ontvangen het bericht via een met twee factor login beveiligd portal. De ontvanger moet met een SMS code zijn identiteit bevestigen.
6.1.11 Communicatievertrouwelijkheid	Ja	• Gedurende het transport is het bericht encrypted via TLS en is het daarmee niet leesbaar voor onbevoegden.
6.1.12 Verzendingsgrond	Nee	• Het beleid en toezien op correcte uitvoering van dat beleid ligt bij de organisatie van de professional.
6.1.13 Internationaal ad-hocberichtenverkeer	Ja	• Door de toepassing en verificatie van STARTTLS, SPF en DKIM wordt het berichtenverkeer voldoende beveiligd gedurende het transport. • Er worden geen berichten verstuurd buiten de EU/EER zone.

6.1.14 Continuïteit van ad-hocberichtenverkeer - beantwoorden	Ja	• Een ontvanger van een bericht in het veilige portaal kan deze ook beantwoorden en bijvoorbeeld voorzien van een bijlage.
6.1.15 Continuïteit van ad-hocberichtenverkeer - doorsturen	Ja	• Het is mogelijk om berichten in het veilige berichtenportaal te downloaden en door te sturen. • Doorsturen is voor verantwoordelijkheid van de betreffende persoon.
6.1.16 Veiligheid als gemak	Ja	• Al het berichtenverkeer dat via Bastion 365 gaat, is veilig conform de definities van NTA 7516. • Het is aan de organisatie van de professional om te bepalen welk berichtenverkeer via Bastion 365 gaat. • Gebruikers kunnen zelf veilige berichten initiëren • Berichten en bijlagen kunnen worden onderzocht op medische en persoonlijke informatie om te voorkomen dat er ongewenst toch iets onveilig wordt verstuurd.
6.1.17 Leesbaarheid	Ja	• De professional kan gebruik maken van zijn bestaande e-mail client-software in Microsoft 365. Er zijn geen plugins of andere extra technische voorzieningen vereist. • De (twee factor) authenticatie van de persoon voor het veilige berichtenportaal vereist geen registratie of technische implementaties. • Het berichtenportaal voldoet aan de eisen van EN 301 549.

6.1.18 Eigen kopie	Ja	• In de door Microsoft 365 ter beschikking gestelde e-mail client-software is het mogelijk om berichten (beveiligd) op te slaan. • In het veilige berichtenportaal van Bastion 365 is het mogelijk om berichten en bijlagen op te slaan.
6.1.19 Dossierkoppeling	Deels	• De dossierkoppeling valt niet binnen de scope van Bastion 365. Maar wordt er ook niet door beperkt door in de implementatie.
7.2 Multikanaalcommunicatie	Ja	• Bastion 365 zal elk ad-hocbericht verwerken conform NTA 7516, mits de (mailprovider van de) ontvanger voldoet aan de technische eisen van de norm. • Indien uit de verificaties van Bastion 365 blijkt dat de ontvanger niet voldoet aan de technische eisen van NTA 7516 zal het ad-hocbericht beschikbaar worden gesteld in het veilige berichten portaal.

BIJLAGE B: OVERZICHT FEATURES BASTION 365 R2

BEHEER	Inloggen met Azure AD
	Meerdere domeinen inrichten
	Berichten worden verstuurd vanaf eigen domein
	Validatie domein(-en)
	Eigen gebruiker beheer
	Data wordt opgeslagen in EU/EER
	Eigen storage kunnen gebruiken voor MFA berichten
	Transactielogs
MICROSOFT 365	Geen plugin's
	Werkt met alle Outlook versies en devices
	Script generator voor eenvoudige Exchange integratie
	Functionele & shared mailboxen
VEILIG MAILEN	Gasten kunnen veilige berichten via eigen website initiëren
	NTA 7516 - berichten versturen
	• NTA 7516 - bijlage B (geen DNSSEC)
	• NTA 7516 - bijlage C (geen DANE)
	NTA 7516 - berichten ontvangen van alle NTA 7516 mailproviders
	Alternatieve veilige route als ontvanger niet voldoet aan NTA 7516
	DKIM handtekening
	Aanmaken eigen veilige kanalen
	Bepalen hiërarchie van veilige kanalen
	Routering naar meest passende veilige kanaal
	Veilig mailen vanuit applicatie
GROTE BESTANDEN	Veilig grote bestanden versturen (tot 2GB)
	Veilig grote bestanden ontvangen (tot 2GB)
EXTRA ZEKERHEDEN	Digitaal afleverbericht
	Digitaal afleverbewijs
DIGITALE HANDTEKENING - CAdES	Eigen certificaat
	Integriteit
	Authenticatie
	Juridisch onweerlegbaar
MULTI-FACTOR AUTHENTICATIE	Ontvangers kunnen veilig berichten beantwoorden (met bijlagen)
	Ondersteunde bijlagen bij beantwoorden
	Keuze eigen SMS provider
	Bewaartermijn inrichten

	Ontvanger kan bericht opslaan (en doorsturen)
	Inrichtbaar met eigen tekst en huisstijl
	Notificatie (ontvanger) dat een veilige mail is verstuurd
	Notificatie (verzender) dat het telefoonnummer niet klopt
	Notificatie (verzender) dat ontvanger het bericht heeft gelezen
	Notificatie (verzender) dat het bericht is verlopen
	Notificatie (verzender) bij intrekken bericht
	Notificatie (ontvanger) bij intrekken bericht
	Gebruikers hebben overzicht verstuurde berichten
	Gebruikers kunnen eigen berichten terugtrekken
	Adressenbeheer
	Import 06 nummers
	Meerdere 06 nummers bij email adres
AUTOMATISCHE HERKENNING	Sensitivity label in Outlook bericht
	Bijlagen inspecteren
	Bijlagen herkennen (bijv. PDF, EDIFACT, HL7, FHIR, Microsoft Office, Open Office)
	Trefwoorden in bericht
	Zoeken in onderwerp
	Lijst met geadresserden
	Sector specifieke woordenboeken
	Burgerservice nummer
	Andere personal identifiers (PID)
	PDF, Office, OpenOffice, XML
	HL7, EDIFACT, CDA, FHIR
	Eigen classifiers maken
	Microsoft DLP labelling

BIJLAGE C: VEILIGE E-MAIL STANDAARDEN

Veilig e-mailen is meer dan encryptie. Encryptie maakt alleen de overdracht tussen twee eindpunten veiliger. Als een van de twee eindpunten kan worden misleid of vervalst, zullen de gegevens beveiligd naar een onbedoeld kanaal stromen en nog steeds in verkeerde handen vallen. Dit betekent dat beveiligde e-mail niet alleen om beveiliging gaat, maar ook om het valideren of de twee eindpunten (zender en ontvanger) zijn wie ze beweren te zijn. Dit wordt bereikt door een combinatie van een aantal beveiligings- / authenticatiemaatregelen:

DNSSEC (Domain Name System Security Extensions)

De DNS van een domein wordt gebruikt om "mensvriendelijke" domeinnamen (zoals microsoft.com) te vertalen naar "machinevriendelijke" IP-adressen (zoals 192.0.578.4) die via internet kunnen worden gerouteerd. De authenticatie van beiden is onmogelijk in een gewone DNS.

DNSSEC maakt gebruik van digitale handtekeningen om de herkomst en integriteit van de ontvangen gegevens te verifiëren. Bastion 365 controleert dan ook als eerste of het domein van de ontvanger DNSSEC heeft, zodat het zeker weet dat informatie verkregen van dat DNS ook betrouwbaar is, zoals bijvoorbeeld het NTA 7516 record.

STARTTLS

Met STARTTLS laat de e-mailclient de e-mailserver weten dat de verbinding moet worden opgeschaald naar een beveiligde verbinding via TLS.

DANE (DNS-based Authentication of Named Entities)

DANE maakt het mogelijk om een extra verificatiebron te zoeken, door een TLSA-certificaat te publiceren waarmee klanten kunnen verifiëren of de TLS-informatie overeenkomt met de informatie die via HTTPS wordt gepubliceerd. Als het overeenkomt, kan de afzender er zeker van zijn dat het eindpunt correct is en dat de gegevens kunnen worden overgedragen. DANE wordt afgehandeld via Bastion 365.

De combinatie DNSSEC / DANE / STARTTLS zorgt er in hoge mate voor dat een veilige verbinding tussen verzender en ontvanger van een e-mail tot stand kan worden gebracht. Dit gebeurd door het domein te valideren en pas het e-mailbericht te verzenden als de validatie is geslaagd.

SPF (Sender Policy Framework)

Met SPF kan de e-mailserver van de ontvanger controleren of een e-mail die beweert afkomstig te zijn van een specifiek domein, is verzonden door een IP-adres dat is geautoriseerd door de beheerders van dat domein. De lijst met geautoriseerde mailservers voor het domein wordt gepubliceerd in een zgn. SPF-record.

DKIM (Domain Keys Identified Mail)

Met DKIM wordt een handtekening in de e-mail geplaatst, waarmee de ontvanger kan controleren of een e-mail inderdaad is verzonden en geautoriseerd door de eigenaar van dat domein. Bastion 365 ondertekent een NTA 7516 bericht voordat deze wordt verstuurd.

DMARC (Domain-based Message Authentication, Reporting & Conformance)

Een DMARC-beleid stelt de afzender in staat om aan te geven dat hun berichten worden beschermd door SPF en/ of DKIM en vertelt een ontvanger wat te doen als geen van deze authenticatiemethoden slaagt. Om als veilig te worden beschouwd, moet dit beleid worden ingesteld op ‘reject’ (zorgt ervoor dat alle potentieel schadelijke e-mail wordt gestopt) of ‘quarantaine’ (ontvangt de e-mail die de DMARC-verificatiecontrole niet doorstaat, maar behandelt deze met extra voorzichtigheid).

De e-mails die worden verzonden en ontvangen door een mailprovider die ze valideert, worden als veilig beschouwd als alle bovenstaande standaarden correct zijn geïmplementeerd.

BIJLAGE D: INTEROPERABILITEIT

Een belangrijk onderdeel van de NTA 7516 is de interoperabiliteit tussen mailproviders. In eerste instantie is de NTA 7516 standaard juist opgezet om ad-hoc veilig en gemakkelijk te communiceren zodat er buiten de voorwaarden van de NTA 7516 geen aanvullende eisen mogen worden gesteld. Bastion 365 voldoet hier volledig aan en stelt geen enkele aanvullende eisen aan het versturen en ontvangen van NTA 7516 berichten.

Inkomende berichten

Bastion 365 weigert geen inkomende berichten van andere mailproviders. Zelfs als deze niet (helemaal) aan de NTA 7516 voldoen. De inkomende berichten worden niet aangepast.

Het is wel mogelijk om berichten te voorzien van een banner in Outlook, zodat herkenbaar is dat deze als NTA 7516 berichten zijn binnengekomen of dat er bijvoorbeeld juist iets niet klopt.

Uitgaande berichten

Bastion 365 stuurt NTA 7516 berichten onaangepast naar alle gecertificeerde NTA 7516 mailproviders zonder aanmelding, certificaatuitwisselling of andere voorwaarden. Sommige NTA 7516 mailproviders hebben hier echter wel bepaalde voorwaarden, maar wij hebben met deze providers wel op hun voorwaarden interoperabiliteit bereikt. Hieronder zijn enkele uitzonderingsgevallen opgevoerd die voor kunnen komen:

Zorgmail

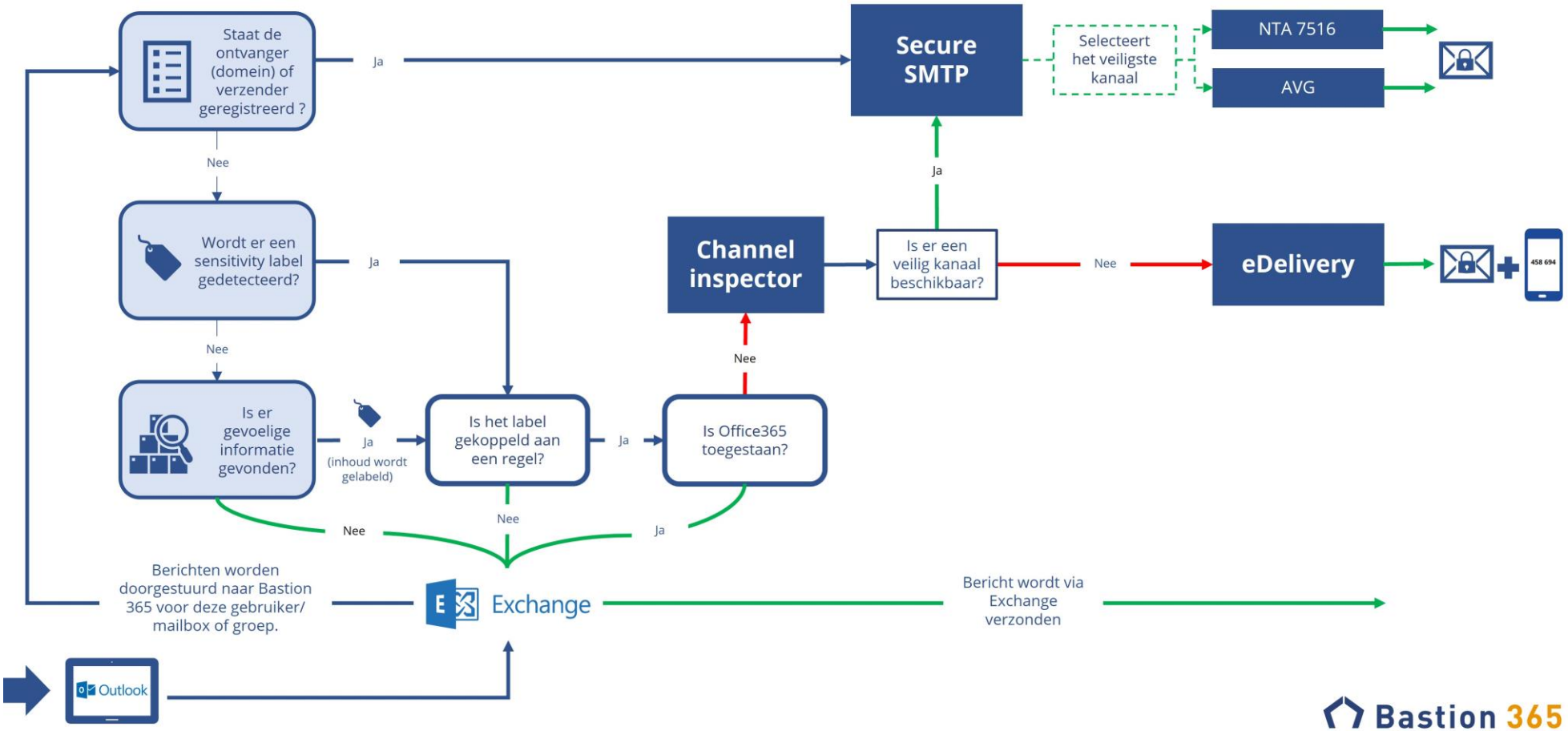
Domein met Zorgmail als NTA 7516 provider
Of dit ontvangende domein met een NTA 7516 record ook een NTA 7516 bericht kan ontvangen, hangt er (ook) van af of de betreffende organisatie de NTA 7516 verklaring hebben getekend met Zorgmail. Het is mogelijk dat er wel een NTA 7516 record aanwezig is op een domein, maar dat het domein toch geen NTA 7516 berichten kan ontvangen. Voordat hier teruggevallen wordt op een eDelivery bericht, kan er ook gepoogd worden om een bericht via het AVG kanaal te sturen om te voorkomen dat er telefoonnummers moeten worden ingevoerd.

@zorgmail.nl adres
Bij @zorgmail e-mailadressen is het niet mogelijk om een NTA 7516 record op te vragen, omdat het een generiek domein betreft. Gebruikers van @zorgmail.nl adressen kunnen wel een NTA 7516 overeenkomst tekenen, zodat zij wel berichten van buiten het Zorgmail domein kunnen ontvangen. Indien dit niet het geval is, wordt er in Bastion 365 om een telefoonnummer gevraagd.

Zivver

Bij Zivver als NTA 7516 provider wordt er geen NTA 7516 MX server aangegeven in het record en dient de mailserver van het domein (de MX server) te worden gebruikt om NTA 7516 berichten af te leveren. Dit mag volgens de NTA 7516, maar het kan er wel voor zorgen dat een bericht toch niet via NTA 7516 kan worden afgeleverd. Dit komt omdat de mailserver zich bijvoorbeeld buiten de EU/EER bevindt. Er zal dan toch uiteindelijk op een eDelivery bericht moeten worden teruggevallen en om een telefoonnummer worden gevraagd.

SCHEMA 1: Bastion 365 proces



Bastion 365

SCHEMA 2: Inrichting

DNS	Microsoft 365			Bastion 365		
	Azure	Outlook	Exchange	**Inrichting**	**Inspector**	**MFA portaal**
Domein is DNSSEC	MFA toegang op de werkplek	Gebruiker heeft toegang tot e-mail	Connectors	Profiel Dataopslag Gebruikers	Berichtlabels - Inrichten bericht classificaties - Inrichten personal identifiers - Inrichten termen - Eigen classificaties	Bewaartermijn Beantwoorden toestaan - met bijlagen - toegestaane bijlagen SMS - provider - naam afzender - bericht
NTA 7516 TXT record aanmaken	Beleid voor toegang tot gevoelige informatie	Gebruiker mag gevoelige informatie delen	Mail flow rules	Beheerders toevoegen / verwijderen	Bericht regels	Portal huisstijl en teksten
Bastion 365 toevoegen in SPF	Sensitivity labels inrichten voor de organisatie	Gebruiker kan sensitivity label op bericht zetten of bijlage kan label bevatten		Domeinen inrichten en valideren	Beveiligde kanalen	Notificaties huisstijl en teksten
DKIM selectors aanmaken				Scripts for connectors en mailflow rules genereren		Mail forms
DMARC policy inrichten						