Bastion 365

VERKLARING IN- EN UITSLUITINGEN

NTA 7516

CRITERIA VOOR COMMUNICATIE DIENSTENAANBIEDERS

VERSIE: 2.1

31/1/2022

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 versturen van een e-mail.
6.1.3 Maximale uitvalduur	Ja	• De maximale uitvaltijd van Bastion 365 bedraagt minimaal (??) 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 ondertekend het bericht vóór het versturen, volgens 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 volgens 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 portaal. De ontvanger moet met een code per SMS zijn identiteit bevestigen.

6.1.11 Communicatievertrouwelijkheid	Ja	• Gedurende het transport is het bericht encrypted via TLS en is 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-hoc berichtenverkeer	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-hoc berichtenverkeer - 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-hoc berichtenverkeer - 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 Dossier koppeling	Deels	• De dossierkoppeling valt niet binnen de scope van Bastion 365, maar wordt ook niet erdoor beperkt in de implementatie.
7.2 Multi kanaalcommunicatie	Ja	• Bastion 365 zal elk ad-hoc bericht verwerken volgens NTA 7516, mits de (mailprovider van de) ontvanger voldoet aan de technische eisen van de norm. • Als uit de verificaties van Bastion 365 blijkt dat de ontvanger niet voldoet aan de technische eisen van NTA 7516 zal het ad-hoc bericht beschikbaar worden gesteld in het veilige berichten portaal.