Programma van Eisen

NTA 7516

Jouw organisatie dient zelf een overzicht op te stellen van de minimale eisen (grenswaarden) en de onderbouwing daarvan voor de in de norm genoemde criteria. Dit betreft de paragrafen 6.1.2 - 6.1.19. Wij hebben alvast een programma van eisen voor je opgesteld dat je als uitgangspunt kunt gebruiken voor jouw organisatie. Een programma van eisen is onmisbaar bij het selecteren van een leverancier en een dienst, maar blijft ook nadat het selectieproces is afgerond relevant. De NTA schrijft voor dat jaarlijks de geschiktheid van de geselecteerde en geïmplementeerde communicatiemogelijkheden wordt vergeleken met de criteria die daarvoor zijn vastgelegd en elke twee jaar de vastgelegde criteria worden beoordeeld op geschiktheid en passendheid.

Onderdeel NTA 7516	Element	Eis/wens
6.1.2	Hoeveel tijd per jaar (in %) moet er gecommuniceerd kunnen worden?	Minimaal 99,8% per jaar.
6.1.3	Hoelang mag ad-hocberichtenverkeer onafgebroken onbeschikbaar zijn?	Maximaal 24 uur.
6.1.4	Hoeveel gegevens mogen er in het ad-hocberichtenverkeer verloren raken?	Tenzij de verzender binnen 24 uur na verzending wordt geïnformeerd over (mogelijk) gegevensverlies, is geen enkel gegevensverlies vanaf de verzendende client-software en de technische infrastructuur acceptabel.
6.1.5	Hoe zeker weet de ontvanger dat de afzender daadwerkelijk is wie zij/hij zegt dat hij is?	• Toegang tot een mailbox vanaf elke cliënt (bijvoorbeeld Outlook vanaf de werkplek, een app vanaf mobiel of webmail vanaf thuis) mag alleen maar mogelijk zijn na inloggen met (geverifieerde) 2FA (gelijk aan niveau eIDAS substantieel). Toegang tot gevoelige informatie met alleen een wachtwoord mag dus niet mogelijk zijn. • Alle e-mails met persoonlijke gezondheidsinformatie moeten worden verstuurd met DKIM-ondertekening op de wijze die in de betreffende passages uit de 'Technische handreiking NTA 7516 voor e-mail dienstenleveranciers' is toegelicht.
6.1.6	Hoe weten verzender en ontvanger zeker dat het verstuurde ad-hocbericht ongeschonden is ontvangen?	Er moet gewaarborgd zijn, dat de ontvangen inhoud gelijk is aan de verzonden inhoud. Om dit te bewerkstelligen, dient de communicatie tussen alle e-mailclients en de mailserver van de organisatie beveiligd zijn met de juiste waarborgen: TLS 1.2 of hoger en certificaat validatie.
6.1.7	Hoe wordt voorkomen dat de afzender kan ontkennen dat deze een ad-hocbericht heeft verstuurd?	• Gewaarborgd is dat alle ad hoc e-mails met persoonlijke gezondheidsinformatie worden verstuurd met DKIM, SPF en DMARC op de wijze die in de betreffende passages van de technische handreiking voor e-mail dienstenleveranciers zijn toegelicht. • Bij de ontvanger zichtbaar is wie de afzender is van een ad hoc bericht, ook als dit bericht vanuit een functionele mailbox is verstuurd. • De ontvanger (visueel) kan vaststellen dat een bericht veilig is verstuurd. • Een bericht kan alleen verstuurd worden nadat de verzender zich heeft geauthentiseerd met betrouwbaarheidsniveau conform UeIDAS 'substantieel'.

6.1.9	Hoe wordt voorkomen dat een opgeslagen ad-hocbericht in onbevoegde handen komt?	Toegang tot de opgeslagen ad-hocberichten door partijen die daartoe geen geldige grond hebben, moet onmogelijk zijn. De opgeslagen berichtgegevens moeten in het geval ze onverhoopt in handen van onbevoegden komen, onleesbaar zijn. Daartoe dienen: • berichten versleuteld opgeslagen te worden op zowel de e-mailservers van de leveranciers als op de servers van de cliëntsoftware binnen de Europese Economische Ruimte (EER). • onbevoegden geen toegang hebben tot de data of de sleutels die toegang geven tot de informatie. • er met alle leveranciers die betrokken zijn bij het verzenden en ontvangen van e-mail met persoonlijke gezondheidsinformatie een (verwerkers)overeenkomst afgesloten te zijn.
6.1.10	Hoe wordt voorkomen dat een ontvangen ad-hocbericht wordt gelezen door een onbevoegde?	• Toegang tot ad-hocberichten is niet toegestaan met authenticatiemiddelen lager dan 'substantieel' voor personen en 'hoog' voor gegevens waarop het wettelijk beroepsgeheim van de professional berust. • Verstuurde e-mails met persoonlijke gezondheidsinformatie voor ontvangers die niet voldoen aan de NTA zijn alleen maar toegankelijk nadat de ontvanger zich heeft geauthentiseerd met 2FA van het niveau 'substantieel', bijvoorbeeld via een SMS naar een geverifieerd telefoonnummer. Dit is om te verifiëren dat de ontvanger werkelijk de beoogde persoon is.
6.1.11	Hoe wordt voorkomen dat gegevens tijdens het transport in onbevoegde handen komen?	Toegang tot ad-hocberichten door partijen die daartoe geen geldige grond hebben, moet onmogelijk zijn door toepassing van TLS 1.2. Als een ad-hocbericht onverhoopt toch in handen van onbevoegden komt, dan moet het ad-hocbericht onleesbaar zijn.
6.1.13	Hoe wordt ervoor gezorgd dat ad-hocberichten verstuurd aan een ontvanger buiten Nederland voldoen aan NTA 7516?	Ad-hocberichtenverkeer mag slechts in overeenstemming met de AVG de buitengrenzen van de Europese Economische Ruimte (EER) overschrijden. Dat betekent dat de mailserver van de communicatiedienstenaanbieder zich binnen de EER moet bevinden.
6.1.14	Hoe wordt bewerkstelligd dat elke ontvanger van een ad-hocbericht hier veilig op kan reageren (reply)?	Een ontvanger moet visueel kunnen vaststellen of een ad-hocbericht veilig is verzonden of niet. Beantwoorden door een persoon van een ad-hocbericht dat eerder door een professional is toegestuurd, moet veilig kunnen plaatsvinden, zonder dat hier een account of download voor nodig is.
6.1.15	Hoe wordt bewerkstelligd dat elke ontvanger van een ad-hocbericht het veilig kan versturen naar een derde (forward)?	Doorsturen door een persoon van een ad-hocbericht dat eerder door een professional is toegestuurd, is voor verantwoordelijkheid van de betreffende persoon. Als het doorsturen niet veilig kan plaatsvinden, moet de persoon hierop worden gewezen.
6.1.16	Hoe wordt voorkomen dat veilig verzenden pas mogelijk is nadat ingewikkelde opties zijn geselecteerd en aangezet?	Alle keuzemogelijkheden moeten standaard op de veiligste keuze aanstaan.
6.1.17	Hoe wordt bewerkstelligd dat elke ontvanger een ad-hocbericht kan lezen zonder dat hij daarvoor aanvullende programma's moet installeren?	Ad-hocberichten zelf (exclusief eventuele bijlagen) moeten zonder aanvullende programmatuur en zonder de verplichting van het aanmaken van een account bij de betreffende communicatiedienstenaanbieder door de persoon of professional, te lezen zijn door personen en professionals. De op een persoon gerichte online-omgeving moet voldoen aan de eisen van EN 301 549.
6.1.18	Hoe wordt bewerkstelligd dat elke ontvanger een ad-hocbericht kan downloaden en kan opslaan op een door hem of haar zelfgekozen locatie?	• Een ontvanger kan de veilige berichten downloaden als PDF-document of als een .eml. • De ontvanger kan kiezen om een onversleutelde kopie van het bericht naar zijn inbox te versturen. • Bijlagen kunnen eenvoudig worden gedownload met één muisklik. • De gebruiker kan zelf specificeren waar het bericht of bijlage wordt opgeslagen.
6.1.19	Hoe wordt het toevoegen van ad-hocberichten aan een dossier makkelijk gemaakt?	De oplossing moet ons faciliteren in het maken van een dossierkoppeling volgens de huidige processen.
7.2	De veilige e-maildienst kan koppelen met andere NTA 7516 diensten waardoor ontvangers zonder extra handelingen een bericht kunnen bekijken en de ontvanger een bericht van een ander product direct kan bekijken (in de norm heet dit interoperabel/ multikanaalcommunicatie)?	Interoperabiliteit met diensten van andere communicatiedienstenaanbieders die voldoen aan NTA 7516, moet mogelijk zijn binnen dezelfde functionaliteit.