Programma van Eisen

Veilig Mailen

MGR Rijk van Nijmegen

ICT Rijk van Nijmegen

Referentienummer: MGR-ICT-2021-02

25 augustus 2021

Programma van Eisen - Algemeen

1	NTA 7516 gecertificeerd	De aanbieder moet NTA7516-gecertificeerd zijn
2	Versleuteld transport	Gegarandeerd moet zijn dat gevoelige informatie versleuteld is gedurende het transport [in transit], volgens best practice transport-beveiligingsmaatregelen, en gegarandeerd moet zijn dat informatie niet ingezien kan worden in het geval van onderschepping
3	Versleutelde opslag met zero-knowledge	Gegarandeerd moet zijn dat gevoelige informatie versleuteld is tijdens de opslag en dat alleen de verzender en de ontvangers de data kunnen ontsleutelen. Leveranciers mogen niet de (technische) mogelijkheid hebben om toegang te krijgen tot de opgeslagen data
4	Sterke authenticatie van gebruikers	Gegarandeerd moet zijn dat gebruikers, zowel zenders of ontvangers die dezelfde oplossing gebruiken, enkel toegang hebben tot informatie ná een sterke authenticatie. Om ongeautoriseerde toegang te voorkomen is het niet afdoende om met slechts een toegangscode toegang te verkrijgen tot een e-mailbox en de gevoelige informatie te kunnen lezen
5	Werken vanuit bestaande applicaties	De oplossing moet integreren met huidige en toekomstige versies van Outlook zodat gebruikers hun werkwijzen niet (significant) hoeven te wijzigen
6	Eenvoudig e-mailen vanuit Outlook op alle apparaten, zonder aparte applicatie	Het moet mogelijk zijn om veilig te kunnen communiceren vanuit zowel de desktop als vanuit een Outlook-applicatie. Dit zou kunnen door middel van een add-on of bijvoorbeeld een Relay Server. Belangrijk hierbij is dat geen gebruik gemaakt wordt van een separate applicatie omdat dit de menselijke fout in de hand werkt.
7	Security by default	Per organisatie moet ingesteld kunnen worden of veilig verzenden standaard aan of uit staat.
8	Eenvoudig kiezen voor beveiliging	De verzender moet de mogelijkheid hebben om met een muisklik veilig mailen aan of uit te zetten, per e-mailbericht en vanuit het opstelvenster van de e-mail
9	Direct kunnen lezen van vertrouwelijke berichten	De medewerker van de gemeente moet de mogelijkheid hebben om binnenkomende beveiligde berichten direct in Outlook te kunnen lezen, zonder extra te hoeven klikken
10	Eenvoudige toegang voor gastontvangers	Gastontvangers moeten de mogelijkheid hebben om berichten en bijlagen te lezen, zonder de verplichting om een account aan te maken of specifieke software te moeten downloaden en te installeren
11	Ondersteuning voor het reageren op gevoelige berichten	Gastontvangers moeten de mogelijkheid hebben om beveiligd te kunnen reageren op gelezen berichten, ook met de mogelijkheid om grote bijlagen mee te sturen, zonder de verplichting om een account aan te maken of specifieke software te moeten downloaden en te installeren
12	Downloaden van berichten en bijlagen	Gastontvangers moeten de mogelijkheid hebben om berichten te downloaden voor archivering en/of het gebruik in hun eigen (e-mail) omgeving, zonder de verplichting om een account aan te maken of specifieke software te moeten downloaden en te installeren
13	Uitgebreide onboarding en implementatie	Het is van belang dat de verschillende organisaties binnen de regio Rijk van Nijmegen worden ondersteund door de leverancier bij het technisch en organisatorisch implementeren van de oplossing.
14	Eigen domeinnaam	Het moet mogelijk zijn om de eigen domeinnamen van de organisaties te gebruiken. Op deze manier komt het bericht op een vertrouwelijke manier binnen bij de ontvanger
15	Veilig naar functionele mailboxen versturen	Als een mail wordt gestuurd naar functionele mailboxen moet het mogelijk zijn om deze met behulp van een (sterke) authenticatie te openen
16	Verwerkersovereenkomst	Leverancier accepteert onverkort de VNG-standaard voor verwerkersovereenkomsten
17	Inkoopvoorwaarden	Leverancier accepteert de meest actuele GIBIT en iRvN-Inkoopvoorwaarden
18	Techniek	De oplossing moet passen binnen de infrastructuur en de kantoorautomatisering van het Rijk van Nijmegen. De primaire mailfaciliteit is op basis van Microsoft365 en Exchange Online
19	Multifactor authenticatie	De oplossing moet voor multifactor-authenticatie meer mogelijkheden bieden dan alleen 06-nummer

Wensen - Gebruik		
1	Verhogen van de bewustwording van medewerkers voor het werken met gevoelige informatie	Maak een medewerker bewust van gevoelige informatie in zijn/haar e-mail. Dit moet plaatsvinden gedurende het opstellen van het bericht terwijl de workflow niet nadelig beïnvloed wordt
2	Detecteer externe ontvangers	Waarschuw een medewerker wanneer gevoelige informatie op het punt staat om onbeveiligd gedeeld te worden met externe ontvangers. Dit moet plaatsvinden gedurende het opstellen van het bericht terwijl de workflow niet nadelig beïnvloed wordt
3	Adviseer en pas maatregelen toe	Ondersteun de medewerker bij het gedegen beschermen van gevoelige informatie die wordt verzonden, gebaseerd op de inhoud van het bericht en het beleid van de organisatie
4	Blokkeren berichten, ontvangers en/of bestanden	Stel gebruikers in staat om berichten en bijlagen te blokkeren met de garantie dat een nog niet ingezien bericht ook daadwerkelijk leidt tot het hebben van geen datalek, óók voor berichten die verzonden zijn aan externe ontvangers. Ook moet er een bevestiging zijn dat een bericht succesvol is ingetrokken/geblokkeerd voor de ontvanger.
5	Traceren	Bied mogelijkheden om te controleren, per ontvanger, of mails en/of bijlagen reeds zijn geopend om de impact te bepalen van een (mogelijk) datalek of voor een effectieve opvolging van een gesprek met een ontvanger
6	Gemakkelijk in het gebruik	De oplossing moet intuïtief zijn, met minimale inspanning voor gebruikers en met minimale verstoring van werkprocessen voor het versturen van niet-privacygevoelige én privacygevoelige e-mails
7	Ondersteuning voor e-mail en grote bijlagen	De gebruiker moet de mogelijkheid hebben om erg grote bestanden te delen via e-mail vanuit hun opstelvenster. Bijlagegroottes mogen geen belemmering zijn voor de verzender en ontvanger
8	Beveiligd reageren op berichten	De gastontvanger moet de mogelijkheid hebben om beveiligd te kunnen reageren op gelezen berichten via zowel de AAN-, de CC- en/of de BCC-knop

Wensen - Inrichting		
1	ISO27001 gecertificeerd	De aanbieder moet ISO27001-gecertificeerd zijn
2	Geen zware belasting plugin	Indien gebruik gemaakt wordt van een plugin mag deze plugin geen zware belasting geven op de server
3	Toegankelijkheid	De gebruiker moet niet extra hoeven in te loggen om veilig te kunnen mailen. Toegang tot Microsoft365 zou voldoende moeten zijn. Het is ongewenst dat men in de ochtend als gebruiker extra moet inloggen om veilig te kunnen mailen want dit zorgt voor menselijke fouten
4	Communicatieportalen	Derden moeten de mogelijkheid hebben om zelf een gesprek te initiëren of op een veilige manier bestanden te kunnen achterlaten, zonder dat één van de eigen medewerkers dit initieert
5	Minimaal onderhoud	Het onderhoud van de oplossing moet niet de standaard-bedrijfsvoering hinderen of het gebruik van de oplossing limiteren. Dit geldt zowel voor onderhoud aan de oplossing als aan eventuele hardware, backups, accountmanagement etc.
6	Werken vanuit bestaande applicaties	De oplossing is te koppelen aan door de deelnemers gebruikte (zaak)systemen zodat rechtstreeks vanuit die applicaties beveiligd ge-maild kan worden.
7	Input voor gastverificatie delen	Als men via telefoonnummer met 2FA een e-mail wil verzenden, moet een versleuteld telefoonboek aanwezig zijn waarin telefoonnummers organisatiebreed kunnen worden ingevoerd. Zodat slechts één gebruiker eenmalig een telefoonnummer hoeft in te vullen en vervolgens de hele organisatie daar gebruik van kan maken
8	Eenvoudig gebruikersbeheer	De installatie van de oplossing moet eenvoudig zijn en moet zoveel mogelijk geïntegreerd zijn met huidige oplossingen zoals ons Active Directory e/o onze Azure/AD voor authenticatie en autorisatie
9	Een eigen bibliotheek aan triggerwoorden die naar eigen hand is te zetten	Het is wenselijk om een branche-specifieke woordenlijst te ontvangen. De organisatie moet zelf kunnen bepalen welke woorden wel en welke woorden niet worden gebruikt, zonder tussenkomst van de leverancier. Daarnaast is het wenselijk dat de organisatie zelf een aangepaste lijst kan maken met op maat gemaakte triggerwoorden en reguliere expressies
##	Eigen huisstijl doorvoeren	Het moet mogelijk zijn om de oplossing te voorzien van de huisstijlen van de organisaties op het vlak van kleurschema en logo. Dit ondersteunt de huisstijl herkenbaarheid voor gasten en externen
##	Instellen van termijnen om data te bewaren	De oplossing moet de mogelijkheid bieden om een standaardverloopdatum in te stellen voor berichten met de optie om dit ook op berichtniveau in te kunnen stellen of wijzigen
##	Ondersteuning voor functionele/team accounts	De gebruiker moet de mogelijkheid hebben om effectief gevoelige berichten te kunnen versturen en lezen vanuit een functionele mailbox wanneer deze gebruiker volgens de Active Directory e/o Azure/AD hier rechten toe heeft. Dit dient mogelijk te zijn zonder opnieuw in te loggen, met volledige logging en audittrailing op persoonlijk niveau van de individuele medewerker met zijn of haar toegangen en acties