Den Haag

Aansluitvoorwaarden SMTP Relay Service

Colofon

Naam document

Aansluitvoorwaarden SMTP Relay Service.

Versiebeheer en eigenaarschap

Het voorliggende document betreft versie 1.0. De eigenaar van dit document is de Werkgroep Informatieveiligheid (WGIV). Het beheer van dit document berust bij Expertisecentrum Security van de Gemeente Den Haag.

Geldigheid

Dit document is geldig voor drie jaar vanaf de datum van vaststelling. Review zal plaatsvinden bij grote relevante wijzigingen op het onderwerp en ten minste drie jaar na de vaststellingsdatum. Indien een nieuw beleidskader binnen deze termijn nog niet is vastgesteld, dan blijft het huidige beleidskader tot dat moment van toepassing.

Beleidshiërarchie

De vertrouwelijkheid is vastgesteld op classificatie Openbaar.

BIO-compliance

Dit document en eventuele aanverwante documenten waarborgen dat de gemeente Den Haag voldoet aan BIO-norm 13.2 (Informatietransport).

Goedkeuring en opvolging

Dit document is ter informatie aangeboden aan de gelieerde Expertisecentra Architectuur en Security. Daarna is dit document goedgekeurd in de WGIV op DD-MM-YYYY. Per die datum is het vigerend beleid binnen de gemeente Den Haag.

Wijzigingshistorie

Versie	Datum	Naam	Wijziging / Actie
0.1	06-01-2021	Magdalena Simidzioski	Opzet en initiële vulling
0.2	11-01-2021	Magdalena Simidzioski	Aanvulling/ Feedback verwerken
0.3	17-01-2021	Magdalena Simidzioski	Verwerken feedback Architectuur
0.9	19-01-2021	Magdalena Simidzioski	Verwerken feedback Architectuur, Security
1.0	28-01-2021	Magdalena Simidzioski	Feedback Jean-Philippe Gorsira, Peter van Eijk
1.1	30-04-2021	Magdalena Simidzioski	Aanpassing voorwaarden

1. Beleidsuitgangspunten

In de BIO beschrijft de normen 13.2.1 en 13.2.2 en 13.2.3 het volgende:

ID	BBN	Verantwoordelijke	Omschrijving
13.2.1	1	Secretaris/ algemeen directeur	Beleid en procedures voor informatietransport Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.
13.2.2	1	Proceseigenaar Dienstenleverancier	Overeenkomsten over informatietransport Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.
13.2.3	1	Dienstenleverancier	Elektronische berichten Informatie die is opgenomen in elektronische berichten behoord passend te zijn beschermd

Dit beleid is gebaseerd op beleidsuitgangspunten die zijn ontleend aan het vigerend Strategisch Beleidskader Informatieveiligheid Gemeente Den Haag.

Uitgangspunten:

- Afwijkingen op beleid vinden plaats in afstemming met de auteur van dit document.

2. Onderliggende documentatie

Relevante documenten:

ID	Titel	Auteur	Datum	Versie
1	**Guidelines on Electronic Mail Security**	NIST	06-01-2021	2.0 https://www.nist.gov/publications/guidelines-electronic-mail-security
2	**ICT-beveiligings-richtlijnen voor Transport Layer Security (TLS)**	NCSC	10-01-2020	2.0 https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls
3	**Verplichte Standaarden**	Forum Standaardisatie	06-01-2021	https://forumstandaardisatie.nl/open-standaarden/verplicht
4	**Factsheet Beveilig verbindingen van mailservers**	NCSC	06-01-2021	https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-beveilig-verbindingen-van-mailservers
5	**SMTP Service Extension for Secure SMTP over Transport Layer Security**	IETF	06-01-2021	https://tools.ietf.org/html/rfc3207

3. Inleiding en scope

Het is mogelijk voor externe partijen of Cloud gebaseerde diensten om email te versturen namens de gemeente Den Haag. Om gebruikt te maken van deze service moet de externe partij voldoen aan de aansluitvoorwaarde zoals beschreven in dit document.

Voor Cloud gebaseerde diensten wordt er onderscheid gemaakt tussen SaaS, Paas en IaaS oplossingen. Deze hebben verschillende maten van eigenaarschap. Het uitgangspunt is dat de Cloud gebaseerde oplossingen SaaS-oplossingen zoals beschreven concept in het shared responsibility model in bijlage B.

Met ‘afnemer’ van de SMTP Relay Service wordt bedoeld de Cloud gebaseerde dienstleverancier. Met deze leverancier is een passende SLA en een verwerkersovereenkomst opgesteld met de gemeente.

4. Aansluitvoorwaarden

a. Uitgangspunt

1. Email versturen namens de gemeente Den Haag dient ter ondersteuning van een primair proces vanuit de dienst. Als het om niet primaire dienstproces gaat wordt er een andere oplossing conform de standaarden gebruikt over de email voorziening.
2. Het domein denhaag.nl is in eigendom te zijn van de gemeente Den Haag;
3. Alle standaarden met betrekking tot veilige e-mail dienen te worden geïmplementeerd, dit is van toepassing op zowel externe als interne mailomgevingen. De standaarden zijn beschreven in bijlage A.
    - SPF en DNSSEC is uitsluitend bedoeld voor server to server communicatie.
4. Mailserver externe partij mag niet ingezet worden als open relay server naar denhaag.nl of namens denhaag.nl;
5. Op verzoek van de gemeente Den Haag dient ieder moment een logbestand te kunnen worden opgeleverd met daarin alle verzonden mail naar of van denhaag.nl of andere bij gemeente Den Haag geregistreerde domeinen.
6. Bij misbruik wordt het IP-adres van de afnemer zonder discussie afgesloten van de service.
7. Het is aan de afnemers van deze service om ervoor te zorgen dat ze de SMTP-aansluiting op hun server inrichten.
8. Het is aan de afnemer om beveiliging te implementeren (captcha’s op formulieren, beveiligingsupdates bijhouden, rate-limiting, monitoring, transport layer security) enz.
9. Maatregelen als anti-virus, anti-spoofing en intrusion detection technieken dienen gebruikt te worden door de afnemer.
10. De uitgangspunten dienen door de afnemer gerespecteerd te worden. Als de afnemer niet kan voldoen aan deze uitganspunten dan zal de afnemer geen gebruik kunnen maken van de dienst.

b. Voorwaarden

- Het gebruik van het email adres denhaag.nl dient ter ondersteuning te zijn van een primair proces vanuit de dienst.
- De aansluiting met de SMTP Relay verloopt via smtprelay.denhaag.nl 217.68.49.15 poort TCP 25. Voor deze aansluiting is TLS 1.2 of hoger een vereiste.
- Een onderscheid tussen het afzenderadres per Clouddienst en omgeving moet helder zijn. De gehanteerde naamgevingsconventie van de benaming voor een afzender adressen kan zijn het volgende:

- Applicatienaam.omgeving.noreply@denhaag.nl

- Het is niet nodig om een mailbox in te stellen. Het aangeven van de naam is voldoende
- Géén bulkmail (alle mail is het gevolg van een interactie met de gebruiker). De standaard instelling is 100 berichten per uur. Er wordt geen queue bijgehouden op de relay service. De afzender is hier zelf verantwoordelijk voor.
- De afnemer van de SMTP-service moet ervoor zorgen dat de mail afgeleverd wordt bij de SMTP-relay. Indien nodig moet het mogelijk zijn om via een queue email later af te leveren. Dit kan voorkomen wanneer er meer emails zijn verzonden dan vastgesteld in het limiet. De SMTP-relay geeft dit aan middels een foutmelding.
- Géén mail met persoon als afzender. Alleen no-reply, info, enz.
- Bij aanvraag door externe partij of Cloud gebaseerde dienst dient de lijst met toegestane afzender adressen opgeleverd te worden (afzender whitelisting). Deze worden ter goedkeuring aangeboden aan afdeling Security. Ná goedkeuring mogen alleen deze afzender adressen door aanvrager gebruikt worden.
- Volgens de richtlijnen van het NIST en NSCS is het gebruikt van STARTTLS verplicht.
- Deze dienst wordt aangeboden op basis van het IP-adres van de Cloud server (IP whitelisting). Het is dus niet toegestaan dat andere afnemers hetzelfde adres gebruiken.
- Relaying voor derde partijen is niet toegestaan (een aangesloten server mag dus niet voor andere servers relayen)
- De relay service is bedoeld voor alle gemeentelijke systemen ongeacht van de data classificatie.
- De SaaS leverancier is zelf verantwoordelijk voor het versleutelen van de PayLoad. De functie van de relay service is het beveiligd transporteren van de data.

5. Aanvraag proces

De volgende stappen dienen te worden gevolgd om gebruik te kunnen maken van deze dienst.

1. Via het standaard aanvraag proces (NSW) kan de aanvrager (of Project) een aanvraag doen bij Expertise Centrum Security.
2. Binnen de aanvraag dient het verzoek om aan te sluiten op de SMTP Relay Service te worden onderbouwd. Dit kan middels een beschrijving of een architectuurstuk (HLD/PSA/Plan van Aanpak).
3. De volgende punten moeten minimaal in de aanvraag:
    a. Naam aanvraag
    b. Onderbouwing
    c. Email adres van aanvrager
    d. IP-adres van de te verzenden server
    e. Naam Serviceaccount
    f. Eigenaar/ verantwoordelijke
4. De afnemer dient een verzoek in om lid te worden van de SMTP-authenticatie groep. Deze aanvraag dient te worden goedgekeurd door Securitymanagement. De account waarmee SMTP-authenticatie moet worden gedaan moet lid zijn van de volgende groep:

    - Groepsnaam: XG_RS_SMTP

    - Volledig pad van de groep: KA.HAAGNET.NET/Beheer/ServiceAccounts/SMTPRelay/XG_RS_SMTP

    - Volledig pad van de groep in X.500 notatie:

    CN=XG_RS_SMTP,OU=SMTPRelay,OU=Service Accounts,OU=Beheer,DC=KA,DC=HAAGNET,DC=NET

    *** Let wel: dit is over het algemeen dus een serviceaccount. Het is niet de bedoeling dat er per gebruiker apart SMTP-authenticatie via de relay wordt ingesteld. Normaal gesproken is dit 1 serviceaccount per

applicatie/ website!

5. Als deze aanvraag is goedgekeurd wordt de aanvraag door Securitymanagement doorgezet naar HaagNet voor uitvoering.

6. Rapportage

Er bestaat een mogelijkheid om rapportages te leveren aan diensten die gebruik maken van de SMTP-service. Om rapportages te kunnen ontvangen dient de eigenaar bekend te zijn en het email adres van de eigenaar of ontvanger van de rapportages.

Deze rapportages kunnen worden ingevuld in overleg maar dienen in elk geval de volgende informatie te bevatten:

- Een overzicht van kwetsbaarheden en/of virussen.
- Een overzicht van outbreak filters.
- Een overzicht van inkomende (tegengehouden) email.
- Een overzicht over uitgaande email

Een rapportage kan worden aangevraagd bij Securitymanagement.

Bijlage A – Email standaarden

Verplicht

i. STARTTLS

STARTTLS maakt het mogelijk om SMTP-verkeer tussen mailservers over een met TLS versleutelde verbinding te laten lopen[1].

ii. SPF

SPF is een techniek waarmee een domeinhouder de IP-adressen van verzendende mailservers kan publiceren in de DNS. Een ontvangende mailserver kan deze IP-adressen gebruiken om te controleren of een e-mail daadwerkelijk afkomstig is van een verzendende mailserver van de betreffende domeinhouder [2].

iii. DNSSEC

Met DNSSEC kan de ontvanger de echtheid van de domeinnaaminformatie (waaronder IP-adressen) controleren. Dit voorkomt bijvoorbeeld dat een aanvaller het IP-adres ongemerkt manipuleert (DNS-spoofing) en daarmee verstuurde e-mails omleidt naar een eigen mailserver of gebruikers misleidt naar een frauduleuze website [3].

Wenselijk

iv. DKIM

DKIM is een techniek waarmee e-mailberichten kunnen worden gewaarmerkt. Het gebruik van DKIM verkleint de kans op misbruik van e-mailadressen doordat ontvangers legitieme e-mails van phishing mails of spam kunnen onderscheiden. Ook kunnen ontvangers controleren of de inhoud van de e-mail door derden is gemanipuleerd [4].

v. DMARC

DMARC geeft de verzendende partij de mogelijkheid om beleid te formuleren wat er met e-mails moet gebeuren wanneer de echtheidswaarmerken niet kloppen. Het gebruik van DMARC kan daarmee ingezet worden voor het verminderen en/of voorkomen van misbruik van de domeinnaam middels e-mail. Ook kan door het gebruik van de standaard worden voorkomen dat e-mailmailingen door e-mailproviders onterecht voor spam worden aangezien[5].

vi. DANE

DANE, dat voortbouwt op DNSSEC, geeft zekerheid over de identiteit van de ontvangende mailserver. Dit voorkomt dat een aanvaller zich kan uitgeven als ontvangende-mailserver, waardoor hij het mailverkeer kan onderscheppen. Daarnaast dwingt DANE het gebruik van TLS af. Dit voorkomt dat een aanvaller het opzetten van STARTTLS kan blokkeren, om zo toegang tot de on-versleutelde berichten te krijgen [6].

[1] https://tools.ietf.org/html/rfc3207
[2] https://tools.ietf.org/html/rfc7208
[3] https://tools.ietf.org/html/rfc4033
[4] https://tools.ietf.org/html/rfc6376
[5] https://tools.ietf.org/html/rfc7489
[6] https://tools.ietf.org/html/rfc7671

Bijlage B – SaaS Shared Responsibility Matrix