Forum Standaardisatie

Wilhelmina v Pruisenweg 104
2595 AN Den Haag
Postbus 84011
2508 AA Den Haag
www.forumstandaardisatie.nl

Nationaal Beraad Digitale Overheid

Aan:	Nationaal Beraad Digitale Overheid		
Van:	Forum Standaardisatie		
Datum:	19 september 2016	**Versie**	1.0
Betreft:	Opname standaarden op de 'pas toe of leg uit'-lijst		

2016-0000567354

Het Forum Standaardisatie vraagt het Nationaal Beraad in te stemmen met:

1. De opname van de open standaard *STARTTLS in combinatie met DANE* ter versleuteling van communicatie tussen e-mailservers op de 'pas toe of leg uit'-lijst voor het hieronder geformuleerde toepassings- en werkingsgebied;
2. De additionele adviezen ten aanzien van de adoptie van de open standaard STARTTLS in combinatie met DANE.

Toelichting op 'pas toe of leg uit'-beleid

Het is kabinetsbeleid dat overheden gebruikmaken van open standaarden op basis van een 'pas toe of leg uit'-regime voor standaarden van de 'pas toe of leg uit'-lijst van het Forum Standaardisatie. De bekrachtiging van de standaarden die op deze lijst worden geplaatst, op advies van het Forum Standaardisatie, ligt bij Nationaal Beraad.

Overheden en semi-overheden zijn verplicht om de relevante standaarden met de status 'pas toe of leg uit' te vragen bij aanschaf of (ver)bouw van ICT-systemen/-diensten ('pas toe'). Afwijken mag alleen met zwaarwegende redenen en hierover moet verantwoording worden afgelegd in het jaarverslag ('leg uit').

Gebruik van deze standaarden verbetert veilige en betrouwbare uitwisseling en (her)gebruik van gegevens tussen overheidsorganisaties en bedrijven, tussen overheidsorganisaties en burgers en tussen overheidsorganisaties onderling en daarmee de samenwerking (interoperabiliteit). Daarnaast kunnen open standaarden door iedere leverancier worden ingebouwd, wat de leveranciersafhankelijkheid (vendor lock-in) voor overheden vermindert. Het proces voor het toetsen van standaarden is transparant en robuust op basis van expertsessies en openbare consultaties.

Toelichting op de standaarden

Datum
16 juni 2016

STARTTLS en DANE zijn (e-mail)beveiligingsstandaarden die kunnen worden gebruikt om een beveiligde, versleutelde verbinding tussen mailservers op te zetten.

STARTTLS zorgt ervoor dat een niet-versleutelde, en daarmee onbeveiligde, verbinding tussen een uitgaande en ontvangende mailserver geüpgrade wordt naar een versleutelde TLS-verbinding. Het toepassen van DANE zorgt er voor dat een beveiligde verbinding alleen tot stand wordt gebracht wanneer het certificaat van de ontvangende mailserver is gecontroleerd door de verzendende mailserver. DANE bouwt voort op DNSSEC dat al op de 'pas toe of leg uit'-lijst staat. Hierdoor is het voor aanvallers niet mogelijk om berichtenverkeer 'af te luisteren' of te manipuleren.

Het ondersteunen van STARTTLS en DANE betekent dat partijen die naar de overheid willen mailen dat altijd via een beveiligde, versleutelde server verbinding kunnen doen.

De standaarden zijn complementair aan de e-mailauthenticatiestandaarden, SPF en DKIM, die reeds op de 'pas toe of leg uit'-lijst staan en gericht zijn op het voorkomen van spoofing en phishing.

Beslispunt (opname en additionele adviezen)

Op basis van de toetsingsprocedure met expertgroep en openbare consultatie waarin beide open standaarden zijn getoetst tegen de criteria (business case) voor opname op de 'pas toe of leg uit'-lijst[1] adviseert het Forum aan het Nationaal Beraad om in te stemmen met:

1. *De opname van de open standaard STARTTLS in combinatie met DANE (RFC 7672) ter versleuteling van communicatie tussen e-mailservers op de 'pas toe of leg uit'-lijst voor het hieronder geformuleerde toepassings- en werkingsgebied;*

    - Functioneel toepassingsgebied: Voor inkomende mailservers STARTTLS (SMTP over STARTTLS, oftewel ESMTPS) in combinatie met DANE toe te passen, zodat verzendende mailservers daarmee een versleutelde verbinding over een onvertrouwd netwerk (zoals internet) kunnen opzetten. Dit voorkomt dat aanvallers het mailverkeer kunnen afluisteren (passieve aanvallers) en/of kunnen manipuleren (actieve aanvallers).

    - Organisatorisch werkingsgebied: overheden (Rijk, provincies, gemeenten en waterschappen) en overige instellingen uit de publieke sector.

2. *De additionele adviezen ten aanzien van de adoptie van de open standaard STARTTLS in combinatie met DANE.*

[1] *Documentatie over de procedure, het expertadvies en het forumadvies met adoptiemaatregelen en toelichting op het toepassingsgebied zijn te vinden op: https://www.forumstandaardisatie.nl/standaard/starttls-en-dane*

a. Het Forum Standaardisatie wordt opgeroepen om een infographic over e-mailbeveiligingsstandaarden op te stellen om zodoende de relatie met andere e-mailstandaarden (zoals DKIM en SPF) beter inzichtelijk te maken.
b. NCSC wordt opgeroepen om, in aanvulling op de whitepaper 'ICT beveiligingsrichtlijnen voor Transport Layer Security (TLS)', een advies uit te brengen over het implementeren van STARTTLS en DANE.
c. Platform Internetstandaarden wordt opgeroepen om het advies van NCSC als uitgangspunt te hanteren in de e-mailtest op Internet.nl.
d. Forum Standaardisatie wordt opgeroepen bij de mailstandaarden op de lijst met gangbare standaarden die tussen mailclient en mailserver gebruikt kunnen worden (SMTP, IMAP en POP3), aan te geven dat deze bij voorkeur met TLS beveiligd moeten worden.
e. KING wordt opgeroepen om beveiligingsstandaarden als STARTTLS en DANE op te nemen in de GEMMA Softwarecatalogus.
f. Forum Standaardisatie worden opgeroepen om met behulp van Internet.nl een overheidsbrede 0-meting te laten uitvoeren naar het gebruik van STARTTLS en DANE.
g. De Shared Service Centra van het Rijk (zoals SSC-ICT en DICTU) worden opgeroepen om STARTLS en DANE te implementeren en hen hierop via ICCIO of CTO-raad aan te spreken.
h. Forum Standaardisatie wordt opgeroepen om een jaar na opname van de standaarden te toetsen (in samenspraak met de expertgroep) hoe het verloopt met de implementatie en of het functioneel toepassingsgebied ook moet worden uitgebreid tot uitgaande mailstromen.
i. NCSC wordt opgeroepen de ontwikkelingen rondom de aanverwante concept-standaard SMTP STS in de gaten te houden en wanneer SMTP STS een ontwikkelde standaard is de relatie tussen de standaarden opnieuw te duiden.