notitie

Forum Standaardisatie

Wilhelmina v Pruisenweg 104
2595 AN Den Haag

Postbus 84011
2508 AA Den Haag

www.forumstandaardisatie.nl

30 maart 2016

FORUM STANDAARDISATIE 20 april 2016
Agendapunt 2E. Forum-advies STARTTLS en DANE
Stuknummer 2E Forum-advies STARTTLS en DANE

Van:	Stuurgroep open standaarden
Aan:	Forum Standaardisatie
Datum:	20 april 2016

Aanleiding en achtergrond
STARTTLS en DANE zijn (e-mail)beveiligingsstandaarden die kunnen worden gebruikt om een beveiligde verbinding tussen mailservers op te zetten. STARTTLS zorgt er voor dat een niet-versleutelde, en daarmee onbeveiligde, SMTP-verbinding geüpgrade wordt naar een versleutelde TLS-verbinding.

De toepassing van DANE zorgt er voor dat een verbinding pas tot stand wordt gebracht wanneer het DNS-record van de ontvangende mailserver is gecontroleerd door de verzendende mailserver. Hierdoor is het voor aanvallers niet mogelijk om berichtenverkeer 'af te luisteren' of te manipuleren. Gebruikers van STARTTLS en DANE moeten de verbinding verbreken wanneer er geen beveiligde verbinding via STARTTLS opgezet kan worden, maar deze wel aanwezig is volgens het DNS-records.

Tijdens de openbare consultatie is er een nieuwe standaard (SMTP STS) gepubliceerd, ondersteunt door de grotere mail platformen (Gmail, Yahoo, Microsoft). Deze standaard kan gezien worden als potentiële concurrent van DANE. Geadviseerd wordt om een aanvullend onderzoek uit te voeren naar deze ontwikkeling alvorens de combinatie STARTTLS en DANE op te nemen op de lijst met open standaarden.

Betrokkenen en proces
In eerste instantie is alleen DANE aangemeld voor opname op de lijst met open standaarden. Tijdens het intakegesprek is naar voren gekomen dat DANE in toenemende mate wordt toegepast met STARTTLS om een beveiligde verbinding tussen mailservers op te kunnen zetten. Daarom is besloten om STARTTLS samen met DANE in behandeling te nemen. Vervolgens heeft een expertbijeenkomst plaatsgevonden op 28 januari 2016. De conclusie van de expertgroep was om STARTTLS en DANE op te nemen op de lijst met open standaarden, onder

voorwaarde dat er binnen het organisatorisch werkingsgebied tenminste twee organisaties de standaarden succesvol hebben geïmplementeerd. Naar aanleiding hiervan is een meting op gebruik uitgevoerd, waaruit bleek dat aan deze voorwaarde is voldaan.

Tijdens de openbare consultatie van het expertadvies van 16 februari tot 16 maart 2016 is één reactie ontvangen. Wel is tijdens de openbare consultatie een nieuwe standaard gepubliceerd ondersteund door de grotere mail platformen (Gmail, Yahoo, Microsoft), die een grote impact kan hebben op de adoptie van de combinatie STARTTLS en DANE. In samenspraak met de experts is het advies om hier een aanvullende onderzoek naar te doen.

Consequenties en vervolgstappen
Het gebruik van de standaarden is binnen het geadviseerde organisatorische werkingsgebied nog beperkt, met name waar het DANE betreft. Het NCSC heeft de standaarden onlangs succesvol geïmplementeerd. Ook zijn er positieve signalen bij andere overheidspartijen om de standaarden op korte termijn in gebruik te nemen. Gezien de recente ontwikkeling met betrekking tot SMTP STS is het belangrijk om meer inzicht te krijgen in gebruik van de standaarden bij de grote mailplatformen.

Verder zijn er enkele adviezen om de adoptie van de standaard te bevorderen. Deze staan in onderstaand advies.

Advies

Het Forum Standaardisatie wordt gevraagd om:
1. Kennis te nemen van de werking en toegevoegde waarde van standaarden STARTTLS en DANE.
2. In te stemmen met een aanvullend onderzoek naar de SMTP STS-standaard (een potentiële concurrent van DANE) en de mogelijke impact op het verplichten van de combinatie STARTTLS en DANE en het toepassingsgebied.

<u>Ad 1/2 Opname van STARTTLS en DANE op de lijst met open standaarden</u>
Op dit moment is gecombineerd gebruik van de standaarden voor inkomende e-mail nog beperkt. STARTTLS als zodanig wordt wel veel gebruik, maar alleen een gecombineerd opname zou wenselijk zijn voor echt veilige mailuitwisseling omdat STARTTLS gevoelig is voor 'man in the middle' aanvallen. Er zijn echter positieve signalen over toekomstig gebruik. Zo heeft ten tijde van het opstellen van dit Forumadvies heeft het NCSC de standaarden succesvol geïmplementeerd op alle inkomende mailservers. En vanuit het platform Internet.nl is een meting uitgevoerd naar het gebruik van de twee standaard onder overheidsorganisaties.

Het expertadvies was dan ook om de combinatie STARTTLS en DANE op te nemen op de lijst met open standaarden. Tijdens de openbare consultatie is er echter een nieuwe standaard gepubliceerd (SMTP Strict Transport Security). Deze kan gezien worden als concurrent van DANE en is ontwikkeld door de grotere partijen binnen

de 'e-mailwereld' (Google, Yahoo en Microsoft). Deze partijen hebben de standaard ook breed onder de aandacht gebracht.[1]

Daarom is het advies om aanvullend onderzoek uit te voeren naar deze standaard en de impact hiervan op de mogelijk gecombineerde opname van STARTTLS en DANE. Op basis van dit onderzoek kan besloten worden hoe om te gaan met SMTP STS, DANE en STARTTLS, de (gecombineerde) opname van de standaarden op de lijst en het geadviseerde toepassingsgebied.

Toelichting

1. Waar gaat het inhoudelijk over?

Met de toenemende digitalisering is ook het beveiligingsrisico aanzienlijk toegenomen. De overheid gebruikt gevoelige informatie van zowel burgers als bedrijven. Ook maakt de overheid veel gebruik van e-mail, en verstuurt en ontvangt zij e-mails van andere overheden, bedrijven en burgers mét gevoelige informatie. Dit vraagt om aandacht voor de dreiging van digitale (economische) spionage en identiteitsdiefstal. Zonder adequate beveiligingsmaatregelen kan in een kort tijdsbestek een grote hoeveelheid aan informatie op de facto anonieme wijze worden verzameld. Informatie kan worden geblokkeerd, en onder bepaalde voorwaarden worden aangepast en vervalst.

De Nederlandse overheid heeft vanuit haar rol de taak en verplichting om (toevertrouwde) vertrouwelijke informatie te beschermen tegen afluisteren door aanvallers, zoals criminele partijen en statelijke actoren. Onder de te beschermen informatiestromen valt ook feitelijk communicatie tussen overheidspartijen, tussen de overheid en bedrijven en tussen overheden en burgers.

STARTTLS
E-mails worden door de mailserver van de verzendende partij verstuurd naar de mailserver van de ontvangende partij. Historisch gebeurt dit zonder enige versleuteling of beveiliging, waardoor het aanpassen of injecteren van mailverkeer relatief eenvoudig is.

De extensie STARTTLS is in veel gevallen aanwezig op beide mailservers. Zij kunnen daarmee een niet-versleutelde, en daarmee onbeveiligde, verbinding opwaarderen naar een met TLS versleutelde verbinding. Met een met TLS versleutelde verbinding wordt voorkomen dat een passieve aanvaller het berichtenverkeer kan 'afluisteren'. Let op: een passieve aanvaller is een aanvaller die het berichtenverkeer niet manipuleert, maar slechts ongemerkt onderschept.

Het gaat hier bijvoorbeeld om e-mails met gevoelige informatie of e-mails waarbij documenten mee zijn gestuurd. Om STARTTLS in werking te laten treden is het noodzakelijk dat zowel de verzendende als de ontvangende mailserver STARTTLS ondersteunen.

Wanneer STARTTLS door één van de servers niet wordt ondersteund of een versleutelde verbinding om een andere reden niet tot stand kan worden gebracht, wordt automatisch teruggevallen op een niet-versleutelde verbinding. Dit wordt opportunistische encryptie genoemd. Door het terugvallen op een onbeveiligde

[1] *Zie bijvoorbeeld: http://www.rtlz.nl/tech/google-en-microsoft-willen-jouw-e-mails-beter-beveiligen en http://tweakers.net/nieuws/109595/internetbedrijven-willen-e-mailbeveiliging-via-smtp-verbeteren.html*

verbinding wordt voorkomen dat de leveringszekerheid kleiner zou worden bij de toepassing van STARTTLS. Dit is echter een groot nadeel voor de vertrouwelijkheid en integriteit van e-mailverkeer.

Een actieve aanvaller kan het gebruik van STARTTLS eenvoudig blokkeren, een zogeheten STRIPTLS- aanval. Een actieve aanvaller manipuleert het berichtenverkeer. Het tot stand brengen van een beveiligde TLS-verbinding met STARTTLS gebeurt immers via een niet-versleutelde verbinding. Door in het eerste stadium het aanbod van een versleutelde verbinding te blokkeren, gaat de verzendende server er vanuit dat TLS niet beschikbaar is. De verzendende server kiest er dan voor om door te gaan met de niet-versleutelde verbinding. Door deze manipulatie van het berichtenverkeer is het voor de actieve aanvaller mogelijk om de verbinding af te luisteren en e-mails te lezen. Recent onderzoek heeft aangetoond dat dergelijke aanvallen wereldwijd op grote schaal plaatsvinden[2].

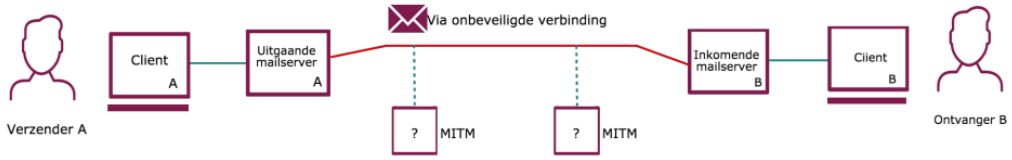
DANE
Bij het maken van een veilige verbinding naar een onbekende partij is een online controle op de authenticiteit van de verzendende partij en de eindbestemming wenselijk. Dit kan door middel van (gepubliceerde) certificaten die door certificaatautoriteiten (CA's) binnen het PKI-stelsel zijn uitgegeven of door self-signed certificates.

DANE maakt het voor de eigenaar van een domein mogelijk om via een met DNSSEC beveiligd DNS-record extra informatie bovenop de offline certificaten aan te reiken. Hierdoor kan real-time een controle worden gedaan op de authenticiteit van de server en of de server-to-server-verbinding legitiem is en niet wordt gemanipuleerd. DANE is dan ook met name belangrijk tegen actieve aanvallers.

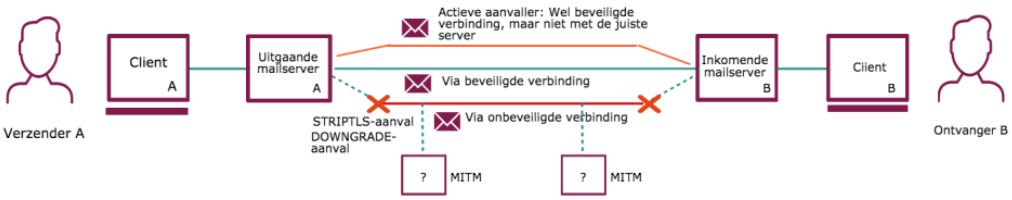
Het DANE-record kan gezien worden als een digitale vingerafdruk. Hierdoor kan het naast (of in plaats van) de certificaten van CA's worden gebruikt. DANE biedt real-time validatie per individueel certificaat, in plaats van offline per aanbieder: dit zou het gebruik van domain validated certificates op termijn overbodig kunnen maken.

Toepassing van STARTTLS in combinatie met DANE
De toepassing van STARTTLS in combinatie met DANE maakt het mogelijk om verbindingen die in principe niet als beveiligd beschouwd mogen worden (hetzij omdat er geen enkele beveiliging op zit, hetzij omdat alleen zogenaamde 'opportunistische' encryptie mogelijk is) om te zetten naar een gecontroleerde, beveiligde verbinding voor e-mailverkeer. Hierdoor is het voor aanvallers niet meer mogelijk om berichtenverkeer 'af te luisteren' of te manipuleren. Door het gebruik van STARTTLS en DANE weet de verzendende mailserver dat de e-mail daadwerkelijk via een versleutelde verbinding is verstuurd naar een mailserver van de ontvangende partij. De toepassing van STARTTLS in combinatie met DANE kan worden gezien als een 'HTTPS' voor e-mail.

[2] http://dl.acm.org/citation.cfm?id=2815695.



Figuur 1. E-mailverkeer zonder gebruik van TLS, STARTTLS en DANE



Figuur 2. E-mailverkeer met gebruik van TLS en STARTTLS

Figuur 3. E-mailverkeer met gebruik van TLS, STARTTLS en DANE

Als functioneel toepassingsgebied voor STARTTLS en DANE wordt dan ook geadviseerd:
Inkomende mailservers passen STARTTLS (SMTP over STARTTLS, oftewel ESMTPS) in combinatie met DANE toe, 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).[3]

Dit functioneel toepassingsgebied geldt voor alle mailverbindingen buiten de eigen (besloten) infrastructuur. Met andere woorden: de communicatie met mailservers buiten de eigen invloedssfeer. Het toepassen van de combinatie van STARTTLS en DANE voor inkomend e-mailverkeer zorgt dat alle partijen veilig e-mailberichten kunnen sturen aan de organisaties in het organisatorisch werkingsgebied.

In diverse baselines zoals de Baseline Informatiebeveiliging Rijksdienst (BIR), Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en de Baseline Informatiebeveiliging waterschappen (BIWA) is opgenomen dat persoonsgegevens niet onversleuteld over onbeveiligde/onvertrouwde netwerken verzonden mogen worden. Het gebruik van geforceerde encryptie wordt zodoende afgedwongen door deze baselines.

Als organisatorisch werkingsgebied van STARTTLS en DANE wordt geadviseerd:
Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-)publieke sector.

[3] IETF RFC 3207 (https://tools.ietf.org/html/rfc3207), RFC 3848 (https://tools.ietf.org/html/rfc3848) en IETF RFC 7672 (https://tools.ietf.org/html/rfc7672).

2. Hoe is het proces verlopen?

Om tot dit forumadvies te komen hebben achtereenvolgens een intakegesprek, experttoetsing en openbare consultatie plaatsgevonden. Naar aanleiding van de intake is besloten om STARTTLS en DANE in behandeling te nemen. Aan de experttoetsing hebben (toekomstig) eindgebruikers, leveranciers, adviseurs en andere kennishebbers deelgenomen.

De conclusie uit de expertgroep was om STARTTLS en DANE op te nemen op de lijst met open standaarden met 'pas toe of leg uit'-verplichting, onder voorwaarde dat er binnen het organisatorisch werkingsgebied tenminste twee organisaties de standaarden succesvol hebben geïmplementeerd.

Het expertadvies is gepubliceerd ten behoeve van een openbare consultatie waarbij gevraagd is naar STARTTLS en DANE. Naar aanleiding hiervan is één reactie ontvangen. Deze reactie heeft geen invloed op onderliggend forumadvies. Wel zijn er ontwikkelingen in de markt met betrekking tot SMTP STS die aanvullend onderzoek vergen.

3. Hoe scoren de standaarden op de toetsingscriteria?

Toegevoegde waarde

De Nederlandse overheid moet vertrouwelijke informatie beschermen tegen afluisteren door aanvallers, hieronder wordt ook de communicatie tussen overheden onderling, tussen overheden en het bedrijfsleven en tussen overheden en burgers verstaan. Technisch zijn de standaarden eenvoudig en tegen geringe kosten te implementeren. Door de implementatie van de standaarden ontstaat een relatie tussen e-mailbeheerders en DNS-beheerders. Zij moeten bijvoorbeeld afstemmen over de toevoeging en het onderhoud van DANE-records in de DNS. Hoewel deze partijen niet vanzelfsprekend een samenwerkingsrelatie hebben is afstemming tussen deze partijen noodzakelijk. De kosten voor deze afstemming kan per implementatie verschillen.

Geconcludeerd wordt dat de standaarden voldoende toegevoegde waarde hebben binnen het gekozen functioneel toepassingsgebied en organisatorisch werkingsgebied. Het is echter op dit moment niet duidelijk of, en in welke mate, de onlangs geïntroduceerde standaard SMTP STS invloed heeft op de toegevoegde waarde van de combinatie STARTTLS en DANE.

Open standaardisatieproces

STARTTLS en DANE worden beheerd door de Internet Engineering Task Force (IETF), een internationale standaardisatieorganisatie. Geconcludeerd wordt dat het het standaardisatieproces van IETF voldoende open is: IETF kent goed gedocumenteerde en open beheerprocedures, er is geen lidmaatschap, het beheerproces en de besluitvorming hieromtrent is open en transparant. Documentatie is kosteloos verkrijgbaar.

IETF beheert naast STARTTLS en DANE ook andere standaarden op het gebied van internet en e-mail, zoals DNSSEC, TLS, IMAP, SMTP, POP3, HTTP(S), IPv6, DKIM en SPF.

Draagvlak
Het gebruik van de standaarden is binnen het geadviseerde organisatorische werkingsgebied nog beperkt. Het NCSC heeft de standaarden onlangs succesvol geïmplementeerd. Ook zijn er positieve signalen bij andere overheidspartijen om de standaarden op korte termijn in gebruik te nemen.

Opname bevordert de adoptie
Opname van de standaarden is een passend middel om een bredere adoptie van de standaard binnen de (semi-)overheid te bevorderen. Het gebruik van de standaarden is nog niet in alle gevallen vanzelfsprekend.

Toelichting van eventuele risico's
Er zijn geen specifieke risico's geïdentificeerd.

4. Wat is de conclusie van de expertgroep en de consultatie?

Conclusie van de expertgroep
De expertgroep adviseert het Forum Standaardisatie en het Nationaal Beraad Digitale Overheid om STARTTLS en DANE op te nemen op de lijst met open standaarden, met 'pas toe of leg uit'-verplichting.

Eventuele aanvullingen vanuit de consultatie
Tijdens de openbare consultatie van het expertadvies heeft OpenFortress positief gereageerd. OpenFortress onderschrijft het belang van de standaarden en opname op de lijst met open standaarden met de status 'pas toe of leg uit'.

5. Welke additionele adviezen zijn er ten aanzien van de adoptie van de standaard?
De expertgroep doet het Nationaal Beraad de aanbeveling om bij opname op de lijst met open standaarden de volgende oproepen ten aanzien van de adoptie van de standaarden te doen:

1. Het Forum Standaardisatie wordt opgeroepen om een infographic over e-mailbeveiligingsstandaarden op te stellen om zodoende de relatie met onder andere S/MIME, PGP, IMAP(S), POP3(S), x509, DMARC, SPF en DKIM beter weer te geven.
2. NCSC wordt opgeroepen om, in aanvulling op de whitepaper 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)', een factsheet uit te brengen over het implementeren van STARTTLS en DANE. Dit dient Internet.nl vervolgens ook als uitgangspunt te nemen in hun metingen.
3. Het Forum Standaardisatie wijst er bij de mailstandaarden op de lijst met gangbare standaarden die tussen mailclient en mailserver gebruikt kunnen worden (POP, IMAP, SMTP) op dat deze bij voorkeur met TLS beveiligd moeten worden.
4. KING wordt opgeroepen om beveiligingsstandaarden als STARTTLS en DANE op te nemen op de GEMMA Softwarecatalogus.
5. Forum/Nationaal Beraad 0-meting uitvoeren naar gebruik van de standaarden.
6. Mailproviders van het Rijk aanspreken via ICCIO/CTO-raad (SSC-ICT/DICTU /Defensie).

De opgeroepen partijen worden gevraagd om één jaar na opname van de standaard over de voortgang op deze punten te rapporteren aan het Forum Standaardisatie.

Bijlagen

- Expertadvies STARTTLS en DANE
- Overzicht reacties consultatieronde