Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Beveilig verbindingen van mailservers

STARTTLS en DANE beschermen e-mailverkeer op internet

Factsheet FS-2017-01 | versie 1.1 | 4 april 2017

Verbindingen tussen mailservers zijn van oudsher zeer zwak beveiligd. STARTTLS is een uitbreiding om bestaande protocollen te voorzien van verbindingsbeveiliging. Als u alleen STARTTLS gebruikt om verbindingen tussen mailservers te beveiligen, helpt dat tegen zogenaamde passieve aanvallers. Een actieve aanvaller kan het gebruik van STARTTLS eenvoudig ongedaan maken. U kunt met behulp van DANE op een betrouwbare manier duidelijk maken dat uw mailservers via een beveiligde verbinding bereikbaar zijn.

Het NCSC adviseert om STARTTLS en DANE in te schakelen voor al het inkomende en uitgaande e-mailverkeer van uw organisatie.

Achtergrond

Verbindingen tussen mailservers zijn van oudsher zeer zwak beveiligd. Het protocol voor e-mailverkeer, SMTP, stamt al uit 1982.[1] De ontwerpers van het protocol hebben toen niet opgenomen dat verbindingen tussen mailservers versleuteld moeten worden. Veel mailservers staan daarom nog altijd onversleutelde verbindingen toe.

STARTTLS is een uitbreiding om bestaande protocollen te voorzien van verbindingsbeveiliging. Voor SMTP is het gebruik van STARTTLS gestandaardiseerd in RFC 3207.[2]

Doelgroep

Informatiebeveiligers en beheerders van e-mail en DNS-servers

Aan deze factsheet hebben bijgedragen:

Atos, dmarcian, Forum Standaardisatie, Gemeente 's-Hertogenbosch, KPN CISO, NLnet Labs, SIDN Labs, Sonnection, SSC-ICT

[1] Het SMTP-protocol is voor het eerst gestandaardiseerd in RFC 821. De huidige versie is RFC 5321: https://datatracker.ietf.org/doc/rfc5321/.
[2] Zie https://datatracker.ietf.org/doc/rfc3207/.

Wat is er aan de hand?

Als u alleen STARTTLS gebruikt om verbindingen tussen mailservers te beveiligen, helpt dat tegen zogenaamde ***passieve*** aanvallers. STARTTLS voorkomt afluisteren van de verbinding als een aanvaller de inhoud van de verbinding slechts leest en dus niet verandert. Een aanvaller die zich zo gedraagt noemt men een passieve aanvaller. Een ***actieve*** aanvaller, die het verkeer dus wel verandert, kan het gebruik van STARTTLS eenvoudig ongedaan maken. De aanvaller verandert het verkeer zó, dat de verzendende mailserver denkt dat de ontvangende mailserver geen STARTTLS ondersteunt. Andersom doet hij dat ook. Populair spreekt men dan van een STRIPTLS-aanval.

U kunt met behulp van DANE duidelijk maken dat uw mailservers via een beveiligde verbinding bereikbaar zijn en dat een beveiligde verbinding uw voorkeur heeft.[3] DANE is een protocol om informatie over verbindingsbeveiliging aan te bieden via DNS. Deze informatie is verifieerbaar met DNSSEC.[4] Een STRIPTLS-aanval is niet meer mogelijk als de verzender en ontvanger van een e-mail DANE gebruiken. Als u DANE gebruikt, kunnen andere mailservers betrouwbaar berichten versturen naar uw mailservers. Ook kan uw organisatie betrouwbaar e-mailen naar organisaties die DANE gebruiken voor hun mailservers.

Het Nationaal Beraad heeft in september 2016 besloten om STARTTLS en DANE voor e-mailverkeer toe te voegen aan de pas-toe-of-leg-uit-lijst met open standaarden.[5] Daarmee is voor overheden verplicht om deze standaarden toe te passen bij het investeren in e-mailsystemen.

Wat kan er gebeuren?

Als u geen STARTTLS en DANE gebruikt om verkeer van en naar uw mailservers te beveiligen, kunnen kwaadwillenden het netwerkverkeer van en naar uw mailservers onderscheppen. Dit netwerkverkeer bevat de inhoud van alle e-mails die deze mailserver afhandelt. Een aanvaller moet daarvoor wel toegang hebben tot het netwerkverkeer van uw mailserver. Voor een buitenlandse inlichtingendienst of een criminele organisatie is dit een realistisch aanvalsscenario.

Het is niet te zeggen hoeveel passieve aanvallen er plaatsvinden op onversleuteld verkeer van en naar mailservers. Het gedrag van de aanvaller is immers volledig onzichtbaar. Zulke aanvallen zijn echter erg rendabel. Ze leveren aanvallers immers veel vertrouwelijke informatie op van de organisatie die het doelwit is.

STRIPTLS-aanvallen komen in de praktijk voor. In 2015 toonden onderzoekers aan dat de STARTTLS-bescherming naar mailservers van Google vanuit zeven landen bij meer dan twintig procent van de e-mail gestript wordt. In bepaalde gevallen liep dit percentage op tot bijna honderd procent.[6] Deze e-mails zijn dus onversleuteld over het internet verstuurd.

STARTTLS en DANE beschermen tegen andere dreigingen dan OpenPGP en S/MIME

Er bestaan meer standaarden om vertrouwelijke e-mails veilig te versturen. U kunt e-mail end-to-end versleutelen met behulp van de standaarden OpenPGP of S/MIME. U versleutelt dan de inhoud van de e-mail zelf. Iemand die meeluistert op de verbinding kan de inhoud van de e-mail niet lezen.

Enerzijds beschermt OpenPGP of S/MIME tegen dreigingen waar STARTTLS en DANE niet tegen beschermen. Als een aanvaller binnendringt op de mailserver, kan hij alsnog de inhoud van de e-mails niet lezen. Anderzijds beschermen STARTTLS en DANE *alle* e-mails tussen mailservers die deze standaarden toepassen. De gebruiker hoeft hiervoor niets te doen. Verder beschermen STARTTLS en DANE de hele e-mail, inclusief metadata als verzender en onderwerpregel. OpenPGP of S/MIME beschermt alleen de inhoud van de e-mail.

Wat adviseert het NCSC?

Het NCSC adviseert om STARTTLS en DANE in te schakelen voor al het ***inkomende*** e-mailverkeer van uw organisatie. Op die manier kan elke andere organisatie betrouwbaar communiceren met uw mailservers.

Het NCSC adviseert verder om STARTTLS en DANE in te schakelen voor al het ***uitgaande*** e-mailverkeer van uw organisatie. Andere organisaties zullen ook STARTTLS en DANE inschakelen voor hun inkomende e-mailverkeer. Uw organisatie kan dan betrouwbaar communiceren met andere organisaties die STARTTLS en DANE toepassen op hun inkomende mailservers.

STARTTLS en DANE op inkomend e-mailverkeer

Om STARTTLS en DANE op inkomend e-mailverkeer te implementeren, schakelt u eerst STARTTLS in op elke inkomende mailserver. Vervolgens publiceert u voor deze

[3] Dit gebruik van DANE is gestandaardiseerd in RFC 7672: https://datatracker.ietf.org/doc/rfc7672/.
[4] DNSSEC is gestandaardiseerd in RFC 4033 (https://datatracker.ietf.org/doc/rfc4033/), RFC 4034 (https://datatracker.ietf.org/doc/rfc4034/) en RFC 4035 (https://datatracker.ietf.org/doc/rfc4035/).
[5] Zie verder https://www.forumstandaardisatie.nl/nieuws/nationaal-beraad-verplicht-starttls-en-dane.
[6] Bron: Neither Snow Nor Rain Nor MITM...: An Empirical Analysis of Email Delivery Security, https://dl.acm.org/citation.cfm?id=2815695.

TLSA-records maken

U maakt voor elke mailserver twee TLSA-records aan. Het ene record, het '2 1 1'-record, verwijst naar de CA. Het andere record, het '3 1 1'-record, verwijst naar het certificaat zelf. Op die manier leiden kleine fouten in de configuratie niet meteen tot onbeschikbaarheid van uw e-mailvoorziening.[8]

Gebruik de tool tlsa uit het pakket hash-slinger om eenvoudig TLSA-records te genereren.[9][10]

Download eerst de certificaten van de server (server.pem) en de CA (CA.pem) naar uw werkstation. In de voorbeelden nemen we aan dat uw mailserver de FQDN mail.example.nl heeft.

Aanmaken van een '2 1 1'-record:

```
$ python tlsa --create --port 25 --usage 2
--selector 1 --certificate CA.pem
mail.example.nl
```

Aanmaken van een '3 1 1'-record:

```
$ python tlsa --create --port 25 --usage 3
--selector 1 --certificate server.pem
mail.example.nl
```

servers TLSA-records in de DNS-zone van de servers. De DNS-zones moeten beschermd zijn met DNSSEC.

Inventariseer op welke mailservers uw organisatie e-mail ontvangt. Neem de servers op die e-mail ontvangen van andere externe mailservers. Dat kunnen ook servers zijn die u niet beheert, zoals servers van een spamfilterdienst. Neem elke server op die in de MX-records van de domeinnamen van uw organisatie staat. U kunt ook interne e-mailstromen beveiligen met STARTTLS en DANE. U kunt deze e-mailstromen echter ook met alternatieve maatregelen beveiligen, zoals het pinnen van een certificaat. Mogelijk gebruikt uw organisatie zulke maatregelen al.

Kies of u STARTTLS aanbiedt met behulp van een openbare certificaatautoriteit (CA) of een eigen certificaatautoriteit.[7] Gebruik alleen een eigen CA als u de kennis en middelen heeft om deze op te zetten en te onderhouden. Zorg dat elke mailserver zijn eigen certificaat heeft. Zet de fully qualified domain name (FQDN) van de mailserver in het certificaat als Subject Alternative Name.

Schakel op elke mailserver op uw lijst STARTTLS in. Stel STARTTLS in op basis van de ICT-beveiligingsrichtlijnen voor Transport Layer Security.[11] Gebruik het certificaat dat u voor deze server heeft aangemaakt. Stel de server zo in dat hij de hele keten van certificaten tot en met de CA meestuurt.

Controleer of de server ook daadwerkelijk via STARTTLS bereikbaar is. Gebruik daarvoor bijvoorbeeld de e-mailtest op internet.nl. Sommige firewalls zijn standaard zo ingesteld dat ze STARTTLS strippen van alle inkomende e-mailstromen. Als uw server niet bereikbaar is via STARTTLS, pas dan de netwerkconfiguratie aan om de server wel via STARTTLS bereikbaar te maken.

Publiceer voor elke mailserver informatie over het certificaat en de CA in TLSA-records in de DNS-zone van de mailserver. Handelt bijvoorbeeld de mailserver mail.example.nl de e-mail af van het domein example.org, dan plaatst u de TLSA-records in de DNS-zone example.nl. Zie het kader 'TLSA-records maken' voor gedetailleerde instructies.

Zorg dat DNSSEC is ingeschakeld, zowel op de DNS-zone van het e-maildomein als op de DNS-zone waarin de TLSA-records staan.[12] DNSSEC zorgt ervoor dat verzendende mailservers de authenticiteit van informatie in TLSA-records kunnen controleren. Alleen met DNSSEC heeft het publiceren van TLSA-records effect.

Controleer regelmatig of uw instellingen kloppen en werken.[13] Gebruik daarvoor bijvoorbeeld de mailtest op internet.nl of de DANE SMTP-tool van sys4.[14] Controleer ook of uw DNSSEC-instellingen kloppen en werken. Als u DANE en STARTTLS gebruikt voor e-mail, hangt de beschikbaarheid van uw e-mailvoorziening af van DNSSEC.

[7] In dit scenario is het externe gebruik van een interne CA geoorloofd omdat het vertrouwen in de CA afgeleid wordt uit de informatie in DNS. Verzendende mailservers kunnen deze informatie controleren met behulp van DNSSEC.

[8] Deze methode is gebaseerd op de analyse uit http://postfix.1071664.n5.nabble.com/WoSign-StartCom-CA-in-the-news-td86436.html#a86444 en volgt het advies in de publicatie 'Trustworthy Email' van het NIST (https://www.nist.gov/node/1099976).

[9] Zie https://github.com/letoams/hash-slinger. Hash-slinger is ook beschikbaar in package managers van populaire Linuxdistributies.

[10] U kunt TLSA-records ook genereren met OpenSSL (voorbeeld in https://www.dnssec.nl/cases/tweeluik-dane-deel-ii-tlsa-records-voor-mail.html).

[11] Zie https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html.

[12] Voor Nederlandse overheden is het gebruik van DNSSEC al sinds 2012 verplicht via de pas-toe-of-leg-uit-lijst van open standaarden: https://www.forumstandaardisatie.nl/standaard/dnssec.

[13] Een overzicht van veelgemaakte fouten bij het toepassen van DANE en STARTTLS staat op https://dane.sys4.de/common_mistakes.

[14] Zie https://dane.sys4.de/.

Certificaten vervangen

Vervang het certificaat van een mailserver als het binnenkort verloopt, of als u het vermoeden heeft dat een aanvaller de geheime sleutel heeft weten te stelen.

Genereer eerst het nieuwe certificaat en laat het ondertekenen door uw eigen of de openbare CA. Stel het in op de mailserver. Wijzig daarna het TLSA-record met type '3 1 1' van de mailserver zodat het verwijst naar het nieuwe certificaat.

Wisselen van certificaatautoriteit

De voorgaande instructies voor het vervangen van een certificaat gaan ervan uit dat het nieuwe certificaat is uitgegeven door dezelfde certificaatautoriteit als het oude certificaat. In de periode tussen het vervangen van het oude certificaat en het aanpassen van het TLSA-record met type '3 1 1' vindt validatie plaats op basis van het '2 1 1'-record.

Wilt u een nieuw certificaat gebruiken van een andere certificaatautoriteit, vervang dan eerst het TLSA-record met type '2 1 1' door een TLSA-record met type '2 1 1' dat verwijst naar de nieuwe CA. Wacht vervolgens tot de TTL (time-to-live) van de TLSA-records verlopen is. Het oude '2 1 1'-record komt dan niet meer in caches van DNS-servers voor. Voer vervolgens de procedure uit de sectie 'Certificaten vervangen' uit: genereer een nieuw certificaat, laat het ondertekenen door de nieuwe CA, stel het in op de mailserver en vervang het '3 1 1'-record.

STARTTLS en DANE op uitgaand e-mailverkeer

Om STARTTLS en DANE op uitgaand e-mailverkeer te implementeren, schakelt u DANE-validatie in op elke uitgaande mailserver van uw organisatie. Deze mailserver moet daarvoor wel DNSSEC-validatie uit kunnen voeren.

Inventariseer welke mailservers e-mail versturen voor uw organisatie. Neem de servers op die e-mail versturen aan andere externe mailservers. U kunt ook interne e-mailstromen beveiligen met STARTTLS en DANE. U kunt deze e-mailstromen echter ook met alternatieve maatregelen beveiligen, zoals het pinnen van een certificaat. Mogelijk gebruikt uw organisatie zulke maatregelen al.

Ga van elke mailserver op uw lijst na of de gebruikte mailserversoftware DANE en STARTTLS ondersteunt voor uitgaande e-mail. Raadpleeg hiervoor de documentatie van uw mailserver of vraag het aan uw leverancier.

Ondersteunt een mailserver DANE en STARTTLS, schakel dit dan in. Gebruik de optie om DANE-validatie alleen te doen als er TLSA-records beschikbaar zijn. Deze optie heet ook wel 'opportunistische DANE-validatie'. Zorg dat de mailserver beschikt over een betrouwbare verbinding naar een DNSSEC-validerende recursive DNS-nameserver. Doe dit bijvoorbeeld door er lokaal op de mailserver een te draaien.

Als een mailserver geen DANE maar wel STARTTLS ondersteunt, dan kan deze mailserver verbindingen met externe mailservers niet automatisch beveiligen tegen actieve aanvallers. Vraag de leverancier van uw mailserversoftware wanneer hij DANE zal gaan ondersteunen. Richt als tijdelijk alternatief een aparte mailserver in als relay voor deze mailserver. Gebruik op deze nieuwe mailserver software die wel STARTTLS en DANE ondersteunt.[15] Gebruik certificate pinning om de verbinding tussen de bestaande en de nieuwe server te beveiligen. Schakel ondersteuning voor STARTTLS en DANE in op de nieuwe server, volgens de instructies uit de vorige alinea.

Tot slot

Als u al uw e-mailverkeer wilt beveiligen met DANE en STARTTLS, moet u dit implementeren op uw inkomende én uw uitgaande e-mailverkeer. Dit hoeft u echter niet tegelijk te doen. U kunt bijvoorbeeld besluiten om nu al uw inkomende verkeer te voorzien van bescherming met DANE en STARTTLS, maar uw uitgaande verkeer pas later te doen. Zo bent u voor uw contacten al wel via een betrouwbare verbinding te bereiken.

Het heeft pas zin om uw inkomende e-mailverkeer voor een bepaald e-maildomein te beschermen met DANE en STARTTLS als u dat voor alle inkomende mailservers van dat e-maildomein doet. Een actieve aanvaller kan anders de toegang tot de beveiligde mailservers blokkeren om zo een onversleutelde verbinding af te dwingen. Voor uitgaand e-mailverkeer geldt dit niet. Elke uitgaande mailserver die u voorziet van bescherming met DANE en STARTTLS is een vooruitgang.

Schakel in elk geval STARTTLS in voor al uw inkomende en uitgaande e-mailverkeer, ook als u het toepassen van DANE nog uitstelt. Tegen passieve aanvallers is STARTTLS op zichzelf een effectieve maatregel.

Monitor de mate waarin de certificaten van uw mailservers geldig zijn en de TLSA-records kloppen. Er zijn twee TLSA-records voor elke mailserver. Van deze twee moet er op elk gegeven moment een kloppen om de mailserver bereikbaar te houden. Zorg daarom dat u problemen opmerkt voordat beide TLSA-records niet meer kloppen.

[15] Bij publicatie van deze factsheet ondersteunen Postfix en Halon al DANE en STARTTLS. De ontwikkelaars van Exim werken aan ondersteuning.

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

FS-2017-01 | versie 1.1 | 4 april 2017