edustandaard

Uniforme Beveiligingsvoorschriften

Veilig en betrouwbaar e-mailverkeer

Datum	23-12-2021
Versie	1.0 Definitief
Auteur	Edustandaard werkgroep Uniforme Beveiligingsvoorschriften

INHOUDSOPGAVE

Historie

Versie	Auteur	Toelichting	Datum
0.1	Jordy van den Elshout	Eerste concept	11 augustus 2020
0.2	Jordy van den Elshout	Commentaar van de bijeenkomst (Sep 2020) verwerkt in de voorschriften.	6 oktober 2020
0.3	Jordy van den Elshout	Commentaar van de bijeenkomst (Sep 2020) verwerkt in de voorschriften.	2 november 2020
0.4	Jordy van den Elshout	Voorschriften incl. implementatie ervan aangevuld en aangescherpt. Tevens een gefaseerde aanpak toegevoegd in hoofdstuk 5.	8 december 2020
0.5	Jordy van den Elshout	Laatste opmerkingen verwerkt. Versie ter consultatie.	9 februari 2021
0.9	Jordy van den Elshout	Op basis van laatste opmerkingen - waaronder uit de consultatie - bijgewerkt. Versie ter vaststelling.	27 mei 2021
1.0	Jordy van den Elshout	Op basis van advies Bureau Edustandaard bijgewerkt. Versie na goedkeuring Standaardisatieraad.	23 december 2021

1 Inleiding

1.1 Achtergrond

Bureau Edustandaard heeft een (advies)verzoek van het 'Ketenregieoverleg PO-VO' (hierna: KRO) gekregen voor de implementatie van de WDO-beveiligingsstandaarden in het onderwijs. Bureau Edustandaard heeft daarvoor de werkgroep Uniforme beveiligingsvoorschriften (UBV) de opdracht gegeven om WDO-beveiligingsstandaarden in onderwijscontext te plaatsen en uit te werken in voorschriften.

De WDO-beveiligingsstandaarden zijn opgesteld voor overheidsorganisaties, zoals ministeries, uitvoeringsorganisatie en gemeentes. Dat zijn andere soorten organisaties, dan een schoolinstelling. Qua omvang en beschikbare middelen, zoals expertise. Dat betekent dat er ook extra aandacht besteed wordt aan effectiviteit van de WDO-beveiligingsstandaarden en de wijze van implementatie: stappenplan in combinatie met voorbeeld configuraties (best practices).

De WDO-Beveiligingsstandaarden verwijzen naar de verplichte lijst van Forum Standaardisatie, met open standaarden. Deze lijst wordt als uitgangspunt genomen, maar niet uitputtend. Ook andere relevante standaarden en of configuraties daarvan die bijdragen aan een veilig en betrouwbare e-mail worden meegenomen. Ambitie van de werkgroep UBV is om de relevante WDO beveiligingsstandaarden uit te werken tot maatregelen die goed implementeerbaar zijn en effectief zijn voor het onderwijs domein. In dit document worden afspraken voor veilig en betrouwbaar e-mailverkeer behandeld. Dat betekent dat de voorschriften van toepassing zijn rondom het verkeer en niet over het e-mailbericht zelf of de verdere afhandeling daarvan in de e-mailtoepassing. De voorschriften (*donkergroen gemarkeerd*) zijn verplicht en vallen onder een pas-toe-leg-uit principe. Voor een advies (*lichtgroen gemarkeerd)* geldt dat niet.

1.2 Doel

Het in samenhang presenteren van een eenduidige set van beveiligingsvoorschriften waarmee de veiligheid en betrouwbaarheid van e-mailverkeer in het onderwijs bevorderd wordt.

1.3 Doelgroep

Deze voorschriften gelden voor onderwijsinstellingen en andere organisaties die e-mail verzorgen en/of beheren voor het onderwijs. Dat geldt voor de hele onderwijssector (PO, VO, MBO en HO).

1.4 Samenhang met andere initiatieven

Deze voorschriften zijn onderdeel van de Uniforme beveiligingsvoorschriften (UBV) voor het onderwijs.

De meeste voorschriften komen voort uit de WDO-Beveiligingsstandaarden, de lijst met verplichte standaarden van Forum Standaardisatie.

Sommige voorschriften gelden op basis van een BIV-classificatie. Hiervoor wordt gebruikt gemaakt van het 'Certificeringsschema informatiebeveiliging en privacy ROSA' van Edustandaard.

1.5 Taken en verantwoordelijkheden

Het eigenaarschap van deze voorschriften is belegd binnen Edustandaard, waar ook andere afspraken binnen het onderwijsdomein worden beheerd. Het beheer en de doorontwikkeling wordt uitgevoerd door de Edustandaard werkgroep Uniforme Beveiligingsvoorschriften (UBV).

1.6 Beheer en doorontwikkeling

Binnen Edustandaard wordt periodiek (minimaal eenmaal per jaar) de opzet en de werking van de voorschriften besproken met alle relevante stakeholders die vertegenwoordigd zijn in de Standaardisatieraad. Hiertoe wordt input verzameld vanuit de Edustandaard werkgroep Uniforme beveiligingsvoorschriften en vanuit Edu-K.

2 Algemeen

2.1 Welke standaarden

SPF, DKIM & DMARC worden vaak in één adem genoemd. En dat is logisch aangezien ze gezamenlijk het meest effectief zijn. Het gebruik van deze standaarden vergroot de afleverbetrouwbaarheid van email en voorkomt misbruik (e-mail)domeinnaam door derden (phishing). De ontvangende partij moet de configuratie van deze standaarden wel controleren, wat betekent dat naast het instellen voor uitgaande verkeer, de filtering op ingaande verkeer ook ingesteld moet worden.

Voor een veilige configuratie zijn bovengenoemde standaarden afhankelijk van DNSSEC. Ook is het een belangrijke randvoorwaarden voor de werking van DANE, want *"Alleen met DNSSEC heeft het publiceren van TLSA records[1] effect"* (NCSC, Factsheet Beveilig verbindingen van mailservers). Deze standaard komt breder aan bod onder het thema UBV - TLS.

STARTTLS & DANE zorgt dat communicatie - de verbinding, niet het e-mailbericht zelf - tussen mailservers beveiligd is, zodat de integriteit en vertrouwelijkheid van het e-mailverkeer wordt beschermd. DANE voorkomt een downgrade attack naar een onversleutelde verbinding van SMTP.

Op de website internet.nl kan eenvoudig de toepassing van deze standaarden worden gecontroleerd.

2.2 Bron voor voorschriften

Voor de voorschriften wordt waar mogelijk gebruik gemaakt van 'hoger gelegen' afspraken. Bij voorkeur internationale afspraken (zoals van IANA), indien nodig nationale afspraken (zoals van Forum Standaardisatie en NCSC) en alleen als die niet voldoen aanvullende afspraken die in deze werkgroep worden gemaakt. Voor de volledigheid worden deze in basis overgenomen en voor details verwezen. Afwijken van bovenliggende afspraken wordt onderbouwd.

2.2.1 Forum Standaardisatie

De WDO-beveiligingstandaarden verwijzen naar de lijst met verplichte standaarden van Forum Standaardisatie. Welke relevant zijn voor e-mail (DKIM, DMARC, SPF, STARTTLS en DANE) worden als uitgangspunt genomen.

2.2.1 NCSC Factsheet

Voor voorschriften wordt in basis het advies uit de factsheets van NCSC gevolgd. Bij het maken van nadere invulling wordt gerefereerd aan deze factsheets. Dat betekent dat deze geraadpleegd kunnen worden voor aanvullende informatie.

Advies: MAIL-ALG-01
Raadpleeg de factsheets 'Bescherm domeinnaam tegen phishing'[2] en 'Beveilig verbindingen van mailservers'[3] van NCSC voor aanvullende informatie.

[1] Een TLSA-record (Transport Layer Security Authentication) wordt gebruikt om aan te geven wat het certificaat of publiek key is voor de TLS-verbinding voor de domeinnaam.
[2] https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-bescherm-domeinnamen-tegen-phishing
[3] https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-beveilig-verbindingen-van-mailservers

3 Bescherm domeinnamen tegen misbruik

Een domeinnaam dient beschermd te worden, zodat ongeautoriseerden niet met die domeinnaam e-mail kunnen verzenden en misbruiken voor een aanval, zoals phishing. Wanneer een domein beschermd is, draagt dit ook bij aan een hogere afleverbetrouwbaarheid van e-mail; de kans dat deze niet aankomt of in de SPAM-folder komt, wordt daarmee verkleind.

"Het NCSC adviseert om elke domeinnaam van uw organisatie te voorzien van e-mailauthenticatie met behulp van SPF, DKIM en DMARC. Daarnaast adviseert het NCSC om alle uitgaande e-mail van uw organisatie met behulp van DKIM te ondertekenen"

Dit is een citaat uit de factsheet van NCSC Bescherm domeinnamen tegen phishing. Deze factsheet beschrijft tevens de aanleiding hiervan en geeft een beschrijving van SPF, DKIM en DMARC. Ook wat de voor- en nadelen hiervan zijn. Daarom wordt dit hier niet nader toegelicht. De nadruk ligt meer op de wijze van implementatie en effectiviteit daarvan in het onderwijsdomein.

3.0 Niet gebruikte domeinnamen blokkeren

Om misbruik van een niet gebruikte domeinnaam te voorkomen, dient deze geblokkeerd te worden op het versturen van e-mail. Dat geldt dus ook voor domeinnamen die alleen geregistreerd zijn en niet gebruikt worden (geparkeerde domeinnamen).

Voorschrift: MAIL-BESCHERM-001 (Betrouwbaarheid)
Wanneer een domeinnaam niet gebruikt wordt voor e-mail, plaats dan per domeinnaam: - een zogenaamd “null MX” record in de DNS zone. - een “SPF -all” record in de DNS zone. - een “DMARC p=reject” record in de DNS Zone. - geen DKIM record.

Implementatie: er is inzicht nodig welke domeinnamen in bezit zijn en welke daarvan niet gebruikt worden voor e-mail. Op dat moment is de implementatie met weinig middelen te realiseren.

3.1 E-mailconfiguratie scheiden in (sub)domeinen

De toepassing van SPF, DKIM en DMARC kan het nodige werk met zich meebrengen. Ook kan het nodig zijn om verschillend beleid toe te passen voor verschillende soorten e-mail(stromen). Bijvoorbeeld automatische berichten uit een systeem versus e-mail van medewerkers of studenten. Mocht er een fout in de configuratie ontstaan of een domein op de blacklist komen, dan heeft dit niet direct impact op alle e-mailstromen. Dit verkleint ook de kans op het bereiken van het maximale aantal *lookups* van een SPF-record (maximum is 10).

Advies: MAIL-BESCHERM-002 (Betrouwbaarheid)
Advies is om per e-mailstroom één (sub)domein te hanteren.

Een goed voorbeeld hiervan is de scheiding tussen de e-mailstroom voor marketing en de standaard e-mail van medewerkers. Indien een (sub)domein geblokkeerd wordt door een marketingactie, zou dit geen effect moeten hebben op de beschikbaarheid van e-mail voor medewerkers.

Implementatie: er is inzicht nodig in e-mailstromen. Dat inzicht kan bewerkstelligd worden met DMARC-rapportage (zie §3.2.4. DMARC Rapportage). Vervolgens kan de scheiding bepaald en geconfigureerd worden. Hoeveelheid werk is afhankelijk van het aantal e-mailstromen en systemen die e-mail versturen,

3.2 Configuratie per (sub)domein

Elk (sub)domein dat gebruikt wordt voor e-mail, dient geconfigureerd te worden. Het is wel van belang dat de configuratie in fases plaatsvindt, om verstoringen te voorkomen. Dat betekent dat de configuratie in de implementatiefase mag afwijken van de voorschriften. Zie hoofdstuk 5. voor de ‘Aanpak voor implementatie’.

Voorschrift: MAIL-BESCHERM-003 (Betrouwbaarheid)
Elk (sub)domein dient beveiligd te zijn tegen misbruik door toepassing van SPF, DKIM en DMARC.

Implementatie: er is inzicht nodig welke e-mailstromen er zijn. Op dat moment is de implementatie met weinig middelen te realiseren: elke e-mailstroom/systeem krijgt zijn eigen (sub)domein. Bijvoorbeeld noreply@nieuwsbrief.domeinnaam.nl als afzendadres voor het versturen van nieuwsbrieven.

3.2.1 SPF-Policy

Met *Sender Policy Framework* (SPF) kan aangegeven worden vanaf welke mailservers (IP-adressen) de e-mail van een e-maildomein verstuurd mag worden. Dit wordt met een DNS-record op het domein kenbaar gemaakt. Deze informatie is daarmee publiek bekend en wordt door de ontvangende mailserver gebruikt om controleren of de e-mail van een legitieme mailserver afkomstig is.

Per domeinnaam dient (maar) één SPF-record aangemaakt te worden: een regel die bepaalt vanaf welke mailservers e-mail afkomstig mag zijn en hoe de ontvangende server moet acteren als dit niet klopt. Daarnaast mag een SPF-record maximaal 10 DNS opvragingen bevatten: het aantal DNS-verzoeken die nodig zijn om alle ip-adressen van alle legitieme mailservers op te vragen. De test op internet.nl kan dit controleren. De opties die geen bescherming bieden “+all” (altijd accepteren) en “?all” (geen policy; bericht doorlaten), mogen niet gebruikt worden. Dat betekent dat de overige optie “~all” (softfail) of “-all” (fail) per domeinnaam toegepast moet worden.

Voorschrift: MAIL-BESCHERM-004 (Betrouwbaarheid)
Het SPF-record bestaat altijd uit de *optie* “~all” (softfail) of “-all” (fail) en alleen uit verwijzingen (ip-adres of dns-record via maximaal 10 DNS opvragingen) van servers die e-mail mogen verzenden.

Implementatie: er is inzicht nodig vanaf welke servers (IP-adressen, al dan niet via dns-record[4]) e-mail verstuurd wordt. Op dat moment is de implementatie met weinig middelen te realiseren. Inzicht kan middels een (handmatige) inventarisatie, of gebruik te maken van de DMARC-Rapportage functie. Zie hiervoor de aanpak in hoofdstuk 5. ‘Aanpak voor implementatie’.

3.2.2 DKIM

Domain Keys Identified Mail (DKIM) is het toepassen van een authenticatie op de e-mail. Hiermee kan de ontvangende partij controleren of de e-mail daadwerkelijk afkomstig is van de desbetreffende domeinnaam en niet aangepast is gedurende het transport. Alle uitgaande e-mail moet daarvoor ondertekend worden met de DKIM-sleutel, die correspondeert met de sleutel in het DNS-record (van de desbetreffende domeinnaam).

Voorschrift: MAIL-BESCHERM-005 (Betrouwbaarheid)
Alle uitgaande e-mail wordt ondertekend met DKIM, die correspondeert met de DKIM-sleutel in het DNS record van het domeinnaam (van het afzendadres). Geadviseerd wordt om dit op de relay mailserver toe te passen en andere mailservers hiervan gebruik te laten maken, zodat de configuratie niet op elk afzonderlijke mailserver toegepast hoeft te worden.

Daarnaast wordt geadviseerd om een sleutelbeleid te hanteren, zodat meerdere DKIM-sleutels worden toegepast en tijdig worden vernieuwd. Op dat moment kan een DKIM-sleutel die is gecompromitteerd, snel en eenvoudig naar een nieuwe sleutel omgeschakeld worden. De frequentie van preventief vervangen is bepalend voor de kans dat de sleutel wordt gecompromitteerd. Tegelijkertijd neemt een hogere frequentie meer werkzaamheden met zich mee. Met name met een e-mailstroom die door een derden partij wordt verzorgt. Op dat moment moet elke keer de DKIM-sleutel op een veilige wijze uitgewisseld worden. Daarin adviseert de M³AAWG[5] de frequentie van twee keer per jaar aan te houden.

[4] Een verwijzing kan via IP-adres of DNS-records, zoals a, mx of cname -record.
[5] https://www.m3aawg.org/sites/default/files/m3aawg-dkim-key-rotation-bp-2019-03.pdf

Advies: MAIL-BESCHERM-006 (Betrouwbaarheid)
Geadviseerd wordt om een sleutelbeleid te hanteren voor DKIM-sleutels waarbij een tijdige rotatie plaatsvindt en bij compromittatie snel en eenvoudig naar een andere DKIM-sleutel overgeschakeld kan worden. Frequentie van preventief vervangen kan naar eigen inzicht bepaald worden aan de hand van de situatie en gevoeligheid van de e-mailstroom. Advies hiervoor is twee keer per jaar.

Implementatie: de toepassing van DKIM vergt meer kennis en middelen dan de toepassing van SPF. Om DKIM toe te passen moet er aanvullende software geïnstalleerd (en of geconfigureerd) worden op de mailserver. Hierdoor afhankelijk van de gebruikte software van mailservers en/of providers. Wel kan er gebruik gemaakt worden van een relay mailserver, mocht een andere mailserver de ondersteuning niet bieden. Voor e-mail van leerlingen en medewerkers wordt veelal een Office 365 of Google G-Suite omgeving gebruikt. Deze omgevingen ondersteunen DKIM. Dat geldt ook voor veel andere applicaties en platformen.

3.2.3 DMARC Beleid

Domain-based Message Authentication, Reporting & Conformance (DMARC) helpt ontvangende partijen hoe om te gaan met ontvangen e-mailberichten. Het geeft instructie aan de mailserver hoe de mail af te handelen als dit afwijkt van de SPF of DKIM informatie. Het beleid zou ‘p=quarantine of ‘p=reject’ moeten zijn, om effect te hebben. Dat geldt ook voor subdomeinen (sp=quarantine of ‘sp=reject’). De beleidsoptie ‘None’ heeft geen effect, maar is wel bruikbaar voor de implementatiefase waarbij eerst alleen rapportage wordt gebruikt om inzicht te krijgen in het e-mailverkeer van op een domeinnaam.

Voorschrift: MAIL-BESCHERM-007
Het DMARC beleid is zowel voor het hoofddomein als voor de subdomeinen ‘Quarantine’ of ‘Reject’. In de implementatiefase MAG dit ‘None’ zijn.

Daarnaast kan de mate van alignment bepaald worden. De ontvangende mailserver controleert of het getoonde afzenderadres overeenkomt met het domein opgegeven onder SPF en DKIM. De waarde ‘strict’ zorgt voor een exacte vergelijking, terwijl de mailserver bij ‘relaxed’ controleert of het afzendadres binnen hetzelfde domein valt.

Voorschrift: MAIL-BESCHERM-008
Het DMARC beleid voor ‘alignment’ is minimaal ‘relaxed’.

Implementatie: vergt een gedegen aanpak, om te voorkomen dat de e-mailstroom niet verstoord wordt en uiteindelijk voldoende veiligheid en betrouwbaarheid biedt (zie aanpak in Hoofdstuk 5). Het kan met een txt-record toegevoegd worden, wat door de meeste DNS-systemen ondersteund wordt. Het zorgt ervoor dat de ontvanger weet wat er met de e-mail gedaan moet worden; als een DKIM-sleutel en SPF niet overeenkomt. Daarmee heeft het een positieve impact: betrouwbaarheid van aflevering.

3.2.4 DMARC Rapportage

Naast publiceren van het beleid, kan DMARC de domeineigenaren inzicht gevens vanaf welke servers (lees: ip-adressen) e-mail verstuurd wordt. Ook wordt hiermee inzichtelijk wat de resultaten zijn ten opzichte van het beleid . Bijvoorbeeld of het e-mailverkeer overeenkomt met DKIM en SPF (‘pass’ or ‘fail’). Het advies is om van deze functie gebruik te maken. Met name voor de implementatie, maar ook voor het onderhoud ervan: het geeft inzicht wanneer een domein misbruikt wordt of een legitieme server geblokkeerd wordt. Bijvoorbeeld door een wijziging in de ICT-omgeving waarbij het IP-adres van de mailserver is veranderd. Of wanneer een reclamebureau de opdracht heeft gekregen voor het versturen van een mailing, zonder dat hiervoor de configuratie van SPF, DKIM en DMARC is aangepast. Op dat moment voldoet de e-mailstroom niet aan het DMARC-beleid en wordt de e-mail ongewenst bij de ontvangende geweigerd of in quarantaine geplaatst.

Advies: MAIL-BESCHERM-009
Geadviseerd wordt om elk DMARC-record te voorzien van een e-mailadres voor reporting, zodat de e-mailstromen per domeinnaam inzichtelijk wordt. Het is daarbij tevens van belang dat de controle van deze rapportages geborgd is, zowel tijdens de implementatie als daarna voor het beheer.

Implementatie: er is inzicht nodig in de gebruikte domeinnamen. Het toevoegen van de juiste DMARC-record met e-mailadres voor reporting zijn eenvoudig toe te voegen, met name door gebruik van een DMARC-generator. Het analyseren van DMARC-rapportage kan omvangrijk zijn, waardoor tooling nodig kan zijn. Deze tooling breed beschikbaar en maakt het tevens op een gebruiksvriendelijke manier inzichtelijk. Ook de voortgang ervan.

3.3 Toepassing op inkomende e-mail

Voor een volledige bescherming (binnen de sector), dient naast de toepassing van SPF, DKIM en DMARC deze ook gecontroleerd te worden bij inkomende e-mail.

Voorschrift: MAIL-BESCHERM-010
Inkomende e-mail wordt gecontroleerd op SPF en DKIM volgens het DMARC-beleid van de verzendende partij.

4 Beveilig verbinding van mailservers

E-mailberichten worden door verschillende mailservers over het internet verstuurd. De communicatie hiervan kan versleuteld worden met TLS. Daarmee wordt niet de versleuteling van het e-mailbericht zelf bedoeld, maar van de verbinding tussen mailservers. Dat staat ook nader toegelicht in het het advies van NCSC; in de Factsheet Beveilig verbindingen van mailservers.

4.1 STARTTLS

Met STARTTLS wordt de communicatie tussen de mailservers beveiligd met TLS. Hiermee wordt de kans verkleind dat e-mail onderweg door ongeautoriseerde wordt aangepast of onderschept. Het biedt echter onvoldoende bescherming voor een veilige e-mailcommunicatie, gezien de afhankelijkheid van andere mailservers op het internet. Als deze geen STARTTLS ondersteunen, wordt de e-mail alsnog onbeveiligd over het internet verstuurd. Daarnaast kan een actieve aanvaller, die het verkeer verandert, STARTTLS eenvoudig ongedaan maken (*downgrade attack*).

Het advies van NCSC is: *"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."*

Net zoals bij HTTPS kan er bij STARTTLS gebruik worden gemaakt van verschillende versies en configuraties(opties) voor TLS. Aangezien niet alle versies en opties voldoende bescherming bieden, dient de configuratie veilig te zijn. Tegelijkertijd dient voorkomen te worden dat er door de beperkte configuraties teruggevallen wordt op een onbeveiligde verbinding. Uitgangspunt punt is dan ook beter minder veilig, dan onveilig.

Voorschrift: MAIL-BEVEILIG-001

Configureer STARTTLS op alle publieke mailservers (die bereikbaar zijn via het internet) voor inkomende en uitgaande e-mailverkeer.

Dit conform de 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)', waarbij zoveel mogelijk *algoritmeselecties* worden toegepast, tenzij deze 'onvoldoende' zijn.

Daarnaast wordt geadviseerd om dit ook voor het interne e-mailverkeer toe te passen, de interne mailservers en systemen die e-mail versturen. Met name als deze systemen direct bereikbaar zijn voor gebruikers; geen scheiding in netwerken.

Implementatie: de meeste providers ondersteunen dit standaard en hebben dit reeds geïmplementeerd, zoals binnen Office 365[6] en Google[7] het geval is. Indien het beheer van de mailomgeving zelfstandig wordt uitgevoerd, dient dit zelf geconfigureerd te worden met een SSL-certificaat. Software en dienstleveranciers hebben de implementatie daarvan doorgaans beschreven.

4.2 DANE

Met DANE, kort voor DNS-based Authentication of Named Entities, wordt richting andere mailservers duidelijk gemaakt dat de mailserver via een beveiligde verbinding bereikbaar is en dat een beveiligde

[6] *"By default, Microsoft 365 or Office 365 sends mail using TLS encryption, provided that the destination server also supports TLS"* - *Set up connectors for secure mail flow with a partner organization | Microsoft Docs*

[7] *"Outgoing mail: Mail won't be delivered and will bounce. You'll get a non-delivery report (NDR). Only one send attempt is made (no tries again). Incoming mail: Mail is rejected without any notification to you, although the sender will receive an NDR"* - *Require mail to be transmitted via a secure (TLS) connection - Google Workspace Admin Help*

verbinding de voorkeur heeft. Dit voorkomt dat STARTTLS niet gebruikt wordt en zorgt dus dat e-mail altijd over een beveiligde verbinding verstuurd wordt. Met DANE kan ook het gebruikte servercertificaat gepubliceerd worden, met een zogeheten TLSA-record. Hiermee kan de cliënt het aangeboden certificaat verifiëren en vaststellen of dit certificaat te vertrouwen is.

"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." De toepassing van DANE biedt hier bescherming voor.

De implementatie is afhankelijk van de mogelijkheden in de enerzijds de mailprovider[8] en anderzijds de mogelijkheid van DNSSEC (van het domein van de e-mailprovider). DANE is een protocol dat alleen effectief is als DNSSEC actief is. Indien configuratie niet mogelijk is of (nog) onvoldoende effectief kan zijn, kunnen er ook andere maatregelen genomen worden. Zoals het beveiligen van het e-mailbericht zelf of andere kanalen te gebruiken om informatie waarvan de integriteit en vertrouwelijkheid noodzakelijk is.

Een alternatief op DANE is MTA-STS, echter is deze standaard alsnog kwetsbaar voor een man-in-the-middle-aanval (MITM-aanval). Het is immers niet gebaseerd op DNSSEC, waardoor DNS informatie gemanipuleerd kan worden. Daarnaast is DANE opgenomen in de pas-toe-leg-uit-lijst van Forum Standaardisatie. Vanuit het oogpunt van interoperabiliteit en efficiëntie, wordt daarom de voorkeur gegeven aan DANE. Daarmee mag MTA-STS wel als alternatief - of wanneer DANE wel beschikbaar is, aanvullend - toegepast worden. Daarnaast kunnen partijen onderling afspraken maken en configureren voor een - vaste - veilige verbinding.

Voorschrift: MAIL-BEVEILIG-002
Configureer DANE als dit mogelijk is, voor zowel uitgaand verkeer als inkomend verkeer

Implementatie: indien benodigde DNSSEC standaard ondersteund wordt, is deze standaard meestal eenvoudig te implementeren. Het betreft een optie die ingeschakeld kan worden. Dat geldt ook voor DANE bij een mailprovider, zoals met Office 365 of (soortgelijke functie) binnen Google G-suite. Daarvan kan het ingeschakeld worden of is dit automatisch van toepassing. In geval van een on-premise omgeving, waarbij het beheer zelf wordt uitgevoerd, is de nodige expertise en deskundigheid benodigd. Hierbij is het belangrijk met name aandacht te besteden aan de key rollover wanneer het certificaat op de mailserver zal worden vervangen. Voordat het certificaat verloopt dient het TLSA record van het nieuwe certificaat te worden gepubliceerd. Als er voldoende tijd is verstreken i.v.m. DNS propagaties, kan het nieuwe certificaat worden geconfigureerd, en het oude TLSA record worden verwijderd.

Let op! STARTTLS i.c.m. DANE is geen oplossing voor de bescherming van vertrouwelijkheid en integriteit van het e-mailbericht zelf. Daarvoor dient het e-mailbericht versleuteld en ondertekend te worden. Een alternatief hiervoor is het delen van informatie via een link specifiek geadresseerd op e-mailadres. Dat is een standaard optie in de meest gebruikte platformen, zoals Office 365 en Google G-suite.

[8] Office 365 gaat DANE ondersteunen:
https://techcommunity.microsoft.com/t5/exchange-team-blog/support-of-dane-and-dnssec-in-office-365-exchange-online/ba-p/1275494
G-Suite zou dit al ondersteunen, echter spreekt men niet sec over DANE
https://support.google.com/a/answer/2520500?hl=nl&ref_topic=2683828

5. Aanpak voor implementatie

Geadviseerd wordt om de voorschriften uit hoofdstuk 3 gefaseerd toe te passen. Met name om verstoringen te voorkomen. Suggesties voor verbetering kunnen gemaild worden naar info@edustandaard.nl onder het onderwerp UBV - Veilig en Betrouwbaar e-mailverkeer.

Fase 1. Inzicht creëren

a. Maak een overzicht van domeinnamen en welke daarvan wel of niet gebruikt worden voor e-mail. De aanwezige domeinnamen kunnen meestal opgehaald worden uit het portaal waar de domeinnamen worden geregistreerd en aangekocht.
b. Domeinnamen die niet gebruikt worden kunnen geblokkeerd worden (zie §3.0). Is er onduidelijkheid of een domeinnaam wel of niet wordt gebruikt. Zorg dan eerst voor bevestiging; controleer of er geen e-mail op verstuurd wordt (zie volgende punt).
c. Maak emailstromen inzichtelijk door de toepassing van DMARC-rapportage (zie §3.2.4) op alle domeinnamen. Hierbij kan het DMARC-beleid op ‘p=none’ staan. Op dat moment is alleen de rapportagefunctie actief, zonder dat dit effect heeft op het e-mailverkeer. Met de rapportage wordt per domeinnaam inzichtelijk welke ip-adressen (en dus welke systemen) e-mail versturen. Indien SPF en of DKIM reeds geactiveerd is, wordt tevens inzichtelijk of deze reeds correct zijn ingesteld: status is dan ‘pass’; anders ‘fail’.
d. Overweeg om onderscheid te maken in e-mailstromen (zie §3.1). Doe dit voorafgaand aan de implementatie, om extra werkzaamheden in de toekomst te voorkomen.

Fase 2. Implementatie SPF en DKIM per domeinnaam

a. Configureer DMARC-beleid (zie §3.2.3) tijdelijk op ‘p=none’ om verstoringen tijdens configuratie te voorkomen.
b. Configureer SPF door middel van een SPF-record op het domeinnaam die verwijzingen bevat naar mailservers die mail mogen verzenden (zie §3.2.1)
c. Configureer DKIM zodat alle uitgaande mail ondertekend wordt met een sleutel. Pas hiervoor een sleutelbeleid toe (zie §3.2.2)

Fase 3. Pas op het juiste moment het DMARC-beleid toe (per domeinnaam)

a. Controleer de DMARC-rapportage en voer op basis daarvan verbeteringen door.
b. Wanneer het gewenste slagingspercentage is behaald, dan kan het DMARC-beleid toegepast worden (van ‘None’ naar ‘Quarantine’ of ‘Reject’ (zie §3.2.3). Het gewenste slagingspercentage is afhankelijke van de situatie en wens; het balans tussen het actief hebben van het beleid waarbij de kans bestaat op onbezorgde e-mail versus niet actief hebben van het beleid en kans op misbruik.

Fase 4. Borging van de monitoring

a. Zorg ervoor dat de DMARC-rapportages periodiek gecontroleerd worden en of automatisch wordt gemonitord (§3.2.4). Door wijzigingen in de infrastructuur (van leveranciers), kunnen e-mailstromen veranderen en leiden tot verstoring.

Overige voorschriften zijn niet afhankelijk van bovengenoemde aanpak en kunnen afzonderlijk geïmplementeerd worden, zoals controle op inkomend verkeer (paragraaf 3.3) en beveiliging verbinding van mailservers (hoofdstuk 4)