Best Practice voor E-mail verificatie - Optimal Maniers om SPF, DKIM en DMARC te implementeren

Inhoud

Inleiding

In deze handleiding worden drie meest gebruikte e-mailverificatietechnieken beschreven - SPF, DKIM en DMARC - en worden verschillende aspecten van de implementatie ervan besproken. Verschillende situaties van de e-mailarchitectuur in het echte leven worden besproken, en richtlijnen voor het uitvoeren ervan op de Cisco e-mail security productset. Aangezien dit een handleiding is voor praktijkgerichte optimale werkwijzen, zal een deel van het ingewikkelder materiaal worden weggelaten. Indien nodig kunnen bepaalde concepten worden vereenvoudigd of verkort om het inzicht in de voorgestelde materie te vergemakkelijken.

Productkennisvereisten

Deze handleiding is een document op hoog niveau. Om door te gaan met het gepresenteerde materiaal moet de lezer productkennis van de Cisco e-mail security applicatie hebben op het niveau van Cisco e-mail security Veldengineering. Bovendien moeten de lezers een sterk commando hebben van DNS en MTP en hun werking. Toegankelijkheid aan de basis van SFP, DKIM en DMARC is een pluspunt.

E-mailverificatie - Een kort overzicht

Sender Policy Framework (SFP)

Het Sender Policy Framework werd voor het eerst gepubliceerd in 2006, als RFC4408. De huidige versie wordt gespecificeerd in RFC7208 en bijgewerkt in RFC7372. In wezen biedt het een eenvoudige manier voor een Domeineigenaar om hun legitieme e-mailbronnen aan de Ontvangers te adverteren met DNS. Hoewel SPF hoofdzakelijk het retourpad (MAIL VANAF)-adres authenticeert, wordt in de specificatie aanbevolen (en wordt een mechanisme ter beschikking gesteld) om ook een TCP/EHLO-argument (FQDN van de gateway van de zender, zoals verzonden tijdens een gesprek in MSTP) voor echt te maken.

SPF gebruikt DNS-resourcerecords van het TXT-type van tamelijk eenvoudige syntaxis:

```
spirit.com       tekst = "v=spf1 mx a ip4:38.103.84.0/24 a:mx3.spira.com
a:mx4.spiri.com omvatten:spf.protection.outlook.com ~all"
```

Het verslag-Spirit Airlines maakt het mogelijk dat e-mail van de adressen van @spirity.com afkomstig is van een bepaalde/24-subunit, twee machines geïdentificeerd door een FQDN en de omgeving van Microsoft Office365. De "~all"-versterker aan het einde geeft ontvangers de opdracht om alle andere bronnen als zachte fouten te beschouwen - één van de twee soorten SFP's. Let erop dat de zenders niet specificeren wat de ontvangers moeten doen met falende berichten, in welke mate ze falen.

Delta daarentegen maakt gebruik van een ander SFP-schema:

```
delta.com tekst = "v=spf1 a:smtp.hosts.delta.com
omvatten:_spf.seller.delta.com -all"
```

Om het aantal vereiste DNS vragen te minimaliseren, creëerde Delta één "A" record met al zijn TCP-gateways. Ze leveren ook een afzonderlijk SPF-record voor hun verkopers in "_spf.seller.delta.com". Ze bevatten ook instructies voor **harde** fout berichten die niet voor echt zijn bevonden door SPF ("-all"-kwalificatieprocedure). We kunnen het verslag van de verkopers verder opzoeken:

```
Sommige zijn:_spf-delta.vrli.com om het volgende te omvatten:_spf-
delta.ncr.delta.com a:delta-spf.niceondemand.com om te
lezen:_spf.airfrance.fr bevat:_spf.qemailserver.com ook:skytel.com
omvat:l1.com ""
```

E-mails van zenders @delta.com kunnen dus terecht afkomstig zijn van bijvoorbeeld de e-mailgateways van Air France.

Verenigde Staten daarentegen maken gebruik van een veel eenvoudiger SFP-systeem:

```
united.com text = "v=spf1 including:spf.enviaremails.com.br
including:spf.usa.net.com including:coair.com ip4:161.215.0.0/16
ip4:209.87.112.0/20 ip4:74.112.71.93 ip4:74.209.251.0/24 mx ~all"
```

Behalve hun eigen bedrijfspostgateways omvatten zij hun e-mailmarketingaanbieders ("usa.net" en "enviaremails.com.br"), bestaande Continental Air Lines gateways, evenals alle in hun MX records ("MX") opgesomde gegevens. Houd er rekening mee dat MX (een **inkomende** e-mailgateway voor een domein) mogelijk niet hetzelfde is als **uitgaande**. Hoewel zij voor kleinere bedrijven gewoonlijk hetzelfde zullen zijn, zullen grotere organisaties afzonderlijke infrastructuur hebben voor het verwerken van binnenkomende post en afzonderlijke verwerking van uitgaande levering.

Opgemerkt zij ook dat alle bovenstaande voorbeelden uitgebreid gebruik maken van extra DNS-verwijzingsmechanismen (ook-mechanismen). Vanwege prestatieredenen beperkt de SPF-specificatie echter het totale aantal DNS-raadpleging dat nodig is om een definitief record op te halen tot **tien**. Elke SPF-raadpleging met meer dan 10 niveaus van DNS-recursie zal mislukken.

Domain Keys Identified Mail (DKIM)

DKIM, gespecificeerd in RFC's 5585, 6376 en 5863, is een fusie van twee historische voorstellen: DomainKeys van Yahoo en Cisco's Identified Internet Mail. Het biedt een eenvoudige manier voor zenders om cryptografisch uitgaande berichten te ondertekenen en de handtekeningen (samen met andere verificatiemedia) op te nemen in een e-mailheader ("DKIM-Signature"). Senders publiceren hun openbare sleutel in het DNS, en maken het voor elke ontvanger gemakkelijker om de sleutel terug te halen en handtekeningen te controleren. DKIM stelt de bron van de fysieke berichten niet echt vast, maar is afhankelijk van het feit dat als de bron in het bezit is van de privé-sleutel van de afzender, zij impliciet gemachtigd is om een e-mail in hun naam te versturen.

Om DKIM uit te voeren, zou de verzendende organisatie één of meer openbare sleutelparen genereren en de openbare toetsen in de DNS als TXT-records publiceren. Elk belangrijk paar wordt voorzien door een 'selector' zodat de DKIM-verificateurs kunnen differentiëren tussen de toetsen. Uitgaande berichten worden getekend en er wordt een DKIM-Signature-header ingevoegd:

```
DKIM-Handtekening: v=1; a=rsa-sha1; c=ontspannen/ontspannen; s=verenigd;
d=news.united.com;h=MIME-versie:Content-type:Content-Transfer-
Encoding:Datum:To:Reantwoordt-To:Betreft:List-Unsubscribe:Bericht-ID;
i=MileagePlus@news.united.com; bh=IBSWR4yzI1PSRYtWLx4SRDSWII4=;

b=HrN5QINgnXwqkx+Zc/9VZys+yhikrP6wSZVu35KA0jfgYzhzSdfA2nA8D2JYIFTNLO8j4D
GmKH1MMTyYGWYQ
T01rEwL0V8MEY1MzxTrzijkLPGqt/sK1WZt9pBacEw1fMWRQLf3BXZ3jaYtLoJMRwxtgoWdf
HU35CsFG2CNYL O=
```

Het formaat van de handtekening is vrij eenvoudig. "a" tag geeft aan welke algoritmen worden gebruikt voor het tekenen, "c" geeft het/de gebruikte kanonicalisatieschema(s) aan [1], "s" is de selector of de referentie, "d" is het ondertekenende domein. De rest van deze DKIM-Signature header is berichtspecifiek: "h" lijsten van ondertekende kopregels, "i" maakt een lijst van de identiteit van de gebruiker en tenslotte eindigt de header met twee aparte streepjes: "bh" is een hash van ondertekende kopregels, terwijl "b" de hashwaarde is voor de inhoud van het bericht.

Wanneer de ontvanger een door DKIM ondertekend bericht ontvangt, zal de ontvanger de openbare sleutel bekijken door de volgende DNS-query te construeren:

```
<selector>._domainkey.<ondertekenen domein>
```

zoals gespecificeerd in de DKIM-Signature header. Voor het bovenstaande voorbeeld zou onze query "united._domainkey.news.united.com" zijn:

```
verenigd._domainkey.news.united.com tekst = "g=*\; k=rsa\; n=" "Contact"
"postmaster@responsys.com"" met" "enige" "vragen" "betreffende" "deze"
"ondertekening" "\";
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/Vh/xq+sSRLhL5CRU1drFTGX/Q2KkWG
L35hO v6dTy5Qmxcuv5Awx
Liz9d0jBaxtuvYALjlGxmk5MemgAOcCr97GlW7Cr11eLn87qdTmyE5LevnTXVDMjQJt6OFZm
w6Tp1t00 NPWh0PbyOohZYt4qpcbiz9Kc3UB2IBwIDAQAB\";
```

Teruggegeven DNS record bevat de toets, evenals andere optionele parameters. [2]

Het belangrijkste probleem met DKIM is dat de oorspronkelijke specificatie geen reclame mogelijk maakte die door een afzender wordt gebruikt. Indien een bericht dus niet ondertekend is, is het voor een ontvanger niet gemakkelijk te weten dat het ondertekend had moeten worden en in dat geval waarschijnlijk niet authentiek is. Aangezien één enkele organisatie meerdere selectors kan (en meestal zal) gebruiken, is het niet triviaal om te "raden" of een domein is ingeschakeld met DKIM. Om dit te kunnen bestrijken is een aparte norm ontwikkeld, Auteur Domain Signing Practices, maar vanwege het lage gebruik en andere kwesties werd in 2013 zonder opvolger verworpen.

Domain-Based Message Authentication, Reporting and Conforme (DMARC)

DMARC is de jongste van de drie technologieën voor e-mailverificatie die onder de richtlijn vallen en is speciaal ontwikkeld om de tekortkomingen van zowel SPF als DKIM aan te pakken. In tegenstelling tot de andere twee, authenticeert het de Kop van een bericht en koppelt het aan de controles die eerder door de andere twee worden uitgevoerd. DMARC wordt gespecificeerd in RFC7489.

Toegevoegde waarde van DMARC via SPF en DKIM bestaat uit:

- Zorg ervoor dat alle beschikbare identiteiten (HELO, MAIL VAN en/of DKIM signaaldomein) op elkaar zijn afgestemd (precies passend of ondergeschikt) met Van header
- Verstrekken van een middel voor de afzender domeineigenaar om een beleid voor ontvangers te specificeren over hoe zij failliete berichten **moeten** verwerken
- Verstrekken van een terugkoppelingsfaciliteit voor eigenaren van verzendende domeinnamen om op de hoogte te worden gesteld van eventuele falende berichten, zodat het gemakkelijk is om phishing campagnes of fouten in de beleidstaak SPF/DKIM/DMARC te identificeren

DMARC gebruikt ook een eenvoudig DNS-gebaseerd beleidsdistributiesysteem:

```
_dmarc.aa.com tekst = "v=DMARC1\; p=geen\; t = 1\; rr=3600\;
rua=mailto:american@rua.agari.com,mailto:dmarc@aa.com\;
ruf=mailto:american@ruf.agari.com,mailto:dmarc@aa.com"
```

De enige verplichte tag in de DMARC beleidsspecificatie is "p", die het beleid specificeert dat

moet worden gebruikt bij falende berichten. Het kan één van de drie zijn: Geen, quarantaine, nee.

De meeste gebruikte optionele parameters hebben te maken met de rapportage: "rua" specificeert een URL (of een mailto: of een http:// URL met POST-methode) om dagelijkse geaggregeerde rapporten te verzenden over alle falende berichten die afkomstig zijn van een bepaald domein. "ruf" specificeert een URL om onmiddellijke gedetailleerde mislukkingsrapporten over elk falend bericht in te dienen.

Volgens de specificatie **moet** een curator het aangeprezen beleid volgen. Als dat niet het geval is, **moeten** zij de eigenaar van het verzendende domein in het verzamelrapport op de hoogte stellen.

Het centrale concept van DMARC is de zogenaamde identificatieuitlijning. Identifier-uitlijning definieert hoe een bericht DMARC-verificatie kan doorgeven. De SPF- en DKIM-identificatoren worden afzonderlijk aan elkaar gekoppeld en een bericht moet **een** van deze kenmerken doorgeven om DMARC in zijn geheel te kunnen doorgeven. Er is echter een DMARC-beleidsoptie waarbij de verzender kan vragen om een mislukkingsrapport te genereren zelfs als de ene uitlijning passeert, maar de andere faalt. We zien dit in het bovenstaande voorbeeld met de "fo"-tag ingesteld op "1".

Er zijn twee manieren waarop berichten zich kunnen houden aan DKIM of SPF-herkenningsuitlijning, strikt en relaxed. Streng kleven betekent dat FQDN van Kop Van volledig moet overeenkomen met de Signing Domain ID ("d"-tag) van DKIM signatuur of FQDN van MAIL VANUIT MIDDEL-opdracht voor SPF. Relaxed daarentegen maakt het mogelijk dat Kop uit FQDN een subdomein van de twee eerder genoemde fore is. Dit heeft belangrijke gevolgen wanneer het delegeren van uw e-mailverkeer aan derden wordt toegestaan, wat later in het document zal worden besproken.

Aandacht voor SPF-implementatie

SPF voor ontvangers

SF-verificatie is niet eenvoudig te configureren op Cisco e-mail security applicatie of cloude-mail security virtuele apparaten. Voor de rest van dit document zal elke verwijzing naar het Europees Stelsel van Economische Rekeningen ook CES omvatten.

SPF-verificatie is ingesteld in beleid voor Mail Flow - de makkelijkste manier om deze mondiaal te laten lopen is door ze in het vak Default Policy parameters van de juiste luisteraar(s) in te schakelen. Als u dezelfde luisteraar gebruikt voor inkomende en uitgaande e-mailverzameling, zorg er dan voor dat uw "RELAYED" Mail Flow Policy heeft ingesteld op "Off".

Aangezien het SFP geen bepaling van de beleidsactie toelaat, wordt het bericht alleen geverifieerd door de SPF-verificatie (en de DKIM, zoals we later zullen zien) en wordt voor elke uitgevoerde SPF-controle een reeks kopregels ingevoegd:

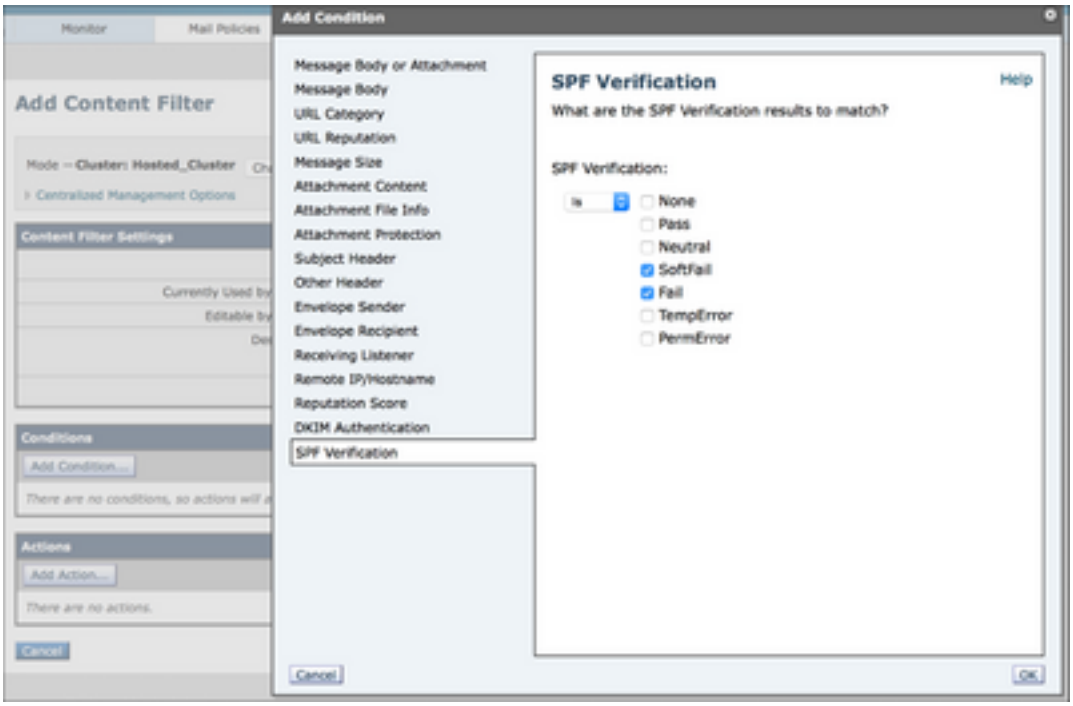
```
Ontvangen-SPF: Pass (mx1.hc4-93.c3s2.smtpi.com: domein van

  united.5765@envfrm.rsys2.com wordt 12.130.136.195 aangewezen als

  geoorloofde afzender) id=mailfrom;

  client-ip=12.130.136.195; ontvanger=mx1.hc4-93.c3s2.smtpi.com;
```

```
  enveloppe-from="united.5765@envfrm.rsys2.com";

  x-sender="united.5765@envfrm.rsys2.com";

  x-conformiteit=sidf_compatibel; x-record-type="v=spf1"

Ontvangen-SPF: Geen (mx1.hc4-93.c3s2.smtpi.com: geen zender

  uit het domein van

  postmaster@omp.news.united.com) identiteit=helo;

  client-ip=12.130.136.195; ontvanger=mx1.hc4-93.c3s2.smtpi.com;

  enveloppe-from="united.5765@envfrm.rsys2.com";

  x-sender="postmaster@omp.news.united.com";

  x-conformiteit=sidf_compatibel
```

Let erop dat voor dit bericht twee "identiteiten" door SPF zijn geverifieerd: "mailfrom" zoals voorgeschreven door de specificatie, en "helo" zoals aanbevolen door dezelfde specificatie. Het bericht zal formeel door het SPF worden doorgegeven, aangezien alleen het eerste relevant is voor de naleving van het SFP, maar sommige ontvangers kunnen ook sancties opleggen aan verzenders die geen SPF-gegevens voor hun HELO-identiteit bevatten. Daarom is het een goede praktijk om de hostname van uw vertrekkende postgateways in uw SPF-gegevens op te nemen.

Zodra het beleid van de Post Flow een bericht verifieert, is het aan de lokale beheerders om een actie te vormen die moet worden ondernomen. Dit gebeurt met behulp van Berichtfilterregel SPF-status() [3], of door een inkomende contentfilter te maken met hetzelfde gebruik en toe te passen op het juiste inkomende postbeleid.

Afbeelding 1: SPF-verificatie contentfilterconditionering



Aanbevolen filteracties zijn om berichten die falen ("-all" in de SPF-opname) en quarantaineberichten die Softphone ("~all" in de SPF-opname) in een Policy Quarantine te laten vallen, hoewel dit afhankelijk van uw beveiligingsvereisten kan verschillen. Sommige ontvangers labelen slechts falende berichten, of nemen geen zichtbare actie, maar rapporteren het aan de beheerders.

De laatste tijd is de populariteit van het SFP aanzienlijk toegenomen, maar veel domeinen publiceren onvolledige of onjuiste gegevens van het SFP. Om veilig te zijn, wil je mogelijk alle SPF-falende berichten in quarantaine houden, en de quarantaine een tijdje bewaken, om er zeker van te zijn dat er geen "valse positieven" zijn.

Als u e-mailservices biedt voor andere domeinen of derden

Als u e-mailbezorging of hostservices voor derden biedt, moeten ze hostnamen en IP-adressen toevoegen die u gebruikt om hun berichten aan hun eigen SPF-records te leveren. De makkelijkste manier om dit te doen is voor de leverancier om een "paraplu" SPF-record te creëren, en klanten toe te voegen "omvat"-mechanisme in hun SPF-records te gebruiken.

```
suncountry.com tekst = "v=spf1 mx ip4:207.238.249.242 ip4:146.88.177.148
ip4:146.88.177.149 ip4:67.109 ip4:107.20.247.57 ip4:207.87.182.66
ip4:199.66.248.0/22 including:cust-spf.exacttarget.com ~all"
```

We kunnen zien dat Sun Country een aantal van zijn e-mails onder zijn eigen controle heeft, maar zijn marketing e-mail is uitbesteed aan een derde. Bij het uitbreiden van de gegevens blijkt dat er een lijst is van de huidige IP-adressen die door hun marketingaanbieder worden gebruikt:

```
cust-spf.exacttarget.com tekst = " v=spf1 ip4:64.132.92.0/24
ip4:64.132.88.0/23 ip4:66.231.80.0/20 ip4:68.232.192.0/20
ip4:199.122.120.0/21 ip4:207.67.38.0/24 ip4:207.67.98.192/27
ip4:207.250.68.0/24 ip4:209 43.22.0/28
ip4:198.245.80.0/204:136.147.128.0/20.ip4:136.min.4.13.00"
```

Met deze flexibiliteit kunnen e-mailserviceproviders schalen zonder dat ze elke klant moeten bereiken om hun DNS-records te wijzigen.

Als u e-mailservices van derden gebruikt

Evenals in de vorige paragraaf, als u e-maildiensten van derden gebruikt en volledige SPF-geverifieerde poststroom wilt invoeren, moet u hun eigen SPF-gegevens in de uwe opnemen.

```
jetblue.com beschrijvende tekst "v=spf1 omvat:_spf.qualtrics.com?all"
```

JetBlue maakt gebruik van de Qualtrics Analytics-service en het enige wat ze hoeven te doen is een correct SPF-record uit Qualtrics. Evenzo verstrekken de meeste andere ESP's in de registratie van hun klanten opgenomen SPF-gegevens.

Als uw ESP of e-mailmarketeer geen SPF-records biedt, zult u hun uitgaande e-mailgateways rechtstreeks in u moeten opgeven. Maar het is dan uw verantwoordelijkheid om deze records nauwkeurig te houden, en als de provider extra gateways toevoegt of IP-adressen of hostnamen wijzigt, kan uw poststroom in gevaar worden gebracht.

Extra gevaar van derden die zich niet bewust zijn van het SFP komt voort uit het delen van

middelen: Als een ESP hetzelfde IP-adres gebruikt om e-mail van meerdere klanten te verzenden, is het technisch mogelijk dat één klant een geldig SPF-bericht oplevert dat doet alsof hij een andere klant is die via dezelfde interface levert. Daarom moet u, voordat u SPF-beperkingen oplegt, het beveiligingsbeleid van uw MSP onderzoeken en e-mailverificatie controleren. Als zij geen antwoorden hebben op uw vragen, rekening houdend met het feit dat SPF een van de basismechanismen van het vertrouwen op het internet is, is het raadzaam uw keuze voor MSP opnieuw te overwegen. Het gaat niet alleen om veiligheid - SPF, DKIM, DMARC en andere door BSP's gebruikte beste praktijken [4] zijn een garantie voor de leverbaarheid. Als uw MSP deze niet correct volgt of niet onjuist volgt zal dit hun betrouwbaarheid met grote ontvangende systemen verminderen en mogelijk uw berichten vertragen of zelfs blokkeren.

(sub)domeinen zonder e-mailverkeer

De meeste organisaties bezitten vandaag verschillende domeinen voor marketingdoeleinden maar gebruiken slechts één actief voor het e-mailverkeer van bedrijven. Zelfs als SPF correct wordt ingezet op het productiedomein, kunnen slechte acteurs nog andere domeinen gebruiken die niet actief worden gebruikt voor een e-mail naar de identiteit van een organisatie. SPF kan voorkomen dat dit zich voordoet via een speciale "ontkennen alle" SPF-record - voor elk van uw domeinen (en subdomeinen!) die geen e-mailverkeer genereren, publiceren "v=spf1-all" in de DNS. Een goed voorbeeld is openspf.org, de website van de SPF Council.

Aangezien de SPF-delegatie alleen geldig is voor één domein, is het van cruciaal belang om ook de SPF-records te weigeren voor alle subdomeinen die u misschien gebruikt en die geen e-mail kunnen genereren. Zelfs als uw productiedomein een "regelmatig" SPF-record heeft, doe dan een extra inspanning om "alle" records aan uw subdomeinen zonder verkeer toe te voegen. En nogmaals - vergeet niet dat ontvangst niet hetzelfde is als verzenden: Een domein kan heel goed e-mail ontvangen, maar zal nooit een bron zijn. Dit geldt zeer voor kortetermijnmarketingdomeinen (bijvoorbeeld evenementen, beperkte tijdbevorderingen, lanceringen van producten...), waar e-mails die binnenkomen in die domeinen aan je productiedomein worden afgeleverd, en alle reacties op die e-mails zullen van het productiedomein komen. Deze kortetermijndomeinen hebben een geldig MX-record maar moeten over een SFP-record beschikken dat ze ook identificeert als geen **bron** van e-mail.

DKIM-implementatieoverwegingen

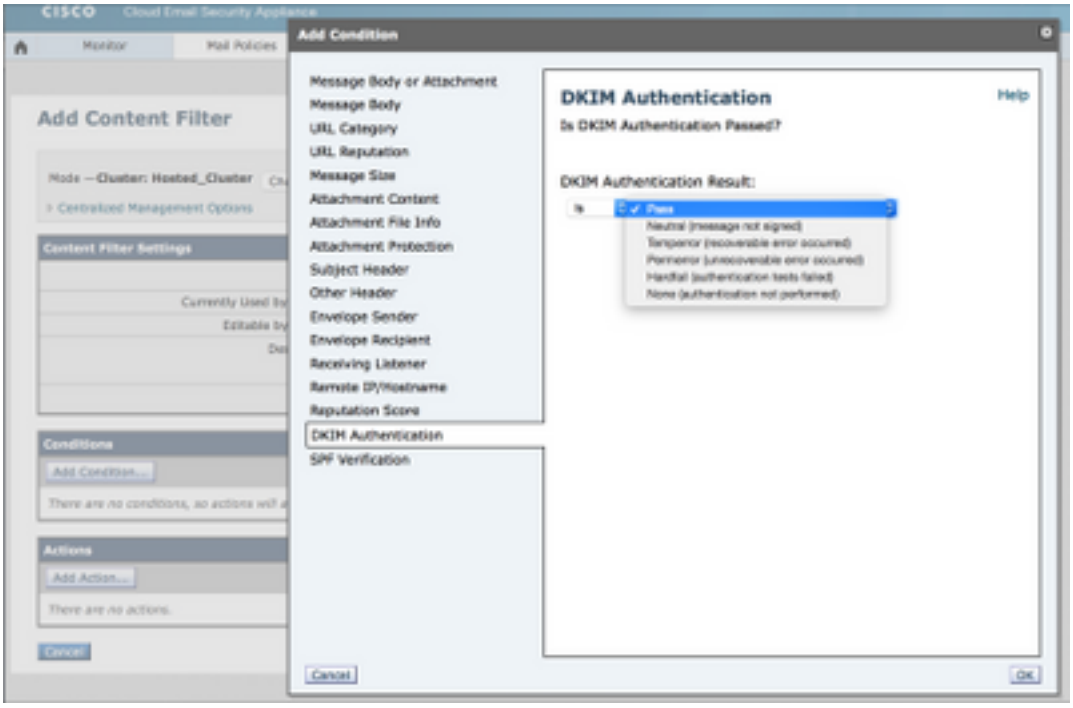
DKIM voor ontvangers

De DKIM-verificatie van de ESA is vergelijkbaar met de SPF-verificatie. In de standaardbeleidsparameters van het beleid van de Mail Flow, schakelt u de DKIM Verificatie eenvoudigweg in "Aan". Opnieuw, omdat DKIM geen beleidsspecificatie toestaat, zal dit eenvoudigweg de handtekening controleren en een header "Verificatie-resultaten" invoegen:

```
Verificatieresultaten: leaving mx1.hc4-93.c3s2.smtpi.com; dkim=pass
(signatuur geverifieerd) header.i=MileagePlus@news.united.com
```

Alle acties op basis van DKIM-verificatieresultaten moeten worden uitgevoerd door contentfilters:

Afbeelding 2: DKIM-verificatie van contentfilter



In tegenstelling tot SPF, wat eenvoudig is, manipuleert DKIM de eigenlijke berichttekst, zodat sommige parameters misschien beperkt zijn. Optioneel kunt u DKIM Verificatieprofielen maken en verschillende verificatieprofielen aan verschillende Mail Flow-beleid toewijzen. Hiermee kunt u de grootte van de handtekeningen beperken die u accepteert, belangrijke mislukkingsacties instellen en de diepte van de DKIM-verificatie configureren.

Als een bericht meerdere poorten passeert, kan het meerdere keren getekend worden en dus meerdere handtekeningen dragen. Om een bericht door te geven dat de DKIM-verificatie moet doorgeven, moeten **alle** handtekeningen worden geverifieerd. ESA zal standaard maximaal vijf handtekeningen verifiëren.

Vanwege de historische openheid van het midden- en kleinbedrijf en de aarzeling van het internet om zich aan te passen aan (positieve) veranderingen, zijn er nog verschillende situaties waarin DKIM-handtekeningen legaal kunnen falen, zoals wanneer lijstmanagers direct berichten doorsturen maar berichten wijzigen, of wanneer berichten direct worden doorgestuurd in plaats van als bijlage aan nieuwe berichten. Dit is de reden dat in het algemeen de beste praktijk voor berichten die niet voldoen aan de DKIM nog steeds in quarantaine of tag zou zitten in plaats van ze te laten vallen.

Voorbereiden op tekenen met DKIM

Voordat u DKIM Signing in uw RELAYED Mail Flow Policy kunt inschakelen, moet u de toetsen genereren/importeren, DKIM Signing Profile(s) maken en de openbare sleutel(s) in de DNS publiceren.

Als u voor één domein tekent, is het proces eenvoudig. Genereert het sleutelpaar, maakt uw enkel Signing Profile in de sectie van de Toetsen van het Domein van het beleid van de Post en klik de "Generate" optie onder "DNS Tekst Record" zodra uw profiel klaar is. Publiceer de toets zoals gegenereerd in uw DNS. Tenslotte schakel DKIM Signing in uw Mail Flow Policy in.

Het wordt gecompliceerder als je voor meerdere aparte domeinen tekent. In dat geval hebt u twee opties:

1. Gebruik één enkel Signing Profile om voor alle domeinen te tekenen. U slaat de (enige) openbare sleutel op in de DNS-zone van het "primaire" domein, en uw DKIM-handtekeningen verwijzen naar die toets. Deze techniek werd in het verleden vaak door ESP's gebruikt - zij konden op grote schaal tekenen zonder met de DNS-ruimte van individuele klanten te hoeven samenwerken [5].
2. Maak een afzonderlijk Signing-profiel voor elk domein waarvoor u tekent. Dit zorgt voor een complexere eerste configuratie, maar biedt veel meer flexibiliteit voor de verdere ontwikkeling. Maak een belangrijk paar voor elk domein, creëer een profiel dat slechts één domein (en zijn subdomeinen) specificeert in de sectie van de "Gebruikers van het profiel" en publicatie de relevante openbare sleutel in de DNS-zone van dat specifieke domein.

Ook al is optie #1 gemakkelijker te starten, vergeet niet dat deze uiteindelijk de DMARC zal breken. Aangezien DMARC vereist dat Signing Domain ID met header From wordt uitgelijnd, zal uw identificator met DKIM falen. U kunt ermee wegkomen als u uw SPF correct configureren en zich op de SPF-herkenningsuitlijning baseren om DMARC-verificatie door te geven.

Maar door optie 2 van het begin toe te passen, hoef je je geen zorgen te maken over DMARC en is het makkelijk om de service voor slechts één domein in te trekken of aan te passen.
Bovendien, als u **wat** e-mailservices aanbiedt voor een derdeursdomein, zal u zeer waarschijnlijk de sleutel moeten krijgen om van hen te gebruiken (en het in uw ESA importeren). Deze toets zal domeinspecifiek zijn, dus moet u een afzonderlijk profiel maken.

Als u e-mailservices van derden gebruikt

Als je DKIM gebruikt om een deel van je e-mailverwerking (bijvoorbeeld marketinge-mails) aan een derde te offload, wil je niet dat die dezelfde sleutels gebruikt als die je bij de productie gebruikt. Dit is een van de belangrijkste redenen voor het bestaan van selectoren in DKIM. In plaats daarvan zou u een nieuw zeer belangrijk paar moeten genereren, het openbare gedeelte in uw DNS zone moeten publiceren en de geheime sleutel aan de andere partij moeten leveren. Dit zal u ook in staat stellen om die bepaalde sleutel in het geval van problemen snel in te trekken terwijl u uw productie DKIM infrastructuur onaangetast houdt.

Hoewel het niet nodig is voor DKIM (berichten voor hetzelfde domein kunnen worden getekend met meerdere sleutels), is het goed gebruik om een apart subdomein te geven voor e-mail die door een derde wordt verwerkt. Het zal het volgen van de berichten gemakkelijker maken en het zal voor een veel schoner implementatie van DMARC in een later stadium mogelijk maken. Neem bijvoorbeeld deze vijf DKIM-Signature headers vanaf meerdere berichten vanuit Lufthansa:

```
DKIM-Handtekening: v=1; a=rsa-sha1; c=ontspannen/ontspannen;
s=lufthansa; d=newsletter.milesandmore.com;

DKIM-Handtekening: v=1; a=rsa-sha1; c=ontspannen/ontspannen;
s=lufthansa2; d=newsletter.lufthansa.com;

DKIM-Handtekening: v=1; a=rsa-sha1; c=ontspannen/ontspannen;
s=lufthansa3; d=lh.lufthansa.com;

DKIM-Handtekening: v=1; a=rsa-sha1; c=ontspannen/ontspannen;
s=lufthansa4; d=e.milesandmore.com

DKIM-Handtekening: v=1; a=rsa-sha1; c=ontspannen/ontspannen;
s=lufthansa5; d=fly-lh.lufthansa.com;
```

We kunnen zien dat Lufthansa vijf verschillende sleutels (selectoren) gebruikt, verdeeld over vijf verschillende subdomeinen van twee primaire productiedomeinen (lufthansa.com en milesandmore.com). Dit betekent dat elk van deze onafhankelijk kan worden gecontroleerd, en elk kan worden uitbesteed aan een andere berichtendienstverlener.

DMARC-implementatieoverwegingen

DMARC voor ontvangers

De DMARC-verificatie op de ESA is op profiel gebaseerd, maar in tegenstelling tot DKIM moet het Default-profiel worden bewerkt om aan de specificatie te voldoen. Het standaardgedrag van de ESA is nooit berichten te laten vallen tenzij de klant expliciet instructies geeft, zodat standaard DMARC verificatieprofiel alle acties heeft ingesteld op "Geen actie". Daarnaast moet u, om de correcte productie van rapporten mogelijk te maken, "Global Settings" van het DMARC-gedeelte van "Mail Policies" bewerken.

Nadat een profiel is ingesteld, wordt de DMARC-verificatie, net zoals de andere twee, ingesteld in het gedeelte Default Policy Settings van Mail Flow Policy. Schakel het vakje in om geaggregeerde feedback-rapporten te verzenden - dit is waarschijnlijk de belangrijkste eigenschap van DMARC voor de afzender. Op het moment van schrijven steunt het ESA het genereren van rapporten over mislukkingen per bericht ('ruf'-tag van het DMARC-beleid) niet.

Aangezien DMARC-beleidsacties door de zender worden geadviseerd, zijn er, in tegenstelling tot SPF of DKIM, geen specifieke acties gepland buiten de profielconfiguratie. Het is niet nodig om inhoudfilters te maken.

DMARC-verificatie voegt extra velden toe aan de kop Verificatie-resultaten:

```
Verificatieresultaten: leaving mx1.hc4-93.c3s2.smtpi.com; dkim=pass
(signatuur geverifieerd) header.i=MileagePlus@news.united.com;
d=news.united.com
```

In het bovenstaande voorbeeld zien we dat DMARC werd geverifieerd op basis van de uitlijning van DKIM-identificatiemiddel, en dat de afzender om een beleid van "geen" verzocht. Dit geeft aan dat ze zich momenteel in de "monitor" fase van DMARC-implementatie bevinden.

Als u e-mailservices biedt voor andere domeinen of derden

De grootste zorg van ESP's voor de naleving van DMARC is het bereiken van een goede herkenningsaanpassing. Wanneer u DMARC plant, zorg er dan voor dat uw SPF correct is ingesteld, dat alle relevante andere domeinen uw vertrekkende gateways in uw SPF records hebben en dat ze geen berichten verzenden die zich niet zullen uitlijnen, vooral door verschillende domeinen te gebruiken voor MAIL VANAF en Kop Van identiteit. Deze fout wordt meestal gemaakt door toepassingen die e-mailmeldingen of waarschuwingen verzenden, omdat toepassingsauteurs zich meestal niet bewust zijn van de gevolgen van de inconsistentie van hun e-mailidentiteit.

Zoals eerder beschreven, zorg er dan voor dat u een afzonderlijk DKIM-signaalprofiel voor elk domein gebruikt en dat uw signaalprofiel naar behoren verwijst naar het domein dat u typt, zoals in Kop Van wordt gebruikt. Als u uw eigen subdomeinen gebruikt, **kunt** u met één enkele sleutel tekenen, maar zorg er dan voor dat u zich aan DKIM houdt om te ontspannen in het DMARC beleid ("adkim="r").

In het algemeen, als je e-maildiensten aanbiedt voor een groter aantal derden waarover je geen directe controle hebt, is het een goede praktijk om een richtsnoer document te schrijven over hoe je een e-mail moet verzenden die waarschijnlijk zal worden afgeleverd. Aangezien e-mail van gebruiker naar gebruiker zich over het algemeen goed gedraagt, zal dit meestal dienen als een beleidsdocument voor toepassingsauteurs in de bovengenoemde voorbeelden.

Als u e-mailservices van derden gebruikt

Als u derden gebruikt om een deel van uw e-mailverkeer af te leveren, is de optimale manier om een afzonderlijk subdomein (of een volledig ander domein) aan de derde provider te delegeren. Op deze manier kunnen zij de SPF records beheren zoals nodig, afzonderlijke DKIM ondertekenen infrastructuur, en kunnen ze niet interfereren met uw productieverkeer. Vervolgens kan het DMARC-beleid voor het uitbesteden van e-mail anders zijn dan voor het binnene. Zoals reeds vermeld, wanneer u overweegt welke derde partij e-mail heeft afgeleverd, zorg er dan altijd voor dat uw identificatoren uitlijnen en dat uw lidmaatschap van DKIM en SPF correct is ingesteld in uw DMARC-beleid.

(sub)domeinen zonder e-mailverkeer

Een andere verbetering van DMARC ten opzichte van eerdere e-mailauthenticatietechnologieën is hoe deze subdomeinen behandelen. Het DMARC-beleid van een bepaald domein is standaard van toepassing op al zijn subdomeinen. Als er bij het ophalen van DMARC-beleidsrecords geen gegevens op Kop Van FQDN-niveau kunnen worden gevonden, zijn ontvangers verplicht om het organisatorische domein [6] van de zender te bepalen en daar een beleidsrecord op te zoeken.

Het DMARC-beleid voor een organisatorisch domein kan echter ook een afzonderlijk Subdomain Policy ("sp" tag van een DMARC-record) specificeren dat van toepassing is op alle subdomeinen waarvoor geen expliciet DMARC-beleid is gepubliceerd.

In het scenario dat eerder in het SPF-hoofdstuk werd besproken, zou u:

1. publiceren van een expliciet DMARC-record voor alle subdomeinen die legitieme e-mailbronnen **zijn**.
2. Publiceer een Subdomein beleid van "verwerpen" in uw organisatorisch domein beleid om e-mails die niet-verzendende domeinen bezitten automatisch te verwerpen

Dit soort structurering van uw e-mailverificatie zorgt voor de best mogelijke bescherming van uw infrastructuur en merk.

Specifieke kwesties in verband met DMARC

Er zijn verschillende mogelijke problemen met DMARC, die allemaal voortkomen uit de aard en tekortkomingen van andere authenticatietechnologieën waarop het zich baseert. Het probleem is dat DMARC deze problemen aan de oppervlakte heeft gebracht door actief aan te dringen op een beleid om de e-mail te verwerpen en door alle verschillende identiteiten in een bericht te correleren.

De meeste problemen doen zich voor met mailing lijsten en mailing list beheersoftware. Wanneer een e-mail naar een mailinglijst wordt verstuurd, wordt deze opnieuw verdeeld onder alle ontvangers. De resulterende e-mail, met een verzender-adres van de oorspronkelijke verzender, zal echter worden afgeleverd door de ontvangende infrastructuur van de adreslijstbeheerder, waardoor de SPF-controles op Kop Van (de meeste directeuren van de mailinglijst gebruiken het

lijstadres als Envelope From (MAIL VANAF) en het adres van de oorspronkelijke afzender als Kop Van).

Aangezien DMARC niet voor SPF zal werken, kunnen we op DKIM vertrouwen. Maar de meeste mailinglist managers voegen ook voetregels toe aan berichten, of tagonderwerpen met de lijstnaam, waardoor de DKIM-handtekening wordt geblokkeerd.

Auteurs van DKIM stellen verschillende oplossingen voor het probleem voor. Deze komen allemaal neer op de mailinglist managers die het adres van de lijst in alle adressen moeten gebruiken en het oorspronkelijke verzendadres op een andere manier moeten aangeven.

Gelijkaardige problemen ontstaan door berichten die door slechts het kopiëren van het originele bericht over MTP aan de nieuwe ontvanger worden doorgestuurd. De meeste e-mailgebruikers die vandaag in gebruik zijn, zullen echter correct een nieuw bericht vormen en het doorgestuurd bericht of inline of als bijlage aan het nieuwe toevoegen. Berichten die op deze manier worden doorgestuurd, zullen DMARC doorgeven als de verzendende gebruiker passeert (de authenticiteit van het oorspronkelijke bericht kan natuurlijk niet worden vastgesteld).

Actieplan ter uitvoering van e-mailverificatie

Hoewel de technologieën zelf eenvoudig zijn, kan de weg om een volledige e-mailauthenticatie-infrastructuur in te voeren lang en gedraaid zijn. Voor kleinere organisaties en bedrijven met gecontroleerde poststromen zal dit vrij eenvoudig zijn, terwijl grotere omgevingen het uitzonderlijk moeilijk kunnen vinden. Het is niet ongewoon voor grote ondernemingen om consulenten in te huren om het uitvoeringsproject te beheren.

Stap 1: DKIM

DKIM is relatief ongehinderd omdat niet-ondertekende berichten geen afkeuring ondergaan. Houd rekening met alle eerder genoemde punten alvorens de richtlijn daadwerkelijk ten uitvoer wordt gelegd. Neem contact op met derden waarmee u ondertekening kunt delegeren, zorg ervoor dat uw derden de DKIM-ondertekening ondersteunen en overweeg uw strategie voor het selectiebeheer. Sommige organisaties zouden afzonderlijke sleutels (selectoren) voor verschillende organisatorische eenheden bewaren. U kunt overwegen de toetsen periodiek te roteren voor extra beveiliging maar zorg ervoor dat u de oude toetsen niet verwijdert totdat al uw berichten tijdens het transport worden afgeleverd.

Bijzondere aandacht dient te worden besteed aan de belangrijkste afmetingen. Hoewel in het algemeen "meer beter is", moet u er rekening mee houden dat het maken van twee digitale handtekeningen per bericht (inclusief kanonicalisatie, etc.) een zeer dure CPU-taak is, en de prestaties van uitgaande mailgateways kan beïnvloeden. Vanwege de berekening overhead is 2048 bits de grootste praktische sleutelgrootte die gebruikt kan worden, maar voor de meeste implementaties maken 1024-bits toetsen een goed compromis tussen prestatie en beveiliging.

Voor een succesvolle daaropvolgende implementatie van DMARC dient u:

1. identificeer alle domeinen die u als subdomeinen stuurt
2. genereren DKIM-toetsen en maken tekenprofielen voor elk domein
3. de betrokken privé-sleutels aan derden te bezorgen
4. alle openbare toetsen in de desbetreffende DNS-zones publiceren
5. nagaan of derden klaar zijn voor ondertekening

6. schakel DKIM-ondertekening in RELAYED Mail Flow Policy in op al uw ESA's
7. derden in kennis stellen van de ondertekening

Stap 2: SFF

Een correcte implementatie van het SFP zal waarschijnlijk het meest tijdrovende en logge deel zijn van de implementatie van een e-mailverificatieinfrastructuur. Omdat de e-mail heel eenvoudig te gebruiken en te beheren was en volledig open was vanuit het oogpunt van veiligheid en toegang, hebben organisaties historisch gezien geen streng beleid afgedwongen rondom wie en hoe het kan gebruiken. Dit resulteerde erin dat de meeste organisaties vandaag de dag geen compleet beeld hadden van alle verschillende bronnen van e-mail, zowel van binnen als van buiten. Het grootste probleem bij de tenuitvoerlegging van het SFP is te ontdekken wie momenteel terecht e-mails naar u stuurt.

Wat u kunt zoeken:

1. voor de hand liggende doelstellingen - Wisselings- of andere servers of uitgaande e-mailgateways
2. alle DLP-oplossingen of andere e-mailverwerkingssystemen die externe meldingen kunnen opleveren
3. CRM-systemen die informatie verzenden die met klanten in interactie is
4. verschillende toepassingen van derden die e-mail kunnen verzenden
5. lab-, test- of andere servers die e-mail kunnen verzenden
6. personal computers en apparaten ingesteld om een externe e-mail rechtstreeks te verzenden

De bovenstaande lijst is niet volledig, aangezien organisaties verschillende omgevingen hebben, maar moet worden beschouwd als een algemene leidraad voor wat er moet worden gezocht. Als (de meeste) uw e-mailbronnen zijn geïdentificeerd, kunt u een stap terug zetten en in plaats van elke bestaande bron te autoriseren, de lijst schoonmaken. Idealiter zouden al uw uitgaande e-mailberichten via uw vertrekkende e-mailgateways moeten worden geleverd met een paar terechte uitzonderingen. Als u uw eigen e-mailoplossing hebt of een oplossing van derden gebruikt voor marketing-mail, zou u afzonderlijke infrastructuur dan e-mailgateways moeten gebruiken. Als uw postnetwerk bijzonder gecompliceerd is, kunt u doorgaan met het documenteren van de huidige staat in uw SFP, maar u hebt wel tijd nodig om de situatie in de toekomst op te ruimen.

Als u meerdere domeinen via dezelfde infrastructuur bedient, kunt u één universeel SFP record creëren en het in individuele domeinen verwijzen met behulp van het "inclusieve" mechanisme. Zorg ervoor dat uw SPF-gegevens niet te breed zijn; Bijvoorbeeld als slechts vijf machines in een /24 netwerk mp verzenden, voeg die vijf individuele IP adressen aan uw SPF toe, in plaats van het volledige netwerk. Bedoel dat uw gegevens zo specifiek mogelijk zijn om de kans op een kwaadaardige e-mail waardoor uw identiteit wordt bedreigd, te minimaliseren.

Begin uit met een optie voor een softphone voor niet-conforme zenders ("~all"). Verander deze optie alleen maar om het bestand hard te maken (-all) als u 100% zeker bent dat u **alle** bronnen van uw e-mail hebt geïdentificeerd, anders loopt u het risico dat u mail over de productie verliest. Later, na het uitvoeren van DMARC en het een tijdje in de monitor modus uitvoeren, kunt u alle systemen die u hebt gemist identificeren en uw SPF records bijwerken om volledig te zijn. Alleen dan is het veilig om uw SFP in te stellen op een harde ondergang.

Stap 3: DMARC

Zodra uw DKIM en SPF zo volledig als u kunt zijn ingesteld, is het tijd om uw DMARC-beleid te maken. Neem alle verschillende situaties in overweging die in vorige hoofdstukken zijn vermeld en bereid zich voor om meer dan één DMARC record in te zetten als u een complexe e-mailinfrastructuur hebt.

Maken e-mailaliases die rapporten zullen ontvangen, of creëren een toepassing van het Web die hen kan opnemen. Er zijn geen strikt gedefinieerde e-mailadressen die hiervoor gebruikt moeten worden, maar het helpt als ze beschrijvend zijn, bijvoorbeeld rua@domain.com, dmarc.rua@domain.com, mailauth-rua@domain.com, etc. Zorg ervoor dat u een proces hebt waarin een operator deze adressen kan bewaken en de configuratie van SPF, DKIM en DMARC correct kan wijzigen, of waarschuwt het beveiligingsteam in het geval van een tapecampagne. Aanvankelijk is de werklast substantieel naarmate u de records scherpt om alles te bedekken wat u tijdens de SPF- en DKIM-configuratie hebt gemist. Na een tijdje duiden de rapporten waarschijnlijk alleen op spoofing pogingen.

Stel uw DMARC-beleid aanvankelijk in op "niets" en uw forensische optie om rapporten te verzenden voor eventuele foutieve controles ("fo=1"). Dit zal snel alle fouten in uw SPF en DKIM ontdekken zonder het verkeer te beïnvloeden. Als u tevreden bent met de inhoud van de ingediende rapporten, verander dan het beleid in "quarantaine" of "verwerpen", afhankelijk van uw veiligheidsbeleid en uw voorkeur. Controleer opnieuw of de operatoren uw ontvangen DMARC-rapporten voortdurend analyseren op valse positieven.

Het volledig en correct implementeren van DMARC is geen kleine of korte taak. Hoewel sommige resultaten (en formele ‘implementatie' van DMARC) verkregen kunnen worden door het publiceren van een onvolledige reeks records en een beleid van ‘geen', is het in het belang van zowel de verzender-organisatie als het internet in zijn geheel dat iedereen dit ten volle uitvoert.

Wat betreft tijdlijnen, hier is een zeer grove schets van individuele stappen voor een typisch project. En weer, omdat elke organisatie anders is, zijn deze verre van accuraat:

1. DKIM-planning en -voorbereiding	2-4 weken
2. DKIM-tests	2 weken
3. SPF - rechtmatige identificatie van de afzender	2-4 weken
4. Voorbereiding van het beleid	2 weken
5. Testrun op SFP- en DMARC-bestanden	4-8 weken
6. Testrun op SFP met harde onderbreking	2 weken
7. DMARC-test met quarantaine/weigering	4 weken
8. Monitoring of DMARC meldt en past SPF/DKIM dienovereenkomstig aan	continu

Kleine organisaties zullen waarschijnlijk een kortere duur van de meeste stappen ervaren, vooral Stap 3 en 4. Hoe eenvoudig je e-mailinfrastructuur ook is, toewijzen altijd de ruim beschikbare tijd tijdens de test, en controleren feedback rapporten nauwkeurig op alles dat je hebt gemist.

Grotere organisaties zouden een nog langere duur van dezelfde stappen kunnen ervaren, met striktere testvereisten. Het is niet ongewoon voor bedrijven met een complexe e-mailinfrastructuur om externe hulp in te huren, niet alleen voor het technische aspect van de implementatie van e-mailverificatie, maar ook om het hele project te beheren en te coördineren tussen teams en afdelingen.

Aanvullende referenties

- Referentielocatie voor SPF: http://www.openspf.org
- De DKIM-Raad: http://www.dkim.org
- Hoofdwebsite DMARC, gerund door The Trusted Domain Project: http://www.dmarc.org
- dmarcus - een help- en resources-site die wordt gerund door Tim Draegen, een van de auteurs van DMARC. Kijk in het gedeelte "Gereedschappen": http://www.dmarcian.com
- Online Trust Alliance's Record Validator-instrument: https://otalliance.org/resources/spf-dmarc-record-validator
- DMARC Record Assistant - een ander handig gereedschap om u te helpen uw DMARC-records te creëren: http://www.kitterman.com/dmarc/assistant.html
- PPF-testtools: http://www.kitterman.com/spf/validate.html
- "Wees geen Phish: Deep Dive In Email Verifier-technieken", een Cisco Live 2014-presentatie BRKSEC-3770: https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=76627

[1] Kanonicalisatie valt buiten het toepassingsgebied van dit document. Raadpleeg het gedeelte "Aanvullende referenties" voor meer informatie over DKIM-kanonicalisatie.

[2] DKIM DNS-recordparameters vallen ook buiten het toepassingsgebied van dit document.

[3] Het maken van berichtfilters valt buiten het toepassingsgebied van dit document. Raadpleeg AsyncOS voor e-mailgebruikershandleidingen voor ondersteuning.

[4] M3AAWG heeft een uitstekende reeks beste praktijken gedefinieerd die door de meeste bedrijfstakken worden toegepast en nageleefd. Hun document met beste praktijken is beschikbaar op https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Senders_BCP_Ver3-2015-02.pdf

[5] Dit gedrag maakt misbruik van het feit dat DKIM oorspronkelijk de bron van het bericht niet verifieert zoals in MAIL VANAF of Kop Van in het geheel. Er wordt alleen geverifieerd dat de Signing Domain ID ("d"-parameter van DKIM Signature en de "Domain Name"-parameter in uw Signing Profile) inderdaad de openbare sleutel van het paar ontvangt dat wordt gebruikt om het bericht te tekenen. Zender authenticiteit wordt impliciet door de "Van" header te laten ondertekenen. Zorg ervoor dat u een lijst maakt van alle domeinen (en subdomeinen) waarvoor u inlogt in de sectie "Gebruikers van het profiel".

[6] Gewoonlijk is er een niveau van domein één onder TLD of relevante CcTLD-prefix (.ac.uk,.com.sg enz.).