DMARC INSTELLEN VOOR UW ORGANISATIE

Voordat er een Verified Mark Certificate (VMC) kan worden uitgegeven aan een organisatie, moet de betreffende organisatie eerst voldoen aan het DMARC-protocol, wat staat voor Domain-based Message Authentication, Reporting & Conformance. In deze gids bespreken we de stappen die u moet nemen om ervoor te zorgen dat DMARC op de juiste manier is geïmplementeerd in uw organisatie.

digicert®

digicert®

WAT IS DMARC?

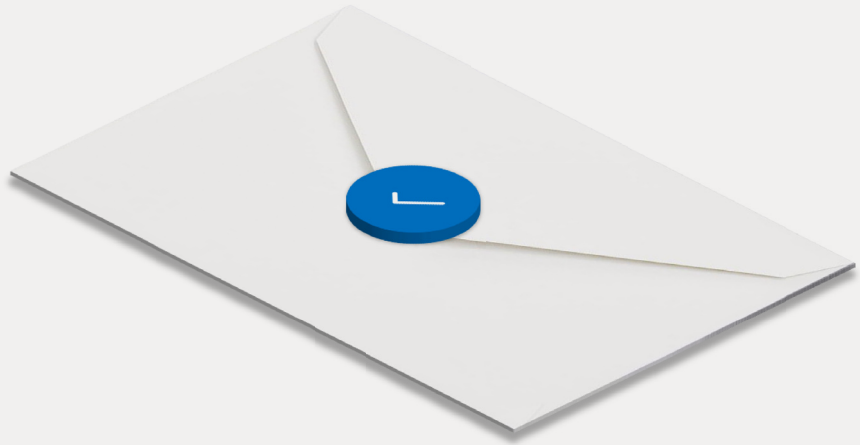
DMARC is een protocol voor het verifiëren van, instellen van beleid voor en rapporteren over e-mail, waarmee organisaties hun domein kunnen beschermen tegen ongeoorloofd gebruik, zoals afzendervervalsing en phishing.

De korte uitleg:

- DMARC is een TXT-record dat in het DNS is opgeslagen en waarmee ontvangers van e-mail de echtheid van een ontvangen bericht kunnen verifiëren.
- Het is bedoeld om te functioneren binnen de bestaande verificatieprocessen voor inkomende mail, en helpt ontvangers te bepalen of een bericht 'overeenkomt' met wat de ontvanger weet over de afzender.
- Een organisatie heeft drie beleidsopties voor het afhandelen van berichten die niet overeen komen:

- “p = none” (geen handhaving)
- “p = quarantine” (quarantaine)
- “p = reject” (weigeren)

- Voor de correcte werking van DMARC moeten de protocollen Sender Policy Framework (SPF) en DomainKeysIdentified Mail (DKIM) van tevoren zijn ingesteld.
- De controle van het DMARC-record van een organisatie kan worden gedaan met bestaande hulpmiddelen op internet, zoals deze van valimail.com.



BETERE E-MAILVERIFICATIE BEGINT BIJ DMARC

Het doel van DMARC is het opzetten van een systeem waarin afzenders en ontvangers samenwerken aan betere e-mailverificatiemethoden door afzenders, zodat ontvangers niet-geverifieerde berichten kunnen weigeren.

digicert®

WAAROM DMARC?

Het implementeren van DMARC biedt vier belangrijke voordelen:

1. **Beveiliging**

   Bescherm mensen tegen spam, fraude en phishing door ongeoorloofd gebruik van uw e-maildomein te voorkomen.

2. **Zichtbaarheid**

   Ontvang gedetailleerde overzichten wie (en/of wat) over internet e-mails verstuurt met uw domainnaam.

3. **Bezorging**

   Verhoog het bezorgen van uw e-mails met 5-10% en voorkom dat ze worden gemarkeerd als spam.

4. **Merkbescherming**

   Bescherm uw merk tegen identiteitsgerichte aanvallen.

van de klanten is minder geneigd in zee te gaan met een merk als ze slachtoffer zijn geworden van phishing waarbij de naam van die organisatie is gebruikt.

digicert®

SPF INSTELLEN:

1. Verzamel de IP-adressen die worden gebruikt voor het verzenden van e-mail vanuit uw domain, zoals de adressen van:
    - de webserver;
    - de interne mailserver;
    - de mailserver van de provider;
    - eventuele mailservers van derden.
2. Stel een lijst op van uw verzendende en niet-verzendende domeinen.
3. Maak een SPF-record in tekstindeling met een geschikt programma (Notepad++, Vim, Nano enzovoort).

    Voorbeeld 1: v=spf1 ip4:1.2.3.4 ip4:2.3.4.5 ip4:x.x.x.x -all
    Voorbeeld 2: v=spf1 ip4:1.2.3.4 ip4:2.3.4.5 include:derdepartij.com -all

4. Publiceer uw SPF naar het DNS.

    Als u zelf uw DNS beheert, voegt u gewoon een TXT-record toe met daarin de tekst van de SPF. Als u niet zelf uw DNS beheert, moet u de serverbeheerder vragen om het record toe te voegen.

5. Wanneer het record is toegevoegd aan het DNS, kunt u het raadplegen met een SPF-controletool.

WAT IS SPF?

Loop geen risico met ongeautoriseerde afzenders.

SPF is de norm voor het verifiëren van e-mail op basis van het domein. Het verhindert spoofing omdat domeineigenaren de IP-adressen van servers die bevoegd zijn voor het verzenden van e-mail namens het bedrijf automatisch kunnen goedkeuren. Als een mailserver probeert e-mail te verzenden namens dat domein terwijl het IP-adres van die server niet op de lijst staat, mislukt de SPF-verificatie.

digicert®

DKIM INSTELLEN:

1. Kies een DKIM-selector.

Dit moet een eenvoudige, door u zelf samengestelde tekenreeks zijn (bijv. 'standaard') die wordt toegevoegd aan de domeinnaam voor het herkennen van de openbare DKIM-sleutel.

Voorbeeld: “standaard._domein.voorbeeld.com” = hostnaam

2. Genereer een sleutelpaar met een openbare en persoonlijke sleutel voor uw domein.

- In Windows kunt u PUTTYGen gebruiken
- In Linux en Mac kunt u ssh-keygen gebruiken

3. Maak en publiceer een nieuw TXT-record.

Maak een nieuw record via uw DNS-beheerconsole met de openbare sleutel van het hierboven genoemde sleutelpaar.

Voorbeeld: v=DKIM1; p=UwOpenbareSleutel

WAT IS DKIM?

Voorkom dat er met e-mails wordt geknoeid terwijl ze onderweg zijn

DKIM is een norm voor e-mailverificatie die gebruikmaakt van cryptografie op basis van openbare en persoonlijke sleutels voor het ondertekenen van e-mailberichten.

DKIM wordt gebruikt om te verifiëren dat een email afkomstig is van het domein waaraan de DKIM-sleutel is gekoppeld, en dat de e-mail tijdens de verzending niet is gewijzigd.

digicert®

DMARC-MONITORINGMODUS INSTELLEN

1. Zorg dat u SPF en DKIM goed hebt ingesteld
2. Maak een DNS-record.

   De teksttekenreeks in het DMARC-record moet lijken op het volgende: '_dmarc.uw_domein.com'.

   Voorbeeld: “v=DMARC1;p=none; rua=mailto:dmarcreports@uw_domein.com”.

   Als u het DNS voor uw domein beheert, maakt u een DMARC-record met 'p=none' (monitoringmodus) op dezelfde manier als u dat voor SPF- en DKIM-records doet.

   Als u het DNS niet zelf beheert, vraagt u de DNS-provider om het DMARC-record voor u te maken.

3. Test uw DMARC-record met een DMARC-controle tool

   Opmerking: de replicatie duurt meestal 24 tot 48 uur.

WAT IS DMARC-MONITORINGMODUS?

Een volledig beeld van wat er vanuit uw domein wordt verzonden

In de monitoringmodus kunnen domeineigenaars de DMARC-overzichten met het e-mailverkeer voor het domein controleren.

In de overzichten staan de berichten die mogelijk in quarantaine zouden worden geplaatst of zouden worden geweigerd wanneer DMARC wordt ingesteld op volledige handhaving. Daarnaast bevatten ze informatie over alle systemen en services die e-mails verzenden vanuit het gemonitorde domein.

OPMERKING: de monitoringmodus biedt geen enkele vorm van handhaving. E-mail die de verificatie niet doorstaat, wordt op de gebruikelijke wijze bezorgd. Hiermee voorkomt u mogelijke verstoringen tijdens de implementatie van DMARC.

digicert®

VEELGEBRUIKTE TAGS IN DMARC TXT-RECORDS

TAGNAAM	VEREIST	DOEL
V	VEREIST	PROTOCOLVERSIE
P	VEREIST	BELEIDVERSIE
PCT	OPTIONEEL	% VAN BERICHTEN DAT WORDT GEFILTERD
RUA	OPTIONEEL	UTI VAN SAMENGEVOEGD RAPPORT
SP	OPTIONEEL	BELEID VOOR SUBDOMEINEN VAN HET DOMEIN

digicert®

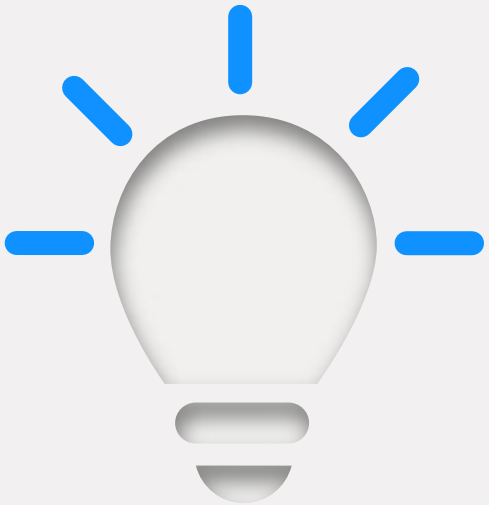
WELKE INFORMATIE BEVAT HET DMARC-OVERZICHT?

In het overzicht kunnen domeineigenaren zien in hoeveel frauduleuze berichten hun domein wordt gebruikt, waar ze vandaan komen en of ze kunnen worden geblokkeerd met het DMARC-beleid 'quarantaine' of 'weigeren'.

Het overzicht van elke ontvanger is een XML-bestand dat de volgende velden bevat:

- Het aantal berichten van elk van de IP-adressen
- Wat er met de berichten is gedaan op basis van het weergegeven DMARC-beleid
- De SPF-resultaten voor deze berichten
- De DKIM-resultaten voor deze berichten

Hoewel het XML-overzicht leesbaar is, is de indeling niet gebruiksvriendelijk. U kunt gebruikmaken van een verwerkingsservice voor DMARC-overzichten, zoals Valimail of een andere DMARC-serviceprovider.



VIER MANIEREN OM HET DMARC-OVERZICHT TE BENUTTEN

Begin met handhaven vanaf een goede baseline

1. Spoor verkeer op dat als niet-legitiem wordt aangemerkt.

2. Identificeer legitieme e-mails die door DMARC als niet-legitiem worden aangemerkt. Afhankelijk van het ingestelde beleid worden die berichten geweigerd of in quarantaine geplaatst wanneer u de handhaving inschakelt.

3. Laat systeem- en applicatie-eigenaars weten waarom hun e-mails als niet-legitiem worden aangemerkt.

4 Update indien nodig uw SPF-record door de legitieme IP-adressen die nog niet op de lijst staan op de whitelist te zetten.

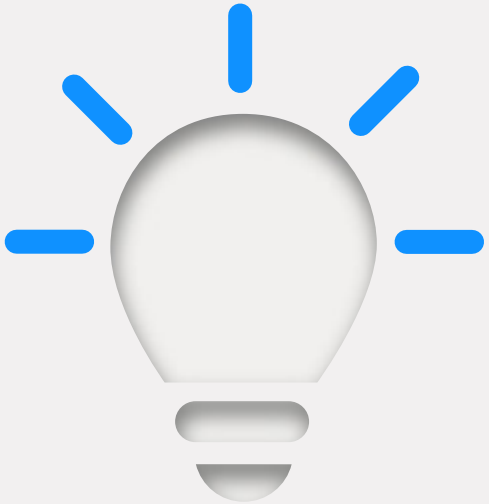
digicert®

GEBRUIK DMARC-OVERZICHTEN OM ORDE OP ZAKEN TE STELLEN VOORDAT U HANDHAVING INSCHAKELT

Het analyseren van DMARC-overzichten kan behoorlijk tijdrovend zijn. Maar de kans bestaat dat als domeineigenaars afzenders over het hoofd zien of verkeerd identificeren, ze 'goede' e-mails blokkeren wanneer het DMARC-beleid wordt ingesteld op handhaven ('quarantaine' of 'weigeren'). En dat kan leiden tot problemen die nog veel meer tijd kosten.

Hier volgen een paar suggesties voor dingen om te doen voordat u DMARC-handhaving inschakelt:

- Stel een lijst op met alle afzenders die staan vermeld in het DMARC-overzicht en alle afzenders die door stakeholders worden opgegeven
- Identificeer de eigenaars van elke service/e-mailafzender
- Categoriseer de verzendende services als geautoriseerd, ongeautoriseerd of kwaadaardig
- Spoor met hulp van de stakeholders eventuele afzenders op die niet in het DMARC-overzicht zijn opgenomen
- Verifieer elke gevonden afzender bij de stakeholders
- Update uw SPF-record met de IP-adressen van de nieuw gevonden legitieme afzenders



AANBEVELINGEN VOOR DE COMMUNICATIE VOORAFGAAND AAN DE HANDHAVING

Vijf tips voor een vlotte acceptatie

- Stel een implementatiebeleid op om te delen met stakeholders.
- Vraag ondersteuning bij een leverancier zoals Valimail als het werken met DMARC te ingewikkeld is of u hulp nodig hebt.
- Communiceer nieuwe bevindingen in DMARC-overzichten zodra ze beschikbaar zijn.
- Start de implementatie van DMARC als een intern project.
- Laat de directie de belangrijkste projectsponsors zijn.

HOELANG MOET DMARC IN DE MONITORINGMODUS WORDEN GEBRUIKT?

Dit varieert van bedrijf tot bedrijf. Een grote onderneming zal hier meer tijd voor moeten uittrekken dan een kleinere organisatie. Houd rekening met weken en wellicht maanden.

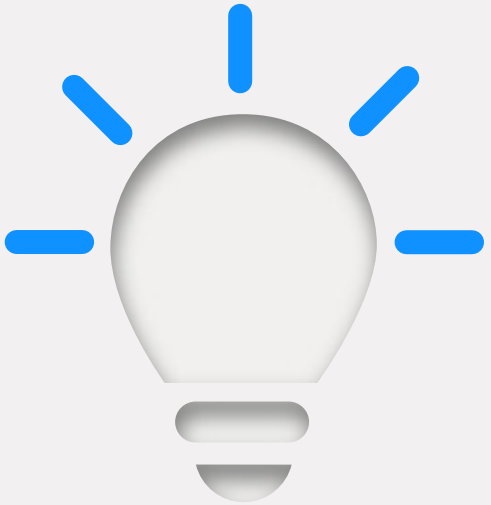
Wanneer u zeker weet dat uw inventarisatie compleet is, alle geautoriseerde afzenders in kaart zijn gebracht en iedereen in de organisatie volledig op de hoogte is, kunt u overgaan naar de quarantainefase.

Wanneer de quarantainemodus is ingeschakeld, worden berichten waarvan de verificatie mislukt in quarantaine geplaatst. Dit betekent meestal dat ze in de spammap van de gebruiker terechtkomen.

DMARC-QUARANTAINEBELEID INSTELLEN VOOR UW ORGANISATIE

1. Meld u aan bij uw DNS-server en zoek het DMARC-record
2. Open het DMARC-record voor het opgegeven domein en verander het beleid van 'p=none' in 'p=quarantine'
   Voorbeeld:
   "v=DMARC;p=quarantine;pct=10;rua=mailto:dmarcreports@uw_domein.com"
3. Voeg de vlag 'pct' toe (het percentage berichten dat wordt gefilterd). We raden aan om te beginnen met 10%.
4. Naarmate u meer vertrouwd raakt met het proces, kunt u het percentage geleidelijk opvoeren naar 100% ('pct=100').

   OPMERKING: Het percentage moet 100% zijn om te voldoen aan de DIMI- en VMC-normen, maar uw beleid mag zowel 'quarantaine' als 'weigeren' zijn.



HOE MARKEREN WERKT

- Als u een beleid anders dan 'p=none' opgeeft, wordt dat beleid toegepast op het percentage aangegeven met de vlag 'pct'.
- Op de rest van de berichten wordt het volgende minder restrictieve beleidsniveau toegepast. Bijvoorbeeld: met een DMARC-record waarin 'p=quarantine' en 'pct=10', wordt 10% van het e-mailverkeer waarvan de verificatie mislukt in quarantaine geplaatst. De overige 90% wordt gewoon bezorgd.

digicert®

WANNEER U EENMAAL 100% FILTERT, BENT U KLAAR VOOR HET HOOGSTE HANDHAVINGSNIVEAU, 'P=WEIGEREN'.

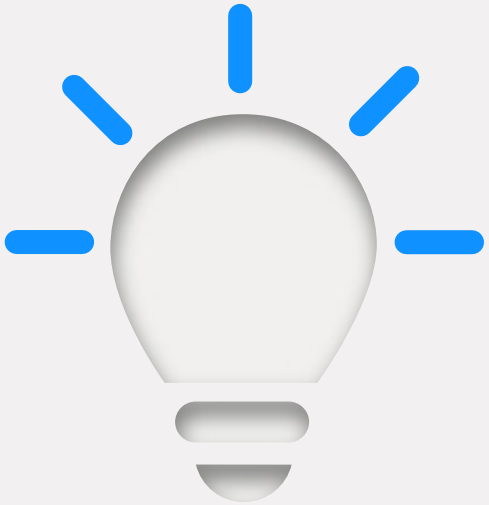
DMARC-WEIGERINGSBELEID INSTELLEN VOOR UW ORGANISATIE

1. Open het DMARC-record in uw DNS-console.
2. Verander 'p=quarantine' in 'p=reject'.
   Voorbeeld: “v=DMARC;p=reject;pct=100;rua=mailto:dmarcreports@uw_domein.com".
3. Sla het record op.

TIP: in deze fase is het met name belangrijk om te blijven monitoren, om zeker te weten dat er geen legitieme e-mails worden geweigerd en verwijderd.

Heeft u meer vragen? E-mail ons vandaag nog op contactus@digicert.com of bezoek ons op https://www.digicert.com/nl/tls-ssl/verified-mark-certificates/?

digicert®



WAT DOET HET WEIGERINGSBELEID MET E-MAILS?

Alle berichten die de DMARC-controle niet doorstaan (ongeautoriseerde e-mails) worden geblokkeerd en verwijderd. De beoogde ontvanger krijgt het bericht nooit te zien en weet niet eens dat het is verwijderd.