DMARC Analyzer

Your data-driven **solution** that helps **to secure** your **e-mail**

Wie verstuurt er namens jouw domein e-mail?

Phishing is een *'hot topic'* en komt de laatste tijd geregeld in het nieuws. *'Gemeente Breda waarschuwt over afvalservice phishing mails'*, *'De Belastingdienst waarschuwt voor een phishingmail in omloop'*, *'Valse e-mails in omloop voor vervanging bankpas'* en zo zijn er nog vele andere voorbeelden op te noemen. De toepassing van DMARC is een eenvoudige oplossing om domeinen te beschermen. Zo wordt niet alleen een domein beschermd, maar wordt ook inzichtelijk welke partijen namens jouw domein e-mails versturen.

Wat is phishing?

Het doen van online aankopen en digitale administratie maken internet inmiddels onmisbaar. Belangrijke, vertrouwelijke informatie zoals bankrekeningnummers en persoonlijke gegevens worden massaal gedeeld en ingevoerd. Dat is logisch omdat veel diensten anders niet gebruikt kunnen worden. Spammers en fraudeurs maken hier misbruik van en versturen massaal phishing e-mails (een vorm van internetfraude).

Een e-mail is eenvoudig te frauderen en gemakkelijk inzetbaar. Met enkele klikken liggen privégegevens zo op straat. Een herkenbaar logo met bijhorende huisstijl wekken de illusie dat een mail valide is. Het is (bijna) niet te zien dat het een phishing e-mail is. De ontvanger vertrouwt de e-mail en stelt gevoelige info beschikbaar. Dit zorgt vaak voor nadelige gevolgen voor zowel de ontvanger als voor de organisatie van het misbruikte domein.

Definitie phishing e-mail

Een e-mail die verstuurd wordt met als doelstelling om informatie te verkrijgen met frauduleuze doeleinde(n), waarbij de daadwerkelijke verzender zich voordoet als een andere afzender.

Wat zou jij doen?

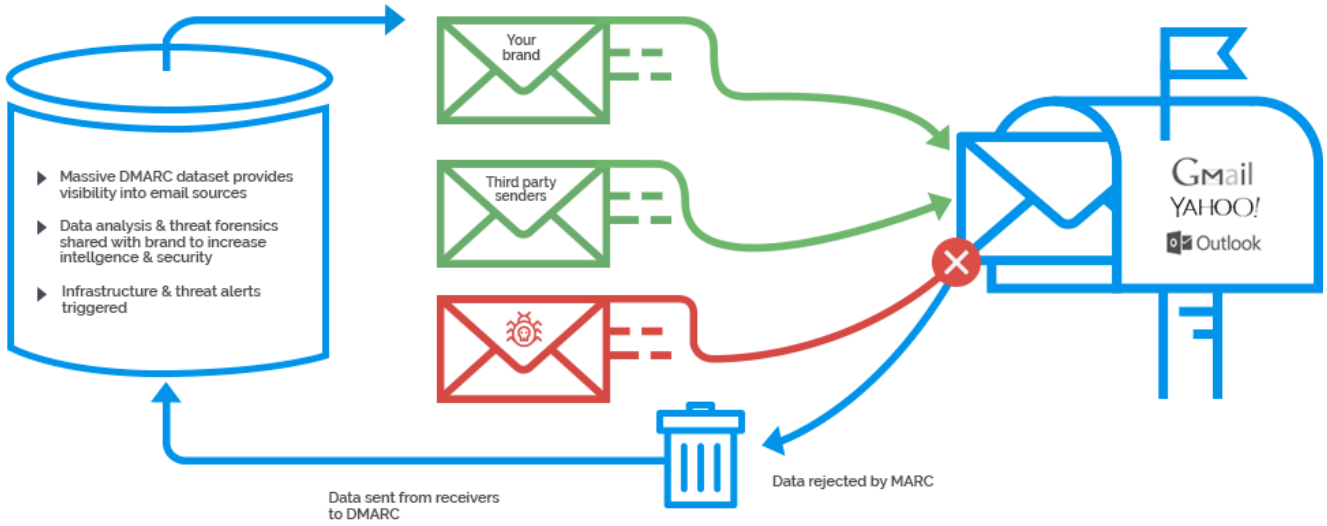
Heb je wel eens een phishing mail ontvangen? De kans hierop is groot. Heb je vóór het vergeven van gevoelige informatie ontdekt dat de e-mail niet afkomstig was van de daadwerkelijke afzender, dan heb je geluk. Maar stel je voor: Wat zou er kunnen gebeuren als iemand zich voordoet als de directeur van jouw bedrijf en je vraagt om iets te doen? Neem je het risico om deze mail te negeren? Of voer je de werkzaamheden plichtsgetrouw uit?

Wie verstuurt er namens jouw e-mail?

Weet je al wie er namens jouw domein e-mails verstuurt? Het antwoord: *'Ja, dat ben ik alleen'* is het meest gegeven antwoord. Helaas, klopt dit in de meeste gevallen niet.

Third party senders en phishers

Wellicht gebruik je tools voor jouw e-mailmarketing (zoals eFuture Engine), heb je een helpdesk ingericht die e-mails kan sturen (Zoals Zendesk/ Freshdesk) of gebruik je een CRM dat e-mails stuurt (Salesforce). Dit zijn enkele voorbeelden van geldige *'third party senders'*, derden die door jou gerechtigd zijn om e-mail te versturen. Echter zijn er mogelijk ook partijen die dit niet zijn zoals phishers, daar ligt het gevaar!



De implementatie van DMARC zorgt per domein voor inzicht in de verzenders van het e-mailverkeer. Maar wat houdt DMARC precies in? En waarom is het belangrijk? Lees hieronder een toelichting over DMARC.

Wat is DMARC?

DMARC is een technische specificatie die erop gericht is om phishing te bestrijden. Het staat voor: **D**omain-based **M**essage **A**uthentication, **R**eporting & **C**onformance. De technische policy vereist dat de afzender van de e-mail (de afzender die in de inbox zichtbaar is) bewijst dat hij ook de daadwerkelijke afzender is. Dit wordt mede gedaan door validatie van de beveiligingstechnieken SPF en DKIM. Deze technieken zijn noodzakelijk om een e-mail correct af te leveren. Er worden dankzij DMARC meerdere belangrijke aspecten toegevoegd, wat de implementatie ervan belangrijk maakt.

Wat biedt DMARC extra?

DMARC heeft enkele interessante eigenschappen die er voor zorgen dat het een erg populaire techniek aan het worden is.

Alignment - Het is mogelijk om een e-mail correct met DKIM en SPF te versturen, maar toch een *'andere'* afzender te gebruiken. Wellicht gebruik je Gmail en is het je wel eens opgevallen dat er bij sommige berichten de tekst *'via eenverzender@domein.nl'* staat. In dit geval is de *'technische afzender'* van de e-mail niet gelijk aan het *'Van'* domein. Dit zorgt ervoor dat het bericht voor DMARC ongeldig wordt. Voor geldige berichten kan dus met zekerheid worden gezegd dat de afzender (het *'Van'* domein) de e-mail heeft verzonden.

Reporting – Alle ISP's die e-mail ontvangen met jouw domein als *'Van'* domein, zullen op dagelijkse basis een rapport sturen naar een door jou op te geven adres. Dit kunnen per dag tientallen rapporten worden. Wil je eenvoudige verwerking van deze rapporten? eFuture Engine biedt de software *'DMARC Analyzer'* aan. Dit pakket helpt je bij het implementeren van DMARC.

Policy – Het is mogelijk om een *'policy'* in te stellen. Door middel van deze policy kan er aangegeven worden wat een ISP dient te doen met ongeldige berichten. Daarnaast is het mogelijk om een gefaseerde overgang van de ene naar de andere policy te doen. De mogelijke waarden zijn:

Policy waarden:

none – Deze policy heeft geen invloed op de verzonden berichten. De rapportages worden wel verzonden.

quarantine – Bij deze policy worden de ongeldige berichten door de ISP in de *'spambox'* van de ontvanger geplaatst.

reject – Bij deze policy worden de ongeldige berichten totaal door de ISP genegeerd en krijgt de ontvanger ze niet te zien.

Gebruik een goede tool

Indien er gestart wordt met de implementatie van DMARC worden er veel rapporten opgesteld. Zonder software om deze rapporten goed en duidelijk te kunnen lezen is het erg lastig om DMARC te implementeren.

DMARC Analyzer

eFuture Engine biedt de software oplossing DMARC Analyzer aan. Met behulp van deze tool kunnen de aangeleverde XML rapporten eenvoudig (en automatisch) verwerkt worden tot leesbare overzichten. Dankzij de tool blijf je dagelijks op de hoogte van de huidige implementatie status van jouw DMARC setup.

Gebruikers van eFuture Engine kunnen de gegevens zelfs inzien vanuit hun bestaande account zonder hiervoor te hoeven inloggen. Uiteraard is het wel noodzakelijk om de aangegeven DNS record te plaatsen.

Gedetailleerd inzicht mogelijk

Naast de rapporten met gegroepeerde data die de ISP's sturen, is het ook mogelijk om detail berichten te ontvangen van specifieke e-mails die niet *'DMARC compliant'* zijn. Deze *'forensische rapporten'* kunnen erg waardevol zijn bij de implementatie van DMARC.

*Aan het gebruik van de forensische rapporten zitten privacy risico's verbonden.
Overleg zodoende met een privacy officer alvorens dit in te schakelen.

Bescherm je domein en verhoog je reputatie

Het implementeren van DMARC zorgt ervoor dat je jouw eigen domein(-en) kunt beschermen tegen phishing. Doordat je bij de ISP's aangeeft actief met e-mailbeveiliging bezig te zijn (door je policy op reject te zetten), zal de betrouwbaarheid van jouw domein verhogen. De betrouwbaarheid van een domein is voor veel ISP's een belangrijke graadmeter in de bepaling van de reputatie van een domein. Is DMARC volledig geïmplementeerd? Dan zorgt dit voor een betere reputatie voor al je e-mails. Dit heeft ook nog eens een positieve invloed op de deliverability.

eFuture Engine helpt je naar p=reject

Ons team van kundig DMARC consultants kan je desgewenst helpen om tot p=reject te komen.
Heb je hiervoor interesse of vragen over DMARC? Neem dan contact met ons op.