Hoe te werken met

Mail Spectator

Whitepaper door SecurityHive

SECURITYHIVE

Inhoudsopgave

Inleiding

Het maakt niet uit bij wat voor bedrijf je werkt. Of dit nu een klein, middelgroot en groot bedrijf is. De e-mail is een onmisbaar hulpmiddel geworden om met je werknemers, partners en klanten te communiceren. Iedere dag worden e-mails in grote aantallen verstuurd en ontvangen door bedrijven uit verschillende bronnen. Daarnaast zijn er ook organisaties die externe leveranciers in dienst hebben die geautoriseerd zijn om namens het bedrijf e-mails te versturen. Het gevolg van dit alles is dat het steeds moeilijker wordt om onderscheid te maken tussen legitieme en kwaadaardige bronnen.

Met Mail Spectator voorkom je dat phising in jouw inbox terecht komt. In deze Whitepaper vertellen we hoe je kunt werken met de oplossing van Mail Spectator.

1. Waarom is werken met Mail Spectator belangrijk?

Phising en e-mail spam zijn de grootste kansen voor hackers om het netwerk van een organisatie binnen te komen. Uit onderzoek van The Hacker News blijkt dat 62% van alle cyberaanvallen in 2021 zijn gebaseerd op e-mail. Er hoeft maar één medewerker binnen een organisatie te zijn die op een kwaadaardige e-mail klikt om het hele bedrijf in gevaar te brengen. De schade die wordt veroorzaakt door phising-aanvallen leidt jaarlijks tot miljarden euro's aan verliezen. Dan hebben we het nog niet eens over de gevoelige bedrijfsinformatie en gezondheidsinformatie die misbruikt kan worden.

Door deze redenen is het van cruciaal belang om te evalueren wat de staat is van jouw e-mailbeveiliging en welke maatregelen je kunt nemen om deze te verbeteren.
Mail Spectator biedt een oplossing waardoor jouw domeinnaam gemonitord wordt. Dit met als doel om phishing en bijvoorbeeld CEO-fraude te voorkomen.

62% van alle cyberaanvallen in 2021 waren gebaseerd op e-mail

E-mail fraude is met 220% toegenomen de laatste twee jaren

Business Email Compromise (BEC) is door de FBI gerapporteerd als de meest financieel schadelijke cybercrime van 2020

2. Wat is Mail Spectator?

Mail Spectator controleert continu jouw domeinnaam. Wanneer iemand hier misbruik van maakt of wanneer jouw domeinnaam verkeerd is geconfigureerd, dan krijg je hier een melding van. Dankzij Mail Spectator kun je dus de beveiliging verbeteren en de afleverbetrouwbaarheid controleren. Mail Spectator voert de check uit aan de hand van SPF, DKIM en DMARC. Dit zijn de drie belangrijkste e-mailbeveiligingsprotocollen. Omdat ze elkaar aanvullen bieden deze drie samen de beste bescherming. Klinken deze drie termen als nieuw voor jou? Dat is geen probleem. Hierna geven we wat toelichting.

Sender Policy Framework (SPF)

Dit is een e-mailverificatieprotocol dat domeineigenaren gebruiken om de e-mailservers te specificeren van waaruit de e-mail verstuurd wordt. Hierdoor wordt het voor fraudeurs moeilijker om afzenderinformatie te vervalsen. Het SPF e-mailbeleid wordt over heel de wereld gebruikt. Je kunt het zien als een openbare lijst, waardoor iedereen weet waarvandaan de e-mail verstuurd wordt. Komt de e-mail niet overeen met de lijst? Dan moet de ontvanger deze e-mail als 'nep' behandelen.

Waarom is SPF belangrijk?
SPF speelt een sleutelrol in e-mailbeveiliging, omdat ze ervoor zorgen dat je domein alleen e-mail verstuurd vanuit een geverifieerde lijst met servers die je opgegeven hebt. Dit zorgt ervoor dat je e-mailbeveiliging drastisch verbeterd wordt. Een sterk SPF e-mailbeleid heeft belangrijke voordelen:

- **Leverbaarheid verbeteren**
Wanneer je jouw e-mailserver met SPF beveiligt, kunnen aanvallers je domein niet gebruiken om spam te versturen. Dit helpt om je domein van de zwarte lijsten te houden. Dit zorgt er weer voor dat de leverbaarheid van je e-mailservers wordt verbeterd.

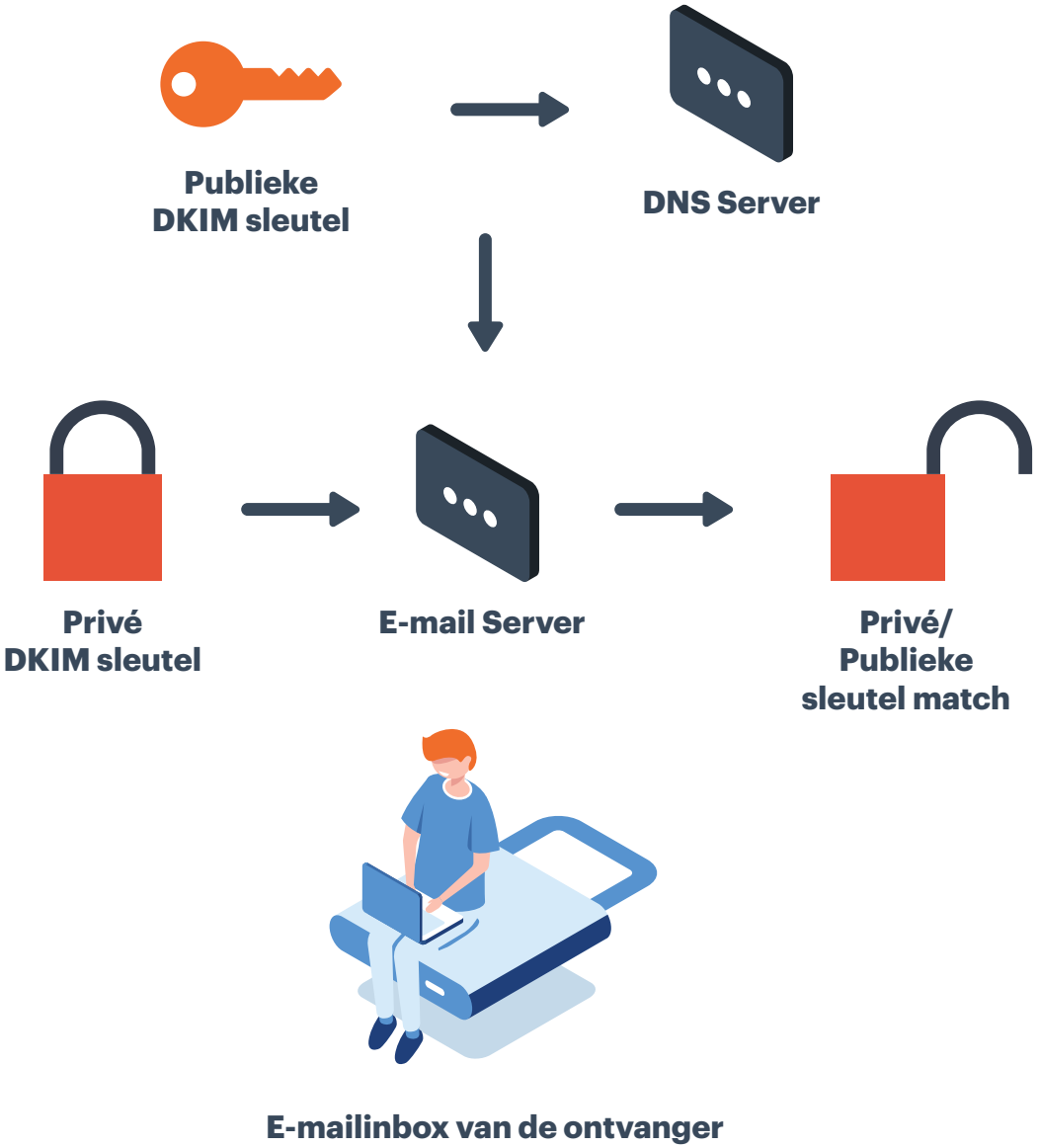
- **Bestrijd e-mailspoofing**
Bij e-mail spoofing wordt er een e-mail gestuurd vanuit een e-mailadres dat niet echt van de afzender is. Deze e-mail kan bijvoorbeeld vanuit jouw eigen e-mailadres, maar ook vanuit het e-mailadres van iemand anders. Een voorbeeld daarvan is CEO-fraude. Hierbij denken de medewerkers dat ze een mailtje krijgen van de leidinggevende. In realiteit is dit een mail van een crimineel die zich voordoet als de baas. Vaak wordt er gevraagd om geld naar hem over te maken. Omdat de medewerkers geneigd zijn om snel te doen wat de CEO vraagt, werkt deze vorm van fraude goed. SPF helpt om spoofing en phishing te voorkomen. Dit gebeurt door het IP-adres van de afzender te verifiëren in vergelijking met de domeineigenaar.

- **Verbetert de domeinreputatie**
Als je een SPF e-mailbeleid op bepaalde plaatsen hebt, dan krijgt je domein een betere reputatie. Je laat hiermee andere servers en sites op de zwarte lijst zien dat je je inzet voor e-mailbeveiliging. Hierdoor wordt de kans drastisch verkleint dat uitgaande e-mails ten oprechte als spam worden gemarkeerd. Tot slot helpt dit je ook om je positie binnen firewalls en andere cyberbeveiligingsdatabases te verbeteren.

Domain Keys Identified Mail (DKIM)

DKIM is een techniek die jouw domeinnaam gebruikt om je e-mail te ondertekenen met een digitale 'handtekening'. Hierdoor weten je klanten dat jij het echt bent die deze e-mails verstuurd en dat het tijdens het transport niet is gewijzigd. Fraudeurs kunnen bijvoorbeeld doen alsof een e-mail door iemand anders is verstuurd met behulp van een vervalst afzenderadres. Hierdoor kunnen fraudeurs e-mails sturen naar de werknemers die van de CEO lijken te komen, of e-mails naar klanten die van jou lijken te komen.

Hieronder is met een infographic afgebeeld hoe DKIM werkt. DKIM gebruikt een paar sleutels, een privé en een openbaar, om berichten te verifiëren. Een privédomeinsleutel voegt een versleutelde handtekeningkop toe aan alle uitgaande berichten die vanaf jouw domein worden verzonden. Een overeenkomende openbare sleutel wordt toegevoegd aan de Domain Name System (DNS)-record voor je domein.



Domain-based Message Authentication, Reporting & Conformance (DMARC)

Dit laatste protocol is een hele mond vol om uit te spreken. DMARC maakt het voor internetserviceproviders makkelijker om kwaadaardige e-mailpraktijken te voorkomen, zoals domein spoofing en phishing. Het stelt de afzender van de e-mail in staat om te specificeren hoe e-mails afgehandeld moeten worden die niet geverifieerd zijn met SPF en DKIM. Afzenders kunnen ervoor kiezen om deze e-mails naar de map met ongewenste e-mail te versturen of om al deze e-mail te blokkeren. Door dit te toen kunnen spammers beter worden geïdentificeerd en kan worden voorkomen dat kwaadaardige e-mails in de inbox van werknemers, partners of klanten binnendringen.

Waarom is DMARC belangrijk?

Reputatie
Het publiceren van DMARC beschermt de organisatie door te voorkomen dat niet-geverifieerde partijen e-mails versturen vanaf je domein. In sommige geval len kan alleen al het publiceren van een DMARC-record ervoor zorgen dat je een positieve reputatie krijgt.

Zichtbaarheid
DMARC-rapporten vergroten de zichtbaarheid van je e-mailprogramma door jou te laten weten wie een e-mail verstuurd vanaf je domein.

Beveiliging
DMARC helpt om een consistent beleid op te stellen over het omgaan met berichten die niet kunnen worden geverifieerd. Hierdoor wordt het hele e-mail systeem in het algeheel veiliger en betrouwbaarder.

SPF, DKIM en DMARC gecombineerd

Wanneer we het dus hebben over e-mailauthenticatie, dan hebben we het over SPF, DKIM en DMARC. De twee primaire authenticatieprotocollen zijn SPF en DKIM. Zij helpen om te valideren dat een e-mailbericht afkomstig is van de persoon waarvan het beweert afkomstig te zijn. Gelaagd bovenop SPF en DKIM is DMARC. DMARC gebruikt SPF en DKIM en biedt een reeks instructies voor de ontvangende e-mailservers, wat ze moeten doen als ze een niet-geverifieerde e-mail ontvangen in hun mailbox. Waar het ene protocol een beperking heeft, vult de ander dat weer aan. Daarom is het de meest optimale situatie voor je e-maildomein beveiliging wanneer deze drie beveiligingsprotocollen tegelijk gebruikt worden.

3. Wat zijn de voordelen van het gebruik van Mail Spectator?

De e-mailwereld wordt overspoeld door een stroom aan spam en phishing-berichten. Daarom wordt het steeds belangrijker om je berichten die je verstuurd correct in te richten en te verifiëren. Mail Spectator heeft een aantal voordelen voor jouw e-mail-beveiliging:

- ☑ De kans om prooi te worden van domein spoofing en phishing-aanvallen wordt zo klein mogelijk gemaakt
- ☑ Je krijgt de volledige controle over het e-mailecosysteem van je domein
- ☑ Je ervaart een boost op je merkreputatie, geloofwaardigheid en authenciteit
- ☑ In de loop van de tijd ervaar je een toename van het aantal e-mails dat bezorgd wordt
- ☑ De kans dat legitieme e-mails als spam worden gemarkeerd is klein.

Deze voordelen werken het beste wanneer je ernaar streeft om een zo hoog mogelijke score van je domeinbeveiliging te krijgen in Mail Spectator. Hierdoor kun je jouw bedrijfsdomein voldoende beschermen en zijn je e-mails veilig.

4. Hoe kan ik werken met de oplossing van Mail Spectator?

De eerste stap om de e-mailbeveiliging van je domein te verbeteren, is het beoordelen hoe goed het is beveiligd tegen inbraak, e-mailfraude en spoofing. Daarom begin je bij Mail Spectator door jouw domeinnaam in te vullen. Mail Spectator start dan met monitoren om de SPF-, DKIM- en DMARC-records van je domein te controleren en te testen. Hiermee kun je direct controleren of je domein beveiligd is tegen fraude. Er zijn vier verschillende functionaliteiten waarmee Mail Spectator jouw e-mailverkeer beter kan beveiligen.

1. De SPF, DKIM & DMARC check
Wanneer je domein een lage beoordeling heeft, dan kan dit te wijten zijn aan een slechte infrastructuur voor e-mailbeveiliging en onvoldoende of onjuiste e-mailverificatieprotocollen. In beide gevallen kan de reputatie en geloofwaardigheid van je domein geschaad worden. Een hoge score betekent dat je domein de beste bescherming biedt tegen alle soorten aanvallen en pogingen tot imitatie.

2. Waarschuwing
Mail Spectator geeft vervolgens een waarschuwing wanneer de configuratie is gewijzigd of wanneer het securityniveau is gedaald. Op deze manier kun je eenvoudig ontdekken of de domeinnaam wordt misbruikt.

3. Rapporten
Via Mail Spectator ontvang je rapporten van e-mailservers die e-mails met jouw domeinnaam hebben ontvangen. Hierdoor kun je direct ontdekken of jouw domeinnaam verkeerd is geconfigureerd of dat er misbruik van wordt gemaakt door anderen.

4. Monitor
Zodra de vorige stappen ingericht zijn wordt het monitoren vooral belangrijk. Mail Spectator maakt inzichtelijk welke e-mailstromen niet voldoen aan de geconfigureerde records. Voorbeelden hiervan kunnen zijn dat een hacker misbruik probeert te maken van de domeinnaam. Een ander voorbeeld is dat de marketingafdeling bijvoorbeeld gebruik maakt van een nieuwe tool voor nieuwsbrieven, maar de IT-afdeling vergeet in te lichten. Hierdoor kunnen de e-mails in de spam box terecht komen. Vooral bij dit laatste voorbeeld is te zijn dat het niet altijd kwaadaardige bedoelingen zijn. Daarom blijft het monitoren belangrijk.

OVER SECURITYHIVE

"Iemand heeft een slechte bijlage geopend"
mag nooit de reden zijn waarom het hele bedrijf niet kan werken.

SecurityHive - opgericht in 2017 door Nederlandse techneuten - ontwikkelt oplossingen om cybersecurity maximaal eenvoudig te maken. Het is ons doel om bedrijven een veilige toekomst te bieden en zo ongestoord te groeien. Het resultaat van onze visie is dat cybersecurity toepasbaar en begrijpelijk is voor iedereen. Wereldwijd vertrouwen partners en organisaties op de technologie van SecurityHive. Samen met het beste netwerk aan partners, beschermen wij grote en kleine bedrijven in elke sector.

Kom in contact met SecurityHive-experts voor meer informatie.

Securityhive.nl | LinkedIn.com/SecurityHive

SECURITYHIVE