DMARCSaaS™

SPF, DKIM en DMARC as a Service

Bescherm uw e-mailcommunicatie tegen financiële- en reputatieschade.

Stay in control and secure your communication with DMARCSaaS™

E-mailcommunicatie is al lang niet meer weg te denken uit de hedendaagse manier van communiceren. E-mail vormt een essentiële en vaak zelfs kritische manier om informatie te delen en zaken te doen. Er zitten helaas een paar kwetsbaarheden in het ontwerp van het e-mail communicatiesysteem. Het is pijnlijk gebleken dat organisaties hierdoor financiële- en reputatie risico's lopen. Vandaar dat het zaak is dat uw e-mail betrouwbaar blijft. DMARCSaaS™ helpt u op een geautomatiseerde manier deze zwakheden en risico's eenvoudig te verhelpen.

Voorbeelden van e-mailrisico's

Onderstaand enkele voorbeelden van e-mail risico's die worden afgevangen met DMARCSaaS™:

Beveiliging tegen:

- Financiële schade
- Reputatieschade
- E-mails komen niet aan
- Verlies vertrouwelijke gegevens

1) CEO-fraude: Een argeloze werknemer of manager van de financiële afdeling ontvangt een ogenschijnlijk betrouwbaar e-mailbericht van de CEO of CFO met het verzoek om gevoelige data te delen of om geld over te schrijven naar een rekening van de fraudeur.
2) Spookfactuur: De inkoopafdeling ontvangt van een ogenschijnlijk betrouwbaar e-mailbericht van een bekende leverancier met een betalingsverzoek naar een rekening van de fraudeur.
3) Attorney Impersonation: Fraudeurs doen zich via een ogenschijnlijk betrouwbaar e-mailbericht voor als een advocaat of iemand van het advocatenkantoor om cruciale en vertrouwelijke zaken te ontvreemden.
4) Persoonlijke gegevensdiefstal: Medewerkers van personeelszaken of de boekhouding ontvangen een ogenschijnlijk betrouwbaar e-mailbericht met het verzoek om persoonlijk identificeerbare informatie (PII) of belastingaangiften van werknemers en leidinggevenden te sturen.
5) E-mail reputatie / SPAM blacklist: Een vertrouwd e-maildomein van een organisatie wordt ergens wereldwijd misbruikt om SPAM te verspreiden, waardoor het gehele e-maildomein op één of meerdere SPAM blacklists komt te staan. Hierdoor wordt tijdelijk al de e-mailberichten vanuit dat domein niet meer geaccepteerd, totdat de organisatie het lukt om van de blacklist af te worden gehaald.
6) Phishing en schadelijke e-mails naar uw klanten: Klanten ontvangen via een ogenschijnlijk betrouwbaar e-mailadres van een organisatie het verzoek om een accountaanpassing, waarbij gevoelige privédata door de fraudeur wordt ontfutseld, of klanten worden geïnfecteerd door mogelijke malware in deze e-mails.

Amitron BV
Maasstraat 15A
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

DMARCSaaS™

DMARCSaaS™ is een geautomatiseerde workflow service voor het inrichten, monitoren en beheren van drie bekende toegepaste e-mail authenticatie technieken voor het inkomende en uitgaande e-mailverkeer: SPF, DKIM en DMARC. Hiermee worden de bovenstaande e-mail risico's voorkomen. Zie voor verdere uitleg van de gebruikte open standaarden en technieken van SPF, DKIM en DMARC: https://www.amitron.nl/dmarcsaas

> DMARCSaaS™ & e-mail marketing campagnes
>
> Door het gebruik van DMARCSaaS™ loopt uw email marketingcampagne veel beter, omdat DMARCSaaS™ er voor zorgt dat uw e-mail bij de beoogde ontvanger aankomt.

DMARCSaaS™ bestaat uit een initiële inrichtingsperiode en een opvolgende monitoringsperiode.

Inrichtingsperiode

De volgende stappen worden door DMARCSaaS™ tijdens de inrichtingsperiode uitgevoerd:

1) **Analyse e-maildomein(en):** Analyse van de initiële SPF, DKIM en DMARC instellingen van de e-maildomein(en).
2) **Instructiestappen:** Aan de hand van de analyse van stap 1 worden duidelijke instructiestappen voor de aanpassingen in de publieke DNS (SPF, DKIM en DMARC) en e-mailserver aangereikt. Deze dienen te worden uitgevoerd door de e-mailbeheerder van de opdrachtgever.
3) **Controle:** De juiste invoer van de instructiestappen wordt automatisch gecontroleerd.
4) **Analyse:** De resultaten van elke instructiestap worden geanalyseerd en gepresenteerd.
5) **Automatische vervolgstap:** Na elke analyse volgt weer de volgende instructie, controle en analyse. Dit herhaalt zich totdat het einddoel is bereikt: een strenge ("reject") DMARC policy.
6) **Afronding:** De inrichtingsperiode wordt na deze geleidelijke en gecontroleerde periode van automatische workflow afgesloten, nadat het DMARC securitybeleid naar het einddoel: "reject" is gebracht. Na een succesvolle afronding heeft de organisatie haar eigen e-mail authenticatie securitybeleid gedicteerd naar de buitenwereld.

Monitoringsperiode

Na de inrichtingsperiode volgt de monitoringsperiode en gaat de DMARCSaaS™ dienst over tot het continue monitoren, rapporteren en het periodiek adviseren van de drie authenticatiemethoden. Dit omvat de volgende stappen:

> DMARCSaaS ™ & de overheid
>
> Alle overheidsinstellingen in Nederland moeten aan de SPF, DKIM en DMARC verplichtingen gaan voldoen. Door het gebruik van DMARCSaaS ™ heeft u dit goed geregeld.

1) **Controle en test:** Controle en test van de SPF, DKIM en DMARC statussen van de e-maildomein(en).
2) **Analyse:** De resultaten van de controles worden geanalyseerd en gepresenteerd. Daarnaast worden wereldwijd verstuurde DMARC-rapportages over afgeleverde e-mails en misbruik in één overzichtelijke rapportage samengevoegd. Hiermee verkrijgt uw organisatie continu inzicht in potentiële pogingen tot misbruik en de effectiviteit van DMARCSaaS™.
3) **Advies:** Automatisch en continu bijhouden van actieve en niet actieve IP-adressen van uw e-mailservers voor een eventueel opschoningsadvies van overbodige SPF-records en het geautomatiseerde advies voor het digitale sleutelmanagement ten behoeve van DKIM. Door deze monitoring blijft de door DMARCSaaS™ ingerichte e-mailbescherming gezond.

Amitron BV
Maasstraat 15A
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

De voordelen DMARCSaaS™

DMARCSaaS™ zorgt ervoor dat:

1) financiële schade door onder andere CEO-fraude, Business Email Compromise, et cetera wordt voorkomen;
1) uw medewerkers niet onbewust onderdeel worden van frauduleuze acties;
2) phishing e-mails en eventuele malware bij u en uw klanten worden geblokkeerd;
3) wereldwijd misbruikpogingen van uw e-mail domeinen worden gemonitord en gerapporteerd;
4) uw e-maildomein niet op SPAM blacklists belandt waardoor uw e-mailberichten geblokkeerd worden en u email als onbetrouwbaar wordt bestempeld;
5) er niet geïnvesteerd hoeft te worden in de kennis en ervaring van uw IT-medewerkers in de complexe SPF, DKIM en DMARC materie. De kennis wordt tijdens het DMARCSaaS™-proces stap voor stap opgebouwd;
6) e-mail security awareness groeit onder uw IT-medewerkers;
7) er geen additionele hoge kosten voor SPF, DKIM en DMARC consultants worden gemaakt met complexe trajecten en u de software niet hoeft aan te schaffen;
8) DMARC-policy geleidelijk en volledige gecontroleerd geïmplementeerd wordt;
9) tijdens de monitoringsperiode de drie geïmplementeerde technologieën (SPF, DKIM en DMARC) zodanig worden gecontroleerd en beheerd, dat deze niet op de achtergrond verdwijnen of ineffectief worden;
10) DMARC rapportages geconsolideerd worden in één overzichtelijke rapportage.

DMARCSaaS™ (SPF, DKIM en DMARC as a Service)	Fase
✓ Inrichtingsperiode SPF, DKIM en DMARC (aanlevering DNS records en signatures)	I
✓ Progressielijn inrichtingsfase (DMARC p=none naar p=reject)	I
✓ Monitoring van actieve domeinen	I, M
✓ Automatische analyse DMARC XML-rapportages inclusief adviesstappen	I, M
✓ Automatische rapportages over subdomeinen	I, M
✓ Automatische meldingen en adviesstappen inclusief detail beschrijving uit te voeren werkzaamheden	I, M
✓ Automatische periodieke DMARC, SPF, DKIM-controles inclusief adviesstappen en status updates	I, M
✓ Automatische verwerking van DMARC-rapportages (RUA)	I, M
✓ Automatische verwerking van DMARC-rapportages (RUF)	M
✓ Onbeperkt aantal inactieve domeinen	I, M
✓ Onbeperkte e-mail stroom	I, M
✓ Onbeperkt aantal gebruikers	I, M
✓ > 1 jaar datahistorie	I, M
✓ Groeperen van domeinen per portal en rapportage	I, M

I = Inrichtingsperiode DMARCSaaS™
M = Monitoringsperiode DMARCSaaS™

Stay in control and secure your communication with DMARCSaaS™

Heeft u na het lezen van deze datasheet interesse in DMARCSaaS ™? Neem dan contact op.

T: +31 (0)10 870 01 50
E: info@amitron.nl

Amitron BV
Maasstraat 15A
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl