CENTRE FOR CYBERSECURITY BELGIUM

dnsbelgium

DMARC INTEGRATIE & IMPLEMENTATIE

Inhoud

DOCUMENT CONTROL AND REVIEW

Document Control	
Author	
Owner	
Date created	
Last revised by	
Last revision date	

.

VERSION CONTROL

Version	Date of approval	Approved by	Description of change
1.0			

Inleiding: Waarom DMARC implementeren?

In de huidige digitale wereld vormt e-mail een essentieel communicatiemiddel, zowel binnen organisaties als met klanten en partners. Tegelijkertijd is e-mail een van de meest misbruikte aanvalsvectoren voor cybercriminelen, die gebruik maken van technieken zoals phishing, spoofing en fraude om vertrouwelijke gegevens te stelen of schade toe te brengen aan organisaties.

Om deze risico's effectief aan te pakken, is de implementatie van **DMARC** een cruciale stap. DMARC is een e-mailauthenticatieprotocol dat organisaties in staat stelt de afzenderidentiteit van hun e-mails te beschermen, misbruik van hun domein te voorkomen en transparantie te bieden in e-mailverkeer door middel van rapportages. Het bouwt voort op bestaande protocollen zoals SPF (Sender Policy Framework) en DKIM (DomainKeys Identified Mail) en voegt een extra laag van controle en beheer toe.

Hieronder volgen de belangrijkste redenen waarom DMARC een essentieel onderdeel is van een robuust e-mailbeveiligingsbeleid:

1. Bescherming tegen e-mailspoofing

DMARC biedt een krachtige verdediging tegen e-mailspoofing, een techniek waarbij aanvallers e-mails versturen die lijken te komen van een legitieme afzender. Door te eisen dat e-mails zowel SPF als DKIM valideren en door een afkeuringsbeleid (zoals quarantaine of blokkeren) af te dwingen, voorkomt DMARC dat frauduleuze e-mails worden afgeleverd bij ontvangers.

2. Verbetering van de e-mailreputatie

Wanneer een domein wordt misbruikt voor phishing- of spamactiviteiten, kan dit leiden tot reputatieschade en een verhoogde kans dat legitieme e-mails als spam worden gemarkeerd. DMARC helpt organisaties hun e-mailreputatie te beschermen door te voorkomen dat onbevoegde partijen misbruik maken van hun domein.

3. Versterking van klantvertrouwen

Fraude via e-mail kan leiden tot verlies van vertrouwen bij klanten en partners, vooral als ze worden getroffen door spoofingaanvallen die de naam van het bedrijf misbruiken. Door DMARC te implementeren, toont een organisatie aan dat ze proactief maatregelen neemt om haar klanten en partners te beschermen tegen cyberdreigingen.

4. Inzicht in e-mailverkeer en bedreigingen

Een van de unieke voordelen van DMARC is het rapportagemechanisme. Door DMARC-rapportages in te schakelen, krijgen organisaties inzicht in:

- Welke servers e-mails verzenden namens hun domein.
- Hoe vaak SPF en DKIM verificaties slagen of falen.
- Pogingen tot misbruik van het domein door onbevoegde partijen.

Dit biedt waardevolle informatie om beveiligingsincidenten te detecteren en e-mailinfrastructuur te optimaliseren.

5. Voldoen aan wettelijke en branchevereisten

In bepaalde sectoren, zoals de financiële en gezondheidssector, worden strenge eisen gesteld aan gegevensbeveiliging en privacy. DMARC kan bijdragen aan het voldoen aan regelgeving zoals de GDPR, PCI DSS, en NIS2, door te zorgen voor beter beveiligde e-mailcommunicatie.

6. Verbetering van e-mailbezorgbaarheid

Door DMARC te implementeren, kunnen organisaties de kans vergroten dat legitieme e-mails correct worden afgeleverd. Wanneer ontvangers vertrouwen hebben in de authenticiteit van e-mails van een domein, verminderen ze de kans dat e-mails als spam worden gemarkeerd.

7. Kostenbesparing

De gevolgen van een phishingaanval of e-mailfraude kunnen enorm zijn, zowel financieel als operationeel. Dit omvat kosten voor incidentrespons, herstel van reputatieschade, juridische boetes en verlies van klantvertrouwen. DMARC helpt deze risico's te beperken en biedt een kosteneffectieve manier om proactief beveiligingsmaatregelen te nemen.

8. Bescherming van merken en intellectueel eigendom

Een van de grootste bedreigingen voor bedrijven is het misbruik van hun merknaam in phishing- en frauduleuze e-mails. Dit kan leiden tot verlies van vertrouwen bij klanten en schade aan intellectueel eigendom. DMARC beschermt merken door te voorkomen dat derden onrechtmatig gebruik maken van een bedrijfsdomein.

9. Synergie met andere protocollen

DMARC werkt samen met andere e-mailbeveiligingsprotocollen zoals SPF en DKIM. Terwijl SPF en DKIM zorgen voor technische authenticatie van e-mails, voegt DMARC een beleids- en rapportagelaag toe. Deze combinatie biedt een uitgebreide beveiliging tegen de meest voorkomende e-maildreigingen. De implementatie van DNSSEC zorgt dan weer voor de integriteit van het DMARC record.

10. Eenvoudige implementatie met stapsgewijze aanpak

Hoewel DMARC aanvankelijk complex lijkt, kan het stapsgewijs worden geïmplementeerd. Organisaties kunnen beginnen met een "none"-beleid (geen acties uitvoeren) om inzicht te krijgen in hun e-mailstromen en later overgaan op strengere beleidsregels zoals "quarantine" of "reject". Dit maakt de implementatie beheersbaar en flexibel.

11. Conclusie

DMARC is een essentieel onderdeel van een robuust e-mailbeveiligingsbeleid en biedt bescherming tegen een breed scala aan bedreigingen die voortvloeien uit het misbruik van e-maildomeinen. Naast het voorkomen van spoofing, versterkt het de e-mailreputatie, verhoogt het klantvertrouwen, biedt het inzicht in e-mailverkeer en draagt het bij aan naleving van regelgeving.

Met DMARC kan een organisatie niet alleen haar eigen beveiliging verbeteren, maar ook bijdragen aan een veiliger internetecosysteem als geheel.

12. Hoe werkt DMARC?

DMARC voegt een extra laag toe bovenop SPF en DKIM door drie hoofdfuncties te bieden:

12.1 AUTHENTICATIECONTROLE

Bij ontvangst van een e-mail controleert de ontvangende mailserver of de e-mail:

1. **SPF-compliant** is: Het verzendende IP-adres moet in het SPF-record van het domein staan.
2. **DKIM-compliant** is: De digitale handtekening in de e-mail moet geldig zijn.
3. **Alignment** heeft: SPF- en/of DKIM-waarden moeten overeenkomen met het **"From"-domein** dat de gebruiker ziet.

12.2 BELEIDSAFDWINGING

DMARC stelt domeineigenaren in staat om een beleid te definiëren dat aangeeft hoe de ontvangende server moet omgaan met e-mails die niet voldoen aan de authenticatieregels:

- none: Geen actie, alleen rapporteren (vaak gebruikt bij het testen).
- quarantine: Markeer niet-authentieke e-mails als verdacht of plaats ze in de spammap.
- reject: Weiger niet-authentieke e-mails volledig.

12.3 RAPPORTAGE

DMARC biedt twee soorten rapporten:

1. **Aggregate Reports**: Een overzicht van alle e-mails die namens een domein worden verzonden, inclusief resultaten van SPF/DKIM-controles.
2. **Failure Reports** (optioneel): Gedetailleerde rapporten over mislukte authenticatiepogingen.

Deze rapporten worden verzonden naar het e-mailadres dat is opgegeven in het DMARC-record.

13. DMARC-records opbouwen

DMARC wordt geconfigureerd als een **TXT-record** in DNS en heeft de volgende syntaxis:

v=DMARC1; p=<beleid>; rua=mailto:<rapportage-email>; ruf=mailto:<foutmeld-email>; fo=<opties>; sp=<subdomeinbeleid>; pct=<percentage>

Belangrijke tags:

- **v=DMARC1**: Geeft aan dat dit een DMARC-record is (verplicht).
- **p**: Beleidsregel (none, quarantine, reject) (verplicht).
- **rua**: E-mailadres voor aggregate rapporten (optioneel).
- **ruf**: E-mailadres voor failure rapporten (optioneel).
- **fo**: Failure-opties, bijv. 1 (geef een rapport bij één mislukking) of d (geef een rapport voor alleen DKIM-fouten).
- **sp**: Beleid voor subdomeinen (optioneel).
- **pct**: Percentage van e-mails waarop het beleid wordt toegepast (standaard: 100).

Voorbeeld van een DMARC-record:

v=DMARC1; p=reject; rua=mailto:dmarc-reports@voorbeeld.nl; ruf=mailto:dmarc-errors@voorbeeld.nl; fo=1; sp=reject; pct=100

- p=reject: Weiger e-mails die niet slagen voor SPF/DKIM.
- rua: Aggregate rapporten worden verzonden naar dmarc-reports@voorbeeld.nl.
- ruf: Failure rapporten worden verzonden naar dmarc-errors@voorbeeld.nl.
- fo=1: Stuur een rapport bij een enkele fout.
- sp=reject: Zelfde beleid geldt voor subdomeinen.
- pct=100: Pas beleid toe op 100% van de inkomende e-mails.

14. Stapsgewijze implementatie van DMARC

14.1 ANALYSEER BESTAANDE E-MAILINFRASTRUCTUUR

- Identificeer alle systemen en diensten die e-mails verzenden namens je domein (bijv. mailservers, marketingtools, CRM-systemen).
- Zorg ervoor dat SPF en DKIM correct zijn ingesteld.

14.2 START MET EEN "NONE"-BELEID

Begin met het implementeren van een DMARC-record met het p=none beleid. Dit verzamelt gegevens over e-mails zonder daadwerkelijk actie te ondernemen. Gebruik een record zoals:

v=DMARC1; p=none; rua=mailto:dmarc-reports@voorbeeld.nl

14.3 ANALYSEER DMARC-RAPPORTEN

- Gebruik tools zoals DMARC-analyzers (bijv. DMARCian of Valimail) om inzicht te krijgen in verzendende bronnen en misbruikpogingen.
- Identificeer ongeldige bronnen en pas SPF/DKIM aan om deze te autoriseren, indien legitiem.

14.4 SCHAKEL OVER NAAR EEN "QUARANTINE"-BELEID

Wanneer je vertrouwen hebt in de configuratie, wijzig het beleid naar p=quarantine. Hierdoor worden verdachte e-mails in de spammap geplaatst:

v=DMARC1; p=quarantine; rua=mailto:dmarc-reports@voorbeeld.nl

14.5 VERHOOG STRENGHEID NAAR "REJECT"

Zodra je zeker bent dat alle legitieme bronnen correct zijn ingesteld, wijzig het beleid naar p=reject om frauduleuze e-mails volledig te blokkeren:

v=DMARC1; p=reject; rua=mailto:dmarc-reports@voorbeeld.nl

15. Monitor en optimaliseer continu

- Blijf DMARC-rapporten analyseren om te controleren op nieuwe bedreigingen.
- Voeg nieuwe geautoriseerde e-mailbronnen toe aan SPF/DKIM-configuraties indien nodig.

16. Technische voordelen van DMARC

- **End-to-end beveiliging**: DMARC zorgt ervoor dat alleen geautoriseerde bronnen e-mails namens het domein mogen verzenden.
- **Transparantie**: Het rapportagemechanisme biedt real-time inzicht in e-mailverkeer.
- **Bescherming tegen impersonatie**: Voorkomt dat aanvallers succesvol phishingcampagnes uitvoeren met een gespoofd domein.
- **Controle over subdomeinen**: Specifiek beleid kan worden toegepast op subdomeinen met de sp-tag.

17. Veelvoorkomende uitdagingen en oplossingen

Uitdaging	Oplossing
Correct configureren van SPF/DKIM	Controleer records met tools zoals MXToolbox of SPF/DKIM-validator.
Verkeerd beleid leidt tot geblokkeerde e-mails	Start altijd met een "none"-beleid en analyseer rapporten voordat je naar strengere beleidsregels gaat.
Complexiteit bij meerdere e-mailbronnen	Houd een gedetailleerde lijst van geautoriseerde bronnen bij en gebruik de include-mechanismen in SPF.

18. Synergie met andere protocollen

DMARC werkt in harmonie met:

- **SPF**: Valideert of het verzendende IP-adres bevoegd is.
- **DKIM**: Controleert of de inhoud van de e-mail tijdens verzending niet is gewijzigd.
- **BIMI** (Brand Indicators for Message Identification): Combineer DMARC met BIMI om merklogo's weer te geven in compatibele e-mailclients.
- **DNSSEC:** zorgt voor de integriteit van het DMARC record.

Disclaimer