CENTRE FOR CYBERSECURITY BELGIUM

dnsbelgium

SPF 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

Inleiding: Waarom SPF implementeren?

In een tijdperk waarin e-mail de ruggengraat vormt van digitale communicatie, wordt de beveiliging van e-mailverkeer steeds belangrijker. Cybercriminelen maken op grote schaal gebruik van kwetsbaarheden in e-mailprotocollen om phishing, spoofing en andere vormen van e-mailfraude uit te voeren. Een van de meest effectieve methoden om deze risico's te mitigeren, is de implementatie van **Sender Policy Framework (SPF)**.

SPF (Sender Policy Framework) is een e-mailauthenticatiemechanisme waarmee domeineigenaren kunnen specificeren welke mailservers bevoegd zijn om e-mails te verzenden namens hun domein. Ontvangende mailservers gebruiken deze informatie om te controleren of een inkomende e-mail legitiem is. Dit gebeurt door het SPF-record van het domein van de afzender te raadplegen, dat is opgeslagen in het Domain Name System (DNS).. Hieronder worden enkele van de belangrijkste redenen voor het implementeren van SPF uiteengezet:

1. Bescherming tegen e-mailspoofing

E-mailspoofing is een techniek waarbij aanvallers e-mails versturen die lijken te komen van een vertrouwde afzender, zoals een bank of een intern bedrijfsadres. Dit is een van de meest gebruikte methoden in phishing-aanvallen. SPF helpt dergelijke aanvallen te voorkomen door alleen geautoriseerde servers toe te staan e-mails te verzenden namens een domein.

2. Versterking van bedrijfsreputatie

Een succesvolle spoofingaanval kan ernstige reputatieschade veroorzaken voor een organisatie. Klanten en partners die frauduleuze e-mails ontvangen, verliezen vertrouwen in het merk. SPF draagt bij aan het behoud van de betrouwbaarheid en integriteit van de bedrijfscommunicatie.

3. Verbetering van e-mailbezorgbaarheid

SPF helpt bij het verbeteren van de bezorgbaarheid van legitieme e-mails. Zonder SPF kunnen e-mails afkomstig van een domein als verdacht worden gemarkeerd en in de spamfolder van de ontvanger terechtkomen. Met SPF wordt de kans groter dat e-mails correct worden afgeleverd.

4. Voldoen aan compliance en regelgeving

In veel sectoren, zoals de financiële en gezondheidssector, worden strikte eisen gesteld aan gegevensbeveiliging en communicatieprotocollen. SPF kan een cruciaal onderdeel zijn van een breder beveiligingsbeleid om aan deze eisen te voldoen.

5. Kostenbesparing

Een succesvolle phishing- of spoofingaanval kan leiden tot aanzienlijke financiële schade, zoals herstelkosten en boetes. Door SPF te implementeren, kunnen organisaties het risico op dergelijke incidenten drastisch verkleinen en dus kosten besparen op lange termijn.

6. Eenvoudige implementatie en brede ondersteuning

SPF is relatief eenvoudig te implementeren via een DNS-record en wordt breed ondersteund door moderne e-mailservers. Dit maakt het een kosteneffectieve en toegankelijke maatregel voor organisaties van elke omvang.

7. Synergie met andere e-mailbeveiligingsprotocollen

SPF werkt goed samen met andere beveiligingsprotocollen zoals DKIM (DomainKeys Identified Mail) en DMARC (Domain-based Message Authentication, Reporting, and Conformance). Samen vormen deze protocollen een krachtig framework om de veiligheid en betrouwbaarheid van e-mailverkeer te waarborgen.

8. Conclusie

Door SPF te implementeren, legt een organisatie een solide basis voor een veiliger en betrouwbaarder e-mailsysteem. Het is een eerste stap richting een uitgebreide aanpak van e-mailbeveiliging die niet alleen bijdraagt aan de bescherming van de organisatie zelf, maar ook van haar klanten, partners en stakeholders.

9. Hoe werkt SPF?

9.1 SPF-RECORD IN DNS

Een domeineigenaar publiceert een SPF-record als een **TXT-record** in de DNS-instellingen van het domein. Dit record bevat een lijst van geautoriseerde mailservers (bijvoorbeeld IP-adressen, domeinnamen of subdomeinen).

9.2 VERZENDING VAN EEN E-MAIL

Wanneer een e-mail wordt verzonden, bevat deze een **"MAIL FROM" adres** in de SMTP-headers. Dit is het adres dat door SPF wordt gecontroleerd.

9.3 CONTROLE DOOR DE ONTVANGENDE MAILSERVER

Bij ontvangst van een e-mail controleert de ontvangende mailserver de DNS van het domein van de afzender om het SPF-record op te halen. Vervolgens worden de volgende stappen uitgevoerd:

- **Extractie van de verzendende IP-adres**: Het IP-adres van de server die de e-mail heeft verzonden, wordt bepaald.
- **Vergelijking met SPF-record**: Het verzendende IP-adres wordt gecontroleerd tegen de lijst van geautoriseerde servers in het SPF-record.
- **Resultaat bepalen**: De ontvangende server evalueert het resultaat van de SPF-check en neemt een beslissing:
    - **Pass**: Het verzendende IP-adres staat in het SPF-record. De e-mail wordt geaccepteerd.
    - **Fail**: Het verzendende IP-adres staat niet in het SPF-record. De server kan de e-mail markeren als spam of weigeren.
    - **Softfail**: De e-mail wordt niet volledig vertrouwd, maar niet geweigerd. Meestal gemarkeerd als verdacht.
    - **Neutral**: Geen expliciete regels in het SPF-record. De e-mail wordt normaal verwerkt.
    - **Permerror**: Het SPF-record is ongeldig of onleesbaar.

10. SPF-records opbouwen

SPF-records worden geconfigureerd als TXT-records in DNS. De syntax bevat verschillende mechanismen en qualifiers:

10.1 ALGEMENE OPBOUW

v=spf1 <mechanismen> <modifiers>

- v=spf1: Geeft aan dat dit een SPF-record is (verplicht).
- <mechanismen>: Regels die bepalen welke servers geautoriseerd zijn.
- <modifiers>: Optionele parameters voor meer geavanceerde configuratie.

10.2 VEELGEBRUIKTE MECHANISMEN

- ip4:<ip-adres>: Autoriseert een specifiek IPv4-adres of subnet.
- ip6:<ip-adres>: Autoriseert een specifiek IPv6-adres of subnet.
- a: Autoriseert het IP-adres dat aan het "A-record" van het domein is gekoppeld.
- mx: Autoriseert de mailservers (MX-records) van het domein.
- include:<domein>: Autoriseert SPF-records van een ander domein (handig voor externe providers zoals Google Workspace of Microsoft 365).
- all: Wordt gebruikt als afsluiter, geeft aan wat te doen met alle niet-gematchte adressen (bijvoorbeeld -all voor blokkeren).

10.3 VOORBEELD SPF-RECORD

Een SPF-record voor een domein dat mail verstuurt via een eigen server (IP: 192.0.2.1) en Google Workspace zou er als volgt uitzien:

v=spf1 ip4:192.0.2.1 include:_spf.google.com -all

- ip4:192.0.2.1: Staat een specifiek IP-adres toe.
- include:_spf.google.com: Stelt e-mails toe van servers die door Google zijn geautoriseerd.
- -all: Verwerpt alle andere Emails.

11. Implementatiestappen

11.1 BEPAAL VERZENDENDE E-MAILSERVERS

- Identificeer alle servers of providers die e-mails versturen namens jouw domein.
- Vergeet geen externe providers zoals nieuwsbrievenservices (Mailchimp, etc.).

11.2 CONFIGUREER HET SPF-RECORD

- Voeg een nieuw TXT-record toe aan de DNS van je domein.
- Zorg ervoor dat het record alle benodigde mechanismen bevat.

11.3 TEST HET SPF-RECORD

- Gebruik online tools zoals MXToolbox, https://nl.internet.nl/ of SPF Record Checker om je SPF-record te valideren.
- Controleer of het SPF-record correct wordt geïmplementeerd en geparsed door DNS-servers.

11.4 MONITOR HET E-MAILVERKEER

- Controleer of legitieme e-mails goed worden afgeleverd.
- Gebruik tools zoals DMARC-rapportage om inzicht te krijgen in SPF-fails.

12. Beperkingen van SPF

Hoewel SPF effectief is, heeft het enkele beperkingen:

- **Forwarding-problemen**: SPF faalt vaak bij e-mailforwarding omdat de forwarder niet in het originele SPF-record staat.
- **Afhankelijkheid van DNS**: Ontvangers moeten DNS-query's uitvoeren, wat kan falen bij netwerkproblemen.
- **Alleen MAIL FROM-check**: SPF beschermt alleen het "MAIL FROM"-adres en niet het "From"-adres dat gebruikers zien.

13. SPF in combinatie met andere protocollen

SPF werkt het best in combinatie met andere e-mailbeveiligingsprotocollen:

- **DKIM**: Verifieert dat de inhoud van een e-mail niet is gewijzigd tijdens transport.
- **DMARC**: Biedt een beleidsraamwerk om SPF en DKIM te combineren en misbruik te rapporteren.

Disclaimer