CENTRE FOR CYBERSECURITY BELGIUM

dnsbelgium

SPF-INTEGRATION UND -IMPLEMENTIERUNG.

Inhalt

DOKUMENTENKONTROLLE UND -PRÜFUNG

Dokumentenkontrolle	
Autor	
Eigentümer	
Datum der Erstellung	
Zuletzt überarbeitet von	
Datum der letzten Überarbeitung	

.

VERSIONSKONTROLLE

Version	Datum der Genehmigung	Genehmigt durch	Beschreibung der Änderung

Einführung: Warum SPF einführen?

In einer Zeit, in der die E-Mail das Rückgrat der digitalen Kommunikation ist, wird die Sicherung des E-Mail-Verkehrs immer wichtiger. Cyber-Kriminelle nutzen häufig Schwachstellen in E-Mail-Protokollen aus, um Phishing, Spoofing und andere Formen des E-Mail-Betrugs durchzuführen. Eine der wirksamsten Methoden zur Eindämmung dieser Risiken ist die Implementierung des **Sender Policy Framework (SPF)**.

SPF (Sender Policy Framework) ist ein E-Mail-Authentifizierungsmechanismus, mit dem Domänenbesitzer angeben können, welche Mailserver berechtigt sind, E-Mails im Namen ihrer Domäne zu versenden. Die empfangenden Mailserver nutzen diese Informationen, um zu prüfen, ob eine eingehende E-Mail legitim ist. Dies geschieht durch Abfrage des SPF-Eintrags der Domäne des Absenders, der im Domain Name System (DNS) gespeichert ist. Einige der Hauptgründe für die Implementierung von SPF werden im Folgenden erläutert:

1. Schutz gegen E-Mail-Spoofing

E-Mail-Spoofing ist eine Technik, bei der Angreifer E-Mails versenden, die scheinbar von einem vertrauenswürdigen Absender stammen, z. B. von einer Bank oder einer internen Firmenadresse. Dies ist eine der am häufigsten verwendeten Methoden bei Phishing-Angriffen. SPF hilft, solche Angriffe zu verhindern, indem es nur autorisierten Servern erlaubt, E-Mails im Namen einer Domäne zu versenden.

2. Stärkung der Unternehmensreputation

Ein erfolgreicher Spoofing-Angriff kann dem Ruf eines Unternehmens schweren Schaden zufügen. Kunden und Partner, die betrügerische E-Mails erhalten, verlieren das Vertrauen in die Marke. SPF hilft, die Zuverlässigkeit und Integrität der Unternehmenskommunikation zu wahren.

3. Verbesserung der Zustellbarkeit von E-Mails

SPF trägt dazu bei, die Zustellbarkeit von legitimen E-Mails zu verbessern. Ohne SPF können E-Mails, die von einer Domäne kommen, als verdächtig eingestuft werden und im Spam-Ordner des Empfängers landen. Mit SPF ist die Wahrscheinlichkeit größer, dass E-Mails korrekt zugestellt werden.

4. Einhaltung von Vorschriften und Regeln

In vielen Branchen, z. B. im Finanz- und Gesundheitswesen, gibt es strenge Anforderungen an die Datensicherheit und die Kommunikationsprotokolle. SPF kann ein wichtiger Teil einer umfassenderen Sicherheitsstrategie sein, um diese Anforderungen zu erfüllen.

5. Kosteneinsparungen

Ein erfolgreicher Phishing- oder Spoofing-Angriff kann zu erheblichen finanziellen Verlusten führen, z. B. durch Wiederherstellungskosten und Geldstrafen. Durch die Einführung von SPF können Unternehmen das Risiko solcher Vorfälle drastisch verringern und so langfristig Kosten sparen.

6. Einfache Umsetzung und breite Unterstützung

SPF ist relativ einfach über einen DNS-Eintrag zu implementieren und wird von modernen E-Mail-Servern weitgehend unterstützt. Dies macht es zu einer kostengünstigen und leicht zugänglichen Maßnahme für Organisationen jeder Größe.

7. Synergie mit anderen E-Mail-Sicherheitsprotokollen

SPF funktioniert gut mit anderen Sicherheitsprotokollen wie DKIM (DomainKeys Identified Mail) und DMARC (Domain-based Message Authentication, Reporting, and Conformance). Zusammen bilden diese Protokolle einen leistungsfähigen Rahmen, um die Sicherheit und Zuverlässigkeit des E-Mail-Verkehrs zu gewährleisten.

8. Schlussfolgerung

Mit der Einführung von SPF legt eine Organisation eine solide Grundlage für ein sichereres und zuverlässigeres E-Mail-System. Dies ist ein erster Schritt zu einem umfassenden Ansatz für die E-Mail-Sicherheit, der nicht nur das Unternehmen selbst, sondern auch seine Kunden, Partner und Interessengruppen schützt.

9. Wie funktioniert der SPF?

9.1 SPF-EINTRAG IM DNS

Ein Domäneninhaber veröffentlicht einen SPF-Eintrag als **TXT-Eintrag** in den DNS-Einstellungen der Domäne. Dieser Eintrag enthält eine Liste der zugelassenen Mailserver (z. B. IP-Adressen, Domänennamen oder Subdomänen).

9.2 VERSENDEN EINER E-MAIL

Wenn eine E-Mail gesendet wird, enthält sie eine **"MAIL FROM"-Adresse** in den SMTP-Kopfzeilen. Dies ist die Adresse, die von SPF kontrolliert wird.

9.3 KONTROLLE DURCH DEN EMPFANGENDEN MAILSERVER

Beim Empfang einer E-Mail prüft der empfangende Mailserver den DNS der Domäne des Absenders, um den SPF-Eintrag abzurufen. Anschließend führt er die folgenden Schritte durch:

- **Extraktion der Absender-IP-Adresse**: Die IP-Adresse des Servers, der die E-Mail versendet hat, wird ermittelt.
- **Abgleich mit SPF-Datensatz**: Die sendende IP-Adresse wird mit der Liste der zugelassenen Server im SPF-Datensatz verglichen.
- **Ergebnis ermitteln**: Der empfangende Server wertet das Ergebnis der SPF-Prüfung aus und trifft eine Entscheidung:
    - **Pass**: Die IP-Adresse des Absenders ist im SPF-Eintrag enthalten. Die E-Mail wird akzeptiert.
    - **Fail**: Die Absender-IP-Adresse ist nicht im SPF-Eintrag enthalten. Der Server markiert die E-Mail möglicherweise als Spam oder weist sie zurück.
    - **Softfail**: Die E-Mail ist nicht vollständig vertrauenswürdig, wird aber nicht zurückgewiesen. Normalerweise als verdächtig markiert.
    - **Neutral**: Keine expliziten Regeln im SPF-Eintrag. Die E-Mail wird normal verarbeitet.
    - **Permerror**: Der SPF-Eintrag ist ungültig oder unlesbar.

10. Erstellung von SPF-Einträgen

SPF-Einträge werden im DNS als TXT-Einträge konfiguriert. Die Syntax umfasst mehrere Mechanismen und Qualifizierer:

10.1 ALLGEMEINER AUFBAU

v=spf1 <Mechanismen> < modifiers >

- v=spf1: Gibt an, dass es sich um einen SPF-Eintrag handelt (obligatorisch).
- <Mechanismen>: Regeln, die bestimmen, welche Server zugelassen sind.
- <modifiers>: optionale Parameter für eine erweiterte Konfiguration.

10.2 HÄUFIG VERWENDETE MECHANISMEN

- ip4:<ip-adresse>: Autorisiert eine bestimmte IPv4-Adresse oder ein Subnetz.
- ip6:<ip-adresse>: Autorisiert eine bestimmte IPv6-Adresse oder ein Subnetz.
- a: Autorisiert die IP-Adresse, die mit dem "A"-Eintrag der Domäne verbunden ist.
- mx: Autorisiert die Mailserver der Domäne (MX-Einträge).
- include:<Domäne>: Erlaubt SPF-Einträge von einer anderen Domäne (nützlich für externe Anbieter wie Google Workspace oder Microsoft 365).
- all: Wird als Terminator verwendet und gibt an, was mit allen nicht übereinstimmenden Adressen geschehen soll (z.B. -all für blockieren).

10.3 BEISPIEL SPF-EINTRAG

Ein SPF-Eintrag für eine Domain, die E-Mails über ihren eigenen Server (IP: 192.0.2.1) und Google Workspace versendet, würde wie folgt aussehen:

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

- ip4:192.0.2.1: Erlaubt eine bestimmte IP-Adresse.
- include:_spf.google.com: Erlaubt E-Mails von durch Google autorisierten Servern.
- -alle: Weist alle anderen E-Mails ab.

11. Schritte zur Umsetzung

11.1 BESTIMMEN SIE DIE SENDENDEN E-MAIL-SERVER

- Identifizieren Sie alle Server oder Provider, die E-Mails im Namen Ihrer Domäne versenden.
- Vergessen Sie nicht externe Anbieter wie Newsletter-Dienste (Mailchimp usw.).

11.2 KONFIGURIEREN SIE DEN SPF-EINTRAG

- Fügen Sie einen neuen TXT-Eintrag in den DNS Ihrer Domäne ein.
- Vergewissern Sie sich, dass der Datensatz alle notwendigen Mechanismen enthält.

11.3 TESTEN SIE DEN SPF-EINTRAG

- Verwenden Sie Online-Tools wie MXToolbox, https://nl.internet.nl/ oder SPF Record Checker, um Ihren SPF-Eintrag zu überprüfen.
- Prüfen Sie, ob der SPF-Eintrag korrekt implementiert ist und von DNS-Servern geparst wird.

11.4 E-MAIL-VERKEHR ÜBERWACHEN

- Überprüfen Sie, ob legitime E-Mails ordnungsgemäß zugestellt werden.
- Verwenden Sie Tools wie DMARC-Berichte, um SPF-Fehlschläge zu verstehen.

12. Beschränkungen von SPF

SPF ist zwar wirksam, hat aber einige Einschränkungen:

- **Probleme bei der Weiterleitung**: SPF schlägt bei der E-Mail-Weiterleitung oft fehl, weil der Weiterleitungsanbieter nicht im ursprünglichen SPF-Eintrag steht.
- **DNS-Abhängigkeit**: Die Empfänger müssen DNS-Abfragen durchführen, die im Falle von Netzwerkproblemen fehlschlagen können.
- **Nur MAIL FROM prüfen**: SPF schützt nur die "MAIL FROM"-Adresse und nicht die "From"-Adresse, die die Benutzer sehen.

13. SPF in Kombination mit anderen Protokollen

SPF funktioniert am besten in Kombination mit anderen E-Mail-Sicherheitsprotokollen:

- **DKIM**: Verifiziert, dass der Inhalt einer E-Mail während der Übertragung nicht verändert wurde.
- **DMARC**: Stellt ein Regelwerk zur Verfügung, um SPF und DKIM zu kombinieren und Missbrauch zu melden.

Haftungsausschluss

DIESER LEITFADEN WURDE VOM ZENTRUM FÜR CYBERSICHERHEIT BELGIEN IN ZUSAMMENARBEIT MIT DNS BELGIUM ERSTELLT. ALLE TEXTE, LAYOUTS, DESIGNS UND ELEMENTE JEGLICHER ART IN DIESEM LEITFADEN SIND URHEBERRECHTLICH GESCHÜTZT. AUSZÜGE AUS DIESEM LEITFADEN DÜRFEN NUR FÜR NICHT-KOMMERZIELLE ZWECKE UNTER ANGABE DER QUELLE VERÖFFENTLICHT WERDEN. DAS ZENTRUM FÜR CYBERSICHERHEIT BELGIEN UND DNS BELGIUM LEHNEN JEDE HAFTUNG FÜR DEN INHALT DIESES LEITFADENS AB. Die bereitgestellten Informationen : - sind nur allgemeiner Natur und gehen nicht auf die spezifische Situation einer natürlichen oder juristischen Person ein. - Sie sind nicht notwendigerweise vollständig, genau oder aktuell. - Sie stellen keine professionelle oder rechtliche Beratung dar. - Sie sind kein Ersatz für eine fachliche Beratung. - Sie garantieren keinen sicheren Schutz.