CENTRE FOR CYBERSECURITY BELGIUM

dnsbelgium

INTÉGRATION ET MISE EN ŒUVRE DU SPF

Contenu

CONTRÔLE ET RÉVISION DES DOCUMENTS

Contrôle des documents	
Auteur	
Propriétaire	
Date de création	
Dernière révision par	
Date de la dernière révision	

.

CONTRÔLE DES VERSIONS

Version	Date d'approbation	Approuvé par	Description du changement

Introduction : pourquoi mettre en œuvre le SPF ?

À une époque où le courrier électronique constitue l'épine dorsale de la communication numérique, il devient de plus en plus important de sécuriser le trafic de courrier électronique. Les cybercriminels exploitent largement les vulnérabilités des protocoles de courrier électronique pour réaliser des opérations de phishing, de spoofing et d'autres formes de fraude par courrier électronique. L'une des méthodes les plus efficaces pour atténuer ces risques est la mise en œuvre du **Sender Policy Framework (SPF)**.

SPF (Sender Policy Framework) est un mécanisme d'authentification du courrier électronique qui permet aux propriétaires de domaines de spécifier les serveurs de messagerie autorisés à envoyer des courriers électroniques au nom de leur domaine. Les serveurs de messagerie récepteurs utilisent ces informations pour vérifier si un courriel entrant est légitime. Pour ce faire, ils interrogent l'enregistrement SPF du domaine de l'expéditeur, qui est stocké dans le système de nom de domaine (DNS). Les principales raisons de la mise en œuvre de SPF sont décrites ci-après.

1. Protection contre l'usurpation d'adresse électronique

L'usurpation d'adresse électronique est une technique par laquelle les attaquants envoient des courriels qui semblent provenir d'un expéditeur de confiance, tel qu'une banque ou une adresse interne de l'entreprise. C'est l'une des méthodes les plus couramment utilisées dans les attaques par hameçonnage. Le SPF aide à prévenir de telles attaques en permettant uniquement aux serveurs autorisés d'envoyer des courriels au nom d'un domaine.

2. Renforcer la réputation de l'entreprise

Une attaque réussie de spoofing peut porter gravement atteinte à la réputation d'une organisation. Les clients et les partenaires qui reçoivent des courriels frauduleux perdent confiance dans la marque. Le SPF contribue à maintenir la fiabilité et l'intégrité des communications de l'entreprise.

3. Améliorer la délivrabilité du courrier électronique

Le SPF permet d'améliorer la distribution des courriels légitimes. Sans SPF, les courriels provenant d'un domaine peuvent être signalés comme suspects et se retrouver dans le dossier spam du destinataire. Grâce au SPF, les courriels ont plus de chances d'être délivrés correctement.

4. Respecter la conformité et la réglementation

Dans de nombreux secteurs, tels que la finance et les soins de santé, il existe des exigences strictes en matière de sécurité des données et de protocoles de communication. Le SPF peut être un élément essentiel d'une politique de sécurité plus large visant à répondre à ces exigences.

5. Économies de coûts

Une attaque réussie de phishing ou de spoofing peut entraîner des pertes financières importantes, telles que des coûts de récupération et des amendes. En mettant en œuvre le SPF, les organisations peuvent réduire considérablement le risque de tels incidents et donc économiser des frais à long terme.

6. Facilité de mise en œuvre et large soutien

Il est relativement facile de mettre en œuvre le SPF par le biais d'un enregistrement DNS et celui-ci est largement pris en charge par les serveurs de messagerie modernes. Il s'agit donc d'une mesure rentable et accessible pour les organisations de toutes tailles.

7. Synergie avec d'autres protocoles de sécurité du courrier électronique

Le SPF fonctionne très bien en combinaison avec d'autres protocoles de sécurité tels que DKIM (DomainKeys Identified Mail) et DMARC (Domain-based Message Authentication, Reporting, and Conformance). Ensemble, ces protocoles forment un cadre puissant pour garantir la sécurité et la fiabilité du trafic de courrier électronique.

8. Conclusion

Une organisation qui met en œuvre le SPF pose les bases solides d'un système de messagerie électronique plus sûr et plus fiable. Il s'agit d'un premier pas vers une approche globale de la sécurité du courrier électronique qui contribue à protéger non seulement l'organisation elle-même, mais aussi ses clients, ses partenaires et ses parties prenantes.

9. Comment fonctionne le SPF ?

9.1 ENREGISTREMENT SPF DANS LE DNS

Le propriétaire d'un domaine publie un enregistrement SPF sous forme d'**enregistrement TXT** dans les paramètres DNS du domaine. Cet enregistrement contient une liste de serveurs de messagerie autorisés (adresses IP, noms de domaine ou sous-domaines par exemple).

9.2 ENVOI D'UN COURRIER ÉLECTRONIQUE

Lorsqu'un courrier électronique est envoyé, il contient une **adresse "MAIL FROM"** dans les en-têtes SMTP. C'est cette adresse que contrôle le SPF.

9.3 CONTRÔLE PAR LE SERVEUR DE MESSAGERIE DESTINATAIRE

Lors de la réception d'un courriel, le serveur de messagerie destinataire vérifie le DNS du domaine de l'expéditeur pour récupérer l'enregistrement SPF. Il effectue ensuite les opérations suivantes :

- **Extraction de l'adresse IP d'envoi** : L'adresse IP du serveur qui a envoyé l'e-mail est déterminée.
- **Comparaison avec l'enregistrement SPF** : l'adresse IP d'envoi est comparée à la liste des serveurs autorisés dans l'enregistrement SPF.
- **Déterminer le résultat** : le serveur destinataire évalue le résultat du contrôle SPF et prend une décision:
    - **Réussite (Pass)** : l'adresse IP d'envoi figure dans l'enregistrement SPF. L'e-mail est accepté.
    - **Échec (Fail)** : l'adresse IP d'envoi ne figure pas dans l'enregistrement SPF. Le serveur peut marquer l'e-mail comme spam ou le rejeter.
    - **Échec partiel (Softfail)**: le courriel n'est pas totalement fiable, mais n'est pas rejeté. Il est généralement considéré comme suspect.
    - **Neutre** : aucune règle explicite dans l'enregistrement SPF. L'e-mail est traité normalement.
    - **Erreur permanente (PermError)** : L'enregistrement SPF est invalide ou illisible.

10. Création d'enregistrements SPF

Les enregistrements SPF sont configurés comme des enregistrements TXT dans le DNS. La syntaxe comprend plusieurs mécanismes et qualificatifs :

10.1 STRUCTURE GÉNÉRALE

v=spf1 <mécanismes> <modifiers>

- v=spf1 : indique qu'il s'agit d'un enregistrement SPF (obligatoire).
- <mécanismes> : règles qui déterminent quels serveurs sont autorisés.
- <modifiers> : paramètres facultatifs pour une configuration plus avancée.

10.2 MÉCANISMES COURAMMENT UTILISÉS

- ip4:<adresse-ip> : autorise une adresse ou un sous-réseau IPv4 spécifique.
- ip6:<adresse-ip> : autorise une adresse ou un sous-réseau IPv6 spécifique.
- a : autorise l'adresse IP associée à l' “enregistrement A” du domaine.
- mx : autorise les serveurs de messagerie du domaine (enregistrements MX).
- include:<domaine> : autorise les enregistrements SPF d'un autre domaine (utile pour les fournisseurs externes tels que Google Workspace ou Microsoft 365).
- all : utilisé comme clôture, indique ce qu'il faut faire avec toutes les adresses non appariées (par exemple -all pour le blocage).

10.3 EXEMPLE D'ENREGISTREMENT SPF

Un enregistrement SPF pour un domaine envoyant du courrier via son propre serveur (IP : 192.0.2.1) et Google Workspace se présenterait comme suit :

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

- ip4:192.0.2.1 : autorise une adresse IP spécifique.
- include:_spf.google.com : permet d'envoyer des courriels à partir de serveurs autorisés par Google.
- -all : rejette tous les autres courriers électroniques.

11. Étapes de la mise en œuvre

11.1 DÉFINITION DES SERVEURS D'ENVOI DE COURRIER ÉLECTRONIQUE

- Identifiez les serveurs ou fournisseurs qui envoient des courriels au nom de votre domaine.
- N'oubliez pas les fournisseurs externes tels que les services de newsletter (Mailchimp, etc.).

11.2 CONFIGURATION DE L'ENREGISTREMENT SPF

- Ajoutez un nouvel enregistrement TXT au DNS de votre domaine.
- Assurez-vous que l'enregistrement contient tous les mécanismes nécessaires.

11.3 TEST DE L'ENREGISTREMENT SPF

- Utilisez des outils en ligne tels que MXToolbox ou SPF Record Checker pour valider votre enregistrement SPF.
- Vérifiez que l'enregistrement SPF est correctement implémenté et analysé par les serveurs DNS.

11.4 SURVEILLANCE DU TRAFIC DE COURRIER ÉLECTRONIQUE

- Vérifiez que les courriels légitimes sont bien acheminés.
- Utilisez des outils tels que les rapports DMARC pour comprendre les échecs de SPF.

12. Limites du SPF

Bien que le FPS soit efficace, il présente certaines limites :

- **Problèmes de transfert** : le SPF échoue souvent dans le cas d'un transfert de courrier électronique parce que le transitaire ne figure pas dans l'enregistrement SPF d'origine.
- **Dépendance au DNS** : les destinataires doivent effectuer des requêtes DNS, qui peuvent échouer en cas de problèmes de réseau.
- **Vérification de l'adresse "MAIL FROM" uniquement** : le SPF ne protège que l'adresse "MAIL FROM" et non l'adresse "From" visible par les utilisateurs.

13. SPF en combinaison avec d'autres protocoles

Le SPF fonctionne de manière optimale en combinaison avec d'autres protocoles de sécurité du courrier électronique :

- **DKIM** : vérifie que le contenu d'un courrier électronique n'a pas été modifié en cours de route.
- **DMARC** : fournit un cadre stratégique pour combiner SPF et DKIM et signaler les abus.

Clause de non-responsabilité

CE GUIDE A ÉTÉ PRÉPARÉ PAR LE CENTRE POUR LA CYBERSÉCURITÉ BELGIQUE EN COLLABORATION AVEC DNS BELGIUM. TOUS LES TEXTES, MISES EN PAGE, DESSINS ET ÉLÉMENTS DE TOUTE NATURE CONTENUS DANS CE GUIDE SONT PROTÉGÉS PAR LE DROIT D'AUTEUR. DES EXTRAITS DE CE GUIDE NE PEUVENT ÊTRE PUBLIÉS QU'À DES FINS NON COMMERCIALES, À CONDITION QUE LA SOURCE SOIT MENTIONNÉE. LE CENTRE POUR LA CYBERSÉCURITÉ BELGIQUE ET DNS BELGIUM DÉCLINENT TOUTE RESPONSABILITÉ QUANT AU CONTENU DE CE GUIDE. Les informations fournies : - Sont de nature générale uniquement et ne traitent pas de la situation spécifique d'une personne physique ou morale. - Ne sont pas nécessairement complètes, exactes ou à jour. - Ne constituent pas un avis professionnel ou juridique. - Ne remplacent pas l'avis d'un expert. - Ne garantissent pas une protection sûre.