# DEFEND & DELIVER

## DMARC

Email authentication for better email security

ONLINE BOOTCAMP


**Shehzad Mirza**

Directeur des Operations

smirza@globalcyberalliance.org

gca-dmarc@globalcyberalliance.org

Traduction FR : **Leo Gonzales**

CEO Devensys / Merox.io

Partenaire GCA

leo.gonzales@devensys.com

# Introduction à SPF et DKIM

# SPF
# (Sender Policy Framework)

# SPF
## Sender Policy Framework

- Défini quels serveurs de messagerie sont autorisés à envoyer des emails pour le nom de domaine de l'organisation
- Utilise le "envelope from" pour determiner le domaine d'envoi (expéditeur dans le header pas le champ "de")
- Enregistrement DNS de type TXT
  - Il ne peut y avoir qu'une seule entrée SPF par domaine (rappel : un sous-domaine est un domaine)

# Enregistrement DNS SPF TXT

- Basique :

  Domaine : <*domaine*> ou @ ou laissé vide

  Valeur : `"v=spf1 mx -all"`

- Complexe :

  Domaine : <*domaine*>

  Valeur : `"v=spf1 mx a:`<*serveurs emails supplémentaires*>
  `include:`<*domaine externe/tiers*> `ip4:`<*adresse IP / Plage*> `-all"`

# Tags SPF

| | |
|---|---|
| v=spf1 | L'enregistrement TXT commence toujours par cela. Il défini la version utilisée de SPF. A date, la version 1 est la seule de disponible. |
| mx | Si mx est présent alors tous les serveurs emails entrants (MXs) du domaine sont aussi autorisés à envoyer des emails depuis ce domaine. |
| a:<*domaine*> | Cet élément ne doit être présent que s'il y a d'autres systèmes, autres que les serveurs emails, autorisés à envoyer des emails depuis le domaine. |
| include: <*domaine externe*> | Tout ce qui est considéré comme légitime par un domaine externe de confiance sera légitime pour le domaine de l'organisation. |
| ipv4:<IP/Plage><br>ipv6:<IP/Plage> | Pour définir si ce sont des adresses IP (ou plages). |

# Tags SPF (suite)

**ptr**

- Utilise le PTR (pointeur) de l'adresse IP source et une requete "reverse"

**exists**

- L'existence (tout enregistrement A valide) du domaine spécifié permet au test de "passer«

**redirect**

- Redirige la vérification pour utiliser les enregistrements SPF du domaine spécifié

**exp**

- Définit une entrée DNS (TXT) dont le texte de l'enregistrement peut être retourné avec le message d'échec (exp = explaination)
- Doit être mis à la fin de la politique

**Macro-expressions** - complexe et déroutant

# Tag SPF *“all”*

- **-all – Hard Fail / échec “fort”**
  - seuls les serveurs de messagerie du domaine (et ceux de ‘A’ et 'include') sont autorisés à envoyer du courrier pour le domaine. Les autres sont interdits.
- **~all – Soft Fail / échec “léger”**
  - Si l’email provient d’un serveur/hote qui ne se trouve pas dans la politique, le message est accepté mais marqué comme non conforme.
- **?all**
  - Précise « explicitement » que rien ne peut être dit sur la validité.
- **+all**
  - signifie que n’importe quel serveur/hôte peut envoyer du courrier pour le domaine. **Ne doit jamais être utilisé.**

# Exemples d’enregistrements SPF

- v=spf1 mx include:_spf.google.com -all
- v=spf1 mx include:spf.protection.outlook.com –all
- v=spf1 include:spf.protection.outlook.com ip4:161.11.10.20 –all

# Eléments nécessaires pour SPF

- Accès au DNS public de l'organisation
- Déterminer si les enregistrements MX sont utilisés
- Adresse IP ou domaines des systèmes émetteurs pour le compte de (en tant que) l'organisation
- Si les fournisseurs tiers supportent SPF
  - Bien verifier ce qu'ils préconisent
- Confirmer l'alignement SPF (s'assurer que le domaine d'envoie utilise le domaine de l'organisation)

# Alignement SPF

**Bon :**

From: info@globalcyberalliance.org

Return-Path: <info@globalcyberalliance.org>

Received-SPF: pass (google.com: domain of info@globalcyberalliance.org designates 2607:f8b0:4864:20::d34 as permitted sender) client-ip=2607:f8b0:4864:20::d34;

**Echec** :

From: info@globalcyberalliance.org

Return-Path: < bounce-mc.us15_71628198.660451-8bd9e9bfe7@mail58.atl11.rsgsv.net >

Received-SPF: pass (google.com: domain of bounce-mc.us15_71628198.660451-8bd9e9bfe7@mail58.atl11.rsgsv.net designates 205.201.133.58 as permitted sender) client-ip=205.201.133.58;

**Pour atteindre un alignment SPF à “pass”, le domaine du header ”From:” doit correspondre au domaine utilisé pour l’authentification SPF (par ex., enveloppe “mail from:” domaine “return-path).**

# Alignement SPF

| SPF DMARC | SPF pure | SPF Domaine |
|---|---|---|
| non aligné | bon | mail95.suw111.mcdlv.net |
| non aligné | bon | mail95.suw111.mcdlv.net |

| SPF DMARC | SPF pure | SPF Domaine |
|---|---|---|
| aligné | bon | globalcyberalliance.org |
| aligné | bon | globalcyberalliance.org |
| aligné | bon | globalcyberalliance.org |
| aligné | bon | globalcyberalliance.org |
| aligné | bon | globalcyberalliance.org |
| aligné | bon | globalcyberalliance.org |
| aligné | bon | globalcyberalliance.org |
| aligné | bon | globalcyberalliance.org |
| aligné | bon | globalcyberalliance.org |
| aligné | bon | globalcyberalliance.org |

# Lacunes

- Le serveur du destinataire doit décider lui-même comment traiter les messages en échecs
- Une fois implémenté, il n’existe aucun mécanisme permettant de déterminer si le message a été « rejeté » ou « bounced »
- Utilisé seul, tout autre domaine utilisant le même hébergeur/hébergement peut falsifier le courrier d’autres domaines
- Limite de « recherche » à 10x lookups (domaines)
- Ne valide pas le “header from”, mais utilise le “envelope from” pour determiner le domaine d’envoi

# Paliatif à la limite des 10x lookups

- Aplatissement SPF (flattening)
  - Utiliser l'adresse IP à la place du nom de domaine
  - Soyez extrêmement prudent
- SPF dynamique
  - Possibilité offerte par divers éditeurs de solutions DMARC
  - Utilisation de macros
- Sous-domaines dédiés aux flux d'e-mails
- Limiter les "include" non nécessaires

# SPF 2.0

- Ce n'est pas Sender Policy Framework
- **C’est Sender ID**
  - c'est un protocole obsolète et indépendant
  - conçu pour améliorer SPF
- Différence
  - Ce qui est en cours de validation
    - SPF 2.0 vérifie PRA et / ou MFROM
    - SPF vérifie les identités MAIL FROM et HELO
  - chacun fonctionne sur différentes «couches» du système de messagerie

# DomainKeys Identified Mail (DKIM)

# DKIM
## DomainKeys Identified Mail

Valide l’identité d’un domaine associée à un email à l’aide d’une authentification sous la forme d’une signature numérique

Enregistrement DNS de type TXT ou CNAME

- Peut avoir plus d’un enregistrement

# Générer les clés DKIM

- Deux clés
  - Clé privée
  - Clé publique
- La génération de clés dépend :
  - Si vous utilisez un service externe pour vos emails et DNS (ex. Google G.Suite ou Microsoft Office 365)
  - Si l'organisation dispose de son propre serveur de messagerie ou passerelle

# DKIM avec des fournisseurs de messagerie tiers et systèmes marketing

- Le fournisseur de messagerie vous fournira la clé publique. Cette clé publique est ensuite publiée sous la forme d'un enregistrement TXT ou CNAME dans vos DNS.
  - Dans certains cas, le fournisseur de messagerie fournira l'enregistrement TXT DNS complet.
- La clé privée est détenue par le fournisseur de messagerie et n'est généralement pas fournie à l'organisation (vous).

# DKIM avec les passerelles ou les serveurs de messagerie des organisations

- Certaines passerelles de messagerie généreront les clés DKIM (ex., Cisco Ironport, Mimecast…).
- Linux - un projet open source appelé **opendkim** (http://www.opendkim.org/) est disponible.
    - Contient divers outils pour aider à créer la clé DKIM et à intégrer la signature DKIM dans divers systèmes de messagerie
- MS Exchange – dkim-exchange (github)
- Une autre option consiste à utiliser OpenSSL pour générer les clés DKIM.
    - Clé privée: **openssl genrsa -out dkim-private.pem 1024 -outform PEM**
    - Clé publique: **openssl rsa -in dkim-private.pem -out dkim-public.pem -pubout -outform PEM**
- Déplacez la clé privée DKIM dans l'emplacement spécifié par l'installation DKIM.
    - **Assurez-vous qu'il se trouve dans un dossier avec accès restreint.**

# Enregistrement DKIM DNS TXT

**Nom :** <selector>._domainkey.<*domaine*>

**Valeur =** "k=rsa;
p=MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhAKJ2lzDLZ8XlVambQfMXn
3LRGKOD5o6l;"

# DKIM Record Name

- **<selector>**
  - nom de la clé DKIM dans les DNS. N'importe quel nom peut être utilisé avant le « . », cependant il doit y avoir « _domainkey » après.

- **_domainkey - Obligatoire**

- **<*domaine*> -** peut ne pas être nécessaire

# Tags DKIM

- **k=rsa** – définit l'algorithme utilisé
- **p=<clé du fichier de clé publique généré précédemment>** – définit la « string » de la clé publique
  - 1024 – taille la plus commune
  - 2048*

# Eléments nécessaires pour DKIM

- Accès au DNS public
- Définir le sélecteur
- Générateur de clés DKIM et outil de signature
  - Intégré au serveur de messagerie ou à la passerelle de sécurité de messagerie
  - Fourni par le fournisseur de messagerie tiers
- Si les fournisseurs tiers supportent DKIM
  - Ce qui doit être ajouté au DNS (enregistrement TXT ou CNAME)
- Vérifier l'alignement DKIM (assurez-vous que le serveur de signature utilise le domaine de l'organisation)

# Alignement DKIM

En-tête de message:

De: info@globalcyberalliance.org

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=globalcyberalliance.org; s=gca; h=mime-version:references:in-reply-to:from:date:message-id:subject:to:cc;

| DKIM DMARC | DKIM pure | DKIM d= |
|---|---|---|
| aligné | bon | globalcyberalliance.org |
| non aligné | bon | mail9.mcsignup.com |
| aligné | bon | globalcyberalliance.org |
| aligné | bon | globalcyberalliance.org |
| aligné | bon | globalcyberalliance.org |
| non aligné | bon | mail13.mcsignup.com |
| non aligné | bon | mail8.mcsignup.com |
| non aligné | bon | gmail.mctxapp.net |
| non aligné | bon | mail10.mcsignup.com |
| non aligné | bon | gmail.mctxapp.net |

# Lacunes

- Ne définit PAS ce qu'il faut faire si la « signature » est bonne/echec
- Pas de mécanisme de reporting
- Ne détermine PAS si le serveur expéditeur est autorisé à envoyer du courrier sortant pour (en tant que) un domaine spécifique
- Laisse aux filtres du destinataire la détermination de l'authenticité du message envoyé
  - Le serveur du destinataire doit decider quoi faire des messages en échec

# DMARC

**D**omain-based **M**essage
**A**uthentication, **R**eporting, & **C**onformance

≈ “Authentification, Reporting et Conformité” basés sur le domaine

Politique qui va définir SPF et DKIM (le A ou Authentication dans DM**A**RC) et doit travailler de pair avec le niveau de politique définit par votre organisation (le C de Conformance dans DMAR**C**), en plus d’ajouter une fonctionnalité de reporting (le R ou Reporting dans DMA**R**C).

Utilise le serveur DNS pour définir la politique.

# DMARC avec SPF et DKIM

- Corrige/résout la plupart des problèmes de SPF et DKIM
- Domains using the same hosting provider or coming from org mail servers – Implement SPF and DKIM
  - DMARC will utilize SPF and DKIM checking
- Rapports DMARC
- Le DMARC va indiquer quoi faire avec le message si l'un ou l'autre "échoue" ou "passe" (fail / pass)

# Ressources “Bootcamp”

- Forum de communautaire : community.globalcyberalliance.org
- Page de ressources : dmarc.globalcyberalliance.org/dmarc-bootcamp/

GLOBAL CYBER ALLIANCE

merox
BY DEVENSYS CYBERSECURITY

# Questions / Réponses

# Merci !

**Shehzad Mirza**

Directeur des Operations

smirza@globalcyberalliance.org

gca-dmarc@globalcyberalliance.org

Traduction FR : **Leo Gonzales**

CEO Devensys / Merox.io

Partenaire GCA

leo.gonzales@devensys.com