DMARC 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

C’est quoi DMARC?

Une politique DMARC permet à un émetteur d’indiquer
que ses messages sont protégés, et dit au destinataire
quoi faire si l’une des méthodes d’authentification « passe »
ou « échoue » (comme laisser passer le message
le mettre en spam, le rejeter).

Elements necessaires pour l'implémentation

- Connaitre le(s) système(s)/serveur(s) emails utilisé(s) par l'organisation
- Accès admin aux DNS de l'organisation
- Liste des sous-domaines (le cas échéant)
- SPF et DKIM (si disponible)

Enregistrement DMARC DNS TXT

- Basique :

  Domaine : `_dmarc`

  Valeur : `v=DMARC1; p=none; rua=mailto:<adresse email>; ruf=mailto:<adresse email>;`

- Complexe :

  Domaine : `_dmarc`

  Valeur : `v=DMARC1; p=none; rua=mailto:<adresse email>; ruf=mailto:<adresse email>; fo=1; adkim=r; aspf=r; pct=100; rf=afrf; ri=86400; sp=reject;`

Que signifient chaque “tag” ?

Obligatoire :

- v=DMARC1 - version
- p= - niveau de la politique
- rua= - rapports agrégés

Recommandé :

- ruf= - rapports forensiques/echecs

Envisager d’utiliser

sp= - sub-domain policy

Tags optionnels :

- fo= envoie des extraits des emails qui ont échoué soit SPF et/ou DKIM
- adkim= Mode d’alignement pour DKIM
- aspf= Mode d’alignement pour SPF
- pct= - % des messages concernés
- rf= - format des rapports
- ri= - intervalle de reporting

Détails des Tag DMARC
p=

Défini le niveau de la politique (stratégie) DMARC

“v=DMARC1; p=none;”

“v=DMARC1; p=quarantine;”

“v=DMARC1; p=reject;”

DMARC

Qu’advient-il des messages?

- Dépend du paramètre de la politique (stratégie) :
  - **None** – (~aucune) signale les messages suspects ; mais tout le courrier est tout de même envoyé (transmis) dans la boîte de réception
  - **Quarantine** – (~quarantaine) échec SPF/DKIM et alignement ; le message est envoyé (transmis) dans le dossier spam/indésirable
  - **Reject** – (~rejeter) échec SPF/DKIM et alignement, le message est « dropped » (supprimé), donc non transmis du tout
- La recommandation consiste à commencer par « None » et à passer progressivement à « Reject »

Détails des Tag DMARC (suite)
rua & ruf

rua – rapports agrégés

ruf – rapports forensique/echec

“v=DMARC1; p=none; rua=mailto:<adresse email>; ruf=mailto:<adresse email>;”

Exemples :

“v=DMARC1; p=none; rua=mailto:**dmarc-rua**@company.com; ruf=mailto:**dmarc-ruf**@company.com;”

“v=DMARC1; p=none; rua=mailto:**dmarc-rua**@company.com, mailto:admin@company.com; ruf=mailto:**dmarc-ruf**@company.com;”

Détails des Tag DMARC (suite)
fo

Optionnel – utilisé pour les rapports forensique/échecs

• envoie des extraits des emails qui ont échoué soit SPF et/ou DKIM

“v=DMARC1; p=none; rua=mailto:<adresse email>; ruf=mailto:<adresse email>; fo=<0,1d,s>”

0 - **(défaut) -** Générer un rapport si tous les mécanismes d’authentification sous-jacents ne produisent pas un résultat "passe" aligné.

1 - Générer un rapport si un mécanisme d’authentification sous-jacent produit autre chose qu’un résultat "passe" aligné.

d - Générer un rapport d’échec DKIM si le message a une signature qui a échoué à l’évaluation, quel que soit son alignement.

s - Générer un rapport d’échec SPF si le message a échoué à l’évaluation SPF, quel que soit son alignement.

Détails des Tag DMARC (suite)
adkim & aspf

Optionnel – définit le mode d'alignement pour DKIM et SPF

"v=DMARC1; p=none; rua=mailto:<adresse email>;
ruf=mailto:<adresse email>; fo=1; adkim=<s,r>; aspf=<s,r>"

s = alignment "strict"

r = alignment "relaxé" **(défaut)**

Détails des Tag DMARC (suite)
rf & ri

Optionnel

"v=DMARC1; p=none; rua=mailto:<addresse email>; ruf=mailto:<addresse email>; fo=1; adkim=r; aspf=r; rf=<afrf>; ri=<seconds>"

rf – format des rapports

- afrf **(default)** – Abuse Report Format (RFC 5965)
- iodef – Incident Object Description Exchange Format (RFC 5070)

ri – intervale de reporting en secondes

- 84600 (24 heures) par défaut

Détails des Tag DMARC (suite)
pct

Optionnel

“v=DMARC1; p=none; rua=mailto:<adresse email>; ruf=mailto:<adresse email>; fo=1; adkim=r; aspf=r; rf=afrf; ri=84600; pct=<0-100>”

- Valeur = 0-100 (100 par défaut)
- Si vous faites ‘p=quarantine; pct=0;’ c’est comme p=none
- Si vous faites ‘p=reject; pct=0;’ c’est comme p=quarantine

Détails des Tag DMARC (suite)
sp

Optionnel, mais devrait être utilisé dans l'idéal

"v=DMARC1; p=none; rua=mailto:<adresse email>; ruf=mailto:<adresse email>; fo=1; adkim=r; aspf=r; rf=afrf; ri=86400; sp=<niveau de la politique/stratégie>;"

- Mêmes niveaux de politique/stratégie que p=, mais s'applique à tous les sous-domaines
  - Si non défini, défaut à 'p='.
- Quand l'utiliser :
  - Pas de sous-domaine et encore à p=none. Implémenter sp=reject
  - De multiples sous-domaines et prêt à basculer le domaine principal (top level) à p=reject ou p=quarantine. Implémenter sp=none

Enregistrement DMARC DNS TXT

- Simple :

  Domaine : _dmarc

  Valeur : v=DMARC1; p=none; rua=mailto:*<adresse email>*; ruf=mailto:*<adresse email>;*

- Complexe :

  Domaine : _dmarc

  Valeur : v=DMARC1; p=none; rua=mailto:*<adresse email>*; ruf=mailto:*<adresse email>*; fo=1; adkim=r; aspf=r; pct=100; rf=afrf; ri=86400; sp=reject;

Demonstration :

Créer les enregistrements DNS

Prochaines étapes

Allez-y, et implémentez DMARC
à p=none pour votre organisation.

Domaine : _dmarc
Valeur : “v=DMARC1; p=none;
rua=mailto:<*adresse email*>;
ruf=mailto:<*adresse email*>;”

Posez des questions au besoin - email ou forum (community.globalcyberalliance.org), ou n’hésitez pas à programmer une conférence téléphonique avec nous pour avancer étape par étape.

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