CENTRE FOR CYBERSECURITY BELGIUM

dnsbelgium

INTÉGRATION ET MISE EN ŒUVRE DE DMARC

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
1.0			

Introduction : pourquoi mettre en œuvre DMARC ?

Dans le monde numérique d'aujourd'hui, le courrier électronique est un moyen de communication essentiel, tant au sein des organisations qu'avec les clients et les partenaires. Parallèlement, le courrier électronique est l'un des vecteurs d'attaque les plus utilisés par les cybercriminels, qui recourent à des techniques telles que l'hameçonnage, l'usurpation d'identité et la fraude pour voler des données confidentielles ou causer des dommages aux organisations.

Pour faire face efficacement à ces risques, la mise en œuvre de **DMARC** est une étape cruciale. DMARC est un protocole d'authentification du courrier électronique qui permet aux organisations de protéger l'identité de l'expéditeur de leurs courriers électroniques, d'empêcher l'utilisation abusive de domaines et d'assurer la transparence du trafic de courrier électronique par l'établissement de rapports. Il s'appuie sur des protocoles existants tels que le SPF (Sender Policy Framework) et le DKIM (DomainKeys Identified Mail) et ajoute une couche supplémentaire de contrôle et de gestion.

Voici les principales raisons pour lesquelles DMARC est un élément essentiel d'une politique solide de sécurité du courrier électronique :

1. Protection contre l'usurpation d'adresse électronique

DMARC constitue un puissant moyen de défense contre l'usurpation d'adresse électronique, une technique par laquelle les attaquants envoient des courriels qui semblent provenir d'un expéditeur légitime. En exigeant que les courriels soient validés à la fois par le SPF et DKIM et en appliquant des politiques de rejet (telles que la mise en quarantaine ou le blocage), DMARC empêche les courriels frauduleux d'être délivrés aux destinataires.

2. Amélioration de la réputation du courrier électronique

L'utilisation abusive d'un domaine à des fins d'hameçonnage ou de spam peut nuire à la réputation de l'entreprise et augmenter la probabilité que des courriels légitimes soient marqués comme étant des spams. DMARC aide les organisations à protéger la réputation de leur courrier électronique en empêchant les parties non autorisées d'abuser de leur domaine.

3. Renforcement de la confiance des clients

La fraude par courrier électronique peut entraîner une perte de confiance chez les clients et les partenaires, en particulier s'ils sont victimes d'attaques par usurpation d'identité qui détournent le nom de l'entreprise. En mettant en œuvre DMARC, une organisation démontre qu'elle prend des mesures proactives pour protéger ses clients et ses partenaires contre les cybermenaces.

4. Compréhension du trafic de courrier électronique et des menaces

L'un des avantages uniques de DMARC est son mécanisme de rapport. En activant le rapport DMARC, les organisations peuvent obtenir des informations sur :

- quels sont les serveurs qui envoient des courriels au nom de leur domaine.
- la fréquence de réussite ou d'échec des vérifications SPF et DKIM.
- les tentatives d'utilisation abusive du domaine par des parties non autorisées.

Ces informations sont précieuses pour détecter les incidents de sécurité et optimiser l'infrastructure de messagerie.

5. Respect des exigences légales et sectorielles

Dans certains secteurs, tels que la finance et les soins de santé, les exigences en matière de sécurité et de confidentialité des données sont très strictes. DMARC peut aider à respecter des réglementations telles que GDPR, PCI DSS et NIS2 en garantissant des communications par courrier électronique plus sûres.

6. Amélioration de la délivrabilité du courrier électronique

En mettant en œuvre DMARC, les organisations peuvent augmenter les chances que les courriels légitimes soient délivrés correctement. Lorsque les destinataires se fient à l'authenticité des courriels provenant d'un domaine, ils réduisent les risques que les courriels soient marqués comme étant du spam.

7. Économies de coûts

Les conséquences d'une attaque par hameçonnage ou d'une fraude par courrier électronique peuvent être énormes, tant sur le plan financier que sur le plan opérationnel. Ils comprennent notamment les coûts de réponse aux incidents, du rétablissement de la réputation, des amendes légales et de la perte de confiance des clients. DMARC contribue à atténuer ces risques et constitue un moyen rentable de prendre des mesures de sécurité proactives.

8. Protection des marques et de la propriété intellectuelle

L'une des plus grandes menaces pour les entreprises est l'utilisation abusive du nom de leur marque dans des courriels frauduleux ou de phishing. Cela peut entraîner une perte de confiance de la part des clients et des atteintes à la propriété intellectuelle. DMARC protège les marques en empêchant les tiers d'utiliser illégalement le domaine d'une entreprise.

9. Synergie avec d'autres protocoles

DMARC fonctionne avec d'autres protocoles de sécurité du courrier électronique tels que le SPF et DKIM. Alors que le SPF et DKIM assurent l'authentification technique des courriers électroniques, DMARC ajoute une couche de politique et de rapport. Cette combinaison offre une sécurité complète contre les menaces les plus courantes qui pèsent sur le courrier électronique. Par ailleurs, la mise en œuvre de DNSSEC garantit l'intégrité de l'enregistrement DMARC.

10. Mise en œuvre facile grâce à une approche étape par étape

Bien que DMARC puisse à priori sembler complexe, sa mise en œuvre peut être progressive. Les organisations peuvent commencer par une politique "none" (soit n'entreprendre aucune action) pour mieux connaître leurs flux de courrier électronique et passer ensuite à des politiques plus strictes telles que "quarantine" ou "reject". La mise en œuvre est ainsi plus facile à gérer et plus souple.

11. Conclusion

DMARC est un élément essentiel d'une politique solide de sécurité du courrier électronique et offre une protection contre un large éventail de menaces découlant de l'utilisation abusive des domaines de courrier électronique. Outre la prévention de l'usurpation d'identité, il renforce la réputation du courrier électronique, accroît la confiance des clients, permet de mieux comprendre le trafic de courrier électronique et contribue à la conformité aux réglementations.

Avec DMARC, une organisation peut non seulement améliorer sa propre sécurité, mais aussi contribuer à un écosystème internet plus sûr dans son ensemble.

12. Comment fonctionne DMARC ?

DMARC ajoute une couche supplémentaire à SPF et DKIM en assurant trois fonctions principales :

12.1 CONTRÔLE D'AUTHENTIFICATION

Lors de la réception d'un e-mail, le serveur de messagerie de réception vérifie si l'e-mail :

1. est **conforme au SPF** : l'adresse IP d'envoi doit figurer dans l'enregistrement SPF du domaine.
2. est **conforme à DKIM** : la signature numérique du courrier électronique doit être valide.
3. est **aligné** : les valeurs SPF et/ou DKIM doivent correspondre au **domaine "From"** vu par l'utilisateur.

12.2 APPLICATION DE LA POLITIQUE

DMARC permet aux propriétaires de domaines de définir des politiques qui spécifient comment le serveur de réception doit traiter les courriels qui ne sont pas conformes aux règles d'authentification :

- none : pas d'action, uniquement rapport (souvent utilisé dans les tests).
- quarantaine : marque les courriels inauthentiques comme suspects ou les place dans le dossier spam.
- rejet : rejet total des courriels inauthentiques.

12.3 RAPPORTS

DMARC propose deux types de rapports :

1. **Rapports agrégés** : aperçu de tous les courriels envoyés au nom d'un domaine, y compris les résultats des vérifications SPF/DKIM.
2. **Rapports d'échec** (facultatif) : rapports détaillés sur les échecs des tentatives d'authentification.

Ces rapports sont envoyés à l'adresse électronique spécifiée dans l'enregistrement DMARC.

13. Création d'enregistrements DMARC

DMARC est configuré comme un **enregistrement TXT** dans le DNS et a la syntaxe suivante :

v=DMARC1 ; p=<politique> ; rua=mailto:<report-email> ; ruf=mailto:<error-report-email> ; fo=<options> ; sp=<subdomain-policy> ; pct=<pourcentage>

Tags clés :

- **v=DMARC1** : indique qu'il s'agit d'un enregistrement DMARC (obligatoire).
- **p** : règle de politique (none, quarantaie, reject) (obligatoire).

- **rua** : adresse électronique pour les rapports globaux (facultatif).
- **ruf** : adresse électronique pour les rapports d'échec (facultatif).
- **fo** : options d'échec, par exemple 1 (émission d'un rapport pour un échec) ou d (émission d'un rapport pour les erreurs DKIM uniquement).
- **sp** : politique pour les sous-domaines (facultatif).
- **pct** : Pourcentage de courriels auxquels la politique est appliquée (par défaut : 100).

Exemple d'enregistrement DMARC :

v=DMARC1 ; p=rejet ; rua=mailto:dmarc-reports@exemple.fr ; ruf=mailto:dmarc-errors@exemple.fr ; fo=1 ; sp=rejet ; pct=100

- p=reject : rejet des courriels qui ne répondent pas aux critères SPF/DKIM.
- rua : les rapports agrégés sont envoyés à dmarc-reports@voorbeeld.nl.
- ruf : les rapports d'échec sont envoyés à dmarc-errors@voorbeeld.nl.
- fo=1 : envoie un rapport en cas d'erreur unique.
- sp=reject : la même politique s'applique aux sous-domaines.
- pct=100 : applique la politique à 100 % des courriels entrants.

14. Mise en œuvre pas à pas de DMARC

14.1 ANALYSER L'INFRASTRUCTURE DE MESSAGERIE EXISTANTE

- Identifiez tous les systèmes et services qui envoient des courriels au nom de votre domaine (par exemple, les serveurs de messagerie, les outils de marketing, les systèmes de gestion de la relation client).
- Assurez-vous que SPF et DKIM sont correctement paramétrés.

14.2 COMMENCER PAR UNE POLITIQUE "NONE".

Commencez par mettre en œuvre un enregistrement DMARC avec la politique p=none. Cela permet de collecter des données sur les courriels sans réellement prendre de mesures. Utilisez un enregistrement tel que :

v=DMARC1 ; p=none ; rua=mailto:dmarc-reports@exemple.fr

14.3 ANALYSER LES RAPPORTS DMARC

- Utilisez des outils tels que les analyseurs DMARC (par exemple DMARCian ou Valimail) pour comprendre les sources d'envoi et les tentatives d'abus.
- Identifiez les sources non valides et ajustez SPF/DKIM pour les autoriser, si elles sont légitimes.

14.4 PASSER À UNE POLITIQUE DE "QUARANTINE"

Si vous avez confiance dans la configuration, changez la politique en p=quarantine. Les courriels suspects seront ainsi placés dans le dossier spam :

v=DMARC1 ; p=quarantaine ; rua=mailto:dmarc-reports@exemple.fr

14.5 AUGMENTER LA SÉVÉRITÉ À "REJECT"

Une fois que vous êtes sûr que toutes les sources légitimes sont correctement définies, modifiez la politique en p=reject pour bloquer complètement les courriels frauduleux :

v=DMARC1 ; p=reject ; rua=mailto:dmarc-reports@exemple.fr

15. Contrôler et optimiser en permanence

- Continuez à analyser les rapports DMARC pour détecter de nouvelles menaces.
- Ajoutez de nouvelles sources de courrier électronique autorisées aux configurations SPF/DKIM si nécessaire.

16. Avantages techniques de DMARC

- **Sécurité de bout en bout** : DMARC garantit que seules les sources autorisées peuvent envoyer des courriels au nom du domaine.
- **Transparence** : Le mécanisme de rapport fournit une vision en temps réel du trafic de courrier électronique.
- **Protection contre l'usurpation d'identité** : Empêche les attaquants de mener à bien des campagnes d'hameçonnage en utilisant un domaine usurpé.
- **Contrôle des sous-domaines** : Des politiques spécifiques peuvent être appliquées aux sous-domaines à l'aide de la balise sp.

17. Défis communs et solutions

Défi	Solution
Configuration correcte de SPF/DKIM	Vérifiez les enregistrements à l'aide d'outils tels que MXToolbox ou SPF/DKIM validator.
Une mauvaise politique conduit à des courriels bloqués	Commencez toujours par une politique "none" et analysez les rapports avant de passer à des politiques plus strictes.
Complexité liée à la multiplicité des sources de courrier électronique	Conservez une liste détaillée des sources autorisées et utilisez les mécanismes d'inclusion du SPF.

18. Synergie avec d'autres protocoles

DMARC fonctionne en harmonie avec :

- **SPF** : permet de vérifier si l'adresse IP d'envoi est autorisée.
- **DKIM** : vérifie que le contenu de l'e-mail n'a pas été modifié pendant la transmission.
- **BIMI** (Brand Indicators for Message Identification) : Combinez DMARC et BIMI pour afficher les logos des marques dans les clients de messagerie compatibles.
- **DNSSEC :** garantit l'intégrité de l'enregistrement DMARC.

Clause de non-responsabilité