CENTRE FOR CYBERSECURITY BELGIUM

dnsbelgium

INTÉGRATION ET MISE EN ŒUVRE DE DKIM

dnsbelgium

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

.be

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 : la nécessité de la mise en œuvre de DKIM

Le courrier électronique est l'un des canaux de communication les plus utilisés au sein des organisations et joue un rôle crucial dans les processus d'entreprise. Cependant, la commodité et l'accessibilité du courrier électronique en font également une cible populaire pour les cybercriminels. L'hameçonnage, l'usurpation d'identité et d'autres formes de fraude par courrier électronique constituent une menace sérieuse pour la sécurité et la fiabilité du trafic de courrier électronique.
Pour atténuer ces risques et garantir la crédibilité des communications par courrier électronique, il est impératif que les organisations mettent en œuvre de solides mécanismes d'authentification du courrier électronique. L'une des méthodes les plus efficaces est le **DomainKeys Identified Mail (DKIM)**. DKIM est un moyen efficace de garantir l'intégrité et l'authenticité des courriers électroniques sortants, afin de protéger à la fois l'expéditeur et le destinataire.

1. Pourquoi DKIM ?

1.1 ACCROÎTRE LA CONFIANCE DANS LA COMMUNICATION PAR COURRIER ÉLECTRONIQUE

DKIM permet d'établir qu'un courriel provient effectivement de l'expéditeur déclaré. Cela renforce la confiance dans les courriels envoyés depuis votre domaine, ce qui est essentiel pour la communication avec les clients, les partenaires et les parties prenantes internes.

1.2 PROTÉGER CONTRE L'USURPATION D'ADRESSE ÉLECTRONIQUE

Le spoofing est une technique par laquelle les attaquants utilisent une fausse adresse électronique pour établir la confiance et tromper les victimes. Grâce au DKIM, il est plus difficile pour les attaquants d'utiliser des noms de domaine légitimes à mauvais escient, car l'authenticité des courriels peut être validée de manière cryptographique.

1.3 AMÉLIORER LA DÉLIVRABILITÉ DU COURRIER ÉLECTRONIQUE

Les fournisseurs d'accès à Internet (ou ISP) et les fournisseurs de courrier électronique tels que Gmail, Outlook et Yahoo! utilisent la signature DKIM pour déterminer si un courrier électronique doit être considéré comme légitime. Les courriels dépourvus de signature DKIM peuvent être signalés comme suspects et se retrouver dans le dossier spam, même s'ils sont légitimes. La signature DKIM contribue donc à augmenter le taux de distribution.

1.4 S'INSCRIRE DANS UNE STRATÉGIE DE SÉCURITÉ DU COURRIER ÉLECTRONIQUE PLUS LARGE

DKIM fonctionne de manière transparente avec d'autres mécanismes d'authentification du courrier électronique tels que **SPF (Sender Policy Framework)** et **DMARC (Domain-based Message Authentication, Reporting, and Conformance)**. Ensemble, ces technologies forment un système intégré qui permet de lutter contre la fraude par courrier électronique et de réduire le risque de fuite de données.

1.5 CONFORMITÉ ET EXIGENCES LÉGALES

Dans des secteurs tels que les services financiers, les soins de santé et l'administration, les exigences en matière de protection des données et de prévention de la fraude sont de plus en plus strictes. La mise en œuvre de DKIM peut aider à respecter les normes et les réglementations, telles que le **RGPD (Règlement général sur la protection des données)**.

1.6 PROTECTION DE LA RÉPUTATION DE L'ENTREPRISE

Une infrastructure de courrier électronique compromise peut nuire gravement à la réputation d'une organisation. DKIM permet d'éviter que votre nom de domaine soit utilisé à des fins malveillantes, comme l'envoi de courriels d'hameçonnage.

2. Conclusion

Compte tenu de la fréquence et de la complexité croissantes des menaces liées au courrier électronique, la mise en œuvre de DKIM n'est pas un luxe, mais une nécessité. DKIM offre une solution rentable pour garantir la fiabilité du courrier électronique, prévenir la fraude par courrier électronique et améliorer la sécurité globale de votre organisation. Dans le présent document, nous décrirons le fonctionnement technique de DKIM, les avantages de son implémentation et les étapes à suivre pour la mettre en œuvre avec succès au sein de votre organisation. En la mettant en œuvre avec soin et en la contrôlant régulièrement, vous pouvez améliorer de manière significative la sécurité du courrier électronique. Combinée à SPF et DMARC, DKIM constitue une défense solide contre les abus en matière de courrier électronique.

3. DKIM : explication technique et mise en œuvre

3.1. QU'EST-CE QUE DKIM ?

DKIM (DomainKeys Identified Mail) est un mécanisme de vérification des courriers électroniques qui garantit qu'un courrier électronique n'a pas été modifié en cours de route. Il fonctionne en ajoutant une signature numérique à un courrier électronique, qui peut être validée par le serveur de messagerie destinataire.

- **Caractéristiques principales** :
  - Vérification de l'expéditeur
  - Garantie de l'intégrité du contenu du courrier électronique
  - Prévention de la manipulation du courrier électronique en cours de transmission.

3.2. COMMENT FONCTIONNE LA NORME DKIM ?

3.2.1 CONCEPTS CLÉS

1. **Signature numérique** :
   - Le serveur d'envoi génère une signature cryptographique à l'aide d'une clé privée.
   - Cette signature est incluse dans l'en-tête DKIM de l'e-mail.
2. **Clé publique dans le DNS** :
   - La clé publique associée à la clé privée est publiée dans un enregistrement DNS TXT.
   - Les serveurs récepteurs utilisent cette clé publique pour valider la signature.
   - DNSSEC garantit que la consultation du DNS est également authentifiée de manière cryptographique.
3. **Sélecteur** :
   - Un identifiant unique indiquant la clé utilisée pour la signature. Cela permet de gérer plusieurs clés.

3.2.2 FONCTIONNEMENT TECHNIQUE DE DKIM

1. **Génération de signatures** :
   - Le serveur d'envoi sélectionne des parties spécifiques de l'e-mail à signer, par exemple :
     - En-têtes : "From", "To", "Subject".
     - Le corps du message.
   - Un algorithme de hachage (par exemple SHA-256) est utilisé pour créer un hachage des parties sélectionnées.
   - Ce hachage est crypté à l'aide de la clé privée, ce qui donne la signature DKIM.

2. **Ajout de l'en-tête DKIM** :
   - La signature est ajoutée au courrier électronique sous la forme d'un nouvel en-tête. Un en-tête DKIM typique se présente comme suit :

```
DKIM-Signature : v=1 ; a=rsa-sha256 ; c=relaxed/relaxed ; d=example.com ;
s=selector1 ;
h=from:to:subject:date ; bh=base64_body_hash ;
b=base64_signature
```

- **v=1** : version DKIM.
- **a=rsa-sha256** : algorithme de signature.
- **d=example.com** : domaine de l'expéditeur.
- **s=selector1** : sélecteur de la clé publique dans le DNS.
- **h=from:to:subject:date**: en-têtes utilisés lors de la signature.
- **bh=base64_body_hash** : hachage du corps de l'e-mail.
- **b=base64_signature**:sgnaturenumérique.

3. **Validation par le serveur destinataire** :
    - Le serveur de réception récupère la clé publique du domaine via le DNS.
    - Le serveur utilise cette clé publique pour :
        - recalculer le hachage du corps.
        - décoder la signature.
        - comparer les valeurs pour vérifier si l'e-mail est inchangé.

4. Avantages de DKIM

- **Contrôle d'intégrité** : DKIM garantit que le contenu d'un courrier électronique n'a pas été modifié en cours de route.
- **Meilleur filtrage des spams** : de nombreux fournisseurs de services de messagerie électronique accordent un score plus élevé aux courriels vérifiés, ce qui améliore la distribution.
- **Protection de la réputation du domaine** : réduit la probabilité d'une utilisation abusive d'un domaine dans le cadre d'un hameçonnage.

5. Étapes de la mise en œuvre de DKIM

5.1 OFFICE 365

https://learn.microsoft.com/en-us/defender-office-365/email-authentication-dkim-configure

5.2 GCP

https://support.google.com/a/answer/174124?hl=en

6. Bonnes pratiques pour DKIM

1. **Utilisez une cryptographie forte** :
   - Utilisez des clés RSA d'au moins 2048 bits pour assurer une sécurité résistante à l'informatique quantique.
2. **Faites tourner les clés régulièrement** :
   - Prévoyez une rotation annuelle des clés DKIM pour minimiser les risques.
3. **Gérez les sélectionneurs avec soin** :
   - Utilisez des sélecteurs uniques pour les différents environnements (par exemple, prod1, test1) afin de faciliter la gestion.
4. **Combinez avec SPF et DMARC** :
   - À lui seul, DKIM n'offre pas une protection totale contre l'usurpation d'identité. Combinez-le avec SPF et DMARC pour une sécurité complète du courrier électronique.
5. **Vérifiez s'il y a des erreurs de configuration** :
   - Les enregistrements DKIM expirés ou mal configurés peuvent bloquer les courriels. Testez-les régulièrement à l'aide d'outils de contrôle.(https://nl.internet.nl/)

7. Erreurs possibles et solutions

Problème : "No DKIM signature found" (Aucune signature DKIM n'a été trouvée).

- **Cause** : Le serveur de messagerie n'est pas correctement configuré pour signer les e-mails.
- **Solution** : Vérifiez la configuration et assurez-vous que la clé privée utilisée est correcte.

Problème : "DKIM validation failed" (échec de la validation DKIM)

- **Cause** : La clé publique du DNS ne correspond pas à la clé privée.
- **Solution** : Publier la clé publique correcte dans l'enregistrement DNS TXT.

Clause de non-responsabilité