CENTRE FOR CYBERSECURITY BELGIUM

dnsbelgium

INTÉGRATION ET MISE EN ŒUVRE DE DNSSEC.

dnsbelgium

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

.be

Contenu

CONTRÔLE ET RÉVISION DES DOCUMENTS

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

.

CONTRÔLE DES VERSIONS

Version	Date d'approbation	Approuvé par	Description du changement

GLOSSAIRE

Résolveur DNS	Un résolveur DNS est un élément essentiel du système de noms de domaine (DNS). Il s'agit d'un logiciel chargé de traduire les noms de domaine en adresses IP numériques.
Attaques par amplification	Il s'agit d'un type d'attaque par déni de service distribué (DDoS) dans lequel l'attaquant envoie un petit volume de trafic à un serveur ou à un service, qui génère ensuite un volume de trafic beaucoup plus important vers une cible. L'effet de l'attaque est ainsi "amplifié", ce qui permet de submerger la cible sans que l'attaquant n'ait besoin de beaucoup de ressources.

Introduction : pourquoi mettre en œuvre DNSSEC ?

Le système de noms de domaine (DNS) est un élément essentiel de l'internet. Chaque requête en ligne - de l'ouverture d'un site web à l'envoi d'un courrier électronique - commence par une requête DNS. Malheureusement, le DNS n'a pas été conçu à l'origine avec la sécurité comme priorité, ce qui le rend vulnérable à diverses cyberattaques. Le DNSSEC (Domain Name System Security Extensions) remédie à ces lacunes et joue un rôle essentiel en garantissant l'intégrité de l'internet moderne. Voici les principales raisons de mettre en œuvre le DNSSEC :

1. Protection contre les attaques DNS critiques

1.1 PROTECTION CONTRE LES ATTAQUES DE TYPE "MAN-IN-THE-MIDDLE

Dans une attaque de type "man-in-the-middle", un attaquant intercepte les requêtes DNS et modifie les réponses pour induire les utilisateurs en erreur. Avec DNSSEC, les réponses DNS sont validées cryptographiquement, ce qui rend impossible toute manipulation en cours de route.
L'usurpation de DNS, également connue sous le nom d'empoisonnement du cache DNS.

- Cela conduit à :
    - Redirection du trafic : les utilisateurs sont dirigés vers des sites web malveillants sans s'en rendre compte.
    - L'interception de données : Grâce à la redirection, les attaquants peuvent voler des données sensibles telles que les mots de passe et les détails des cartes de crédit.

DNSSEC prévient de telles attaques en fournissant des réponses DNS avec des signatures numériques. Cela permet aux résolveurs de vérifier que les données reçues sont authentiques

1.2 DÉFENSE CONTRE LA FORCE BRUTE SUR DES DOMAINES INEXISTANTS

Les attaques DNS, telles que le "NXDOMAIN flooding", tentent de submerger les résolveurs en demandant des domaines inexistants. Les serveurs DNS effectuant la validation DNSSEC peuvent utiliser les enregistrements NSEC/NSEC3* pour prouver efficacement qu'un domaine n'existe pas sans charge supplémentaire.

2. Renforcer la confiance et la crédibilité

2.1 CONFIANCE ENTRE LES UTILISATEURS

Les utilisateurs veulent être sûrs qu'ils se connectent au véritable site web ou service auquel ils se réfèrent. En mettant en œuvre le DNSSEC, une organisation renforce la crédibilité de son domaine et réduit le risque de fraude. Après tout, un service internet non sécurisé porte atteinte à la réputation et aux finances. C'est important pour les utilisateurs d'internet, car l'internet est de plus en plus utilisé comme plateforme pour stocker des informations précieuses et effectuer des transactions financières. Pensez aux services bancaires en ligne, aux investissements en ligne et aux paiements dans les boutiques en ligne. DNSSEC garantit aux utilisateurs que leur trafic internet arrive au bon endroit.

2.2 CONFORMITÉ JURIDIQUE ET RÉGLEMENTAIRE

Dans certains secteurs, tels que les services financiers, les soins de santé et le gouvernement, les normes de sécurité sont souvent obligatoires. DNSSEC peut aider à répondre aux exigences de conformité, telles que NIS2, en garantissant l'intégrité des requêtes DNS.

*Voir le point 9.3 de ce guide pour plus de détails.

3. Base pour les protocoles de sécurité avancés

DNSSEC est plus qu'une technologie de sécurité autonome. Il fournit une base pour des protocoles de sécurité nouveaux et supplémentaires, tels que :

3.1 DANE (AUTHENTIFICATION DES ENTITÉS NOMMÉES BASÉE SUR LE DNS).

Le DNSSEC permet le DANE, un protocole qui améliore la fiabilité des certificats SSL/TLS. DANE permet à un propriétaire de domaine de capturer une chaîne de certificats TLS spécifique dans des enregistrements signés DNSSEC, ce qui empêche la falsification des certificats.

3.2 AUTHENTIFICATION POUR LE COURRIER ÉLECTRONIQUE (PAR EXEMPLE AVEC LES ENREGISTREMENTS TLSA)

DNSSEC permet aux serveurs de messagerie d'utiliser des enregistrements validés cryptographiquement, ce qui renforce les mécanismes de sécurité tels que MTA-STS et STARTTLS.

3.3 SÉCURITÉ DE L'IDO

Avec la croissance de l'IoT, il y a un besoin urgent de solutions de sécurité légères et évolutives. DNSSEC comble cette lacune en sécurisant les requêtes DNS contre la falsification, ce qui est essentiel pour assurer une communication fiable entre les appareils IoT et leurs serveurs. Par conséquent, DNSSEC fournit une couche de sécurité solide dans les écosystèmes où les méthodes traditionnelles ne sont pas réalisables ou efficaces.

4. Protéger la réputation des entreprises

4.1 PRÉVENIR LES ATTEINTES À LA RÉPUTATION

Une attaque DNS réussie, telle que la redirection d'un site web vers une page frauduleuse, peut porter gravement atteinte à la réputation d'une organisation. Les clients perdent confiance dans la fiabilité de l'entreprise, ce qui entraîne des pertes financières immédiates et une atteinte à la réputation à long terme.

4.2 LIMITER LA RESPONSABILITÉ JURIDIQUE

Les organisations qui ne mettent pas en œuvre des mesures de sécurité telles que le DNSSEC risquent d'être tenues pour responsables en cas de violation de données ou de fraude. En utilisant le DNSSEC, vous réduisez le risque de complications juridiques.

5. Avantages opérationnels

5.1 RENFORCEMENT DES PROCESSUS INFORMATIQUES INTERNES

Le DNSSEC oblige les organisations à obtenir une vue d'ensemble détaillée de leur infrastructure DNS. Cela conduit souvent à l'amélioration des processus internes et des normes de gestion, telles que la gestion et la surveillance des clés.

5.2 COMPATIBILITÉ AVEC LES TECHNOLOGIES MODERNES

Avec de plus en plus d'appareils et d'applications supportant le DNSSEC, le DNSSEC est crucial pour garantir l'authenticité des messages DNS.

6. Protection de l'avenir

6.1 NORMALISATION ATTENDUE

Avec la menace croissante des cyberattaques, il est probable que le DNSSEC devienne un jour une norme obligatoire pour tous les domaines. En procédant à une mise en œuvre précoce, les organisations peuvent prendre une longueur d'avance et minimiser les coûts de migration futurs.

6.2 PRÉPARATION À L'INFORMATIQUE QUANTIQUE

Les algorithmes cryptographiques pris en charge par DNSSEC peuvent être adaptés à des variantes résistantes à l'informatique quantique, ce qui en fait un investissement durable à long terme.

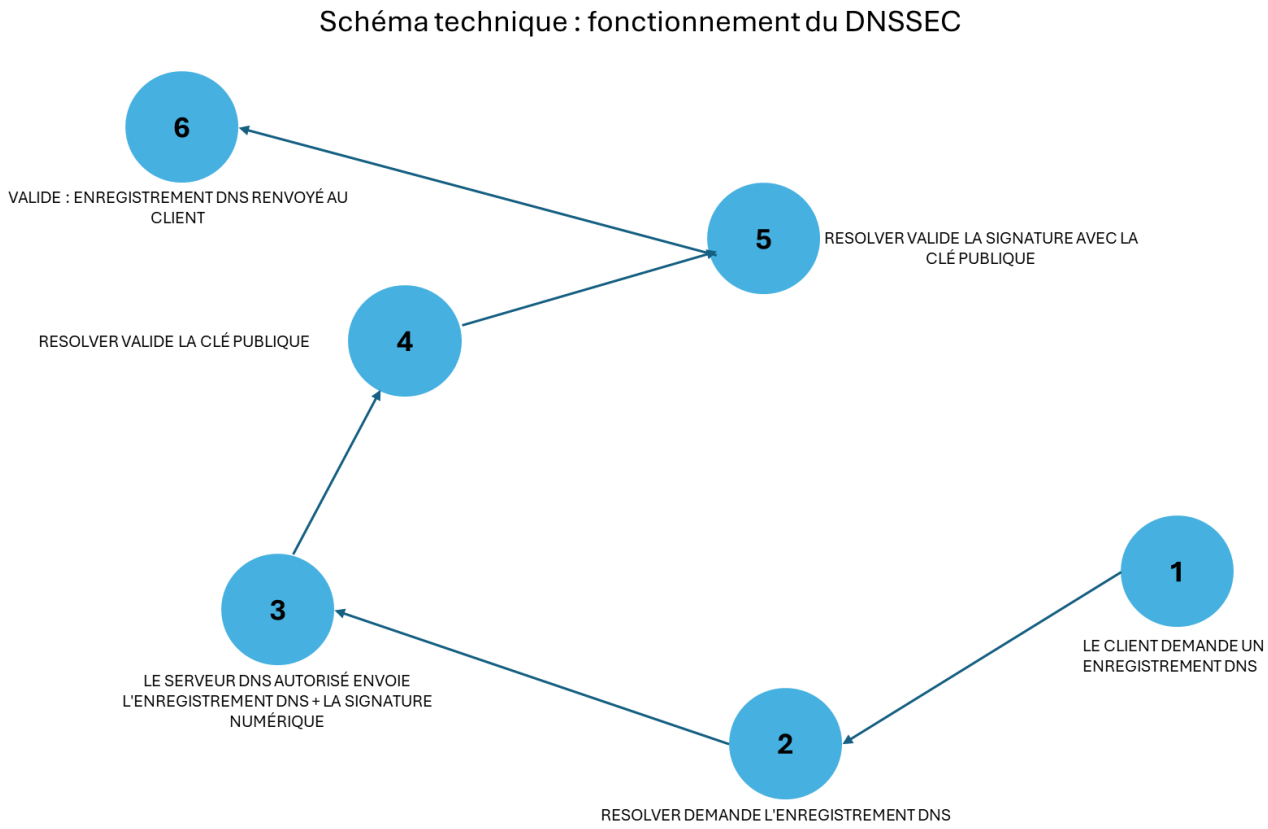
7. Résumé des avantages

Catégorie	Avantages
Sécurité	Protection contre l'usurpation d'identité DNS, l'empoisonnement du cache et les attaques de type "man-in-the-middle".
Confiance	Accroissement de la confiance des utilisateurs, conformité réglementaire
Innovation	Fondation pour des technologies telles que DANE et la sécurité de l'IoT
Réputation	Prévient les dommages causés par les incidents liés au DNS.
Protection de l'avenir	Préparation aux normes futures.

8. Décision

Avec DNSSEC, une organisation investit dans une sécurité robuste et renforce la fiabilité de son domaine. À une époque où les cybermenaces se multiplient, le DNSSEC n'est pas un simple complément aux mesures de sécurité existantes, mais une exigence de base.

9. Comment fonctionne techniquement le DNSSEC ?



9.1 EXPLICATION DU SCHÉMA

1. LE CLIENT DEMANDE UN ENREGISTREMENT DNS

Le **client** (par exemple un navigateur web) envoie une requête à un résolveur DNS pour récupérer les informations relatives à l'adresse IP d'un nom de domaine (par exemple example.com).

- **Rôle du DNSSEC** : aucune sécurité n'est encore appliquée à cette étape ; la demande est une requête DNS standard.

2. LE RÉSOLVEUR DEMANDE UN ENREGISTREMENT DNS

Le résolveur (souvent le serveur DNS d'un fournisseur d'accès) transmet la demande au **serveur DNS faisant autorité** pour le domaine.

- **Rôle de DNSSEC** : Le serveur faisant autorité est configuré avec DNSSEC et sait que l'enregistrement DNS doit être sécurisé.

3. LE SERVEUR DNS FAISANT AUTORITÉ ENVOIE L'ENREGISTREMENT DNS + LA SIGNATURE NUMÉRIQUE

Le serveur DNS faisant autorité renvoie l'enregistrement DNS demandé accompagné d'une **signature numérique** (un enregistrement RRSIG). Cette signature est générée à l'aide d'une clé privée.

- Elle est **importante** :
  - La signature garantit que l'enregistrement DNS est authentique et n'a pas été modifié en cours de route.

- La clé publique nécessaire pour vérifier cette signature est publiée dans un enregistrement DNSKEY.

4. LE RÉSOLVEUR VALIDE LA CLÉ PUBLIQUE

Le résolveur effectue les actions suivantes :

- Le résolveur récupère la **clé publique** correspondante (enregistrement DNSKEY) via DNS.
- Les **enregistrements DS** (Delegation Signer) et la signature correspondante dans la zone parentale (par exemple .be) prouvent que la clé publique est valide.
- Ce processus se répète jusqu'à la **zone racine**, dont la clé publique est déjà considérée comme digne de confiance (l'"ancre de confiance").

- Le résolveur récupère la **clé publique** correspondante (enregistrement DNSKEY) via DNS.

5. LE RÉSOLVEUR VALIDE LA SIGNATURE AVEC LA CLÉ PUBLIQUE

Le résolveur valide la signature reçue. Pour ce faire, le résolveur vérifie si la signature est valide.

6. SI ELLE EST VALIDE : L'ENREGISTREMENT DNS EST RENVOYÉ AU CLIENT

Si toutes les vérifications sont réussies, le résolveur renvoie l'enregistrement DNS original au client.

Si la validation échoue (par exemple en raison d'une incompatibilité de signature), une erreur est renvoyée et le client ne reçoit pas de réponse DNS.

9.2 PRINCIPES DE BASE

DNSSEC fonctionne grâce à un système hiérarchique de signatures numériques et de clés publiques :

1. **Listes et enregistrements de zone** :
   - Les enregistrements DNS sont dotés d'une signature numérique. La signature est générée à l'aide d'une clé privée.
   - La clé publique correspondante est stockée dans un enregistrement DNSKEY dans la même zone.
2. **Validation par une chaîne de confiance** :
   - Pour garantir l'intégrité des réponses DNS, les résolveurs compatibles dnssec valident la signature par rapport à la clé publique.
   - Ce processus remonte hiérarchiquement dans l'arborescence du DNS (par exemple, du domaine → TLD → racine).

9.3 COMPOSANTS TECHNIQUES

1. **Enregistrements DNSKEY** :
   - Contient la clé publique de la zone.
   - Deux types de clés :
     - **ZSK (Zone Signing Key)** : Signe les enregistrements DNS à l'intérieur de la zone.
     - **KSK (Key Signing Key**) : Signe la ZSK pour renforcer la chaîne de confiance.
2. **Enregistrements RRSIG** :
   - Chaque enregistrement DNS d'une zone est associé à un enregistrement RRSIG qui contient la signature numérique.
3. **Enregistrements DS (Delegation Signer**) :
   - Ils sont utilisés pour créer une chaîne de confiance entre une zone enfant et la zone mère (par exemple, entre un domaine et son TLD).
4. **Enregistrements NSEC/NSEC3** :
   - Utilisés pour vérifier cryptographiquement qu'un enregistrement n'existe pas.

- Ils offrent une sécurité contre les attaques par force brute sur des domaines inexistants. (non activé globalement par défaut)
- NSEC affiche le prochain domaine disponible, tandis que NSEC3 utilise le hachage pour une sécurité supplémentaire.

9.4 LE PROCESSUS DE VALIDATION

1. Un résolveur DNS demande les enregistrements DNS d'un domaine.
2. Les enregistrements sont renvoyés avec leurs enregistrements RRSIG.
3. Le résolveur vérifie
   - s'il existe un ou plusieurs enregistrements DNS pour la zone dans le parent
   - si la signature correspond à la clé DNS.
   - si la clé DNSKEY est légitime, en la validant via les enregistrements DS de la zone parente.
   - Pas de DS => PAS de validation
4. Le processus se répète jusqu'à la zone racine, dont la clé publique est connue et sert d'ancre de confiance.

10. Étapes de la mise en œuvre

10.1 PRÉPARATION

1. **Vérifier la prise en charge du DNSSEC** :
   - Assurez-vous que votre fournisseur DNS ou votre logiciel de serveur de noms supporte DNSSEC (par exemple BIND, Knot ou NSD en tant que logiciel DNS faisant autorité et BIND ou Unbound en tant que logiciel de résolution DNS).
2. **Générer des clés** :
   - Créer un KSK et un ZSK à l'aide des outils DNSSEC. Avec BIND, cela peut être fait via la commande :

     dnssec-keygen -a RSASHA256 -f KSK -b 2048 -n ZONE example.com
     dnssec-keygen -a RSASHA256 -b 2048 -n ZONE exemple.com

3. **Publier la clé publique** :
   - Ajoutez les enregistrements DNSKEY à votre fichier de zone DNS.

10.2 CONFIGURATION

1. **Signez la zone** :
   - Utilisez un outil tel que dnssec-signzone pour signer le fichier de zone :

     dnssec-signzone -K /path/to/keydir -o example.com -t example.com.zone

     exemple : Si vous avez stocké les clés dans /etc/dnssec/keys/ et que vous disposez d'un fichier de zone example.com.zone, la commande se présente comme suit :

     dnssec-signzone -K /etc/dnssec/keys/ -o example.com -t example.com.zone

2. **Configurez la zone parentale** :
   - Téléchargez l'enregistrement DS auprès de votre fournisseur de TLD pour former la chaîne de confiance.
3. **Mettez à jour les résolveurs** :
   - Configurez vos résolveurs pour qu'ils utilisent la validation DNSSEC. Pour Unbound, vous pouvez l'activer avec :

server : auto-trust-anchor-file : "/var/lib/unbound/root.key"

10.3 TESTER ET VÉRIFIER L'ÉTAT D'UNE ZONE DNS (DNSVIZ.NET)

VÉRIFIER LA CONFIGURATION AVEC DES OUTILS TELS QUE :

- dnssec-debugger.verisignlabs.com
- dig +dnssec exemple.com

11. Avantages et inconvénients

11.1 AVANTAGES

1. **Protection contre la falsification** :
   - DNSSEC empêche les attaques telles que l'empoisonnement du cache et l'usurpation de DNS.
2. **Fondement d'une sécurité plus poussée** :
   - DNSSEC est une base pour des technologies telles que DANE (par exemple pour la sécurité du courrier électronique via les enregistrements TLSA).
3. **Confiance accrue** :
   - Les utilisateurs et les systèmes peuvent avoir confiance dans l'authenticité des données DNS.

11.2 INCONVÉNIENTS

1. **Complexité** :
   - La gestion des clés et la signature des zones nécessitent une expertise.

2. **Paquets DNS plus volumineux** :
   - Les enregistrements supplémentaires (RRSIG, DNSKEY, NSEC) augmentent la taille des réponses DNS, ce qui peut poser des problèmes avec les systèmes existants.

3. Les attaques par **amplification** peuvent en tirer parti.
   Comment le protocole DNSSEC est spécifiquement utilisé dans les attaques par amplification

   - Réponses élevées dues à DNSSEC :

     - Enregistrements DNSKEY : contiennent les clés publiques et peuvent être très volumineux (en particulier lors de l'utilisation d'une cryptographie forte telle que RSA 2048).
     - Enregistrements RRSIG : signatures numériques pour chaque zone protégée par DNSSEC.
     - Enregistrements NSEC/NSEC3 : jeux d'enregistrements indiquant le nom suivant dans la zone, utilisés pour la protection contre le "zone-walking", mais également de grande taille.

   - Résolveurs ouverts :

     - Les attaquants utilisent des résolveurs ouverts mal configurés, qui acceptent les requêtes DNS de n'importe qui.
     - Ces résolveurs renvoient des réponses à la cible avec des enregistrements DNSSEC volumineux.

   - Facteur d'amplification :

     - Le rapport entre la taille de l'entrée (requête DNS) et de la sortie (réponse DNS) est appelé facteur d'amplification.
     - Avec DNSSEC, ces facteurs d'amplification peuvent atteindre 50 fois ou plus. Par exemple, une requête de 60 octets peut générer une réponse de 3000 octets.

4. **Pas de cryptage** :

- DNSSEC ne protège que l'intégrité et l'authenticité ; les données ne sont pas cryptées.

5. Marche de zone :
   - En raison de NSEC, il est possible que le contenu de la zone soit énuméré. Dans certaines situations, cela n'est pas souhaitable. NSEC3 rend l'énumération des zones beaucoup plus difficile.

12. Meilleures pratiques pour les DNSSEC

1. **Utiliser des algorithmes sûrs** :
   - Choisissez des algorithmes modernes conformément aux recommandations RFC 8624 (par exemple ECDSAP256SHA256.)

2. **Gestion régulière des clés** :
   - Rotation des ZSK tous les 3 à 6 mois et des KSK tous les ans.

3. **Vérifier régulièrement la configuration** :
   - Mettre en place une surveillance active pour vérifier que les signatures et les clés n'ont pas expiré.

4. **Mettre en œuvre des options de repli** :
   - Configurer les résolveurs pour gérer les problèmes de validation DNSSEC sans interruption de service.

13. Coût et maintenance

- **Configuration des DNSSEC** :
  - Configuration initiale : 5 à 15 heures de travail en fonction de la complexité.
  - Maintenance : rotation périodique des clés, mises à jour des fichiers de zone.

- **Indication de coût** :
  - **Petits domaines** : ~100 à 300 € par an.
  - **Grandes organisations** : Coûts supplémentaires pour le personnel, la formation et la surveillance.

Avis de non-responsabilité