CENTRE FOR CYBERSECURITY BELGIUM

dnsbelgium

DNSSEC INTEGRATIE & IMPLEMENTATIE.

dnsbelgium

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

.be

Inhoud

DOCUMENT CONTROL AND REVIEW

Document Control	
Author	
Owner	
Date created	
Last revised by	
Last revision date	

.

VERSION CONTROL

Version	Date of approval	Approved by	Description of change

GLOSSARY

DNS-resolver	Een DNS-resolver is een essentieel onderdeel van het Domain Name System (DNS). Het is software die verantwoordelijk is voor het vertalen van domeinnamen naar numerieke IP-adressen.
Amplification attacks	zijn een type Distributed Denial of Service (DDoS)-aanval waarbij de aanvaller een kleine hoeveelheid verkeer stuurt naar een server of dienst, die vervolgens een veel grotere hoeveelheid verkeer naar een doelwit genereert. Dit resulteert in een "versterking" van het effect van de aanval, waardoor het doelwit overweldigd kan worden zonder dat de aanvaller veel middelen nodig heeft.

Inleiding: Waarom DNSSEC implementeren?

Het Domain Name System (DNS) is een onmisbare kern van het internet. Elk online verzoek—van het openen van een website tot het verzenden van een e-mail—begint met een DNS-query. Helaas is DNS oorspronkelijk niet ontworpen met veiligheid als prioriteit, wat het kwetsbaar maakt voor verschillende cyberaanvallen. DNSSEC (Domain Name System Security Extensions) biedt een oplossing voor deze tekortkomingen en speelt een essentiële rol in het waarborgen van de integriteit van het moderne internet. Hier zijn de belangrijkste redenen om DNSSEC te implementeren:

1. Bescherming tegen kritieke DNS-aanvallen

1.1 BESCHERMING TEGEN MAN-IN-THE-MIDDLE-AANVALLEN

Bij een man-in-the-middle-aanval onderschept een aanvaller DNS-verzoeken en wijzigt de antwoorden om gebruikers te misleiden. Met DNSSEC worden DNS-antwoorden cryptografisch gevalideerd, waardoor manipulatie tijdens het transport onmogelijk wordt.
DNS-spoofing, ook bekend als DNS-cache poisoning,.

- Dit leidt tot:
    - Omleiding van verkeer: Gebruikers worden naar kwaadaardige websites geleid zonder het te beseffen.
    - Data-interceptie: Als gevolg van omleiding, kunnen aanvallers gevoelige gegevens zoals wachtwoorden en creditcardgegevens stelen.

DNSSEC voorkomt dergelijke aanvallen door DNS-antwoorden te voorzien van digitale handtekeningen. Hierdoor kunnen resolvers controleren of de ontvangen data authentiek is

1.2 VERDEDIGING TEGEN BRUTE-FORCE OP NIET-BESTAANDE DOMEINEN

DNS-aanvallen, zoals "NXDOMAIN flooding", proberen resolvers te overweldigen door naar niet-bestaande domeinen te vragen. DNS-servers die DNSSEC-validatie uitvoeren kunnen NSEC/NSEC3-records*gebruiken om efficiënt te bewijzen dat een domein niet bestaat zonder extra belasting.

2. Versterken van vertrouwen en geloofwaardigheid

2.1 VERTROUWEN BIJ GEBRUIKERS

Gebruikers willen zeker weten dat ze verbinding maken met de echte website of service die ze bedoelen. Door DNSSEC te implementeren, versterkt een organisatie de geloofwaardigheid van haar domein en vermindert het risico van fraude. Een onveilige internetdienst levert immers zowel reputatie- als financiële schade op. Dit is belangrijk voor internetgebruikers, dit omdat het internet steeds meer wordt gebruikt als een platform voor de opslag van waardevolle informatie en het uitvoeren van financiële transacties. Denk aan internetbankieren, online beleggen en betalingen bij webshops. DNSSEC is voor de gebruiker een garantie dat zijn internetverkeer op de juiste plaats terecht komt.

2.2 WETTELIJKE EN REGELGEVENDE NALEVING

In bepaalde sectoren, zoals financiële diensten, gezondheidszorg en overheid, zijn beveiligingsstandaarden vaak verplicht. DNSSEC kan helpen bij het voldoen aan compliance-eisen, zoals NIS2 door de integriteit van DNS-verzoeken te waarborgen.

*Zie 9.3 in deze guide voor meer details

3. Basis voor geavanceerde beveiligingsprotocollen

DNSSEC is meer dan een zelfstandige beveiligingstechnologie. Het vormt een fundament voor nieuwe en aanvullende beveiligingsprotocollen, zoals:

3.1 DANE (DNS-BASED AUTHENTICATION OF NAMED ENTITIES)

DNSSEC maakt DANE mogelijk, een protocol dat de betrouwbaarheid van SSL/TLS-certificaten verbetert. Met DANE kan een domeineigenaar een specifieke TLS-certificaatketen vastleggen in DNSSEC-ondertekende records, wat certificaatvervalsing voorkomt.

3.2 AUTHENTICATIE VOOR E-MAIL (BIJVOORBEELD MET TLSA-RECORDS)

Met DNSSEC kunnen mailservers cryptografisch gevalideerde records gebruiken, wat beveiligingsmechanismen zoals MTA-STS en STARTTLS versterkt.

3.3 IOT-BEVEILIGING

Met de groei van IoT is er een dringende behoefte aan lichte, schaalbare beveiligingsoplossingen. DNSSEC vult dit gat door DNS-verzoeken te beveiligen tegen manipulatie, wat essentieel is voor het waarborgen van betrouwbare communicatie tussen IoT-apparaten en hun servers. Hierdoor biedt DNSSEC een robuuste beveiligingslaag in ecosystemen waar traditionele methoden niet haalbaar of effectief zijn.

4. Bescherming van de bedrijfsreputatie

4.1 VOORKOMEN VAN REPUTATIESCHADE

Een succesvolle DNS-aanval, zoals het omleiden van een website naar een frauduleuze pagina, kan ernstige schade toebrengen aan de reputatie van een organisatie. Klanten verliezen vertrouwen in de betrouwbaarheid van het bedrijf, wat leidt tot directe financiële verliezen en lange-termijn imagoschade.

4.2 BEPERKING VAN JURIDISCHE AANSPRAKELIJKHEID

Organisaties die nalaten beveiligingsmaatregelen zoals DNSSEC te implementeren, lopen het risico aansprakelijk te worden gesteld voor datalekken of fraude. Door DNSSEC te gebruiken, verklein je de kans op juridische complicaties.

5. Operationele voordelen

5.1 VERSTERKEN VAN INTERNE IT-PROCESSEN

DNSSEC dwingt organisaties om een gedetailleerd overzicht van hun DNS-infrastructuur te verkrijgen. Dit leidt vaak tot verbeterde interne processen en beheerstandaarden, zoals sleutelbeheer en monitoring.

5.2 COMPATIBILITEIT MET MODERNE TECHNOLOGIEËN

Met steeds meer apparaten en applicaties die DNSSEC ondersteunen, DNSSEC is cruciaal om de authenticiteit van DNS berichten te garanderen.

6. Toekomstbestendigheid

6.1 VERWACHTE STANDAARDISATIE

Met de groeiende dreiging van cyberaanvallen is het waarschijnlijk dat DNSSEC op termijn een verplichte standaard wordt voor alle domeinen. Door vroeg te implementeren, kan een organisatie een voorsprong nemen en toekomstige migratiekosten minimaliseren.

6.2 BEREIDHEID VOOR QUANTUM COMPUTING

De cryptografische algoritmen die DNSSEC ondersteunt kunnen worden aangepast aan quantum-bestendige varianten, waardoor het een duurzame investering is voor de lange termijn.

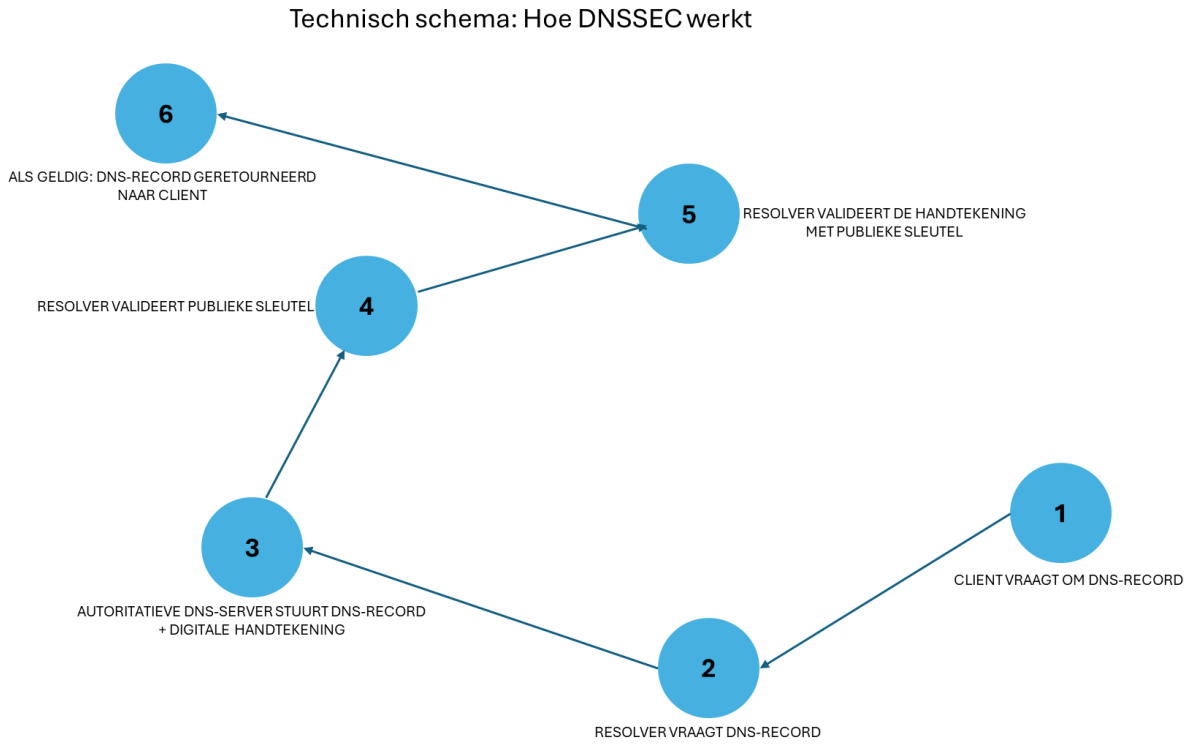
7. Samenvatting van de voordelen

Categorie	Voordelen
Beveiliging	Bescherming tegen DNS-spoofing, cache poisoning en man-in-the-middle-aanvallen
Vertrouwen	Verhoogt vertrouwen bij gebruikers, naleving van regelgeving
Innovatie	Fundament voor technologieën zoals DANE en IoT-beveiliging
Reputatie	Voorkomt schade door DNS-gerelateerde incidenten.
Toekomstbestendigheid	Bereidheid voor toekomstige standaarden.

8. Besluit

Met DNSSEC investeert een organisatie in robuuste beveiliging en versterkt het de betrouwbaarheid van haar domein. In een tijdperk waarin cyberdreigingen toenemen, is DNSSEC niet alleen een aanvulling op bestaande beveiligingsmaatregelen, maar een basisvereiste

9. Hoe werkt DNSSEC technisch?



9.1 DUIDING BIJ HET SCHEMA

1.CLIENT VRAAGT OM DNS-RECORD

De **client** (bijvoorbeeld een webbrowser) stuurt een verzoek naar een DNS-resolver om de IP-adresinformatie van een domeinnaam op te halen (bijvoorbeeld example.com).

- **Rol van DNSSEC**: Nog geen beveiliging toegepast in deze stap; het verzoek is een standaard DNS-query.

2. RESOLVER VRAAGT DNS-RECORD

De resolver (vaak een DNS-server van een internetprovider) stuurt het verzoek door naar de **autoritatieve DNS-server** die verantwoordelijk is voor het domein.

- **Rol van DNSSEC**: De autoritatieve server is geconfigureerd met DNSSEC en weet dat het DNS-record beveiligd moet zijn.

3. AUTORITATIEVE DNS-SERVER STUURT DNS-RECORD + DIGITALE HANDTEKENING

De autoritatieve DNS-server stuurt het opgevraagde DNS-record terug, samen met een **digitale handtekening** (een RRSIG-record). Deze handtekening wordt gegenereerd met behulp van een private sleutel.

- **Belangrijk**:
  - De handtekening garandeert dat het DNS-record authentiek is en niet onderweg is gewijzigd.
  - De publieke sleutel, die nodig is om deze handtekening te controleren, is gepubliceerd in een DNSKEY-record.

4. RESOLVER VALIDEERT PUBLIEKE SLEUTEL

De resolver doet volgende acties:

- De resolver haalt de bijbehorende **publieke sleutel** op (DNSKEY-record) via DNS.
- De **DS-records** (Delegation Signer) en respectievelijke handtekening in de parent-zone (bijvoorbeeld .be) bewijzen dat de publieke sleutel geldig is.
- Dit proces herhaalt zich tot aan de **root-zone**, waarvan de publieke sleutel al als betrouwbaar is vastgelegd (de "trust anchor").

- De resolver haalt de bijbehorende **publieke sleutel** op (DNSKEY-record) via DNS.

5. RESOLVER VALIDEERT DE HANDTEKENING MET PUBLIEKE SLEUTEL

De resolver valideert de ontvangen handtekening. Om dit te doen controleert de resolver of de handtekening geldig is.

6. ALS GELDIG: DNS-RECORD GERETOURNEERD NAAR CLIENT

Als alle controles succesvol zijn, retourneert de resolver het originele DNS-record naar de client.

Als de validatie mislukt (bijvoorbeeld door een mismatch in de handtekening), wordt een fout geretourneerd en ontvangt de client geen DNS-respons

9.2 DE BASISPRINCIPES

DNSSEC werkt door een hiërarchisch systeem van digitale handtekeningen en publieke sleutels:

1. **Zonelijsten en records**:
    - DNS-records worden voorzien van een digitale handtekening. De handtekening wordt gegenereerd met een private sleutel.
    - De bijbehorende publieke sleutel wordt opgeslagen in een DNSKEY-record in dezelfde zone.
2. **Validatie via een keten van vertrouwen**:
    - Om de integriteit van DNS-antwoorden te garanderen, valideren de dnssec enabled resolvers de handtekening tegen de publieke sleutel.
    - Dit proces gaat hiërarchisch omhoog in de DNS-boomstructuur (bijv. van domein → TLD → root).

9.3 TECHNISCHE COMPONENTEN

1. **DNSKEY-records**:
    - Bevat de publieke sleutel van de zone.
    - Twee typen sleutels:
        - **ZSK (Zone Signing Key)**: Ondertekent DNS-records binnen de zone.
        - **KSK (Key Signing Key)**: Ondertekent de ZSK om de keten van vertrouwen te versterken.
2. **RRSIG-records**:
    - Elke DNS-record in een zone heeft een bijbehorend RRSIG-record dat de digitale handtekening bevat.
3. **DS-records (Delegation Signer)**:
    - Worden gebruikt om een keten van vertrouwen te creëren tussen een child-zone en de parent-zone (bijv. tussen een domein en zijn TLD).
4. **NSEC/NSEC3-records**:
    - Wordt gebruikt om cryptografisch te verifieren dat een record niet bestaat.
    - Bieden beveiliging tegen brute-force aanvallen op niet-bestaande domeinen. (niet per default wereldwijd enabled)
    - NSEC toont het volgende beschikbare domein, terwijl NSEC3 hashing gebruikt voor extra veiligheid.

9.4 HET VALIDATIEPROCES

1. Een DNS-resolver vraagt om de DNS-records van een domein.
2. De records worden samen met hun RRSIG-records geretourneerd.
3. De resolver controleert:
    - Of er een of meerdere DS zijn voor de zone in de parent
    - Of de handtekening klopt met de DNSKEY.
    - Of de DNSKEY legitiem is, door deze te valideren via de DS-records in de parent-zone.
    - Geen DS => GEEN validatie
4. Het proces herhaalt zich tot de root-zone, waarvan de publieke sleutel bekend is en als vertrouwd anker dient.

10. Stappen voor implementatie

10.1 VOORBEREIDING

1. **Controleer DNSSEC-ondersteuning**:
    - Zorg ervoor dat je DNS-provider of nameserversoftware DNSSEC ondersteunt (bijv. BIND, Knot of NSD als authoritative DNS software en BIND of Unbound als DNS resolver software).).
2. **Genereer sleutels**:
    - Maak een KSK en ZSK met behulp van DNSSEC-tools. Bij BIND kan dit via het commando:

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

3. **Publiceer de publieke sleutel**:
    - Voeg de DNSKEY-records toe aan je DNS-zonefile.

10.2 CONFIGURATIE

1. **Onderteken de zone**:
    - Gebruik een tool zoals dnssec-signzone om de zonefile te ondertekenen:

      dnssec-signzone -K /pad/naar/keydir -o example.com -t example.com.zone

      voorbeeld: Als je de sleutels hebt opgeslagen in /etc/dnssec/keys/ en een zonebestand example.com.zone hebt, ziet het commando er als volgt uit:

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

2. **Configureer de parent-zone**:
    - Upload het DS-record naar je TLD-provider, zodat de keten van vertrouwen wordt gevormd.
3. **Update resolvers**:
    - Configureer je resolvers om DNSSEC-validatie te gebruiken. Voor Unbound kun je dit inschakelen met:

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

10.3 TEST EN CHECK DE STATUS VAN EEN DNS-ZONE (DNSVIZ.NET)

CONTROLEER DE CONFIGURATIE MET TOOLS ZOALS:

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

11. Voor- en nadelen

11.1 VOORDELEN

1. **Bescherming tegen manipulatie**:
    - DNSSEC voorkomt aanvallen zoals cache poisoning en DNS-spoofing.
2. **Fundament voor verdere beveiliging**:
    - DNSSEC is een basis voor technologieën zoals DANE (bijvoorbeeld voor e-mailbeveiliging via TLSA-records).
3. **Meer vertrouwen**:
    - Gebruikers en systemen kunnen erop vertrouwen dat DNS-data authentiek is.

11.2 NADELEN

1. **Complexiteit**:
    - Sleutelbeheer en zone-ondertekening vereisen expertise.

2. **Grotere DNS-pakketten**:
    - Door extra records (RRSIG, DNSKEY, NSEC) worden DNS-responses groter, wat potentiële problemen met oudere systemen kan veroorzaken.

3. **Amplifications** attacks kunnen hiervan gebruiken maken.
   Hoe DNSSEC specifiek wordt gebruikt in amplification attacks

    - Hoge responses door DNSSEC:

        - DNSKEY-records: Bevat de publieke sleutels en kunnen erg groot zijn (vooral bij gebruik van sterke cryptografie zoals RSA 2048).
        - RRSIG-records: Digitale handtekeningen voor elke DNSSEC-beveiligde zone.
        - NSEC/NSEC3-records: Recordsets die de volgende naam in de zone aangeven, gebruikt voor beveiliging tegen zone-walking, maar ook groot van omvang.

    - Open resolvers:

        - Aanvallers maken gebruik van slecht geconfigureerde open resolvers, die DNS-query's van iedereen accepteren.
        - Deze resolvers sturen antwoorden terug naar het doelwit met de grote DNSSEC-records.

    - Amplification factor:

        - De verhouding tussen de grootte van de input (DNS-query) en de output (DNS-respons) wordt versterkingsfactor genoemd.
        - Bij DNSSEC kunnen deze versterkingsfactoren oplopen tot 50x of meer. Een query van bijvoorbeeld 60 bytes kan een antwoord van 3000 bytes genereren.

4. **Geen encryptie**:
    - DNSSEC beschermt alleen integriteit en authenticiteit; gegevens worden niet versleuteld.
5. Zone walking:
    - Omwille van NSEC bestaat de mogelijkheid dat de content van de zone kan geënumereerd worden. In sommige situaties kan dit niet gewenst zijn. NSEC3 maakt het enumereren van de zone significant moeilijker.

12. Best Practices voor DNSSEC

1. **Gebruik veilige algoritmen**:
   - Kies voor moderne algoritmen conform de aanbevelingen RFC 8624 (e.g. ECDSAP256SHA256.)

2. **Regelmatig sleutelbeheer**:
   - Roteer ZSK's elke 3-6 maanden en KSK's jaarlijks.

3. **Controleer configuratie regelmatig**:
   - Implementeer actieve monitoring om te controleren op verlopen handtekeningen en sleutels.

4. **Implementeer fallback-opties**:
   - Configureer resolvers om problemen met DNSSEC-validatie op te vangen zonder serviceonderbrekingen.

13. Kosten en onderhoud

- **DNSSEC-configuratie**:
  - Initiële configuratie: 5-15 uur werk afhankelijk van complexiteit.
  - Onderhoud: Periodieke rotatie van sleutels, updates aan zonebestanden.

- **Kostenindicatie**:
  - **Kleine domeinen**: ~€100-€300 per jaar.
  - **Grote organisaties**: Extra kosten voor personeel, training en monitoring.

Disclaimer