CENTRE FOR CYBERSECURITY BELGIUM

dnsbelgium

DNSSEC-INTEGRATION UND -IMPLEMENTIERUNG.

dnsbelgium

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

.be

Inhalt

DOKUMENTENKONTROLLE UND ÜBERPRÜFUNG

Kontrolle der Dokumente	
Autor	
Eigentümer	
Datum der Erstellung	
Letzte Überarbeitung durch	
Datum der letzten Überarbeitung	

.

VERSIONSKONTROLLE

Version	Datum der Genehmigung	Genehmigt von	Beschreibung der Änderung

GLOSSAR

DNS-Auflöser	Ein DNS-Resolver ist ein wesentlicher Bestandteil des Domain Name System (DNS). Es handelt sich um eine Software, die für die Übersetzung von Domänennamen in numerische IP-Adressen zuständig ist.
Verstärkungsangriffe	sind eine Art von Distributed Denial of Service (DDoS)-Angriff, bei dem der Angreifer eine kleine Menge an Datenverkehr an einen Server oder Dienst sendet, der dann eine viel größere Menge an Datenverkehr an ein Ziel erzeugt. Dadurch wird die Wirkung des Angriffs "verstärkt", so dass das Ziel überwältigt werden kann, ohne dass der Angreifer viele Ressourcen benötigt.

Einführung: Warum DNSSEC implementieren?

Das Domain Name System (DNS) ist ein unverzichtbares Herzstück des Internets. Jede Online-Anfrage - vom Öffnen einer Website bis zum Senden einer E-Mail - beginnt mit einer DNS-Abfrage. Leider wurde das DNS ursprünglich nicht unter dem Gesichtspunkt der Sicherheit entwickelt, was es anfällig für verschiedene Cyberangriffe macht. DNSSEC (Domain Name System Security Extensions) behebt diese Unzulänglichkeiten und spielt eine wichtige Rolle bei der Gewährleistung der Integrität des modernen Internets. Hier sind die wichtigsten Gründe für die Einführung von DNSSEC:

1. Schutz vor kritischen DNS-Angriffen

1.1 SCHUTZ VOR MAN-IN-THE-MIDDLE-ANGRIFFEN

Bei einem Man-in-the-Middle-Angriff fängt ein Angreifer DNS-Anfragen ab und verändert die Antworten, um die Benutzer in die Irre zu führen. Mit DNSSEC werden DNS-Antworten kryptografisch validiert, was eine Manipulation während der Übertragung unmöglich macht.
DNS-Spoofing, auch bekannt als DNS-Cache-Poisoning,.

- Dies führt zu:
    - Umleitung des Datenverkehrs: Benutzer werden auf bösartige Websites umgeleitet, ohne es zu bemerken.
    - Abfangen von Daten: Durch die Umleitung können Angreifer sensible Daten wie Passwörter und Kreditkartendaten stehlen.

DNSSEC verhindert solche Angriffe, indem DNS-Antworten mit digitalen Signaturen versehen werden. Dadurch können die Resolver überprüfen, ob die empfangenen Daten authentisch sind.

1.2 SCHUTZ VOR BRUTE-FORCE-ANGRIFFEN AUF NICHT EXISTIERENDE DOMÄNEN

DNS-Angriffe wie "NXDOMAIN flooding" versuchen, Resolver zu überfordern, indem sie nach nicht existierenden Domänen fragen. DNS-Server, die eine DNSSEC-Validierung durchführen, können NSEC/NSEC3-Einträge* verwenden, um effizient und ohne zusätzlichen Aufwand zu beweisen, dass eine Domäne nicht existiert.

2. Stärkung von Vertrauen und Glaubwürdigkeit

2.1 VERTRAUEN ZWISCHEN NUTZERN

Die Benutzer wollen sicher sein, dass sie sich mit der echten Website oder dem echten Dienst verbinden, auf den sie sich beziehen. Durch die Einführung von DNSSEC stärkt eine Organisation die Glaubwürdigkeit ihrer Domäne und verringert das Risiko von Betrug. Schließlich schadet ein unsicherer Internetdienst sowohl dem Ruf als auch dem Geldbeutel. Dies ist für Internetnutzer wichtig, da das Internet zunehmend als Plattform für die Speicherung wertvoller Informationen und die Durchführung finanzieller Transaktionen genutzt wird. Man denke an Online-Banking, Online-Investitionen und Zahlungen in Online-Shops. DNSSEC ist eine Garantie für die Nutzer, dass ihr Internetverkehr an der richtigen Stelle ankommt.

2.2 EINHALTUNG VON GESETZEN UND VORSCHRIFTEN

In bestimmten Bereichen wie Finanzdienstleistungen, Gesundheitswesen und Behörden sind Sicherheitsstandards oft vorgeschrieben. DNSSEC kann bei der Erfüllung von Compliance-Anforderungen wie NIS2 helfen, indem es die Integrität von DNS-Anfragen sicherstellt.

*Siehe 9.3 in diesem Leitfaden für weitere Einzelheiten.

3. Grundlage für erweiterte Sicherheitsprotokolle

DNSSEC ist mehr als nur eine eigenständige Sicherheitstechnologie. Es bietet eine Grundlage für neue und zusätzliche Sicherheitsprotokolle, wie z.B.:

3.1 DANE (DNS-BASED AUTHENTICATION OF NAMED ENTITIES).

DNSSEC ermöglicht DANE, ein Protokoll, das die Vertrauenswürdigkeit von SSL/TLS-Zertifikaten verbessert. DANE ermöglicht es einem Domänenbesitzer, eine bestimmte TLS-Zertifikatskette in DNSSEC-signierten Einträgen zu erfassen, was Zertifikatsfälschungen verhindert.

3.2 AUTHENTIFIZIERUNG FÜR E-MAIL (Z. B. MIT TLSA-EINTRÄGEN)

DNSSEC ermöglicht es Mailservern, kryptografisch validierte Einträge zu verwenden, was Sicherheitsmechanismen wie MTA-STS und STARTTLS stärkt.

3.3 IOT-SICHERHEIT

Mit dem Wachstum des Internet der Dinge (IoT) besteht ein dringender Bedarf an leichtgewichtigen, skalierbaren Sicherheitslösungen. DNSSEC füllt diese Lücke, indem es DNS-Anfragen vor Manipulationen schützt, was für die Gewährleistung einer zuverlässigen Kommunikation zwischen IoT-Geräten und ihren Servern unerlässlich ist. Folglich bietet DNSSEC eine robuste Sicherheitsebene in Ökosystemen, in denen herkömmliche Methoden nicht durchführbar oder effektiv sind.

4. Schutz des Unternehmensrufs

4.1 VERHINDERUNG VON RUFSCHÄDIGUNG

Ein erfolgreicher DNS-Angriff, z. B. die Umleitung einer Website auf eine betrügerische Seite, kann den Ruf eines Unternehmens ernsthaft schädigen. Die Kunden verlieren das Vertrauen in die Zuverlässigkeit des Unternehmens, was zu unmittelbaren finanziellen Verlusten und langfristigen Rufschädigungen führt.

4.2 BEGRENZUNG DER RECHTLICHEN HAFTUNG

Organisationen, die keine Sicherheitsmaßnahmen wie DNSSEC einführen, riskieren, für Datenschutzverletzungen oder Betrug haftbar gemacht zu werden. Durch die Verwendung von DNSSEC verringern Sie das Risiko rechtlicher Komplikationen.

5. Operative Vorteile

5.1 STÄRKUNG DER INTERNEN IT-PROZESSE

DNSSEC zwingt Organisationen dazu, sich einen detaillierten Überblick über ihre DNS-Infrastruktur zu verschaffen. Dies führt häufig zu verbesserten internen Prozessen und Verwaltungsstandards, wie z. B. Schlüsselverwaltung und Überwachung.

5.2 KOMPATIBILITÄT MIT MODERNEN TECHNOLOGIEN

Da immer mehr Geräte und Anwendungen DNSSEC unterstützen, ist DNSSEC von entscheidender Bedeutung für die Gewährleistung der Authentizität von DNS-Nachrichten.

6. Zukunftssicherheit

6.1 ERWARTETE STANDARDISIERUNG

Angesichts der zunehmenden Bedrohung durch Cyberangriffe ist es wahrscheinlich, dass DNSSEC schließlich zu einem obligatorischen Standard für alle Domänen wird. Durch eine frühzeitige Implementierung können sich Unternehmen einen Vorsprung verschaffen und die künftigen Migrationskosten minimieren.

6.2 BEREITSCHAFT FÜR QUANTENCOMPUTING

Die kryptografischen Algorithmen, die DNSSEC unterstützt, können an quantenresistente Varianten angepasst werden, was sie zu einer nachhaltigen Langzeitinvestition macht.

7. Zusammenfassung der Vorteile

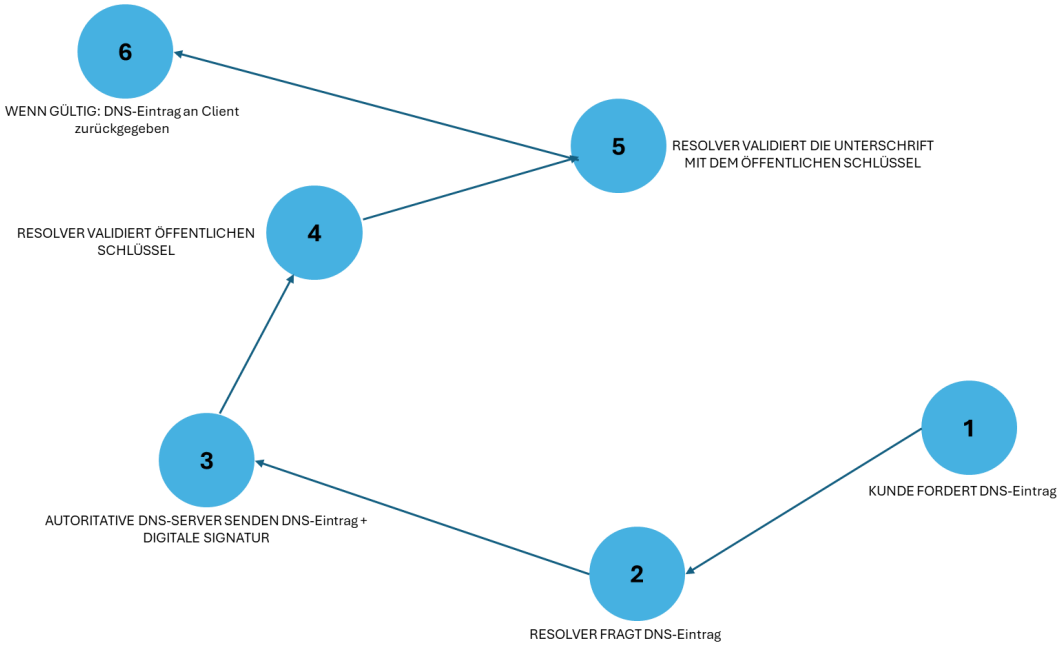
Kategorie	Vorteile
Sicherheit	Schutz vor DNS-Spoofing, Cache Poisoning und Man-in-the-Middle-Angriffen
Vertrauen	Erhöht das Vertrauen der Nutzer, Einhaltung von Vorschriften
Innovation	Grundlage für Technologien wie DANE und IoT-Sicherheit
Reputation	Verhindert Schäden durch DNS-bezogene Vorfälle.
Zukunftssicher	Bereitschaft für zukünftige Standards.

8. Entscheidung

Mit DNSSEC investiert eine Organisation in robuste Sicherheit und stärkt die Zuverlässigkeit ihrer Domain. In einer Zeit zunehmender Cyber-Bedrohungen ist DNSSEC nicht nur eine Ergänzung zu bestehenden Sicherheitsmaßnahmen, sondern eine Grundvoraussetzung.

9. Wie funktioniert DNSSEC technisch?

Technisches Schema: So funktioniert DNSSEC



9.1 Erklärung des Schemas

1. DER KUNDE FORDERT EINEN DNS-EINTRAG AN

Der **Client** (z. B. ein Webbrowser) sendet eine Anfrage an einen DNS-Resolver, um die IP-Adressinformationen eines Domänennamens (z. B. example.com) abzurufen.

- **Rolle von DNSSEC**: In diesem Schritt wird noch keine Sicherheit angewendet; die Anfrage ist eine Standard-DNS-Abfrage.

2. RESOLVER FORDERT DNS-EINTRAG AN

Der Resolver (häufig der DNS-Server eines ISP) leitet die Anfrage an den für die Domäne **zuständigen autoritativen DNS-Server** weiter.

- **Rolle von DNSSEC**: Der autoritative Server ist mit DNSSEC konfiguriert und weiß, dass der DNS-Eintrag sicher sein muss.

3. AUTORITATIVER DNS-SERVER SENDET DNS-EINTRAG + DIGITALE SIGNATUR

Der autorisierende DNS-Server sendet den angeforderten DNS-Eintrag zusammen mit einer **digitalen Signatur** (einem RRSIG-Eintrag) zurück. Diese Signatur wird mit einem privaten Schlüssel erzeugt.

- **Wichtig**!
  - Die Signatur garantiert, dass der DNS-Eintrag authentisch ist und während der Übertragung nicht verändert wurde.
  - Der öffentliche Schlüssel, der zur Überprüfung dieser Signatur erforderlich ist, wird in einem DNSKEY-Eintrag veröffentlicht.

4. RESOLVER VALIDIERT ÖFFENTLICHEN SCHLÜSSEL

Der Resolver führt die folgenden Aktionen durch:

- Der Resolver ruft den entsprechenden **öffentlichen Schlüssel** (DNSKEY-Eintrag) über DNS ab.
- Die **DS-Einträge** (Delegation Signer) und die entsprechende Signatur in der übergeordneten Zone (z. B. .be) beweisen, dass der öffentliche Schlüssel gültig ist.
- Dieser Prozess wiederholt sich bis zur **Root-Zone**, deren öffentlicher Schlüssel bereits als vertrauenswürdig eingestuft ist (der "Vertrauensanker").

- Der Resolver ruft den entsprechenden **öffentlichen Schlüssel** (DNSKEY-Eintrag) über DNS ab.

5. RESOLVER VALIDIERT DIE SIGNATUR MIT ÖFFENTLICHEM SCHLÜSSEL

Der Resolver validiert die empfangene Signatur. Dazu prüft der Resolver, ob die Signatur gültig ist.

6. FALLS GÜLTIG: RÜCKGABE DES DNS-EINTRAGS AN DEN KUNDEN

Wenn alle Prüfungen erfolgreich sind, gibt der Resolver den ursprünglichen DNS-Eintrag an den Kunden zurück.

Schlägt die Validierung fehl (z. B. aufgrund einer ungültigen Signatur), wird ein Fehler zurückgegeben und der Kunde erhält keine DNS-Antwort.

9.2 DIE GRUNDPRINZIPIEN

DNSSEC funktioniert über ein hierarchisches System von digitalen Signaturen und öffentlichen Schlüsseln:

1. **Zonenlisten und Datensätze**:
    - DNS-Einträge werden mit einer digitalen Signatur versehen. Die Signatur wird mit einem privaten Schlüssel erzeugt.
    - Der zugehörige öffentliche Schlüssel wird in einem DNSKEY-Eintrag in derselben Zone gespeichert.
2. **Validierung durch eine Vertrauenskette**:
    - Um die Integrität von DNS-Antworten zu gewährleisten, validieren dnssec-fähige Resolver die Signatur anhand des öffentlichen Schlüssels.
    - Dieser Prozess verläuft in der DNS-Baumstruktur hierarchisch nach oben (z. B. von Domain → TLD → Root).

9.3 TECHNISCHE KOMPONENTEN

1. **DNSKEY-Einträge**:
    - Enthält den öffentlichen Schlüssel der Zone.
    - Zwei Arten von Schlüsseln:
        - **ZSK (Zone Signing Key)**: Signiert DNS-Einträge innerhalb der Zone.
        - **KSK (Key Signing Key)**: Signiert den ZSK, um die Vertrauenskette zu stärken.
2. **RRSIG-Einträge**:
    - Jeder DNS-Eintrag in einer Zone hat einen zugehörigen RRSIG-Eintrag, der die digitale Signatur enthält.
3. **Delegation Signer (DS)-Einträge**:
    - Werden verwendet, um eine Vertrauenskette zwischen einer untergeordneten Zone und der übergeordneten Zone zu schaffen (z. B. zwischen einer Domäne und ihrer TLD).
4. **NSEC/NSEC3-Einträge**:
    - Werden verwendet, um kryptografisch zu verifizieren, dass ein Datensatz nicht existiert.
    - Bieten Sicherheit gegen Brute-Force-Angriffe auf nicht existierende Domains. (standardmäßig nicht global aktiviert)
    - NSEC zeigt die nächste verfügbare Domäne an, während NSEC3 Hashing für zusätzliche Sicherheit verwendet.

9.4 DER VALIDIERUNGSPROZESS

1. Ein DNS-Resolver fragt nach den DNS-Einträgen einer Domäne.
2. Die Einträge werden zusammen mit ihren RRSIG-Einträgen zurückgegeben.
3. Der Resolver prüft:
    - ob es einen oder mehrere DS für die Zone im Parent gibt
    - Ob die Signatur mit dem DNSKEY übereinstimmt.
    - ob der DNSKEY legitim ist, indem er ihn anhand der DS-Einträge in der übergeordneten Zone validiert.
    - Kein DS => KEINE Validierung
4. Der Prozess wiederholt sich bis zur Root-Zone, deren öffentlicher Schlüssel bekannt ist und als vertrauenswürdiger Anker dient.

10. Schritte der Implementierung

10.1 VORBEREITUNG

1. **Prüfen Sie die DNSSEC-Unterstützung**:
    - Vergewissern Sie sich, dass Ihr DNS-Anbieter oder Ihre Nameserver-Software DNSSEC unterstützt (z. B. BIND, Knot oder NSD als autorisierende DNS-Software und BIND oder Unbound als DNS-Auflösungssoftware).
2. **Erzeugen Sie Schlüssel**:
    - Erstellen Sie einen KSK und ZSK mit DNSSEC-Tools. Bei BIND kann dies mit dem Befehl:

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

3. **Veröffentlichen Sie den öffentlichen Schlüssel**:
    - Fügen Sie die DNSKEY-Einträge zu Ihrer DNS-Zonendatei hinzu.

10.2 KONFIGURATION

1. **Signieren Sie die Zone**:
    - Verwenden Sie ein Tool wie dnssec-signzone, um die Zonendatei zu signieren:

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

      Beispiel: Wenn Sie die Schlüssel in /etc/dnssec/keys/ gespeichert haben und eine Zonendatei example.com.zone haben, sieht der Befehl wie folgt aus:

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

2. **Konfigurieren Sie die übergeordnete Zone**:
    - Laden Sie den DS-Eintrag zu Ihrem TLD-Anbieter hoch, um die Vertrauenskette zu bilden.
3. **Aktualisieren Sie die Resolver**:
    - Konfigurieren Sie Ihre Resolver für die Verwendung der DNSSEC-Validierung. Für Unbound können Sie dies mit aktivieren:

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

10.3 TEST UND ÜBERPRÜFUNG DES STATUS EINER DNS-ZONE (DNSVIZ.NET)

ÜBERPRÜFEN SIE DIE KONFIGURATION MIT TOOLS WIE:

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

11. Vorteile und Nachteile

11.1 VORTEILE

1. **Schutz vor Manipulationen**:
   - DNSSEC verhindert Angriffe wie Cache Poisoning und DNS-Spoofing.
2. **Grundlage für weitere Sicherheit**:
   - DNSSEC ist eine Grundlage für Technologien wie DANE (z. B. für E-Mail-Sicherheit über TLSA-Einträge).
3. **Erhöhtes Vertrauen**:
   - Benutzer und Systeme können darauf vertrauen, dass DNS-Daten authentisch sind.

11.2 NACHTEILIGE ASPEKTE

1. **Komplexität**:
   - Schlüsselverwaltung und Zonensignierung erfordern Fachwissen.

2. **Größere DNS-Pakete**:
   - Durch zusätzliche Datensätze (RRSIG, DNSKEY, NSEC) werden DNS-Antworten größer, was bei älteren Systemen zu Problemen führen kann.

3. Dies kann für Amplifikationsangriffe ausgenutzt werden.
   Wie DNSSEC speziell bei Amplifikationsangriffen eingesetzt wird

   - Hohe Antworten aufgrund von DNSSEC:

     - DNSKEY-Datensätze: Enthalten die öffentlichen Schlüssel und können sehr groß sein (insbesondere bei Verwendung starker Kryptographie wie RSA 2048).
     - RRSIG-Einträge: Digitale Signaturen für jede DNSSEC-geschützte Zone.
     - NSEC/NSEC3-Datensätze: Datensätze, die den nächsten Namen in der Zone angeben und zum Schutz gegen Zone-Walking verwendet werden, aber auch sehr groß sind.

   - Offene Auflöser:

     - Angreifer verwenden schlecht konfigurierte offene Resolver, die DNS-Anfragen von jedermann akzeptieren.
     - Diese Resolver senden die Antworten mit den großen DNSSEC-Datensätzen an das Ziel zurück.

   - Verstärkungsfaktor:

     - Das Verhältnis zwischen der Größe der Eingabe (DNS-Anfrage) und der Ausgabe (DNS-Antwort) wird als Verstärkungsfaktor bezeichnet.
     - Bei DNSSEC kann dieser Verstärkungsfaktor das 50-fache oder mehr betragen. So kann beispielsweise eine Anfrage von 60 Byte eine Antwort von 3000 Byte erzeugen.

4. **Keine Verschlüsselung**:
   - DNSSEC schützt nur die Integrität und Authentizität; die Daten werden nicht verschlüsselt.
5. Zonenwanderung:
   - Aufgrund von NSEC besteht die Möglichkeit, dass Zoneninhalte aufgezählt werden können. In manchen Situationen ist dies nicht wünschenswert. NSEC3 erschwert die Aufzählung von Zonen erheblich.

12. Bewährte Verfahren für DNSSEC

1. **Verwenden Sie sichere Algorithmen**:
   - Wählen Sie moderne Algorithmen in Übereinstimmung mit den Empfehlungen von RFC 8624 (z. B. ECDSAP256SHA256.)

2. **Regelmäßige Schlüsselverwaltung**:
   - Rotieren Sie die ZSKs alle 3-6 Monate und die KSKs jährlich.

3. **Regelmäßige Überprüfung der Konfiguration**:
   - Implementieren Sie eine aktive Überwachung, um auf abgelaufene Signaturen und Schlüssel zu prüfen.

4. **Implementierung von Fallback-Optionen**:
   - Konfigurieren Sie die Resolver so, dass sie DNSSEC-Validierungsprobleme ohne Dienstunterbrechungen behandeln können.

13. Kosten und Wartung

- **DNSSEC-Konfiguration**:
  - Erstkonfiguration: 5-15 Arbeitsstunden je nach Komplexität.
  - Wartung: Regelmäßige Rotation der Schlüssel, Aktualisierung der Zonendateien.

- **Kostenangabe**:
  - **Kleine Domains**: ~100-€300 pro Jahr.
  - **Große Organisationen**: Zusätzliche Kosten für Personal, Schulung und Überwachung.

Haftungsausschluss