DNS - DNSSEC

DNSSEC (Domain Name System Security Extensions) adalah seperangkat ekstensi keamanan untuk **DNS (Domain Name System)** yang dirancang untuk melindungi pengguna dari manipulasi data DNS, seperti **DNS spoofing** atau **cache poisoning**. DNSSEC memastikan bahwa informasi yang dikirim melalui DNS berasal dari sumber yang tepercaya dan tidak diubah selama proses transmisi.

Fungsi Utama DNSSEC:

1. **Otentikasi Sumber Data**: Memastikan bahwa data DNS berasal dari server yang benar (asli).
2. **Integritas Data**: Menjamin bahwa data DNS tidak diubah atau dimanipulasi dalam perjalanan.
3. **Perlindungan dari Serangan**: Melindungi dari serangan seperti *DNS spoofing* atau *cache poisoning*.

Cara Kerja DNSSEC:

1. **Tanda Tangan Digital (Digital Signature)**:
   - Zona DNS yang diaktifkan DNSSEC akan menandatangani setiap respons menggunakan **kriptografi kunci publik**.
   - Setiap rekam DNS (seperti A, AAAA, MX) memiliki tanda tangan digital yang diverifikasi oleh resolver DNS.
2. **Verifikasi Kunci (Chain of Trust)**:
   - Dimulai dari **root zone** DNS, setiap lapisan zona DNS memverifikasi kunci publik zona di bawahnya.
   - Ini membentuk **rantai kepercayaan** (chain of trust) dari root hingga domain yang diakses.

Rekaman DNS Khusus di DNSSEC:

- **RRSIG**: Menyimpan tanda tangan digital.
- **DNSKEY**: Menyimpan kunci publik.
- **DS (Delegation Signer)**: Menghubungkan zona ke induknya.
- **NSEC/NSEC3**: Mencegah pencacahan zona dan menunjukkan catatan yang tidak ada.

Keuntungan DNSSEC:

- Perlindungan dari manipulasi data DNS.
- Meningkatkan kepercayaan dan keamanan di internet.
- Mencegah pengguna diarahkan ke situs palsu atau berbahaya.

⚠ **Kelemahan DNSSEC:**

- Kompleksitas dalam implementasi dan pengelolaan.
- Memerlukan dukungan dari seluruh rantai DNS (termasuk registrar dan resolver).
- Penambahan overhead karena verifikasi tanda tangan.

Revision #1
Created 19 March 2025 04:48:53 by Kevin
Updated 19 March 2025 04:49:49 by Kevin