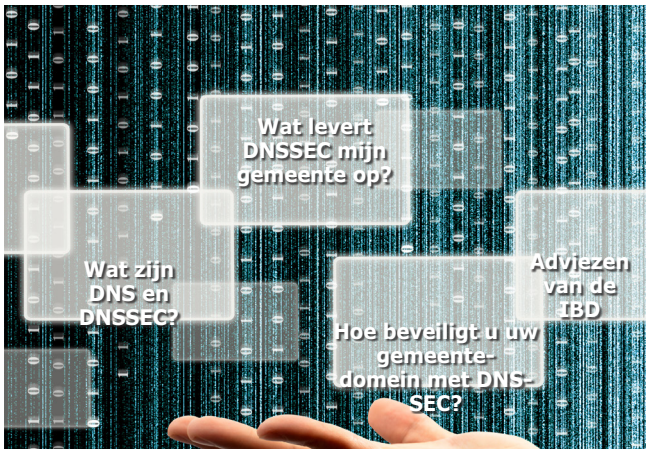
INFORMATIE BEVEILIGINGS DIENST

FS-20160315.06E

DNSSEC: VOORKOM DOMEINNAAMFRAUDE

DNSSEC beveiligt uw Domain Name System (DNS)-informatie. Met Domain Name System Security Extensions (DNSSEC) kan een gebruiker er op rekenen dat deze te maken heeft met bijvoorbeeld de authentieke web- of mailserver van uw gemeente. DNSSEC beschermd de integriteit van de DNS-informatie en zorgt ervoor dat het DNS-antwoord authentiek is en afkomstig van de juiste bron. Zo wordt voorkomen dat kwaadwillenden ongemerkt verkeer kunnen omleiden. De implementatie van de DNSSEC-standaard is relatief eenvoudig en levert een belangrijke bijdrage aan veilig internetverkeer. De IBD adviseert dan ook om de DNSSEC-standaard in uw gemeente te implementeren.



WAT LEVERT DNSSEC MIJN GEMEENTE OP?

DNSSEC heeft voordelen voor iedere domeinnaamhouder en voorkomt dat kwaadwillenden de DNS-informatie kunnen manipuleren en gebruikers of hun gegevens naar een malafide omgeving verwijzen. Als de gemeentelijke domeinnamen zijn beveiligd met DNSSEC wordt de informatie bij de omzetting van domeinnaam naar IP-adres en vice versa beschermd. Het resultaat is dat het internet weer een stukje veiliger is gemaakt voor zowel gebruikers (bijvoorbeeld burgers, ketenpartners, et cetera) als aanbieders (bijvoorbeeld gemeenten) van digitale producten en diensten. Tevens zorgt DNSSEC ervoor dat bestaande beveiligingsprotocollen, zoals voor e-mailauthenticatie, van een extra bescherming kunnen worden voorzien.

"DNSSEC IS EEN BELANGRIJKE STAP IN HET VEILIGER MAKEN VAN INTERNETVERKEER"

Deze factsheet richt zich op gemeenten die het DNS-beheer hebben uitbesteed en gebruik willen maken van de beveiligingsstandaard DNSSEC. Hierbij wordt achtereenvolgens aandacht besteed aan de beveiligingsvoordelen van DNSSEC, de DNS en DNSSEC-standaard, hoe uw gemeente gebruik kan maken van DNSSEC en tenslotte het IBD advies. Voor uitgebreidere en meer technische achtergrondinformatie wordt verwezen naar de uitgebreide versie van deze factsheet op de website van de IBD.

Pas-toe-of-leg-uit

De DNSSEC-standaard is sinds 2012 opgenomen op de lijst met verplichte open standaarden voor de gehele publieke sector ('pas-toe-of-leg-uit-lijst') van het Forum Standaardisatie. Dit betekent dat overheden en semi-overheden DNSSEC dienen toe te passen en alleen in geval van zwaarwegende redenen daarvan mogen afwijken. Tevens adviseert het Nationaal Cyber Security Centrum (NCSC) DNSSEC in het verdiepingsdocument van de ICT-Beveiligingsrichtlijnen voor Webapplicaties.

Wat is DNS en DNSSEC?

Het Domain Name System (DNS) verzorgt de vertaling van domeinnamen naar IP-adressen en vice versa. Zo zal een browser een DNS-server raadplegen voor de domeinnaam www.ibdgemeenten.nl alvorens contact te kunnen zoeken met de webserver op het Internet Protocol versie 4 (IPv4)-adres 83.137.17.164 of IPv6-adres 2001:4038:200:43::164. DNS is dan ook een fundamentele factor om al het internetverkeer goed te laten verlopen. Nagenoeg alle software die verbonden is met het internet en gebruik maakt van domeinnamen maakt gebruik van dit DNS-systeem. Het is hierbij cruciaal dat de informatie die door de DNS-server geleverd wordt

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

betrouwbaar is zodat wordt voorkomen dat kwaadwillenden ongemerkt verkeer omleiden. DNS is kwetsbaar voor dit soort omleidingen. Op deze wijze kunnen gebruikers worden omgeleid, dit heet DNS-spoofing, naar een phishingsite of computers worden besmet met kwaadaardige software. Dit terwijl de gebruikte domeinnaam juist is.

Een belangrijke stap in het veiliger maken van het DNS is Domain Name System Security Extensions (DNSSEC). Dit is een beveiliging die een digitale handtekening toevoegt aan DNS-informatie. Op deze manier wordt de integriteit van de DNS-informatie beschermd en kan worden gecontroleerd of het DNS-antwoord authentiek is en afkomstig is van de juiste bron.

Systemen die DNSSEC-ondersteuning bieden zijn compatibel met systemen die DNSSEC nog niet ondersteunen. Voor deze (oudere) systemen geldt natuurlijk dat de DNS-informatie niet is voorzien van een digitale handtekening.

DNSSEC bestaat uit twee hoofdtaken:
- Signeren: Het generen en opnemen van de digitale handtekening bij een domeinnaam in het DNS-systeem.
- Valideren: Het controleren van de digitale handtekening als een domeinnaam wordt opgevraagd.

Als de digitale handtekening succesvol is gevalideerd, is met zekerheid vastgesteld dat de inhoud van bijvoorbeeld www.ibdgemeenten.nl ook daadwerkelijk van het IP-adres afkomstig is dat bij de domeinnaam hoort. De gebruiker heeft in dit voorbeeld te maken met de authentieke webserver van www.ibdgemeenten.nl. Dit is niet hetzelfde als het garanderen van de privacy (vertrouwelijkheid) en data-integriteit tussen twee communicerende computersystemen, een client en een server. Hiervoor dient men gebruik te maken van het Transport Layer Security (TLS)-protocol. Zie hiervoor de factsheet 'HTTPS zorgt voor veilige verbinding met de gemeente-website' op www.ibdgemeenten.nl

Hoe beveiligt u uw gemeentedomein met DNSSEC?
De eenvoudigste manier is een aanvraag hiervoor te doen bij de organisatie die het DNS-systeem beheert met de gemeentelijke domeinnaam. Dit heeft ook de minste impact voor gemeenten. Het beheer kan door een externe organisatie zoals uw Internet Service Provider (ISP) of hostingpartij worden uitgevoerd maar kan ook door de gemeente zelf.[1] Als niet bekend is wie de beheerder is van uw gemeentelijke domeinnaam kan dit met behulp van openbare WHOIS domeinnaamregistratie achterhaald worden. Voor het .nl-domein wordt de WHOIS informatie aangeboden door Stichting Internet Domeinregistratie Nederland (SIDN).

Aandachtspunten met betrekking tot het DNS-beheer:
- Als u een gemeentelijke domeinnaam wilt laten registreren let dan bij de keuze van de DNS-beheerder of DNSSEC wordt ondersteund. Welke organisaties DNSSEC ondersteunen kan nagegaan worden op de website van SIDN, de beheerder van de .nl-domeinnamen.[2]
- Als u al een gemeentelijke domeinnaam hebt geregistreerd maar nog geen gebruik maakt van DNSSEC, vraag dan of uw DNS-beheerder DNSSEC ondersteuning biedt. Het zou kunnen dat de DNS-beheerder hiervoor eenmalige of jaarlijkse kosten in rekening brengt. Veel DNS-beheerders bieden DNSSEC overigens kosteloos aan.

Mocht de huidige DNS-beheerder geen DNSSEC ondersteuning bieden, dan kunt u overwegen om de registratie van uw gemeentelijke domeinnaam te verhuizen naar een andere organisatie. U kunt ook overwegen om deze registratie te verhuizen als de bijkomende kosten voor DNSSEC ondersteuning voor uw gemeente niet acceptabel zijn. Het verhuizen van de registratie van uw gemeentelijke domeinnaam betekent niet dat u ook de gemeente-website moet verhuizen. Verhuizen is in de regel een eenvoudig proces.

Een ander aandachtspunt is of uw Internet Access Provider (IAP), die de internet toegang verzorgt, de digitale handtekening van domeinnamen controleert. Dit wordt namelijk niet door iedere IAP ondersteund. De DNS-beheerder is van belang voor het plaatsen van de digitale handtekening en de IAP zou deze digitale handtekening dienen te valideren. De DNS-beheerder en IAP kunnen een en dezelfde organisatie zijn.

1 Gemeenten die DNS in eigen beheer hebben zijn bijvoorbeeld Den Haag, Heerlen, Maastricht en Rotterdam.

2 https://www.sidn.nl/registrars/. Via de optie 'Alleen DNSSEC laten zien'.

Advies IBD met betrekking tot DNSSEC

De IBD geeft het advies om:
- de gemeentelijke domeinnamen te beveiligen met DNSSEC. Vraag hiervoor aan de registrar of deze DNSSEC ondersteunen.
- DNSSEC te valideren. Vraag hiervoor aan uw IAP of deze DNSSEC validatie ondersteunt.

Op de website internet.nl kunt u eenvoudig de veiligheid van uw gemeentelijke domeinnamen controleren. Tevens kunt u via deze website DNSSEC-validatie uitvoeren voor e-mail of uw internetverbinding. Dit levert direct inzicht of DNSSEC aan staat en goed werkt. U kunt de gedetail-leerde testrapportage gebruiken om de DNS-beheerder te vragen DNSSEC aan te zetten of eventuele problemen op te lossen.

MEER INFORMATIE

MEER INFORMATIE OVER ONZE DIENSTVERLENING VINDT U IN DE ANDERE FACTSHEETS VAN DE IBD EN OP DE WEBSITE WWW.IBDGEMEENTEN.NL. HIER KUNNEN GEMEENTEN BOVENDIEN VIA DE COMMUNITY RELEVANTE INFORMATIE MET ELKAAR DELEN, VRAGEN AAN ELKAAR STELLEN EN DOCUMENTEN UITWISSELEN. DE HELPDESK VAN DE IBD IS TE BEREIKEN TIJDENS KANTOORUREN VAN 9:00 TOT 17:00 UUR OP HET NUMMER 070 373 8011 OF VIA HET E-MAILADRES INFO@IBDGEMEENTEN.NL. TIJDENS DEZE KANTOORUREN REAGEERT DE IBD BINNEN 30 MINUTEN OP EEN INCIDENTMELDING. BUITEN KANTOORUREN IS DE IBD OP HETZELFDE NUMMER BEREIKBAAR VOOR SPOEDEISENDE MELDINGEN EN ZAL DE IBD BINNEN 60 MINUTEN REAGEREN OP EEN TELEFONISCHE OPROEP.