FS-20130903.07F

GEMEENTEN CONTRO INTERNETADRES

GEMEENTE HEERLEN IMPLEMENTEERT DNSSEC

DNSSEC zorgt voor de beveiliging van domeinnamen. De standaard biedt de gebruiker de mogelijkheid om te controleren of hij wordt 'doorverbonden' met het juiste internetnummer. Sinds juni 2012 staat dit systeem op de 'pas toe of leg uit'-lijst van het Forum en College Standaardisatie, en heeft daarmee een 'verplichte' status gekregen voor overheden en semi-publieke instellingen. Inmiddels zijn de domeinnamen van meer dan 30 overheden ondertekend. En de gemeente Heerlen is ook bezig met de andere kant, namelijk de controle op de geldigheid van de DNSSEC-handtekening van opgevraagde domeinnamen.

Tekst: Bart Knubben en Roeland Coomans, Bureau Forum Standaardisatie en Michiel Henneke, Stichting Internet Domeinregistratie Nederland (SIDN)

DNSSEC past bij de onderhoudsbeurt die het internet nodig heeft. De nu gebruikte internetstandaarden zijn ontworpen in de jaren zeventig en voldoen niet meer. Ze kunnen de aantallen gebruikers niet meer aan, en hun veiligheidsniveau is onvoldoende, gezien de waarde die online-transacties vertegenwoordigen. Recente internet-incidenten, zoals de Diginotar-affaire, tonen aan dat kwetsbaarheden in de internet-infrastructuur potentieel grote gevolgen kunnen hebben.

Domain Name System (DNS) zorgt voor de vertaling van een internet-domeinnaam, zoals http://www.s-hertogenbosch.nl, naar IP-adressen, bijvoorbeeld 5.200.8.185 (IPv4) en 2a00:1630:32::5 (IPv6). Bij het opvragen van een website maakt de computer van de gebruiker, na de DNS-vertaling, contact met de webserver via het IP-adres. DNS is kwetsbaar. Daardoor kan een kwaadwillende een domeinnaam aan een ander IP-adres koppelen en de gebruiker misleiden.

DNSSEC lost dit op door middel van een digitale handtekening. Als de eindgebruiker een domeinnaam opvraagt, bijvoorbeeld via zijn webbrowser, dan kan hij de geldigheid van de handtekening geautomatiseerd controleren. DNSSEC werkt als aanvulling op SSL-certificaten op basis van PKI die in de webbrower vaak met een slotje worden weergegeven. Deze certificaten zorgen voor de integriteit en vertrouwelijkheid van de gegevensuitwisseling met een bepaalde domeinnaam, maar kunnen niet garanderen dat er met het correcte IP-adres wordt gecommuniceerd. DNSSEC kan dat wel.

LEREN ECHTHEID

DNSSEC zorgt voor een veiligere internet-infrastructuur en is op zichzelf een relatief laagdrempelige beveiligingsmaatregel. Bovendien biedt het een fundament waarop kan worden voortgebouwd met complementaire beveiligingsstandaarden, zoals DKIM (e-mailauthenticatie) en DANE (SSL-certificaatcontrole).

STEEDS MEER ONDERTEKENDE DOMEINNAMEN

SIDN – het bedrijf dat de uitgifte en registratie van .nl-domeinnamen verzorgt – heeft ondertekening met DNSSEC in mei 2012 mogelijk gemaakt voor alle .nl-domeinnamen. Op dit moment zijn bijna 1,5 miljoen .nl-domeinnamen voorzien van DNSSEC, meer dan een kwart van het totaal. Ook overheden pakken het op. Zo is een groeiend aantal domeinnamen van de overheid, waaronder rijksoverheid.nl, pleio.nl en woerden.nl, beveiligd.

Mede door de sterk gegroeide hoeveelheid ondertekende domeinnamen (ook in het buitenland), zien steeds meer DNS-beheerders het belang van DNSSEC-validatie in. De verwachting is dat validatie straks ook standaardonderdeel van de webbrowser wordt. Nu kan dat in de meeste browsers alleen via een 'add-on'.

VALIDATIE IN HEERLEN VERLOOPT SOEPEL

De gemeente Heerlen is met DNSSEC-validatie aan de slag gegaan. 'Wij exploiteren onze eigen DNS-omgeving. Sinds half december valideren wij DNSSEC op onze externe caching DNS-servers', vertelt ICT-architect John Dautzenberg. Het blijkt dat men via de collega-IT-beheerders de gebruikers op de hoogte heeft gesteld hiervan, met de waarschuwing dat validatie ook voor bereikbaarheidsproblemen kan zorgen. Een website met een niet-valide DNSSEC-handtekening is namelijk niet langer benaderbaar.

De gemeente Heerlen liep tegen beveiligde, geactiveerde, domeinnamen aan die door domeinnaamhouders niet goed waren geconfigureerd. Om dit probleem te omzeilen houdt men voorlopig de oude caching DNS-servers in de lucht. Wat betreft deze specifieke domeinen wordt er vanuit de interne caching DNS-servers naar deze niet-validerende systemen geforward. Gelukkig heeft men dit voor slechts een heel klein aantal domeinnamen zo moeten 'inregelen'.

DNSSEC-validatie was voor Heerlen een op zichzelf staand project. 'We hebben enkel twee nieuwe DNS-servers hoeven in te richten naast de bestaande systemen', zegt Dautzenberg. 'Omdat het allemaal virtuele servers zijn, is de installatie van een extra systeem een fluitje van een cent.'

> OP DIT MOMENT ZIJN BIJNA 1,5 MILJOEN .NL-DOMEINNAMEN VOORZIEN VAN DNSSEC

Zelf is de gemeente bij SIDN aangesloten als registrar. Voor niet-.nl-domeinen maken ze gebruik van de diensten van Networking4all en Argeweb. Maar ook daarvoor doen ze zelf de DNS-dienst. Alles bij elkaar beheert Heerlen zo'n tweehonderd domeinnamen voor diverse Zuid-Limburgse gemeenten, voor de Brandweer Zuid-Limburg en voor enkele andere non-profit organisaties.

Dautzenberg laat weten dat Heerlen binnenkort ook haar autoratieve DNS-servers onder handen gaat nemen, wat het mogelijk maakt om de beheerde domeinnamen met DNSSEC te ondertekenen. Hij vervolgt: 'We zetten daarvoor drie nieuwe installaties op, waarna we de te ondertekenen domeinen naar deze systemen migreren. Overigens is het aan onze "klanten" of zij hun domeinen wel of niet willen laten ondertekenen. We hopen in het najaar met de eerste ondertekende domeinen te kunnen beginnen.'

Ook de gemeente Woerden heeft haar domeinnaam ondertekend met DNSSEC.

Meer weten?
www.dnssec.nl
www.forumstandaardisatie.nl