Wat betekent het inschakelen van DNSSEC voor mijn domein?

Wat levert DNSSEC op?

DNSSEC voegt een aantal essentiële eigenschappen toe aan het DNS protocol die kwetsbaarheden in dit protocol oplossen. Wat DNSSEC toevoegt is:

- **authenticiteit** - clients die informatie uit DNS over een domein opvragen kunnen met DNSSEC met zekerheid vaststellen dat de informatie authentiek is (dat wil zeggen: ingevoerd door de legitieme beheerder van het domein).
- **integriteit** - clients kunnen er zeker van zijn dat een DNS bericht niet is veranderd terwijl het verzonden werd over het internet.

Naast deze twee belangrijke eigenschappen maakt DNSSEC ook een aantal nieuwe toepassingen mogelijk, zoals het registreren van informatie over X.509 certificaten in DNS en het registreren van informatie over SSH servers.

Hoe schakel ik DNSSEC in?

DNSSEC is in SURFdomeinen eenvoudig in te schakelen. Meer informatie daarover kunt u vinden in de handleiding van SURFdomeinen.

Hoe schakel ik DNSSEC uit?

Het uitschakelen van DNSSEC komt momenteel in praktijk weinig voor. Op dit moment is er dan ook een handmatige handeling door een DNS beheerder van SURFnet nodig om DNSSEC uit te schakelen (er wordt gewerkt aan het automatiseren hiervan). U kunt het best contact opnemen met SURFnet DNS beheer via e-mail als u DNSSEC voor een domein wilt uitschakelen, via dns-beheer@surfnet.nl.

Situaties waarin u mogelijk DNSSEC moet uitschakelen zijn:

- Verhuizing van het domein naar een andere registrar.
- Wijziging van de name servers voor het domein, waarbij u het beheer niet langer via SURFdomeinen uitvoert, maar bijvoorbeeld zelf DNS gaat beheren voor het domein.

Welke risico's en nadelen zijn er?

DNSSEC is een stuk complexer dan regulier DNS. Zo moeten de sleutels die gebruikt worden voor het zetten van digitale handtekeningen in DNS regelmatig worden vervangen en moeten de digitale handtekeningen zelf ook regelmatig worden ververst. SURFnet gebruikt hiervoor een volledig geautomatiseerd systeem op basis van OpenDNSSEC. Om te garanderen dat dit systeem goed functioneert zet SURFnet bovendien 24x7 monitoring in die de integriteit van domeinen met DNSSEC die worden beheerd via SURFdomeinen controleert en garandeert.

Waar u zich van bewust moet zijn is dat DNSSEC uitschakelen een handmatige handeling vereist (zie "Hoe schakel ik DNSSEC uit?" hierboven). Een nadeel van het inschakelen van DNSSEC is dan ook dat als u het weer uit wilt zetten dit enige tijd (uren tot dagen) kan duren. Als u nog niet zeker weet of u een domein zult blijven beheren via SURFdomeinen raden wij u aan om te wachten met het inschakelen van DNSSEC tot het moment dat u hierover een beslissing hebt genomen.

Waar kan ik meer informatie vinden over DNSSEC?

Op de SURF website staan een aantal documenten over DNSSEC:

- Hardening the Internet - the Impact and Importance of DNSSEC - deze white paper uit 2009 bevat uitgebreide organisatorische en technische informatie over DNSSEC.

- Deploying DNSSEC Validation - in deze white paper uit 2012 leest u hoe u DNSSEC validatie kunt inschakelen op de DNS resolvers van uw instelling. De white paper bevat praktische stappenplannen voor de meestgebruikte DNS software (BIND, Unbound, Windows Server 2012). De DNS resolver van SURFnet ondersteunen ook DNSSEC validatie, meer informatie daarover kunt u vinden op de SURF website.

Zoek in deze wiki:

Snel naar een andere vraag: