Instellen van DNSSEC voor uw domein tbv de NTA 7516

De NTA 7516 en de bijbehorende technische handreiking beschrijft een groot aantal maatregelen die een organisatie moet nemen om veilig gebruik te kunnen maken van e-mail voor de uitwisseling van persoonlijke gezondheidsinformatie. Het beveiligen van de domeinnaamserver (DNS) van een organisatie door het ‘aanzetten’ van DNSSEC is een van deze maatregelen die vereist is om interoperabiliteit tussen e-maildiensten mogelijk te maken. DNSSEC is ook een van de verplichte standaarden op de ‘pas-toe-leg-uit-lijst’ van het forum standaardisatie.

Wat is DNS?

DNS is een belangrijk onderdeel van ons internet. Wanneer je een domeinnaam intypt in een browser, bijvoorbeeld www.dwangindezorg.nl, dan wordt in de DNS het juiste ip-adres opgezocht van de server waarop deze website wordt gehost, een zogenaamde lookup, waarna de browser de webpagina ophaalt van die betreffende server en weergeeft in de browser. DNS wordt ook gebruikt om de IP-adressen op te zoeken van de servers die een e-mail ontvangen die aan de desbetreffende organisatie geadresseerd is, zogenaamde mailservers.

Wat is DNSSEC?

DNSSEC is een uitbreiding op DNS om dit oude protocol veiliger te maken. Met DNS zonder DNSSEC is het voor kwaadwillende personen mogelijk om de lookup te beïnvloeden en andere foutieve informatie terug te geven (zogeheten cache poisoning of 'man-in-the-middle' aanvallen). Dus bijvoorbeeld bij een lookup naar www.dwangindezorg.nl een ander ip-adres teruggeven. In het geval van een e-mail wordt deze dus bij een verkeerde server afgeleverd waardoor onbevoegden de informatie in de e-mail kan lezen. DNSSEC maakt dat deze beïnvloeding niet langer mogelijk is.

Hoe zet ik DNSSEC aan?

Beveiligen van de DNS-server van je domein kan alleen als je een eigen domeinnaam hebt. Als u gebruikmaakt van een gratis (gedeelde) e-maildienst (bijv. @gmail.com of @outlook.com) dan kunt u geen veilige e-mails ontvangen volgens de NTA 7516. U voldoet dan ook niet aan geldende wet- en regelgeving rondom informatiebeveiliging als u met deze e-mailadressen persoonlijke gezondheids-informatie verstuurt. Het is zeer aan te raden om een eigen domeinnaam en een (veilige) e-mailservice daaraan te koppelen.

Als u wel een eigen domeinnaam heeft dan is deze mogelijk al beveiligd met DNSSEC; inmiddels heeft namelijk bijna 55% van de Nederlandse domeinnamen al DNSSEC ingesteld staan. Controleer of op uw domeinnaam al DNSSEC actief is op https://internet.nl/test-mail/. Vul onderaan de pagina het domein van uw e-mailadres in (alles na het @-teken) en klik op ‘Start Test’. Zijn onder het kopje ‘DNSSEC - E-mailadresdomein’ beide schildjes groen, dan voldoet uw domein aan deze beveiligings-standaard.

Blijkt uw domein nog niet te beschikken over DNSSEC? Bij de meeste domeinaanbieders (registrars) kunt u dit aan (laten) zetten. Weet u niet wie uw registrar is, kijk dan op https://www.sidn.nl/whois. Vul boven aan de pagina uw domeinnaam in en klik op ‘Check’. Klik op de volgende pagina op ‘Toon mij de gegevens’. Daar staat onder het kopje 'Registrar' de domeinaanbieder waar u uw domeinnaam hebt

geregistreerd. U kunt dan het beste naar de website van uw domeinaanbieder gaan en zoeken op DNSSEC of contact opnemen met de helpdesk.
Ondersteunt uw registrar geen DNSSEC? Dan is het verhuizen van uw domeinnaam naar een andere registrar de enige optie om voor het onderdeel interoperabiliteit te kunnen voldoen aan de NTA. Dit is relatief eenvoudig en kost u vaak slechts enkele euro's. Op de websites van de meeste registrars staat een duidelijke beschrijving van hoe dit moet. Zorg uiteraard wel dat uw nieuwe registrar wel DNSSEC ondersteunt.
Controleer nadat u DNSSEC heeft aangezet of uw domeinnaam heeft verhuisd, of dit is gelukt door bovenstaande controle opnieuw te doen.

Meer informatie

Kijk ook op de website van het SIDN voor meer informatie over DNSSEC, registers, etc.