# De internetstandaarden

Joep Bär

## Voldoet jouw website daaraan?

Om wereldwijd gegevens tussen verschillende computers te kunnen uitwisselen, zijn internationale afspraken nodig over de manier waarop de computers met elkaar communiceren. Zeg maar de digitale ‘stekkers en stopcontacten’ die alles met elkaar verbinden. Deze afspraken noemen we Internetstandaarden of -protocollen.

Een voorbeeld is SMTP (simple mail transport protocol), een bekend protocol voor het versturen van e-mail. Deze technische kern van internet is voor de meeste gebruikers onzichtbaar en onbekend, maar cruciaal voor de werking van internet vandaag en in de toekomst.

Hoewel Nederland als eerste Europese land in 1988 internettoegang kreeg, loopt het niet voorop met moderne Internetstandaarden. We gebruiken nog te veel verouderde standaarden die tekortschieten in betrouwbaarheid. Het niet gebruiken van moderne standaarden is een risico voor de individuele internetgebruiker, maar ook voor de ‘BV Nederland’ en voor de gehele wereld.

Voorbeeld: vroeger werd alle e-mail zonder versleuteling uitgewisseld tussen je computer en de e-mailprovider. Omdat hierdoor, via aftappen van communicatielijnen, e-mails door anderen gelezen konden worden werd een nieuw protocol ingevoerd: versleutelde e-mailcommunicatie. Beide bestaan nu naast elkaar, net als veel andere oude en nieuwe standaarden. Je moet zelf de versleutelde communicatie instellen in je e-mailprogramma. Zie link 1.

## Waarom is het belangrijk om up-to-date te zijn?

De oorspronkelijke internetstandaarden stammen uit de jaren ´70 en ´80, toen er nog maar weinig internetgebruikers waren. Wereldwijd zijn er inmiddels ruim drie miljard internetgebruikers! Deze mensen gebruiken het internet steeds meer voor privacygevoelige informatie en financiële transacties. De oude standaarden kunnen deze schaalvergroting niet aan en voldoen niet aan de huidige veiligheidseisen.

Criminelen misbruiken de SMTP-standaard om het afzenderadres van een e-mail te vervalsen om phishing mails, nepaanbiedingen en andere ongewenste mails te verzenden. Daarom moeten we dus nieuwe, slimmere standaarden gaan gebruiken die ervoor zorgen dat ons internet betrouwbaar blijft. Deze veiliger en moderne Internetstandaarden zijn beschikbaar! We moeten ze alleen benutten!

## Wat kun je zelf doen?

De eerste reactie zal zijn: mijn provider zorgt toch voor beveiliging!?! Dat klopt voor de internettoegang thuis, maar is slechts deels waar voor je eigen website. Je kunt je provider erop aanspreken, maar dat helpt meestal niet als je een alleen een standaarddienst afneemt. Je kunt natuurlijk wel overstappen naar een provider die e.e.a. ‘beter op de rit’ heeft.

In deze aflevering behandel ik aanpassingen aan je website die je zelf kunt doen. In een volgend artikel neem ik de aanpassingen voor het e-mailverkeer door.

## Welke aanpassingen kun je doen en hoe test je die?

- Gebruik IPv6: is de website bereikbaar via modern internetadres? (link 2)
- DNSSEC: is de domeinnaam ondertekend? (link 3)
- HTTPS: is de verbinding beveiligd? (link 4)
- Beveiligingsopties: zijn de applicatie-beveiligingsopties ingesteld? (link 5)

## Achtergrondinformatie DNS (link 6)

Diverse van de hieronder genoemde aanpassingen kunnen in het Domain Name System (DNS) worden doorgevoerd. Het DNS is de wereldwijde database waarin alle internet diensten van iedere internet aansluiting zijn vastgelegd. Niet alleen welke computer (server) handelt de dienst af, maar ook welke beveiligingen zijn ingeschakeld. En hoe is die computer / server te bereiken.

## Voorbeelden van diensten zijn:

- Op welke server staat welke website;
- Omzetten van de naam van een website naar het IP-adres van de computer waar de website op staat (link 7);
- Welke computer ontvangt de e-mail naar mijn e-mailadres;
- Op welke computer staat mijn e-mail;
- Op welke manier kan ik bestanden versturen naar een specifieke computer.

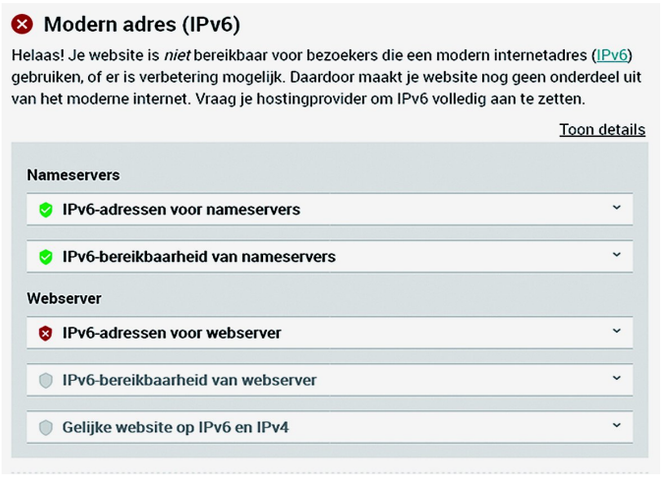
Het DNS is niet één centrale database maar bestaat uit zeer vele databases, waarvan vele bij providers worden onderhouden. Wijzigingen worden continu naar alle aangesloten DNS-databases doorgegeven.

## Test je eigen website

Ga naar https://internet.nl vul de naam van je website in en klik op ‘Start test’. Binnen 200 seconden is het resultaat te zien. Ieder testonderdeel kan aangeklikt worden om uitleg te krijgen over wat ermee wordt bedoeld en vaak hoe eventuele verbeteringen mogelijk zijn.


## Resultaat: modern adres (IPv6)

Een apparaat (computer / server / camera / gadget / …) dat op internet aangesloten is moet bereikt kunnen worden via een adres (een soort huisnummer) dat wereldwijd uniek moet zijn. Er is begonnen met IPv4, de oude standaard. Het aantal adressen (computers) dat hiermee bereikt kan worden is al jaren kleiner dan het aantal apparaten dat via internet is aangesloten. Via IPv6 kan ieder apparaat wereldwijd een uniek adres krijgen.




Deze test geeft aan of IPv6 adressen worden gebruikt. In het DNS zijn de nameservers opgenomen waarin het IPv4 en/of het IPv6 staat. Van beide worden de instellingen onderhouden door de DNS- resp. webserver-providers. Als je zelf een webserver beheert moet het IPv6 adres door jezelf worden ingesteld, net als dat van het IPv4 adres. (link 7)

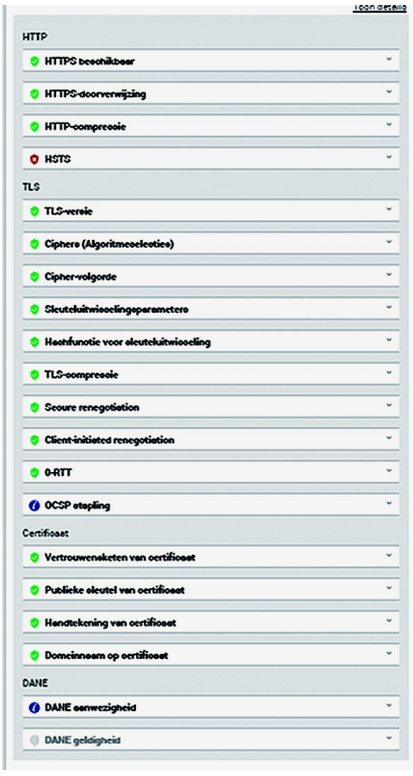

## Resultaat: ondertekende domeinnaam (DNSSEC)

DNSSEC wordt nagenoeg altijd ingesteld door je provider. Ook als je zelf DNS-instellingen kunt aanpassen.

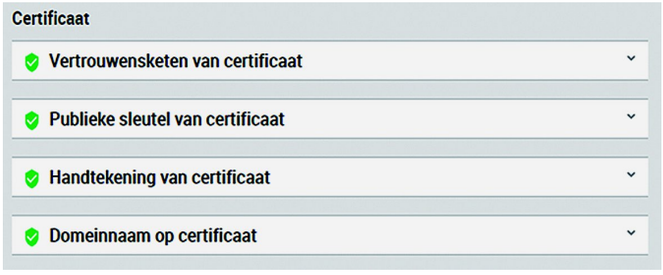
## Resultaat: beveiligde verbinding (HTTPS)

De onderdelen HTTP, op HSTS na, TLS en DANE zijn de verantwoordelijkheid van de provider / degene die de server inricht. HSTS (HTTP Strict Transport Security) ofwel het afdwingen dat de webbrowser bij een volgend bezoek altijd HTTPS moet gebruiken.

Via veel controlpanels voor websites, zoals cPanel, Plesk en DirectAdmin, kan worden ingesteld dat het bezoek altijd via SSL / HTTPS verloopt. Als alternatief kan dit ook via een .htaccess bestand. (link 8)




**Onderdeel certificaat**
Om de website met een beveiligde verbinding (HTTPS) te laten bezoeken moet een SSL-certificaat (via het controlpanel van de website) aan de website worden gekoppeld. Voor eenvoudige websites is een gratis certificaat van Let's Encrypt voldoende. Maar is er meer garantie nodig dat de website van de organisatie is zoals die zich voordoet, dan zal een betaald certificaat nodig zijn. Bijvoorbeeld voor een webwinkel of een multinational.
Soms wordt dit certificaat verzorgd door de provider. Anders kan (meestal) het certificaat via het controlpanel worden ingesteld.




## Resultaat: beveiligingsopties

Dit is het moeilijkste onderdeel: je provider zal en kan dat nagenoeg nooit voor je verzorgen, omdat de instellingen website-afhankelijk zijn. Soms kunnen de instellingen via de website worden ingesteld; diverse Content Management Systemen hebben hiervoor een plug-in of module. Maar het kan altijd via een .htaccess bestand (link 9).

Ik gebruik meestal dezelfde set instellingen via een .htaccess bestand. Deze geef ik hieronder. Controleer via de beschrijving of de instelling voor jouw website aangepast moet worden.


Voor de 'Content-Security-Policy' heb ik geen standaardinstelling. Ik heb wel een policy opgenomen die aangepast kan worden aan de eigen website, en een link naar een website met diverse voorbeelden (link 10).

Daarnaast heb ik nog enkele extra beveiligingsinstellingen opgenomen.

*(Zie het script op de volgende pagina)*

## Tot slot

In een volgend artikel zal ik de test en verbeteringen voor e-mail instellingen beschrijven.

```
<IfModule mod_headers.c>
  Header always set X-Frame-Options SameOrigin
  Header always set X-Content-Type-Options nosniff
  Header set Content-Security-Policy default-src 'none'; script-src 'self'; connect-src 'self';
      img-src 'self'; style-src 'self';base-uri 'self';form-action 'self'

  Header set Referrer-Policy "strict-origin-when-cross-origin"

  # Extra.
  # Disable Proxy header, since it's an attack vector.
  RequestHeader unset Proxy
  Header always set X-XSS-Protection "1; mode=block"
  Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"
  Header set Expect-CT "max-age=86400, enforce"
  Header set Feature-Policy "vibrate 'none'; sync-xhr 'none'; midi 'none'; payment 'none';
      geolocation 'none'; notifications 'none'; push 'none'; microphone 'none'; camera 'none';
      magnetometer 'none'; gyroscope 'none'; speaker 'none'; fullscreen 'none';"
</IfModule>
```

## Links

1. E-mail instellen: **https://www.vimexx.nl/help/email-instellingen-imap-pop3-smtp**
2. IPV6: **https://internet.nl/faqs/ipv6**
3. DNSSEC: **https://internet.nl/faqs/dnssec**
4. HTTPS: **https://internet.nl/faqs/https**
5. Beveiligingsopties: **https://internet.nl/faqs/appsecpriv**
6. DNS: **https://nl.wikipedia.org/wiki/Domain_Name_System**
7. IP-adres: **https://nl.wikipedia.org/wiki/IP-adres**
8. Forceer HTTPS via .htaccess: **https://realhosting.nl/helpdesk/hoe-forceer-ik-ssl-https-in-een-htaccess-bestand**
9. .htaccess bestand maken: **https://www.strato.nl/hosting/htaccess-trucs**
10. Content-Security-Policy: h**ttps://content-security-policy.com/**