Zo Simpel is het Internet

Website eigenaren worden tegenwoordig overspoeld met eisen waar zij aan moeten voldoen. Vaak in onduidelijke vaktaal. Zo'n vraag wordt dan al snel doorgestuurd naar een webontwikkelaar. Thuiswinkel.org en Forus-P bv hebben voor u een overzicht gemaakt van de meest voorkomende vaktermen met een eenvoudige uitleg.

Hoe werkt het internet?

We gebruiken het internet tegenwoordig veel, maar bijna niemand weet hoe 't echt werkt. Als u in de browser bijvoorbeeld naar www.google.nl gaat, verandert het adres naar https://www.google.nl en verschijnt de populaire zoekmachine binnen een paar seconden in beeld. Maar wat gebeurt er op de achtergrond en waarom staat er ineens https:// voor?

Om een idee te krijgen hoe het werkt, vergelijken we het internet even met een post en huisadres. Elke straat heeft een naam, huisnummer en postcode, zoals Industrieweg Oost 21, 6662 NE. Een straatnaam is er alleen voor ons gemak; het is immers lastig voor een postbode om een huis alleen middels een huisnummer en postcode te vinden. Op het internet werkt dat precies hetzelfde. Alleen hier heet de straatnaam een **domeinnaam**. En de combinatie huisnummer en postcode is het **IP-adres (Internet Protocol-adres)**.

IP-adressen

Alle servers, huis- en bedrijfsaansluitingen hebben een publiek IP-adres (postcode en huisnummer). Dit netwerk van publieke IP-adressen noemen we een **WAN (Wide Area Network)**. Een netwerk binnen een huis of bedrijf noemen we een **LAN (Local Area Network)**. Zo'n binnen IP-adres is het unieke adres van uw computer en is alleen zichtbaar voor mensen binnen dit netwerk.

Wanneer we het publieke IP-adres van Google (172.217.17.132) bezoeken, komen we uit op de domeinnaam www.google.com. De domeinnaam is een stuk makkelijker te onthouden dan een IP-adres. Toch zijn ze in feite hetzelfde, www.google.com geeft alleen de inhoud van 172.217.17.132 weer.

Uw computer en u zelf kunnen natuurlijk nooit voor elke website het bijbehorende IP-adres onthouden. Elke keer dat u het adres van een website intypt dat uw computer niet kent wordt er een publiek telefoonboek geraadpleegd, het **DNS (Domain Name Service)**. Dit leggen we later in dit document verder uit. Het eerste telefoonboek dat wordt geraadpleegd wordt vaak door uw **ISP (Internet Service Provider)** onderhouden; er zijn echter ook andere aanbieders zoals Google en 1.1.1.1.

Nieuwe IP-adressen (IPv6)

Op dit moment maken we gebruik van **versie 4 IP-adressen (IPv4)**. De laatste jaren zijn hostingproviders en internet providers, zoals KPN, Ziggo en Tele2, de nieuwere **versie 6 IP-adressen (IPv6)** beschikbaar gaan maken. Dit omdat de combinatie van beschikbare IPv4 adressen op is. Doordat we in een overgangsfase zitten, wordt er vaak een IPv4 én IPv6 adres toegewezen. Dit komt omdat beide versies nog niet compatibel zijn. Wanneer iemand nu dus alleen over een IPv6 adres beschikt, zou deze persoon alleen domeinnamen kunnen bezoeken waaraan ook een IPv6 adres gekoppeld is. Voor de toekomst is het dus van belang dat servers zowel IPv4 als IPv6 ondersteunen.

Voor IPv6 kunt u terecht bij de hostingpartij van uw webserver.

De server

Websites staan opgeslagen op servers. Dit zijn computers met vaak veel opslagruimte die bedoeld zijn om toegankelijk te zijn vanaf het internet. Servers kunnen in zijn geheel worden gehuurd (dedicated hosting) of worden gedeeld met meerdere websites (shared hosting). Doordat servers hun eigen pagina voor het grote DNS-telefoonboek (zie volgende hoofdstuk) aanleveren, is het geen probleem om meerdere websites op één server te hebben staan; de server regelt dit zelf.

Wanneer de server is gevonden in het telefoonboek, ontvangt uw computer het IP-adres wat bij de domeinnaam hoort. Uw computer legt dan een verbinding met de server en vraagt daar naar de website. De server stuurt de website dan in kleine pakketjes naar uw computer. De pakketten zijn opgedeeld in hele kleine stukjes zodat deze sneller verstuurd en geladen kunnen worden. Wanneer er één of meerdere pakketten niet juist ontvangen worden, kunnen deze makkelijk en snel opnieuw verstuurd worden.
Uw computer plakt de pakketten aan elkaar zodat de website één geheel wordt.

DNS

Voor alle domeinnamen hebben we een online telefoonboek, dit heet **DNS (Domain Name System)**. DNS zet de domeinnaam, die u in de browser typt, automatisch om naar een IP-adres. DNS-servers zijn door grotere organisaties onderhouden servers; zonder DNS zou het internet niet meer werken.

Elk domeinnaam heeft eigen DNS-records die publiekelijk toegankelijk zijn. Deze DNS-records laten via een bepaald protocol weten naar welk IP-adres wordt doorverwezen. Zo weten browsers naar welke website ze moeten. In deze DNS-records worden ook doorverwijzingen bekend gemaakt naar e-mail en een aantal andere zaken, zoals SPF en DMARC, welke later in dit document worden uitgelegd.

Elke computer heeft een **eigen geheugen (DNS-cache)** waarin de combinatie van website en server wordt opgeslagen. Hiermee wordt het opvragen van een website versnelt. Wanneer een domeinnaam nog niet in het eigen geheugen voorkomt, wordt er bij een DNS-server gevraagd naar de juiste combinatie.

DNSSEC

Het DNS-protocol verstuurt de gegevens onbeschermd en heeft een aantal bekende kwetsbaarheden. Over het algemeen levert dit geen problemen op, maar er zijn gevallen waarin deze kwetsbaarheden zijn misbruikt.

DNSSEC (Domain Name System Security Extensions) is een uitbreiding op het DNS en verhelpt een aantal kwetsbaarheden. Hierdoor wordt de 'bewegwijzering' van het internet veiliger en betrouwbaarder. DNSSEC is een server instelling en kan door uw hostingpartij worden geregeld.

Voor DNSSEC kunt u terecht bij de hostingpartij van uw webserver of bij de partij die uw domeinnaam beheert, vaak is dit dezelfde partij.

HTTP

Het internet werkt doordat hele kleine pakketten met data, waaronder stukjes afbeeldingen, tekst, wachtwoorden en creditcardnummers, worden geïnterpreteerd en omgezet naar bruikbare informatie. En door zo'n pakket te voorzien van de IP-adressen van de verzender en de ontvanger kan er over en weer gecommuniceerd worden. Het protocol waarmee data wordt verzonden heet **HTTP (Hypertext Transfer Protocol)**.

HTTPS

De huidige versie van het HTTP-protocol heeft zijn laatste update in 2015 gehad en data werd toen niet versleuteld.

De beveiligde versie van HTTP voegt een S toe, wat staat voor 'Secure'. **HTTPS (Hyper Text Transport Protocol Secure)** versleutelt de verstuurt data (beide kanten op) en garandeert de integriteit van de verzonden en ontvangen data. Door deze beveiligde verbinding kan niemand anders dan de ontvanger de data lezen. Voor de werking van HTTPS is het nodig een certificaat toe te wijzen aan de domeinnaam/server. Dit **SSL-certificaat (Secure Sockets Layer)** kan bij verschillende organisaties worden aangevraagd en is tegenwoordig ook gratis te verkrijgen. Hierbij worden er controles gedaan om te verifiëren dat de aanvrager ook daadwerkelijk bevoegd is op die domeinnaam/server. Er zijn verschillende soorten certificaten, waarbij de meest simpele, **Domain Validation**, voldoet.

Sinds een aantal jaar zijn we over op **TLS (Transport Layer Security)**. Dit is de opvolger van **SSL**. In de volksmond en onder IT'ers wordt TLS vaak nog SSL genoemd, terwijl dit feitelijk onjuist is.

Voor TLS (SSL) kunt u terecht bij uw webontwikkelaar en/of uw hostingpartij.

E-Mail

Het is bijzonder eenvoudig om een e-mail vanaf een vervalst afzenderadres te versturen. Een internetgebruiker zal niet door hebben dat de mail die hij/zij zojuist heeft ontvangen eigenlijk een phishing-bericht is. Het afzenderadres ziet er vaak echt uit. Pas bij grondiger onderzoek zal blijken dat deze e-mail helemaal niet bij deze instelling vandaan komt, maar er juist een kwaadwillende partij achter zit die probeert achter waardevolle gegevens te komen. Om het e-mailverkeer veiliger te maken, is er een aantal nieuwe beveiligingsstandaarden bepaald: SPF, DKIM en DMARC.

SPF

SPF (Sender Policy Framework) is een anti-spam toepassing voor e-mail gebruik. Deze kijkt of de server die de e-mail verzendt ook daadwerkelijk geautoriseerd is om dat vanaf die domeinnaam te doen. Dit gebeurt door de DNS-instellingen van die domeinnaam te bevragen. Als de versturende mailserver niet in het SPF-record van de domeinnaam is opgenomen, zal de e-mail vanaf deze server direct als verdacht worden aangemerkt. De ontvangende partij heeft dan de mogelijkheid om e-mails toe te laten, in 'quarantaine' te plaatsen of simpelweg tegen te houden.

DKIM

DKIM (DomainKeys Identified Mail) lijkt sterk op SPF maar is op zichzelf geen anti-spam toepassing. DKIM wordt gebruikt om de echtheid van een e-mail bericht te waarborgen. Iemand die DKIM gebruikt kan een e-mailbericht ondertekenen met een hash (uitkomst van een wiskundige berekening ter waarborging van de authenticiteit). Hierdoor kan de ontvanger zien dat het verzonden bericht onderweg niet is aangepast. Het gebruiken van DKIM vermindert de kans dat e-mail van een persoon of organisatie als spam wordt bestempeld.

DMARC

DMARC (Domain-based Message Authentication, Reporting & Conformance) geeft aan wat de ontvangende mailserver met de ontvangen e-mail moet doen als deze niet door de SPF- of DKIM-test komt. De verzendende partij geeft in zijn DNS aan wat er moet gebeuren als een e-mail geen DKIM handtekening bevat of wanneer de verzendende server niet in het SPF staat. Hierdoor heeft de verzendende partij meer controle over het gebruik van hun domeinnaam.

Voor SPF, DKIM en DMARC kunt u terecht bij de hostingpartij van uw mailserver en bij de partij die uw domeinnaam beheert.

Support

Omdat het gebruik van veilige standaarden bijdraagt aan een hogere veiligheid en consumentenvertrouwen, vinden we het belangrijk hier aandacht aan te schenken.

Daarom verzoeken we uw website en e-mail na te kijken en deze standaarden door uw hosting provider te laten instellen. Mocht u hierbij problemen ondervinden, laat dit dan weten via support@forus-p.com met vermelding van uw hosting partij, contactpersoon en telefoonnummer, zodat Forus-P bv contact met hen op kan nemen.

Zelf een test uitvoeren

Om zelf een test uit te voeren, gaat u naar https://www.internet.nl waar u uw domeinnaam kunt invoeren. Ook kunt u daar uw e-mail beveiliging testen. Uw website en e-mail worden op de volgende onderdelen getest:

- Verbinding voldoende beveiligd (HTTPS/TLS (SSL))
- Domeinnaam ondertekend (DNSSEC)
- Aanwezigheid van veilige e-mail standaarden DMARC, DKIM, SPF en (start)TLS

Contact

Voor support en/of meer informatie kunt u contact opnemen met:

Forus-P bv
T: +31 481 377265
E: support@forus-p.com
W: https://forus-p.com