Technische Universiteit
Eindhoven

0K830 Recht, techniek, samenleving 4

www.domeinnaam-problematiek.com

A. Engelfriet (383104)
J. Claassens (417762)
E. Jans (405607)

Begeleiders:

1. Prof. dr. ir. J.M. Smits
2. Mr. drs. E.F. Clarkson

November 1997

Voorwoord

Op de Technische Universiteit Eindhoven wordt het vak Actualiteiten Recht, Techniek en Samenleving gedoceerd. In dit vak wordt er door de studenten een actueel maatschappelijk en informatietechnisch probleem bestudeerd. Van dit probleem worden allerlei aspecten bekeken, met een nadruk op de juridische en technische aspecten.

Dit jaar, september 1997, is ervoor gekozen om de problematiek betreffende domeinnamen in kaart te brengen. De auteurs leggen de nadruk op de technische en juridische problemen.

Het werken aan dit project is door de auteurs ervaren als zeer leerzaam en heeft echter wel de nodige zweetdruppels opgeleverd. Vooral het werken in teamverband en de manier waarop een project moet worden aangepakt is erg leerzaam, want hier zal men later in de werksituatie ook geregeld mee te maken krijgen.

de auteurs *Eindhoven, november 1997*

Jurgen Claassens,
Arnoud Engelfriet,
Erik Jans.

Inhoudsopgave

Inleiding

Dit rapport biedt een kort overzicht van de verschillende aspecten van de domeinnaam-problematiek, met de nadruk op de juridische en technische aspecten. Vanwege de beperkte tijd kunnen helaas niet alle aspecten besproken worden, wij hebben daarom een keuze moeten maken.

In hoofdstuk 1 wordt eerst de geschiedenis van het Domain Naming Systeem besproken en de manier waarop dit functioneert. Als voorbeeld is hierin uitgewerkt hoe bij een naam een adres wordt opgezocht. Hoofdstuk 2 bespreekt hoe domeinnamen geregistreerd kunnen worden, bij wie en onder welke voorwaarden.

In hoofdstuk 3 worden enkele technische problemen die spelen bij domeinnamen besproken. Hieronder vallen zowel problemen bij de implementatie en het gebruik van de software, als problemen veroorzaakt door de enorme groei van het aantal domeinnamen.

De juridische conflicten over domeinnamen worden in hoofdstuk 4 besproken. In dit hoofdstuk staan onder andere enkele voorbeelden van dit soort conflicten.

Voor de problemen en conflicten uit hoofdstuk 3 en 4 zijn natuurlijk oplossingen voorgesteld. Oplossingen die door de WIPO en het IAHC zijn voorgesteld, worden in hoofdstuk 5 besproken. In dit hoofdstuk worden ook enkele oplossingen besproken die door ons zelf voorgesteld worden.

Het laatste hoofdstuk bevat de conclusies en aanbevelingen bij het door ons uitgevoerde onderzoek, alsmede enkele kanttekeningen.

1

Wat is het Domain Naming System?

1.1 Het gebruik van domeinnamen

Elke computer die aangesloten is op het Internet is uniek bekend door zijn zogeheten *IP-adres*. Dit adres is een 32-bits getal, dat meestal wordt geschreven in vier groepjes, gescheiden door punten. Een voorbeeld is `131.155.140.135`. In de volgende versie van het Internet Protocol [8] worden deze adressen 128 bits lang. Dit is noodzakelijk om de groei van het aantal computers op het Internet bij te kunnen houden.

Het gebruik van nummers is weliswaar efficient, maar voor mensen erg onpraktisch. Om die reden werd al vanaf het begin gebruik gemaakt van namen waarmee een computer aangeduid kon worden. Het protocol waarmee deze namen beheerd worden heet het *Domain Naming System* (DNS).

1.2 Geschiedenis van het Domain Naming System

1.2.1 Het vroegere naamsysteem

Oorspronkelijk was de beheerder van elke computer die op het netwerk aangesloten was vrij om elke naam te kiezen. De registratie van namen was centraal. Iedere systeembeheerder kopieerde regelmatig de officiële lijst van namen en de bijbehorende adressen van een centrale computer (deze stond bij het Stanford Research Institute in California). Deze lijst stond bekend als `hosts.txt` (het formaat hiervan staat beschreven in Request For Comments 810 [2]) of ook wel “de `/etc/hosts` file”, naar de naam van het bestand waar de lijst op de meeste computers in bewaard werd.

De initiële opzet was strikt globaal. Voor elke computer werd een unieke naam gebruikt, waarmee hij op het hele netwerk herkenbaar was. Deze namen werden bijvoorbeeld gebruikt in het zogeheten “UUCP” protocol om e-mail te versturen. De route van een e-mail bericht kon daarin gegeven worden als een lijst van computers, zoals bijvoorbeeld `alpha!beta!gamma!john`, waarbij “john” de ontvanger is op computer “gamma”, “alpha” de verzendende computer is en “beta” de computer die deze twee met elkaar verbindt.

Het nadeel van deze aanpak was dat naarmate het aantal aangesloten computers groeide, het moeilijker werd om een globaal unieke naam te kiezen. In 1983 werd daarom het concept van “domeinen” geïntroduceerd (in RFC 881 [6]). De nieuwe opzet werd hiërarchisch van aard. Men begon met alleen het `arpa` domein, maar dit werd later uitgebreid (zie paragraaf 1.3.1).

Een tweede probleem, dat ongeveer in dezelfde tijd begon te ontstaan, was dat de centrale lijst van namen en bijbehorende adressen te hard groeide. Het aantal aanpassingen, toevoegingen en verwijderingen maakte het onmogelijk voor een systeembeheerder om continu up-to-date te zijn. Ook het doorzoeken van deze lijst (georganiseerd als een platte lijst, met één regel per naam/adres-combinatie) werd onpraktisch.

1.2.2 Ontwikkeling van het DNS

Het Domain Naming System, meestal aangeduid als DNS, was ontworpen om aan deze problemen een einde te maken. Dit systeem werd ontwikkeld in 1983 en 1984, maar het duurde tot eind jaren tachtig voordat alle aangesloten systemen overgestapt waren.

De belangrijkste eigenschappen van DNS zijn: [4]

- Een hiërarchische structuur voor namen.
- Een protocol-onafhankelijke manier om computers aan te duiden.
- Een gedistribueerde database in plaats van een gecentraliseerde lijst.
- De mogelijkheid om informatie over een naam op te vragen.

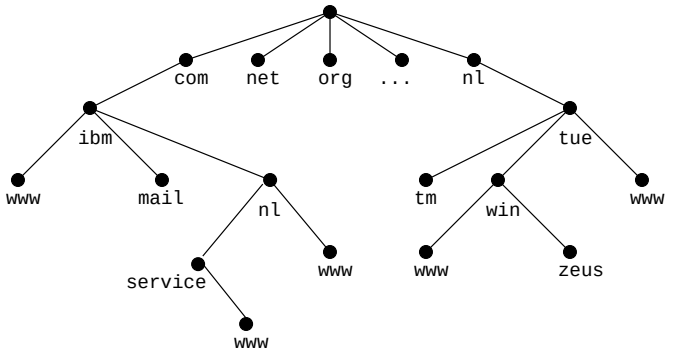
Het belangrijkste verschil is dat er nu op diverse plaatsen in het netwerk zogeheten "nameservers" (zie paragraaf 1.4.1) zijn. Deze kennen namen en adressen van een gedeelte van het netwerk en wisselen deze met elkaar uit.

1.3 De opzet van het DNS

Zoals hierboven is besproken, is het DNS opgezet volgens een hiërarchische structuur. In plaats van namen van computers wordt nu, zoals de naam al aangeeft, gewerkt met *domeinen*.

1.3.1 Wat is een domein?

De hiërarchie binnen DNS wordt meestal weergegeven in een boomstructuur. Een knoop in deze structuur heet een *domein*. Elk domein heeft een naam die bestaat uit een uniek voorvoegsel, gevolgd door een punt en daarna de naam van het direct er boven liggende domein.



Figuur 1.1: De boomstructuur van DNS

Door langs een tak naar beneden[1] te lopen kan men nagaan wat de plaats in de hiërarchie is van een bepaalde organisatie of computer. De afbeelding hiernaast[2] illustreert dit. De naam van de knoop "zeus" is dus `zeus.win.tue.nl`.

Een domein heeft een naam van maximaal 63 tekens en mag alleen bestaan uit letters, cijfers en koppelstreepjes [4]. Hoofd- en kleine letters maken geen verschil; de conventie is om domeinnamen te noteren met alleen kleine letters. Zo is bijvoorbeeld `tue` de naam van het domein van de Technische Universiteit Eindhoven.

Een blad in deze boomstructuur is meestal de naam van een fysieke computer die op het Internet is aangesloten. Er wordt dan niet gesproken van "domeinnaam" maar van "hostnaam".

In principe kan de naam van een domein relatief ten opzichte van elk bovenliggend domein genomen worden. Een naam is *absoluut* of *Fully Qualified* wanneer hij niet relatief ten

[1] In tegenstelling tot biologen tekenen informatici bomen altijd met de wortel boven en de takken naar beneden.
[2] De fictieve situatie in deze afbeelding zal in de rest van de tekst worden gebruikt als voorbeeld.

opzichte van een of ander domein genomen wordt. De naam eindigt dan op een punt. In het voorbeeld van figuur 1.1 is de naam `www.win.tue.nl.` dus absoluut. De naam `win` is relatief ten opzichte van het domein `tue.nl.` en wordt ook wel het "*subdomein* `win` binnen domein `tue.nl.`" genoemd.

Vaak worden absolute namen genoteerd zonder punt op het einde, omdat het uit de context duidelijk is dat de namen absoluut zijn. Dit kan echter problemen opleveren (zie paragraaf 3.1.2) en het opzoeken van informatie bij de naam vertragen (zie paragraaf 1.4.2).

Het *root*-domein

Het *root*-domein is de top in de boom van het DNS. Dit domein heeft geen naam. Een absolute naam (ook wel *Fully Qualified Domain Name* of FQDN geheten) is dus eigenlijk relatief ten opzichte van het *root*-domein. Omdat de punt wordt gebruikt om namen van knopen van elkaar te scheiden en het *root*-domein geen naam heeft, eindigt een FQDN dus op een punt. Vaak wordt hierom geclaimd dat de naam van het *root*-domein dus "." is, maar dit is incorrect.

Top-level domeinen

Direct onder het *root*-domein bevinden zich de zogeheten *top-level* domeinen. Deze maakt gebruik van een classificatie naar zowel functie als naar geografische lokatie per land. Deze classificatie werd voorgesteld in RFC 920 [7]. De hierin gegeven definities voor functionele top-level domeinen zijn inmiddels wat veranderd. Onderstaande lijst geeft de huidige interpretatie.

`com` Dit domein wordt gebruikt voor commerciële instanties. Oorspronkelijk was dit bedoeld ter identificatie van het domein van bedrijven zelf, maar tegenwoordig wordt het gebruikt voor vrijwel alles dat maar enigszins met commercie te maken heeft.

`net` Dit domein was oorspronkelijk bedoeld voor instellingen die informatie aanbieden die nodig is voor het functioneren van het Internet. Tegenwoordig wordt dit ook wijder geïnterpreteerd en kunnen allerhande organisaties die (meestal uit ideële motieven) informatie aanbieden van dit domein gebruik maken.

`org` Dit domein was oorspronkelijk bedoeld voor alle organisaties die niet onder een van de andere definities vielen, maar het wordt nu gebruikt voor alle niet-commerciële organisaties.

`int` Dit domein is bedoeld voor internationale organisaties, dat wil zeggen organisaties die zich niet alleen op de VS richten.[3]

`edu` Deze naam wordt gebruikt voor onderwijsinstellingen in de VS. Tegenwoordig is dit beperkt tot universiteiten en ander hoger onderwijs.

`mil` Alleen voor gebruik door defensie-instellingen van de VS. Deze instellingen zijn nu grotendeels "los" van het Internet, maar toen dit systeem werd opgezet, was het aantal overheids- en defensie-instellingen veel groter. Deze naam is een overblijfsel uit de tijd van het ARPAnet (het netwerk opgezet door het Advanced Research Project Agency, een onderdeel van het ministerie van defensie van de VS).

`gov` Deze naam wordt gebruikt voor instellingen binnen de federale overheid van de VS. Nationale instellingen moeten gebruik maken van het `us` domein, dat verder ingedeeld is per staat (zie onder).

[3] Amerikanen hebben nog wel eens problemen met het concept van "wereldwijd."

`arpa` Dit domein werd geïntroduceerd in de overgangsfase van platte naar hiërarchische structuur. Het werd gebruikt om alle platte namen binnen de hiërarchie te kunnen plaatsen, door ze in het `arpa` domein op te nemen. Op dit moment bestaat alleen het `in-addr.arpa` domein nog (zie paragraaf 1.4.4 voor een beschrijving van het doel hiervan).

Deze classificatie kent een nogal sterke bias voor instanties binnen de VS. Dit is eenvoudig te verklaren, aangezien er op het moment van ontwerpen nog vrij weinig aansluitingen uit andere landen waren. Met uitzondering van de `edu`, `mil` en `gov` domeinen mogen bovenstaande domeinen door organisaties over de hele wereld gebruikt worden.

Naast bovengenoemde functionele domeinnamen bestaan er ook domeinen voor elk land ter wereld. Deze domeinnamen zijn gebaseerd op de landencodes uit ISO 3166 [3], met één uitzondering. Het Verenigd Koninkrijk van Groot-Brittannië wordt aangeduid met `uk` en niet met het in deze standaard vereiste `gb`.[4]

1.3.2 Naamgeving van verdere domeinen

Een organisatie is vrij om binnen het voor haar meest geschikte top-level domein een naam te kiezen. De regels hiervoor hangen af van het top-level domein dat wordt gebruikt. Hoofdstuk 2 geeft de regels binnen het domein van Nederland. Het `us` domein, al eerder genoemd, kent een subdomein voor elke staat binnen de VS. Elke staat deelt haar domein weer verder in, meestal ook op staatkundige basis (provincies, steden, lokale overheid, enzovoorts).

De regels voor subdomeinen binnen het domein van een organisatie mogen door die organisatie zelf vastgesteld worden. Een indeling op basis van functie of departement binnen de organisatie ligt voor de hand.

Wanneer een computer die op het Internet is aangesloten een bepaalde dienst verleent (zoals bijvoorbeeld een WWW-server, een mail server, een login machine of een gateway), is het handig om hiervoor een standaard naam te gebruiken. Door deze conventie is het mogelijk om makkelijk te onthouden wat b.v. de naam is van de WWW-server van IBM (`www.ibm.com`). Dit is echter geen verplichting!

Meestal is deze naam een “bijnaam” en niet de echte naam van de computer. Hierdoor is het mogelijk om de service te verplaatsen naar een andere computer zonder dat de rest van de wereld hier iets van merkt. Er hoeft slechts één instelling te worden veranderd.

1.3.3 Informatie over een domein

Alhoewel tot nu toe steeds is gesproken over de mogelijkheid om bij een naam een adres op te zoeken, kan DNS meer. Het systeem is ontworpen om bij een gegeven naam zogeheten *Resource Records* (RRs) te kunnen leveren. De mogelijke soorten informatie die in RRs kunnen worden aangeboden, zijn gegeven in RFC 1035 [5]. De belangrijkste zijn:

NS (Nameserver) - Geeft het adres van de nameserver (zie 1.4.1) voor het domein.

A (Address) - Geeft het adres voor de naam van dit domein.

CNAME (Canonical name) - Geeft de echte naam van dit domein. Hiermee kunnen meerdere namen (aliassen) worden gebruikt voor één domein.

MX (Mail eXchange) - Geeft de naam van een mail server van dit domein. Om e-mail bij een bepaald systeem af te leveren, kan de verzendende computer dus het MX record opvragen van het domein van de ontvanger om te zien aan welke computer de post doorgegeven moet worden.

[4] De discussie over deze keuze was lang en heftig, mede gezien de status van Noord-Ierland, dat zich wel in het Verenigd Koninkrijk bevindt, maar niet in Groot-Brittannië.

TXT (Text) - Kan elke tekst bevatten. Dit kan gebruikt worden om bijvoorbeeld contactinformatie beschikbaar te stellen.

De mogelijkheid om een alias te definiëren voor een domein wordt vooral gebruikt voor computers die diensten aanbieden. Hierdoor is het mogelijk om die dienst te verhuizen naar een andere computer zonder dat de rest van de wereld haar verwijzingen moet aanpassen. Er hoeft alleen één wijziging gemaakt te worden in het CNAME RR voor het betreffende domein.

1.3.4 Domeinen en zones

Voor het beheer van adres- en overige informatie is de indeling in domeinen vaak te veel. Dit zou betekenen dat elk domein, ook wanneer er slechts enkele computers in dat domein aanwezig zijn, deze informatie zou moeten hebben en aan de wereld kunnen aanbieden. Omdat dit erg onpraktisch is, wordt gewerkt met zogeheten *zones*.

Een zone omvat één of meer domeinen en beschikt over een centraal punt waar informatie over alle domeinen die in die zone liggen op te vragen is. Dit is de zogeheten *nameserver* (zie paragraaf 1.4.1) voor de zone. Meestal zijn er twee nameservers per zone, de primaire en de secundaire. De primaire nameserver heeft toegang tot de database met resource records voor de zone, de secundaire niet. Deze laatste server dient dan ook als backup wanneer de primaire nameserver overbelast is of tijdelijk niet functioneert.

1.3.5 De relatie tussen een domeinnaam en een IP-adres

Er is geen vaste relatie tussen een domeinnaam en een IP-adres. De beheerder van de nameserver voor die domeinnaam kan elk adres invullen in het A record van dat domein. Hierdoor is het mogelijk dat één nameserver voor meerdere netwerken werkt. Ook “verhuizen” naar een andere provider is eenvoudig; de oude provider verwijdert de regel voor het domein uit zijn nameserver database, en de nieuwe voegt er een toe.

1.4 Hoe functioneert het DNS?

1.4.1 De nameservers

Binnen een zone fungeren zogeheten *nameservers* als het centrale aanspreekpunt voor informatie. Zij kunnen *queries* of verzoeken beantwoorden en beschikken over de Resource Records voor “hun” zone. Daarnaast bewaren nameservers vaak informatie die zij van andere nameservers ontvangen, om toekomstige queries sneller af te kunnen handelen. Dit staat bekend als “caching”.

Het bekendste programma voor nameservers heet BIND en is ontwikkeld door Kevin Dunlap in 1985. Voor meer informatie over dit pakket wordt verwezen naar het boek *DNS and BIND* [1].

Verreweg de belangrijkste nameservers zijn wel de “root nameservers”, die het root domein en de top-level domeinen in hun zone hebben. Wanneer deze servers niet functioneren, is het onmogelijk om welke naam dan ook op te zoeken buiten de eigen zone.

1.4.2 Absolute en relatieve domeinnamen

Een absolute domeinnaam is een naam die gegeven wordt inclusief het root domein. De naam eindigt dan dus op een punt. In alle andere gevallen wordt de naam beschouwd als een relatieve domeinnaam.

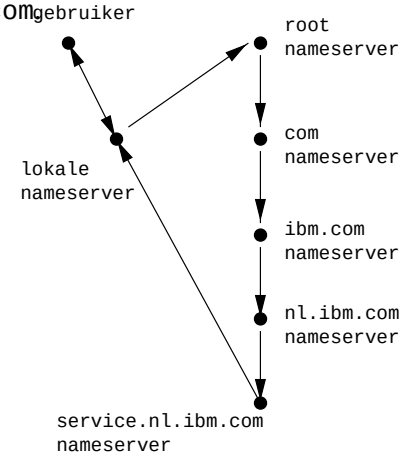
Om de gebruiker typewerk te besparen, is het vaak mogelijk om namen binnen hetzelfde domein als waar de gebruiker zich bevindt op te geven zonder de volledige naam te hoeven geven. In het eerder gegeven voorbeeld zou bijvoorbeeld een gebruiker op `zeus.win.tue.nl.` de naam `www` kunnen gebruiken om `www.win.tue.nl.` aan te duiden.

Deze naam wordt “vertaald” naar een absolute naam (een FQDN) door een aantal opgegeven domeinen achter de opgegeven naam te plaatsen. Dit noemt men vaak de “zoekdomeinen” of “default domains”. In het voorbeeld is dus `win.tue.nl` een zoekdomein, maar ook `tue.nl` of zelfs `nl` zou dit kunnen zijn. Dit laatste is overigens niet verstandig, aangezien het de mogelijkheid biedt tot “domeinkaping”. Zie paragraaf 3.1.2 voor een meer volledige bespreking van dit probleem.

Het gebruik van een groot aantal zoekdomeinen kan het opzoeken van informatie bij een naam vertragen; immers, alle zoekdomeinen moeten worden getest. Wanneer de naam een FQDN is, maar zonder punt wordt gegeven, worden *alle* zoekdomeinen zonder resultaat geprobeerd. Pas daarna zal de naam zelf worden opgezocht. Het toevoegen van een punt kan dus een behoorlijk verschil maken!

1.4.3 Opzoeken van een IP-adres bij een naam

Stel dat een gebruiker van computer `zeus.win.tue.nl` het adres wil weten van computer `www.service.nl.ibm.com`. Deze gebruiker zal dan zijn applicatie een *query* laten doen bij de nameserver van de `win.tue.nl` zone (aangezien dat de zone is waarin zijn computer zich bevindt). Deze nameserver zal nu het adres proberen op te zoeken. Het antwoord wordt (meestal binnen een minuut) teruggegeven aan de applicatie. Dit is een zogeheten *iterative query*.



Figuur 1.2: Een recursieve query

Om het antwoord te kunnen geven, zal de nameserver eerst controleren of de gevraagde naam binnen zijn zone valt. Als dit zo is, kan hij direct antwoord geven. Anders moet hij de query doen bij de nameserver van de zone waarin de gevraagde naam zich bevindt. Om dit uit te vinden worden de volgende stappen gevolgd:

1. Door een query te doen aan een root nameserver wordt achterhaald welke nameserver verantwoordelijk is voor het top-level domein van de gevraagde naam. In dit voorbeeld zal de betreffende root nameserver als antwoord het adres van de nameserver voor het `.com` TLD geven.

2. Aan deze nameserver wordt vervolgens gevraagd welke nameserver het domein `ibm.com` beheert.

3. Vervolgens wordt aan de nameserver van het domein `ibm.com` gevraagd wie verantwoordelijk is voor de zone waarin het gevraagde domein ligt. Dit kan deze server zelf zijn, maar ook een andere. In het laatste geval wordt doorverwezen naar de nameserver voor de betreffende zone. In dit voorbeeld nemen we aan dat de Nederlandse afdeling van IBM haar eigen nameserver heeft. De nameserver van `ibm.com` weet niet of de subdomeinen binnen `nl.ibm.com` hun eigen zones hebben en verwijst dus door naar de nameserver van het `nl.ibm.com` domein.

4. De query wordt vervolgens bij deze nameserver ingediend. Als we aannemen dat de service-afdeling van IBM Nederland ook haar eigen nameserver heeft, worden we nu nogmaals doorverwezen.

5. Uiteindelijk komen we dan terecht bij de nameserver voor de zone waarin `www.service.nl.ibm.com` zich bevindt. Deze geeft het adres van deze host (of meldt dat deze niet bestaat) en de query is beantwoord.

Het kan nodig zijn dat stap 4 meerdere malen gemaakt wordt, wanneer de hiërarchie erg groot is. Dit proces staat bekend als een *recursive query*. Figuur 1.2 illustreert waarom.

In het bovenstaande is voor het gemak weggelaten dat een nameserver informatie over een ander domein kan leveren. Dit maakt voor de te volgen procedure niets uit. Zie paragraaf 1.4.5 voor een uitleg over dit zogeheten “cachen”.

1.4.4 Opzoeken van een naam bij een IP-adres

Het DNS-systeem is ontworpen om gemakkelijk bij een naam een adres op te kunnen zoeken. De enige manier om bij een adres een naam terug te kunnen vinden is hierin het doorzoeken van de volledige boom, want computers binnen hetzelfde domein kunnen totaal verschillende adressen hebben.

Aangezien dit nogal onpraktisch is, is er een andere oplossing verzonnen. Er is een speciaal domein geïntroduceerd: `in-addr.arpa`. In dit domein bevinden zich alle IP-adressen. De notatie is precies omgekeerd aan de normale manier: het IP-adres 131.155.140.135 heeft domein `135.140.155.131.in-addr.arpa.`

Om nu bij een IP-adres een naam op te zoeken, wordt dezelfde procedure gebruikt als bij een “normale” query. Namen van computers kunnen nu met dezelfde DNS-software worden bijgehouden voor elk “domein”, dat wil zeggen, elk IP-adres en elk netwerk.

1.4.5 Hergebruik van zoekresultaten

Om het netwerk niet nodeloos te belasten, kan een nameserver eerder ontvangen informatie onthouden. Zo zal het bijvoorbeeld vanwege het grote aantal domeinen binnen het `.com` toplevel domein vaak voorkomen dat een nameserver moet opzoeken wie de nameserver voor dit domein is. Als deze informatie een maal opgevraagd wordt en vervolgens lokaal onthouden wordt, scheelt dat de volgende keren een hoop tijd en worden de root nameservers minder belast.

Ook kunnen een aantal namen en adressen lokaal opgeslagen worden, zodat de volgende client die het adres bij die naam wil weten direct antwoord kan krijgen. Deze informatie wordt slechts tijdelijk bewaard, meestal 1 dag lang.

Er ontstaat nu wel een probleem. Immers, elke nameserver zou nu antwoord kunnen geven op elke query, door zogenaamd een gecached stuk informatie te sturen. Om dit te voorkomen, wordt onderscheid gemaakt tussen “authoritative” en “non-authoritative” antwoorden. Wanneer een nameserver informatie over een andere zone in zijn cache opslaat, en deze informatie later gebruikt, is deze informatie gemarkeerd als “non-authoritative”. Alleen informatie over de eigen zone kan als “authoritative” worden aangemerkt.

Literatuur

[1] P. Albits and C. Liu. *DNS and BIND.* O'Reilly & Associates, 1997.

[2] E. Feinler, K. Harrenstien, Z. Su, and V. White. *DoD Internet Host Table Specification*. RFC 810, 1982.

[3] ISO. *Codes for the Representation of Names of Countries.* ISO-3166, International Standards Organization, 1981.

[4] P.V. Mockapetris. *Domain names - concepts and facilities*. RFC 1034, 1987.

[5] P.V. Mockapetris. *Domain names - implementation and specification*. RFC 1035, 1987.

[6] J. Postel. *Domain names plan and schedule.* RFC 881, 1983.

[7] J. Postel and J. Reynolds. *Domain requirements.* RFC 920, 1984.

[8] Dr Feit Sidnie. *TCP/IP : Architecture, Protocols, and Implementation With IPv6 and IP Security*. McGraw-Hill Series on Computer Communications, 1996.

2

Het aanvragen van een domeinnaam

Zoals in hoofdstuk 1 te lezen valt worden op het Internet domeinnamen gebruikt om computers te identificeren. In dit hoofdstuk wordt besproken hoe de registratie en aanvraag van domeinnamen verloopt, zowel nationaal en internationaal.

2.1 Algemene procedure

Er zijn verschillende soorten top-level domeinen voor domeinnamen, men kan ze in twee groepen indelen: (zie paragraaf 1.3.1)

- De functionele top-level domeinen,
- De geografische top-level domeinen.

De aanvraag voor een geografisch top-level domein dient men in het corresponderende land in te dienen. Elk land heeft een organisatie die de domeinnamen met een landencode-TLD uitdeelt. Deze organisatie zet de verwijzingen naar een domein in haar nameserver. In Nederland worden de domeinnamen uitgedeeld en geregistreerd door de Stichting Internet Domeinregistratie Nederland (zie paragraaf 2.2).

De top-level domeinen worden door één organisatie uitgegeven. Indien men een domeinnaam wil met als top-level domein `.com`, `.org`, `.gov`, `.net` of `.edu`, dient men het Amerikaanse bedrijf InterNIC te consulteren (zie paragraaf 2.3).

2.2 Aanvragen domeinnaam in Nederland

Zoals al gezegd is, worden domeinnamen met als TLD `.nl` (bijvoorbeeld `philips.nl` of `tue.nl`) door de *Stichting Internet Domeinregistratie Nederland* uitgedeeld. Deze domeinnamen worden echter niet rechtstreeks aan particulieren verstrekt. Het verkrijgen van een domeinnaam dient te gaan via een provider.[1]

Er zijn een aantal regels waar een aanvrager aan moet voldoen voordat een provider een domeinnaam verstrekt. Deze regels zijn opgesteld door de stichting.[2] De volgende eisen worden gesteld:

- De aanvrager dient ingeschreven te staan bij de Kamer van Koophandel.
- De aanvrager dient het recht op de domeinnaam aan te tonen (moet overeen stemmen met merk of handelsnaam van de aanvrager).
- De aanvrager dient de provider en de Stichting Internet Domeinregistratie Nederland te vrijwaren van inbreuk op eventuele rechten van derden.

[1] Deze provider participeert in de stichting en betaalt hier elk jaar een bedrag voor.

[2] Dit zijn de meest recente voorwaarden, zij dateren van 14 oktober 1996. De voorwaarden zijn te vinden op `http://www.domain-registry.nl/nieuwreg.html`

- Het is niet toegestaan om algemene namen of gereserveerde woorden als domeinnaam te gebruiken ook al stemt dit overeen met een eigen merk of handelsnaam. Algemene namen zijn bijvoorbeeld woorden als “aardappel” en “adel”.[3] Gereserveerde woorden zijn woorden als “bbs” en “homepage.”[4]

Als technische voorwaarde wordt gesteld dat er twee computers dienen te zijn die als nameserver kunnen dienen. Voor de domeinnaam dient men te betalen, het bedrag verschilt per provider.

Domeinnamen worden uitgedeeld op een “first-come, first-served” basis. Het is dus zaak een domeinnaam zo spoedig mogelijk aan te vragen, want anders bestaat de kans dat de domeinnaam door iemand met dezelfde handelsnaam of met hetzelfde merk je voor is (zie ook hoofdstuk 4 voor problemen die hierdoor kunnen ontstaan).

2.3 Aanvragen domeinnaam bij InterNIC

InterNIC registreert en deelt domeinnamen met als Top Level Domain `.com`, `.org`, `.net`, `.edu` en `.gov` uit. De aanvraag hoeft hier niet via een provider te verlopen, dit kan overigens wel. Het is ook mogelijk om InterNIC rechtstreeks te benaderen. Een domeinnaam kan via hun website[5] aangevraagd worden. Je doorloopt een aantal stappen waarin je vragen beantwoord en vervolgens krijg je enkele dagen later de bevestiging dat je de domeinnaam hebt of een afwijzing. Ook InterNIC stelt een aantal voorwaarden:[6]

- De aanvrager dient te verklaren dat hij het recht heeft om de domeinnaam te gebruiken.
- De aanvrager dient te verklaren dat hij de domeinnaam regelmatig zal gebruiken.
- De aanvrager dient te verklaren dat hij de domeinnaam niet voor onrechtmatige daden gebruikt.
- De aanvrager dient de eventuele provider en InterNIC te vrijwaren van inbreuk op eventuele rechten van derden.

Voor een domeinnaam betaal je een basisbedrag van 100 dollar een voor elk volgend jaar betaal je 50 dollar onderhoudskosten. Als technische voorwaarde wordt gesteld dat er twee computers dienen te zijn die als nameserver kunnen dienen.

Het grootste verschil tussen het aanvragen van een domeinnaam bij InterNIC en in Nederland is dus dat men in Nederland eist dat de domeinnaam overeenstemt met een handelsnaam of merknaam van de aanvrager en dat dit bij InterNIC (nog) niet het geval is. Dit heeft tot gevolg dat men bij InterNIC domeinnamen kan kapen. Dit probleem wordt in hoofdstuk 4 besproken.

[3] Voor een complete lijst zie `http://www.domain-registry.nl/blocked.html`

[4] Voor een complete lijst zie `http://www.domain-registry.nl/blockedzones.html`

[5] Te vinden op `http://www.internic.net/`

[6] Dit zijn de meest recente voorwaarden, zij dateren van 9 september 1996. De voorwaarden zijn te vinden op `ftp://rs.internic.net/policy/internic/internic-domain-4.txt`

3

Technische problemen bij het Domain Naming Systeem

3.1 Problemen bij de implementatie

3.1.1 Het Britse JANET systeem

In het Verenigd Koninkrijk werd in de jaren tachtig gebruik gemaakt van het JANET-netwerk voor academische instellingen. Dit systeem had haar eigen hiërarchische structuur voor naamgeving, analoog aan DNS, met als verschil dat de componenten andersom werden opgeschreven. Een DNS domein als `cambridge.ac.uk` (van Cambridge University) stond binnen JANET bekend als `uk.ac.cambridge`. Om de vertaalslag tussen deze twee systemen te kunnen maken, bevatten de eerste versies van DNS software routines die keken of de naam begon met "`uk.`" en als dit zo was, werd de naam per component andersom geschreven.

Alhoewel dit prima werkte, had het wel als onverwacht nadeel dat het nu onmogelijk was om een computer de naam `uk` te geven. Immers, de domeinnaam `uk.win.tue.nl` werd aangezien voor een naam in het JANET-formaat en dus eerst andersom geschreven. Het opzoeken van het bijbehorende adres lukte dus nooit. Ook had het als nadeel dat gebruikers van dit systeem met de hand adressen moesten wijzigen als zij e-mail uitwisselden met Internet-gebruikers, of als zij een verbinding wilden maken met een computer op Internet. Om deze redenen is JANET in 1993 overgestapt op de DNS-ordening [4].

3.1.2 Te generieke zoekdomeinen

Voor de jaren negentig was het in principe mogelijk om elke domeinnaam te registreren. Een interessant probleem ontstond toen iemand het domein `edu.com` registreerde. Veel nameservers waren ingesteld met erg generieke zoekdomeinen (zie paragrafen 1.4.2 en 1.4.3 voor de technische details). Wanneer een gebruiker het adres van `web.mit.edu` wilde bepalen, werden alle zoekdomeinen geprobeerd. Echter, op het moment dat het `.com` zoekdomein werd gebruikt (d.w.z., de nameserver probeerde de naam `web.mit.edu.com.` op te zoeken), werd de gebruiker doorgestuurd naar de nameserver van het `edu.com` domein. De beheerder van de nameserver van dit domein was nu in staat om zijn eigen computers door te laten gaan voor die van MIT of elke andere onderwijsinstelling!

In 1993 verscheen RFC 1535 [2] waarin dit probleem werd besproken en werd aanbevolen om maatregelen hiertegen te nemen. Het is tegenwoordig niet langer mogelijk om dit soort domeinen te registreren.

3.1.3 Gebruik van sterk gelijkende namen

Een meer recente techniek om een verzoek om informatie over een domein te "kapen" is het registreren van een domein dat sterk lijkt op een ander domein. De afwijking komt overeen met veelgemaakte typefouten, zodat gebruikers die per ongeluk een punt vergeten of een letter "O" voor het cijfer "0" aanzien bij de verkeerde server uitkomen. Enkele voorbeelden zijn `wwwyahoo.com` versus `www.yahoo.com` of `micros0ft.com` versus `microsoft.com`.

Gebruikers van de *Webcrawler* zoekmachine kwamen, wanneer zij per ongeluk de "w" en de "l" omwisselden in de domeinnaam `www.webcrawler.com`, uit bij een pagina waarop

stond dat de site vernieuwd werd. Echter, elke zoekpoging leidde tot dezelfde serie resultaten, waarin uitsluitend porno-sites te vinden waren.[1]

Dit is eigenlijk meer een juridisch dan een technisch probleem. De persoon met deze domeinnaam probeert zich immers voor te doen als de eigenaar van het domein waar zijn domeinnaam op lijkt. Verdere bespreking van dit probleem staat dan ook in paragraaf 4.4.4.

3.1.4 DNS *spoofing*

Het DNS staat of valt met de informatie die nameservers aan elkaar doorgeven. Hoe hoger een nameserver in de "boom" zit, hoe groter het effect dat foutieve informatie op de rest van het netwerk heeft. Een root nameserver die onjuiste informatie doorgeeft over een top-level domein kan zo *alle* domeinen binnen dat top-level domein onbereikbaar maken.

Ook het "cachen", het lokaal bewaren van eerder ontvangen informatie (zie paragraaf 1.4.5), kan voor problemen zorgen. Een verandering in de informatie van een domein wordt niet direct door het hele netwerk "zichtbaar", omdat een aantal nameservers nog de verouderde lokale kopie van de informatie gebruikt. Het kan ruim een dag duren voordat alle nameservers in het netwerk de gecachede informatie hebben vervangen door de nieuwe.

Wanneer men opzettelijk foutieve informatie aan een nameserver geeft, is sprake van *DNS spoofing*. De eenvoudigste manier om dit te doen is door een vervalst Resource Record aan een nameserver te sturen, zogenaamd als antwoord op een query die hij zou hebben gedaan. Als deze server dit antwoord zonder meer accepteert en in zijn cache opslaat, is de eigenlijke host onbereikbaar geworden. Een gebruiker die nu bij deze server een query doet, zal immers het vervalste antwoord krijgen. De "spoofer" kan zo dus een computer onbereikbaar maken of mensen omleiden naar zijn eigen systeem.

Tegenwoordig hebben nameservers beveiligingen tegen dit soort trucs, bijvoorbeeld door bij te houden welke queries al beantwoord zijn en antwoorden daarop te negeren, net zoals antwoorden op queries die niet gedaan zijn. Ook kan gebruik worden gemaakt van beveiligde en/of geauthenticeerde verbindingen tussen nameservers, zodat een "spoofer" geen vervalste informatie door kan geven.

3.1.5 Denial of service attacks

Denial of service wil zeggen dat het gebruik van een dienst onmogelijk gemaakt wordt. Dit kan het eenvoudigste worden bewerkstelligd door de nameserver van het slachtoffer te overbelasten (bijvoorbeeld door grote hoeveelheden informatie op te vragen of een groot aantal antwoorden binnen een zeer kort tijdsbestek te sturen) zodat deze niet meer functioneert. Gebruikers van die nameservers kunnen dan over geen enkele domeinnaam meer informatie opvragen.

Hiertegen is eigenlijk geen beveiliging mogelijk. Hoogstens kan een beheerder van een nameserver deze zo afstellen dat er slechts een beperkt aantal antwoorden per minuut worden gegeven en dat verzoeken om al te veel informatie tegelijk worden geweigerd. Bij een aantal nameservers is het bijvoorbeeld al niet meer mogelijk om alle hosts binnen diens domein op te vragen.

3.2 Problemen door de groei van DNS

3.2.1 De groei van het aantal domeinen

Sinds 1993 is het aantal hosts en domeinen binnen het DNS enorm gegroeid. Volgens een onderzoek van *Network Wizards*, dat elk half jaar wordt uitgevoerd, is het aantal hosts op

[1] Zie `http://www.news.com/News/Item/0,4,12414,00.html`

het Internet gegroeid van 1.313.000 in januari 1993 tot 19.540.000 in juli 1997. Het aantal domeinen[2] is in diezelfde periode gestegen van 21.000 tot 1.734.473 [6].

Het `.com` domein heeft de grootste groei ondergaan. In juli 1997 bestonden er 1.077.094 domeinen binnen dit top-level domein, meer dan de helft van het totaal [5]. In januari 1995 bestonden er nog slechts 31.036 domeinen binnen dit top-level domein.[3]

In de top 100 van alle hostnamen staat `www` bovenaan met 754.718 voorkomens, de nummer twee (`mail`) volgt met 121.649 voorkomens op grote afstand [7]. De domeinnaam van de vorm `www.naam.com` is verreweg de meest populaire.

De reden dat deze domeinnaam zo populair is, is eenvoudig. Veel bedrijven willen "op Internet" met hun eigen website en registreren daarom hun bedrijfsnaam als domeinnaam. Omdat zij alleen een website willen opzetten, wordt binnen dit domein alleen de host `www.bedrijfsnaam.com` gebruikt. Veel zogeheten "web hosting" firma's bieden de mogelijkheid om de WWW-server voor het bedrijf te beheren. Zij registreren dan het domein bij InterNIC (zie hoofdstuk 2) en gebruiken hun eigen nameserver voor alle domeinen van hun klanten. Hierdoor is er slechts één nameserver nodig voor vele tientallen domeinen.

Naast bedrijfsnamen worden ook vaak namen van produkten of diensten geregistreerd. Zo worden bijvoorbeeld de meeste Amerikaanse films tegenwoordig aangeprezen inclusief WWW adres met domeinnaam `www.naam.com` waarbij "naam" de naam is van de film. De website van de recente film "Men in black" is te vinden op de host `www.meninblack.com`. De laatste *Star Trek* film kreeg de domeinnaam `startrek.first-contact.com`, waarbij dus de punt (die de scheiding in de hiërarchie aangeeft) werd gebruikt als "spatie"!

Het bedrijf Proctor & Gamble heeft in 1995 96 domeinnamen geregistreerd, die allemaal betrekking hadden op produkten en/of diensten van dit bedrijf. Deze namen variëren van "Always", "Papertowel" of "Tissue" tot "Diarrhea" en "Dandruff".

Er zijn een aantal redenen waarom het registreren van dergelijke domeinnamen zo populair is:

1. Een naam van deze vorm is gemakkelijk te onthouden. De voor- en achtervoegsels (`www` en `com`) zijn altijd hetzelfde, dus als de gekozen naam al bekend is, is de domeinnaam het ook.

2. De meeste namen zijn kort en kunnen dus op radio of TV geadverteerd worden.

3. Gebruikers die de website van een bedrijf willen bezoeken, zullen proberen of `www.bedrijfsnaam.com` bestaat, omdat dit de meest voorkomende vorm is. Als een bedrijf dus deze naam gebruikt, heeft hij meer kans dat potentiële klanten hem vinden.

4. Voor produkten geldt een analoge reden. Het zoeken naar informatie over een produkt begint vaak door te proberen of de domeinnaam `www.produktnaam.com` bestaat. Overigens zal in een aantal browsers automatisch `www` en `com` worden toegevoegd aan een naam, wanneer die naam niet blijkt te bestaan. Zo wordt de gebruiker typewerk bespaard.

   Deze techniek wordt ook gebruikt om het mogelijk te maken dat gebruikers een bepaalde zinsnede of woordcombinatie op kunnen geven. Zo bestaat er bijvoorbeeld een website waarin negatieve kritieken worden geleverd op andere websites, te vinden op de host
   `www.webpagesthatsuck.com`.

   Met name de sex-geörienteerde websites maken gebruik van dit soort "namen".[4]

[2] Hierbij zijn *alleen* domeinen direct onder een top-level domein geteld, niet verdere subdomeinen.
[3] Voor historische gegevens over de groei van het Internet tussen 1981 en 1991 wordt verwezen naar RFC 1296 [3].
[4] Voorbeelden te over, maar deze zijn nogal expliciet.

Een interessant verschijnsel is de opkomst van het aantal domeinen in landen als Tonga of IJsland, landen waar je niet direct een grote hoeveelheid bedrijven zou verwachten die zich op de internationale markt richten. De reden is hier echter dat deze landen "handige" landencodes hebben, waardoor het mogelijk is om gemakkelijk te onthouden domeinnamen te maken. Een bedrijfje in Tonga heeft de domeinnaam `come.to` geregistreerd, waardoor URLs als `http://come.to/philips` mogelijk worden. In IJsland is om dezelfde reden het domein `this.is` geregistreerd. In Nederland bestaat het domein `het.net`, waarmee diverse creatieve expressies mogelijk zijn (denk aan `weg.met.het.net` of `uwnaamhier.op.het.net`). De Belgische Internet-provider Globe heeft als domeinnaam `glo.be`.

3.2.2 Het probleem: DNS wordt steeds platter

Bij de introductie van het DNS werd gekozen voor een hiërarchische structuur, omdat de bestaande platte structuur niet schaalbaar bleek voor een systeem met een groot aantal machines. De voorgestelde functionele indeling van top-level domeinnamen (zie paragraaf 1.3.1) hield geen rekening met de recente enorme toename van het aantal commerciële instellingen.

Door deze toename is de "subboom" binnen het `.com` domein enorm uitgegroeid. De nameserver voor dit top-level domein moet nu feitelijk een gigantische database beheren, alhoewel de software hier absoluut niet op berekend is. Dit zorgt voor vertragingen en overbelasting. Er zijn nu inmiddels 10 machines ingezet die parallel als nameserver voor dit domein functioneren, en zelfs met zo veel hardware zijn storingen niet te vermijden.

Uit de lijst in de vorige paragraaf wordt duidelijk dat het DNS gebruikt wordt om een eenvoudige database te implementeren. De gebruiker geeft een zoekterm op, en als er een domein `www.zoekterm.com` bestaat, dan krijgt de gebruiker de informatie die hij zoekt. [5]

Natuurlijk kan een gebruiker ook een zoekmachine gebruiken om te proberen te vinden dat hij zoekt. Dit is echter meestal trager en produceert vaak vele tientallen resultaten, waarin dan nog verder moet worden gezocht. Het is dus lang niet zo handig als gewoon een term intypen in het "Open URL" veld van je browser en dan naar een relevante site gaan.

Browser-fabrikant Netscape heeft vlak na het uitbrengen van versie 3.0 van haar browser voorgesteld om in versie 4.0 een direkte koppeling met een zoekmachine te installeren. Hierdoor zouden gebruikers eenvoudiger en sneller informatie kunnen zoeken op Internet. Dit is echter niet doorgegaan, omdat men bang was dat dit oneerlijke concurrentie zou zijn ten opzichte van alle andere zoekmachines.

Het nut van een eenvoudig zoeksysteem op Internet staat niet ter discussie. Het probleem is echter dat het DNS in zijn huidige vorm eenvoudigweg niet geschikt is om deze rol te vervullen. De enige manier om dit te realiseren is door een uitgebreidere hiërarchie te introduceren, zodat bedrijven, produkten, instellingen en diensten geclassificeerd kunnen worden zonder dat er een "subboom" met tienduizenden bladeren ontstaat. Het Internet Ad-Hoc Comité heeft in 1996 een eerste voorstel hiervoor gedaan [1], maar dit ondervond nogal wat kritiek (zie hoofdstuk 5).

Een andere oplossing is de introduktie van een echt zoeksysteem, zodat DNS weer kan worden gebruikt om de namen van netwerken te beheren. Dit zoeksysteem zou dan het Internet-equivalent worden van de "Gouden Gids." Deze oplossing wordt meer volledig besproken in hoofdstuk 6.

[5] Althans, dat nemen we dan maar aan.

Literatuur

[1] International Ad Hoc Committee. *Recommendations for Administration and Management of gTLDs.* http://www.gtld-mou.org/draft-iahc-recommend-00.html, 1997.

[2] E. Gavron. *A Security Problem and Proposed Correction with Widely Deployed DNS Software.* RFC 1535, 1993.

[3] M. Lottor. *Internet Growth (1981-1991).* RFC 1296, 1992.

[4] S. Shaw and G. Howat. *Consequences of reversing JANET NRS names.* JNT, 1993.

[5] Network Wizards. *Host Distribution by Top-Level Domain Name.* http://www.nw.com/zone/WWW/dist-bynum.html, 1997.

[6] Network Wizards. *Internet Domain Survey.* http://www.nw.com/zone/WWW/report.html, July 1997.

[7] Network Wizards. *Top 100 Host Names.* http://www.nw.com/zone/WWW/firstnames.html, 1997.

4

Conflicten over domeinnamen

4.1 Ontstaan van conflicten

Het Internet kan voor ontzettend veel doeleinden gebruikt worden. Behalve het opvragen van informatie is het bv. ook mogelijk om te communiceren of artikelen te kopen of verkopen. Het Internet is de laatste jaren steeds commerciëler geworden. Voor een eigenaar van een website is het dan ook erg gunstig als zijn/haar website gemakkelijk gevonden kan worden door de gebruikers. Domeinnamen zouden hierbij kunnen helpen als de domeinnaam een indicatie geeft om wat voor soort website het gaat. Als een organisatie het Internet op wil, dan wordt als domeinnaam dus ook vaak de handelsnaam van de betreffende organisatie gekozen. Van de domeinnaam `cnn.com` zou je af kunnen leiden dat het hier om het televisiestation gaat.

Handelsnamen staan identieke registraties van dezelfde namen toe als het gaat om niet-concurrerende goederen of services waarbij er ook geen verwarring omtrent de naam mag kunnen ontstaan (zie paragraaf 5.1.1). Neem bijvoorbeeld de bedrijven Apple Computers en Apple Records. Bij domeinnamen kan er maar één domeinnaam `apple.com` zijn. De vraag die nu ontstaat is: Welke partij heeft nu recht op de domeinnaam `apple.com`?

4.2 Soorten conflicten

Er kunnen 3 soorten conflicten ontstaan omtrent een domeinnaam:

1. Een organisatie wil het Internet op en wil een domeinnaam registreren. Deze domeinnaam is het merk van de organisatie. Tijdens het registreren komt de organisatie er achter dat de domeinnaam al gebruikt wordt door iemand anders, die geen registratie van dat merk heeft. Deze persoon of organisatie kan dat met verschillende bedoelingen doen.

   - Iemand anders kan deze domeinnaam geregistreerd hebben om te profiteren van de uitstraling van de organisatie of om hiermee financieel voordeel te behalen. Het komt voor dat iemand het merk van een organisatie registreert als domeinnaam om de domeinnaam daarna voor flink wat geld te verkopen aan die organisatie. Een voorbeeld hiervan is het conflict tussen Dennis Toeppen en Panavision (zie paragraaf 4.4.2).
   - Het komt ook voor dat een organisatie het merk van de concurrent registreert als domeinnaam en op de bijbehorende website negatieve informatie publiceert over de concurrent. Een voorbeeld hiervan is het conflict tussen Princeton Review en Kaplan (zie paragraaf 4.4.1).

   Bovenstaande aktiviteiten worden ook wel *domain grabbing* of *domain hijacking* genoemd.

2. Het kan voorkomen dat een andere organisatie de domeinnaam al geregistreerd heeft, omdat de domeinnaam ook het merk is van die andere organisatie. Dit is mogelijk omdat het toegestaan is om een handelsnaam te registreren, terwijl een andere organisatie die handelsnaam ook al heeft geregistreerd.

Het is ook mogelijk dat een andere organisatie een gedeelte van het merk gebruikt van een andere organisatie. Als voorbeeld kan dienen American Airlines en American Standard. Wie heeft nu het recht op `american.com`? Een vergelijkbaar conflict dat zich afspeelde in Nederland wordt toegelicht in paragraaf 4.4.3.

3. Er kunnen ook conflicten ontstaan omdat een bepaalde partij niet het merk van een andere partij heeft geregistreerd, maar een domeinnaam die er heel sterk op lijkt en bijvoorbeeld zeer gevoelig kan zijn voor typefouten. Voorbeelden hierbij zijn: `teubner.com` en `tuebner.com` (zie paragraaf 4.4.4), `webcrawler.com` en `webcralwer.com`, `infoseek.com` en `infosek.com`, `yahhoo.com` en `yahoo.com`, `microsoft.com` en `micros0ft.com`.

4.3 Wat te doen bij problemen

Alvorens een domeinnaam geregistreerd wordt, wordt er een heel proces doorlopen (zie hoofdstuk 2). Steeds meer uitgevende instanties verlangen een vrijwaring van inbreuk op eventuele rechten van derden voor het geval zij zelf worden aangesproken. Ook proberen zij er voor te zorgen dat er zich minder conflicten kunnen voordoen. Stichting Internet Domeinregistratie Nederland (SIDN) heeft t.o.v. InterNIC de extra regel dat bij registratie van een domeinnaam de aanvrager een uittreksel van het handels-, verenigings- of stichtingenregister moet kunnen tonen, waardoor een aantal conflicten al preventief vermeden worden.

Als een organisatie het idee heeft dat er inbreuk gemaakt wordt op het merk- of handelsnaamrecht van de organisatie, dan kan zij hier protest tegen aantekenen bij de instantie die de domeinnaam uitgegeven heeft. InterNIC heeft een aantal regels om een conflict op te lossen. Als er een klacht van iemand binnen komt over een domeinnaam, dan mag de domeinnaam eigenaar deze domeinnaam blijven gebruiken als: [1]

1. de eigenaar de domeinnaam geregistreerd heeft, voordat de aanklager over deze naam het merkrecht verworven heeft, of voordat de eigenaar dit merk heeft laten registreren,
2. er een borgsom wordt betaald,
3. InterNIC gevrijwaard blijft van verantwoordelijkheid en kosten.

Als de eigenaar aan deze eisen voldoet, mag de eigenaar de domeinnaam blijven gebruiken en kan er eventueel een rechtszaak volgen. Mocht de rechtbank beslissen dat de eigenaar de domeinnaam niet mag behouden, dan zal InterNIC zich hier aan onderwerpen.

Als de eigenaar niet beschikt over een registratie van de domeinnaam als merk, dan wordt de eigenaar dringend verzocht om afstand te doen van de domeinnaam. Gebeurt dit niet dan wordt de domeinnaam na 90 dagen in de status “hold” gezet. Dit wil zeggen dat de domeinnaam onbruikbaar is totdat er overeenstemming is bereikt of totdat de rechter uitspraak heeft gedaan. In het laatste geval zal de aanklager de rechter er van moeten overtuigen dat er sprake is van het maken van merkinbreuk of een andere vorm van onsportief gedrag.

In het geval van zeer bekende merknamen en onder dreiging van juridische stappen kunnen de meeste domain-grabbers er wel toe worden bewogen om de domeinnaam vrijwillig over te dragen. Vaak wordt er door de domain-grabbers ook wel een symbolisch geschenk gevraagd (zie paragraaf 4.4.1).

4.4 Voorbeelden van conflicten

4.4.1 Domain grabbing met als doel de concurrent te benadelen

Een duidelijk voorbeeld van domain-grabbing met als doel het benadelen van de concurrent is het conflict tussen Princeton Review en de Stanley Kaplan Review [2, 3]. Princeton Review houdt zich bezig met het vervaardigen en distribueren van materialen om studenten

voor te bereiden op examens. De Stanley Kaplan Review is de concurrent van Princeton Review. Toen Princeton Review het Internet op wilde, registreerden ze een aantal domeinnamen waaronder princeton.com en review.com. Zij registreerden ook de domeinnaam kaplan.com om daar een website onder te beginnen om daarop de concurrent Kaplan zwart te maken en te dwarsbomen. Kaplan Review tekende hier natuurlijk protest tegen aan en eiste van Princeton om de domeinnaam kaplan.com op te geven. Princeton wilde op deze eis ingaan als ze van Kaplan een krat bier kregen. Dit werd geweigerd door Kaplan Review waardoor er een procedure werd begonnen. Uiteindelijk is door arbitrage Kaplan Review in het gelijk gesteld, waardoor Princeton de domeinnaam kaplan.com moest opgeven.

Domain grabbing conflicten vallen in de meeste gevallen gunstig uit voor de partij die de klacht indient.

4.4.2 Domain grabbing met als doel om financieel voordeel te behalen

Er is een conflict geweest tussen een bekende Amerikaanse domain grabber (Dennis Toeppen) en Panavision Internation L.P. [3] Toeppen registreerde de domeinnaam panavision.com en panaflex.com. Panavision heeft recht op de namen Panavision en Panaflex. Omdat Toeppen deze namen geregistreerd had, kwam er protest van Panavision. Toeppen wilde de domeinnamen wel afstaan, maar dan wilde hij daar wel $ 13.000 voor krijgen. Panavision beweerde dat Toeppen alleen de domeinnamen registreerde om die daarna te verkopen voor een flink bedrag. Dit resulteerde in een rechtszaak. De rechter oordeelde dat Toeppen andermans merken gebruikte voor commercieel gebruik.

4.4.3 Conflict over mogelijke verwarring

Dit conflict speelde zich af in Nederland [3]. Spaarnestad is merkhoudster op Ouders van Nu. Ouders Online brengt een website met domeinnaam ouders.nl uit dat een elektronisch tijdschrift bevat. Ouders Online is als merk geregistreerd voor telecommunicatie en dan in het bijzonder via Internet en programmering voor elektronische dataverwerking. Het conflict ontstond doordat Spaarnestad van mening was dat er hier sprake is van merkinbreuk door Ouders Online en Spaarnestad wilde dan ook dat Ouders Online de namen “ouders” en “ouders online” niet meer zou gebruiken in een domeinnaam. Volgens Spaarnestad deed Ouders Online net alsof ze een elektronische uitgave van Ouders van Nu aanbood. Dit conflict werd uitgevochten in een kort geding. De President had een aantal uitgangspunten:

- Ondanks het verschil in medium vertonen het papieren Ouders van Nu en het elektronische Ouders Online gezien inhoud en bestemming voldoende verwantschap om soortgelijke waren in de zin van artikel 13.A lid 1 onder b Benelux Merken Wet (BMW) te zijn.
- Een domeinnaam (die dient als aanduiding van een vindplaats van een elektronisch tijdschrift) moet worden aangemerkt als gebruik van een teken in een waar in de zin van artikel 13.A lid 1 onder b BMW.

Uiteindelijk is het kort geding positief uitgevallen voor Ouders Online, want de rechter was van mening dat noch de domeinnaam noch het merk Ouders Online inbreuk maken op het merk van Spaarnestad.

4.4.4 Conflict waarbij misbruik wordt gemaakt van typefouten

Onderstaand conflict ging tussen Teubner & Associates en American International Facsimile Products (AIFP).[1] Teubner & Associates, een high-technology software bedrijf heeft de naam teubner.com geregistreerd. Teubner heeft een fax distributie produkt FAXGATE, dat concurreert met de Hostfax van AIFP. Een klant van Teubner probeerde eens de domeinnaam

[1] Zie http://www.teubner.com/faxgate/new/pressrel/pressrel/hijackpr.htm

`tuebner.com` (een veel voorkomende foutieve spelling van `teubner`) om te kijken of hij dan ook bij Teubner uitkwam. Dat gebeurde niet, want hij kwam notabene bij de concurrent AIFP terecht. AIFP had dus de vaak verkeerd gespelde naam "tuebner" als domeinnaam geregistreerd. Uiteindelijk heeft Teubner de domeinnaam `tuebner.com` gekregen en heeft AIFP hem dus af moeten staan.

4.5 Wat kan men doen om problemen te voorkomen

De beste manier om de bovengenoemde conflicten op te lossen is om deze te vermijden. Het zou voor een organisatie verstandig zijn om, ook al hebben ze op het moment geen domeinnaam nodig, er toch al een te registreren. Daardoor kunnen domain-grabbers hun slag niet meer slaan. Het komt vaak voor dat men dan een "bare bones" website opzet.[2] Op zo'n site staat dan bijvoorbeeld alleen de naam, adres en telefoonnummer van de organisatie.

Bij het registreren van een domeinnaam is het zorgvuldig zoeken naar het al of niet bestaan van je voorgestelde domeinnaam van groot belang. Je moet er zeker van zijn dat deze domeinnaam beschikbaar is en dat de kans klein is dat er conflicten met anderen kunnen ontstaan. Stel je eens voor wat voor gevolgen het kan hebben als je ontzettend veel geld in een website hebt geïnvesteerd en er opeens een organisatie opduikt die de domeinnaam opeist.

Kies de domeinnaam identiek aan het geregistreerde merk of handelsnaam van de organisatie. Het kan ook verstandig zijn om indien de domeinnaam niet geregistreerd staat als merk of handelsnaam, deze naam wel te laten registreren. SIDN voorziet hierin door bij het registreren te eisen dat de domeinnaam geregistreerd staat als merk of handelsnaam. Bij InterNIC wordt dit niet geëist. Met deze voorzorgsmaatregelen in het achterhoofd kan er veel ellende bespaard worden.

[2] Zie `http://www.inet-sciences.com/iss/barebone.htm`

Literatuur

[1] J. Agmon, S. Halpern, and D. Pauker. *What's in a Name?* http://www.law.georgetown.edu/lc/internic/introd1.html, 1996.

[2] J. Agmon, S. Halpern, and D. Pauker. *What's in a Name?* http://www.law.georgetown.edu/lc/internic/recent/rec2.html#kaplan, 1996.

[3] A.P. Meijboom. Domeinnamen op Internet - Wat, Waarom, Hoe en Waarheen? *Intellectueel eigendomsrecht en Reclamerecht*, February 1997.

5

Mogelijke oplossingen voor de DNS-problematiek

5.1 Mogelijkheden binnen het merkenrecht

In het geval van juridische conflicten met betrekking tot het gebruiken van een domeinnaam kan men zich afvragen welk type intellectuele eigendomsrecht men het best kan toepassen.

Het intellectueel eigendomsrecht regelt de belangen van individuen en van het bedrijfsleven die op het gebied van de concurrentiestrijd liggen. Er bestaan verschillende soorten intellectueel eigendomsrecht deze worden in de volgende paragraaf kort besproken.

5.1.1 Soorten intellectueel eigendomsrecht

Het intellectueel eigendomsrecht regelt dus de belangen van een bedrijf of individu. Bescherming biedt men niet alleen in het belang van de betrokkenen maar ook in het algemeen belang, zodat als gevolg van de bescherming de technologische ontwikkeling wordt gestimuleerd. De onderwerpen die in het intellectueel eigendomsrecht besproken worden zijn onder andere: [6]

- Het octrooirecht verschaft patent op een voortbrengsel of werkwijze. Een domeinnaam is geen werk of voortbrengsel dus dit recht is niet van toepassing.
- Het auteursrecht verschaft de maker van een werk de uitsluitende beslissingsbevoegdheid over openbaar maken en verveelvoudigen. Artikel 10, lid 1 van de Auteurswet stelt dat op enkele woorden geen auteursrecht kan worden verkregen, ook al zijn deze woorden nieuw en origineel. Soms wordt een uitzondering gemaakt voor een titel of slogan. Een domeinnaam is slechts een enkel woord en valt dus niet in deze categorie.
- Er zijn nog enkele vormen van intellectueel eigendomsrecht, zoals het portretrecht, de topografiewet, het kwekersrecht en de beeldende kunst maar ook deze kunnen niet voor een domeinnaam gebruikt worden.

De tot dusver bekeken vormen van intellectueel eigendomsrecht zijn duidelijk niet geschikt. Mogelijke kandidaten zijn het handelsnaamrecht en het merkenrecht. Deze worden in de volgende paragraaf besproken.

5.1.2 Handelsnaamrecht en merkenrecht

Als eerste wordt het *handelsnaamrecht* behandeld. De handelsnaam is de naam waaronder een onderneming wordt gedreven. Hiervoor is geen registratie vereist. Het handelsnaamrecht beschermt de naam tegen verwarringwekkend gebruik. Daarbij kijkt men naar de aard van de onderneming en het gebied waar ze gevestigd is.

Dezelfde naam kan door ondernemingen in verschillende takken van handel of industrie gevoerd worden. Zelfs gelijksoortige ondernemingen die in verschillende regio's werkzaam zijn mogen dezelfde naam voeren. Moeilijkheden ontstaan indien twee bedrijven met dezelfde naam, die zich aanvankelijk op de plaatselijke markt bewogen, zich gaan uitbreiden en in elkaars gebied komen.

Degene die de naam als eerste in het nieuwe gebied voerde of er de grootste bekendheid had gaat dan voor. Hetzelfde verhaal geldt voor verandering of uitbreiding in produkten of diensten. Degene die verandert zal dan moeten wijken.

Voor het *merkenrecht* geldt dat de eigenaar het merk moet deponeren. Men kan het merk deponeren bij het Benelux-depot of bij het internationaal depot in Genève. De grondslag van de bescherming van merken ligt in de noodzaak van een zo ongestoord mogelijke marktwerking. Door middel van merken worden produkten geïdentificeerd. De houder van het merk krijgt een exclusief recht dat hij kan gebruiken tegen aantasting van het merk in zijn functies. Bescherming wordt geboden tegen ongerechtvaardigd voordeel uit of afbreuk aan onderscheidend vermogen of reputatie. Ongerechtvaardigd voordeel valt in de praktijk in drie categorieën: [6]

1. Algemeen bekende merknamen, zoals Philips, Coca-Cola, Ferrari[1] en IBM zijn zo bekend dat ze beschermd zijn tegen welk gebruik dan ook. Deze merken mogen dus niet door een andere onderneming gevoerd worden, ook al betreft het een compleet ander dienst of produkt.

2. Wanneer een merknaam een negatieve uitstraling heeft op een ander merk, mag deze ook niet gebruikt worden. De eigenaar van het chocolade-merk “Merci” heeft met succes bezwaar gemaakt tegen het gebruik van de naam “Merci” voor kattevoer.[2]

3. Een merknaam mag ook niet worden gebruikt indien er sprake kan zijn van verwarring met een ander merk. Dit kan gebeuren als er soortgelijkheid is tussen twee merken. Als maatstaf voor soortgelijkheid kijkt men naar verwantschap in eigenschappen, gebruikersbestemming, produktiewijze, produktieplaatsen, grondstoffen of handelskanalen. Een voorbeeld van soortgelijkheid zijn drop en kruidenkoekjes (zelfde afzetkanalen en beiden etenswaren).[3] Een tweede voorbeeld zijn kleding en zonnebrillen (zelfde couturiers).[4]

Het grote verschil met het handelsnaamrecht is dus dat een merk internationale bescherming kan bieden en een handelsnaam slechts plaatselijke bescherming biedt. Men moet het merk dus in het internationale depot deponeren, men heeft dan bescherming in de aangesloten landen. De Benelux-landen eisen echter ook nog een apart verzoek van de deposant. Het merk is net zoals de handelsnaam beschermd tegen verwarringwekkend gebruik.

5.1.3 Conclusie: merkenrecht of handelsnaamrecht

Uit het bovenstaande blijkt dat met het merkenrecht tenminste dezelfde bescherming geboden wordt tegen verwarringwekkende domeinnamen in dezelfde branche. Het handelsnaamrecht biedt deze bescherming niet, omdat dit slechts binnen de werkzame regio van toepassing is.

Er wordt geen bescherming geboden voor gebruik van dezelfde merknamen in verschillende branches. Het probleem van de computerleverancier Apple en de fruitzaak Apple kan hiermee dus niet worden opgelost.

Een mogelijke oplossing is: wie ’t eerst komt wie ’t eerst maalt [2]. Diegene die het eerst de domeinnaam aanvraagt heeft het meeste recht erop. Een grote belanghebbende kan een kleinere dan uitkopen, indien deze eerst was. Als deze dat niet toelaat kan eventueel een beroep gedaan worden op misbruik van recht (Art. 3-13 BW).

[1] Ferrari, 261. Arrondissementsrechtbank Koophandel Brussel 27 januari 1992. Revue de Droit Intellectuel.

[2] Merci, 14. President Arrondissementsrechtbank Haarlem 19 november 1984. Intellectueel Eigendoms- & Reclamerecht.

[3] President Arrondissementsrechtbank Amsterdam 11 december 1991. Bulletin van de Beneluxverenigingen van merken- en modellengemachtigden, nr 1 blz. 20.

[4] Kidcool, 168. Arrondissementsrechtbank Koophandel Brussel 31 oktober 1991. Reveu de Droit Intellectual.

Een tweede oplossing is om degene die het merk als eerste heeft gedeponeerd, deze persoon/bedrijf de domeinnaam te gunnen. Deze optie heeft ons inziens de voorkeur, omdat deze zeer duidelijke regel eenvoudig toe te passen is en niet zal leiden tot juridische conflicten. Bovendien wordt hiermee voorkomen dat *domain grabbers* namen kunnen registreren om deze later duur door te verkopen aan bedrijven die met deze namen hun produkten of diensten willen gaan aanbieden op Internet.

Anders ligt het natuurlijk indien iemand een domeinnaam registreert terwijl hij geen aanspraak kan maken op een gedeponeerd merk of een handelsnaam. Er kan dan meestal een beroep worden gedaan op de regeling depot “te kwader trouw” Ook is er de regeling van 6bis van het Unieverdrag dat voorziet in nietigverklaring van depots van derden van “algemeen bekende merken”.

5.2 Het voorstel van de IAHC

Een voorstel (het zogeheten gTLD-MoU) dat gedaan is door het Internet International Ad Hoc Committee (IAHC)[5] op 4 februari 1997, is om het aantal top-level domeinnamen uit te breiden met 7 nieuwe top-level domeinnamen. Dit is gedaan met het doel om de enorme interesse die er bestaat te kunnen verdelen over de top-level domeinnamen. Door deze maatregel moeten er ook instanties gezocht worden, waarbij men domeinennamen met deze top-level domeinnamen kan laten registreren. Deze oplossing is er dus met name op gericht om het aantal domeinnamen per top-level domein niet uit de hand te laten lopen, of indien dit al het geval was, te beperken.

5.2.1 De zeven nieuwe top-level domeinnamen

De voorgestelde top-level domeinnamen zijn: [1]

`firm` Bedoeld voor bedrijven.

`store` Bedoeld voor winkels.

`web` Bedoeld voor instanties die zich bezig houden met aktiviteiten die gericht zijn op het World Wide Web.

`arts` Bedoeld voor instanties die culturele en amusements-aktiviteiten organiseren.

`rec` Bedoeld voor instanties die veel vrijetijds-aktiviteiten organiseren.

`info` Bedoeld voor instanties die informatie-services aanbieden.

`nom` Bedoeld voor privé-personen die een domeinnaam willen die gebaseerd is op hun naam.

Deze namen zijn nog niet definitief en kunnen altijd nog veranderd worden. Op dit moment is nog niet bekend of en wanneer deze top-level domeinnamen ingevoerd zullen worden, aangezien de instanties die ze moeten gaan beheren hiervoor nog niet klaar zijn of zelfs nog niet eens bestaan.

5.2.2 Kanttekeningen bij dit voorstel

- De voorgestelde top-level domeinnamen overlappen. Het zal voor instanties vaak onduidelijk zijn bij welke top-level domeinnaam zij behoren.

[5] Zie `http://www.gtld-mou.org/docs/faq.html\#whatis`

- De kans bestaat, mede doordat de top-level domeinnamen overlappen, dat een instantie een domeinnaam laat registreren voor elke top-level domeinnaam die met de instantie te maken heeft. Dit zal dan ook leiden tot een toename van het aantal conflicten over domeinnamen.
- De instanties die de administratie en registratie van de domeinnamen gaan verzorgen, bestaan op dit moment nog niet eens of ze hebben geen enkele ervaring in de taken die ze uit moeten voeren.
- De instantie die de administratie en registratie van de domeinnamen gaan verzorgen, worden verdeeld over de hele wereld. Dit staat concurrentie-vorming onder deze instanties in de weg. Ook worden er strenge regels voorgeschreven voor beheerders van nieuwe domeinnamen. Dit heeft als nadeel dat de instanties niet zo snel bereid zullen zijn om hun services steeds beter te laten worden. Omdat dit geen concurrerende markt zal worden, zal er ook minder in ge ïnvesteerd worden.

5.3 Het voorstel van de WIPO

Een voorstel dat gedaan is door het WIPO [3] is gebaseerd op het ontwerpen van een merkgerelateerde top-level domeinnaam. In de eenvoudigste vorm betekent dit een top-level domein zoals b.v. `.tm` waarin alle handelsmerken geregistreerd kunnen worden. Een instantie die een domeinnaam wil registreren met een `.tm` top-level domeinnaam, moet dan ook merkrechten hebben over de voorgestelde naam. Wanneer twee of meer instanties recht hebben op hetzelfde merk, kan door middel van een numerieke of andere code onderscheid gemaakt worden. Er moet ook een top-level domeinnaam bedacht worden die aangeeft dat de domeinnaam correspondeert met een geregistreerd merk. Dit kan bijvoorbeeld `.tm` of `.trade` zijn.

5.3.1 Kanttekeningen bij dit voorstel

- Het aantal domeinnamen in dit top-level domein zal erg groot zijn, elk handelsmerk ter wereld zou hier immers in opgenomen kunnen worden.
- Bij conflicten tussen meerdere gebruikers van een handelsmerk (die daar allebei recht op hebben) is er geen “mooie” oplossing mogelijk. Het gebruik van een numerieke code om onderscheid te maken is niet intuitief voor de gebruiker.
- Er is geen relatie tussen een domein in `.tm` en bijvoorbeeld `.com` of `.firm`, waardoor het probleem in deze hiërarchieën nog steeds niet opgelost wordt.

Een andere suggestie die door het WIPO gedaan wordt, is om een wereldwijd toegankelijke database te bouwen waarin alle geregistreerde merknamen vermeld staan [4]. Voordat een domeinnaam dan geregistreerd wordt, kan er eerst even gekeken worden of de kans groot is dat er conflicten onstaan.

5.4 Gebruik maken van de hiërarchie

Zoals in paragraaf 3.2.2 werd opgemerkt, wordt de “subboom” binnen het `.com` domein gebruikt als platte database. Er is geen enkele reden waarom het DNS niet als database gebruikt kan worden, mits de structuur van deze database hiërarchisch en niet plat van opzet is. Gebruik maken van de bestaande DNS-infrastructuur heeft een aantal belangrijke voordelen boven het opzetten van een geheel nieuw systeem:

- Er zijn geen aanpassingen nodig in WWW-browsers en andere software die gebruik maken van hostnamen of op een andere manier DNS gebruiken.

- De software voor DNS hoeft niet te worden aangepast.

- Bij het gebruik van de juiste namen is de indeling ook voor mensen te onthouden. Denk hierbij aan indelingen als `windows95.microsoft.computers` of `dr-no.jamesbond.thrillers.movies`.

De beste manier om dit aan te pakken is om een aantal nieuwe top-level domeinnamen te introduceren, waarbinnen dan weer een verdere classificatie mogelijk is. Een eerste voorstel hiervoor is gedaan door het International Ad Hoc Committee [1], maar hun voorstel ondervond nogal wat kritiek (zie paragraaf 5.2.2). Er werden slechts zeven nieuwe top-level domeinnamen voorgesteld, terwijl er voor een goede classificatie toch veel meer nodig zijn.

Een probleem hierbij is dat elke categorie (binnen het DNS kan dit het beste als een aparte *zone* worden geïmplementeerd) onder het beheer van een instelling moet worden gebracht. Er zullen dus regels moeten worden opgesteld om dit gemakkelijk te laten verlopen. Ook moet worden vastgelegd hoe een produkt of dienst het beste geclassificeerd kan worden.

Het grote nadeel van dit systeem is dat de gemakkelijk te onthouden namen van de vorm `www.naam.com` nu worden vervangen door lange namen als `www.naam.ergens.diep.in.hiërarchie`. Dit maakt adverteren van namen een stuk lastiger.

Een systeem dat hiermee vergelijkbaar is, wordt op dit moment al gebruikt bij de discussiegroepen van UseNet. Elke discussiegroep heeft een naam binnen de hiërarchie, waardoor meteen duidelijk wordt wat het onderwerp is van deze groep. Zo heet bijvoorbeeld de discussiegroep over schaken `rec.games.chess`, terwijl de discussiegroep over schaakcomputers `rec.games.chess.computer` heet. De namen worden hier dus van links naar rechts gelezen. De hoofdcategorie is hier `rec`, *recreational* of ontspanning. Andere categorieën zijn `talk` (discussie), `biz` (business), `soc` (sociaal), `news` (administratief), `comp` (computergerelateerd) en `misc` (overig). Dit systeem functioneert goed, al is het soms een probleem om tot een consensus te komen om te bepalen wat de naam wordt van een nieuwe discussiegroep. [6]

De meeste newsreaders (programma's om UseNet discussiegroepen te kunnen lezen) beschikken over systemen om de vele duizenden namen gemakkelijk weer te geven, zodat de gebruiker gemakkelijk kan zoeken. Meestal worden hierbij de namen in een boomstructuur weergegeven, waardoor de gebruiker eenvoudig door alle categorieën kan zoeken. Een dergelijke interface zou kunnen worden gebruikt om deze hiërarchische classificatie te gebruiken.

5.5 Het opzetten van een database

Alhoewel het opzetten van een hiërarchische structuur voor produkten en diensten binnen DNS mogelijk is, blijven de mogelijkheden dan beperkt. Zo kan er bijvoorbeeld bij een naam niet worden aangegeven of het gaat om een merknaam of een generieke naam, iets wat toch essentieel is om te bepalen of de informatie op de corresponderende site algemeen of produktspecifiek is. Ook ontbreekt de mogelijkheid om geregistreerde handelsmerken aan te kunnen geven.

Om deze beperkingen op te heffen, kan worden gekozen voor een echt database systeem, waarin bedrijven en instellingen zich kunnen registreren met alle gewenste informatie. Gebruikers kunnen hierin zoeken met behulp van sleutelwoorden, of bladeren door de categorieën. De feitelijke namen van de hosts hoeven nu niet meer "plat" opgezet te worden, aangezien deze nu alleen nog door computerprogramma's verwerkt worden en niet meer onthouden of geadverteerd hoeven te worden. Er is dan wel een manier nodig om een record in deze database direct aan te kunnen spreken. Hiervoor zijn diverse systemen mogelijk. De manier die op dit moment de meeste aandacht krijgt is de URN.

[6] De discussie over de naam `rec.sex` versus `talk.sex` duurde driekwart jaar en leidde uiteindelijk tot de creatie van een geheel nieuwe hiërarchie.

5.5.1 URNs in plaats van URLs

Momenteel wordt met name op het WWW gebruik gemaakt van zogeheten *Uniform Resource Locations* (URLs), waarmee aangegeven wordt op welke server en waar op die server een informatiebron (Engels: *resource*) te vinden is. Aan dit systeem kleven diverse beperkingen:

- Wanneer de opgegeven lokatie niet bestaat, moet de gebruiker zelf op zoek naar alternatieve lokaties.
- Een URL kan verdwijnen wanneer de informatiebron verhuist wordt, waardoor iedereen die naar die URL verwijst dit moet veranderen.
- De leesbaarheid van een URL is beperkt, vaak worden cryptische namen en afkortingen gebruikt.

Momenteel wordt gewerkt aan het opstellen van een methode om informatiebronnen zodanig weer te kunnen geven dat de bovenstaande beperkingen niet langer opgaan. De bedoeling is dat aan elke informatiebron een naam kan worden gegeven, die altijd kan worden gebruikt. Specifieke lokaties en dergelijke worden centraal beheerd, zodat aanpassing eenvoudig is. Dit voorstel voor *Uniform Resource Names* (URNs) in plaats van URLs. De volledige lijst met functionele eisen voor URNs is gegeven in RFC 1737 [5].

5.5.2 Het beheer van een namen-database

Een belangrijke kwestie bij het gebruik van een database-gebaseerd systeem is wie deze mag beheren. Het is natuurlijk mogelijk dat er meerdere systemen opgezet worden, zodat de gebruiker kan kiezen welke “Gouden Gids” hij wil gebruiken. Zo hoeft geen enkele aanbieder alle informatiebronnen in zijn database op te nemen. Het nadeel hiervan is dat een informatie-aanbieder nu wellicht in meerdere databases geregistreerd wil staan, wat hem dus meerdere malen geld kan kosten.

Ook is er het probleem van het up-to-date houden van de database. Voor een goede prestatie is het noodzakelijk dat er diverse systemen zijn die de database ter beschikking stellen, zodat het niet mogelijk is dat het uitvallen van één computer het hele netwerk onbruikbaar maakt. De verschillende versies van de database moeten dan wel up-to-date gehouden worden.

Overstappen op een totaal nieuw systeem kost jaren. Tot die tijd moet er dus met een “dubbel” systeem worden gewerkt om alle bronnen voor iedereen toegankelijk te houden. Ook moet er een eenvoudige, eenduidige interface worden opgezet waarmee gezocht kan worden.

Met dit systeem wordt het probleem van de classificatie niet opgelost, maar er komt zo wel een effectief systeem om verwijzingen te beheren.

Literatuur

[1] International Ad Hoc Committee. *Recommendations for Administration and Management of gTLDs*. http://www.gtld-mou.org/draft-iahc-recommend-00.html, 1997.

[2] H. Franken, H.W.K. Kaspersen, and A.H. de Wild. *Recht & Computer*. Kluwer, 1997.

[3] World Intellectual Property Organization. *Meeting of Consultants on Trademarks and Internet Domain Names*. http://www.wipo.int/eng/internet/domains/tdnmci1.htm, December 1996.

[4] World Intellectual Property Organization. *Consultative Meeting on Trademarks and Internet Domain Names*. http://www.wipo.int/eng/internet/domains/tdn/cm/cm_i_1.htm, March 1997.

[5] K. Sollins and L. Masinter. *Functional Requirements for Uniform Resource Names*. RFC 1737, 1994.

[6] L. Wickers-Hoeth. *Kort begrip van het intellectuele eigendomsrecht*. W.E.J. Tjeenk Willink, Zwolle, 1993.

6

Conclusies en aanbevelingen

In dit rapport zijn technische en juridische problemen met betrekking tot domeinnamen besproken. Er zijn natuurlijk nog diverse andere probleemgebieden, echter in het gegeven tijdsbestek is het niet mogelijk deze allemaal te analyseren en te bespreken. De in het rapport besproken problemen zijn ons insziens de belangrijkste.

Dit hoofdstuk presenteert de conclusies en aanbevelingen die volgen uit ons onderzoek. Helaas vrezen wij dat de door ons gedane aanbevelingen niet op korte termijn realiseerbaar zijn, vanwege de institutionele implicaties ervan. De manier waarop deze aanbevelingen het beste geïmplementeerd kunnen worden, verdient zeker nader onderzoek.

Bestaande onderzoeken op dit terrein zijn schaars, de meeste betrokken organisaties realiseren zich kennelijk niet de impact van deze problematiek. Wij hopen dan ook dat ons onderzoek kan bijdragen aan een aanzet om deze problemen op te lossen.

6.1 Conclusies

Uit dit rapport zijn de volgende conclusies te trekken:

1. De in hoofdstuk 3 genoemde technische problemen bij de implementatie zijn ook technisch op te lossen. In de meeste gevallen zijn deze problemen het gevolg van het gebruik van verouderde of verkeerd ingestelde software.

2. Echter, de technische problemen die veroorzaakt worden door de groei zullen alleen maar groter worden als er geen drastische maatregelen genomen worden. Het aantal bedrijven, instellingen en particulieren dat een eigen domeinnaam wil hebben stijgt enorm (zie paragraaf 3.2.1). Binnen het huidige systeem betekent dit dat vrijwel al deze domeinnamen binnen het `.com` top-level domein worden geplaatst, waardoor de hiërarchie hierbinnen volledig verloren gaat. Door de grootte van de *zone* en het feit dat de software niet berekend is op dit soort “plat” gebruik, wordt het hele systeem steeds trager en uiteindelijk volledig onbruikbaar. Wil men verder met het hiërarchische DNS, dan *moet* worden overgestapt op een andere manier om bedrijven en instellingen een domeinnaam te geven.

3. Wie in Nederland een domeinnaam wil registreren, dient het recht hierop aan te tonen door middel van een handelsmerk of handelsnaam. Dit heeft als voordeel dat *domain-hijacking* of *domain-grabbing* voorkomen wordt. Het nadeel is echter dat het registreren van domeinnamen voor de particulier veel minder toegangelijk is. Bij internationale domeinnamen geldt dit nadeel niet.

4. Het toepassen van het merkenrecht op domeinnamen kan allerlei problemen, zoals *hijacking* en het misbruik maken van spelfouten (zie paragraaf 4.4.4) voorkomen. De problemen die ontstaan wanneer twee bedrijven met verschillende produkten of diensten dezelfde domeinnaam willen hebben, worden hiermee echter niet opgelost. Er zijn hiervoor twee mogelijke oplossingen: (1) wie het eerst komt, die het eerst maalt, of (2) diegene die als eerste de naam als merk registreerde, heeft recht op de domeinnaam. Deze laatste heeft onze voorkeur, omdat hiermee wordt voorkomen dat iemand een naam registreert om deze later duur door te verkopen aan een bedrijf dat onder deze naam zijn produkten of diensten op Internet wil promoten.

5. De beste oplossing voor de technische problemen veroorzaakt door de gigantische groei van het aantal bedrijven en instellingen is de introductie van een database-systeem. De noodzaak voor het gebruik van eenvoudige, platte domeinnamen verdwijnt nu, bovendien kunnen gebruikers nu makkelijker zoeken naar een informatiebron, produkt of dienst. Ook andere informatie over het bedrijf kan nu beschikbaar worden gesteld. Introductie van dit systeem zal echter nogal moeilijk zijn, omdat het aanpassingen vereist in alle bestaande software. Er wordt echter wel een markt gecreëerd voor bedrijven als de “Gouden Gids.”

6. Om de handelsmerken-problematiek op te lossen, is eigenlijk alleen een wereldwijde merkregistratie voldoende. Dit heeft echter vergaande consequenties voor bestaande bedrijven, die in verschillende gedeelten van de wereld lokaal opereren op dezelfde markt. Om dit op te lossen zou gebruik gemaakt kunnen worden van nationale en internationale classificaties, waardoor lokale en internationale bedrijven elkaar “niet voor de voeten lopen.” Dit kan bijvoorbeeld door gebruik te maken van de bestaande indeling met landencodes, maar dit levert weer problemen op als een bedrijf b.v. in de Benelux werkzaam is.

6.2 Tekortkomingen

De tekortkomingen van dit rapport zijn onder meer:

1. De autoriteit van instanties als InterNIC en de Stichting Internet Domeinregistratie Nederland is niet aan bod gekomen. De vraag wie er gerechtigd is om domeinnamen uit te geven moet daarom onbeantwoord blijven. Interessant is wel dat het voorstel van de IAHC (zie paragraaf 5.2) vooral kritiek ondervond vanwege het feit dat dit voorstel strikte regels bevatte voor de beheerders van de nieuwe domeinnamen.

2. De lijst van oplossingen is helaas niet volledig. Diverse instanties houden zich bezig met deze problematiek, maar helaas betreft dit voornamelijk voorbereidend onderzoek en zijn daar nog geen concrete resultaten uit naar voren gekomen.

6.3 Aanbevelingen

De volgende aanbevelingen worden door ons gedaan;

1. Om te voorkomen dat het DNS volledig onbruikbaar wordt, moet op korte termijn overgestapt worden op een hiërarchische classificatie van informatiebronnen, produkten en diensten. De nadelen van deze stap zijn dat namen van websites minder eenvoudig te onthouden zijn, maar dit is voornamelijk een kwestie van gewenning.

2. Op de lange duur is de enige zinvolle manier om een dergelijk groot aantal hosts te kunnen doorzoeken het gebruik van een database systeem. Diensten als Yahoo of de Gouden Gids kunnen hierbij als voorbeeld dienen.

3. In de huidige situatie is het voor een bedrijf ten zeerste aan te bevelen om een domeinnaam te registreren wanneer het bedrijf verwacht ooit “op Internet” te zullen gaan. Hierdoor wordt voorkomen dat domain grabbers dezelfde domeinnaam kunnen registreren om hier misbruik van te maken.

4. Ter voorkoming van problemen dient altijd eerst een gedegen onderzoek naar het bestaan van kandidaats-domeinnamen te worden verricht. Ook namen die lijken op die van het bedrijf zouden eventueel kunnen worden geregistreerd, zodat concurrenten of grapjassen geen misbruik kunnen maken van verwarring of typefouten van gebruikers.

5. Een te registreren domeinnaam kan het beste gelijk aan het handelsmerk van het bedrijf of de organisatie genomen worden. Als de naam van het bedrijf niet geregistreerd is, kan het verstandig zijn dit alsnog te doen, om toekomstige claims over de domeinnaam te voorkomen.