11.3 DNS (Domain Name System)

Vom bisher besprochenen System her ist klar, dass jeder Rechner in einem Netzwerk durch die IP-Adresse definiert und angesprochen wird. Doch schon früh wurde deutlich, dass ein solches Zahlensystem nicht wirklich benutzerfreundlich ist. So wurde ein System zur Namensauflösung eingeführt, basierend auf einer Textdatei, *hosts.txt* (später nur noch: *hosts*) genannt, welche eine Tabelle enthält, die eine IP-Adresse einem Hostnamen zuordnet.

11.3.1 hosts

Bei *hosts* handelt es sich um eine Textdatei, die lokal auf dem System abgelegt wird und eine Zuordnung zwischen IP-Adresse und Hostname vornimmt. Die Datei existiert betriebssystemunabhängig und wird bei Unix/Linux-Systemen unter */etc/hosts* und auf Windows-Systemen unter *%Systemroot%\system32\drivers\etc* gespeichert.

Die Aktualisierung dieser lokalen Datei war aber aufwendig und die Verteilung ein logistisches Problem, je mehr Internetrechner vorhanden waren.

Die Datei ist typischerweise folgendermaßen aufgebaut:

```
# Kommentarzeilen werden mit # bezeichnet
127.0.0.1     localhost
192.168.1.20  printserv
111.24.15.20  mailsrv
```

Neben der Problematik der Verteilung wurde die *hosts*-Datei auch gerne von Viren benutzt, um Internetseitenaufrufe umzuleiten. So konnte man dann plötzlich auch solche Einträge vorfinden:

```
81.211.105.6  www.adultfindpage.com
```

Zudem war die Datei *hosts* eine Erfindung zu einer Zeit, als alle Rechner im Internet öffentlich waren. Mit der Zunahme privater Netze auf TCP/IP-Basis stellte sich das Problem, dass man diese Netzwerke gar nicht mehr automatisch per FTP aktualisieren konnte. Die ganze Problematik führte zur Definition eines neuen Systems, Domain Name System (DNS) genannt – und vorübergehend auch zu einer von Microsoft entwickelten proprietären Entwicklung namens WINS. Allerdings verfügen auch heutige Clients nach wie vor über eine *hosts*-Datei und gerade im Bereich Gefährdung durch Viren lohnt es sich, diese Datei im Problemfall anzusehen.

11.3.2 Der Windows Internet Naming Service (WINS)

Der Windows Internet Naming Service (WINS) ist die von Microsoft entwickelte Alternative mit einem System zur dynamischen Auflösung von NetBIOS-Namen. WINS konnte man auch dann einsetzen, wenn eine Namensauflösung über Broadcast nicht mehr möglich war, z. B. wegen eines Routers, der dies unterbindet.

Geht ein neuer Host ans Netzwerk, registriert er seinen Namen selbstständig beim WINS-Server, sodass ein manueller Eingriff wie das Editieren der *hosts*-Datei nicht mehr notwendig ist. Zudem registriert der Client neben dem NetBIOS-Namen auch den Namen der Domäne sowie der angemeldeten Benutzer und Gruppen. Auch wenn WINS damit ähnliche Funktionen wie das gleich zu beschreibende DNS bietet, gibt es Unterschiede: WINS arbeitet über die NetBIOS-Ports, DNS arbeitet nur mit TCP/IP. WINS arbeitet auch mit anderen Protokollen – und WINS benötigt gegenüber DNS keine eindeutige Hierarchie.

Mit Einführung von Windows 2000 hat sich Microsoft selbst von WINS wieder verabschiedet und DNS als Namensauflösung für seinen Verzeichnisdienst Active Directory implementiert. Einige Serverdienste von Windows benutzten den WINS-Dienst aber weiterhin, so z. B. Exchange 2000 oder das DFS-Dateisystem. Seit Exchange 2007 wird dagegen nirgends mehr WINS benötigt und nicht mehr eingesetzt.

11.3.3 Das Domain Name System

Das Domain Name System (DNS) wurde erstmalig 1983 beschrieben und ist seit 1987 in RFC 1034 und RFC 1035 definiert.

Das Hauptziel des DNS-Systems besteht darin, Ordnung zu erzeugen. Das bedeutet:

- Es gibt einen einheitlichen Namensraum, der frei ist von IP-Bestandteilen und der alle Knoten eines Netzes umfasst.
- Es existiert eine rasche und automatisierte Aktualisierung der Namenstabellen, damit die Informationen allen Teilnehmern zur Verfügung stehen.
- Es bestehen lokale Speicher (Caches), um die Abfragen zu beschleunigen.
- Der Namensraum kann für verschiedene Dienste und Protokolle und nicht nur für z. B. die Dienste »www« oder »http« verwendet werden.
- Die Forward-Lookup-Zone löst einen Namen in eine IP-Adresse auf.
- Die Reverse-Lookup-Zone löst eine IP-Adresse in einen Namen auf.
- Jeder Name Server kann nur die Namen und Adressen für diejenige Zone auflösen, für die er zuständig ist. Kann er die Auflösung nicht bewerkstelligen, ruft er den nächsten zuständigen Server auf.

11.3.4 Der Aufbau von DNS

In der Praxis bedeutet dies, dass DNS aus drei Bestandteilen aufgebaut ist, um einen einheitlichen Namensraum und einheitliche Verwaltungsstrukturen zu gewährleisten:

- Namensraum
- Name Server
- Resolver

Der Namensraum ist strikt hierarchisch aufgebaut und wird in mehrere Ebenen aufgeteilt. Zuoberst steht der Name ».«, er wird als root-Domain bezeichnet und liegt auf einem zentralen Root-Server (wobei dies nur theoretisch ein Server ist, dazu später mehr). Die zweite Ebene bilden die sogenannten Top-Level-Domains. Die nächstuntere Ebene sind die Second-Level-Domains, welche wiederum durch eine weitere Ergänzung in Third-Level- und weiter Subdomains unterteilt werden können.

Jeder Name muss mindestens ein Zeichen und kann maximal 63 Zeichen lang sein, er muss mit einem alphanumerischen Zeichen beginnen und darf keine Sonderzeichen enthalten sowie nicht mit '-' enden. Jede Ebene schließt mit einem Punkt. Der gesamte Domainname darf inklusive aller Punkte maximal 255 Zeichen lang sein. Groß- und Kleinschreibung werden dabei nicht unterschieden, `IANA.org`, `Iana.org` und `iana.org` führen immer zur selben Adresse. Neuere Entwicklungen lassen zudem auch Umlaute wie »ö« oder »ä« zu und Zeichen aus anderen Zeichensätzen als dem ASCII-Zeichensatz.

Während die root-Domain nur eine einzige Domain umfassen kann, die als ».« dargestellt und meist nicht geschrieben wird, gibt es mehrere Top-Level-Domains. Diese Top-Level-Domains (TLD) werden durch die ICANN verwaltet, welche 1998 gegründet worden ist und diese Funktion von der IANA übernommen hat. Der Name IANA blieb aber bestehen, weshalb es auch zu Verwirrungen über die Bezeichnung kam. Organisatorisch trägt aber seit dem Jahr 2000 die Internet Corporation for Assigned Names and Numbers (ICANN) die Verantwortung. Die ICANN koordiniert die DNS als Ganzes, insbesondere verwaltet sie die Root-Server (letztmalige Aktualisierung im Mai 2015). Zudem wacht sie über die Vergabe öffentlicher IP-Adressen sowie in Zusammenarbeit mit der IETF über die Protokollparameter und Port-Adressen der Internetprotokollfamilie.

Netzwerkpraxis – jetzt sind Sie dran

Schauen Sie sich die aktuelle Liste der Root-Server einmal selbst an unter:

`http://www.internic.net/domain/named.root`

und vergleichen Sie sie z. B. mit der Liste auf Ihrem internen DNS-Server, unter Windows zu finden unter:

%systemroot%\system32\dns\cache.dns

Gab es früher nur einige wenige TLD wie .com, .gov und .net, so hat ihre Zahl in den letzten Jahren laufend zugenommen. Es werden zudem nationale und interessenspezifische TLD unterschieden. Jedes Land hat Anrecht auf eine TLD für seine Nation, diese wird in aller Regel durch zwei Buchstaben dargestellt, also z. B. »at« für Österreich, »de« für Deutschland oder »ch« für die Schweiz. Die Regelung für diese Bezeichnungen wurde von der ISO-Norm 3166 her übernommen, die auch für Regelungen von Ländernamen in anderen Bereichen zuständig ist.

Die bisherigen Second-Level-Domains werden zur Vergabe und Verwaltung von der ICANN an verschiedene Registrarfirmen delegiert. Bekannt sind etwa VeriSign für .com- oder .net-Domänen und die EURID für die .eu-Domänen. Zudem wurden für die meisten Länder Registrare für die nationalen Second-Level-Domains bestimmt, etwa Denic für .de- oder Switch für .ch- und .li-Domänen. Von den Registraren getrennt wiederum sind in vielen Ländern die Provider, welche Adressen »verkaufen«, d. h., Sie selbst beziehen die Adresse von einem Provider, dieser leitet sie an den Registrar weiter. Doch es geht noch weiter.

Heute (d. h. seit 2013) kann jedes Unternehmen und theoretisch auch jede Einzelperson mit genügend Geld bei der ICANN eine neue TLD beantragen. So kamen unzählige neue Domains wie .swiss oder .berlin, .shop, .news oder .design etc. hinzu. Es gibt aber Bedingungen: Sie müssen zuerst einmal eine Bewerbung bei der ICANN einreichen (und bezahlen ...), das kostet Sie so um die 200‘000 Euro. Nach erfolgreicher Bewerbung müssen Sie zudem die komplette Verwaltung und den Betrieb dieser TLD sicherstellen, d. h., Sie unterhalten eigene DNS-Server und müssen die Registrierung von Adressen innerhalb Ihrer TLD verwalten. Dennoch gibt es seither Hunderte (!) neue TLD-Namen und es kommen laufend neue hinzu.

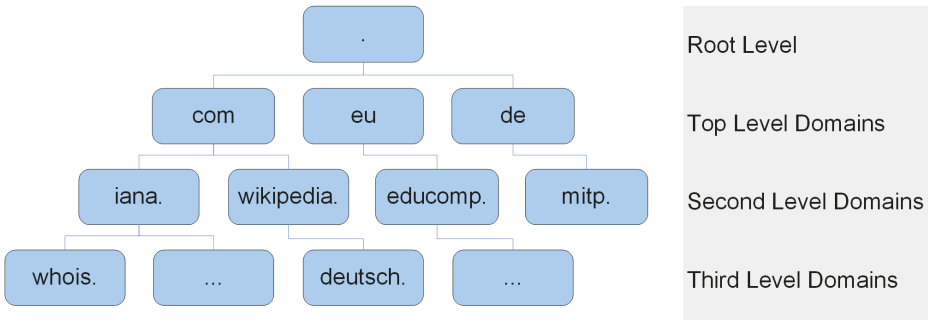

Abb. 11.3: Aufbau der DNS-Struktur

Die vollständige Adresse besteht aus der Listung aller Domains einer Adresse und diese wird dann *Fully Qualified Domain Name* (FQDN) genannt. Ein Beispiel für einen FQDN ist demzufolge `www.educomp.eu`. Man spricht in diesem Fall auch von einer absoluten Adresse, da sie im gesamten Namensraum eindeutig zugewie-

sen ist. Wenn man will, kann man zum FQDN auch noch den Port dazuschreiben, den man mit dieser Verbindung aufruft: `www.educomp.eu:2800` ruft also den Port 2800 auf. Diese Form nennt sich dann aber nicht mehr FQDN, sondern URL (Uniform Ressource Locator).

Die Objekte in der DNS (z. B. die Hosts) werden als Resource Records (RR) in einer Zonendatei gespeichert, diese wird auf einem oder mehreren autorisierten Name Servern vorgehalten. Und jetzt kommen die Root-Server wieder ins Spiel. Sie bilden die oberste Instanz und autorisieren alle unter ihnen liegenden Name Server mit den gültigen Zonendateien. Nun wäre es natürlich logistisch und sicherheitstechnisch undankbar, wenn das tatsächlich nur eine Maschine wäre. Daher werden diese Root-Server genannten Name Server redundant und auf verschiedenen Kontinenten gehalten, damit die Namensanfragen zum einen schnell und zum anderen im Falle eines Ausfalls auch sicher funktionieren. Die Root-Server unterhalten die Zonendatei für die Root-Zone. Diese Datei besteht aus ca. 2500 Einträgen und enthält die Namen und IP-Adressen der für die Top-Level-Domains (wie zum Beispiel .com, .net, .org, .de) zuständigen Name Server. Zurzeit werden 13 Root-Server betrieben, wobei diese wiederum aus mehreren Rechnern zusammengeschlossen sein können, sodass insgesamt über 100 Root-Server im Einsatz stehen.

Die Name Server selbst sind eigentlich Programme, auch wenn für die oberen Level dedizierte Maschinen eingesetzt werden. Diese Programme werden unterschieden in autoritative Name Server, welche eine Zone offiziell verwalten (als »Autorität«) und deren Informationen daher gesichert sind, und in nicht autoritative Server, welche die Informationen über mehrere andere Instanzen beziehen und deren Informationen als nicht gesichert anzusehen sind. Dazu enthält jeder Name Server für die Zonen, für die er zuständig ist, eigene Zonendateien mit den entsprechenden Informationen.

Resolver (Namensauflösungdienste) sind ebenfalls Software, welche auf den Rechnern der DNS-Dienstteilnehmer installiert ist und die zur Auflösung benötigten Informationen von Name Servern abrufen kann. Damit die DNS-Abfrage funktionieren kann, muss jeder Resolver Kontakt zu mindestens einem Name Server herstellen können. Das erklärt beispielsweise, warum Sie bei der Einrichtung einer Client-TCP/IP-Verbindung neben der IP-Adresse und dem Subnetz auch nach dem DNS-Server gefragt werden.

Ein Resolver arbeitet entweder iterativ oder rekursiv. Iterativ bedeutet in diesem Zusammenhang, dass die Anfrage, die er erhält, ihn zum nächsten Name Server weiterleitet und von dort wiederum zum nächsten, bis er die gesuchte Information findet. Rekursiv dagegen bedeutet, dass er die Anfrage des Rechners an den ihm zugeordneten Name Server weitergibt und dieser entweder die Antwort direkt erteilt oder selbst die Anfrage an weitere Name Server weiterleitet und erst zum Schluss die richtige Antwort an den Resolver übergibt. Hier übernimmt also der

Name Server die Arbeit (siehe unten stehendes Beispiel). In der Regel arbeiten die Resolver von Clients rekursiv. Die Resolver von Name Servern arbeiten dagegen iterativ.

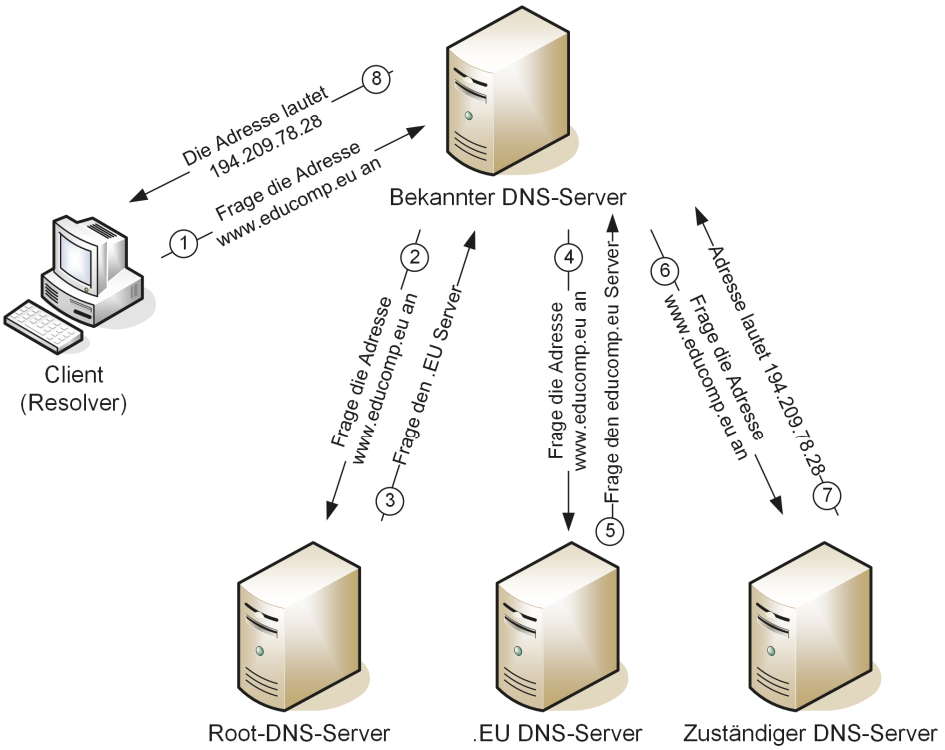

Abb. 11.4: Auflösung der Adresse educomp.eu über mehrere DNS-Instanzen

Diese drei Komponenten führen auch zu drei verschiedenen Sichten des DNS-Dienstes:

- Aus Sicht des Benutzers wird das Domain Name System durch eine einfache Anfrage des Betriebssystems zum lokalen Resolver erreicht. Dabei kann er jede Ebene des Namensraums anfragen – unabhängig davon, wo er sich selbst befindet.
- Aus Sicht des Name Servers besteht das Domain Name System aus einer Anzahl unterschiedlicher lokaler Informationen, welche Zonen genannt werden. Der einzelne Name Server verfügt über lokale Kopien einiger dieser Zonen. Er kann seine Informationen von Zeit zu Zeit aktualisieren, sei es durch aktualisierte Kopien lokaler Dateien oder durch Anfrage an andere Name Server.
- Aus Sicht des Resolvers wiederum besteht das Domain Name System aus einer unbekannten Anzahl von Name Servern. Jeder Name Server verfügt über mehr

oder weniger Informationsteile des ganzen Systems und der Resolver muss sich von diesen Name Servern die Informationen erfragen.

Jeder Domain-Name identifiziert einen Knoten im Netz. Jeder Knoten wird durch einen Satz an Informationen im Resource Record (RR) definiert. Ein vollständiger DNS-Eintrag (DNS Record) besteht aus mehreren Elementen – Owner, TTL, Class, Type und RDATA – und sieht wie folgt aus.

Resource Record:

<NAME> [<TTL>] [<CLASS>] <TYPE> <RDATA>

Owner Domain-Name, unter dem der RR gefunden wird (= Node Name)

TTL Time to Live: gibt an, wie lange der Record gecacht werden darf

Class Protokollgruppe, welcher der Record angehört, fast immer IN für Internet

Type Ist der Typ des Eintrags

rdata Besteht abhängig vom Typ aus verschiedenen Informationen

Hier eine Übersicht von wichtigen Informationen für Type und rdata:

type	Typ des Knotens – typische Angaben sind:	
	A	Host-Adresse unter IPv4
	AAAA	Host-Adresse unter IPv6
	CNAME	Alias-Name
	MX	Mail-Server-Name
	NS	Autoritativer Name Server für diese Domain
	PTR	Pointer, Domain Name Pointer (vergleichbar mit symbolischen Links)
	SOA	Identifiziert den Startpunkt der Zone
rdata	Informationen abhängig von type der Ressource. rdata enthält je nach dem beim Eintrag in der linken folgenden Spalte den Inhalt rechts:	
	A	Die IP-Adresse des Hosts (sofern es sich um einen IN-Klassen-Host handelt) unter IPv4
	AAAA	Die IP-Adresse des Hosts unter IPv6
	CNAME	Der Name der Domain
	MX	Zeigt einen Namen an, wenn der Host als Mail-Server zur Verfügung steht
	NS	Host-Name
	PTR	Domain-Name
	SOA	Diverse Informationen

Tabelle 11.1: Einträge im Resource Record

Abgefragt werden DNS-Einträge zum Beispiel mit:

- nslookup [-type=Recordtyp] Recordname [Name Server].
- nslookup -q=A -debug [Name Server] (zeigt z. B. auch TTL an)

Hierzu ein konkretes Beispiel aus einer Zonendatei:

NAME	TTL	CLASS	TYPE	RDATA
educomp.eu.	171	IN	A	92.43.216.118
www.spiegel.ch.	36383	IN	A	84.72.95.145
Kabera.ch.	7172	IN	MX	elba.interway.ch
educomp.eu.	1	IN	CNAME	www.educomp.eu

11.3.5 Das Konzept des dynamischen DNS

Bislang war von DNS als einem System die Rede, in welchem IP-Adressen fest bestimmten Namen zugeordnet sind. Dies bedingt in öffentlichen Netzwerken, dass Sie für jeden Eintrag, den Sie benötigen, eine fixe öffentliche IP-Adresse »besitzen«. Dies ist aber nicht immer der Fall.

Gerade für Nutzer von DSL-Anschlüssen mit dynamischen IP-Adressen wurden Dienste wie DynDNS oder DNS2go ins Leben gerufen. Ein solcher Dienst erlaubt das dynamische Anmelden von IP-Adressen auf Hostnamen. Dazu muss der DSL-Router diesen Dienst unterstützen oder auf einem PC muss ein DynDNS-Client installiert sein. So lassen sich Zuordnungen auch temporär einrichten, beispielsweise für die Einrichtung von dynamischen VPN-Verbindungen.

11.4 Web- und Mail-Protokolle

Für die Datenübertragung im Internet existieren eine Vielzahl von Protokollen, die je nach Anforderung Daten übermitteln, speichern, anzeigen oder abholen können.

11.4.1 HTTP

Das Hypertext Transfer Protocol (HTTP) ist ein Protokoll zur Übertragung und Anzeige von Daten über ein Netzwerk. Ursprünglich für die Suche in großen lokalen Datenbanken entwickelt, wird es seit einigen Jahren vorwiegend dazu eingesetzt, Webseiten und andere Daten aus dem World Wide Web (WWW) in einen Webbrowser zu laden.

Das Protokoll HTTP wurde Ende der 80er Jahre am CERN in Genf entwickelt, zusammen mit dem URL (Uniform Resource Locator) als Adressierungsschema und der Anzeigesprache HTML (Hypertext Markup Language). Die drei Kompo-

nenten HTTP, HTML und URL führten zum Gebilde des World Wide Web. HTTP ist dabei das Protokoll, um Webseiten oder andere Daten von einem entfernten Computer auf den eigenen zu übertragen und dort anzuzeigen.

HTTP ist ebenso wie die vorhergehenden Protokolle kommandogesteuert. Typische Kommandos sind *GET* (Hole) oder *POST* (Sende) als Methoden, wie mit Daten umgegangen werden soll.

Wenn vom Client, in der Regel ein Webbrowser, eine Anfrage via URL (z. B. http://www.mitp.de/netzwerk.html) an den Host gesandt wird, ruft dieser die angeforderte Datei (in unserem Fall netzwerk.html) auf und leitet sie dann an den Webbrowser zurück, wo sie angezeigt wird.

Was geschieht, wenn Sie im Browser die Adresse http://www.mitp.de/netzwerk.html eingeben?

Der Name www.mitp.de wird zuerst über das DNS-Protokoll (über den Resolver) in eine IP-Adresse umgesetzt, damit sie über das Routing gesucht und gefunden werden kann. Zur Übertragung wird über das TCP-Protokoll des HTTP-Servers auf den Standard-Port 80 eine HTTP-GET-Anforderung gesendet.

GET/netzwerk.html HTTP/1.1 (Befehl, Seite, Version von http)

Host: www.mitp.de (gesuchter Host)

Sobald die Anfrage beim Server angekommen ist, sendet der Host, der einen Webserver (an Port 80) betreibt, seinerseits eine HTTP-Antwort zurück. Diese besteht aus den Header-Informationen des Servers und dem tatsächlichen Inhalt der Nachricht, also dem Inhalt der Datei netzwerk.html. Die Daten werden standardmäßig in der Seitenbeschreibungssprache HTML (neuer XHTML) und ihren Ergänzungen wie Skripts, CSS etc. übertragen. Auch eine dynamische Übertragung wie eine Datenbankabfrage über ein PHP-Skript sind möglich.

Die Antwort kann dann wie folgt aussehen:

HTTP/1.1 200 OK

Server: Apache/2.0.2 (Unix) PHP/4.3.4

Content-Length: (Größe von netzwerkt.html in Byte)

Content-Language: de

Content-Type: text/html

Connection: close

Inhalt von netzwerk.html

Grundlegend ist HTTP ein zustandsloses Protokoll. Das bedeutet auch, dass nach erfolgreicher Datenübertragung die Verbindung zwischen den beiden Kommuni-

kationspartnern nicht aufrechterhalten wird. Sollen weitere Daten übertragen werden, muss zunächst eine weitere Verbindung aufgebaut werden. Dies führt je nach Aufbau der gefragten Seiten (z. B. wegen eingebetteter Bilder) zu einer großen Anzahl offener HTTP-Verbindungen, einem Problem, dem man sich mit der Entwicklung von HTTP1.1 annahm. In HTTP1.1 können mehrere Anfragen und Antworten pro TCP-Verbindung übermittelt werden. Für ein HTML-Dokument wird auch mit mehreren Elementen nur eine TCP-Verbindung benötigt. So wird die Ladezeit für die gesamte Seite signifikant verkürzt. Zusätzlich können bei HTTP/1.1 abgebrochene Übertragungen wieder aufgenommen und fortgesetzt werden.

Eine weitere Entwicklung ist HTTPS (Hypertext Transfer Protocol Secure), das eine zusätzliche Anwendungsschicht zwischen HTTP und dem Transportprotokoll TCP definiert. Ziel von HTTPS ist die Verschlüsselung der Information. Ohne Verschlüsselung sind Webdaten für jeden, der Zugang zum entsprechenden Netz hat, als Klartext lesbar. Das ist an sich schon unschön, aber mit der Ausbreitung von Finanzgeschäften wie Online-Banking und E-Shopping nimmt die Bedeutung der Verschlüsselung laufend zu.

HTTPS wurde von der Firma Netscape entwickelt und zusammen mit SSL 1.0 im Jahr 1994 als Bestandteil des eigenen Netscape-Browsers veröffentlicht. Mit HTTPS wird die Kommunikation zwischen Browser und Webserver auf Applikationsebene verschlüsselt und authentifiziert. Mittlerweile wurde allerdings SSL durch das Protokoll TLS abgelöst. Die Verschlüsselung dient der Lauschsicherheit, die Authentifizierung der Identitätssicherheit – beides Themen, die Sie in Kapitel 15 »Sicherheitsverfahren« noch ausführlicher kennenlernen werden.

Der von Netscape eingeschlagene Weg in der Entwicklung von HTTPS führte dazu, dass HTTPS bis heute im Browser (wie etwa Firefox, Opera, Internet Explorer, Safari) integriert ist. Die Installation zusätzlicher Software ist damit im Unterschied zur Nutzung von SMTP/POP (Mail-Client) oder SSH (Terminal-Client) nicht notwendig.

Quelle: CompTIA Network+

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

ISBN 978-3-95845-857-4
7. Auflage 2018

www.mitp.de
E-Mail: mitp-verlag@sigloch.de
Telefon: +49 7953 / 7189 - 079
Telefax: +49 7953 / 7189 - 082