3 Wie werden Internetdienste erbracht?

Bei der Erbringung der Internetdienste (damit ist die Gesamtheit aller Möglichkeiten des Internets gemeint) sind Server notwendig, die mit zweckmässiger Software und Hardware ausgerüstet sein müssen.

Die hier aufgeführten Anforderungen für einen Internetserver beziehen sich auf einen professionellen Server, der für mehrere Kunden und mehrere Dutzend gliechzeitige Benutzer ausgelegt ist. Solche Server sind vor allem bei einem Internet Service Provider im Einsatz. Für den Betrieb eines Internetservers für eine einzelne, kleinere KMU-Firma reicht es durchaus, die Werte für den professionellen Betrieb zu halbieren, womit der Preis eines eigenen Internet-Servers auch für eine kleinere Unternehmung erschwinglich wird.

3.1 Welche Systeme werden benötigt?

Je nach Budget und Anforderungen empfiehlt es sich in der Praxis, für die einzelnen Dienste jeweils separate (sogenannt «dedizierte») physische Server aufzusetzen. Gründe dafür sind:

- eine erhöhte Leistungsfähigkeit,
- eine verbesserte Sicherheit, die für jedes einzelne System separat konfiguriert werden kann,
- und ein kleineres Ausfallrisiko. Ein «single point of failure» kann vermieden werden, d. h., wenn ein physischer Rechner abstürzt, sind nicht alle Dienste (WWW, E-Mail, FTP etc.) davon betroffen.

Um die Verfügbarkeit noch weiter zu erhöhen, besteht die Möglichkeit, mehrere Server zu einer logischen Einheit zusammenzuschliessen: der Fachbegriff dafür lautet «Cluster». Dabei stehen zwei oder mehr Systeme miteinander in Verbindung, treten aber gegenüber dem Besucher als ein System auf (welches auch unter einer Domain bzw. IP-Adresse erreichbar ist). Ein sogenannter «Load-Balancer» verteilt dabei die Anfragen gleichmässig auf die dahinter liegenden physischen Rechner. Die Last wird so gleichmässig verteilt, und falls ein Rechner ausfällt, übernimmt der «Nachbar» einfach die anstehenden Anfragen und verarbeitet diese weiter. Zu diesem Zweck müssen die beiden Systeme synchronisiert werden; die Software der einzelnen Dienste muss ein solches «clustering» vorzugsweise unterstützen.

Im Rahmen dieses Moduls werden wir die verschiedenen Dienste auf einem einzelnen physischen Rechner aufsetzen und konfigurieren. Clustering und dedizierte Systeme werden in diesem Modul nicht aufgesetzt.

3.2 Die Auswahl der Server-Hardware

Auswahlkriterien

Die für einen Internet-Server benötigte Hardware richtet sich nach verschiedenen Faktoren:

- Dienste, die angeboten werden (WWW, E-Mail etc.)
- Anzahl der Benutzer, die gesamthaft auf den Server zugreifen können (sogenannte «named user») und Anzahl der Benutzer, die gleichzeitig auf den Server zugreifen (sogenannte «concurrent user» oder «concurrent sessions»)
  Die «named user» sind alle berechtigten Benutzer auf einem Server; die «concurrent

user» sind alle Benutzer, die gleichzeitig zugreifen. Es kann beispielsweise 100 berechtigte Benutzer auf einem Server geben, aber es werden maximal 20 gleichzeitig zugreifen.

- Menge an Daten (Volumen), die up- und gedownloaded werden (z. B. hat ein FTP-Server typischerweise eine grosse Datenmenge, die meist heruntergeladen wird; ein statischer Webserver wird ein mittelmässiges Volumen erzeugen und beim Mailserver kommt es stark auf das Benutzerverhalten und die Konfiguration an, insbesondere wenn grosse Anhänge (Attachments) erlaubt sind)
- Geschwindigkeit der Anbindung an das Netzwerk (diese hängt auch von den zu erwartenden Benutzermengen ab)
- Für die Auslastung nicht zu vergessen sind auch andere Systeme, die an den Internetserver angeschlossen sind und sich quasi «selbstständig» bedienen, also Daten abholen oder Daten zur Verfügung stellen (z. B. Datenbank-Server)
- Zukünftige Erwartungen an die oben genannten Faktoren und Investitionsschutz (d. h. man plant und budgetiert von vornherein ein eher grosszügiges und für die aktuellen Bedürfnisse überdimensioniertes System, das auch für zukünftige Anforderungen ausreicht). Dieser Faktor wird oft mit dem Fachbegriff «Skalierbarkeit» ausgedrückt.
- Zur Verfügung stehendes Budget für die Hardware

Rechnerarchitektur und Peripherie

Grundsätzlich unterscheidet man zwischen der «Intel-Architektur», d. h. Servern die auf x86-Architektur aufbauen (Intel, AMD Prozessoren) und SUN-Systemen, die auch oft eingesetzt werden. Grössere Systeme (IBM AS/400 etc.) können zwar auch als Internet-Server betrieben werden, sind aber nicht primär dafür ausgelegt. Mac OS von Apple bietet auch die Möglichkeit, einen Internetserver zu betreiben.

Die verwendete Architektur hat zum Teil direkten Einfluss auf das Betriebssystem, das installiert wird:

- x86-Server werden mit Windows (Version für Server oder Workstation) oder mit Linux betrieben.
- SUN-Server werden mit SUN's eigenem Betriebssystem, Solaris, betrieben.

Für die in diesem Lehrmittel verwendeten Beispiele wird aus lizenzrechtlichen Gründen das freie Betriebssystem Linux (Distribution SuSE, bzw. openSUSE) auf x86-Hardware verwendet.

Ein Internetserver stellt weniger Anforderungen an die Peripheriegeräte als ein herkömmlicher PC/Workstation. So wird im Normalfall weder ein Drucker benötigt, noch sind verschiedene Anschlüsse wie USB, Firewire, Infrarot oder Ähnliches nötig. Spezialisierte Systeme, die sich für den Einbau in Serverschränke eignen (sogenannte «rack-mountable devices») werden in verschiedenen Höhen (gemessen in «height units, HU oder einfach U» oder «HE, Höheneinheiten») angeboten und haben eine Standard-Breite von 19 Zoll. Oft wird für solche 1HU-Einheiten die Bezeichnung «Pizzabox» verwendet, wegen der Ähnlichkeit mit einer Pizzaschachtel.

Hardware-Komponenten

Die wichtigsten Hardware-Komponenten eines Internetservers sind folgende:

- RAM: Je mehr Benutzer vorhanden sind, desto mehr Arbeitsspeicher wird benötigt. Grundsätzlich sollte ein moderner Internetserver, unabhängig von der gewählten Hardware-Architektur, mit mindestens 1 GB RAM betrieben werden.
- Prozessor: Der Prozessor spielt bei einem Webserver eine untergeordnete Rolle. Je mehr Applikationen auf einem Server betrieben werden, desto schneller sollte der Pro-

zessor sein. Ein Internetserver wird aber typischerweise keine hochkomplexen Berechnungen durchführen müssen (das ist die Aufgabe des Applikationsservers). Es wird jedoch empfohlen, einen Server-Prozessor einzusetzen (z. B. Intel's Xeon) und weniger einen Prozessor für mobile Geräte (Intel's Celeron).
Eine Ausnahme gibt es, wenn der Internetserver die Verschlüsselung von Daten vornimmt (z. B. für https/SSL oder als E-Mail-Verschlüsselungs-Gateway). Verschlüsselungsoperationen sind sehr arbeitsintensiv und benötigen deshalb einen entsprechend schnellen Prozessor.

- Harddisk: Die Harddisk sollte so ausgelegt sein, dass sie mindestens doppelt so gross ist wie die zu verwaltende Datenmenge inklusiv Betriebssystem. Besonders berücksichtigt werden muss die anfallende Menge an Log-Dateien, um die Harddisk nicht schon nach wenigen Tagen volllaufen zu lassen. Es empfiehlt sich daher, Log-Dateien auf einem separaten Server zu speichern (sogenannter «Logserver») und nicht auf dem Internetserver. Besonders grosse Platzansprüche haben insbesondere Fileserver (FTP) und E-Mailserver (je nach Anzahl E-Mail-Benutzer und erlaubte Attachments). Wichtig ist bei der Auswahl der Harddisk der Typ. In einem Server sollten grundsätzlich SCSI-Harddisks eingebaut werden, da diese eine höhere Beständigkeit haben als anderen Typen (aber auch teurer sind).
- Netzwerk: Ein Internetserver verfügt über einen oder auch zwei bis mehrere Netzwerkanschlüsse. Dabei wird die Bezeichnung «single homed» (1 Netzwerkanschluss), «dual homed» (2 Netzwerkanschlüsse) oder «multi-homed» (mehrere Netzwerkanschlüsse) verwendet. Für jeden einzelnen (physischen) Netzwerkanschluss besteht die Möglichkeit, eine separate IP-Adresse zu konfigurieren. So kann der Internetserver gleichzeitig in verschiedenen Netzwerken betrieben werden, um so aus Sicherheitsgründen verschiedene Dienste über verschiedene Adressen laufen zu lassen. Typischerweise werden die Benutzerdienste auf dem «externen» Interface betrieben, während die Administration des Servers nur über das «interne» Interface möglich ist. Beim Netzwerk-Interface ist darauf zu achten, dass es für die benötigte Geschwindigkeit ausgelegt ist. Es werden heutzutage folgende drei Typen von Netzwerk-Interfaces unterschieden: 10/100 Mbit, 10/100/1000 Mbit (sogenannte Gigabit-Interfaces) und Kupfer und Gigabit-Lichtleiter (Glasfaser) Interface. Für den normalen Einsatz reicht heutzutage ein 10/100 Mbit Interface grundsätzlich aus, da ein Internet-Server in einer KMU-Firma selten mit einer Gigabit-Leitung ans Internet angebunden wird.

3.3 Die Auswahl der Server-Software

Begriffserklärung

In diesem Zusammenhang muss auf die Doppeldeutigkeit des Wortes «Server» hingewiesen werden: Sowohl der physische Rechner als auch entsprechende Software wird in der Informatikwelt als «Server» bezeichnet. Der Grund ist die Bedeutung des Wortes in der englischen Sprache: «to serve» bedeutet «zu dienen», die Hauptaufgabe des Servers: er dient dem Client (Kunden), der Anfragen an den Server schickt. So ist sowohl die Hardware ein (physischer) Server, wie auch die Software, die die Anfragen des Client beantwortet, ein (software)-Server. Das gleiche gilt übrigens auch für den Client: Der physische Rechner und die Software, die eine Anfrage stellt, werden als (physischer oder Software)-Client bezeichnet. Beispiel: Der Browser (Software-Client), der auf einem physischen Client (Notebook) installiert ist, stellt dem (physischen) Server beim Internet Service Provider eine Anfrage (zeige mir die Webseite der Domain www.symlink.ch). Diese Anfrage wird vom Software-Webserver beantwortet.

Server-Betriebssysteme

Für den Betrieb des Internetservers ist ein Betriebssystem notwenig, das zur Software gezählt wird. Je nach Betriebssystem sind gewisse Software-Pakete für den Betrieb bereits inbegriffen.

Es ist empfehlenswert ein «serverbasiertes» Betriebssystem einzusetzen. Damit ist z. B. Windows 2003 Server oder eine Server-Edition eines Linux-Betriebssystems gemeint. Mac OS verfügt ebenfalls über eine Server-Version. Andere (unix-artige) Betriebssysteme wie beispielsweise SUN's Solaris sind von Grund auf als Serversystem ausgelegt.

Serverbasierte Betriebssysteme haben den Vorteil, dass sie für einen ständigen Betrieb des Systems ausgelegt sind. Überwachungs- und Monitoringmöglichkeiten sind vorhanden, oder entsprechende Schnittstellen sind vorgesehen. Allgemein ist die Stabilität des Betriebssystems für den Dauerbetrieb optimiert. Dieser Vorteil wird durch Verzicht auf Fähigkeiten erkauft, die typischerweise bei Desktop-Betriebssystemen zu finden sind: Audio- und Multimedia-Unterstützung, Treiber für eine Vielfalt von (desktop-typischen) Peripheriegeräten wie z. B. Drucker, hochauflösende Bildschirme, Multimedia-Geräte etc. Die Serversysteme sind ausserdem oft «gehärtet», d. h. grundsätzlich ist nur ein Minimum an Diensten automatisch eingeschaltet, um Sicherheitsrisiken möglichst auszuschliessen.

Desktop-Betriebssysteme

Dies bedeutet nicht, dass heutige moderne Desktop-Betriebssysteme (Windows XP Professional, Linux Workstation Edition) nicht fähig wären, als Internetserver betrieben zu werden. Nötigenfalls müssen aber Konfigurationen angepasst und Dienste deaktiviert werden, damit die nötige Leistungsfähigkeit und Sicherheit erreicht werden kann.

Übungs-Betriebssysteme

Für die Beispiele des Lerhmittels wird das Betriebssystem SuSE Linux 10 OSS (open source system) eingesetzt. Es kann von der Website http://www.opensuse.org herunterggeladen und installiert werden.

Dieses (desktop-basierte) Betriebssystem enthält ausschliesslich open-source-Komponenten und ist deshalb frei von lizenzrechtlichen Einschränkungen. Andere Betriebssysteme müssen sowohl in der Desktop- wie auch in der Server-Variante lizenziert werden. Eine Ausnahme bildet SUN's Solaris, welches inzwischen auch als open-source-Edition verfügbar ist. Da Solaris aber spezielle Anforderungen an Hardware, Installations- und Betriebsvorgehen erfordert, wurde darauf verzichtet.

Software für Anwendungen

Für die Realisierung der verschiedenen Dienste des Internetservers werden die folgende Softwarekomponenten benötigt:

- Webserver: Bekannte Webserver sind Microsoft's Internet Information Server (IIS) und der open-source Webserver «Apache»
- Mailserver: Der Mailserver setzt sich einerseits aus dem sogenannten «Mail Transfer Agent» (MTA) zusammen, der nichts anderes macht als die E-Mails zu versenden. Der MTA wird oft auch als «SMTP-Server» bezeichnet, in Anlehnung an das für den Mailversand benötigte Protokoll SMTP. Neben dem MTA wird für den sinnvollen Betrieb eines Mailservers auch ein Postfach benötigt, wo die E-Mails für die Benutzer gespeichert werden. Das Postfach ist der eigentliche «Briefkasten» und ist (technisch gesehen) unabhängig vom MTA. Der MTA ist sozusagen der «Pöstler», der die Briefe zu-

stellt (entweder an einen anderen, entfernten Mailserver, oder an den «benachbarten» Briefkasten).

- FTP-Server: Der File-Transfer-Server ist technisch gesehen nichts anderes als ein Software-Aufsatz auf das Dateisystem (file system), das die Übertragung der Dateien über das FTP-Protokoll ermöglicht. Neben der Kommunikation mit einem FTP-Client (der nötig ist, um eine Datei über das FTP-Protokoll zu senden oder empfangen) verwaltet der FTP-Server oft auch die Benutzerberechtigungen, d. h. welcher Benutzer auf welchem Verzeichnis lesen oder schreiben darf.
- DNS-Server: Der DNS-Server ist eine Software, die auf dem Port 53 auf Anfragen wartet und diese (sofern der Client der die Anfrage stellt, berechtigt ist) mit den Informationen beantwortet, die der DNS-Server im Konfigurationsfile (das sogenannte «Zonen-File») gespeichert hat. Der DNS-Server ist so gesehen eine relativ einfache Software, die im «Telefonbuch DNS» nach der IP-Adrese sucht, die für einen Domainnamen angefragt wurde.

Die Bearbeitung der Anfrage der verschiedenen Anwendungen

Sie erfolgt mit einem «daemon». Damit wird ein Server-Prozess auf dem Betriebssystem gemeint, der auf bestimmte Anfragen/Ports horcht und diese an den entsprechenden Serverprozess weiterleitet (oder selbst bearbeitet und beantwortet). Der httpd (http-daemon) horcht somit auf dem Port 80 des Webservers auf Anfragen von Clients (Browser). Sobald eine Anfrage eintrifft, erfolgt ein TCP-handshake und die Verbindung wird aufgebaut. Dabei erfolgt der Verbindungsaufbau vom Client aus über einen Port >1023, der http-daemon horcht auf Port 80. Die eigentliche Kommunikation wird daraufhin vom daemon auf einen Port >1023 gelegt, damit der Port 80 für weitere Anfragen frei bleibt. Server und Client kommunizieren nun beide mit Ports >1023, die innerhalb eines definierten Bereichs frei gewählt werden (z. B. Client sendet Anfragen von Port 14411, Server nimmt diese entgegen auf Port 28330). Nur die ursprüngliche Verbindungsanfrage erfolgte auf Port 80, danach einigen sich daemon und Client auf einen nicht-belegten Port >1023.

Weitere Softwarekomponenten

Für den reinen Betrieb des Internetservers wird neben der oben aufgeführten Software der Anwendungen grundsätzlich keine weitere Software benötigt. Oft wird für die Überwachung/Monitoring des Servers weitere Software installiert, die beispielsweise die Fernwartung erlaubt oder bestimmte Meldungen an ein remote-System schickt. Zudem kann der Webserver so konfiguriert werden, dass er auf verschiedenen Ports auf Verbindungsanfragen horcht, sodass z. B. auf Port 80 normale Client-Anfragen an den Webserver beantwortet werden und über Port 8080 ein Administrations-Interface für den Entwickler der Website zur Verfügung gestellt wird.

3.4 Internetprotokolle

Im vorangegangenen Kapitel wurden bereits einige der Internetprotokolle erwähnt. Nachfolgend sind die wichtigsten Grundlagen dazu zusammengefasst. Das reibungslose Zusammenspiel der verschiedenen Protokolle ist durch die eingesetzte Software gewährleistet. Für das Verständnis ist es wichtig, den stufenweisen Aufbau der beteiligten Komponenten zu kennen.

Die Kommunikationsdienste sind auf 7 Stufen (Layers) angeordnet. Diese sind als OSI-Schichtenmodell bekannt geworden. Die TCP/IP-Protokollfamilie hat aber nur 4 Schichten, die dem OSI-Schichtenmodell zugeordnet werden können. Die folgenden detaillierten Erklärungen zu den Schichten und den zugeordneten Diensten sind dem Wikipedia entnommen (http://de.wikipedia.org/wiki/OSI-Modell).

OSI-Schicht Layer	Schichtname Englisch	Schichtname Deutsch	Einordnung	TCRIP-Schicht	Protokollbeispiele
7	Application	Anwendung	Anwendungsorientiert	Application	HTTP FTP HTTPS NCP
6	Presentation	Darstellung			
5	Session	Sitzung			
4	Transport	Transport	Transportorientiert	Transport oder Host to Host	TCP; UDP SPX
3	Network	Vermittlung		Internet	IP IPv6 IPX
2	Data Link	Sicherung		Link oder Network	Ethernet Token Ring FDDI ARC NET
1	Physical	Bitübertragung			

- **Layer 1 (Physical Layer, Bitübertragung):**
  - Koaxial, Kupfer- oder Glasfaser-Verkabelungen mit entsprechenden Steckern (RJ45, Koax etc.)
  - Hardware: Auf dieser Schicht werden Hubs und Bridges eingesetzt.
  - Vergleichbar mit der Strasse in der realen Welt
- **Layer 2 (Data Link Layer, Sicherung):**
  - Für TCP/IP-basierte Kommunikation kommt auf Layer 2 vor allem das Ethernet-Protokoll (802.16) sowie je nach Einsatzzweck Wireless LAN (802.11) zum Einsatz. Um Netzwerke in logische Einheiten zu unterteilen, werden sogenannte «Virtual LANs» gebaut, mit der Abkürzung «VLAN» (nicht zu verwechseln mit WLAN für Wireless LAN).
  - Hardware: Auf dieser Schicht werden Switches eingesetzt.
  - Vergleichbar mit den Strassennummern in der realen Welt (MAC-Adressen als phyisische, eindeutige Adresse der Netzwerkkarte)
- **Layer 3 (Network Layer, Vermittlung)**:
  - IP Internet Protocol (die IP-Adresse)
  - Hardware: Auf dieser Schicht werden Router und Paketfilter eingesetzt.
  - Vergleichbar mit den Namen an den Haustüren (die logische Adresse, d. h. diese kann ändern und ist nicht fest zugeteilt wie die physische MAC-Adresse)
- **Layer 4 (Transport Layer, Transport)**:
  - ICMP Internet Control Message Protocol (time to live, traceroute, PING)
  - TCP Transport Control Protocol (stateful, d. h. eine Verbindung wird aufgebaut mit Informationen, ob ein Paket angekommen ist oder nicht; vergleichbar mit einem eingeschriebenen Brief)
  - UDP User Datagram Protocol (stateless, ohne Verbindungsinformation; keine Informationen, ob ein Paket ankommt; vergleichbar mit einer Postkarte)
  - Hardware: Auf dieser Schicht werden Firewalls eingesetzt.
- **Layer 5 (Session Layer, Sitzung)**:
  - SSL Secure Session Layer (ursprünglich 1995 von Netscape entwickelt, um eine Verschlüsselung primär für http zu ermöglichen; SSL ist kein offizieller Standard)
  - TLS Transport Layer Security (die offizielle Nachfolge von SSL, von der Internet Task Force verabschiedeter Standard)

  - Durch die Positionierung von SSL und TLS auf Layer 5 ist es möglich, die darüberliegenden Protokolle damit abzusichern (dadurch nicht nur http, welches damit zu https wird, sondern auch andere Protokolle wie z. B. POP3 etc. je nach Eignung)
  - Hardware: keine besondere, evtl. SSL/TLS-Accelerator (spezieller Proxy, der die Ver- und Entschlüsselung der Daten vornimmt um andere Geräte nicht zu belasten, insbesondere eingesetzt bei stark besuchten Webseiten mit SSL/TLS-Verschlüsselung)
- **Layer 6 (Presentation Layer, Darstellung)**:
  - Auf der Präsentationsschicht wird geregelt, in welcher Form die Daten auf der Applikationsschicht (Layer 7) ausgetauscht werden; also z. B. um welchen Datentyp es sich bei einem E-Mail-Attachment handelt (Text, binäres Objekt, Bild, PDF-File etc).
  - Hardware: keine besondere
- **Layer 7 (Application Layer, Anwendung)**:
  - **http** Hypertext Transfer Protocol (das Fundament für das World Wide Web, Besonderheit: Hyperlink ermöglicht es, auf andere http-Adressen zu springen), Standardport: 80 (TCP)
  - **https** (durch SSL oder TLS abgesicherte Variante von http), Standardport: 443 (TCP)
  - **ftp** File Transfer Protocol (wird eingesetzt, um Dateien up- oder downloaden), Standardport: 20 (data port bei «active FTP») und 21 (control port bei «active FTP», Standardport für «passive FTP») (TCP)
  - **dns** Domain Name Service (zur Auflösung von Domainnamen in IP-Adressen und umgekehrt), Standardport: 53 (UDP oder TCP; immer TCP für Zonentransfers)
  - **smtp** Simple Mail Transfer Protocol (Dienst, um Mails im Internet zu verschicken und empfangen), Standardport: 25 (TCP)
  - **pop3** Post Office Protocol v3 (Dienst, um Mails von einem Postfach mittels eines E-Mail-Client abzuholen; es gibt auch eine sichere Variante: POP3/S mit SSL/TLS), Standardport: 110, POP3/S: 995 (TCP)
  - **imap4** Internet Message Access Protocol (alternativer Dienst zu POP3, der es erlaubt, das Postfach mittels Befehlen zu verwalten, ohne die Mails downloaden zu müssen; benötigt einen entsprechenden Mailclient, der IMAP beherrscht), Standardport: 143, IMAP mit SSL/TLS: 993
  - Hardware: Auf Schicht 7 kommen Proxies oder sogenannte Application Level Gateways zum Einsatz und natürlich die entsprechenden (physischen) Server wie Webserver, Mailserver, Fileserver etc.

3.5 Technischer Aufbau: die Architektur

Für den Aufbau eines Internetserver stehen verschiedene Architekturen zur Verfügung, die nachfolgend vorgestellt werden:

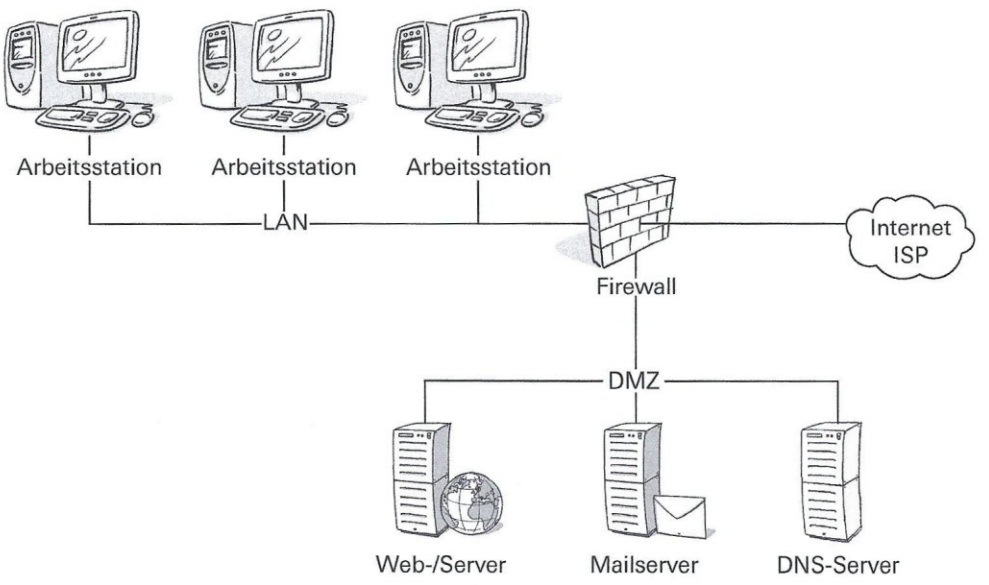
Internetserver in einer demilitarisierte Zone (DMZ)

Mit dieser Zone ist ein geschützter Netzwerkteil gemeint. Dort werden exponierte Systeme (Webserver, Mailserver, DNS Server) aufgebaut und betrieben. Dabei handelt es sich um ein vom restlichen LAN getrenntes Netzwerk mit separater IP-Range bzw. eigenem Subnetz. Die Abtrennung erfolgt durch eine Firewall bzw. Paketfilter. Grundsätzlich erfolgt die Konfiguration wie folgt:

- Von aussen (Internet) in die DMZ: erlaubt ist Web-, Mail- und wenn nötig DNS-Verkehr; weitere Dienste nur soweit nötig
- Von aussen (Internet) in das LAN: keine Verbindungen erlaubt

- Vom LAN nach draussen (Internet): Verbindungen erlaubt (evtl. Restriktion auf Webverkehr, port 80 und 443)
- Vom LAN zur DMZ: je nach Bedarf (z. B. wenn das Intranet ebenfalls auf dem DMZ-Webserver läuft dann Webverkehr erlauben), zudem müssen die E-Mails abgeholt werden können. Oft befindet sich aber der Server mit dem Postfach im LAN und in der DMZ ist nur der SMTP-Server aufgesetzt, der die Mails nach draussen verschickt und entgegennimmt und an das Postfach weiterleitet.

Die demilitarisierte Zone ist die üblichste Architektur für den Betrieb eines Internetservers.



Internetserver beim Internet Service Provider (ISP)

Hosting: Der Internetserver wird nicht vom Unternehmen selber, sondern von einem Provider betrieben. Entsprechend liegt der Internetserver nicht im unternehmenseigenen Netzwerk. Typischerweise sind Dienste wie SMTP und POP3 eingeschaltet (für berechtigte Benutzer) und Webverkehr natürlich auch (da keine Unterscheidung gemacht wird ob interner oder externer Benutzer, da aus Sicht des Providers alle Benutzer von aussen kommen).

Internetserver im LAN

Internetserver im LAN betreiben: Falls keine DMZ möglich ist, kann der Internetserver auch innerhalb des LAN betrieben werden. Dabei handelt es sich aber um eine «gefährliche» Architektur, da ein Angreifer dadurch zumindest auf den freigegebenen Diensten einen Zugriff auf einen Server im LAN hat (den Internetserver). Durch einen Bug kann er so Zugriff aufs interne Netzwerk erlangen, was bei der DMZ nur bedingt möglich ist.

Beim internen Betrieb müssen die entsprechenden Dienste auf der Firewall freigeschaltet werden. Am besten werden die Pakete NUR an den Internetserver weitergeleitet. Oft ist auch NAT (Network Adress Translation) im Einsatz, weshalb ein Port-Forwarding nötig ist, da der Internetserver durch das NAT on aussen nicht sichtbar ist.

3.6 Anbieter und Abnehmer

Ein Internetserver kann in Eigenregie betrieben werden (inhouse), womit sämtliche Administrationsaufgaben vom Administrator durchgeführt werden müssen. Eine andere Möglichkeit besteht darin, den Betrieb des Internetservers an einen Internet Service Provider (ISP) auszulagern. Dabei werden drei hauptsächliche Betriebsarten unterschieden:

- **Hosting**: Beim Hosting wird beim ISP ein sogenannter virtueller Webserver für eine monatliche oder jährliche Gebühr gemietet. Der ISP richtet dafür auf einem physischen Server einen Webserver ein, der für mehrere Domains (und so für verschiedene Kunden) konfiguriert ist. Der Kunde bekommt in diesem Angebot einen definierten Speicherplatz und die Möglichkeit, via FTP oder z. T. auch WebDAV auf das für ihn definierte Verzeichnis zuzugreifen und den Webauftritt zu gestalten. Oft sind auch Datenbanken, Scripts und Auswertungsdienstleistungen im Angebot enthalten sowie die Möglichkeit, ein Postfach mit mehreren Adressen unter der reservierten Domain einzurichten. Die Administrationsmöglichkeiten beschränken sich im Normalfall auf den Zugriff auf das Dateisystem und einer webbasierten Konfigurationsoberfläche. Dabei ist es wichtig, dass es sich physisch um einen einzigen Rechner handelt. Dementsprechend besteht bis auf Layer 4 keine wirkliche Trennung zwischen den einzelnen Domains, d. h. alle Domains sind unter der gleichen IP-Adresse erreichbar (und alle offenen Ports sind für alle Domains geöffnet). Ein Ausfall der Harddisk oder des Netzteils betrifft so alle Domains, die auf diesem Rechner verwaltet werden; gleiches gilt für eine Fehlkonfiguration auf der Netzwerk- oder Benutzerverwaltungsebene und natürlich im Web- oder Mailserver (Layer 7) selbst.
- **Root-Server (Leasing, Renting):** Beim sogenannte root-Server stellt der Provider einen Server zur Verfügung, der voll im Zugriff des Kunden liegt (root = Administrator). Der Provider führt evtl. zusätzliche Dienstleistungen aus (reboot, Back-up), da ein physischer Reboot aus Distanz nicht möglich ist. Für das aufsetzen und pflegen des Servers ist der Kunde selber verantwortlich. Je nach Bedarf kann auch eine Firewall dazu gemietet werden, die ebenfalls selber oder durch den Provider gepflegt wird.
- **Housing/Co-location:** Beim sogenannten Housing stellt der Provider lediglich die Infrastruktur des Rechenzentrums zur Verfügung (Strom, Klima, Platz, Internet-Zugang, Routing). Der Server wird vom Kunden gebracht und an das Netz angeschlossen und völlig unabhängig vom Provider betrieben. Oft stellt der Provider für die Kunden eine Möglichkeit des (physischen) Reset/Reboot zur Verfügung, welche von Remote (d. h. aus Entfernung) genutzt werden kann, da ansonsten für den Reboot der Kunde ins Rechenzentrum müsste.

Repetitionsfragen

20	Welche Systeme werden für einen Internetserver benötigt?
24	Welches sind die zwei Haupt-Einflussfaktoren für die Dimensionierung der Hardware?
2	In welche zwei Typen lässt sich die für einen Internetserver eingesetzte Software einteilen?
7	Welches ist das grundlegende Protokoll, das für einen Internetserver verwendet wird?
12	Was ist der Unterschied zwischen Hosting und Housing?