6 Lösung entwerfen

In den folgenden Kapiteln werden die notwendigen Schritte für den Entwurf eines Internetservers, von der Hardware über Software sowie Setup- und Betriebsdokumentation, im Detail dargelegt.

6.1 Benötigtes Know-how aneignen und planen

Das vorliegende Lehrmittel soll genau das Know-how vermitteln, das für das aufsetzen und betreiben eines Internetservers benötigt wird. Dennoch gibt es in der Praxis oft Fälle, bei denen professionelle Hilfe von aussen benötigt wird oder neue, noch nicht bekannte Technologien oder Systeme eingesetzt werden sollen. Besonders wenn der Internetserver sehr «exponiert» ist, das heisst, er erfüllt eine besonders geschäftskritische Aufgabe, muss der stabile Betrieb absolut gewährleistet werden.

Je nach zur Verfügung stehender Zeit und Budget kann das benötigte Know-how entweder angeeignet werden (mit Kursen, Ausbildungen etc.) oder es wird (zusätzliche) externe Hilfe von professionellen Anbietern beigezogen. Wenn der Internetserver für geschäftskritische Anwendungen (E-Business etc.) eingesetzt wird, empfiehlt es sich oft eine zusätzliche Sicherheitsüberprüfung durch eine spezialisierte Drittfirma vornehmen zu lassen. Damit erhält man eine unabhängige Bestätigung, dass die Anforderungen an das System erfüllt sind.

6.2 Benötigte Hardware festlegen

Bevor die Software für den Internetserver ausgewählt wird, muss der Server physisch aufgebaut werden. Die dazu benötigte Hardware ist zu bestimmen und anzuschaffen. Je nach Einsatzzweck kostet die Hardware für den Internetserver einiges an Geld. Es lohnt sich daher auch, auf die Herkunft und Garantie der Teile zu achten.

Als erstes wird eine Stückliste für die Hardware erstellt:

- Server-Einheit: Prozessortakt, -marke; RAM, Anzahl Netzwerkkarten, Bus-System und -geschwindigkeit, interne und externe Harddisks (Volumen, Typ), CD oder DVD Laufwerk, serieller Anschluss, KVM (Konsole, Video, Maus). Es ist bei der Auswahl der Server-Hardware darauf zu achten, dass diese für einen Dauerbetrieb ausgelegt ist. Eine billige Anschaffung von PC-Komponenten lohnt sich für einen richtigen Internetserver nicht, da solche Komponenten weniger für den Dauerbetrieb und die Anforderungen eines Servers optimiert sind.
- Netzwerk-Anschlüsse, Leitungen, Kabel, Kabelführung, Stromzufuhr, unterbruchfreie Stromversorgung bzw. Notstromaggregat
- Serverschrank (Rack), Zugangsmöglichkeiten, physischer Verschluss des Racks und je nach Modell auch des Servers mit Schlüssel, Belüftung/Ventilation, Klimatisierung des Raumes, Positionierung des Internetservers im Rack zusammen mit anderen Servern (Zugangsmöglichkeiten, Ein- und Ausbau)

Neben der eigentlichen Hardware ist mit den Lieferanten allenfalls auch eine Vereinbarung über Ersatzteillieferung zu treffen. Je nach Hardware kann es einige Tagen oder Wochen dauern, bis diese geliefert werden kann. Bei einem Ausfall muss dafür gesorgt sein, dass Ersatzteile in der benötigten Zeit geliefert werden können oder ab Lager verfügbar sind.

Falls der Internetserver hohe Anforderungen an verschlüsselte Verbindungen (SSL/TLS mit vielen concurrent sessions / aktiven Benutzern) stellt, sollte die Anschaffung von soge-

nannter Verschlüsselungs-Beschleuniger Hardware überlegt werden (sog. «SSL Accelerator» Hardware). Diese spezialisierte Hardware entlastet den Hauptprozessor von Verschlüsselungsaufgaben und sorgt für einen hohe Durchsatzrate (Performance) der verschlüsselten Verbindungen. Der Nachteil solcher Hardware ist meist der hohe Anschaffungspreis.

6.3 Sicherheit gewährleisten mit technischen und organisatorischen Massnahmen

Die Grundanforderungen an die Sicherheit des Servers (Verfügbarkeit, Integrität, Vertraulichkeit) müssen mit organisatorischen und technischen Massnahmen gewährleistet werden. Folgende Punkte sind abzuklären und zu dokumentieren:

Organisatorische Massnahmen:

- Verantwortlichkeiten für den Internetserver (Betrieb/Administration, Back-up, Benutzerverwaltung, Notfallplanung, Ersatzteile, digitale Zertifikate)
- Eskalationsprozedur (Alarmierungsorganisation) im Notfall, z. B. bei einem Virus- oder Hackerangriff aus dem Internet
- Regeln für den Betrieb und die Benutzer, Weisungen für korrektes Verhalten, Regelung, welche Daten auf dem Server wo gespeichert werden (dürfen) und welche Daten keinesfalls auf dem Internetserver gespeichert werden sollen

Technische Massnahmen:

- Firewall (Verantwortung für Konfiguration und Pflege der Firewall ebenfalls festlegen)
- Intrusion Detection System innerhalb der DMZ
- Spamfilter
- Content-Filter (Inhalts-Filter für ein- und ausgehenden Internet- und Mailverkehr)
- Proxy, Reverse Proxy
- Notstromversorgung (USV)
- Sicherer Standort und Zugang (abgeschlossenes Server-Rack)
- Brand- und Wasserschutz

6.4 Betriebssystem für den Internetserver definieren

Nach der Auswahl der geeigneten Hardware (je nach eingesetztem Betriebssystem hat dies Einfluss auf die Hardware, z. B. SUN Solaris), muss das Betriebssystem für den Internetserver ausgewählt werden. Folgende Betriebssysteme eignen sich für den Betrieb eines Internetservers:

- Windows 2000 Server
- Windows 2003 Server (verschiedene Ausführungen) mit Internet Information Server (IIS), jeweils aktuellste Version und Service Pack auswählen!
- Verschiedene Linux-Distributionen (SuSE, RedHat etc.)
- Unix-Derivate der BSD-Familie (FreeBSD, NetBSD etc.)
- SUN's Solaris (benötigt spezielle Hardware)

Für die Beispiele in diesem Lehrmittel wurde SuSE Linux «Open Source Edition» OSS v10 ausgewählt, da dieses Betriebssystem einfach aufzusetzen ist, die meisten benötigten Software-Komponenten für den Internetserver bereits mitbringt und frei erhältlich ist (open source). In der OSS-Edition sind keine nicht-open-source Komponenten enthalten. Alternativ kann auch die «Evaluation Edition» von SuSE Linux v10 verwendet werden. Diese ent-

hält proprietäre Anwendungen wie z. B. Adobe Reader etc. und ist ansonsten gleich zu konfigurieren wie die OSS-Edition.

6.5 Wie werden Applikationen an den Server angebunden?

Werden auf dem Internetserver verschiedene Applikationen angeboten, ist zu überlegen, wie diese an den Internetserver angebunden werden:

- **Direkt:** Die Applikation wird direkt auf dem Internetserver installiert und läuft evtl. auf eigenen Ports. Dabei muss lediglich sichergestellt werden, dass die Applikation auf dem gleichen Server keine Störungen mit anderen Applikationen (Webserver, Mail etc.) verursacht.
- **TCP/IP:** Die Applikation(en) ist auf einem anderen Server installiert und wird über das TCP/IP-Protokoll angesprochen. Dabei ist sicherzustellen, dass die Adresse der Applikation vom Internetserver erreichbar ist. Je nach Bedarf können weitere Sicherheitsmassnahmen getroffen werden, um die Applikation vor Angreifern von aussen zu schützen (z. B. zusätzliche Firewall vor dem Applikationsserver).
- **Proprietäre Protokolle:** Es gibt auch Applikationen, welche über proprietäre Protokolle mit dem Internetserver kommunizieren. Solche Applikationen sind eher selten, die Anbindung und Kommunikation zwischen Internetserver und Applikation soll vor Inbetriebnahme ausführlich getestet werden.

6.6 Beschaffung der Software und Installationsabhängigkeiten

Bei der Wahl der Software für den Internetserver sind einige Fragen zu klären:

- Welche Dienstleistungen werden für welches Publikum angeboten? Wird der Internetserver nur als Webserver gegen aussen und als interner Mailserver, evtl. zusätzlich mit interner DNS-Funktionalität betrieben oder sind Bereiche des Internetservers (Mail, FTP etc.) auch von aussen her zugänglich; von wem und in welcher Art (verschlüsselte Verbindung, ständige Verbindung oder nur temporär)?
- Lizenzmodell des Anbieters? Entscheidet man sich für lizenzpflichtige Software, sind einerseits einmalige Lizenzkosten zu entrichten und oft jährliche Gebühren für Upgrades und Garantie fällig. Solche Kosten sind in der Budgetierung des Internetservers aufzunehmen. Eine wichtige Einflussgrösse auf den Lizenzpreis hat einerseits die eingesetzte Hardware (Anzahl Prozessoren, Server-Typ) sowie die Anzahl der Benutzer (je nach Software werden die konfigurierten Benutzer (Gesamte Anzahl Benutzer) oder die «concurrent user» für die Preisgestaltung verwendet). Bei open-source Software entfallen die Lizenzgebühren, allerdings können Kosten für Pflege und Wartung (Fachpersonen; Anbieter der Software bietet kostenpflichtige Dienstleistungen an wie z. B. SuSE) anfallen.

Wird die Software zudem online gekauft, kann man diese oft downloaden, ohne dass ein zusätzliches Original-Softwarepaket geliefert wird (wobei meist der Preis dadurch etwas günstiger wird). Es ist dabei wichtig, eine oder mehrere Sicherheitskopien der Original-SW zu erstellen, damit auch zu einem späteren Zeitpunkt der Internetserver mit der ursprünglichen SW-Version wiederhergestellt werden kann; unter anderem auch um entsprechende ältere Back-ups wieder erfolgreich aufspielen zu können.

Bei der Auswahl der Software für die Beispiele in diesem Lehrmittel wurde ausschliesslich auf frei erhältliche Software geachtet, um keine Einschränkungen für die Lernenden einzugehen.

6.6.1 Webserver

Der im Lehrmittel verwendete Webserver ist der open-source Webserver Apache 2.0. Für Windows-Server wird üblicherweise der Microsoft-eigene Webserver «Internet Information Server» IIS 6.0 verwendet, wobei auch Apache gut auf Windows-Systemen funktioniert. Grundsätzlich ist Apache auf fast jedem Betriebssystem lauffähig.

Daneben gibt es Dutzende weitere Webserver, die in verschiedenen Sprachen geschrieben sind. Diese werden meist in spezialisierten Projekten/Applikationen eingesetzt, seltener im kommerziellen Umfeld, wo sich Apache und IIS stark verbreitet haben.

6.6.2 FTP Server

FTP-Server gibt es ebenfalls in einer grossen Anzahl, open-source oder kommerziell. Oft ist ein FTP-Server bereits auf dem Betriebssystem vorhanden, v. a. wenn es sich um ein Server-Betriebssystem handelt.

6.6.3 DNS Server

Die wohl bekannteste DNS-Serversoftware ist die Implementierung «BIND». Sie ist zugleich der Ur-FTP-Server und wird heutzutage oft eingesetzt. Daneben gibt es ebenfalls weitere, frei verfügbare DNS-Serversoftware.

6.6.4 Maildienste: SMTP und Postfach/Mailbox

Beim E-Mail wird unterschieden zwischen dem SMTP-Server, der Mails versendet und entgegennimmt, um an die Postfächer zu verteilen. Der SMTP-Server muss nicht zwingend der gleiche Server sein, wo die Postfächer für die Benutzer verwaltet werden.

Den Mail Transfer Agent (MTA, wie der SMTP Server auch genannt wird) gibt es in mehreren Varianten und für verschiedene Betriebssysteme. Die bekanntesten sind:

- MS Exchange für Windows
- Exim (Unix)
- Lotus Domino (Linux, Unix, Windows)
- Postfix, Qmail, Sendmail (Unix/Linux)

Der Mail Delivery Agent (MDA) ist zuständig für die Verteilung der eingehenden Mails in die Mailboxen/Benutzerkonten. Der MDA ist auch zuständig für die Verwaltung der E-Mails wenn diese vom MUA (Mail User Agent, Mailclient) geholt werden mittels POP3 oder IMAP-Protokollen. Die Mailclients sind nicht Bestandteil dieses Moduls.

Der bekannteste MDA unter Linux ist procmail. Unter Windows erfüllt Exchange diese Funktion.

6.7 Zu verwendende Namen für Systeme, Dienste und Daten

Bei der Planung des Internetservers soll auf eine konsistente Namengebung geachtet werden. Bestehen bereits entsprechende Regelungen im Unternehmen, so sind diese soweit anwendbar zu gebrauchen. Ansonsten empfiehlt es sich, gewisse Standards zu definieren:

- Servernamen werden nach einem bestimmten Muster vergeben, z. B. «srvi_01» für «Server, Internet, Nummer 01» oder «srv_db_i01» für «Server: Datenbankserver, Gruppe: i01 (Internetserver)», d. h. Datenbankserver der die Internetserver bedient.
- Die Dienste (http-daemon, ftp-daemon etc.) haben oft bereits voreingestellte Namen, die teilweise änderbar sind. Werden diese geändert, ist auf Abhängigkeiten zu anderen Systemen und Applikationen zu achten, die möglicherweise den Standard-Namen suchen und nicht finden und dadurch eine Kommunikation verhindert wird. Es empfiehlt sich, die Namen der Dienste und Prozesse in der Standardeinstellung zu belassen, sofern dies keine Konflikte mit bereits erfolgten Installationen hervorruft.
- Daten und Verzeichnisse sind ebenfalls nach einheitlichen Mustern zu verteilen und zu bezeichnen. So empfiehlt es sich, Standard-Verzeichnisse z. B. für Installationsdateien, Daten, Applikationen etc. festzulegen. Auch die Namengebung für die Dateien soll soweit möglich aufschlussreich sein, damit leicht erkannt wird, um was für einen Dateityp es sich handelt. Dies ist insbesondere im Unix-/Linux-Umfeld nützlich, da dort nicht alle Dateien eine entsprechende Endung haben. Auch hier ist es wichtig, Abhängigkeiten mit anderen Applikationen oder Diensten zu prüfen. Die Umbenennung von Konfigurationsfiles führt z. B. oft dazu, dass eine Konfiguration der Systeme mit GUI-Werkzeugen nicht mehr möglich ist, da diese nach fest definierten Dateinamen suchen.

6.8 Standardeinstellungen festlegen

Neben den Namenskonventionen ist es sehr wichtig, eine Standard- oder Default-Einstellung für alle installierten Dienste zu definieren. Diese Einstellungen sind entweder schon bei der Installation aufzufinden oder müssen direkt nach der Installation vorgenommen werden. Fortgeschrittene Administratoren können die Installationsscripts bzw. -routinen so anpassen, dass die Software auf vorher festgelegte Verzeichnisse installiert wird und gegebenenfalls von den «Werkseinstellungen» abweichende Konfigurationen aufweist.

Mithilfe der vordefinierten Standardeinstellungen ist es auch für andere Systembetreuer nachvollziehbar und möglich, eine Installation vorzunehmen. Es ist deshalb wichtig, dass die Default-Einstellungen detailliert dokumentiert werden.

Repetitionsfragen

3	Welche Hardware wird bei der Realisierung des Internetservers benötigt bzw. auf den Internetserver abgestimmt?
8	Was ist nach der Beschaffung der Software zu berücksichtigen?