# 5 Soll-Zustand analysieren

Die Definition des Soll-Zustands ist zugleich das Pflichtenheft für den Internetserver. Welche Dienste sollen angeboten werden und für wen? Sind die Dienste auf mehrere physische Server zu verteilen? Müssen Datenbanken angebunden werden? Welche Sicherheitsanforderungen bestehen bezüglich Verfügbarkeit und Vertraulichkeit? Müssen Daten konvertiert werden oder sind ältere Systeme überhaupt in der Lage, mit dem Internetserver zu kommunizieren? Müssen Schnittstellen und Programme geschrieben werden, um ältere Applikationen an das Internet anzubinden?

## 5.1 Welche Applikationen sollen «web-enabled» werden?

Anhand einer Liste der bestehenden Applikationen wird entschieden, welche Daten und Funktionen auch im Web zur Verfügung stehen sollen. Möglicherweise müssen neue Schnittstellen geschaffen werden, um Datenbanken an den Internetserver anzubinden.

Bestehende Applikationen können oft nicht einfach mit dem Internetserver verbunden werden. Die Durchführung einer Bestellung aus dem Web bedingt eventuell, dass eine neue Applikation für den Web-Shop geschrieben wird, und innerhalb des Unternehmen weiterhin eine Client-Server-Applikation eingesetzt wird. Oft ist auch ein ERP-System im Einsatz. Moderne ERP-Systeme verfügen meist über vorbereitete (optionale) Schnittstellen für die Anbindung an das Internet. (Ein sogenanntes Enterprise Resource Planning (ERP) System besteht aus mehreren Anwendungen wie z. B. Lagerverwaltung, Personalverwaltung, Kundenstammdaten, Buchhaltung, welche miteinander verknüpft (integriert) sind und somit die Verwaltung der Daten eines Unternehmens mit einer (grossen) Anwendung, dem ERP-System, erledigt werden kann.)

## 5.2 Allgemeine Sicherheitsrichtlinien im Unternehmen

Falls allgemeingültige Sicherheitsrichtlinien im Unternehmen bestehen, müssen diese auch auf den Internetserver angewendet werden. Benutzerrichtlinien (Passwortvergabe, Benutzerverwaltung) müssen je nach Bedarf für den Internetserver separat erstellt werden (insbesondere wenn die Benutzer des Internetservers nicht mit bestehenden Verzeichnisdiensten wie Active Directory etc. verwaltet werden).

Vorgaben bezüglich der Verfügbarkeit von Systemen und der Integrität und Vertraulichkeit von Daten müssen ebenfalls eingehalten oder für den Internetserver spezifisch erstellt werden.

## 5.3 Datenschutz und Personendaten

Daten über Personen (z. B. Kunden- oder Mitarbeiterdaten) unterliegen besonderen Schutzbestimmungen des Datenschutzgesetzes. Die Leitfäden des Datenschutzbeauftragten geben detaillierte Hinweise, wie solche Daten bearbeitet und geschützt werden müssen: http://www.edsb.ch/d/doku/leitfaeden/index.htm.

Die wichtigsten Kriterien sind:

- Personendaten sind vor unbefugter Bearbeitung (Einsicht, Manipulation, Löschung) mit angemessenen technischen und organisatorischen Massnahmen zu schützen (z. B. Verschlüsselung, Regelung/Weisung zum Umgang mit Personendaten).
- Personendaten müssen richtig sein (Integrität der Daten) und sind bei Bedarf oder auf Anfrage der betroffenen Person zu berichtigen.
- Personendaten dürfen nur zu dem Zweck bearbeitet werden, für den sie gesammelt wurden (also keine Werbung mit Rechnungsadressen aus dem e-shop).
- Der betroffenen Person ist auf Anfrage Auskunft über die gesammelten Daten zu geben.

Ein wichtiger Punkt, der sich für den Betrieb eines Internetservers aus dem Datenschutzgesetz ableitet, ist der Umgang mit Logfiles, die personenbezogene Daten enthalten (d. h. Benutzernamen, die direkte Rückschlüsse auf Personen ermöglichen, z. B. Benutzername «hans.muster». Die Bearbeitung dieser Logfiles muss so sichergestellt sein, dass keine personenbezogenen Auswertungen durch unbefugte Personen möglich sind, und dass die betroffenen Personen bei solchen Auswertungen darüber informiert werden (z. B. welcher Benutzer welche Webseite wann besucht hat, Einsicht in das Mailserver-Logfile um zu sehen, wer wem E-Mails schreibt).

## 5.4 Anforderungen an die Verfügbarkeit (uptime) und Datenvolumen

Die Anforderungen der Kunden an die Verfügbarkeit des Internetservers und der darauf verarbeiteten Daten müssen definiert werden. Insbesondere ist darauf zu achten, dass Backend-Systeme z. T. ausser Betrieb sind (z. B. nachts während des Back-up-Zyklus der Datenbank). Der Internetserver ist typischerweise ständig im Internet erreichbar und die Kunden aus verschiedenen Zeitzonen wissen nicht, dass im Hintergrund ein Back-up läuft und dadurch gewisse Informationen evtl. nicht zur Verfügung stehen.

Falls solche Unterbrüche zu erwarten sind, soll dies klar kommuniziert werden (Text auf der Homepage); bzw. kann heute mit entsprechenden Mitteln dafür gesorgt werden, dass solche Unterbrüche keine Auswirkung auf den Internetserver haben (z. B. Zwischenspeichern/caching der Datenbank auf dem Internetserver während der Back-up läuft).

### 5.4.1 Wie viel Traffic/Volumen wird erwartet; zukünftige Entwicklung?

Anhand von Messungen des Verkehrs (Anzahl Anfragen pro Minute, Stunde, Tag; Download-Datenvolumen pro Stunde, Tag etc.) kann festgestellt werden, wie der Internetserver benutzt wird. Durch ständige Auswertung dieser Daten kann man auch rasch erkennen, wenn die Belastung des Systems zunimmt und entsprechende Massnahmen treffen (mehr Speicherplatz, grösserer Server etc.).

Oft ist es schwierig abzuschätzen, wie hoch der Verkehr nach der Inbetriebnahme ist. Je bekannter die Webseite, je mehr Benutzer auf dem Mailserver, desto höher die Auslastung. Typischerweise nimmt die Auslastung in den ersten Wochen stark zu (bei bekannt werden der Webseite; Benutzer fangen an, E-Mail zu benutzen). Nach einigen Wochen ist der Normalzustand erreicht und die Messungen können beginnen.

Zur Messung eignet sich am besten die Auswertung der Logfiles des Web- und E-Mail-Servers; wichtige Kennzahlen sind:

- Anzahl Hits pro Tag (oder kürzere Abstände wenn nötig, z. B. pro Stunde), Verteilung über verschiedene Tageszeiten (dabei sieht man oft, wann in welchen Teilen der Welt morgen oder abend ist, da der Verkehr dann stark zu- oder abnimmt)
- Anzahl und Menge der Downloads, falls solche Angeboten werden
- Anzahl der eingeloggten Benutzer (sofern eine Möglichkeit für Login besteht, z. B. in einen geschlossenen Benutzerbereich). Diese Kennzahl ist insbesondere wichtig bei SSL-Verbindungen (über https), da die Ver- und Entschlüsselung der Daten zusätzliche Last erzeugt. Je mehr solche verschlüsselten Verbindungen offen sind, desto höher die Prozessorlast. Unverschlüsselte Verbindungen verursachen nicht solch grosse Last auf dem Prozessor. Diese Kennzahl wird auch «concurrent user» genannt, was so viel heisst wie «gleichzeitige Benutzer» und ist die einzige wichtige Kennzahl bezüglich der Benutzer. Unabhängig wie viele Benutzer auf dem System erfasst sind, ist es nur ausschlaggebend, wie viele das System gleichzeitig nutzen. Die Anzahl der «named user», d. h. der definierten/erfassten Benutzer, stellt lediglich die höchstmögliche Anzahl «concurrent user» dar, wird aber in der Praxis nie ausgeschöpft. Zwischen 20–50 % aller Benutzer sind normalerweise gleichzeitig online.
- Anzahl verschickter und empfangener E-Mails; Grösse und Anzahl der verschickten Attachments
- Anzahl und Datenmenge der Downloads via FTP
- Anzahl der Anfragen an den DNS-Server

## 5.5 Welche Benutzerprofile sind vorgesehen?

Je nach Einsatz des Internetservers gibt es verschiedene Benutzer auf dem System, die über entsprechende Rechte verfügen. Nachfolgend werden Möglichkeiten beschrieben, um diese Rechte zu verwalten.

### 5.5.1 CRUD: Create Read Update Delete

Die sogenannte CRUD-Matrix eignet sich vor allem für **Applikationen**, um die verschiedenen Autorisierungen (Berechtigungen) der **Benutzer** übersichtlich aufzuzeigen.

Diese Matrix soll zeigen, welche Rechte den verschiedenen Benutzern erteilt werden:

- C: Create: Dateien erzeugen
- R: Read: Dateien lesen
- U: Update: Dateien verändern
- D: Delete: Dateien löschen

| | Kundenstamm | Produkte-DB | Benutzerverwaltung | E-Mail |
|---|---|---|---|---|
| **Kunde** | R | R | | CRD |
| **Administrator** | CRUD | CRUD | CRUD | CRUD |
| **Internerbenutzer** | CRUD | CRUD | RU | CRD |
| **Support** | RU | RU | RUD | CRD |

### 5.5.2 Zugriffskontrolle (Access Control Lists)

Eine Zugriffskontroll-Liste zeigt listenförmig auf, welcher Benutzer über welche Zugriffe verfügt. Das folgend Beispiel ist eine ACL für einen Webserver:

- Benutzer: Zugriffsart
- admin: Administrator mit Vollzugriff
- b.kaelin: Supportfunktionen
- c.meier: Supportfunktionen
- m.luethi: Kundenfunktionen

### 5.5.3 Administration

Der Administrator verfügt im Normalfall über weitgehende Berechtigungen. Üblicherweise wird dabei das Prinzip der «Gewaltentrennung» eingesetzt, d.h .der Administrator darf nur Änderungen durchführen oder Benutzer erstellen, wenn er von einer anderen (berechtigten) Person dazu ermächtigt wurde. Dadurch wird vermieden, dass der Administrator ohne Kontrolle auf dem System Arbeiten durchführt.

Beispielsweise stellt ein Mitarbeiter der Personalabteilung den Antrag auf ein E-Mail-Account. Die Personalabteilung erteilt danach dem Administrator den Auftrag, den E-Mail-Account zu eröffnen.

Ebenfalls wichtig ist die Dokumentation und Logging der Tätigkeiten des Administrators, damit jederzeit nachvollzogen werden kann, welcher Admin wann was geändert hat. Im Idealfall soll auch der (schritliche) Antrag des Benutzers archiviert werden, damit nachvollziehbar ist, aufgrund welchen Auftrags der Administrator ein neues Benutzerkonto eröffnet hat.

Bei wichtigen Änderungen (z. B. Upgrade des Systems, löschen eines Benutzeraccounts) kann zudem das 4-Augen-Prinzip angewendet werden, d. h., ein zweiter Administrator gibt die Änderung nach einer Kontrolle frei. Dadurch wird vermieden, dass aus Versehen eine Änderung am System zu Ausfällen oder Problemen führt.

### 5.5.4 Externe Zugriffe

Zugriffe von aussen auf ein System sind immer mit grosser Vorsicht zu betreiben. Im Normalfall darf ein externer Zugriff nur durch gesicherte Kommunikationsverbindungen vorgenommen werden (secure shell ssh, https, VPN-Tunnel), und die Tätigkeiten des externen Zugreifers sollen immer protokolliert (Logfile) werden.

Eine übliche Vorgehensweise ist, den externen Zugriff prinzipiell zu sperren und nur auf Anfrage zu öffnen. Dadurch ist sichergestellt, dass immer bekannt ist, wann ein Zugriff erfolgt.

## Repetitionsfragen

| | |
|---|---|
| 21 | Welche Anforderungen sind bei der Definition des Soll-Zustands zu berücksichtigen? |
| 25 | Erklären sie kurz den Unterschied zwischen Datenschutz und Datensicherheit? |