



## **ePages 5**

Technical White Paper





**ePages 5**

Technical White Paper



Die in diesem Dokument enthaltenen Informationen können jederzeit ohne Benachrichtigung geändert werden.

Dieses Werk ist einschließlich aller seiner Teile urheberrechtlich geschützt. Alle Rechte sind ausdrücklich vorbehalten, einschließlich der Rechte auf Vervielfältigung, Reproduktion, Übersetzung, Mikroverfilmung, Speicherung auf elektronischen Medien und Verarbeitung in elektronischer Form.

Alle Firmen-, Produkt- und Markennamen sind Warenzeichen oder eingetragene Warenzeichen der entsprechenden Inhaber. Copyright © 2005 ePages Software GmbH. Alle Rechte vorbehalten.

Sollten Sie Fragen oder Hinweise zu unseren Produkten haben, so wenden Sie sich bitte an folgende Adresse:

ePages Software GmbH  
Leutragraben 1  
07743 Jena  
Tel.: +49 (0) 36 41 – 5 73 – 100  
Fax: +49 (0) 36 41 – 5 73 – 111  
info@epages.de  
www.epages.de

# Inhaltsverzeichnis

<b>1. Einleitung.....</b>	<b>7</b>
<b>2. ePages Systemarchitektur .....</b>	<b>8</b>
2.1 Web-Server .....	8
2.2 Applikations-Server .....	9
2.3 Datenbank-Server.....	9
2.4 File-Server .....	9
<b>3. Mögliche Konfigurationen.....</b>	<b>10</b>
3.1 Minimalkonfiguration .....	10
3.2 Verteilte Installationen .....	10
<b>4. Sicherheitsmechanismen.....</b>	<b>13</b>
4.1 Unabhängige logische Module.....	13
4.2 Passwortschutz .....	14
4.3 Zugriffsrechte .....	15
4.4 Session-Sicherheit.....	15
4.5 Anfragenprüfung .....	16
4.6 Verschlüsselung .....	16
4.7 Kommunikation mit anderen Systemen .....	16
<b>5. Erweiterungsmöglichkeiten .....</b>	<b>17</b>



## 1. Einleitung

Dieses Dokument gibt einen Überblick über die ePages-Architektur, die Sicherheitsmechanismen sowie Anforderungen für bestimmte Größenordnungen von Hardwarekonfigurationen.

**Allgemeines**

Dabei liegt das Augenmerk auf folgenden Punkten:

- ▶ Zugriffsschutz unabhängiger logischer Module untereinander
- ▶ Rechtesystem
- ▶ Hohe Leistungsfähigkeit
- ▶ Skalierbarkeit
- ▶ Hochverfügbarkeit („High Availability“ – HA)
- ▶ Niedrige Gesamtbetriebskosten („Total Cost of Ownership“ - TCO)

Die Daten in diesem Dokument basieren auf Erfahrungen und Messergebnissen und stellen einen möglichst ökonomischen Kompromiss zwischen den unterschiedlichen Zielen für B2B- und B2C-Anwendungen dar. Es handelt sich daher um Beispielszenarien. Gern erstellen wir auch einen spezifischen Hardwarevorschlag. Nutzen Sie dazu unsere Webseite: [www.epages.de/sizing-request](http://www.epages.de/sizing-request)

**Zur Arbeit mit ePages-Software existieren darüber hinaus die Dokumentationen:**

[1] „ePages 5 White Paper“

[2] „ePages 5 Handbuch für Händler“

**Weitere ePages-Dokumentationen**

**Die Installation und der Betrieb eines ePages-Systems werden beschrieben in:**

[3] „ePages 5 Installationshandbuch“

[4] „ePages 5 Handbuch für Business Administratoren“

[5] „ePages 5 Handbuch für Technische Administratoren“

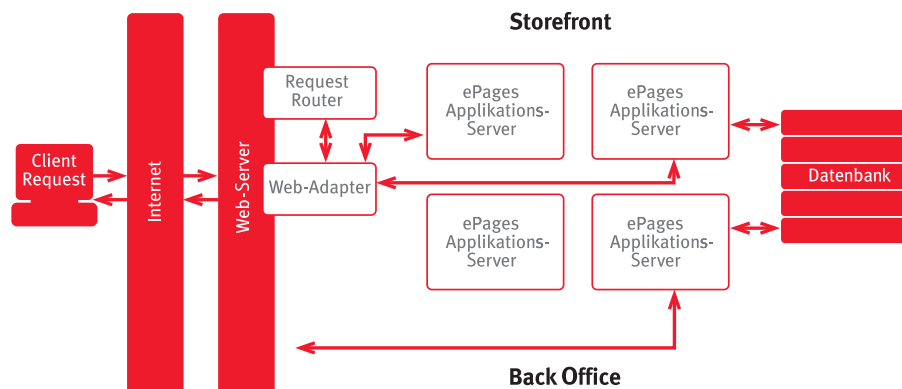
## 2. ePages Systemarchitektur

### Allgemeines

Prinzipiell besteht ePages-Software aus folgenden Komponenten:

- ▶ Web-Server
- ▶ Applikations-Server
- ▶ Datenbank-Server
- ▶ File-Server

Die nachfolgende Abbildung zeigt den grundlegenden Architekturaufbau sowie den Ablauf einer Anfrage an das System.



### Ablauf einer Anfrage an das System

Der Nutzer ruft eine Seite in der Storefront des Shops auf. Diese Anfrage wird an den Web-Server übertragen. Der Request-Router leitet die Anfrage an einen verfügbaren Applikations-Server weiter. Dieser prüft, ob die vom Nutzer angeforderte Seite bereits vorher einmal angefordert wurde. Liegt die Seite bereits auf dem File-Server, wird sie an den Web-Server geschickt und von dort aus über das Internet an den Client ausgeliefert. Ist die angeforderte Seite noch nicht vorkompiliert vorhanden, holt sich der Applikations-Server die entsprechenden Daten aus der Datenbank, erstellt die Seite und leitet sie über den Web-Server an die Storefront.

### 2.1 Web-Server

Welcher Web-Server eingesetzt wird, hängt vom Betriebssystem ab. ePages bietet seine Produkte für folgende Betriebssysteme an:

- @ MS Windows 2000/2003 Server
- @ Sun Solaris 9
- @ Linux Red Hat Enterprise 3

Für Windows empfiehlt ePages als Web-Server den MS-IIS, unter Solaris und Linux Apache (im Lieferumfang enthalten).

Einen besonderen Stellenwert hat der Request-Router. Er verteilt eingehende Anfragen auf die entsprechenden Applikations-Server. Es besteht die Möglichkeit, mehrere Web-Server-Maschinen parallel zu schalten.

## 2.2 Applikations-Server

Der ePages-Applikations-Server ist eine Eigenentwicklung, die mit einer der Web-Standard-sprachen (Perl) programmiert wurde. Für ePages 5 wurde die Perl-Version 5.8 verwendet. Diese unterstützt modernste Technologien wie beispielsweise Web Services.

Auf jeder physischen Maschine können mehrere Instanzen Applikations-Server gestartet werden, wobei die Anzahl vom installierten RAM und den verfügbaren CPU abhängig ist. Je mehr Applikations-Server zur Verfügung stehen, umso mehr Anfragen pro Sekunde können beantwortet werden.

Es besteht die Möglichkeit, mehrere Applikations-Server-Maschinen parallel zu schalten. Da der Applikations-Server am leichtesten zu skalieren ist, wurde ePages 5 so entwickelt, dass hier die Hauptlast der Anwendung liegt. Die gesamte Business-Logik liegt auf dem Applikations-Server, häufig angeforderte Daten werden hier zwischengespeichert. Damit wird der Datenbank-Server entlastet.

## 2.3 Datenbank-Server

ePages verwendet Sybase ASE (Adaptive Server Enterprise) Version 12.5.2 als integrierte Datenbank. Diese hat sich als sehr robust, leistungsfähig und zuverlässig erwiesen.

Anfragen der Applikations-Server werden mit SQL-Anweisungen ausgeführt.

Für ePages 5 Merchant besteht die Möglichkeit, mehrere Datenbank-Server-Maschinen parallel zu schalten – für eine einzelne Datenbank ist dazu ein Cluster erforderlich.

Mit dem ePages 5 Hosting-Produkt können mehrere Datenbanken (mit jeweils mehreren Shops) zu einem System vereint werden. In diesem Fall kann jede einzelne Datenbank ihre eigene physische Maschine haben.

## 2.4 File-Server

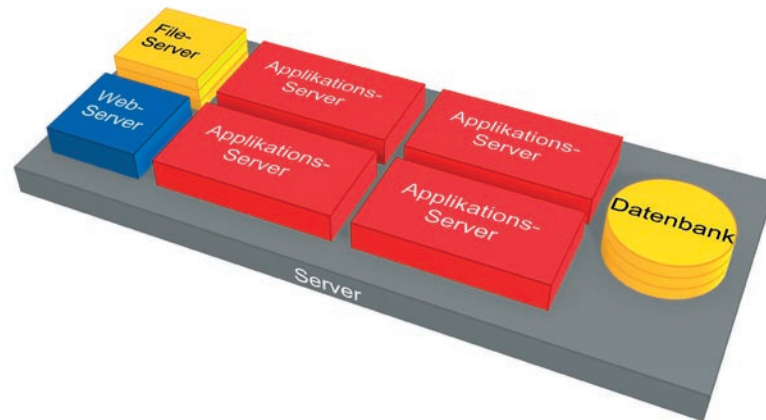
Bilder und andere Multimediadateien werden aus Gründen der Leistungsfähigkeit nicht in der Datenbank gespeichert. Sie liegen im Dateisystem meist auf dem Web-, Applikations- oder Datenbank-Server. In der Datenbank ist lediglich der Verweis auf diese Datei gespeichert. Ebenso werden auf dem File-Server Konfigurationsdateien zentral verwaltet, sowie sämtliche Templates und CSS-Dateien (Cascading Style Sheet), welche für das Design von Storefront und Back Office erforderlich sind.

Meist wird der File-Server nicht auf einer separaten Maschine installiert, sondern häufig entweder auf dem Web- oder dem Applikations-Server betrieben, in bestimmten Fällen auch auf dem Datenbankserver.

### 3. Mögliche Konfigurationen

#### 3.1 Minimalkonfiguration

Die einfachste Variante ist die Installation aller Komponenten auf einer Maschine.

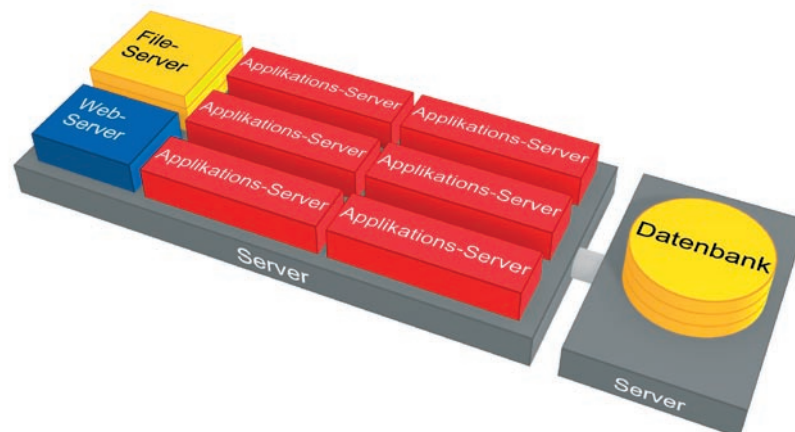


Wie die Grafik verdeutlicht, werden im Standard vier Applikations-Server installiert.

#### 3.2 Verteilte Installationen

##### Einzelner Datenbank-Server

Die Leistungsfähigkeit lässt sich oft durch die Abtrennung des Datenbank-Servers erhöhen. Damit können Datenbankprozesse unabhängig von Zugriffen auf statische Dateien und Applikations-Server-Prozessen laufen.

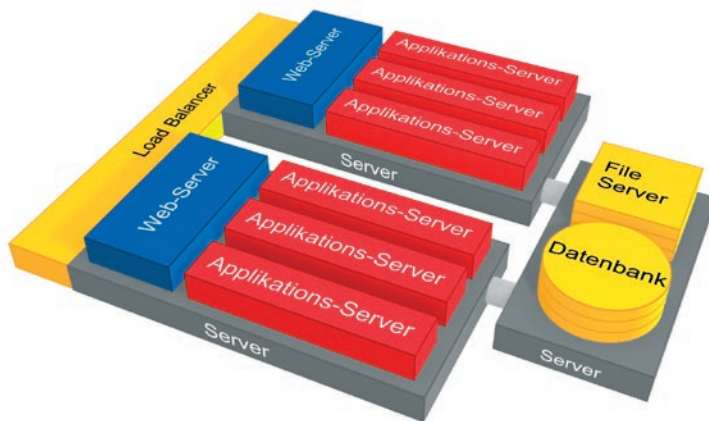


Zusätzlich wurde die Anzahl der Applikations-Server-Instanzen erhöht, um ein breiteres Spektrum für die Behandlung von Anfragen zur Verfügung zu haben.

Einen weiteren Gewinn an Leistungsfähigkeit erreicht man durch die Parallelisierung von Web- und Applikations-Server. Diese Konfiguration ist aus zwei unterschiedlichen Gesichtspunkten interessant:

### Parallelverteilung gemeinsamer Web- und Applikations-Server

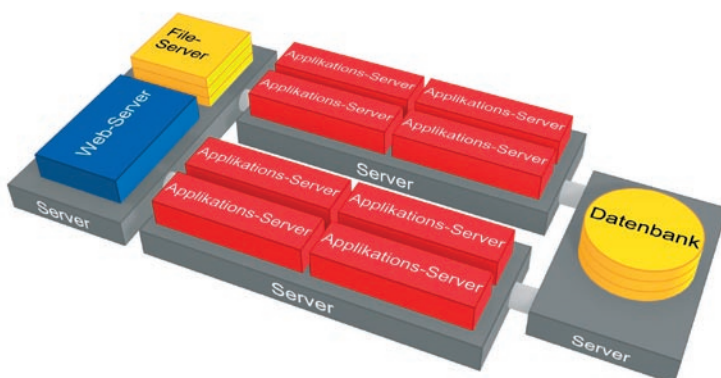
- ▶ Hochverfügbarkeit: Fällt eine Maschine aus, übernimmt die andere Maschine den kompletten Betrieb. Für diese Variante ist ein Load-Balancer erforderlich (nicht im ePages 5 Lieferumfang enthalten).
- ▶ Dedizierte Zuweisung bestimmter Shops (URLs): In einer Multi-Hosting-Umgebung ist es möglich, eine Maschine gezielt für einzelne Shops zu verwenden.



Die Parallelisierung von Web- und Applikations-Servern kann prinzipiell weiter fortgesetzt werden.

Eine Abtrennung des Web-Servers ist immer dann sinnvoll, wenn der Applikations-Server von sehr vielen Webdaten (Bilder, umfangreiche Seiten) entlastet werden soll. Eine Leistungssteigerung ergibt sich vor allem aus der Vorverlagerung des File-Servers auf den Web-Server und dessen Separierung.

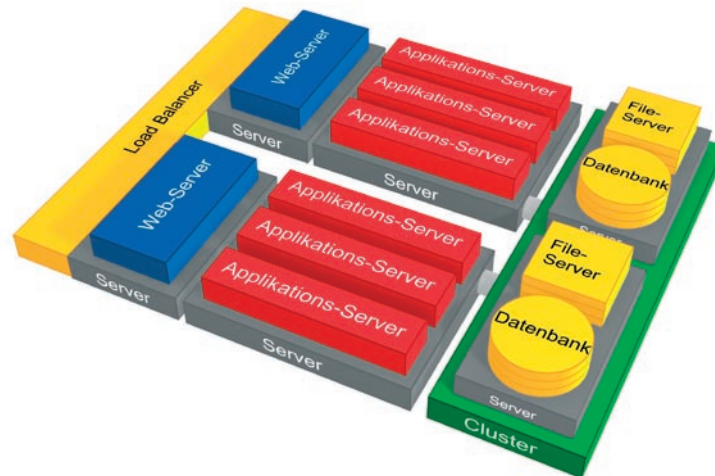
### Parallelverteilung getrennter Web- und Applikations-Server



Die Parallelisierung von Web- und Applikations-Servern kann prinzipiell weiter fortgesetzt werden.

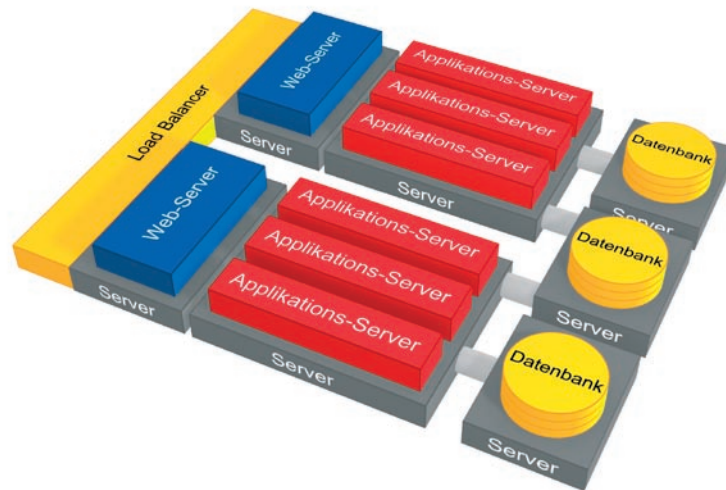
## Datenbank im Cluster

Um die Ausfallsicherheit zu erhöhen, können zwei Datenbank-Server eingesetzt werden. Diese werden in einem sogenannten Cluster betrieben. Die Datenbestände beider Server werden laufend konsistent gehalten. Fällt ein Datenbank-Server aus, würde automatisch der verbleibende Datenbank-Server den Betrieb übernehmen und so die Funktionstüchtigkeit der gesamten Anwendung garantieren. D.h. ein Datenbank-Server ist aktiv, der andere „standby“. Um den „standby“-Server nicht ungenutzt zu lassen, so-lange beide Maschinen fehlerfrei laufen, wird er als File-Server benutzt.



## Verteilung von Datenbanken auf mehrere Datenbank-Server

Falls das Produkt ePages 5 Hosting mit mehreren Datenbanken betrieben wird, können die einzelnen Datenbanken jeweils ihre eigene Maschine erhalten. Damit wird die Leistung datenbankseitig erhöht, Datenbankprozesse werden verteilt und laufen schneller ab.



Zum Betrieb von ePages 5 ist eine sogenannte Site-Datenbank erforderlich. Diese wird vor allem in einer Hosting-Umgebung genutzt, um die einzelnen Shops zu verwalten. Auch diese Datenbank kann auf eine separate Maschine ausgelagert werden.

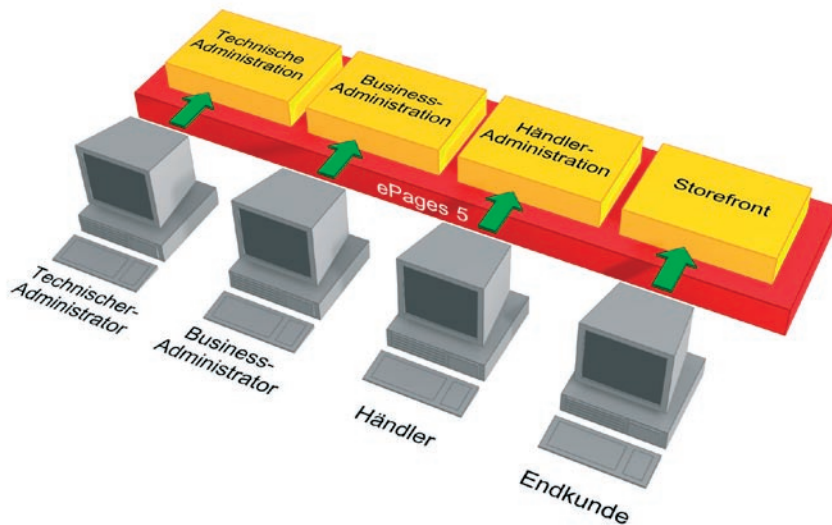
## 4. Sicherheitsmechanismen

### 4.1 Unabhängige logische Module

ePages 5 ist in einzelne Module für

- ▶ die technische Administration
- ▶ die Business-Administration
- ▶ die Administration durch die Händler und
- ▶ die Storefront (die eigentliche Einkaufszone)

getrennt. Die Module sind dabei voneinander isoliert und jedes von ihnen ist speziell für seine Funktionen gestaltet. So wird die Sicherheit des Systems vor unbefugten Zugriffen gewährleistet.



Dank spezieller Zugriffsrechte für jedes einzelne Modul ist der Zugriff nur dem Nutzer mit entsprechender Berechtigung möglich. Zum Beispiel ist ein Zugriff des Händlers auf Funktionen oder Daten der Business-Administration ausgeschlossen. Jedes Modul wird durch eine eigene URL aufgerufen.

Nur der technische Administrator ist in der Lage, Datenbankzuweisungen und Installationen durchzuführen.

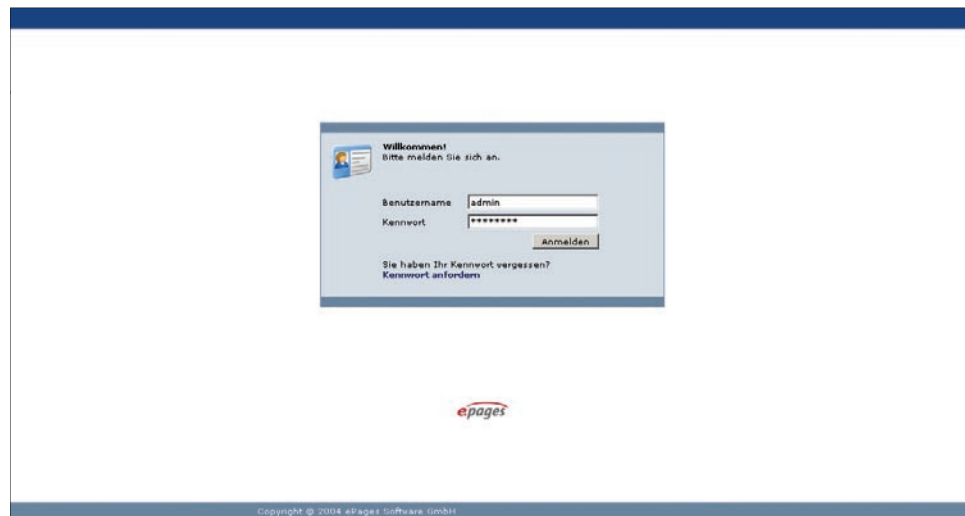
Der technische Administrator stellt dem Business-Administrator Daten bereit, auf deren Grundlage der Business-Administrator Shoptypen definiert und sich einen Überblick über die Shops verschaffen kann. Allerdings kann der Business Administrator nicht auf die eigentlichen Produkt- oder Bestelldaten des Shops zugreifen.

Der Händler verwaltet seinen Shop mit Hilfe von sieben Modulen, in denen er Bestellungen, Produkte, Kunden, etc. bearbeiten kann. Er kann allerdings keinen Einfluss auf den Funktionsumfang nehmen, den der Business-Administrator zur Verfügung stellt.

Der Endkunde hat die Möglichkeit, sich in der Storefront zu bewegen, zu suchen und zu bestellen. Selbstverständlich hat er keinen Einfluss auf die Produktbeschreibungen, Preise, Rabatte, etc..

## 4.2 Passwortschutz

Jedes Administrationsmodul und auch der Zugriff auf persönliche Daten registrierter Endkunden („Mein Konto“) ist durch Login und Passwort geschützt. Struktur und Design von ePages 5 verhindern den Zugriff auf jedwede Information „hinter“ der Loginseite.



Alle Passwortinformationen werden verschlüsselt in der Datenbank gespeichert. Die Verschlüsselung ist irreversibel, d.h. ein einmal gespeichertes Passwort kann durch keinen Nutzer eingesehen werden. Vergessene Passwörter können nach entsprechender Authentifizierung zurückgesetzt werden. Dabei wird vom System ein neues Passwort generiert.

Bei der Wahl eines Passwortes sollten bestimmte Regeln beachtet werden. Passwörter sollten enthalten:

- ▶ mindestens einen Großbuchstaben
- ▶ mindestens einen Kleinbuchstaben
- ▶ mindestens eine Zahl
- ▶ mindestens ein Sonderzeichen

Passwörter sollten in keinem Fall:

- ▶ einzelne Wörter sein, die in einem Wörterbuch (für eine beliebige Sprache) stehen
- ▶ einzelne Wörter sein, die in einem Wörterbuch (für eine beliebige Sprache) stehen und die durch ein numerisches Suffix oder Präfix ergänzt werden (z.B. Haus13 oder 12 Monkeys)
- ▶ Namen von wirklichen oder fiktiven Orten, Personen, Haustieren, Booten, Fahrzeugen, Produkten usw. sein
- ▶ mehr als zwei sich wiederholende Zeichen enthalten (z.B. AAA1111)
- ▶ Zeichen und/oder Ziffern in Folge enthalten (z.B. ABC1234)
- ▶ mehr als zwei Zeichen einer Tastatursequenz enthalten (z.B. QWErt46)
- ▶ mit dem Benutzernamen identisch sein

### 4.3 Zugriffsrechte

Durch die Unabhängigkeit der einzelnen Module untereinander ist auch die Verteilung der Rechte geregelt. Dabei ist es möglich, die Rechte für den Zugriff auf Daten und Funktionen

- grob, d.h. pro Modul oder
- granularer, d.h. im Detail bezogen auf einzelne Aktionen

zu regulieren.

Nach der Anmeldung am jeweiligen Modul per Login und Passwort ist die Rolle des Nutzers klar definiert und damit auch seine Berechtigungen. So hat beispielsweise ein Händler vollen Zugriff auf alle Bestell- und Kundendaten seines Shops. Damit ist es ihm z.B. möglich, eine fehlerhafte Kundenadresse zu korrigieren. Der registrierte Endkunde kann über „Mein Konto“ auf seine Bestellungen zugreifen, diese allerdings lediglich einsehen und nicht ändern.

Ein Quereinstieg in Funktionen bzw. der Zugriff auf Daten, zu denen der Nutzer in seiner Rolle nicht berechtigt ist, ist damit ausgeschlossen – selbst, wenn jemand versucht, per URL oder nachgebautem Formular Aktionen auszuführen.

Einen zusätzlichen Schutz stellt ePages 5 dadurch bereit, dass für Zugriffe auf die Datenbank ein anderer (interner) Nutzer verantwortlich ist. Selbst wenn jemand ein Händlerpasswort ausspioniert hat, sind unerlaubte Direktzugriffe von außen auf die Datenbank unmöglich, da der Datenbankserver zusätzlich hinter einer Firewall steht und nur die Schnittstelle für Datenbankzugriffe (Datenbank-Port) geöffnet haben kann.

### 4.4 Session-Sicherheit

Eine Session (Sitzung) ist die gesamte Dauer einer Reihe von Anfragen an das ePages-System. Dabei muss jede Anfrage des Nutzers an das System stets eindeutig diesem Nutzer zugeordnet werden. ePages 5 generiert dafür eine sogenannte Session-ID, welche der eindeutigen Authentifizierung von Nutzeranfragen an den Server dient. Die Sessioninformation muss dabei auf Seiten des Servers und des Clients (Nutzer, der Anfragen an ePages 5 stellt) vorhanden sein. Erfolgt also eine erneute Anfrage eines Nutzers mit derselben Session-ID, so kann der Server diese zuordnen und entsprechend verarbeiten. Damit ist bspw. gewährleistet, dass ein gefüllter Warenkorb eindeutig zu einer Session, also einem bestimmten Nutzer „gehört“ und weitere Produkte, welche dieser Nutzer dem Warenkorb hinzufügt, in genau diesen Warenkorb gelangen.

**Session-ID**

Auf der Seite des Clients arbeitet ePages 5 mit sogenannten Session-Cookies. Die Sessioninformation wird also in einer kleinen Datei gespeichert, welche sich allerdings lediglich im Arbeitsspeicher des Client-Computers befindet. Die Sessioninformation wird nicht auf der Festplatte gespeichert und geht mit dem Schließen des Browserfensters verloren. Diese Technologie garantiert ein Höchstmaß an Sicherheit, weil die Sessioninformationen nicht in der URL auftauchen und somit nicht in falsche Hände gelangen können. Session-Cookies sind bei allen Internet-Browsern auch bei einem hohen Grad von Sicherheitseinstellungen erlaubt und stellen damit keine Hürde für den Nutzer dar. Die Kombination von Sicherheitslogik sowie die Unabhängigkeit der einzelnen Module und Anfragen verhindern vollständig den unerlaubten Zugriff auf Daten oder die nicht autorisierte Ausführung von Funktionen.

**Session-Cookie**

## 4.5 Anfragenprüfung

Ein weiteres Sicherheitsmerkmal ist die Prüfung aller Anfragen (Requests) an den Server auf Gültigkeit. Parallel zur korrekten Session-ID werden nur gültige Anfragen behandelt. Dabei werden evtl. ungültige Parameter ebenso ignoriert wie der Aufruf einer Back Office-Funktion durch einen Storefront-Nutzer. Selbst wenn der Nutzer die Berechtigung hat, auf das Back Office zuzugreifen, so ist er dennoch nur in der Lage, den für das Back Office und seine Rolle gültigen Funktionsumfang zu nutzen. Beispiel: Selbst wenn ein Administrator Zugriff auf das Back Office hat, so kann er keine Änderungen an einem Warenkorb vornehmen, den ein Kunde gerade in der Storefront zusammenstellt.

Zusätzlich können Anfragen für die Administrationsebenen (Technischer und Business-Administrator) nur für bestimmte IP-Adressen zugelassen werden. Voraussetzung dafür ist ein separater Web-Server für diese Bereiche.

## 4.6 Verschlüsselung

ePages 5 unterstützt selbstverständlich die Verschlüsselung der Seiten und der übermittelten Daten. Dabei wird SSL (Secure Socket Layer) eingesetzt. ePages empfiehlt, alle Administrationsebenen sowie alle Seiten, auf denen in der Storefront persönliche Daten (z.B. Adressen oder Zahlungsinformationen) eingegeben werden, zu verschlüsseln.

## 4.7 Kommunikation mit anderen Systemen

### Kommunikation mit Zahlungssystem verschlüsselt

Bei der Kommunikation von ePages 5 mit anderen Systemen gelten besondere Bedingungen für die Datenübermittlung. So wird beispielsweise für die Bezahlung über ein elektronisches System in jedem Fall eine verschlüsselte Kommunikation (siehe oben) benutzt. Bei den meisten Anbietern derartiger Systeme (z.B. „WorldPay“) werden dabei die Kreditkartendaten nicht innerhalb der ePages-Applikation erfasst. ePages 5 übermittelt auf abhörsicherem Weg lediglich den Betrag und die Währung der Bestellung an das E-Payment-System. Der Endkunde gibt auf diesem die Kreditkarteninformationen ein und autorisiert die Abbuchung für diese Transaktion. ePages 5 und damit auch der Händler erhält lediglich die Bestätigung über den Erfolg (oder Misserfolg) der Transaktion, nicht aber die Kreditkartendaten selbst. Das Plus an Sicherheit liegt hierbei also darin, dass die sicherheitsrelevanten Daten nicht zwischen den verschiedenen Systemen ausgetauscht werden müssen und auch die Shopdatenbank diese Daten nicht verwalten muss.

### Web Services

Eine andere Möglichkeit stellen Web Services dar. Diese Technologie, welche ein spezielles Protokoll (SOAP) und XML-Strukturen als Datencontainer verwendet, wird bspw. bei der Verbindung zwischen ePages 5 und einem Warenwirtschaftssystem (ERP), einem Kundenmanagementsystem (CRM) oder einem Logistiksystem benutzt. Zugriffe über Web Services sollten einerseits verschlüsselt erfolgen (es sei denn, beide Systeme stehen im internen und damit sicheren Netz in Verbindung) und werden andererseits durch die zusätzliche Übermittlung von Login-Name und Passwort abgesichert.

Der Sicherheit der Daten von miteinander kommunizierenden Anwendungen und der Autorisierung der Funktionsaufrufe sollte bei jeder Integration von ePages 5 große Bedeutung beigemessen werden.

## 5. Erweiterungsmöglichkeiten

ePages 5 kann sowohl hinsichtlich der shop-internen Funktionen erweitert werden, als auch bezüglich der Interaktion mit externen Systemen. Diese Anpassungen sind auf verschiedenen Wegen möglich. Um alle Eigenentwicklungen hinsichtlich Design, Datenbankerweiterungen und Perl-Codierung zu vereinen, werden die Eigenentwicklungen in Form von “Cartridges” zusammengefasst und dem Shopsystem hinzugefügt. Cartridges orientieren sich an bestimmten ePages 5 Standards und weisen somit eine Reihe von Vorteilen auf:

- ▶ Sie sind installierbar und deinstallierbar.
- ▶ Sie kennen Abhängigkeiten und Rechte.
- ▶ Sie können sämtliche Funktionen der Standard-API nutzen.

Für die Erstellung von Cartridges stellt ePages eine “Cartridge-Development-Toolbox” zur Verfügung. Diese umfasst hilfreiche Skripte, umfangreiche Dokumentationen mit Code-Beispielen und Datenbankmodellen sowie zwei größere Beispiel-Cartridges.

Im Lieferumfang enthalten ist darüber hinaus eine “Diagnostics-Cartridge”. Diese gibt dem Entwickler einen umfassenden Überblick über Details des ePages-Systems sowie über seine eigenen Entwicklungen.



**ePages Software GmbH**

[www.epages.de](http://www.epages.de)

[info@epages.de](mailto:info@epages.de)