



## WHITEPAPER

---

► **Die Verfügbarkeit von  
Web-Applikationen**

Was versteht man unter  
Systemverfügbarkeit?

Welches Verfügbarkeitslevel  
ist für meine Ansprüche  
wirtschaftlich sinnvoll?

# VERFÜGBARKEIT VON WEB-APPLIKATIONEN

Die Verfügbarkeit ist eine der bekanntesten Säulen der IT-Sicherheit und bleibt doch oft ein theoretischer Begriff. Allerdings nur solange, bis der eigene Web-Server, auf den man als Privatperson oder Unternehmen angewiesen ist, plötzlich ausfällt. Dann steht dieser Begriff programmatisch im Raum und gewinnt urplötzlich an Bedeutung. Denn selbst wenn jemand nur einen kleinen Web-Shop betreibt, muss man mit dem Risiko leben, plötzlich ohne Existenzgrundlage dazustehen, wenn das System dauerhaft ausfällt. Umso mehr gilt dies Schreckensszenario für größere Unternehmen. Daher hat eine Betrachtung der Systemverfügbarkeit einen hohen Stellenwert.

## Verfügbarkeit gleich volle Nutzbarkeit

In der Regel wird von Providern für angebotene Dienste mit dem Kunden eine Verfügbarkeit vereinbart. Dieses so genannte „**Service Level Agreement**“ (SLA) beschreibt, welche Verfügbarkeiten der Anbieter garantiert, und welche Ersatzleistungen fällig sind, sollte die Verfügbarkeit des Systems unterschritten werden.

Die Verfügbarkeit selbst wird dabei per Definition als Kennzahl eines Systems angegeben und berechnet sich wie folgt:

$$V = \left( 1 - \frac{\sum t_a}{T_b} \right) * 100 \%$$

$t_a$  Ausfallzeiten       $T_b$  Betriebszeit

Als Betriebszeit wird ein fest definierter Zeitraum angesetzt, das kann die Gesamtbetriebszeit eines Systems oder aber auch ein fester Zeitraum wie etwa ein Jahr sein. Beispiel: Fällt in einem Jahr ein System, das rund um die Uhr laufen soll, insgesamt 48 Stunden aus, entspricht das folgender Verfügbarkeit:

$$V = \left( 1 - \frac{48}{365 * 24} \right) * 100 \% = 99,45 \%$$

Die in Standardangeboten häufig vorzufindende Angabe einer Verfügbarkeit von 99 % erscheint zwar auf den ersten Blick verlockend – nach genauer Betrachtung wird aber nun klar, dass nach einer solchen Vereinbarung das System mehr als viereinhalb Tage ausfallen

darf, ehe Schadensersatz oder ein ähnlicher Ausgleich geltend gemacht werden kann. Ein solcher Ausfall könnte für den einen oder anderen schon das Aus bedeuten – denn gerade Shop-Betreiber mit einem Massenangebot könnten dadurch herbe Einbußen erleiden, wenn es für die Kunden hinreichend Ausweichmöglichkeiten gibt.

**Aus diesem Grund ist es wichtig, folgende Punkte zu überprüfen:**

- Was kann die Verfügbarkeit eines Systems beeinflussen?
- Welche Gegenmaßnahmen stehen allgemein zur Verfügung?
- Welcher Kostenaufwand ist zu erwarten bzw. sinnvoll?
- Welche Möglichkeiten stehen mir als Kunde offen?

## Analyse des Systems und der Prozesse

Um genau ermitteln zu können, welche Teile eines Systems zur Berechnung der Verfügbarkeit herangezogen werden müssen, ist eine genaue Analyse der Systemlandschaft samt ihrer Infrastruktur notwendig. Dabei ist eine prozessorientierte Sicht der Dinge wichtig, damit sich die Systeme operational einordnen lassen. So lässt sich etwa auf einem physischen Server eine Vielzahl virtualisierter Systeme betreiben. Ein Ausfall würde also nicht nur ein Hardware-System (= Server), sondern auch alle darauf laufenden virtuellen Maschinen mit ihren Applikationen betreffen – und damit auch alle Prozesse, die auf diese Applikationen angewiesen sind.

Mit „Prozess“ sind an dieser Stelle also alle zusammenhängenden Arbeitsabläufe gemeint, die zu einem spezifischen Dienst-Angebot gehören. So ist z.B. der Vorgang „Verkauf eines Artikels über den Online-Shop“ ein Prozess. Das beginnt mit der Auswahl des Artikels, geht über das Hinzufügen zum Warenkorb und dem Gang zur virtuellen Kasse bis hin zum abschließenden Bezahlvorgang. Dieses Beispiel ist zwar sehr grob gefasst, aber jeder Prozess kann wiederum in Unterprozesse aufgeteilt werden, so dass sich eine sinnvolle, hinreichend feinkörnige Prozess-Gliederung für das jeweilige Angebot finden lässt. Nur durch eine solche Darstellung der Systeme bezogen auf die darauf ablaufenden Prozesse lässt sich später eine **Schutzbedarfsermittlung** aufstellen, an Hand derer dann festgelegt werden kann, bei welchen Systemen es sich lohnt, mehr Aufwand zu treiben, um die Systemsicherheit und damit die Verfügbarkeit zu erhöhen.

Man erkennt schnell, dass es hier Vorfälle gibt, mit deren Eintreten weniger zu rechnen ist und andere, die ständig möglich sind: Die Vorfälle haben also eine unterschiedliche **Eintrittswahrscheinlichkeit**. Eine Festplatte fällt hin und wieder aus, wogegen eine Systemunterbrechung durch einen Unfall weniger wahrscheinlich ist.

## Bedrohungen durch mögliche Vorfälle

Als Basis müssen die Bedrohungen bekannt sein, die eine Verfügbarkeit der Systeme gefährden. Die folgende Tabelle zeigt eine Auswahl von Beispielen, mit welchen Vorfällen man bei dem Betrieb von Web-Servern rechnen muss.

Kategorie	Gruppe	Vorfall ausgelöst durch
Hardware	Systeme	Verschleiß (MTBF)
		Konstruktionsfehler
		Überbelastung
Netz-Infrastruktur	Außenanbindung	Unterbrechung der Stromversorgung
		nicht ausreichende Klimaanlage/Kühlung
		Unterbrechung der Netzanbindung
		Gebäudeschäden
Software	Systemfehler	Fehler im Betriebssystem
		Fehler/Ausfall von Schnittstellen
		Fehler in Web-Applikationen
	Wartung	Einspielen von Updates, Patches
	Externe Angriffe	DOS-Attacken auf die Systeme
		XSS/Code-Injection u.ä. auf der Web-Seite
		Datenverlust der Systeme (Folgefehler)
	Malware	Virenbefall durch Spam o.ä.
		Wurmbefall (aktive Attacke)
		Trojanische Pferde
Rootkits		
Infrastruktur	Notfälle	Feuer
		Überschwemmung
		Bombendrohung
		Unfälle
		Sabotage
		Höhere Gewalt

Um nun zu ermitteln, wo die stärksten Bedrohungen der Verfügbarkeit liegen, ist zunächst einmal die obige Tabelle nach den Eintrittswahrscheinlichkeiten zu sortieren. Liegt die eingangs schon erwähnte Analyse der Systeme samt ihrer Verknüpfung mit den Prozessen vor, lassen sich auch zu jedem potenziellen Vorfall die betroffenen Systeme zuordnen und die gefährdeten Prozesse identifizieren. An dieser Stelle kann der IT-Verantwortliche, zumindest grob, eine potenzielle Schadenshöhe beim Ausfall des jeweiligen Prozesses errechnen. Und auch die eigentliche Bedrohung kann so in Klassen eingeordnet werden: Der Ausfall eines Servers, der beispielsweise nur für die statistische Auswertung von Logfiles zuständig ist, stellt eine kleinere Bedrohung dar als der Ausfall des Web-Servers, auf dem der eigentliche Web-Shop zur Verfügung gestellt wird.

## **Berechnung des Vorfaltrisikos**

Auf Basis einer solchen Risiko-Einschätzung lässt sich dann gut ablesen, welches System besonders schützenswert ist, nämlich das mit dem höchsten Risiko. Somit ist nun eine auf dem jeweiligen Risiko basierende Einschätzung möglich, welchen Aufwand ein Unternehmen zum Schutz seines Kerngeschäfts und der weniger kritischen Systeme investieren möchte. Das und nichts anderes stellt die Schutzbedarfsermittlung dar. Dieser Prozess ist übrigens beim ersten Mal sehr aufwändig, und muss, soll das Prinzip greifen, zyklisch aktualisiert werden, da sich die Systemlandschaft in der Regel permanent ändert.

## **Mögliche Gegenmaßnahmen**

Den meisten Aufwand in Sachen Verfügbarkeit zur Abwehr von Bedrohungen investieren Unternehmen in den Betrieb der Systeme. Damit liegt hier der Löwenanteil des Aufwandes in der Regel beim Provider, als Kunde kann man hier nur indirekt Einfluss nehmen. In der Auflistung der Schwachstellen als Baumstruktur sind dafür stichwortartig Maßnahmen passend zu den gelisteten Vorfällen aufgeführt, die in der Regel als Gegenmaßnahmen etabliert sind.

Je nach Schutzbedarf des eigenen Angebots kann es hier sinnvoll sein, mit dem Provider eine entsprechende SLA aufzusetzen und die Umsetzung der Maßnahmen auch zu überprüfen. Denn je nach dem, welche Dienste auf den Servern des Providers angeboten werden sollen, kann es sein, dass man als Anbieter auch gesetzliche Vorgaben hat, ein bestimmtes Sicherheitsniveau einzuhalten.

## **Verantwortung ist nicht delegierbar**

Dazu ein Beispiel: Wenn etwa ein Finanzdienstleister einen Server bei einem Provider betreibt, ist dies ein klassischer Outsourcing-Fall. Hier ist der Finanzdienstleister selbst für die Einhaltung der Sicherheitsstandards, die auch von Gesetzes wegen gefordert sind, verantwortlich und kann diese Verantwortung nicht per SLA auf den Provider abwälzen. Das bedeutet, dass er sich über die Umsetzung passender Maßnahmen, ein gut funktionierendes Patch-Management oder die Durchführung von Notfall-Tests etc. selbst überzeugen muss – genau so, als würde er den Server im eigenen Haus betreiben.

## **Ökonomische Überlegungen**

Nun wird der Provider natürlich unterschiedliche Pakete mit entsprechend höherer, garantierter Verfügbarkeit zu entsprechenden Preisen anbieten. Da diese exponentiell mit der Verfügbarkeit steigen, gilt es, hier die Kosten in Balance zu halten, damit aus der gut gemeinten Vorsicht nicht ein Verlustgeschäft wird. Dafür lässt sich eine einfache Rechnung aufstellen: Anhand der Schutzbedarfsermittlung kann die potenzielle Schadenshöhe bei einem Systemausfall, der während eines bestimmten Zeitintervalls auftritt, ermittelt werden. Setzt man diesen Betrag in Relation zu der Summe der tolerierten Ausfallzeiten, die durch die SLAs festgelegt sind, steht die Summe fest, die man als höchstmöglichen Schaden auf Basis der garantierten Verfügbarkeit annehmen kann. Diese Summe ist nun auf einen monatlichen Betrag herunter zu skalieren, den man innerhalb des betrachteten Zeitraums zurück legen müsste, um den Schaden auffangen zu können.

Ein etwaiger Gewinnverlust sollte hier außen vor gelassen werden, schließlich geht es nur um den notwendigen Betrag, das Web-Angebot verlustfrei zu betreiben. Zu dieser so ermittelten Summe werden nun die monatlichen Kosten des aktuellen Systems hinzu gerechnet.

Damit kann verglichen werden – liegt das Ergebnis deutlich über den Kosten, die der Provider für ein System mit höherer Verfügbarkeit veranschlagt, lohnt sich dieses System. Im anderen Fall ist vielleicht eine andere Lösung vorzuziehen.

### **Eigene Initiative**

Die Verfügbarkeit eines Systems lässt sich deutlich erhöhen, wenn man dieses redundant bei einem hinreichend zertifizierten Provider betreibt. Entweder per se als paralleles System mit Loadbalancing oder als Cluster, das im Fehlerfall den Betrieb übernimmt.

Eine solche Lösung hat in der Regel den Charme, deutlich günstiger zu sein, als eine entsprechend „aufgebohrte“ Verfügbarkeit, sofern dies mit vertretbarem Aufwand technisch machbar ist.

Aber nicht nur der Betrieb der zu Grunde liegenden Server bedarf entsprechender Maßnahmen zur Absicherung der Verfügbarkeit, denn jede Aktivität, die man als Betreiber des Angebots selbst verantwortet, geht in die Verfügbarkeit des Systems ein. Wird beispielsweise bei einem Provider ein Root-Server angemietet, ist dieser nur für die Verfügbarkeit des Systems an sich zuständig. Für die Software und Systeme, die darauf laufen, ist man eigenverantwortlich – stürzt die Software ab oder wird erfolgreich angegriffen, kann der Provider dafür nicht haften. Der Betreiber eines Web-Angebots darf also die eigene Mitwirkung bei der Sicherheit nicht vollkommen aus den Augen verlieren und sollte sich daher genau mit den möglichen Bedrohungen des eigenen Systems und entsprechenden Gegenmaßnahmen auseinandersetzen.

### **Schnelle Reaktionszeiten**

Und wenn doch etwas passiert? Hier hilft nur eins: intensives Monitoring – denn jede Sekunde zählt. Daher ist eine permanente Überwachung der korrekten Funktionalität des eigenen Web-Angebots ein Muss, damit Fehler unverzüglich aufgedeckt und schnellstmöglich korrigiert werden können. Das gilt sowohl auf Betriebs- und somit Provider-Seite als auch auf der Seite des eigentlichen Anbieters: Schließlich kann man eventuell im Notfall noch auf eine Ersatzseite umschalten, um das Schlimmste zu verhindern.

Und damit auch in einem solchen Fall jeder weiß, was zu tun ist, müssen dafür Notfallpläne vorhanden sein, die genau festlegen, welche Maßnahmen ergriffen werden. Nur so lässt sich verhindern, dass in einem solchen Szenario jeder Versuch des Entgegenwirkens im Chaos versinkt und die Verfügbarkeit noch stärker leidet.

### **Über die Host Europe GmbH**

Die Host Europe GmbH entwickelt und vermarktet seit 1997 zuverlässige und innovative Internet-Services für Privat- und Geschäftskunden in Deutschland, Österreich und der Schweiz. Der Einsatz hochausfallsicherer Infrastruktur, Partnerschaften mit kompetenzstarken Technologieunternehmen, ein umfassendes Leistungsspektrum skalierbarer und hochwertiger Internet-Services sowie kundenorientierter Support zeichnen Host Europe als einen der führenden Internet-Hosting-Provider aus.

### **Kontakt**

Rund um die Uhr gebührenfrei aus dem Festnetz: 0800 467 8387

Sie benötigen weitere Informationen zu unseren Managed Hosting-Lösungen?

Unsere Vertriebsmitarbeiter helfen Ihnen gerne weiter: [vertrieb@hosteurope.de](mailto:vertrieb@hosteurope.de)