Internet-Verfügbarkeitssystem –

# Welche Qualität hat das Internet?

**Mit der stetig wachsenden Anzahl an Möglichkeiten und Benutzern im Internet steigt zugleich die Komplexität der IT-Systeme. Auf Grund der zunehmend größeren Bandbreiten entstehen weiterhin neue Dienste zur umfassenderen Nutzung des Internets. So kommt es, dass insbesondere Geschäftsprozesse hinsichtlich der neuen Möglichkeiten optimiert werden, oft auch um einen Wettbewerbsvorteil zu erzielen. Häufig wird bei aller Euphorie in diesem Zusammenhang jedoch übersehen, dass dadurch die Abhängigkeit von diesen Technologien kontinuierlich zunimmt. Trotzdem stehen dem Einsatz der Technologie nicht immer die adäquaten Sicherheitsmaßnahmen gegenüber. Aufgrund dessen kann es zu Funktionsstörungen kommen, die durch technische Defekte, Überlastung oder bösartige Angriffe verursacht werden. Hier bedarf es neben den herkömmlichen Maßnahmen zur Absicherung zukünftig auch neuer Überwachungsmethoden, um die optimale und sichere Nutzung des Internets zu gewährleisten.**

Für den Benutzer ist es in erster Linie wichtig, dass sich die Internet-Dienste auf einer akzeptablen Qualitätsebene bewegen. Die Qualität eines Dienstes im Internet kann anhand von Dienstgütemerkmalen – dem so genannten Quality of Service (QoS) – wie Bandbreite, Verzögerung oder die Standardabweichung in den Antwortzeiten spezifiziert werden. Neben diesen eher leistungsorientierten Merkmalen, die insbesondere für Anwendungen in Echtzeit wie Audio- oder Video-Streaming wichtig sind, gewinnt eine weitere Benutzeranforderung immer mehr an Bedeutung: Wie verfügbar ist ein bestimmter Internet-Dienst inklusiver der entsprechenden Daten. Unter Berücksichtigung der Prämisse 'If you can't messure it, you can't manage it', war das Ziel ein Internet-Verfügbarkeitssystem zu entwickeln, mit dem es möglich ist, schnell einen Überblick über die Verfügbarkeit und die Dienstgüte wichtiger Dienste im Internet zu erhalten. Administratoren setzen eine ganze Reihe von Netzwerkmanagementsystemen ein, um die Funktionsfähigkeit ihrer Server zu überprüfen. Jedoch ist ein funktionierender Server kein Garant dafür, dass dieser auch für einen Benutzer erreichbar ist. Möchte ein Anwender einen Dienst im Internet beanspruchen, so benötigt er einen Provider, ist darauf angewiesen, dass die Router seine Anfragen in weitere autonome Systeme leiten und dass die DNS Server ihre Arbeit verrichten. Nur wenn die Router auf dem Weg, alle notwendigen DNS-Server und der Rechner sowie das Betriebssystem und die eigentliche Software des angebotenen Dienstes funktionieren, kann der angebotene Dienst im Internet beansprucht werden.

## Internet-Verfügbarkeitssystem

Das Internet-Verfügbarkeitssystem stellt die Dienstgüte der wichtigsten Dienste im Internet und der Infrastruktur aus Benutzersicht dar. Dabei werden dienstspezifische Messmethoden verwendet, um die Funktionalitäten zu überwachen. Mittels der jeweils eingesetzten Anwendungsprotokolle der Dienste im Internet wird versucht, zu den zu überwachenden Systemen eine Verbindung aufzubauen und den Dienst zu nutzen. Die Antwortzeiten und weitere Informationen werden gespeichert und dienen als Basis für Auswertungssysteme.

Bei der Messung von QoS-Parametern spielt insbesondere der Übertragungsweg eine entscheidende Rolle. Leitet ein Router, der für die Verbindung zu einem Dienst im Internet verantwortlich ist, Anfragen nur sehr langsam weiter, führt dies zu schlechten Messergebnissen bezüglich des Dienstes. Dies kann beispielsweise dann der Fall sein, wenn der Router überlastet ist. Somit ist es essentiell, dass stets die Ursache der Störung eruiert werden kann; also zum Beispiel, dass ein Problem nicht durch den Server, auf dem der Dienst läuft, verursacht wurde, sondern dass das Problem in der Netzinfrastruktur liegt. Um dies zu erkennen, müssen mehrere Messungen in unterschiedlichen Netzsegmenten erfolgen. Genau dieses Konzept verfolgt das Internet-Verfügbarkeitssystem. Es werden mehrere Messsysteme – im Folgenden Drohnen genannt – in unterschiedlichen Bereichen des Internets platziert. Diese Drohnen führen an jeder Stelle die gleichen Messmethoden durch. Dadurch werden diverse Sichtweisen bezüglich eines zu testenden Dienstes erzeugt und können mit einander verglichen werden. Liefert eine Drohne ein Messergebnis, dass im Vergleich mit anderen völlig aus dem Rahmen läuft, so liegt in diesem Fall eher ein Problem in der Netzinfrastruktur auf dem Weg von der Drohne zum Ziel vor, als ein Serverproblem. Auf diese Weise lassen sich Störungen leichter lokalisieren, Fehler eingrenzen und gezielter beheben.

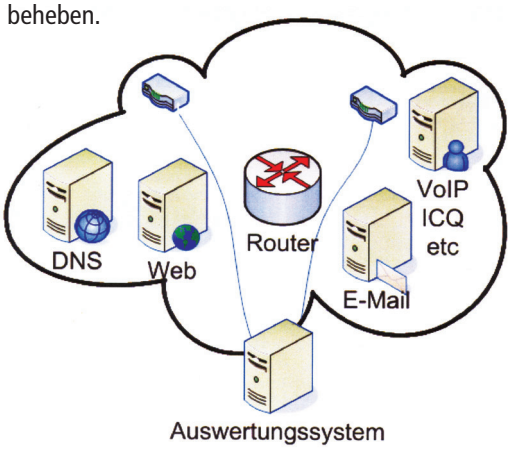



*Abb. 1*
*Die Drohnen beobachten Dienste im Internet und schicken die Ergebnisse zu einem Auswertungssystem*

Die Drohnen arbeiten selbstständig und können in beliebige Netze integriert werden. In den meisten Fällen wird eine Drohne hinter einer Firewall oder einem NAT-Router betrieben und ist deswegen nicht ohne weiteres zur Fern-Administration erreichbar. Daher bauen alle Drohnen automatisch in angegebenen Intervallen eine Verbindung zu einem Vermittlungsserver – dem Controller – auf und übertragen ihre bisherigen Ergebnisse. Zugleich können auf diesem Wege neue Aufgaben an eine Drohne übertragen werden. Der Controller selbst verfügt über keine persistente Datenhaltung, sondern dient als Schnittstelle zwischen den Drohnen und dem Auswertungsserver, welcher eine Datenbank beherbergt. In der Datenbank des Auswertungsservers werden alle Aufgaben der Drohnen sowie die gewonnenen Ergebnisse gespeichert. Zur Aufgabendefinition und zur Anzeige dient eine komfortable Benutzeroberfläche. Sobald eine neue Aufgabe gestellt oder ei-

ne bestehende verändert wird, wird der entsprechenden Drohne bei der nächsten Synchronisation mit dem Controller diese Änderung mitgeteilt. Da die Drohne sich automatisch aktualisiert, muss sie nach ihrem Start nicht mehr direkt administriert werden. Hier genügt es, Veränderungen in der Datenbank des Auswertungsservers über die Benutzeroberfläche durchzuführen.

### Analyse der Datenübertragung

Eine Drohne verfügt über verschiedene Messmodule, die die Tests für verschiedene Dienste übernehmen. Die Messmodule stellen Dienstanfragen an Server und verwenden dabei Protokolle der Anwendungsschicht. Um einen Webserver zu testen wird beispielsweise das HTTP-Protokoll verwendet. Bei jeder Interaktion mit einem Server entsteht Datenverkehr, der im Anschluss analysiert wird, um die Qualität der Verbindung beurteilen zu können. Dabei werden QoS-Parameter und weitere Verbindungseigenschaften bestimmt. Dies geschieht unabhängig von dem beanspruchten Dienst.

### Paketverlustrate (Anzeichen für die Qualität der Verbindung)

Die Paketverlustrate gibt an, wie viel Prozent der versendeten Pakete während der Übertragung verloren gehen. Dies kann durch Überlastungen in der Infrastruktur oder einem Defekt von Netzkoppelelementen (zum Beispiel Router) verursacht werden. Da ein verlorenes Paket erneut versendet werden muss, kostet ein Verlust Zeit und Netzwerkressourcen. Im Normalfall liegt die Paketverlustrate zwischen 0,5 und 0,8 Prozent. Jedoch gibt es einige Ausreißer, bei denen die Verlustrate zwischen drei und vier Prozent liegt.

### Verfügbarkeit

Betreiber von Online-Shops sind absolut davon abhängig, dass ihr System für die Kunden erreichbar ist und schließen deswegen mit ihrem ISP Service Level Agreements (SLA) ab, in denen genau festgelegt ist, wie hoch die Verfügbarkeit sein muss. Eine übliche Angabe ist, dass die Verfügbarkeit bei 99,999 Prozent liegen muss. Das bedeutet, dass innerhalb eines Jahres die gesamte Ausfallzeit maximal bei 5,256 Minuten liegen darf. Für diese Garantie muss der Kunde den ISP bezahlen. Mit dem Internet-Verfügbarkeitssystem ist er jetzt in der Lage, genau zu überprüfen, wie hoch wirklich die Ausfallzeiten sind. Bei einer Überschreitung der vereinbarten Zeit kann er einen Teil des Rechnungsbetrages abziehen und eine Wertminderung vornehmen.

### Reaktionszeit eines Servers

Die Reaktionszeit gibt an, wie lange es nach einer Dienstanfrage dauert, bis eine Antwort des Servers eingetroffen ist. Dies ist eine wichtige Größe bei DNS Servern. Vor jedem Verbindungsaufbau der über einen Domainnamen durchgeführt werden soll (z.B. www.google.de), wird ein DNS Server kontaktiert, um den Domainnamen in eine IP Adresse zu übersetzten. Wenn ein DNS Server langsam reagiert, hat dies Konsequenzen bei dem Verbindungsaufbau mit dem eigentlichen Server. Durchschnittlich antwortet ein Server innerhalb von 100 ms.

### Anzahl der Router-Sprünge (Hops)

Die Anzahl der Hops gibt an, über wie viele Router ein Datenpaket geleitet wird, bis das Ziel erreicht ist. Um Pakete weiterzuleiten, muss jeder Router die Pakete analysieren, die er erhält. Dies kostet Zeit und kann bei einer Überlastung des Routers zu Fehlern führen. Je mehr Router genutzt werden, desto höher ist die Wahrscheinlichkeit, dass ein Fehler auftritt und sich die Übertragung verzögert. Die Anzahl der Router hängt natürlich sehr vom Standort im Internet ab. Typisch für inländische Server sind 8 bis 15 Router.

### Round Trip Time (RTT) der Router und Server

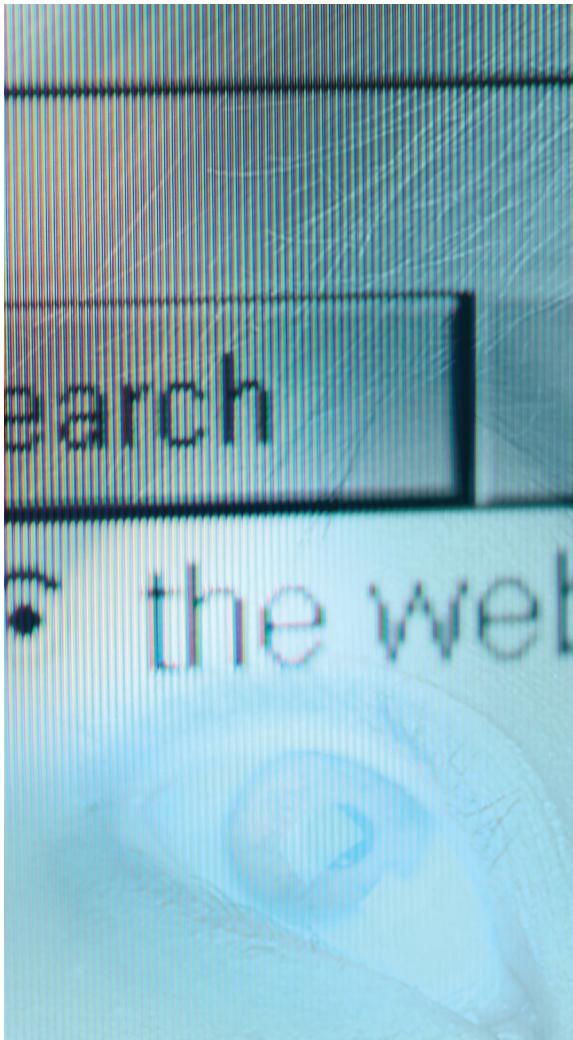
Die Round Trip Time ist die Zeit, die ein Paket vom Sender zum Empfänger und wieder zurück benötigt. Diese Zeiten werden für die Router und der Dienstserver ermittelt, um die Geschwindigkeit der Verbindung und Reaktionszeiten der Router feststellen zu können. Wenn sich die Reaktionszeit eines Servers ändert und gleichzeitig eine Veränderung bei einem verantwortlichen Router feststellbar ist, kann dadurch das schlechte Ergebnis des Servers erklärt werden. Üblicherweise liegt die RTT eines Servers unter 100 ms und die Standardabweichung unter 5 ms. Alle diese Faktoren spielen gerade bei Echtzeitsystemen, wie bei einem VoIP-Gespräch, eine große Rolle. Hier gelten folgende Empfehlungen für einen erfolgreichen Einsatz dieser Technologie.

- Zeit für eine einfache Wegstrecke (Delay) < 150 ms (halbe RTT Zeit)
- Standardabweichung der RTT (Jitter) < 30 ms
- Paketverlustrate < 1 %

Diese Werte werden in der Regel eingehalten, jedoch kommen noch weitere Verzögerungen für die Verwendung des Audio Codecs, der Komprimierung und Verschlüsselung hinzu.
Deswegen kann ein überlasteter Router empfindliche Störungen verursachen. Durch die Bestimmung der QoS-Parameter und der Analyse der Verfügbarkeit von Diensten kann das Internet Verfügbarkeitssystem vielseitig eingesetzt werden.

### Messmodule des IVS

Ein Messmodul geht bei der Kommunikation mit dem Server und der Beanspruchung eines Dienstes schrittweise vor. Es wird geprüft, in wie weit die Dienstnutzung des Servers erfolgreich war und an welcher Stelle gegebenenfalls ein Fehler aufgetreten ist. Diese schrittweise Vorgehensart erlaubt genauere Diagnosemöglichkeiten im Fehlerfall und damit eine schnelle Behebung der Ursachen. Interessant sind die Antworten auf eine Dienstanfrage, die ein Server zurückgibt. Sie geben Aufschluss darüber, in welchem Zustand sich ein Server befindet.



### HTTP Messmodul

Durch das HTTP Messmodul wird eine Verbindung zu einem Webserver aufgebaut und eine Datei zur Übertragung angefordert. Wurde eine Datei übertragen, steht fest, dass der Server erreichbar ist und der entsprechende Dienst seine Arbeit verrichtet. Der Rückgabewert des Servers gibt zusätzlichen Aufschluss über den Zustand des Webservers.

Meldet der Server zum Beispiel den Fehler 404, bedeutet dies, dass der Server selbst zwar einwandfrei funktioniert, die angeforderte Website aber nicht aufgefunden werden kann. Auch in diesem Fall ist das System nicht verfügbar.

### Darstellung der Ergebnisse

Die Ergebnisse werden im zeitlichen Verlauf grafisch dargestellt. Dies ermöglicht eine gute Übersicht und einen schnellen Vergleich der unterschiedlichen Parameter. Die Abbildung 2 zeigt den Verlauf der durchschnittlichen Bandbreite beim Abruf einer Webseite. Deutlich ist ein Einbruch der zur Verfügung stehenden Bandbreite im 2. Viertel der Abbildung zu erkennen.

Wenn man dieses Ergebnis alleine betrachtet, kann die Ursache für diesen Leistungseinbruch viele Gründe haben. Erst ein Vergleich mit weiteren Parametern, lässt eine genauere Einschätzung zu.

Wie in der Abbildung 3 zu sehen ist, hat sich zur selben Zeit, in der die Bandbreite zurückgegangen ist, die Route zum Server geändert. Statt der normalen Route mit üblicherweise 11, sind jetzt 12 Router für den Verbindung verantwortlich.

Deswegen liegt hier Verdacht nahe, dass für den Leistungseinbruch nicht der Server, sondern die Router-Verbindung verantwortlich ist. Damit kann eine genauere Interpretation der Bandbreitenveränderung erfolgen.

### Fazit

Das Internet Verfügbarkeitssystem nimmt Dienste im Internet in Anspruch, wertet die Serverantworten aus und analysiert den dadurch entstandenen Datenverkehr. Es werden Analysen der Transportprotokolle zur Bestimmung der QoS-Parameter vorgenommen und Statusmeldungen auf der Anwendungsebene ausgewertet. Das System eignet sich zur Überwachung, wie beispielsweise die Kontrolle von SLAs oder als Informationsquelle zur Fehlerdiagnose und Statusüberwachung. Die gewonnenen Werte dienen nicht nur zur aktuellen Verfügbarkeitsanzeige, sondern werden für spätere Verwendungen in einer Datenbank gespeichert. Somit lassen sich Langzeitbetrachtungen anstellen und Trendentwicklungen einsehen.

Das Internet Verfügbarkeitssystem ist ein eigenständiges System, wurde aber als Erweiterung des Internet-Analyse-Systems im Institut für Internet-Sicherheit entwickelt. Zusammen stehen damit zwei mächtige Datenquellen zur Verfügung, die von einem Frühwarnsystem genutzt werden könnten.

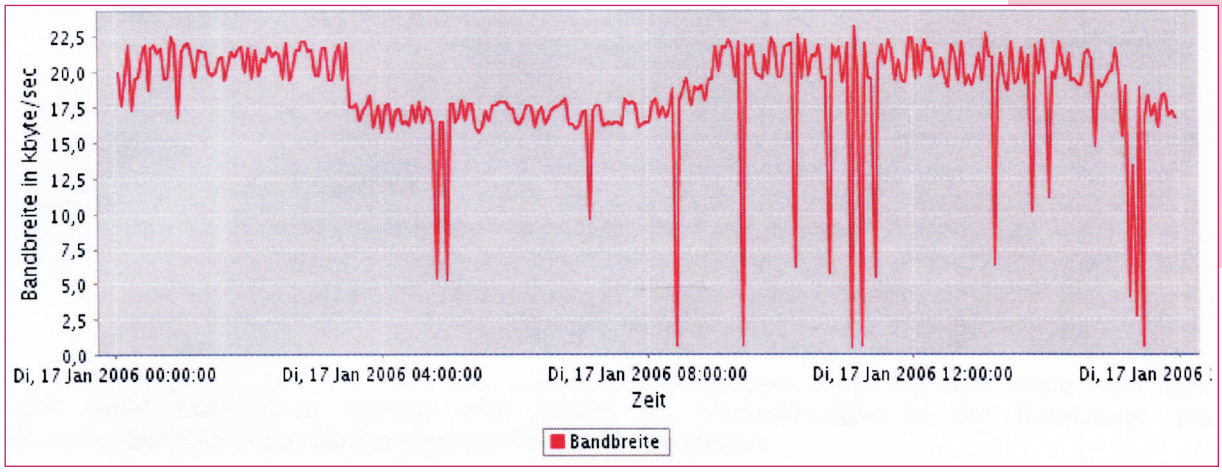



*Abb. 2: Abbildung 2 zeigt den Verlauf der Bandbreite mit einem Einbruch der Leistung.*

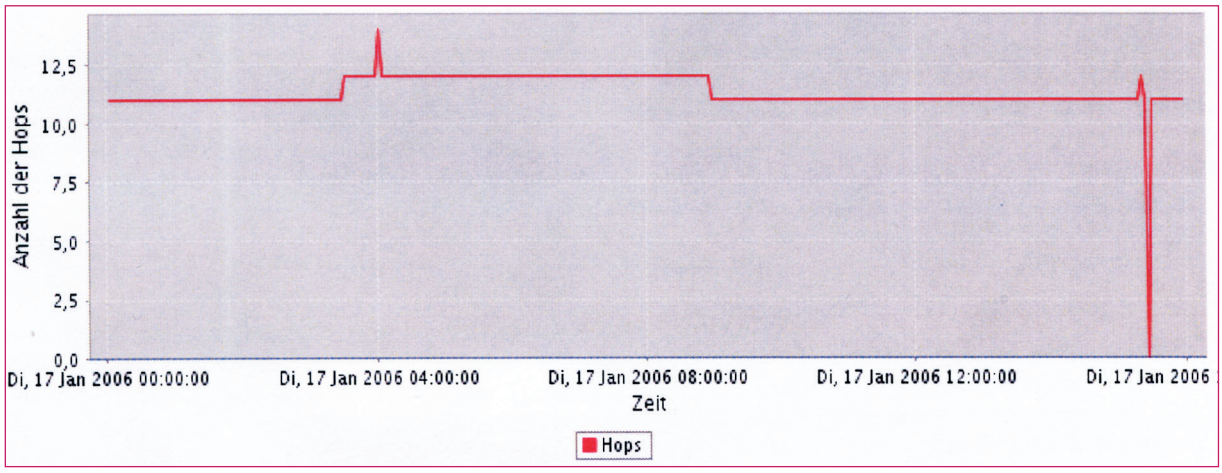



*Abb. 3: Abbildung 3 zeigt eine Veränderung der Route im selben Zeitraum auf, in der die Bandbreite in Abbildung 2 eingebrochen ist.*

Thomas Ostermann, thomas.ostermann@internet-sicherheit.de und Prof. Dr. Norbert Pohlmann, norbert.pohlmann@informatik.fh-gelsenkirchen.de, Institut für Internet-Sicherheit, www.internet-sicherheit.de