Technisches Konzept "Halbautomatische Wartungsanzeige"

Einleitung

Dieses technische Konzept beschreibt im ersten Teil die Problematik, die derzeit während Wartungszeiten oder bei Teilausfällen einer Internet-Anwendung besteht, sowie einen grundsätzlichen Lösungsansatz für diesen Fall.

Im Abschnitt "Technische Systembeschreibung Basissystem" wird eine kurzfristig realisierbare Lösungsmöglichkeit in Form einer halbautomatischen Wartungsanzeige skizziert.

Im dritten Abschnitt werden mögliche Einsatzszenarien für die halbautomatische Wartungsanzeige aufgezeigt.

Problemstellung und Lösungsansatz

Beim Betrieb der Infrastruktur von Internet-Applikationen (Firewalls, Router, Server, Switches) können bei jedem beteiligten Gerät Störungen oder Fehlfunktionen auftreten. Geplante oder ungeplante Wartungsarbeiten können ebenfalls Ausfälle des Systems nach sich ziehen.
Für eine endkundenorientierte Anwendung ist es daher sehr zu empfehlen, anstelle von Systemmeldungen wie „Server ist nicht erreichbar“ spezifische Hinweisseiten auf die Nichtverfügbarkeit von Teilanwendungen oder des Gesamtsystems anzuzeigen.

Eine entsprechende Meldung des Webserver-Systems der betroffenen Internet-Anwendung scheidet dabei aus, sobald vorgeschaltete Komponenten, wie z.B. Router, Firewalls oder der Webserver selbst gewartet werden oder ausgefallen sind.

Es empfiehlt sich daher, ein zusätzliches Gerät vor der Systemfirewall einzusetzen. Da jedoch dieses Gerät damit anfällig für Angriffe ist, sind besondere Vorkehrungen zu treffen, um z.B. spezielle Denial-Of-Service-Attacken abzuwehren, die den Zugang zum Webserver der Internet-Anwendung durch eine provozierte Wartungsanzeige blockieren, obwohl die Applikation einwandfrei läuft.

Da im Falle einer Internet-Applikation ein Webserver benötigt wird, um die Wartungsseite anzuzeigen, sollte hier kein Standard-Webserver verwendet werden, sondern eine Speziallösung, welche ausschließlich für den Zweck der Wartungsanzeige verwendbar ist. So muß z.B. verhindert werden, dass Hacker sittenwidrige Inhalte auf dem System ablegen können und diese anstelle der Wartungsseite angezeigt werden, da dieses System quasi ungeschützt im Internet betrieben wird.

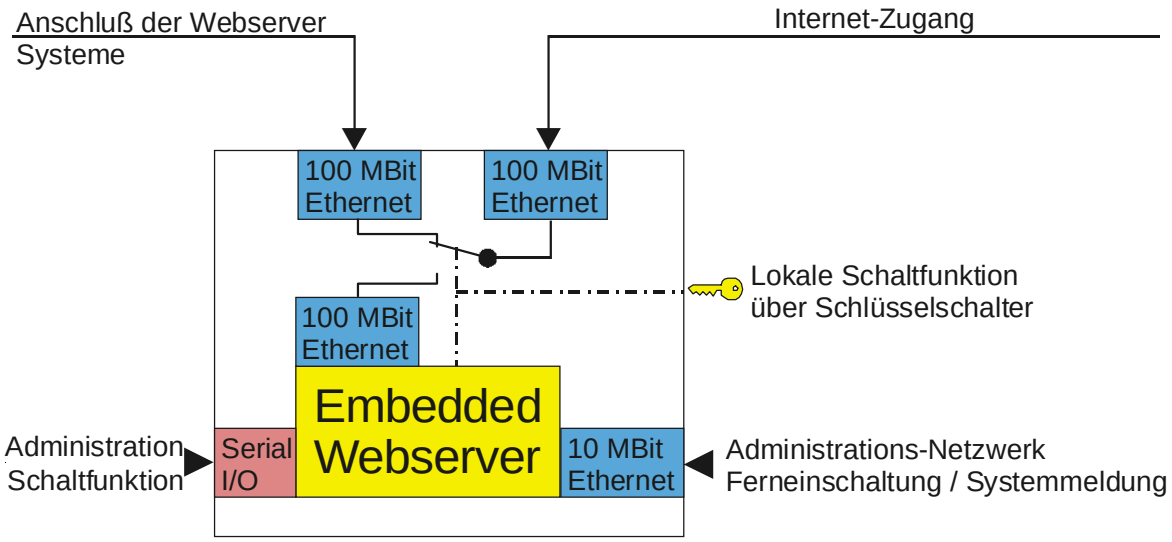
Weitere Anforderungen:

- Das System darf die Netzwerkperformance nicht beeinflussen.
- Das System muß möglichst preisgünstig in der Anschaffung und im Betrieb sein.
- Das System muß ohne Eingriff des Administrators wiederanlauffähig sein.
- Das System muß über eine geschützte Schnittstelle administrierbar sein.

Technische Systembeschreibung Basissystem

Aus Kostengründen und im Hinblick auf die Möglichkeit zukünftiger Erweiterungen wird eine Lösung auf Basis eines Embedded-Linux-Systems skizziert.

Dieses Linux-System wird ohne Dienste und weitestgehend ohne Hilfsprogramme betrieben, um Angriffsmöglichkeiten aus dem Internet zu verhindern. Im Normalbetrieb wird ein Netzwerkbypass geschaltet, welcher den gesamten Datenverkehr direkt weiterleitet.



Im Falle eines Ausfalles oder von Wartungsarbeiten an der Internet-Applikation wird das System über eine der Administrationsschnittstellen oder den Schlüsselschalter manuell auf „Wartungsbetrieb“ umgeschaltet. Zu diesem Zeitpunkt wird die Weiterleitung von IP-Paketen eingestellt und alle Anfragen werden vom Embedded-Webserver mit der Wartungsseite beantwortet.
Bei der Freigabe der Internet-Applikation muß das System wieder manuell in den Normalbetrieb umgeschaltet werden (Bypass).

Einer der Vorteile dieser Lösung besteht im Verzicht auf einen externen Webserver mit entsprechender Sicherheitsfunktionalität und gegebenfalls erforderlichen Schutzmaßnahmen (z.B. zusätzlich vorgeschaltete Firewall).

Um Manipulationen am System vorzubeugen und einen reibungslosen Restart zu ermöglichen, wird das System über Flash-Speicher gestartet und parametriert. Alle Netzwerkparameter lassen sich ausschließlich über die serielle Schnittstelle analog zu verfügbaren Routerlösungen einstellen, was Manipulationen an den Embedded-Webserverfunktionen über das unsichere Internet ausschließt.

Als Administrationsschnittstellen kann eine serielle Schnittstelle oder auch eine dezidierte Netzwerkschnittstelle verwendet werden. Falls die Netzwerkschnittstelle verwendet wird, muß ein spezieller Telnet-Dienst auf dem Wartungsserver benutzt werden, um Angriffsmöglichkeiten einzuschränken.

Erweiterungsmöglichkeiten

Oftmals treten unvorhersehbare Störungen oder Ausfälle einer Internet-Applikation auf, die unverzüglich zu einer Reaktion an der Kundenschnittstelle führen müssen.

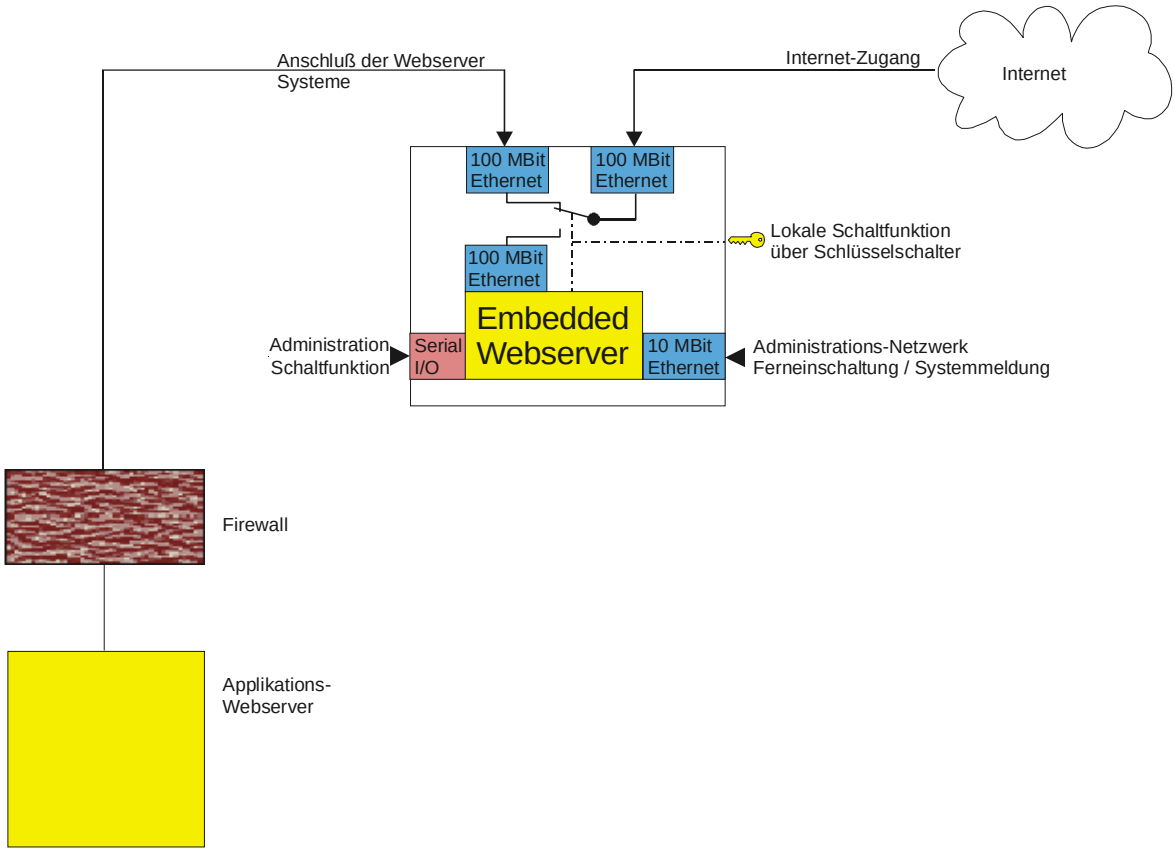
Denkbar wäre hierfür die lokale Erweiterung des Wartungsgateways auf eine automatische Erkennung der Nichtverfügbarkeit, sobald der Webserver auf eine Anforderung des Gateways nicht antworten konnte.

Ein alternativer Ansatz hierzu wäre eine Anbindung an einen Referenz-PC der betreffenden Internet-Anwendung; allerdings ist hierfür eine Sicherheitsanalyse durchzuführen, ob durch eine wie-auch-immer geartete Verbindung das Sicherheitskonzept der Internet-Applikation unterlaufen werden kann.

Das System könnte in einer späteren Ausbaustufe an das vorhandene Überwachungsnetz des Rechenzentrums angeschlossen werden, um so auch die Verfügbarkeit des "Wartungs-Gateways" sicherzustellen.

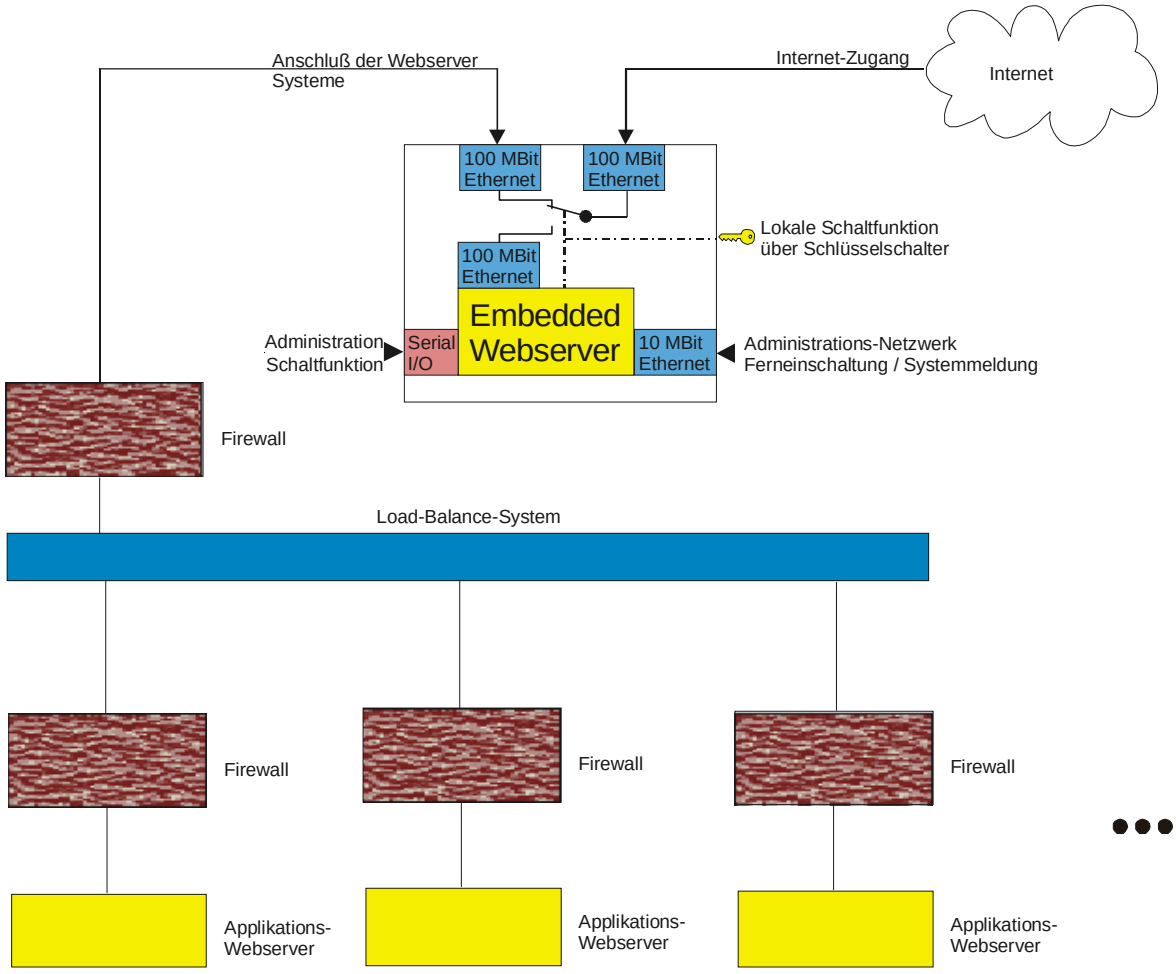
Einsatzszenarien

1. Direkter Betrieb in einem Single-Server-System



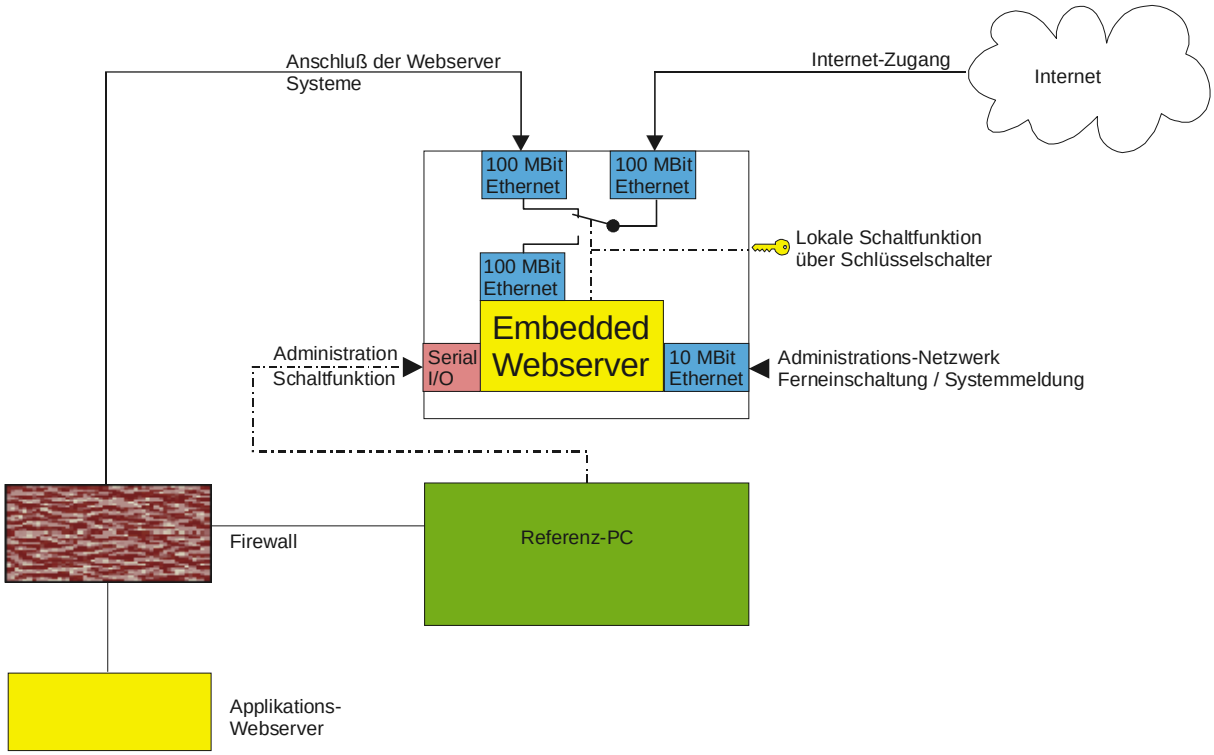
Das Wartungsgateway wird vor der Firewall eingesetzt, um auf bei einer Wartung oder einem Systemausfall der Firewall verwendet zu werden.

2. Betrieb des Wartungsgateways beim Einsatz eines Load-Balance-Systems



In diesem Anwendungsbeispiel wird das Wartungsgateway vor dem Load-Balance-System eingesetzt, um auch Wartungsarbeiten am Load-Balance-System zu ermöglichen. Dies schließt auch Änderungen an der Systemkonfiguration mit ein. (z.B. Austausch oder Erweiterung der Firewalls oder des Load-Balance-Systems selbst).

3. Betrieb eines Referenz-PC in Verbindung mit dem Wartungs-Gateway



In diesem Anwendungsszenario übernimmt der Referenz-PC die automatische Schaltfunktion, wenn innerhalb einer festgelegten Zeit die Internet-Applikation nicht reagiert bzw. wichtige Teile der Anwendung ausgefallen sind. Der Vorteil besteht in der ständigen und automatisierten Überwachung, welche im Fehlerfall den Endkunden der Internet-Applikation vor Fehlermeldungen bewahrt und eine neutrale Anzeige der Wartung auslöst. Alle weiteren Funktionen des Wartungsgateways sind ebenfalls verfügbar und erlauben damit auch ein manuelles „Überbrücken“ der Internet-Anwendung im Wartungsfall.