



ADACOR Infrastruktur

Autor.:
Monika Olschewski

Version:
1.0

Erstellt am:
14.06.2010

Whitepaper

ADACOR Hosting GmbH

Kaiserleistrasse 51
63067 Offenbach am Main

info@adacor.com
www.adacor.com

Die Infrastruktur der ADACOR Hosting GmbH

Die Infrastruktur der ADACOR Hosting GmbH bildet die Grundlage für ihre Leistungen

- Complex Hosting,
- Cloud Services und
- Domain Management.

Von der Infrastruktur und der Vorgehensweise des Unternehmens betrachtet, könnte der Leitsatz heißen: Sicherheit und Flexibilität zu einem fairen Preis. Dieses Whitepaper enthält die wichtigsten Fakten rund um das Thema Infrastruktur. Dazu gehören:

- Rechenzentren der ADACOR Hosting GmbH
 - Maßnahmen zum Schutz der Hardware
 - Netzanbindung
 - Storage
- Einsatz von Open-Source-Software
 - Gründe für den Einsatz von Open-Source-Software
 - Maßnahmen zum Schutz von Applikationen und Daten
 - Überwachung von Hardware, Applikationen und Daten
 - Datensicherungen

■ Seite 2

Rechenzentren der ADACOR Hosting GmbH

Die Server und Netzwerkkomponenten der ADACOR Hosting GmbH sind in drei unterschiedlichen Rechenzentren (RZ) untergebracht:

- e-shelter,
- interxion und
- RIEDEL Communications.

Die räumliche Trennung schließt Totalausfälle, verursacht beispielsweise durch Naturkatastrophen oder Terrorismus, weitestgehend aus. Datensicherungen werden ebenfalls räumlich voneinander getrennt von der jeweiligen Applikation an verschiedenen Standorten vorgehalten, um die Daten im Ernstfall jederzeit wiederherstellen zu können.

Der Hauptstandort ist das Rechenzentrum der e-shelter facility services GmbH in Frankfurt am Main. Ein weiterer Standort ist das Rechenzentrum von interxion, ebenfalls

in Frankfurt am Main. Das dritte Rechenzentrum befindet sich in Wuppertal bei RIEDEL Communications.

E-shelter betreibt in Frankfurt das größte Rechenzentrum Europas mit 60.000 m² RZ-Fläche für hochverfügbare Systeme und Komponenten. Auf dem Gelände, auch als Campus bezeichnet, stehen die verschiedenen Gebäude, in denen Unternehmen wie zum Beispiel die ADACOR Hosting GmbH Bereiche mit der entsprechenden Infrastruktur mieten, zum Beispiel die Anbindung an unterschiedliche Betreibernetzwerke.

Der Campus ist für die Nutzung als hochverfügbares Rechenzentrum konzipiert und umgesetzt worden. Zahlreiche Sicherheitsmechanismen schützen die Systeme und – damit verbunden – die kritischen Applikationen und sensiblen Daten der Kunden. Die ADACOR Hosting GmbH hat auf dem Campus von e-shelter drei Bereiche in verschiedenen Brandabschnitten und Gebäuden für ihre Systeme gemietet.

Gut geschützte Hardware in sicheren Rechenzentren

Exemplarisch für die Rechenzentren der ADACOR Hosting GmbH wird der Hauptstandort für die Hardware, das Rechenzentrum bei e-shelter in Frankfurt am Main, beschrieben. Sicherheitsmaßnahmen, zum Beispiel redundante Stromversorgung oder Kühlsysteme und permanente Überwachung, schützen die Hardware vor physischen Gefahren. Welche Maßnahmen das sind, erfahren Sie in diesem Abschnitt.

■ Seite 3

Der Campus von e-shelter ist von einer Sicherheitszaunanlage umgeben, die elektronisch überwacht wird. Eine Reihe von Findlingen außen im Zaunbereich sichern das Areal vor unberechtigtem Durchfahren von der angrenzenden Straße ab. Sicherheitstore, Schrankenanlagen und ausfahrbare Poller schützen den Campus vor dem unbefugten Eindringen von Kraftfahrzeugen.

Das Gelände ist mit einer lückenlosen Videoüberwachung an Türen und Zugängen sowie zahlreichen Sensoren zur Intrusionserfassung und -alarmierung ausgestattet. Die zertifizierte Notruf- und Betriebsleitstelle ist rund um die Uhr besetzt und wird durch bewaffnetes Sicherheitspersonal unterstützt.

Über berührungslose Chipkarten und Scramble-Tastaturen erfolgt der Zutritt für berechnete Personen. Scramble-Tastaturen sind vandalismussicher und ermitteln nach dem Zufallsprinzip die jeweilige Tastaturbelegung. Nach jeder Benutzung wird die Belegung des Tastenfelds neu berechnet. Das Eingeben des entsprechenden Codes auf der Scramble-Tastatur zu beobachten, nützt nichts, da die Tastaturbelegung bei der nächsten Benutzung bereits eine andere ist.

Brandschutzwände mit einer Feuerwiderstandsdauer von 90 Minuten sind weitere Sicherheitsmaßnahmen des Rechenzentrums. Sämtliche Räume in den Gebäuden sind mit digitalen Brandschutzmeldern und Systemen zur Brandfrüherkennung versehen. Die Brandbekämpfung erfolgt durch Flutung mit Löschgas.

Redundante Kälte- und Umluftkühlsysteme sorgen für die günstigste Temperatur in den Räumen. Das Raumklima wird zusätzlich durch automatisch gesteuerte Be- und Entlüftungsanlagen sowie Anlagen zur Be- und Entfeuchtung optimiert. Ein umfangreiches

Netz von Sensoren überwacht permanent die Raumtemperatur und die relative Luftfeuchte. Sämtliche Leitsysteme für die Gebäudeautomation sind redundant ausgelegt und über die unterbrechungsfreie Stromversorgung (USV) abgesichert.

Ebenfalls redundant ist die Stromversorgung, die über zwei separate Stränge erfolgt. Der Campus verfügt über redundante Netzersatzaggregate, unterbrechungsfreie Stromversorgung und Dieselgeneratoren und kann damit während eines Ausfalls die Stromversorgung für 72 Stunden sicherstellen. Ein eigenes Umspannwerk auf dem Gelände mit redundanten Transformatoren und Schaltanlagen gehört ebenfalls zur Ausstattung des Rechenzentrums.

Anbindung an mehrere Betreibernetzwerke sichert gegen Ausfälle

Der Campus von e-shelter ist an alle großen Betreibernetzwerke angeschlossen und verfügt über Netzanbindungen von 15 verschiedenen Anbietern. Die Wahl des oder der jeweiligen Netzanbieter treffen die Mieter selbst. Die ADACOR Hosting GmbH verfügt auf diesem Campus über 3 Glasfaseranschlüsse bei den Anbietern Cogent Communications und Level 3.

Das Unternehmen hat eine weitere Glasfaserleitung gemietet, deren Bandbreite und Nutzung unbeschränkt ist, jedoch zu keinem Netzwerkbetreiber gehört. Sie verbindet die Systeme auf dem Campus von e-shelter zusätzlich mit dem Rechenzentrum von ancotel. Dort ist die Anbindung an einen Pool weiterer Netzanbieter gegeben. Durch diese Aufteilung ist die Internetanbindung der ADACOR Hosting GmbH auch bei Ausfall einer Leitung oder eines Providers gesichert.

Die Systeme der ADACOR Hosting GmbH sind in einem Mesh-Netzwerk miteinander verbunden. Diese Art von Netzwerken leitet beim Ausfall eines Netzwerkteilnehmers die Kommunikation über einen Alternativweg. Die Berechnung der Ausweichroute und die Umstellung auf die daraus resultierende Netzwerktopologie benötigt nur wenige Millisekunden. Neben den extrem kurzen Wiederherstellungszeiten sind die hervorragende Lastverteilung und die geringen Netzwerkkosten berechtigte Gründe für die Wahl dieser Topologie.

Ihre Daten sind bestens aufgehoben

Verschiedene Maßnahmen zum Schutz von Hardware, Netzwerk und Applikationen wurden in diesem Whitepaper bereits vorgestellt. Dieser Abschnitt beschreibt, wie die Verwaltung der Daten im laufenden Betrieb erfolgt. Zum Thema Datensicherung lesen Sie den Abschnitt „Im Fall des Falles: Backupstrategien der ADACOR Hosting GmbH“.

Große, stetig wachsende Mengen von Daten und ihre Hochverfügbarkeit fordern flexible Lösungen. Abhängig von den jeweiligen Anforderungen eines Projekts kommen unterschiedliche Konzepte zur Datenverwaltung zum Einsatz. Die ADACOR Hosting GmbH setzt dafür die folgenden ein:

- SAN und
- HDFS

Gut bekannt und weit verbreitet ist das Storage Area Network (SAN). Im SAN werden mehrere Platten oder -systeme (Storage Arrays) zu einer virtuellen Platte vereint. Diese virtuelle Platte wiederum wird in verschiedene Partitionen unterteilt. Die einzelnen Partitionen verhalten sich wie separate Festplatten und können als solche in die jeweiligen Systeme eingebunden werden. Dieses Konzept ermöglicht komfortables Erweitern oder Umstrukturieren des bestehenden Plattenlayouts. Wartungsfenster für solche Änderungen entfallen, sodass die Produktion während dieser Änderungen ununterbrochen weiterläuft.

Das SAN wird in Bereichen eingesetzt, die hochverfügbare Systeme erfordern, zum Beispiel in Banken und Telekommunikationsunternehmen. Die Vorteile des SAN sind die leichte Skalierbarkeit im laufenden Betrieb, der hohe Datendurchsatz und der effizient genutzte Speicherplatz.

Deutlich weniger verbreitet als das SAN ist das Hadoop Distributed File System (HDFS). HDFS ist Bestandteil des Apache Hadoop Projektes. Dieses Open-Source-Projekt wurde für zuverlässige und skalierbare Anwendungen auf verteilten Systemen entwickelt.

Die grundlegenden Funktionsprinzipien des HDFS sind das Ablegen von Teilen einer Datei auf verschiedenen Platten und mehrfache Kopien (Repliken) der jeweiligen Dateiteile auf wiederum unterschiedlichen Platten. Datenverlust durch Plattenausfälle werden auf diese Weise minimiert.

Das HDFS arbeitet mit unterschiedlichen Servern: sogenannten DataNodes und NameNodes. Auf den DataNodes liegen die Dateisegmente; die NameNodes sichern Namen und Speicherorte der Dateisegmente. Das ermöglicht einen sehr schnellen Zugriff besonders auf große Dateien, zum Beispiel Videos.

Die Ausfallsicherheit ist einerseits durch die Repliken der Dateisegmente auf den DataNodes gegeben, andererseits durch den Verbund (Cluster) der NameNodes. Dieser Cluster funktioniert nach dem Failover-Prinzip: Ein NameNode ist dabei aktiv; fällt dieser aus, übernimmt ein anderer NameNode sofort seine Funktion.

Auch das HDFS kann im laufenden Betrieb leicht erweitert oder umstrukturiert werden – neben der hohen Zuverlässigkeit und dem schnellen Dateizugriff ist das ein dritter Vorzug dieses Konzepts.

Open-Source-Software – die clevere Wahl

Bei Softwarelösungen setzt das Unternehmen auf Open-Source-Produkte. Das scheint auf den ersten Blick ein unkonventionelles und vielleicht sogar belächeltes Modell zu sein. Doch bei genauerem Hinsehen erweist sich gerade Open-Source-Software als kluge und vorausschauende Lösung: Zeitersparnis durch den Wegfall von Lieferzeiten und finanzielle Vorteile durch den Wegfall von Lizenzgebühren. Außerdem kann durch den frei verfügbaren Quelltext ein möglicher Fehler in der Software von einem Mitarbeiter repariert, der jeweilige Patch getestet und ohne Verzögerung implementiert werden.

Ein Beispiel: Wird ein Fehler in einer Software proprietärer Herkunft festgestellt, vergeht zum Teil viel Zeit, um zunächst die Entwicklungsabteilung des Herstellers zu erreichen,

dann den Fehler zu evaluieren, einen entsprechenden Patch zu produzieren, diesen zu testen und schließlich freizugeben. Das kann Monate und sogar Jahre dauern. So viel Zeit haben die Kunden jedoch selten.

Hier kann die Open-Source-Software ihre Stärken voll ausspielen. Oft sind die Programmierer der Software leicht und direkt zu erreichen. Der direkte Kontakt ermöglicht eine schnelle Behebung des Fehlers. Durch die frei verfügbaren Quelltexte kann die jeweilige Software auch durch einen Programmierer im eigenen Unternehmen verändert werden. Das kann das Implementieren von zusätzlichen Abfragen oder Abbruchmeldungen sein. Es ist auch möglich, das Verbose-Level zu erhöhen, um der Software mehr Informationen während des Fehlers zu entlocken.

Es kann sogar so weit gehen, dass jeder Systemcall – also jeder einzelne, noch so kleine Schritt – vom System angezeigt oder in eine Protokolldatei geschrieben wird. Dadurch sind Fehler schnell erkannt und behoben. Die jeweiligen Lösungen (Patches) wiederum werden im Internet frei verfügbar zum Download abgelegt oder auch in das nächste Release aufgenommen. Das Warten auf eine Problemlösung wird auf ein Minimum reduziert.

Für die Kunden hat die Open-Source-Software gegenüber proprietären Lösungen ganz entscheidende Vorteile: Dienstleister wie die ADACOR Hosting GmbH können extrem flexibel agieren und individuelle, stabil funktionierende und kostengünstige Kundenlösungen anbieten. Zusätzlicher finanzieller Aufwand, zum Beispiel für Lizenzen, entfällt ebenfalls.

■ Seite 6

Firewalls & Co: Ihre Daten und Applikationen in sicheren Händen

Ein sehr wichtiges Kriterium für die Sicherheit von Applikationen und Daten sind Firewalls. Wie Hardware, Netzwerkanbindung oder Backup sind auch die Firewalls der ADACOR Hosting GmbH mehrfach redundant (als Cluster) ausgelegt. Fällt im Clusterverbund ein System (Node) aus, übernimmt automatisch eine andere Node innerhalb dieses Verbunds die Aufgaben der ausgefallenen Komponente.

Verschiedene Firewalls schützen die Systeme, Anwendungen und Daten vor unerlaubten Zugriffen. Das Zentrum besteht aus einem Firewall-Cluster, der für jeden Kunden einen eigenen Bereich für das jeweilige Regelwerk auf derselben Firewall reserviert (Firewall-Sharing). Es kann vorkommen, dass dies von Kundenseite nicht erwünscht oder gestattet ist. In diesem Fall stellt die ADACOR Hosting GmbH separate Firewall-Cluster für diese Kunden zur Verfügung.

Das Unternehmen verwendet das Software-Paket Network Security von Astaro Security Gateway. Das Besondere bei Astaro ist das Vereinen von Netzzugangskontrolle, VPN-Sicherheit und Angriffsabwehr. Häufig werden solche Komponenten nur einzeln angeboten, was dazu führt, dass Softwareprodukte unterschiedlicher Hersteller im Einsatz sind, die nicht immer fehlerfrei miteinander kooperieren. Eine solche Lösung verursacht zusätzlich einen hohen Implementierungsaufwand.

Astaro Security Gateway stellt verschiedene Software-Pakete für die Netzsicherheit zur Verfügung, deren einzelne Komponenten optimal aufeinander abgestimmt sind. So sind Daten und Applikationen optimal vor Angriffen geschützt.

Nagios, die Argusaugen für Ihre Hardware und Applikationen

Die Kundensysteme werden permanent überwacht. Für das Monitoring setzt die ADACOR Hosting GmbH die Open-Source-Software Nagios ein. Nagios hat sich in der Praxis zahlreicher Unternehmen als zuverlässiger Partner bewährt.

In den Nagios-Konfigurationsdateien werden die gewünschten Dienste und Systeme für die Überwachung eingetragen. Ebenfalls festgelegt werden Ansprechpartner für einen eventuellen Fehlerfall. Es ist möglich, mehrere Dienste und mehrere Systeme in der Überwachung zusammenzufassen. Das kann sinnvoll sein, wenn Komponenten voneinander abhängen oder zusammenarbeiten, zum Beispiel ein Cluster, bei dem mehrere Systeme in einem Verbund zusammengeschlossen sind.

Weiterhin werden verschiedene Schwellwerte in den Konfigurationsdateien festgelegt, bei deren Überschreitung ein Alarm ausgelöst werden soll. Die Schwellwerte sind wiederum gekoppelt mit der Art der Benachrichtigung und den jeweiligen Kontakten. Es kann beispielsweise eine E-Mail und eine SMS verschickt oder eine Nachricht in einen Instant Messenger des gewünschten Kontakts, zum Beispiel des Systemadministrators, geschrieben werden.

Es ist auch möglich, bei Überschreiten eines Schwellwertes ein vorher festgelegtes Skript auszuführen. Wenn beispielsweise ein bestimmtes Verzeichnis mit Protokoll-Dateien an die Grenze des dafür vorgesehenen Plattenplatzes kommt, können die ältesten Dateien komprimiert und an eine andere Stelle verschoben werden. Ein anderes Beispiel für eine automatisierte Problemlösung wäre das Nachstarten eines fehlenden Prozesses, zum Beispiel von einer Datenbank.

Nagios enthält ebenfalls ein Eskalationsmanagement. Sollte eine Störung für einen festgelegten Zeitraum nicht behoben sein, ist die nächste Eskalationsstufe erreicht. Im Eskalationsmanagement wird der Ablauf für diesen Fall festgelegt, zum Beispiel ob eine Person über einen vorher bestimmten Weg informiert wird oder ob eine andere, vorher festgelegte Aktion erfolgt.

Sämtliche Alarme werden protokolliert. So werden die Systeme über einen langen Zeitraum systematisch beobachtet, was wiederum Aufschluss gibt über notwendige Erweiterungen, falls Systeme permanent stark ausgelastet sind oder Dateisysteme häufig an die Kapazitätsgrenze kommen. Zusätzlich gibt die langfristige Überwachung Hinweise auch zur Optimierung der Überwachung selbst. Das können beispielsweise das Unterdrücken von unkritischen Systemmeldungen sein, die lediglich der Information dienen.

Nagios ist modular aufgebaut und kann durch selbst programmierte Module leicht erweitert werden. Mit Nagios ist dadurch die Überwachung von nicht standardisierten Komponenten möglich.

Nagios hat zwei verschiedene Möglichkeiten, um sich selbst vor Ausfällen zu schützen, falls zum Beispiel ein Hardwarefehler des jeweiligen Systems auftritt: das verteilte Monitoring und das redundante Monitoring. Das Prinzip des verteilten Monitorings sind mehrere, dezentrale Nagios-Instanzen, die ihre Ergebnisse an einen zentralen Nagios-Server senden. Der zentrale Nagios-Server verarbeitet die eingegangenen Informationen.

Das redundante Monitoring funktioniert wie bei einem Cluster: Zwei Nagios-Instanzen werden im Modus aktiv/passiv (Master/Slave) miteinander gekoppelt. Beide Instanzen prüfen in regelmäßigen Abständen, ob die jeweils andere Instanz erreichbar ist. Würde eine Instanz ausfallen, wäre die Absicherung der Überwachung durch die Redundanz nicht mehr gegeben.

Die beiden Nagios-Instanzen laufen auf je einem Server, jedoch erfolgt die Benachrichtigung bei Alarm nur vom aktiven Nagios-Server. Werden die Nagios-Serverdienste der aktiven Instanz gestoppt oder fällt das System aus einem anderen Grund aus, wechselt die passive Nagios-Instanz umgehend in den aktiven Modus und übernimmt sofort die entsprechende Benachrichtigung.

Im Fall des Falles: Backupstrategien der ADACOR Hosting GmbH

Neben einer sicheren Unterbringung der Hardware, der stetigen Verfügbarkeit – auch der Netzwerkanbindung – und dem Schutz vor unerlaubten Zugriffen ist die Datensicherung ein zentrales Thema für hochverfügbare Applikationen. Die ADACOR Hosting GmbH verfügt über eine ausgeklügelte Backupstrategie, zu der die Sicherung auf räumlich getrennte Storage Arrays und der Einsatz einer zuverlässigen Software gehören.

Auch im Backup-Bereich setzt das Unternehmen auf Open-Source-Software. In diesem Fall auf Bacula. Die Open-Source-Software Bacula ist flexibel und zuverlässig und steht ihren kommerziellen Kollegen wie zum Beispiel dem Legato Networker in nichts nach. Darüber hinaus entfallen die Kosten für etwaige Lizenzgebühren, was sich wiederum günstig auf die Preisgestaltung der Angebote auswirkt.

Die Datensicherung des jeweiligen Projekts wird mit den Kunden bezüglich Häufigkeit und Art besprochen, zum Beispiel nur Voll-Backups oder inkrementelle und vollständige Datensicherung im Wechsel. Die Sicherungen werden mehrfach redundant vorgehalten.

Zusammenfassung

Sämtliche Strukturen, bei denen ein Ausfall möglich ist, sind redundant ausgelegt, zum Beispiel Stromversorgung, Netzzugänge, Firewalls, Datensicherung und Überwachung. So sind Systeme, Applikationen und Daten optimal geschützt. Da das Unternehmen Open-Source-Software einsetzt, können Projekte schnell und preisgünstig umgesetzt werden. Lange Lieferzeiten und Lizenzgebühren entfallen. Durch ihre Arbeitsweise und die Infrastruktur ist die ADACOR Hosting GmbH auch bei Erweiterungen bestehender Projekte sehr flexibel.

Der Leitsatz der ADACOR Hosting GmbH – Sicherheit und Flexibilität zu einem fairen Preis – macht das Unternehmen zu einem zuverlässigen Partner für anspruchsvolle IT-Projekte.

Noch Fragen? Kontaktieren Sie uns!

Adacor Hosting GmbH

Verwaltung (Rechnungsanschrift)

Emmastrasse 70a
D-45130 Essen

NOC (Network Operation Center)

Kaiserleistraße 51
D-63067 Offenbach am Main

Telefon +49 (0)69 905089 0
Telefax +49 (0)69 905089 29
Web <http://www.adacor.com>
Email info@adacor.com