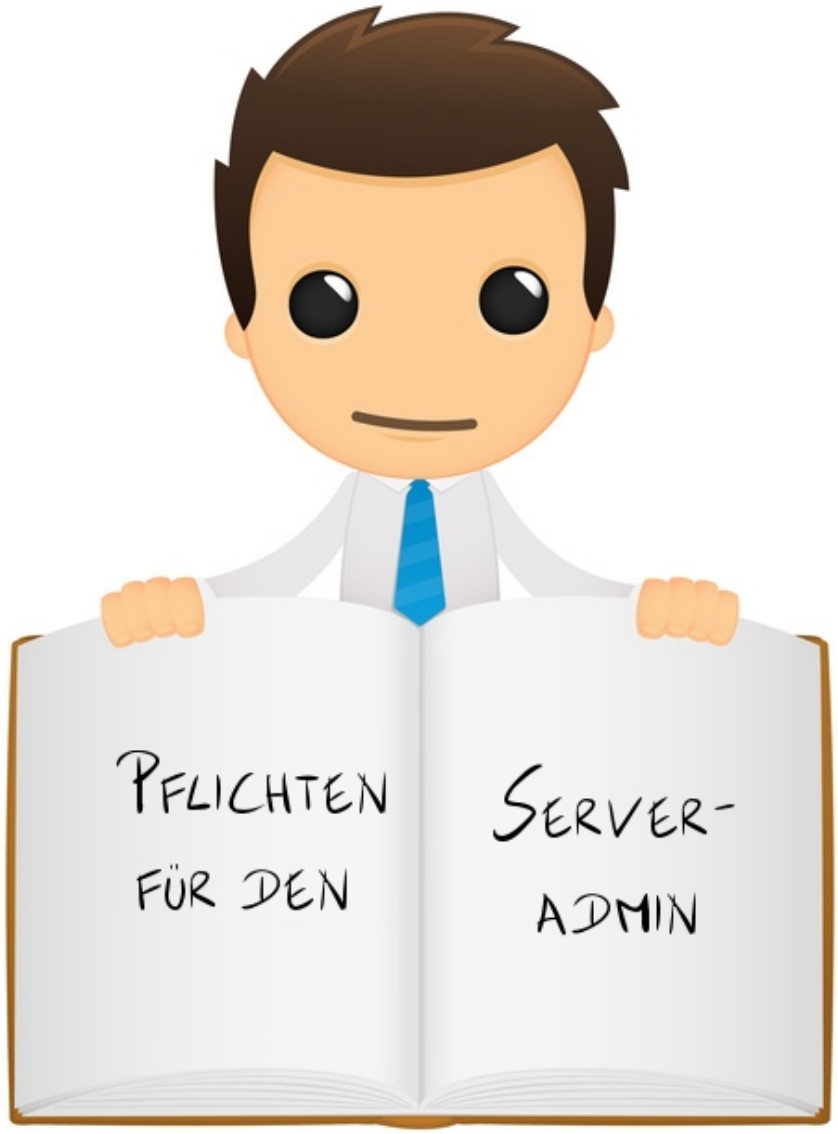
Pflichten
für den
Server-
admin

Inhaltsverzeichnis

Vorwort

Seit über 15 Jahren hostet die HKN GmbH Server für Kunden. Reichlich Zeit, um Dinge richtig zu machen und um aus Fehlern zu lernen.

Im Laufe der Zeit haben wir den ein oder anderen Fehler gemacht und so gelernt, welche Aufgaben ein Serveradministrator auf keinen Fall vernachlässigen darf. Erfahrungen, die jeder Serveradministrator sammelt.

Leider mussten wir in den letzten Jahren aber auch mit ansehen, dass immer mehr Server keine richtigen Administratoren haben. Oft passiert es, dass der einzige technisch interessierte Mitarbeiter auf einmal zum Serveradmin wird oder der, der nicht schnell genug NEIN sagen konnte. Wenn Du in dieser Situation bist – mach Dir keine Sorgen.

In diesem Workshop vermitteln wir Dir die wichtigsten Pflichten eines Serveradministrators.

Pflichten für den Serveradministrator

Für den Serveradministrator gibt es acht Punkte, die relevant sind. Anhand dieser acht Punkte solltest Du einmal jeden Server in Deiner Verantwortung abklopfen. Sollte Dir beim ersten lesen nicht direkt klar sein, was der Punkt soll und wie Du ihn abdecken kannst – keine Panik. Wir erklären es Dir in diesem Workshop.

Hier also die acht Punkte:

1. **Backup:** Stelle sicher, dass Du immer ein aktuelles Backup hast.
2. **Patchen:** Stelle sicher, dass Du regelmäßig die aktuellen Sicherheitsupdates auf Deinem Server einspielst.
3. **Monitoring:** Sei immer über den Status Deines Servers informiert.
4. **Snapshots:** Lege Dir vor Konfigurationsarbeiten einen Snapshot Deines vServers an.
5. **Plan B:** Habe einen Plan B. Die meisten Provider bieten z. B. Remote-Zugänge für Kundenser-

ver an. Halte Dich Informiert, ob das bei Deinem Server auch möglich ist.

6. **Helfer in der Not:** Stell sicher, dass Du die Servicenummern und E-Mail-Adressen von Deinem Provider kennst
7. **Erreichbarkeit:** Sei erreichbar! Sorge dafür, dass Dein Provider immer Deine aktuelle (vom Server unabhängige) E-Mail-Adresse und Telefonnummer hat.
8. **Dokumentiere:** Stelle sicher, dass auch in Deiner Abwesenheit jemand den Server administrieren kann.

Backup

Das Allerwichtigste, wenn Du die Verantwortung für einen Server hast, ist, dass Du regelmäßige Backups der Daten anlegst. Darüber hinaus kann es sinnvoll sein, verschiedene Backups zu haben, so das du auf die Daten verschiedener Zeitpunkte zurückgreifen kannst.

Das Backup erfüllt für Dich zwei wichtige Punkte. Erstens kannst Du nach einem Hardwareausfall mithilfe des Backups Deinen Server schnell wiederherstellen, zweitens kannst Du Daten, die gelöscht wurden wiederherstellen.

Damit ein Backup Sinn macht, darf es natürlich nicht auf Deinem Server liegen.

Bevor Du mit dem Backup loslegst, solltest Du Dir folgende Fragen stellen und beantworten:

1. Wo speichere ich das Backup?
2. Welchen Zeitraum muss ich sichern?
3. Wie spiele ich das Backup wieder zurück?

Wichtig: RAID ist kein Backup!
Bei einem RAID-System bist Du zwar vor einem Defekt einer Festplatte geschützt. Versagt der Server aber ganz oder werden Daten gelöscht, hilft Dir ein RAID nicht weiter.

Solltest Du die Fragen nicht beantworten können, ist das kein Grund beunruhigt zu sein. Frag Deinen Provider ob er Dir eine Backuplösung anbieten kann und stell ihm einfach diese Fragen. Sollte er keine Lösungen für Dich haben oder diese nicht zu Deinem Budget passen, frag Google. Es gibt viele Dienstleister die gerne das Backup für Dich übernehmen. Mit diesen zusammen oder alleine erstellst Du dann einen Backup-Plan. In diesem Plan wird

festgehalten, welche Daten über welchen Zeitraum gesichert werden. Mehr Informationen zum „Disaster Recovery“ findest Du im Kapitel „Plan B/Helfer in der Not“.

Patchen

Ein eigener Server ist eine feine Sache. Man muss seine Ressourcen nicht teilen und als Admin kann man selber entscheiden welche Software auf dem Server installiert ist. Die Kehrseite der Medaille ist natürlich, dass man als Admin selber darauf achten muss, dass die installierte Software aktuell bleibt.

Warum aktuelle Software wichtig ist

Aktuelle Software ist DER wichtigste Aspekt um die Sicherheit seines Servers zu gewährleisten! Potentielle Angreifer suchen in der Regel zuerst Schwachstellen in der Software, die auf dem Server installiert ist. Schwachstellen die durch Softwareupdates geschlossen werden. Erfährt der Hersteller einer Software, dass es zum Beispiel eine Sicherheitslücke in seinem System gibt, schreibt er ein Programm, das die Sicherheitslücke in seiner Software schließt. Einen sogenannten “Patch”.

Als Benutzer von Software solltest Du also immer darauf achten, alle aktuellen Patches auf Deinem System zeitnah einzuspielen.

Nicht den Überblick verlieren

Um also Deinen Server softwareseitig sicher zu halten, musst Du regelmäßig kontrollieren, ob es Patches für die eingesetzte Software gibt. Dabei kann man zwischen zwei Arten von Software unterscheiden – dem Betriebssystem inklusive der Standardsoftware (zum Beispiel Ubuntu Linux mit Apache, PHP und MySQL) und den installierten Applikationen (zum Beispiel das Plesk Servermanagement-Panel oder der WordPress-Blogsoftware).

Für beide Gruppen musst Du als Admin sicherstellen, dass aktuelle Patches zeitnah eingespielt werden. Dafür musst Du natürlich erst einmal wissen, dass es einen Patch gibt.

Applikationen patchen

Bei den Applikationen gestaltet sich das sehr unterschiedlich. Allerdings machen viele Softwarehersteller einem mittlerweile das Leben einfach. So zeigen WordPress und Plesk zum Beispiel dem Admin direkt im Dashboard an, wenn Updates verfügbar sind. Diese kannst Du dann in der Regel mit einem Klick installieren.

Wirst Du von der Software nicht automatisch mit solchen Informationen versorgt, bleibt nur, die Newsletter des Herstellers zu abonnieren oder häufig dessen Webseite zu frequentieren.

Die Art und Weise wie der Softwarehersteller seinen Kunden mit Patches versorgt, sollte durchaus ein Entscheidungskriterium bei der Wahl der Software sein.

Patchen des Betriebssystems

Jedes Betriebssystem wird anders gepatcht. Eine kurze Übersicht wie man Linux-Systeme patcht haben wir im Juni in unserem Blog veröffentlicht. Wenn Du keinen Linuxserver hast und nicht weißt, wie Du Sicherheitsupdates einspielst, solltest Du einfach Google fragen.

Der bessere Ansatz ist es aber wohl, die Sicherheitsupdates von einem Experten erledigen zu lassen. Auch hier sollte Dein Provider Dein erster Ansprechpartner sein. Frag ihn einfach, ob er einen Patchservice für Deinen Server anbietet und wie er diesen realisiert.

Tipps zum Patchen und anderen sicherheitsrelevanten Punkten findest du in unserem Blog unter dem Tag *Security*: http://blog.hkn.de/tag/security

Monitoring

Wenn Du Onlineshop-Betreiber bist, eine eigene Webseite hast oder aus anderen Gründen einen eigenen Server betreibst, solltest Du immer wissen, ob dieser auch läuft. Ausfälle können nicht nur zu ärgerlichen und vermeidbaren Umsatzeinbußen führen, es macht auf Besucher zusätzlich einen sehr schlechten Eindruck, wenn eine Seite längere Zeit nicht zu erreichen ist.

Leider ist es für einen Administrator fast unmöglich, die Erreichbarkeit seines Servers rund um die Uhr zu kontrollieren. Um trotzdem jederzeit über Statusänderungen seines Servers informiert zu sein, gibt es Servermonitoring-Programme. Die schauen sozusagen für den Admin nach, ob al-

les in Ordnung ist und informieren ihn umgehend bei Problemen und Ausfällen.

Damit das funktioniert, darf der Monitoringdienst natürlich nicht auf dem gleichen Server laufen, der überwacht werden soll. Also benötigt man einen zweiten Server oder einen Dienstleister. Auf jeden Fall sollte man immer die Verfügbarkeit seines Servers und die Verfügbarkeit der wichtigsten Dienste überwachen. Bei einem Webserver sind das in der Regel der Apache-Server, der MySQL-Server, FTP- und E-Mail-Server. Bei einem Ausfall wird der Admin sofort per SMS und E-Mail informiert um den Fehler zeitnah zu beheben.

Ein wirklich umfassendes Server-Monitoring sollte so gestaltet sein, dass es nicht nur die unterschiedlichen Ports kontrolliert. Es sollte auch Prozesse wie CPU-Auslastung, Temperatur oder Festplattenkapazität im Blick behalten oder gleichzeitige MySQL-Abfragen erfassen. Kritische Situationen werden so früher erkannt und zum Teil noch vor dem Fehlerfall behoben. Wichtig ist, dass trotz RAID-System die Festplatten einzeln monitort werden, um den Ausfall einer Platte zu erkennen.

Links:
Mehr Informationen zu Nagios und Opsview findest du auf den Herstellerseiten im Web:

- http://www.nagios.org/
- http://www.opsview.com/

Das Monitoring kannst Du natürlich, wie auch das Patchen und das Backup, Dienstleistern überlassen. Alternativ kann man aber auch einen eigenen Server dafür aufsetzen und spezielle Servermonitoringsoftware installieren. Wir haben sehr gute Erfahrung mit Nagios gemacht. Nagios ist eine Open Source-Software zur Überwachung von Netzwerken, Hosts und speziellen Diensten und erfüllt nahezu alle Ansprüche an professionelles Servermanagement. Mit Opsview gibt es außerdem ein professionelles Frontend für eine grafische Verwaltung des Nagios-Servers.

Snapshots beim vServer

Hast Du das Glück, dass Du einen vServer verwaltest, solltest Du Dich informieren, ob Du dafür auch eigene Snapshots vornehmen kannst. Viele Provider bieten diese Möglichkeit an.

Ein Snapshot - was ist das überhaupt? Wie der Name schon vermuten lässt, handelt es sich dabei um eine Momentaufnahme Deines vServers. Durch einen Snaphot ist es möglich, den Stand des vServers an einem bestimmten Punkt quasi 'einzufrieren' und alle Dateien und Einstellungen zu

sichern. Eine solche Momentaufnahme des eigenen vServers zu speichern ist vor allem dann wichtig, bevor Du Deinen vServer wartest, bestimmte Einstellungen oder Installationen testest oder neue Applikationen aufspielst. Hat man eine solche Sicherheitskopie seines Systems vor diesem Zeitpunkt, braucht man sich über mögliche irreparable oder nur schwer rückgängig zu machende Aktionen keine Sorgen zu machen. Die Einstellungen können somit auf den Stand des Snapshots zurückgesetzt werden.

Plan B/Helfer in der Not

Jetzt tritt der schlimmste Fall ein. Du bekommst Anrufe von Deinen Usern und auch das Monitoring sagt Dir, dass etwas mit dem Server nicht stimmt. Jetzt heißt es Ruhe bewahren und analysieren.

Zuerst musst Du in Erfahrung bringen, was nicht funktioniert. Betrifft die Störung einen Dienst wie zu Beispiel Mailempfang, eine Applikation (zum Beispiel das Typo3 Web-Contentmanagement-System einer Webseite) oder ist der Server komplett offline?

Die Antwort darauf sollte einem sein Monitoring geben.

Ist nur eine Applikation betroffen, kann man sich an den Hersteller wenden oder vielleicht einen aktuellen Snapshot aktivieren.

Ist nur ein Dienst nicht zu erreichen, kann man erst einmal versuchen diesen erneut zu starten. Entweder indem man selbst per SSH auf den Server zugreift oder mit Hilfe einer Software. Das Plesk Panel zur Serververwaltung bietet zum Beispiel die Möglichkeit, Dienste neu zu starten, sogar mobil.

Das **Plesk Panel** ist eine Software um einen Webserver zu verwalten und vor allem für unerfahrene Administratoren empfehlenswert. Mehr über das mobile Servermanagement mit Plesk findest Du im HKN Blog. **http://blog.hkn.de/?p=1354**

Sollte der Zugriff via ssh nicht möglich sein, weil ausgerechnet der ssh-Dienst versagt hat oder weil das gesamte System nicht erreichbar ist, hast du noch zwei Chancen:

Bietet Dir Dein Provider Remotezugriff über eine Konsole? Gerade bei vServern bekommt man oft den Zugriff über eine sogenannte vServer-Konsole gestattet. Remote-Konsolen ermöglichen einem den Zugriff auf seinen Server, als würde wenn man mit Tastatur und Maus direkt davor sit-

zen. Außerdem bieten sie die Möglichkeit, den Server neu zu starten.

Gibt es keinen Remotezugriff, kann man vielleicht auf den Stromport zugreifen. Den Strom erst aus und dann ein paar Sekunden später wieder anzustellen, kann dafür sorgen, dass der Server wieder sauber hochfährt. Das ist aber eine Holzhammermethode, die Du nur anwenden solltest, wenn alle anderen Möglichkeiten ausgeschöpft sind. Besser wendest Du Dich an Deinen Notfall-support

Helfer in der Not!

Fast jeder Provider hat einen Notfallsupport. Dieser steht Dir bei Tag und auch bei Nacht zur Verfügung. Hast Du Deinen Provider gut gewählt, kannst Du direkt Techniker anrufen, die Dir bei deinem Problem helfen. Pass nur mit den Preisen auf. Der Notfallsupport ist in der Nacht in der Regel kostenpflichtig. Kostet dich der Ausfall nahezu nichts, der Support aber würde teuer werden, solltest Du vielleicht bis zum nächsten Morgen warten. Wichtig ist, dass Du die Nummer vom Support hast, Deine Kundennummer kennst und die Bezeichnung sowie die IP-Adresse des betroffenen Servers kennst. Am einfachsten machst Du es dem Support, wenn Du vor einem Anruf das Problem schon einmal per E-Mail möglichst genau beschreibst. Stell auch sicher, dass Du immer einen Vertreter hast, der weiß, wie er den Notfallsupport deines Providers erreicht und der dort auch Aufträge geben darf.

Kann der Server nicht wieder gestartet werden weil er tot ist, hilft nur der

Plan B

Jetzt zeigt sich, ob Du Dir beim Einrichten des Backup genug Gedanken gemacht hast und ob Dein „Disaster Recovery“ funktioniert. Zuerst musst Du Dir von Deinem Provider schnell ein Ersatzsystem zur Verfügung stellen lassen. Nutzt Du einen vServer geht das gewöhnlich sehr schnell. Bei dedizierter Hardware kann das länger dauern. Kann Dein Provider Dir nicht kurzfristig einen Ersatz-Hardwareserver stellen, solltest Du vielleicht einen Zwischenschritt über einen vServer als Interimssystem gehen.

Der Begriff **Disaster Recovery** (im Deutschen auch Katastrophen-Recovery oder Notfallwiederherstellung genannt) bezeichnet Maßnahmen, die nach einem Unglücksfall in der Informationstechnik eingeleitet werden. Dazu zählt sowohl die Datenwiederherstellung als auch das Ersetzen nicht mehr benutzbarer Infrastruktur, Hardware und Organisation.

Quelle:
http://de.wikipedia.org/wiki/Disaster_Recovery

Steht das neue System, musst Du Deine Backups darauf zurück spielen. Wie lange das dauert liegt

natürlich an der Datenmenge und dem „Ort“ wo Dein Backup gespeichert ist. Am zügigsten wird das Zurückspielen funktionieren, wenn die Daten direkt beim Provider liegen. Liegen die Daten in einem anderen Rechenzentrum, wird das etwas länger dauern. Hast Du das Backup bei Dir zu Hause und musst es über Deine ADSL-Leitung hochladen, plane viel Zeit dafür ein.

Mein Tipp: Teste Dein „Disaster Recovery“ regelmäßig ohne Not oder überlasse das einem Dienstleister (zum Beispiel Deinem Provider). Dann kannst Du ruhiger schlafen.

Erreichbarkeit

Stelle sicher, dass Du oder eine weitere Person, die autorisiert ist, Deinen Server zu administieren, immer erreichbar sind. Sorge deshalb dafür, dass Du immer Deine aktuelle Telefonnummer und/oder E-Mail-Adresse bei Deinem Provider hinterlegt hast. Wichtig ist dabei, dass die E-Mail-Adresse NICHT auf dem eigenen Mailserver liegen darf, denn wenn dieser ausfällt, kann Dich auch der Support nicht erreichen. Wenn Du im Urlaub bist solltest Du die E-Mails automatisch an Deinen Vertreter weiterleiten. Noch besser ist ein E-Mail-Verteiler. In diesem Fall solltest Du aber vorher festlegen, wer sich wann um die Meldungen kümmert. Das gilt übrigens nicht nur für E-Mails von deinem Provider, sondern auch für die E-Mails vom Monitoring.

Dokumentiere

Gibt es mehrere Administratoren auf einen Server, ist es hilfreich Einzelschritte zu dokumentieren und diese allen Bearbeitern zugänglich zu machen. So haben alle stets einen Überblick über den aktuellen Stand. Es ist sehr es wichtig, dass transparent gehalten wird, wann und von wem welche Änderungen vorgenommen wurden. So lässt sich im Schadensfall auch nachvollziehen, wo der Fehler liegen könnte.

Bist Du überwiegend allein für die Administration Deines Servers zuständig, kannst Du so sicherstellen, dass Dein Server auch im Fall Deiner Abwesenheit (z. B. Urlaub) administriert werden kann. Alle Änderungen sollten dabei in einem so genannten Änderungsprotokoll (Changelog) festgehalten werden. Für ein solches Änderungsprotokoll reicht in der Regel eine einfache Textdatei.

Fazit

Bei der Administration Deines Servers ist es nicht nur ein Weg, der ans Ziel führt, sondern es gibt immer mehrere. Spätestens jetzt solltest Du wissen, was Du tun musst, um die Sicherheit Deines Servers zu gewährleisten, bzw. wie und wo Du Dir Hilfe holen kannst.

Sichergehen, dass Du alles berücksichtigt hast, kannst Du mit unserer Checkliste. Kannst Du hinter bei jedem Punkt einen Haken setzen, kann eigentlich nichts mehr schief gehen.

Checkliste

- ☐ Es werden regelmäßige Backups erstellt
- ☐ Die Backups liegen auf einem separaten Backup-Server.
- ☐ Ich habe einen Backup-Plan.
- ☐ Es können einzelne gelöschte Dateien aus dem Backup zurück gespielt werden.
- ☐ Ich habe sichergestellt, dass mein Betriebssystem regelmäßig gepatcht wird.
- ☐ Ich habe sichergestellt, dass meine Applikationen regelmäßig aktualisiert werden.
- ☐ Ich bin über Statusänderungen meines Servers jederzeit informiert.
- ☐ Ich verfüge ich über Servermonitoring-Software (z. B. Nagios oder Opsview).
- ☐ Mein Monitoringdienst läuft auf einem separaten Server.
- ☐ Ich monitore die Festplatten meines RAID-System separat.
- ☐ Ich erstelle selbst Snapshots von meinem vServer, oder mein Provider tut dies für mich.
- ☐ Ich habe einen Plan B für den Notfall.
- ☐ Ich teste mein Desaster-Recovery regelmäßig.
- ☐ Ich kenne die Nummer des Notfallsupports meines Providers.
- ☐ Ich weiß, wie ich mir im Notfall selbst helfen kann (z. B. Plesk Panel-Servermanagement, vServer-Konsole, etc.).
- ☐ Jemand kann in meiner Abwesenheit dem Support Aufträge erteilen.
- ☐ Ich habe bei meinem Provider eine aktuelle Telefonnummer/E-Mail-Adresse hinterlegt und bin stets erreichbar.
- ☐ Ich dokumentiere alle Änderungen an meinem Server, damit dieser auch während meiner Abwesenheit administriert werden kann.

Die Autoren übereinander

Marco Nöchel

Wenn Marco nicht gerade Workshops wie diesen hier erdenkt, hat er auch noch einen richtigen Job. Als Leiter im Marketing bloggt er u.a. für die HKN GmbH, verleiht dem Social Media-Auftritt der Firma ein Gesicht und verschönert kontinuierlich deren Webseiten. Mit diesem E-Book-Projekt hat er sich einen lang gehegten Wunsch erfüllt, indem er unter die Autoren ging. Mit der neuen deutschen Rechtschreibung steht er auf Kriegsfuß.

Andrea Hanninger

2012 haben wir die Andrea bei der HKN GmbH eingestellt. Seitdem haben wir nicht nur die erste „vollstudierte“ Akademikerin in unserem Team, sondern auch einen Menschen der uns neue Ideen und Sichtweisen auf die IT-Welt gibt. Genau das richtige für Leute die seit 15 Jahren auf dem gleichen Gebiet tätig sind. Darüber hinaus hat Andrea eine unheimliche Zuneigung für die neue deutsche Rechtschreibung.

Profile im Netz

Willst Du über unsere Arbeit auf dem Laufenden bleiben, findest Du viele Seiten im Web, an denen wir mitwirken. Wir freuen uns über jeden neuen Freund, Follower, RSS-Feed-Abonnierer oder Einkreiser ;)

Unser Blog:	http://blog.hkn.de
Facebook:	http://facebook.hkn.de
Twitter:	http://twitter.hkn.de
Google+:	http://google.hkn.de
Webseite:	http://www.hkn.de

Bildrechte