Link: https://www.computerwoche.de/a/sichere-systeme-unterstuetzen-hochverfuegbarkeit,1891059

Hackern keine Chance geben

Sichere Systeme unterstützen Hochverfügbarkeit

Datum: 25.03.2009
Autor(en): Johann Baumeister

Auf den ersten Blick haben Hochverfügbarkeit und Sicherheit wenig miteinander zu tun. Bei genauerem Hinsehen allerdings zeigen sich doch erhebliche Wechselwirkungen und Abhängigkeiten zwischen sicheren und hochverfügbaren Systemen.

Ausfallsicherheit ist die absolute Königsdisziplin in Rechenzentren.

Ausfallzeiten in Zahlen

Schon eine um 0,1 Prozent verringerte Verfügbarkeit bewirkt, dass Server über achteinhalb Stunden still stehen.

Hochverfügbarkeit (in %)	Ausfallzeit/Jahr
99,9	8,7 Stunden
99,99	52 Minuten
99,999	5 Minuten
99,9999	31 Sekunden

Hochverfügbare **Serversysteme**[1] werden häufig mit Clustern gleichgesetzt. Das ist, wenngleich vereinfacht, zumindest in der Vergangenheit durchaus zutreffend. Sicherheit wiederum assoziieren viele IT-Betreuer mit den **Funktionen einer Firewall**[2], eines **Virenscanner**[3] und ähnlichen Produkten. Einen direkten Bezug zwischen beiden Funktionsgruppen würde man eher nicht vermuten. Dennoch sind die Anhängigkeiten größer, als auf den ersten Blick ersichtlich. Wird beispielsweise ein Server durch einen **Virus**[4] lahmgelegt, so senkt das seine Verfügbarkeit. Dabei muss es sich nicht immer um einen vollständigen Ausfall handeln. Auch ein **Trojaner**[5], der einen gekaperten Email-Server nutzt, um über dessen Kanäle SPAM-Mails zu versenden, reduziert gleichzeitig die verfügbaren Ressourcen für seine Benutzer und damit die Verfügbarkeit für den ihm zugedachten Zweck. Was aber ist eigentlich Hochverfügbarkeit und wird sie gemessen? Meist geht man heute bei der **Hochverfügbarkeit**[6] von den Werten aus, die die beistehende Tabelle zeigt (siehe links).

Dabei entspricht der erste Wert der Hochverfügbarkeit eines Systems in Prozent von der gesamten Laufzeit. Der zweite Wert ist die dann maximal erlaubte Ausfallzeit, meist bezogen auf ein Jahr. Wenn also ein Server zweimal im Jahr für vier Stunden nicht verfügbar ist, wird ihm, bei linearer Betrachtung, eine Verfügbarkeit von circa 99,9 Prozent bescheinigt: 364 Tage * 24 Stunden = 8736 Stunden / Jahr; 8 Stunden sind somit circa ein zehntel Prozent, also verbleibt eine Verfügbarkeit von 99,9 Prozent.

Hochverfügbarkeit der Hardware als Grundlage

Dieses lineare Berechnungsmodell nimmt aber noch keine Rücksicht auf den tatsächlichen Bedarf durch die Benutzer. In betriebsarmen Zeiten, wie etwa nachts oder am Wochenende, wirken sich Ausfällen nur gering aus. Völlig anders dagegen verhält es sich zu den Spitzenzeiten. Ferner bezieht sich die Aussage der Hochverfügbarkeit immer auf die **Ausfallsicherheit**[7] der Serverhardware. Das muss sich aber nicht mit den Ergebnissen decken, die beim Anwender letztendlich spürbar werden, denn für ihn zählt nur die Verfügbarkeit seines Dienstes oder der Applikation. Sind diese aber, egal aufgrund welcher Ursachen, überlastet und liefern die Antworten nur verzögert, so reduziert dies ebenso die "Verfügbarkeit" des Dienstes für den Benutzer. Summiert man diese verzögerten Reaktionen ("Mikroausfälle") allerdings auf, so ergeben sich selbst bei nur 2,5 Minuten Verzögerung pro Tag bereits über neun Stunden für das Jahr.

Damit wird eine **hochverfügbare Serverlandschaft**[8] mit einer Ausfallsicherheit von beispielweise 99,9999 Prozent im Nu auf den Wert 99,9 Prozent gesenkt. Dies Beispiel zeigt aber auch, dass der reine Blick auf die Ausfallsicherheit der Hardware kaum genügen kann. Es wäre gerade so, als würde man den die Einsatzmöglichkeiten und den Nutzen eines LKWs alleine an seiner PS-Stärke und der Ladefläche festmachen, ohne Rücksicht auf die Straßenverhältnisse, die Routenführung, Staus und Transportaufträgen.

Benutzerprozesse hochverfügbar machen

Wenngleich die Verfügbarkeit der Serverhardware die elementarste Stufe der Messung darstellen mag, für eine umfassende Bewertung allerdings müssen alle involvierten Komponenten in die Betrachtung einbezogen werden.

Um also einen IT-Dienst - und nicht nur einen Server - im Sinne der Anwender hochverfügbar zu machen, müssen sich diese Dienste am tatsächlichen Bedarf und der abgeforderten Last orientieren. Dies zeigt einmal mehr, dass kein Weg an einer flexibel agierenden IT vorbei führt, bei der die die bereitgestellten Rechnerressourcen **dynamisch an den tatsächlichen Bedarf**[9] angepasst werden. Diese Dynamik wiederum verlangt nach **Automatismen in der Verwaltung der Systeme**[10].

Absicherung von Serversystemen

Die sechs wichtigsten Funktionen des HP-UX 11i

Die Absicherung von Serversystemen wir im angloamerikanischen Sprachgebrauch auch als Hardening bezeichnet. HP-UX 11i umfasst hierzu gleich mehrere dieser Funktionen, um das Betriebssystem gegen Angriffe zu sichern.

1. Bastille: Durch die Funktionen in Bastille erfolgt eine grundsätzliche Absicherung des Systems. Dazu gehört beispielweise das Abschalten nicht benötigter Dienste, das Sperren von Konfigurationen gegen Veränderungen oder die Konfiguration von IP-Filtern für die Kommunikation. Die Bedienung des Verwaltungstool wird durch die Bereitstellung von Assistenten vereinfacht. Die Sicherheitseinstellungen durch Bastille überstreichen die Sicherheitsbelange von Web-Servern, Applikations-Server und Datenbankmanagementsysteme gleichermaßen.

2. HIDS: Bei HIDS handelt es sich um ein Host Intrusion Detection System, dass Angriff auf das Serversystem verhindert. Dies passiert durch die Echtzeitüberwachung des Kommunikationsverhaltens. HIDS hilft damit einen Host-Server gegen Angriffe abzusichern.

3. Secure Resource Partitions (SRP): SRPs werden verwendet, um zusammengehörende Applikationen in einer abgeschlossenen und separierten Instanz des HP-UX zusammenzufassen. Durch diese Separierung einer definierten Gruppe von Applikationen sind diese gleichzeitig gegen Angriffe von außen besser geschützt. Korrespondierend dazu stehen die Security Containment Compartments. Sie bilden die Container, in denen die Applikationen und die Betriebssysteminstanz agieren. Die Verwaltung der SRP erfolgt durch den HP Process Resource Manager. Er ermöglicht eine zentrale Administration und die Separierung der Softwaremodule in die Compartments.

4. IPFilter: Beim IPFilter handelt es sich um eine Stateful Inspection Firewall des jeweiligen Systems. Dieses filtert den Datenverkehr von oder zu einem Serversystem. Der IPFilter liefert damit Funktionen, wie sie durch traditionelle Firewalls geboten werden. Aber im Gegensatz zu den bekannten Firewalls adressiert der IPFilter die Sicherheit eines Serversystems und nicht die Absicherung des Unternehmensnetzes gegen Angriffe von außen.

5. EVFS: Durch das EVFS (Encrypted Volume und File System) erfolgt die Verschlüsselung der Daten auf allen eingesetzten Datenträgern. Selbst wenn es einem Angreifer gelingen mag, Zugriff auf die Speichersysteme zu erhalten, so wird er mit deren Inhalt nichts anfangen können, da diese vor der Ablage auf die Speichersysteme automatisch durch die Dateisystem-Treiber des Betriebssystems verschlüsselt werden.

Die wichtigsten Kriterien

Sucht man nach den Kriterien, welche die Verfügbarkeit der IT-Dienste beeinträchtigen, so lassen sich folgende Gruppen herausarbeiten.

Ausfälle oder Reduzierung[11] der Leistung von Hardwarekomponenten: Um das zu vermeiden, müssen die Hardwarebaugruppen möglichst sicher gestaltet sein. Dies sollte von den elementaren Baugruppen bis hin zu den Betriebssystemen und Applikationsinstanzen gelten.

Überlastung der Softwaresysteme aufgrund von steigender Last oder nicht optimaler Konfiguration der Systeme. Ein Mehr an abgeforderter Leistung lässt sich durch die Techniken der **Virtualisierung**[12] wirksam abfedern.

Überlastung oder Ausfall der Softwaresysteme aufgrund von Angriffen. Dies sind die traditionellen Angriffe auf die Softwaresysteme.

Ausfälle aufgrund von Wartungsarbeiten an der Hard- oder Software: Als Wartungsarbeiten an der Software wird dabei das Einspielen von Patches, das Ändern von Konfigurationen oder **Backup von Daten**[13] und Konfigurationen verstanden.

Häufig wird dabei auch nach den Kriterien der geplanten Ausfälle oder ungeplanten Ausfälle unterschieden. Doch das greift erneut zu kurz, denn wie ist dann die Reduzierung der Leistung aufgrund einer Überlastung einzustufen? Sind diese "Mikroausfälle" geplant oder ungeplant?

Die ersten beiden Aspekte wurden in weiteren Texten dieser Reihe bereits hinreichend behandelt. Sie sollen daher in diesen Teil nicht weiter thematisiert werden. Was noch verbleibt, ist der dritte und vierte Aspekt die Ausfälle aufgrund von Angriffen und Wartungsarbeiten oder Änderungen an den Konfigurationen der Systeme. Insbesondere der Zweig der Wartung ist in seiner Art verhältnismäßig neu und daher auch weniger beachtet.

Die Softwaresysteme der früheren Jahre waren relativ stabil und wurden nur selten geändert. Aufgrund des erhöhten Druckes an Anwender nach neuen Funktionen und den Möglichkeiten, die das Internet mit Online-Updates bietet, sind die Programme heute ständigen Änderungen durch Patches, Software-Updates oder dergleichen unterworfen. Um die Installation der steigenden Flut der Patches in geordneter Bahnen zu lenken, hat beispielweise Microsoft schon vor Jahren seinen Patch Tuesday eingeführt. Dabei sollen nur einmal, an jedem zweiten Dienstag, eines jeden Monats Patches bereitgestellt und installiert werden. Dies gilt jedoch nicht für dringende Änderungen an den Systemen. Sie werden weiterhin auch zwischendurch bereitgestellt und sollten auch sofort installiert werden. Hierzu bietet Microsoft in seinen Betriebssystemen auch Upgrade-Möglichkeiten an, die im Hintergrund arbeiten und meist nur einen Restart des Systems erfordern.

Server-Patches erfordern Auszeiten

Wenngleich die Installation von Patches für Desktop noch automatisiert und im Hintergrund erfolgen mag, für unternehmenswichtige Server wird man das kaum empfehlen. Auch einen Restart eines Servers im Tagesgeschäft wird man nur im äußersten Notfall durchführen wollen. Sind allerdings die Sicherheitsmängel so gravierend, dass sie keinen Aufschub erlauben, so führt kein Weg an einer zeitnahen Installation der Patches vorbei. Ferner werden Änderungen am Softwaresystem eines Servers, wenn möglich, immer erst nach ausgiebigen Tests mit Prototypinstallationen auf Verträglichkeit und Sicherheit erfolgen. Das alles erfordert Zeit und erhöht gleichzeitig den Verwaltungsaufwand und die Ausfallzeiten.

Das Ziel sollte also in einer Reduzierung der Änderungen liegen. Denn je weniger geändert und gepatcht werden muss, umso geringer sind die damit verbunden Risiken. Hierbei hat HP-UX aufgrund seiner Fokussierung auf den Serverbetrieb die Nase vorn. Kaum ein **Hacker**[14] wird **ein HP-UX-System**[15] mitsamt der dabei verwendeten Hardware und einem Speichersubsystem sein eigen nennen, um darauf seine Angriffe vorzubereiten. Die, im Verhältnis zu anderen Systemen, geringere Verbreitung führt damit implizit zu einer höheren Sicherheit. Darüber hinaus hat HP sein Unix-Derivat mit einer Vielzahl an Vorkehrungen ausgestattet, die das System von Grund auf sicherer machen. Dies reduziert nicht nur die Angriffsfläche und damit potentielle Ausfälle, es werden auch Softwareänderungen und Patches auf ein Minimum beschränkt.

Integration in das Betriebssystem ist AddOns vorzuziehen

Dabei ist es vorteilhaft, wenn möglichst viele der Sicherheitsfunktionen bereits zum Standardumfang des Betriebssystems gehören und nicht erst durch separate Produkte, mit eigenen Lizenzen und Management-Tools addiert werden müssen. Diese reduziert erneut den Verwaltungssaufwand und den Bedarf für Patches und Konfigurationen. HP hat all diese Funktionen in seine zentralen Verwaltungstools, wie etwa den **Systems Insight Manager**[16] (SIM) und dem **Virtual Server Environment**[17] (VSE) integriert.

Dessen Rollenmodell bildet bereits die erste Stufe der Sicherheit, denn es bestimmt, welcher Verwalter Zugriff auf die Tools und damit auch die Konfigurationen der Systeme erhält. Dieses Rollenmodell ermöglicht damit auch ein kontrolliertes Change Management, wie beispielweise von ITIL gefordert.

Funktionen des HP-UX 11i

Die Absicherung von Serversystemen wir im angloamerikanischen Sprachgebrauch auch als Hardening bezeichnet. **HP-UX 11i**[18] umfasst hierzu gleich mehrere dieser Funktionen, um das Betriebssystem gegen Angriffe zu sichern (siehe Kasten, oben).

Der wesentlicher Aspekt der Sicherheit ist das Wissen darüber. Erst durch die Gewissheit und den Nachweis, dass die Systeme den geforderten **Sicherheitsansprüchen**[19] genügen, können sie auch als sicher eingestuft werden. Dazu liefern die HP-Werkzeuge unterschiedlichste Auswertung und Analysen. Diese dienen ferner als Grundlage für die die Compliance-Anforderungen. Darüberhinaus erfüllt HP-UX und auch seine Container die Common Criteria Zertifizierung und dessen EAL 4 (Evaluation Assurance Level 4).

Fazit:

Die Datenzentren der Zukunft müssen weitaus dynamischer sein, als die **Rechenzentren**[20] heutiger Couleur. Dies lässt sich durch die Techniken der Virtualisierung erreichen. Dabei darf aber die Sicherheit und Verfügbarkeit nicht vernachlässigt werden. Sicherheit und Hochverfügbarkeit gehen dabei Hand in Hand. Ein verfügbares System, das unsicher ist, stellt eine noch höhere Bedrohung dar, als ein sicheres System, das nicht verfügbar ist, denn letzeres erlaubt auch keine Angriffe. Gleichzeitig erhöht der Schutz gegen Angriffe die Hochverfügbarkeit und entkräftet damit auch den Aspekt eines Single Point of Failure.

Links im Artikel:

[1] **https://www.computerwoche.de/knowledge_center/datacenter_server/1885359/**
[2] **https://www.cio.de/knowledgecenter/security/849104/index2.html**
[3] **https://www.computerwoche.de/knowledge_center/security/172251/**
[4] **https://www.computerwoche.de/knowledge_center/security/1878235/**
[5] **https://www.computerwoche.de/knowledge_center/security/1889434/**
[6] **https://www.computerwoche.de/knowledge_center/datacenter_server/1889791/index.html**
[7] **https://www.cio.de/knowledgecenter/storage/458076/**
[8] **https://www.tecchannel.de/index.cfm?pid=197&pk=429794&p=2**
[9] **https://www.computerwoche.de/knowledge_center/virtualisierung/1885498/**
[10] **https://www.computerwoche.de/knowledge_center/datacenter_server/1887198/**
[11] **https://www.computerwoche.de/knowledge_center/datacenter_server/1889791/index.html**
[12] **https://www.computerwoche.de/knowledge_center/virtualisierung/1885498/**
[13] **https://www.computerwoche.de/schwerpunkt/b/Backup.html**
[14] **https://www.computerwoche.de/knowledge_center/security/1889290/**
[15] **http://whitepaper.computerwoche.de/index.cfm?pid=1&pk=2836&fk=40**
[16] **https://www.computerwoche.de/knowledge_center/datacenter_server/1887846/index4.html**
[17] **https://www.computerwoche.de/knowledge_center/datacenter_server/1887846/**
[18] **http://whitepaper.computerwoche.de/index.cfm?pid=1&pk=2836&fk=40**

[19] **http://www.bsi.bund.de/cc/eal_stufe.htm**

[20] **https://www.computerwoche.de/schwerpunkt/r/Rechenzentrum.html**
