ISSN 1866-4954 APRIL 2009 / 1

Steinbuch Centre for Computing

NEWS

SCC

Servervirtualisierung – mehrere IT-Dienste auf einem Rechner

Datenverschlüsselung – wirksamer Schutz vor unliebsamen Zugriffen

Computernotfallteam für das KIT gegründet

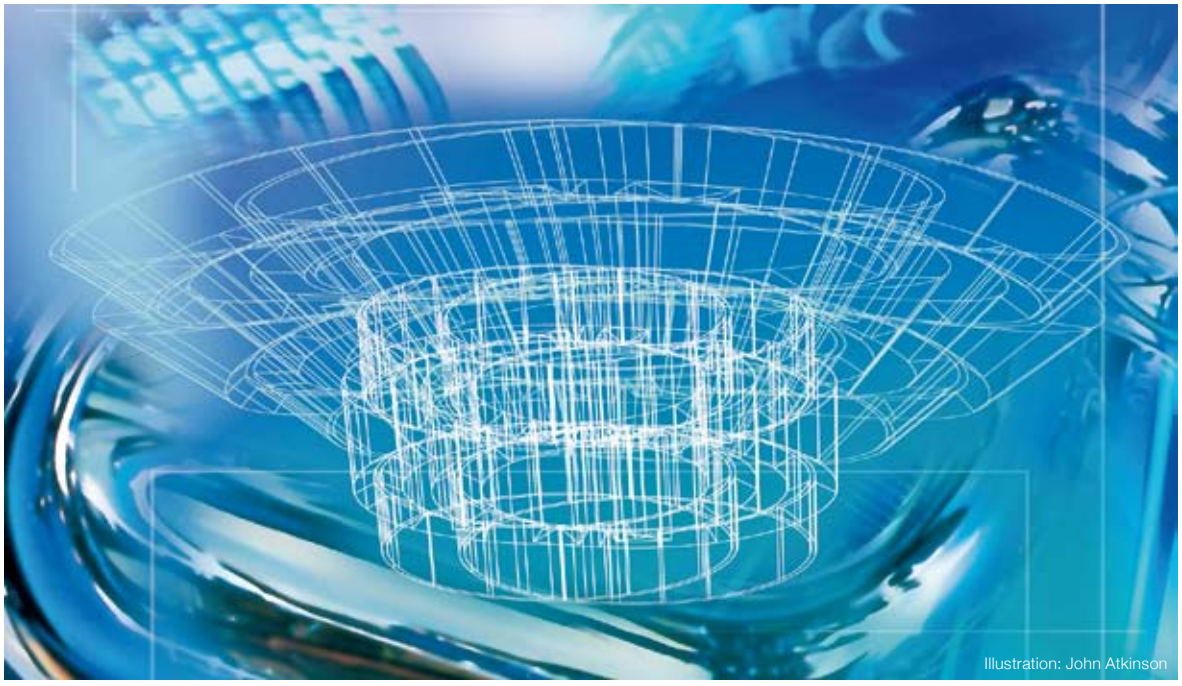


Illustration: John Atkinson

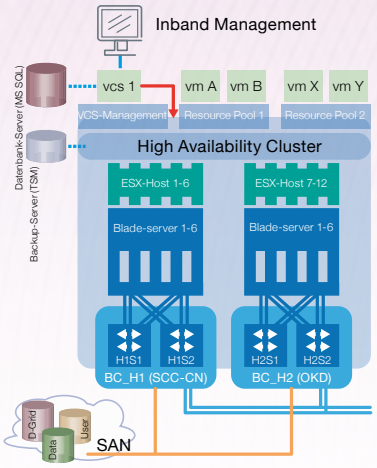
KIT – die Kooperation von Forschungszentrum Karlsruhe GmbH und Universität Karlsruhe (TH)

Karlsruhe Institute of Technology

Forschungszentrum Karlsruhe in der Helmholtz-Gemeinschaft

Universität Karlsruhe (TH) Forschungsuniversität • gegründet 1825

INHALT



4

7

Clustersystem	Taktfrequenz	Anzahl Cores pro CPU	Jahr der Inbetriebnahme
Intel Xeon 3,06 GHz	3,06 GHz	1	2004
AMD Opteron 270	2,00 GHz	2	2006 (Produktion)
Intel Xeon 5160 “Woodcrest”	3,00 GHz	2	2007 (Produktion)
AMD Opteron 2356 “Barcelona”	2,30 GHz	4	2008 (Testsystem)
Intel Xeon E5345 “Clovertown”	2,33 GHz	4	2008 (Produktion)
Intel Xeon E5430 “Harpertown”	2,66 GHz	4	2008 (Produktion)
AMD Opteron 2376 “Shanghai”	2,30 GHz	4	2009 (Testsystem)

10

14

EDITORIAL

Liebe Leserinnen und Leser,

die Zahl der eingesetzten IT Services und die Abhängigkeit von diesen Diensten nehmen seit Jahren stetig zu. Durch den Einsatz von Virtualisierungstechniken ist es möglich, mehrere IT-Dienste auf einem physikalischen Server zu konsolidieren und so die vorhandenen Computerressourcen optimal zu nutzen. Die Vorteile liegen dabei klar auf der Hand: Servervirtualisierung führt nicht nur zu einer Reduktion der Betriebskosten und einer vereinfachten Wartung, sondern bietet auch ganz neue Managementfunktionalitäten. Auch das SCC betreibt mehrere Virtualisierungs-Serverfarmen, um den rund 8.000 Mitarbeitern und mehr als 18.000 Studierenden hochverfügbare IT-Dienste zur Verfügung zu stellen.

Aber nicht nur die angebotenen IT-Dienste werden immer zahlreicher, auch die IT-Ausstattung wird immer vielfältiger und vor allen Dingen mobiler. Viele Leute sind heutzutage mit Notebooks, PDAs, externen Festplatten oder USB-Sticks unterwegs. Mit der Mobilität wächst jedoch auch das Risiko, ein Gerät und damit schützenswerte Daten zu verlieren. Abhilfe bieten geeignete Verschlüsselungsverfahren, die solche Daten vor fremden Zugriffen schützen.

Wenn das Kind jedoch bereits in den Brunnen gefallen ist – sprich ein Angriff erfolgreich war - dann bietet das vom SCC neu gegründete Computernotfallteam für das KIT (KIT-CERT) Unterstützung und Hilfe bei der Wiederaufnahme eines geregelten Betriebs an. Dies gilt natürlich nicht für verloren gegangene Datenträger.

Viel Vergnügen bei der Lektüre wünschen Ihnen

Hannes Hartenstein, Wilfried Juling und Klaus-Peter Mickel

Prof. Dr. Hannes Hartenstein
Foto: Privat

Prof. Dr. Wilfried Juling
Foto: Privat

Klaus-Peter Mickel
Foto: Privat

IMPRESSUM

April 2009
Herausgegeben im Auftrag des Direktoriums des Steinbuch Centre for Computing (SCC) von der Stabsstelle Öffentlichkeitsarbeit und Kommunikation
Anschrift: Steinbuch Centre for Computing (SCC)
Redaktion SCC-News
Zirkel 2
76128 Karlsruhe bzw.
Hermann-von-Helmholtz-Platz 1
76344 Eggenstein-Leopoldshafen
Fax: 0721/32550
http://www.rz.uni-karlsruhe.de/publikationen/scc-news.php

Redaktion:
Ursula Scheller (verantwortlich)
Telefon: 0721/608-4865
E-Mail: ursula.scheller@kit.edu
Layout und Bildredaktion: John Atkinson

Servervirtualisierung – mehrere IT-Dienste auf einem Rechner

Die Zahl der eingesetzten IT-Dienste sowie die Abhängigkeit von diesen nehmen seit Jahren zu, und es ist kein Ende dieses Trends abzusehen. Die klassische Sicht „ein Dienst gleich ein Server" führt zu einem nicht mehr vertretbaren Aufwand für Anschaffung und Betrieb der Systeme. Als Lösung bietet sich an, durch den Einsatz von Virtualisierungstechniken mehrere IT-Dienste auf einem physikalischen Server zu konsolidieren. Neben der Reduktion der Betriebskosten ermöglicht dieser Ansatz auch neue Managementfunktionalitäten. Das SCC stellt den rund 8.000 Mitarbeitern und mehr als 18.000 Studierenden am KIT sowie für nationale und internationale Projekte IT-Dienste in großer Vielfalt zur Verfügung. Dabei kommen im harten 24-Stunden-Produktionsbetrieb an sieben Tagen in der Woche mehrere Virtualisierungs-Serverfarmen auf Basis von VMware ESX zum Einsatz.

Virtualisierung beschreibt Konzepte und Technologien, um Computerressourcen effektiver und flexibler nutzbar zu machen und ist heute eher eine strategische als eine technische Frage. Der Anwender erhält dabei stets eine wunschgemäße, abstrakte Sicht auf physische Ressourcen-Pools. Die optimierte Ressourcennutzung ergibt sich daraus, dass unterschiedliche Anwendungen auf einem physischen Rechner konsolidiert werden können. Eine virtuelle Maschine läuft in einer isolierten Umgebung auf einem realen System und verhält sich dabei wie ein vollwertiger Computer mit eigenen Komponenten wie Bios, CPU, Hauptspeicher, Festplatten, Grafikkarte, Netzwerkkarten, usw. Für die Anwendung selbst ist nicht ersichtlich, dass sie virtualisiert läuft [1].

Die Virtualisierung wird im Server- und Desktop-Bereich bereits seit Ende der 90er Jahre verstärkt genutzt. Allerdings handelt es sich dabei nicht um eine völlig neue Technologie. Tatsächlich wurde die Virtualisierung bei Großrechnern bereits vor über 40 Jahren von IBM mit der Virtual Machine Facility/370, kurz VM/370 eingeführt. Auch damals war das Ziel die optimierte Nutzung der Computerressourcen. Auf der VM/370 wurde Mehrbenutzerbetrieb ermöglicht, indem mehrere Einzelbenutzerbetriebsinstanzen in virtuellen Maschinen ausgeführt wurden. Jede virtuelle Maschine stellt eine vollständige Nachbildung der darunter liegenden, physischen Hardware dar [2]. Heutzutage kann Virtualisierung auch in Mikroprozessorumgebungen ähnlich zuverlässig und skalierbar wie in Großrechnern betrieben werden. Eine virtuelle Infrastruktur kann dabei nahezu alle Aspekte eines modernen Rechenzentrums verwalten, wie Server, Netze, Datenspeicher, Software, Anwendungen, aber auch komplette Desktop-Systeme. Der Zugriff erfolgt in diesem Fall in der Regel über einen energiesparenden Thin-Client. Konsolidierungsfaktoren von bis zu 40 aktiven Desktops auf einem Server sind problemlos möglich.

Kostensenkung durch bessere Hardware-Auslastung

Der Einsatz von Servervirtualisierung und die damit einhergehende Konsolidierung ermöglicht eine bessere Auslastung der Hardware. Dieses führt zu einer Kostensenkung bei Hardware, Verbrauchskosten (Strom, Kühlung), Stellplätzen, Administration, usw. Aktuell wird davon ausgegangen, dass durch den Einsatz von Servervirtualisierung die Investitionen in neue Hard- und Software um bis zu 70% sinken können und Kosteneinsparungen von bis zu 50% erreichbar sind. Virtualisierung zählt laut Gartner zu den wichtigsten Technologien bis zum Jahr 2010. Laut einer IDG (International Data Group)-Studie zum Thema Servervirtualisierung vom Juni 2008 rechnen Unternehmen, die Servervirtualisierung nutzen, 2009 mit einem Zuwachs von 52 Prozent an neu zu virtualisierenden Servern.

Vereinfachte Wartung

Virtuelle Maschinen können über die Funktion der Live-Migration im laufenden Betrieb unterbrechungsfrei zwischen realen Servern verschoben werden, ohne dass die Nutzer dies bemerken. Wartungsarbeiten an der Hardware werden dadurch stark vereinfacht, da diese zu beliebigen Zeiten durchgeführt werden können und hardwarebedingte Wartungsfenster prinzipiell entfallen. Außerdem können durch Hinzufügen weiterer Server den virtualisierten Diensten im laufenden Betrieb zusätzliche Ressourcen zur Verfügung gestellt werden.

Minimale Leistungseinbußen

Der Ausfall einer virtuellen Maschine beeinflusst nicht die Stabilität der übrigen virtuellen Maschinen oder des Hosts. Software-Tests und Software-Entwicklung werden optimiert, denn zusätzliche Testumgebungen können ohne die Bereitstellung weiterer Hardware innerhalb von Minuten aufgesetzt werden. Legacy-Betriebssysteme oder Legacy-Anwendungen, also historische Anwendungen, für die keine Hardware-Unterstützung mehr zu bekommen ist, können durch Virtualisierung am Leben gehalten werden.

Es gibt eigentlich keine Gründe, die gegen den Einsatz von Virtualisierung im Serverkontext sprechen, außer der Sorge des Administrators, dass man auf eine virtuelle Maschine kein Inventar-Label kleben kann. Die Leistungseinbußen virtueller Maschinen liegen im Vergleich zu realer Hardware, nach unseren praktischen Erfahrungen bei lediglich 5%-10%. Bei aktuellen Mehrkernprozessor-Systemen spielt dieser Leistungs-

verlust zunehmend eine untergeordnete Rolle, da genügend CPU-Zyklen zur Verfügung stehen. Ungeeignet für Virtualisierung sind lediglich Systeme mit speziellen Hardware-Anforderungen wie beispielsweise Kopierschutzstecker (Hardwaredongles) oder ISDN-Karten.

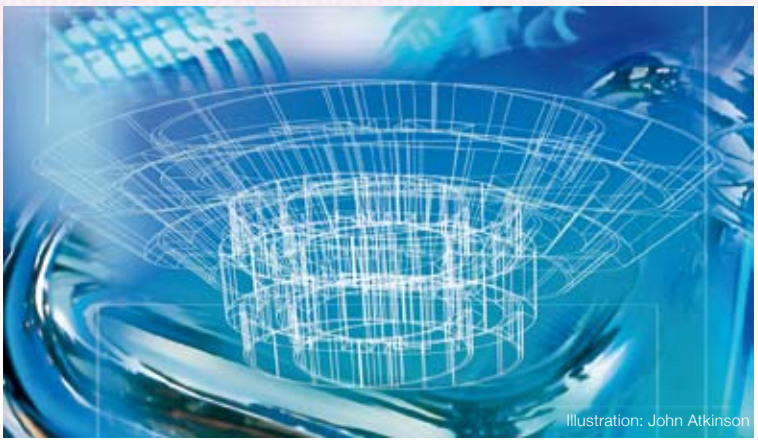


Illustration: John Atkinson

Eine potenzielle Gefahr beim Einsatz von Servervirtualisierung und der damit einhergehenden Serverkonsolidierung ist, dass beim Ausfall eines Hosts mehrere virtuelle Server gleichzeitig ausfallen. Hier sind geeignete Ausfallkonzepte und redundante Installationen notwendig. Da die Sicherung gegen Ausfälle dabei aber zentral auf der Ebene der Virtualisierung erfolgt, entfällt meist die Notwendigkeit, die einzelnen IT-Dienste selbst gegen Ausfall zu sichern. Eine weitere Gefahr ist, dass Sicherheitslücken auf der Virtualisierungsebene das Potenzial haben, laufende virtuelle Maschinen zu kompromittieren. Es existieren aber Lösungen, die auch für die höchsten Sicherheitsstandards zertifiziert sind (zum Beispiel VMware ESX).

Neue Managementfunktionalitäten

Bei der Virtualisierung wird zwischen der Hardware und den virtualisierten Systemen eine zusätzliche Softwareschicht eingezogen. Die dadurch erreichte Kontrolle über die virtualisierten Systeme ermöglicht ganz neue Managementfunktionalitäten. So können beliebige Snapshots von laufenden Systemen angelegt werden, das heißt der momentane Zustand wird abgespeichert und kann jederzeit wieder hergestellt werden. Dadurch lassen sich zentral „von außen“ Backups der virtuellen Systeme erstellen, ohne in jedem virtuellen System eine eigene Backupsoftware installieren zu müssen. In Test- und Entwicklungsszenarien ist es möglich, bestimmte Versionen zu sichern und bei Bedarf ohne größeren Aufwand zu diesen zurückzukehren, falls in der Entwicklung etwas schief geht.

Da virtuelle Maschinen in einem Image-File gespeichert werden, ist die Zeit für die Bereitstellung eines neuen virtuellen Servers inklusive installiertem Betriebssystem und gegebenenfalls installierter Anwendungen im Wesentlichen durch die Dauer des Kopiervorgangs vorgegeben. Durch Anlegen von Template-Bibliotheken lassen sich für vielfältige Zwecke Vorlagen zur schnellen Erzeugung von virtuellen Systemen vorhalten.

Die Virtualisierungsschicht ermöglicht es, die vorhandenen Ressourcen (CPU, RAM, usw.) über mehrere physikalischen Server hinweg zu verwalten. Je nach aktueller Leistungsanforderung der einzelnen virtuellen Server können diese daher zu jedem Zeitpunkt optimal auf die physikalischen Server verteilt werden. Durch Anlegen von Ressourcen-Pools lassen sich die virtuellen Systeme unterschiedlich priorisieren, um Vereinbarungen zu garantierter Güte und Verfügbarkeit (Service Level Agreements) für Ressourcen oder Dienste zu garantieren.

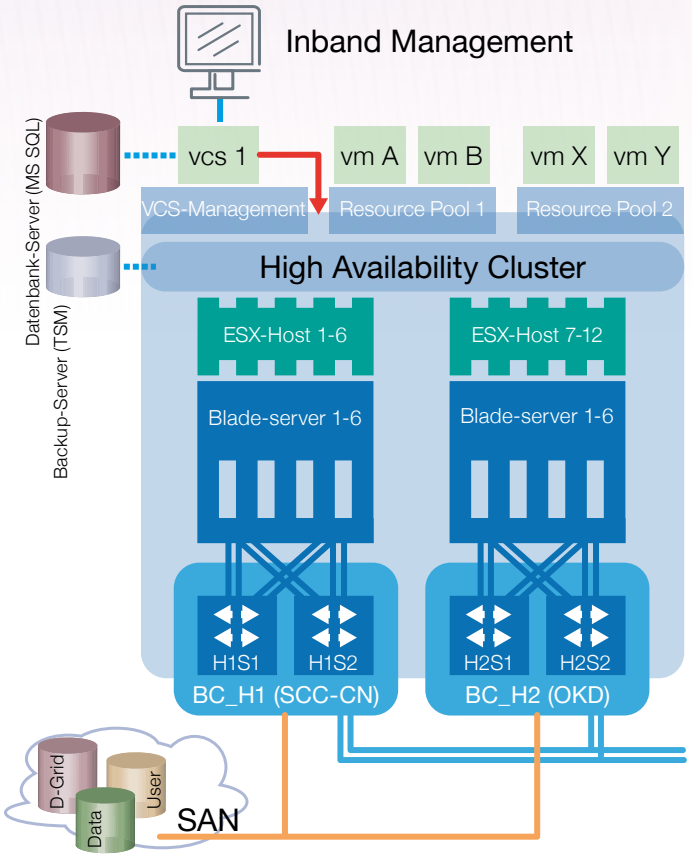
Servervirtualisierung am SCC

Bereits im Sommer 2006 begann die intensive Auseinandersetzung mit Virtualisierungstechniken am SCC. Ziel war es von Anfang an, den Betrieb hochverfügbarer Infrastrukturen zu gewährleisten. Zudem sollten künftige IT-Installationen ressourcenschonende Aspekte vorweisen können – Green IT in der Praxis sozusagen. Das Besondere bei dem angestrebten Projekt war, dass sich nahezu 25 Universitäten und wissenschaftliche Einrichtungen im Zuge der so genannten D-Grid-Initiative zusammengeschlossen hatten, um eine integrierte Ressourcen-Plattform für Hochleistungsrechner zu schaffen, die große Mengen von Daten und Informationen sowie entsprechende Dienstleistungen vereint. Der Betrieb der Basisdienste des verteilten Systems musste dabei natürlich rund um die Uhr gesichert sein [3].

Aufgrund der guten Erfahrungen mit den Virtualisierungsumgebungen lag es auf der Hand, dass weitere IT-Dienste ebenfalls auf virtueller Basis funktionieren sollten. Um die Umsetzung möglichst kontrolliert ablaufen zu lassen, wurde zunächst eine Arbeitsgemeinschaft und schließlich die SCC-Abteilung Integration und Virtualisierung (IVI) gegründet. Ziel ist es, nach und nach möglichst viele Services am Institut zu virtualisieren und eine Strategie „Virtualize first“ bei der Einrichtung neuer Dienste zu etablieren [4].

Derzeit werden mehrere Virtualisierungs-Cluster auf Basis von VMware ESX und Xen am SCC betrieben. Das aus dem oben erwähnten Projekt hervorgegangene VMware-Cluster umfasst momentan 12 IBM-Bladeserver verteilt über zwei Bladecenter an zwei Standorten auf dem Campus Nord des KIT. Insgesamt stehen 48 CPU-Cores mit 112 GHz Leistung und 192 GB RAM zur Verfügung. Für die Speicherung der virtuellen Maschinen stehen etwa 5 TB Plattenkapazität bereit, die über das allgemeine Storage Area Network (SAN) angeschlossen sind. Alle Server sind mit zwei HBAs (Host Bus Adapter) über getrennte Switches an das SAN und mit 4

Netzwerkkarten über zwei getrennte Switches ans Netzwerk (LAN) vollständig redundant angeschlossen. Der Ausfall einer einzelnen Komponente beeinträchtigt daher den Betrieb nicht. Sollte ein Bladeserver ausfallen, werden die betroffenen virtuellen Maschinen von der VMware-HA-Funktionalität (High Availability) vollautomatisch auf anderen Servern neu gestartet und stehen innerhalb weniger Minuten wieder zur Verfügung. Durch die Verteilung der Server auf zwei Standorte ist selbst



Das ESX-Cluster aus 12 Bladeservern ist auf zwei Standorte (SCC und Stabsabteilung Organisation und Kaufmännische Datenverarbeitung) auf dem Campus Nord verteilt. Der Verwaltungsserver (vcs1) läuft als virtuelle Maschine auf dem Cluster. Zur Datensicherung werden Snapshots der virtuellen Maschinen in einem TSM-Bandarchiv gespeichert.

bei komplettem Ausfall eines Standorts noch ein Weiterbetrieb möglich, wenn auch in eingeschränktem Umfang. Neben den ca. 50 VMs, die für Grid-Basisdienste bzw. als Testsysteme für D-Grid eingesetzt werden, laufen auf dem Cluster weitere 90 VMs aus unterschiedlichen Bereichen, darunter beispielsweise das Portal für die Beantragung von X.509-Zertifikaten (GridKa-CA).

Neben der Abteilung IVI betreibt auch die SCC-Abteilung Server und Systeme (SYS) zwei HA-Cluster auf Campus Nord und Süd. Hier stehen insgesamt 7 ESX-Hostsysteme mit 56 CPU-Cores (168 GHz) und 256 GB RAM zur Verfügung. Die beiden Cluster können auf insgesamt 4,4 TB Plattenkapazität zugreifen. Sowohl SAN- als auch LAN-Anbindung sind ebenfalls vollständig redundant ausgelegt. Die etwa 160 virtuellen Maschinen erbringen verschiedenste IT-Dienste wie Domänenkontroller, Web-, Überwachungs-, SAP, Exchange-, Radius-, Antiviren- und Lizenzserver und dienen auch als Test- und Entwicklungssysteme.

Für GridKa, das deutsche Tier1-Zentrum des LHC-Computing-Grids (LHC=Large Hadron Collider), betreibt die SCC-Abteilung Verteilte Systeme und Grid (VSG) zwei weitere ESX-Hostsysteme. Die hier laufenden etwa 25 virtuellen Maschinen stellen verschiedene Grid-Basisdienste bereit bzw. gehören zum „Pre-Production System“, auf dem neue Softwareversionen vor dem produktiven Einsatz getestet werden.

Aber auch weitere Institute innerhalb des KIT nutzen die Vorteile, die der Einsatz der Servervirtualisierung bietet. So betreibt das SCC für das Institut für Prozessdatenverarbeitung und Elektronik (IPE) zwei virtuelle Umgebungen. In einem Fall wird dabei auf einem einzelnen ESX-Hostsystem die komplexe Netzwerktopologie der Datenerfassung für das Auger-Experiment in Argentinien nachgebildet. Die insgesamt 48 virtuellen Maschinen werden mit der originalen hierarchischen Netzwerktopologie auf einem einzigen Server-Blade zusammengefasst und ermöglichen so Entwicklung und Test von Softwarekomponenten unter „realen“ Bedingungen. Die andere virtuelle Umgebung dient der Entwicklung verteilter MATLAB-Anwendungen in Grid-Umgebungen und umfasst 25 virtuelle Maschinen. Für diese wird keine getrennte Hardware eingesetzt sondern das oben bereits erwähnte VMware-Cluster aus 12 IBM-Bladeservern parasitär genutzt. Dies ist ein gutes Beispiel für die Synergieeffekte, die sich durch Virtualisierung erzielen lassen. Weiterhin setzt das Institut für Angewandte Informatik (IAI) zwei VMware-Hostsysteme zur Serverkonsolidierung ein, unter anderem um Kapazitätsengpässe in der Kühlung des eigenen Rechnerraums zu vermeiden.

Christian Baun, Dr. Marcel Kunze, Dr. Jens-Michael Milke

Quellen

[1] Baun C, Kunze M, Ludwig T (2009) Servervirtualisierung. Springer-Verlag. http://www.springerlink.com/content/h387wm5110563745/fulltext.pdf (Zugriff: 6. Februar 2009)

[2] Bengel G, Baun C, Kunze M, Stucky K-U (2008) Masterkurs Parallele und Verteilte Systeme: Grundlagen und Programmierung von Multicoreprozessoren, Multiprozessoren, Cluster und Grid. Vieweg und Teubner, Wiesbaden

[3] Kulla F, Kunze M, Virtualization of Grid Services in D-Grid, 1. GI/ITG KuVS Fachgespräch „Virtualisierung“ Paderborn, 2008 pp.65, http://www.fachgespraech-virtualisierung.de/fileadmin/FGV/TR-RI08291.pdf

[4] Im Namen der Wissenschaft: Virtualisierung beim Steinbuch Centre for Computing am Karlsruhe Institute of Technology. http://www.it-administrator.de/themen/server_client/fachartikel/51584.html (Zugriff: 6. Februar 2009)

Datenverschlüsselung – wirksamer Schutz vor unliebsamen Zugriffen

„Ich habe gar keine geheimen Daten auf meinem Notebook!“. Diese oder eine ähnliche Antwort hört man häufig, wenn es darum geht, die Festplatte eines Rechners zu verschlüsseln. Das Argument, keine geheimen Daten zu haben, mag subjektiv zutreffen, in vielen Fällen wird jedoch der Wert der eigenen Daten massiv unterschätzt. Dabei bieten geeignete Verschlüsselungsverfahren wirksamen Schutz vor fremdem Zugriff.

Während unpublizierte Forschungsergebnisse noch offenkundig schützenswert sind, fällt dies bei vielen anderen Daten nicht sofort auf. Daten, die ebenfalls sensitiv sind, an die aber häufig nicht gedacht wird, sind beispielsweise Personaldaten jeglicher Art, insbesondere auch Beurteilungen und dergleichen, Patentdaten, aber auch Passwörter, Lizenzinformationen und nicht zuletzt persönliche Daten. Sind diese Daten wirklich so unwichtig, wie es den Anschein hat? Dabei sollte man sich selbst einmal fragen: Würde es mir etwas ausmachen, wenn diese Daten allesamt am Schwarzen Brett der Mensa ausgehängt würden? Eine solche Vorstellung ist wohl in den meisten Fällen nicht besonders angenehm.

Darüber hinaus wird die IT-Ausstattung immer mobiler: Notebooks, PDAs, externe Festplatten, USB-Sticks und dergleichen erfreuen sich wachsender Beliebtheit, weil man damit auch von wechselnden Standorten und unterwegs arbeiten kann. Mit der Mobilität wächst aber auch das Risiko, dass ein Gerät und damit auch schützenswerte Daten verloren gehen. Je mobiler ein Gerät ist und je sensibler die darauf enthaltenen Daten, desto wichtiger ist es, angemessene Schutzmaßnahmen zu ergreifen.

Aber nicht nur mobile Geräte sind gefährdet. Ein Weg, auf dem Daten verloren gehen können, wird häufig übersehen: Der Garantiefall. Heutzutage ist es üblich, dass beispielsweise Festplatten, die innerhalb der Garantiezeit ihren Dienst quittieren, eingeschickt werden müssen, um Ersatz zu erhalten. Diese eingeschickten Festplatten, bei denen häufig die Steuerelektronik defekt ist, werden vom Hersteller mit einer neuen Steuerplatine ausgerüstet und dann als Austauschgerät wieder in Umlauf gebracht, und zwar mitsamt allen Daten, die der letzte Anwender aufgespielt hat. Ein Löschen ist vor dem Einschicken an den Hersteller aber nicht mehr so ohne Weiteres möglich, da die Festplatte ja defekt ist. Ein ähnliches Szenario spielt sich häufig dann ab, wenn ein Mitarbeiter ausscheidet und sein Arbeitsplatzrechner einem anderen Kollegen „vermacht“ wird. Auch hier wird mitunter nicht so gründlich aufgeräumt, wie es wünschenswert wäre.

Alle diese Risiken können durch die Verschlüsselung von Daten oder ganzen Datenträgern wirksam umgangen werden, Voraussetzung ist natürlich eine korrekte Anwendung. Kommt ein verschlüsselter Datenträger in die Hände Unbefugter, auf welchem Weg auch immer, so sind die darauf gespeicherten Daten dennoch entsprechend der Stärke der verwendeten Verschlüsselungsalgorithmen und des verwendeten Kennworts sicher.

Die Prozessoren in heutigen Arbeitsplatzrechnern erlauben, vom Anwender in aller Regel völlig unbemerkt, die Verschlüsselung der gesamten Festplatte. Aktuelle Rechner sind typischerweise so leistungsstark, dass selbst die Verschlüsselung der gesamten Festplatte nur ungefähr 5 % der Rechenleistung benötigt, wenn permanent auf der Platte gelesen oder geschrieben wird. Bei USB-Sticks und dergleichen fällt die Verschlüsselung noch weit weniger ins Gewicht, weil bei diesen Geräten die Geschwindigkeit der Datenübertragung in der Regel durch die USB-Schnittstelle viel deutlicher beschränkt ist, als dies bei normalen Festplatten der Fall ist.

Vermeidbare Risiken

Aber die Verschlüsselung von Daten bringt natürlich auch Nachteile mit sich. Das größte Risiko ergibt sich direkt aus der gewünschten Haupteigenschaft der Verschlüsselung: Zugriff auf die Daten kann nur derjenige erlangen, der den korrekten Schlüssel beziehungsweise das Passwort kennt. Vergisst der legitime Besitzer der Daten das Kennwort, mit dem diese Daten verschlüsselt wurden, so gibt es auch für ihn keine Möglichkeit mehr, an die Daten zu gelangen. Dieses Problem wird je nach eingesetzter Software noch verstärkt durch die Tatsache, dass häufig das vom Benutzer eingegebene Kennwort nicht direkt als Schlüssel für die Verschlüsselung verwendet wird. Vielmehr wird der eigentliche Schlüssel seinerseits mit dem Benutzerkennwort verschlüsselt und so gespeichert. Dieses Vorgehen bringt einige wesentliche Vorteile mit sich, aber auch die Gefahr, dass zufällig genau der mit dem Kennwort verschlüsselte Schlüssel verloren geht, beispielsweise indem ein Block der Festplatte beschädigt wird, was relativ häufig vorkommt. Geht nun just der „richtige“ Block kaputt, so ist damit auch der Schlüssel verloren, mit dem die verschlüsselten Daten wieder herzustellen gewesen wären. Mitunter bietet die Verschlüsselungssoftware aus genau diesem Grund die Möglichkeit, diesen wichtigen Schlüsselblock beispielsweise auf eine CD zu brennen, um im Notfall noch eine zweite Kopie zu haben.

Sicherungskopien verschlüsselt oder unverschlüsselt?

Ein weiteres Problem ist das Herstellen von Backups. Jedes Rechnersystem mit einigermaßen wichtigen Daten sollte regelmäßig gesichert werden, um einen Datenverlust zu vermeiden. Typischerweise werden dabei nur die Teile eines Datenträgers gesichert, die sich gegenüber der letzten Sicherung geändert haben, um Platz zu sparen.

Dies wird erschwert oder gar unmöglich gemacht, wenn Teile der Daten verschlüsselt werden. Ein verschlüsselter Datenbereich muss bei der kleinsten Änderung der in ihm enthaltenen Daten komplett gesichert werden. Zudem muss überlegt werden, ob das Backup seinerseits auch wieder verschlüsselt werden muss. Je nachdem, wogegen genau der Einsatz von Verschlüsselung schützen soll, wird das eigentliche Ziel konterkariert, wenn unverschlüsselte Sicherungskopien der Daten angelegt werden.

Möglichkeiten der Verschlüsselung

Wenn auf einem Rechner schützenswerte Daten gespeichert werden, so ist die Verwendung von Verschlüsselung empfehlenswert. Grundsätzlich gibt es in der Praxis drei Möglichkeiten, Daten zu verschlüsseln:

- Verschlüsselung einzelner Dateien
- Verschlüsselung einzelner Datenbereiche (Partitionen, Container)
- Verschlüsselung ganzer Systeme.

Die unmittelbarste Methode ist die Verschlüsselung einzelner Dateien. Jede zu verschlüsselnde Datei wird dabei einzeln verschlüsselt und in verschlüsselter Form auf dem Datenträger gespeichert. Dieses Verfahren ist auch am flexibelsten in dem Sinne, dass der Anwender sehr genau kontrollieren kann, welche Dateien verschlüsselt werden sollen und welche nicht. Zudem kann im Prinzip jede Datei mit einem individuellen Kennwort gesichert werden. Trotzdem hat diese Methode einige gravierende Nachteile. Wesentlicher Nachteil ist es, dass das Verfahren sehr aufwändig ist. Je mehr Daten zu schützen sind, desto mehr muss der Benutzer dafür tun. Zudem läuft der Anwender ständig Gefahr, eine Datei zu übersehen, und zu allem Überfluss können typischerweise nicht alle Dateien eines Systems mit dieser Methode geschützt werden. Gerade Swap-Dateien, in denen das Betriebssystem bei Bedarf Teile des Hauptspeichers auslagert, enthalten häufig interessante Informationen wie Passwörter und ähnliches, sind aber mit dieser Methode in der Regel nicht zu schützen.

Die Verwendung ganzer verschlüsselter Bereiche, häufig „Cryptocontainer" genannt, schafft Abhilfe für einige der genannten Probleme. Die Anwendung ist in der Praxis für den Benutzer relativ einfach, da für einen ganzen geschützten Bereich nur ein einziges Mal beim Systemstart bzw. bei der ersten Benutzung danach ein Kennwort eingegeben werden muss, unabhängig davon, wie viele Dateien in dem Bereich abgelegt sind. Auch sinkt das Risiko, dass wichtige Daten nicht verschlüsselt werden, weil sie übersehen wurden. Systemdateien können aber in aller Regel auch mit diesem Verfahren nicht geschützt werden, so dass beispielsweise die Swap-Datei-Problematik auch hier wieder besteht. Ein weiterer Nachteil ist die geringere Flexibilität, denn der gesamte Cryptocontainer wird zwangsläufig mit einem einzigen Kennwort verschlüsselt. Es ist also nicht mehr möglich, jeder Datei ein eigenes Passwort zuzuordnen.

Die Verschlüsselung des gesamten Systems schließlich löst auch das letztgenannte Problem. Sämtliche Daten eines Systems werden geschützt, so dass keinerlei Gefahr besteht, versehentlich Daten übersehen zu haben. Allerdings ist hierfür ein sehr tiefgehender Eingriff in das Betriebssystem nötig. Insbesondere muss in den Bootvorgang eingegriffen werden, denn das Betriebssystem steht ja nur verschlüsselt zur Verfügung. Es muss also vor dem eigentlichen Laden des Betriebssystems die Festplatte entschlüsselt werden, was entsprechende Software voraussetzt. Dafür ist dieses Verfahren völlig transparent für den Benutzer und sichert das gesamte System ab, ohne dass der Benutzer etwas dafür tun muss, abgesehen von der Eingabe des Kennworts beim Booten.

Bei der Wahl des Verschlüsselungsverfahrens sollten auch noch weitere Aspekte bedacht werden. Sollen Daten mit anderen Rechnern geteilt werden, gar über Betriebssystemgrenzen hinweg? In diesem Fall ist es unerlässlich, ein Verfahren zu wählen, das auf allen relevanten Systemen verfügbar ist. Sollen Daten mit anderen Anwendern geteilt werden? Dann ist es ratsam, ein Produkt zu verwenden, das es erlaubt, mehrere verschiedene Schlüssel zu verwenden, damit jeder einzelne Anwender einen eigenen Schlüssel hat und jeder Schlüssel damit nur einer einzigen Person bekannt ist. Diese und weitere Fragen sollten bei der Entscheidung für ein Verfahren und ein konkretes Produkt zumindest im Hinterkopf präsent sein, um nicht im Nachhinein böse Überraschungen zu erleben.

KIT-CERT empfiehlt Verschlüsselung des Gesamtsystems

Das Computer Emergency Response Team (KIT-CERT) empfiehlt, das gesamte System zu verschlüsseln, wann immer dies möglich ist. Hierfür stehen für verschiedene Betriebssysteme unterschiedliche Softwarepakete zur Verfügung. Nachfolgend werden einige Lösungen vorgestellt, ohne dass Anspruch auf Vollständigkeit erhoben wird.

Windows

Für Windows existieren eine Reihe geeigneter Produkte, die aus Sicht des KIT-CERT empfehlenswert sind. Zusätzlich wird mit Windows Vista bereits mit Bordmitteln die Möglichkeit zur Verschlüsselung des gesamten Systems gegeben; die Windows-eigene Lösung heißt Bitlocker. Von Drittanbietern sind TrueCrypt, BestCrypt und FreeOTFE (Free On-The-Fly Encryption) verfügbar, die unterschiedliche Formen der Verschlüsselung unterstützen. Bei TrueCrypt und FreeOTFE handelt es sich um kostenfreie Software, BestCrypt hingegen ist kommerzielle Software. FreeOTFE gibt es zusätzlich zur normalen Windows-Version auch noch als Windows Mobile Version, so dass es auf Windows Mobile-6-basierten Mobiltelefonen zum Einsatz kommen kann. Leider bietet FreeOTFE im Gegensatz zu den übrigen Produkten nicht die Möglichkeit, das gesamte System zu verschlüsseln, sondern kann lediglich Datenpartitionen oder -container sichern.

Linux

Auch unter Linux gibt es einige Softwarepakete, die das Gewünschte leisten. Unter „Bordmittel" fällt die Verschlüsselung mit Hilfe von LUKS (Linux Unified Key Setup) beziehungsweise dm-crypt. Viele aktuelle Linux-Distributionen unterstützen diese Form der Verschlüsselung bereits nativ. Alternativ hierzu kann man auch auf BestCrypt oder TrueCrypt zurückgreifen; beide Produkte stehen auch in Linux-Versionen zur Verfügung, so dass mit BestCrypt oder TrueCrypt auf

verschlüsselte Daten sowohl unter Windows als auch unter Linux zugegriffen werden kann. Aber auch LUKS-basierte Verschlüsselung kann unter Windows verwendet werden: FreeOTFE unterstützt LUKS-basierte Verfahren.

MacOS X

Unter MacOS X steht neben dem mitgelieferten „hdiutil" auch TrueCrypt zur Verfügung. Wird der Datenaustausch mit Windows- oder Linux-Systemen angestrebt, so sollte folglich TrueCrypt verwendet werden.

Kennwort enorm wichtig

Unabhängig davon, welches Verschlüsselungsverfahren und welches Produkt eingesetzt werden, sollten einige Hinweise stets beachtet werden: Jede Verschlüsselung ist grundsätzlich nur so gut wie das verwendete Kennwort. Es besteht immer die Gefahr eines so genannten „Brute Force-Angriffs", bei dem wahrscheinliche Passwörter einfach stupide durchprobiert werden. Ist das gewählte Passwort zu schwach, so ist es sehr wahrscheinlich, dass die Verschlüsselung auf diese Weise leicht zu brechen ist. Allgemein ist von der Verwendung von Wörtern, Geburtsdaten, Namen und ähnlichem abzuraten; eine probate Methode zum Generieren eines sicheren Passworts ist es, sich einen ganzen Satz auszudenken, der möglichst komplex ist und Zahlen enthält, beispielsweise: „Ich gehe um acht Uhr in die Vorlesung, da ist der Hörsaal immer leer!", und dann die Anfangsbuchstaben, Zahlen und Satzzeichen als Kennwort zu verwenden, im konkreten Beispiel also „Igu8UidV,didHil!" Während das Kennwort schwer zu behalten ist und sicher in keinem Wörterbuch auftaucht, so kann man sich den Merksatz doch leicht einprägen. Dieses Beispiel sollte natürlich nicht mehr verwendet werden.

Je mehr Personen von einem Kennwort wissen, desto höher ist die Wahrscheinlichkeit, dass das Passwort irgendwann kompromittiert wird. Idealerweise ist ein Kennwort genau einem einzigen Anwender bekannt und wird überhaupt nicht mit anderen Personen geteilt. In diesem Zusammenhang sei betont, dass beispielsweise Vertretungsregelungen und ähnliches auch nicht per se erfordern, Passwörter mehreren Personen bekannt zu machen. Viele der vorgestellten Produkte erlauben es, mehrere Kennwörter zu vergeben, mit denen eine Entschlüsselung erfolgen kann. Ein derartiger Ansatz ist dem Teilen von Passwörtern mit Dritten unbedingt vorzuziehen.

Separates Notebook für Dienstreisen

Verschlüsselung schützt letztlich nicht vor staatlichem Zugriff. Obwohl die Verschlüsselung auf technischer Ebene vermutlich in den allermeisten Fällen nicht angegriffen werden kann, wird im Zweifelsfall auf die Herausgabe des Kennwortes hingearbeitet werden. Zu beachten ist außerdem, dass in anderen Ländern durchaus die Verwendung von starker Verschlüsselung illegal sein kann. Gibt es also beispielsweise bei Auslandsdienstreisen Zweifel oder Befürchtungen, dass ernsthaftes Interesse daran besteht, an die fraglichen Daten zu gelangen, so hilft Verschlüsselung nicht weiter. Gerade in letzter Zeit wurde diesbezüglich über einige Staaten in der Tagespresse berichtet. Das KIT-CERT empfiehlt ohnedies ganz allgemein, für Dienstreisen ein separates Notebook zu benutzen, das ganz gezielt nur die allernötigsten Daten enthält und insbesondere nach jedem Einsatz komplett neu aufgesetzt wird. Dies ist beispielsweise im Institutsrahmen mit verhältnismäßig wenig Aufwand möglich. Dasselbe gilt in analoger Weise für Mobiltelefone und PDAs.

Bei der Verschlüsselung mobiler Datenträger, beispielsweise USB-Sticks oder mobilen Festplatten, ist zu bedenken, dass zum Entschlüsseln das Passwort eingegeben werden muss. Wird der Datenträger an einem fremden Rechner entschlüsselt, so besteht damit grundsätzlich die Gefahr, dass die Tastatureingaben protokolliert werden und das Kennwort damit kompromittiert wird. Es gibt zahlreiche Beispiele für Viren und Trojanische Pferde, die ein derartiges Verhalten zeigen; ein solches Protokoll ist also nicht unbedingt auf den Besitzer des fremden Rechners zurückzuführen.

Wird unter Beachtung dieser Grundregeln eine geeignete Form der Verschlüsselung angewendet, so kann das Risiko ungewollten Datenverlusts bereits wirkungsvoll gesenkt werden.

Zweite Datenablage empfehlenswert

Zur Vermeidung von Datenverlusten sollten die originalen Benutzerdaten unbedingt und regelmäßig auch mindestens noch an einer zweiten Stelle abgelegt werden. Dafür bietet das SCC die Datensicherung per TSM (Tivoli Storage Manager) an. Bei sensiblen Daten wird auch hierbei die Möglichkeit der Verschlüsselung empfohlen. Für ein Windows-System geschieht dies beispielsweise über folgende Anweisungen in der TSM-Options-datei „dsm.opt":

```
encryptkey        save
encryptiontype    aes128
include.encrypt   "d:\...\*"
```

Damit werden im oben genannten Beispiel alle zu sichernden Dateien des Laufwerks D über den TSM-Klienten mit dem bei der ersten Verwendung abgefragten Kennwort verschlüsselt und so im Backupsystem abgelegt. Der Benutzer muss auch hier seinen Schlüssel an sicherer Stelle aufbewahren, bei Verlust oder Vergessen kommt niemand mehr an die unverschlüsselten Daten.

Ab TSM Version 5.5.1 gibt es alternativ auch die Möglichkeit, dass das Verschlüsselungskennwort bei der ersten TSM-Sicherung dynamisch erzeugt und in verschlüsselter Form auf dem TSM-Server aufbewahrt wird. Um diesen Mechanismus verwenden zu können, ist in der TSM-Optionsdatei statt der Anweisung „encryptkey save" die Anweisung „encryptkey generate" zu verwenden.

Das KIT-CERT empfiehlt daher allgemein die Verwendung geeigneter Verschlüsselungsverfahren, wo immer dies möglich ist, steht bei Fragen und Problemen gerne zur Verfügung und bietet Unterstützung beim Einrichten von verschlüsselten Datenträgern.

Tobias Dussa, Wolfgang Preuß

Weitere Informationen

http://www.freeotfe.org
http://www.truecrypt.org
http://www.jetico.com
http://de.wikipedia.org/wiki/Festplattenverschlüsselung
http://www.bsi.de/gshb/deutsch/m/m04278.htm
http://testlab.sit.fraunhofer.de/content/output/project_results/bitlocker/BitLocker-Leitfaden.pdf
http://www.fzk.de/fzk/idcplg?IdcService=FZK&node=5302

Neuer CPU-Benchmark im Worldwide LHC Computing Grid

Wie viel Rechenleistung ist beim Grid Computing Centre Karlsruhe (GridKa) momentan verfügbar? Das ist eine häufig gestellte, aber nicht ganz einfach zu beantwortende Frage. Eine internationale Arbeitsgruppe hat jetzt einen neuen Standard erarbeitet, nach dem die großen Hochenergiephysik-Rechenzentren, allen voran die am LHC (Large Hadron Collider)-Projekt beteiligten Grid-Zentren, die von ihnen bereitgestellte CPU-Kapazität messen können. Das SCC war daran maßgeblich beteiligt.

Der Large Hadron Collider (LHC), der voraussichtlich im Spätsommer/Herbst 2009 am Europäischen Forschungszentrum CERN nach Reparatur erneut in Betrieb genommen werden soll, wird gewaltige Datenmengen produzieren. Um allen beteiligten Forschergruppen weltweit einen möglichst effizienten Zugriff auf diese Daten zu ermöglichen, wurde das Worldwide LHC Computing Grid (WLCG) gestartet. Im Rahmen dieses Grid-Projekts werden die LHC-Rohdaten an 12 weltweit verteilte Tier1-Rechenzentren verteilt, auf die wiederum eine Reihe von regionalen kleineren Zentren (Tier2) zugreifen können.

In Deutschland nimmt das vom SCC betriebene Grid Computing Centre Karlsruhe (GridKa) die Rolle des Tier1-Zentrums wahr [1]. Dazu sind zurzeit 4,3 PB (Petabyte, netto) an Plattensystemen installiert, knapp 5 PB sind auf Magnetbändern verfügbar, und daneben gibt es ein „großes“ PC-Cluster zur Auswertung der Daten (Stand: 1. Oktober 2008).

Genaues Messverfahren erforderlich

Apropos „groß“: Wie kann man die „Größe“ eines solchen Clusters messen? Die Anzahl der verwendeten Rechnerschränke (30 bis 35) mag für den Außenstehenden zwar recht anschaulich und verständlich sein, ist aber sicher kein aussagekräftiges Maß. Die Zahl der Systeme (rund 1.100) auch nicht, denn aufgrund der turnusmäßigen, in der Regel jährlichen Erweiterungen sind stets mehrere System-Generationen nebeneinander im Einsatz. Die zurzeit „langsamsten“ Knoten haben 2 Prozessoren mit jeweils 1 Kern (single-core), die schnellsten besitzen dagegen jeweils zwei 4-Kern-CPUs und sind damit um ein mehrfaches leistungsfähiger!

In einem internationalen Gemeinschaftsprojekt wie dem WLCG, in dem die Anforderungen an die von den beteiligten Zentren bereitzustellenden Ressourcen verbindlich festgelegt sind, ist ein wesentlich genaueres, reproduzierbares Messverfahren unbedingt notwendig. Dazu hat man sich auf die SPEC CPU-Benchmarks geeinigt.

Die 1988 von mehreren Workstation-Herstellern gegründete System Performance Evaluation Corporation, später in Standard Performance Evaluation Corporation (SPEC) umbenannt, hat sich das Ziel gesetzt, herstellerneutrale, leicht benutzbare Software zur Messung einer weiten Bandbreite von Systemkomponenten (so genannte Benchmarks) von der CPU-Performance über JAVA, File-, Mail- und Webserver, Grafikkomponenten, Hochleistungsrechner bis hin zur Stromaufnahme von Servern zu entwickeln [2].

WLCG setzt auf SPEC CPU-Benchmark-Suite

Von Anfang an setzte das WLCG auf die SPEC CPU-Benchmark-Suite (anfangs SPEC CPU95, zuletzt auf den Nachfolger SPEC CPU2000). Diese Suite besteht aus jeweils einem Satz von Integer-Benchmarks, welche die Ganzzahl-Rechenleistung der CPU bestimmen sowie Floating-Point-Benchmarks zur Ermittlung der vor allem in wissenschaftlichen Berechnungen wichtigen Gleitkomma-Rechenleistung. Es werden keine fertigen Binärpakete ausgeliefert, sondern die Quellprogramme, die erst vor Ort mit den vorhandenen Compilern in Maschinensprache übersetzt werden. Als Programmiersprache wurden C, C++ und Fortran verwendet.

Wegen der im Hochenergie-Physik (HEP)-Umfeld weitgehend dominierenden Ganzzahl-Berechnungen wurden im WLCG bisher nur die Integer-Benchmarks verwendet. Für viele Systeme sind in der Ergebnisdatenbank der SPEC (www.spec.org) zwar entsprechende, in der Regel von den Herstellern gemessene und veröffentlichte Performancedaten abrufbar. Jedoch wurden die dort veröffentlichten Ergebnisse von den Rechnerherstellern in der Regel in optimierten Systemumgebungen ermittelt und lassen sich nicht unmittelbar auf die bei den WLCG-Zentren installierte Systemumgebung übertragen. Um die Vergleichbarkeit und die Reproduzierbarkeit der Messungen zu garantieren, wurde deshalb seitens des WLCG Management Boards das Betriebssystem, in dem die Messungen vorzunehmen sind (= die von den Zentren installierte Linux-Distribution), der Compiler (bisher gcc-3.4) sowie die zu verwendenden Compiler-Optimierungsoptionen verbindlich vorgeschrieben.

Neuer Standard erarbeitet

Im Laufe der Zeit werden neue Rechnergenerationen immer schneller und mit immer mehr Hauptspeicher ausgestattet. Entsprechend wird die Anwendungssoft-

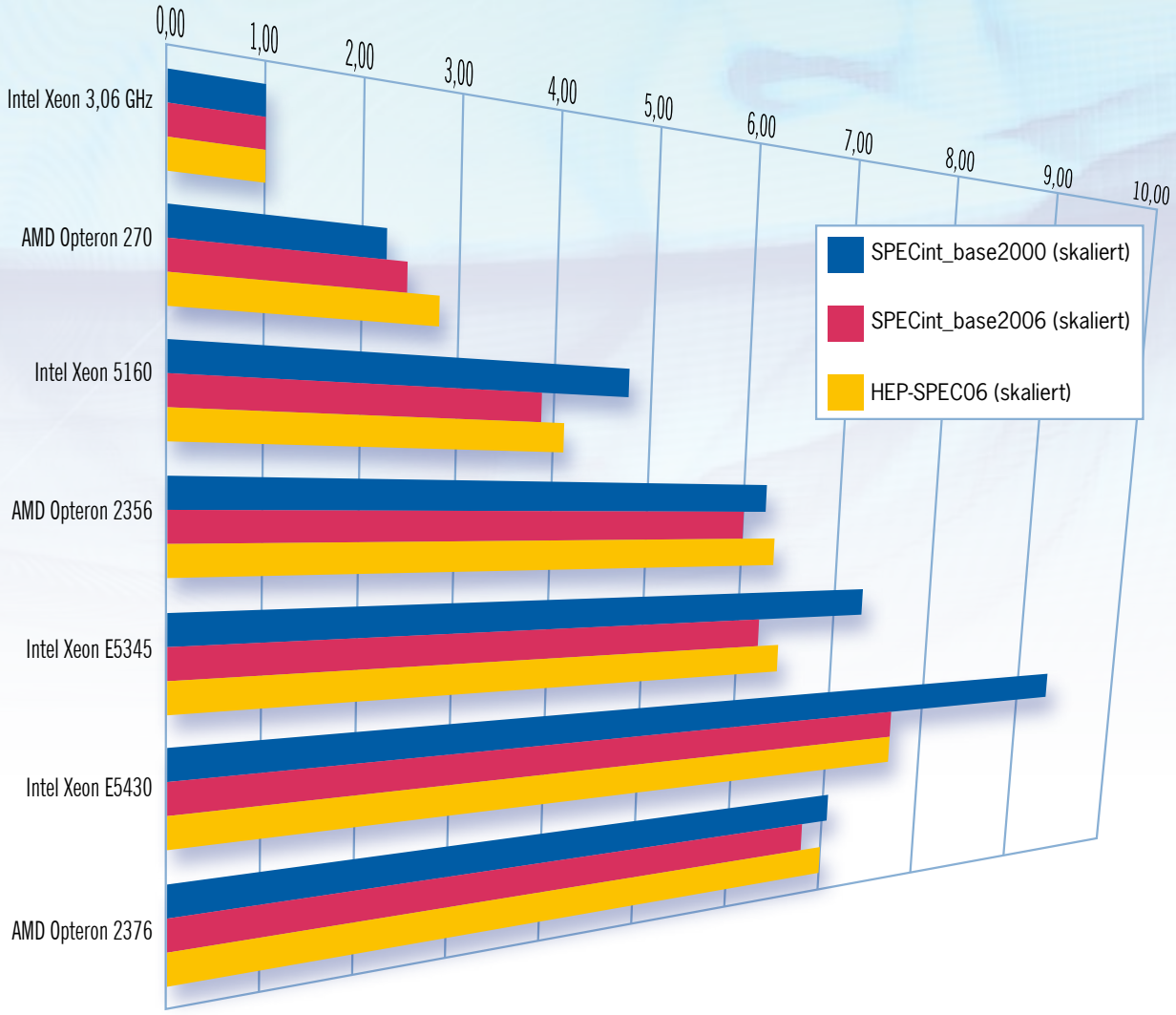


Abb. 1: Vergleichsstudie über die Skalierung verschiedener Varianten der SPEC-CPU-Benchmarks. Dabei wurden die Integer-Benchmarks der Suites SPEC CPU2000 und CPU2006 sowie der Satz der C++-Benchmarks (HEP-SPEC06) auf mehreren Generationen von Clustersystemen gemessen (s. Tabelle 1). Zur besseren Vergleichbarkeit ist jeweils das Verhältnis zum ältesten System (mit CPUs vom Typ Intel Xeon 3,06 GHz) dargestellt. Es fällt auf, dass der ältere Benchmark CPU2000 auf neueren Systemen, vor allem mit Intel-CPUs, deutlich bessere Performancedaten errechnet als der aktuelle CPU2006. Ursache sind die großen lokalen Caches der Intel-CPUs, in denen wesentliche Teile des Benchmarks Platz haben, so dass die vergleichsweise niedrige Zugriffsgeschwindigkeit der CPUs auf den Hauptspeicher nicht angemessen mit berücksichtigt wird. Systemumgebung: Scientific Linux 4, 32bit; Compiler: GNU Compiler Collection (gcc) 3.4; Compileroptionen: -O2 -pthread -fPIC.

ware immer umfangreicher und ressourcenhungriger. Die verwendeten Benchmarks müssen deshalb in regelmäßigen Abständen überprüft und angepasst werden.

2008 war es wieder so weit. Die HEPiX (High Energy Physics UNIX Interest Group) [3], an der nahezu alle großen HEP-Rechenzentren weltweit beteiligt sind, trifft sich zweimal jährlich zu einem einwöchigen Gedankenaustausch. Bei einem der letzten Treffen wurde eine Arbeitsgruppe gegründet, die nun einen aktuellen Standard erarbeitet hat [4, 5].

Dieser muss mehrere Anforderungen erfüllen. In erster Linie muss dieser Standard natürlich mit den Anwendungsprogrammen skalieren: Wenn die realen Rechenjobs (im Mittel) auf Rechner A 50 Prozent schneller sind als auf Rechner B, dann sollen auch die Benchmarkergebnisse für A etwa 50 Prozent besser sein als für B. Beim bisher verwendeten Benchmark auf der Basis des SPEC CPU2000 hat sich gezeigt, dass diese Skalierung zuletzt mit jeder neuen Rechnergeneration schlechter wurde. Ein wesentlicher Grund sind die immer weiter vergrößerten, schnellen CPU-Caches, in denen immer größere Teile des SPEC CPU2000 Platz finden, so dass die Leistungsfähigkeit der Anbindung der CPU an den Hauptspeicher immer weniger in die gemessene Gesamtperformance einfließt. Jedoch ist gerade das - neben der eigentlichen CPU-Architektur - ein wesentlicher Faktor.

Daneben muss ein Benchmark aber auch einfach anwendbar sein. Ein Quasi-Industriestandard wie die SPEC-Benchmarks ist dafür bestens geeignet. Die HEPiX Benchmarking Working Group hat sich für die aktuelle Benchmark-Suite SPEC CPU2006 entschie-

den, die insgesamt 29 Einzel-Benchmarks in 2 Sätzen enthält: 12 Integer-Benchmarks (genannt CINT2006) sowie 17 Floating-Point-Benchmarks (CFP2006) zur Ermittlung der vor allem in wissenschaftlichen Berechnungen wichtigen Gleitkomma-Rechenleistung. Davon sind 12 Benchmarks in der Programmiersprache C, 7 in C++ und 6 in Fortran geschrieben. Vier weitere Benchmarks verwenden sowohl C als auch Fortran.

Mehrere Varianten der aktuellen Suite SPEC CPU2006 – Integer-, Floatingpoint-Benchmarks sowie die Sammlung der in C++ geschriebenen Benchmarks – wurden auf allen derzeit vorhandenen Typen von Clustersystemen gerechnet und auf einigen Knoten auch mit mehreren relevanten HEP-Codes verglichen [6, 7]. Dabei hat sich gezeigt, dass sowohl die Integer- als auch die C++-Benchmarks sehr gut mit den HEP-Anwendungen skalieren. Deshalb fiel die Entscheidung letztendlich auf die C++-Variante, für die der Name HEP-SPEC06 gewählt wurde.

Und um noch einmal auf die ursprüngliche Fragestellung zurückzukommen: GridKa stellt momentan eine CPU-Kapazität von knapp 47.000 HEP-SPEC06 bereit — oder anschaulich ausgedrückt, rund 1.100 Cluster-Systeme mit zusammen rund 6.150 CPU-Kernen bei einer mittleren Rechenleistung von 7,64 HEP-SPEC06 pro Kern bzw. 42,7 HEP-SPEC06 pro Rechner!

Manfred Alef

Literatur

[1] SCC news 2, September 2008, S. 8
[2] http://www.spec.org
[3] https://www.hepix.org
[4] H. Meinhard: IHEPCCC/HEPiX Benchmarking WG Status Report. HEPiX Spring 2008, Genf (http://indico.cern.ch/getFile.py/access?contribId=44&sessionId=11&resId=2&materialId=slides&confId=27391)
[5] H. Meinhard: (IHEPCCC/)HEPiX Benchmarking Working Group Status Update. HEPiX Fall 2008, Taipeh (http://indico.twgrid.org/getFile.py/access?contribId=140&sessionId=91&resId=2&materialId=slides&confId=471)
[6] M. Alef: CPU Benchmarking at GridKa. HEPiX Fall 2008, Taipeh (http://indico.twgrid.org/materialDisplay.py?contribId=139&sessionId=91&materialId=slides&confId=471)
[7] M. Michelotto, M. Alef, M. Bly et.al.: A comparison of HEP code with SPEC benchmark on multicore worker nodes. CHEP 2009

Clustersystem	Taktfrequenz	Anzahl Cores pro CPU	Jahr der Inbetriebnahme
Intel Xeon 3,06 GHz	3,06 GHz	1	2004
AMD Opteron 270	2,00 GHz	2	2006 (Produktion)
Intel Xeon 5160 “Woodcrest”	3,00 GHz	2	2007 (Produktion)
AMD Opteron 2356 “Barcelona”	2,30 GHz	4	2008 (Testsystem)
Intel Xeon E5345 “Clovertown”	2,33 GHz	4	2008 (Produktion)
Intel Xeon E5430 “Harpertown”	2,66 GHz	4	2008 (Produktion)
AMD Opteron 2376 “Shanghai”	2,30 GHz	4	2009 (Testsystem)

Tab. 1: Hardwaredetails der in Abb. 1 dargestellten Clustersysteme.

Computernotfallteam für das KIT gegründet

Um als zentrale Anlaufstelle für das gesamte KIT im Bereich der IT-Sicherheit wirksam arbeiten zu können, hat die SCC-Abteilung IT-Security und Service-Management (ISM) das Computer Emergency Response Team des KIT (KIT-CERT) gegründet. Das KIT-CERT arbeitet sowohl präventiv als auch reaktiv. Einerseits werden mit Methoden der Einbruchs- und Schadsoftwareerkennung der Datenfluss vom und zum KIT auf eventuelle Angriffe hin untersucht und gegebenenfalls entsprechende Abwehrmaßnahmen eingeleitet, andererseits werden bei konkreten Vorfällen den Mitgliedern des KIT Unterstützung und Hilfe bei der Wiederaufnahme eines geregelten Betriebs sowie bei der Eindämmung und Beseitigung von Beeinträchtigungen durch Schadsoftware angeboten. Mit seiner Gründung hat das KIT-CERT die Aufgaben des SCC-Abuse-Teams übernommen.

Webseiten des CERT

Das KIT-CERT unterhält eigene Webseiten, auf denen auch Vorfälle aus dem Bereich der IT-Sicherheit mittels eines Webformulars gemeldet werden können. Die Webseiten sind erreichbar unter http://www.kit.edu/cert/. Falls die Meldung von Vorfällen über elektronische Formulare nicht möglich ist, kann auch auf eine Papier-Alternative zurückgegriffen werden.

Informationen des CERT

Das KIT-CERT betreibt eine Mailingliste, über die Informationen zum KIT-CERT versendet werden. Diese Liste ist öffentlich und kann von jedem abonniert werden (unter https://www.lists.kit.edu/sympa/info/cert-info). Warnungen zu akuten, KIT-relevanten Sicherheitsproblemen werden über die an beiden Standorten einschlägigen Kommunikationskanäle verteilt. Für den Campus Süd ist das die Mailingliste mit den Wartungsankündigungen (https://www.lists.uni-karlsruhe.de/sympa/info/wartung), für den Campus Nord existieren vier Mailverteiler, um die entsprechenden Mitarbeiter zu erreichen: Der IT-Expertenkreis, PC-Arbeitskreis, die LAN- sowie NT- Koordinatoren.

Kooperation mit anderen CERTs

Das KIT-CERT befindet sich derzeit in der Akkreditierungs- und Aufnahmephase in verschiedene CERT-Verbünde, um in engerer Zusammenarbeit mit anderen CERTs effizienter arbeiten zu können. Die dafür notwendigen Voraussetzungen wurden umgesetzt, entsprechende Anträge gestellt und die Aufnahmeprozesse eingeleitet, so dass mit einiger Zuversicht davon ausgegangen werden kann, dass die Mitgliedschaftsanträge in naher Zukunft positiv beschieden werden.

Kontaktinformationen des KIT-CERT

Die Kontaktinformationen des KIT-CERT können auf den Webseiten abgerufen werden. Daneben ist auch der PGP-Fingerabdruck der beiden Teamschlüssel einsehbar. Die Kontaktdaten des KIT-CERT sind folgende:

Telefonnummer: +49 721 608-5678
Faxnummer: +49 721 608-9030
Webseite: http://www.kit.edu/cert
E-Mail: cert@kit.edu
Ansprechpartner: Adrian Wiedemann, Tobias Dussa

PGP-Fingerprint: 69AF DA25 704D FD54 3BA1 C408 291D 553C D742 DE72
E-Mail: abuse@kit.edu
PGP-Fingerprint: FAE4 2005 21A6 9A39 A2AE E796 8331 4ABC 2885 1430

Das KIT-CERT stellt für die sichere Kommunikation per E-Mail PGP-Schlüssel bereit.

Adrian Wiedemann, Tobias Dussa

Das SCC stellt sich vor

In dieser Ausgabe: Die Abteilung Informationsdienste und Datenmanagement (IDA)

Foto: Ulrich Weiß

Rainer Kupsch studierte Mathematik und Physik an der Freien Universität Berlin. Seit März 1973 ist er als Wissenschaftlicher Mitarbeiter am Forschungszentrum Karlsruhe tätig. Zunächst arbeitete er in der Abteilung „Anwendungsunterstützung" mit Schwerpunkt Datenbanken, 1995 übernahm er die Leitung der Gruppe „Anwendungssysteme". Seit August 2002 war er Leiter der Abteilung „Datendienste, Anwendungen, Systemüberwachung und Infrastruktur (DASI)" sowie Stellvertreter des Institutsleiters am Institut für Wissenschaftliches Rechnen (IWR) am Forschungszentrum Karlsruhe. Mit der Gründung des SCC übernahm er die Leitung der Abteilung IDA.

(red)

Foto: Privat

Ulrich Weiß, stellvertretender Abteilungsleiter, absolvierte an der Universität Karlsruhe den Studiengang Informatik mit dem Ergänzungsfach Grafik Design, das er an der University of Oregon in Eugene, USA, studierte. Bereits während seiner Studienzeit arbeitete er im MicroBIT, dem Beratungs- und Informationsteam des Universitätsrechenzentrums. Direkt im Anschluss an sein Studium steuerte er maßgeblich den Aufbau des Internetauftritts der Universität Karlsruhe. Es folgten fünf Jahre Tätigkeiten als Geschäftsführer der PropackExpo GmbH, einer virtuellen Fachmesse im Bereich Prozess- und Verpackungstechnik, sowie die Position des technischen Leiters der Gruner & Jahr Computerchannel GmbH in Frankfurt und München. Seit seiner Rückkehr an das Universitätsrechenzentrum im Jahr 2002 koordiniert Ulrich Weiß mit der Einführung eines zentralen Content Management-Systems den Aufbau, die Struktur und Pflege der Internetauftritte und Portale der Universitätseinrichtungen. Seit 2008 leitet er die IDA-Gruppe „Web-, Informationsdienste und Portale (WIP)".

(red)

Foto: Ulrich Weiß

Jos van Wezel, stellvertretender Abteilungsleiter, studierte Biologie und Informatik an der Universität von Amsterdam in den Niederlanden. Zu Beginn seiner Berufstätigkeit arbeitete er im Bereich Systemadministration an der Vrije Universiteit. Von dort zog es ihn zum Forschungszentrum Karlsruhe, wo er seit sechs Jahren für Massenspeicher und Fileserver des Grid Computing Centre Karlsruhe (GridKa) verantwortlich ist. Seit der Restrukturierung am SCC leitet er zusätzlich die IDA-Gruppe „Data Access Data Management (DADM)", die komplexe Speichersysteme für Anwendungen und Benutzerservices auf dem KIT-Campus und für eine internationale Benutzergemeinde entwickelt, installiert und betreut.

(red)

Effiziente Datenhaltung, Datensicherung, nachhaltige Archivierung und ein ausgeklügeltes Datenmanagement zählen zu den Aufgaben der Abteilung Informationsdienste und Datenmanagement (IDA) unter der Leitung von Rainer Kupsch. Neben Informations-, Workflow- und Content Management-Systemen stehen Datenbanken und deren Anwendungen, Enterprise Search, Portalentwicklung und Webapplikationen sowie eine Organisationseinheiten übergreifende Dokumentverwaltung am KIT im Mittelpunkt des Leistungsspektrums der Abteilung.

Aufteilung in drei Gruppen

Diese Aufgabenschwerpunkte sind auch konsequent in den Gruppen der Abteilung IDA abgebildet. Die Gruppe Data Access Data Management (DADM) unter Leitung von Jos van Wezel ist für Datenmanagement mit Datensicherung zuständig, die Gruppe Datenbanken, Informationsmanagement und Anwendungen (DIA) mit der Gruppenleiterin Dr. Doris Wochele beschäftigt sich hauptsächlich mit der Ablage strukturierter Daten und der Abbildung von Prozessen. Portalentwicklungen, Webauftritte und -anwendungen fallen in die Zuständigkeit der Gruppe Web-, Informationsdienste und Portale (WIP) unter Leitung von Ulrich Weiß.

Die Abteilung IDA ist insbesondere an der Bereitstellung neuer Services für das SCC und KIT beteiligt. In diesem Zusammenhang sind vor allem ein gemeinsames SCC-Abrechnungssystem für IT-Services, die Erstellung eines Ticketsystems für das Service-Desk, der Betrieb der KIM-Portale sowie das SUN-Identitätsmanagement-System für KIM und das SCC zu nennen. Dabei finden integrative Aspekte und die Zusammenführung von zurzeit noch unterschiedlichen Prozessen und Verfahren am SCC-Süd und -Nord besondere Berücksichtigung. Daneben zeichnet sich noch in diesem Jahr ein neuer Schwerpunkt für die Abteilung IDA ab: Zusammen mit externen Partnern und anderen SCC-Abteilungen wird IDA die Federführung für die „Large Scale Data Facility (LSDF)“ übernehmen. Dabei geht es um Massendatenhaltung, Bereitstellung der Daten und Langzeitarchivierung für andere Wissenschaften außerhalb der Hochenergiephysik.

Installiert und betreut komplexe Speichersysteme: Die IDA-Gruppe DADM. (Von links, hintere Reihe): Dorin Lobontu, Verena Geißelmann, Stefan Waldecker, Iris Mayer, Dr. Doris Ressmann, Stephanie Böhringer, Jolanta Bubeline, Heinz Flemming; (von links, vordere Reihe) Xavier Mol, Martin Beitzinger, Dr. Christopher Jung, Dr. Silke Halstenberg, Jos van Wezel, Artem Trunov.
Foto: Ulrich Weiß

Data Access Data Management (DADM)

Die Gruppe DADM installiert und betreut komplexe Speichersysteme für Anwendungen und Benutzerservices auf dem KIT-Campus und für eine internationale Benutzergemeinde. Dabei wird auf über 15.000 Festplatten, 12.000 Bänder, 300 Server und 5 Bandroboter zugegriffen. Die von dieser Speicherumgebung erzeugte Netzwerklast wird in den kommenden Jahren auf 50 GByte/s steigen. Die 14 Mitarbeiter von DADM sind Spezialisten für die Datensicherungssoftware TSM, das globale Filesystem GPFS, die Datenmanagementsoftware dCache und SRM, das Storage Area Network (SAN) sowie vielfältige andere Speicherprotokolle und Systeme.

Gridspeicher für LHC-Massendaten

Für das am SCC angesiedelte Grid Computing Centre Karlsruhe (GridKa) wurde zur Haltung der Massendaten der Large Hadron Collider (LHC)-Experimente am CERN eine Speicherlandschaft von über 10 PByte aufgebaut. Die Grid-Schnittstellen SRM, GridFTP, xroot und das dCache-Datenmanagementsystem ermöglichen den weltweiten Zugang und Datenaustausch mit hunderten von Rechenzentren, die im Worldwide LHC Computing Grid Projekt (WLCG) zusammenarbeiten. Der Aufbau, die Betreuung und Skalierung der Grid Storage Services sind ständige Herausforderungen an die Innovationsfähigkeit der Gruppe. Das dCache-System steht im Zentrum einer der weltweit größten Speichersysteme dieser Art.

Seit einiger Zeit ist der Blick auch auf die optimale Speicherung von Daten anderer wissenschaftlicher Disziplinen gerichtet. Messungen in der Materialforschung, Fest-

körperphysik und Biologie erzeugen heutzutage riesige Datenmengen, die zunächst zur Bearbeitung gespeichert und später zur Referenz archiviert werden müssen: Eine Aufgabe, die sich DADM für die nahe Zukunft gestellt hat. Zusammen mit den beiden anderen IDA-Gruppen und weiteren Abteilungen des SCC und KIT werden Methoden entwickelt, um einen verlässlichen und sicheren Zugriff auf große Datenmengen zu gewährleisten.

Campus Backup, Archivierung und andere Daten-Services

Campusweit wird Benutzern die Möglichkeit geboten, Daten von ihren Rechnern (Server, Workstations und PCs) zentral auf einem Server im SCC über das Netz zu sichern. Dabei werden alle gängigen Betriebssysteme unterstützt. Die Speicherung erfolgt auf einem der fünf Band-Roboter des SCC. In einigen Fällen hat das Zurückladen von versehentlich gelöschten Dateien schon die Arbeit von Wochen oder Monaten gerettet.

Zusätzlich betreut DADM das Storage Area Network (SAN). Dieses fasst verteilten Datenspeicher zu einem logischen Gesamtsystem zusammen und ermöglicht so einen flexiblen und optimalen Einsatz von teuren Speicherressourcen.

Datenbanken, Informationsmanagement und Anwendungen (DIA)

Die Gruppe DIA berät die Kunden des SCC in allen Fragen rund um das Informationsmanagement, um Arbeitsabläufe optimal zu unterstützen. Die Beratungsdienste beziehen sich u.a. auf die übersichtliche Strukturierung von Daten und Dokumenten, den Austausch von Datensätzen zwischen verschiedenen Systemen wie auch auf ereignisgesteuerte Prozessketten, Formatumwandlung und Weiterverarbeitung. Dabei kümmert sich DIA um die gesamte Prozesskette bzw. die vollständige Integration von Anwendungen in die vom SCC unterstützte IT-Infrastruktur: Vom Datenbank-Backend über den Applikationsserver, der Abbildung von Prozessen bis zum Design von Benutzeroberflächen. Das Know-How der Mitarbeiter erstreckt sich insbesondere auf die Gebiete:

- Datenbanken (Oracle, MS SQL-Server, MySQL)
- Workflow Applications
- Document Management Applications
- Formatkonvertierungen
- Development (PHP, Java)
- Application Design

Bei den Datenbanksystemen unterstützt DIA Clusterlösungen, um eine größtmögliche Verfügbarkeit zu garantieren. Beim Aufbau von Redundanzen wird verstärkt auf eine Verteilung der Ressourcen zwischen dem SCC-Süd und -Nord gesetzt. Auch die Ablage von unstrukturierten Daten oder multimedialen Objekten kann mit dem professionellen System Oracle Universal Content Management System (OUCM) optimal unterstützt werden. Darüber hinaus bietet DIA das Action Request System „Remedy“ an, mit dem innerhalb des SCC bereits viele Erfahrungen gesammelt sowie Anwendungen erstellt wurden. Zurzeit wird mit „Remedy“ die Programmierung des Ticket Systems für das ServiceDesk des SCC vorangetrieben.

Berät in allen Fragen rund um das Informationsmanagement: Die IDA-Gruppe DIA. (Von links, hintere Reihe): Doris Lang, Karin Schäfer; (von links, mittlere Reihe) Kamil Wisniewski, Larissa Reinacher, Carsten Rogge, Ronny Wörl; (vordere Reihe) Anja Langner, Dr. Doris Wochele.
Foto: IDA

Web-, Informationsdienste und Portale (WIP)

Web Content Management

Internetauftritte für Einrichtungen des KIT stellen einen Schwerpunkt der Gruppe WIP dar. Das Angebot beginnt bei der Erstberatung zu Strukturen und Inhalten, über technische Realisierungen bis hin zum Betrieb von Servern für Intranet- und Internetauftritte. Für die Umsetzung wird das Web Content Management-System RedDot angeboten.

Das RedDot CMS bringt eine sehr einfach zu bedienende Redaktionsoberfläche mit sich, bietet Unterstützung bei Erstellung und Abgleich multilingualer Auftritte sowie ein feingranulares Berechtigungskonzept inklusive frei definierbarer Workflows wie beispielsweise Chefredakteur-Funktionalität.

Berät KIT-Einrichtungen bei Internetauftritten: Die IDA-Gruppe WIP. (Von links, hintere Reihe): Ulrich Weiß, Heike Reichert, Tobias Zuber, Michael Philipp; (von links vordere Reihe) Hans-Peter Hör, Franziska Wandelmaier, Doris Heathman, Kerstin Schmidt, Sabine Glas.
Foto: Rolf Mayer

Mit Hilfe eigener Erweiterungen in gängigen Skriptsprachen (z.B. PHP) kann die Integration von dynamischen oder datenbankbasierten Inhalten in eigene Webseiten umgesetzt werden.

Für 2009 steht die Migration bestehender Uni bzw. FZK-Intranet-/Internetauftritte in die KIT-Strukturen auf dem Programm. Dieses soll für die KIT-OEs mit möglichst geringem manuellem Aufwand umgesetzt werden. Bestehende Internetauftritte werden auch weiterhin im Oracle UCM (ehemals Stellent) und RedDot CMS durch WIP unterstützt und betrieben.

Zum Auffinden wichtiger Informationen – nicht nur in den Internetauftritten, sondern auch für andere Ablagen wie Filesysteme, Mailboxen oder Groupwaresysteme – wird die Secure Enterprise Search (SES) von Oracle angeboten. Mit Hilfe dieser persönlich konfigurierbaren Suchmaschine ist eine individuelle systemübergreifende Suche realisierbar.

Webserver und Applikationen

Über den CMS-Betrieb hinaus offeriert WIP den Betrieb virtueller Webserver sowohl unter Linux (Apache) als auch unter Windows (IIS) sowie Unterstützung bei gängigen Webanwendungen, beispielsweise Wikis, Foren und Web-Programmiersprachen. Auch für die Entwicklung von Webauftritten von Partnerorganisationen bzw. -Projekten stehen Ressourcen zur Verfügung.

Für Portalfunktionalitäten werden diverse Application Server bzw. Servlet Container (zum Beispiel im Tomcat oder Sun Application Server) angeboten und unterstützt. WIP ist überdies für den technischen Betrieb der KIT-Portale „intra.kit.edu“ und „studium.kit.edu“ verantwortlich, bei denen Microsoft Office Sharepoint Server (MOSS) zum Einsatz kommen.

Für ein zentrales Identitätsmanagement am KIT wird der SUN Identity Manager (IDM) betrieben. WIP sichert den Betrieb sowie den Second Level Support für dieses KIT-weite Authentifizierungs- und Autorisierungssystem, das den Austausch und die Zuordnung von Identitätsinformationen bei sehr hohem Sicherheitsstandard ermöglicht.

Für die Erstellung des gesetzlich vorgeschriebenen Gefahrstoffkatasters muss am KIT der Chemie-Assistent ChemA verwendet werden. Er unterstützt die Mitarbeiter in Laboren und Lagern bei der Verwaltung von Gefahrstoffen, indem alle bereits vorhandenen digitalen Daten übernommen werden, wie beispielsweise die entsprechenden Datensätze von SAP-Bestellungen. Bei WIP liegt die Verantwortung für die Entwicklung von ChemA, deshalb können umfassende Beratungs- und Supportleistungen angeboten werden.

Lehr- und Lernplattform

Zur Unterstützung der Lehre steht die Plattform ILIAS zur Verfügung, über die zum Beispiel Dokumente, Medieninhalte und Kommunikationswerkzeuge bereitgestellt, der Übungsbetrieb abgewickelt oder Selbsttests für die Studierenden angeboten werden können. Der Service umfasst sowohl die Betreuung der Studierenden als auch der Dozenten bei technischen Problemen und Fragen.

Rainer Kupsch, Ulrich Weiß, Jos van Wezel

SCC stellt Offline-Patches für Windows bereit

Das SCC stellt ab sofort sicherheitsrelevante Aktualisierungen für Betriebssysteme aus dem Hause Microsoft über ISO-Abbilder von DVDs bereit. Im Rahmen des Patch-Managements des SCC-Nord und -Süd wurden bereits Aktualisierungen zur Verfügung gestellt, diese waren jedoch in der aktuellen Form nur online über den an den jeweiligen Standorten betriebenen Windows Server Update Service (WSUS) bzw. über den System-Management-Server (SMS) verfügbar. Mögliche ISO-Abbilder wurden bisher nur auf Anfrage von Nutzern erzeugt.

Seit Beginn dieses Jahres sind die ISO-Abbilder in tagesaktueller Form über die Webseiten (s. u.) des SCC verfügbar. Damit ist gewährleistet, dass Aktualisierungen, die außerhalb des monatlichen Patchdays veröffentlicht werden, auch in einer Offline-Version zeitnah zur Verfügung stehen. Derzeit werden die ISO-Abbilder für folgende Betriebssystem-Varianten erzeugt:

- Windows 2000 (alle Editionen)
- Windows XP 32bit (alle Editionen)
- Windows Server 2003 32bit (alle Editionen)
- Windows Server 2003 64bit (alle Editionen)
- Windows Vista 32bit (alle Editionen)
- Windows Vista 64bit (alle Editionen)
- Windows Server 2008 32bit (alle Editionen)
- Windows Server 2008 64bit (alle Editionen)

Es sollte beachtet werden, dass bis Windows Server 2003 die Aktualisierungen sprachabhängig waren, aus diesem Grund müssen für verschiedensprachige Versionen der Betriebssysteme gegebenenfalls mehrere Abbilder heruntergeladen werden. Aktuell werden die Abbilder für die deutsche und englische Sprachversion von Windows erzeugt. Ab der Veröffentlichung von Windows Vista sind die Kernkomponenten sprachunabhängig gestaltet, so dass hier ein Abbild für alle Sprachversionen ausreichend ist.

Das ISO-Abbild mit den Offline-Aktualisierungen ist aufgrund von lizenzrechtlichen Einschränkungen nur innerhalb des KIT verfügbar. Besteht jedoch Bedarf an weiteren Sprachversionen, können diese auch auf Anfrage zur Verfügung gestellt werden. Die Erweiterung des Dienstes auf die Bereitstellung von Aktualisierungen für Office-Anwendungen wird geprüft. Abbilder der DVDs sind auf den Webseiten des SCC abrufbar (www.rz.uni-karlsruhe.de/sl/offline-cd), des Weiteren existiert ein Smartlink mit dem Namen „offline-cd“. Falls einige Kunden keine Möglichkeit haben sollten, aus den Abbildern eine DVD zu erstellen, kann das ServiceDesk des SCC auf dem Campus Süd (Tel. 0721/608-8000) bzw. Nord (Tel. 07247/82-8000) behilflich sein.

Adrian Wiedemann

Greylisting testweise auf Campus Süd aktiviert

Spam-Flut deutlich reduziert

Ende Januar wurde für den Campus Süd kurzfristig das allgemeine Greylisting aktiviert, um die Spam-Flut deutlich zu reduzieren. Bei diesem Verfahren werden, vereinfacht ausgedrückt, Mails mit bisher unbekannter Kombination von Absender, Empfänger und IP-Adresse zunächst abgelehnt und bei erneutem Zustellversuch akzeptiert. Auf dem Campus Nord wurde dieses Verfahren durch Vorstandsbeschluss bereits im Frühjahr 2008 allgemein eingeführt, während im Süden den Einrichtungen nur nahe gelegt worden war, sich dafür zu entscheiden.

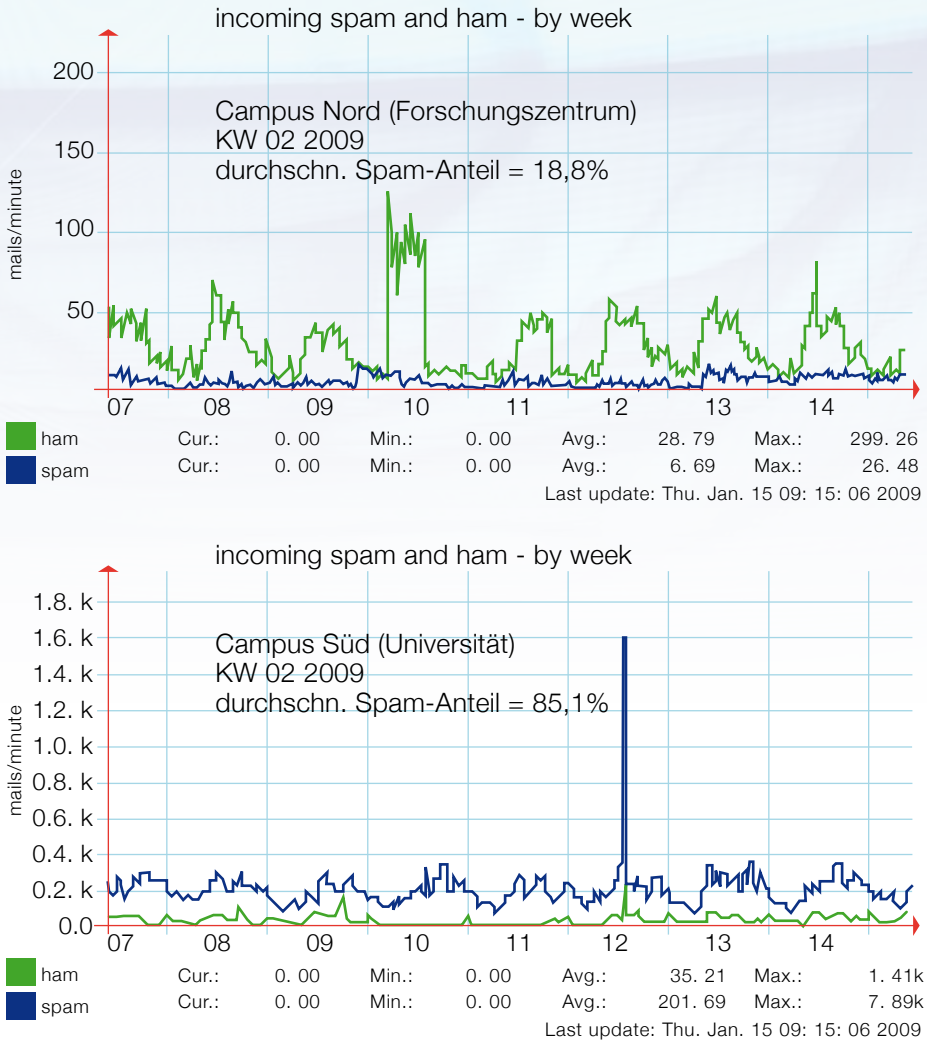


Abbildung 1: Verhältnis Nutzmails (Ham, grün) zu Spam (blau) am Campus Nord (oben) im Vergleich zum Campus Süd (unten).

Dies hatte sich so ausgewirkt, dass auf dem Campus Nord der Spam-Anteil generell unter 20 Prozent lag, während er auf dem Campus Süd immer 80 Prozent überschritt. Dabei waren folgende negative Auswirkungen auf den Mailbetrieb festzustellen:

- In der Kalenderwoche 5/2009 gerieten beide smtp-Server des Campus Süd auf eine Black List, dadurch konnten Mails zumindest über einen Provider nicht mehr zugestellt werden und gingen verloren. Nicht wenige Benutzer leiten Ihre Mails an eine Mailbox bei einem externen Provider weiter, wobei dann auch der gesamte Spam weiter geleitet wird. Ist der Anteil zu hoch, dann gehen mehr und mehr Provider dazu über, solche Sende-Domains für eine gewisse Zeit abzublocken.
- Die Spam-Filter des SCC müssen durch die Benutzer aktiviert werden, dabei beträgt die standardmäßige Vorhaltezeit für Spam 42 Tage. Durch den wachsenden Spam-Anteil und die lange Vorhaltung auf dem Campus Süd treten regelmäßig Engpässe im Festplatten-Spoolbereich auf. Dies führt zu einem Mehrbedarf an Festplatten-platz und notwendigen manuellen Eingriffen.

Durch Greylisting werden der Spam-Anteil und die damit verbundenen Nebenwirkungen deutlich verringert, ohne dass es beispielsweise auf dem Campus Nord bisher zu negativen Effekten oder Beschwerden kam.

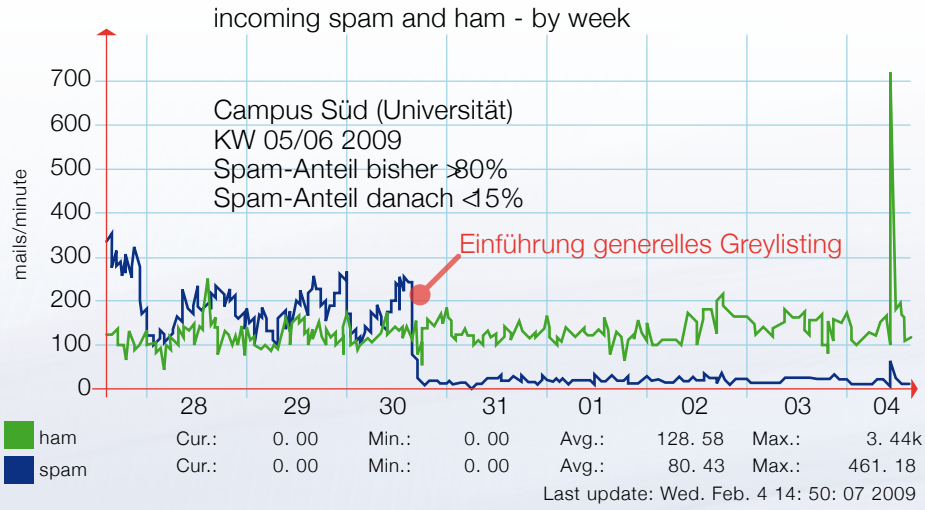


Abbildung 2: Auswirkung der Einführung des allgemeinen Greylistings auf den Spamanteil.

Anhand der Abbildung 2 ist die Wirksamkeit des seit Ende Januar an der Universität allgemein aktivierten Verfahrens zu erkennen: Die Zahl der Spam-Mails hat seitdem signifikant abgenommen.

Spam-Versender unternehmen in der Regel keinen weiteren Zustellungs-versuch, wie er nach RFC 2821 (Request for Comments, eine internationale Übereinkunft, hier zur Mailwiederholung) vorgeschrieben ist. Das SCC beobachtet jetzt das im Campus-Süd-Bereich generell aktivierte Verfahren genau und wird bei durchgehend positiven Erfahrungen beim KIT-Vorstand die allgemeine und unbefristete Freigabe des Greylistings beantragen. In der Sitzung vom 17.2.2009 wurde diese Vorgehensweise vom Ausschuß für Datenverarbeitung (AfD) bereits befürwortet.

Wolfgang Preuß

Weitere Informationen
http://www.rz.uni-karlsruhe.de/download/rznews_04_2007.pdf

SCC baut KIT-weite Bürokommunikationsinfrastruktur auf

Um die Zusammenarbeit am KIT auch durch eine entsprechende IT-Infrastruktur zu unterstützen, baut das SCC derzeit eine KIT-weite Bürokommunikationsumgebung auf.

Am KIT-Nord existiert seit langem eine auf Microsoft Windows basierende, zentral betreute Bürokommunikationsumgebung. Hier werden Dienste wie Benutzerkonten, Datenablagen, Postfächer und Kalender mit Hilfe eines gemeinsamen Verzeichnisdienstes, dem Active Directory (AD), angeboten. Das Active Directory besteht aus der zentralen Domäne FZKA und fünf weiteren Domänen, die auf spezielle Ansprüche einzelner Organisationseinheiten zugeschnitten sind.

Am KIT-Süd gibt es ebenfalls seit vielen Jahren eine auf Microsoft Windows aufgebaute Bürokommunikationsumgebung mit ähnlichem Serviceangebot. Das gemeinsame Verzeichnis umfasst ca. 60 Domänen, die häufig durch Administratoren der einzelnen Institute oder Fakultäten betreut werden. Nicht alle Benutzer nehmen die zentral angebotenen Postfach- und Kalender-Dienste an, die zum Beispiel Terminvereinbarungen deutlich vereinfachen können.

Um die Zusammenarbeit am KIT wesentlich zu erleichtern, baut das SCC derzeit eine KIT-weite Bürokommunikationsumgebung auf Basis der bewährten Dienste Microsoft Active Directory, Microsoft Exchange und Microsoft Office Sharepoint Server neu auf. Entsprechend dem Beschluss des KIT-Senats wird das zugrunde liegende Verzeichnis „kit.edu“ aus Sicherheitsgründen zentral vom SCC als einzelne AD-Domäne betreut.

Einige der in diesem Kontext angebotenen Dienste werden bereits seit längerem genutzt: Die Portale „https://intra.kit.edu“ und „https://studium.kit.edu“ sowie die Team-Portale unter „https://team.kit.edu“ bauen auf der zentralen AD-Domäne „kit.edu“ auf. Die Benutzer melden sich dort mit ihrer neuen Kennung „vorname.nachname@kit.edu“ an. Auch der Mailerreichbarkeitsdienst an die E-Mail-Adresse „vorname.nachname@kit.edu“ ist realisiert. Im Aufbau befinden sich derzeit noch die Dienste der zentralen Postfach-Umgebung samt Kalender und zentraler Datenablage.

Um eine möglichst hohe Ausfallsicherheit zu erreichen, ist das SCC bestrebt, die Dienste redundant aufzusetzen. So stehen die Server zur Authentifizierung (Domänencontroller) an beiden Standorten zur Verfügung. Die Mailserver-Landschaft sieht vor, dass bei einem Ausfall eines Servers am KIT-Süd sofort der entsprechende Server am KIT-Nord die Aufgaben reibungslos übernimmt. Dasselbe gilt im umgekehrten Falle. Eine entsprechende Funktionalität gibt es auch für die Dienste Datenablage und Portaldienst.

Die Standortverbindung soll ebenfalls kein Nadelöhr darstellen. Campus-Nord und Süd werden durch zwei Glasfaser-Leitungen verbunden. Diese werden zunächst mit zwei mal 10 Gigabit Ethernet und sechs mal 4 Gigabit Fibre Channel aufgebaut.

Kerstin Schmidt

Vielfältige Möglichkeiten mit dem KIT-Benutzerkonto

Nach Einrichtung der Benutzerkonten in Form von „vorname.nachname@kit.edu“ ermöglichte das SCC in einem ersten Schritt die Erreichbarkeit über eine E-Mail-Adresse mit der Endung „@kit.edu“. Inzwischen wurden noch weitere Dienste aufgebaut. Unter der Web-Adresse https://intra.kit.edu kann nun das Kompetenzportfolio abgerufen, das KIT-Kommunikationsforum mit Fragen gefüttert oder im Alias-Portal ein E-Mail-Alias beantragt werden. Darüber hinaus können mit Hilfe des KIT-Benutzerkontos Dienste, wie zum Beispiel ein Teamportal zur optimierten Zusammenarbeit in einer über beide Standorte verteilten Arbeitsgruppe genutzt werden. Bei auftretenden Problemen in Zusammenhang mit dem Benutzerkonto hilft das ServiceDesk des SCC (Tel.: 608-8000) gerne weiter.

Kerstin Schmidt

Foto: Privat

Prof. Dr. Adolf Schreiner feiert 80. Geburtstag

Prof. Dr. Adolf Schreiner, emeritierter Ordinarius für Informatik und langjähriger Direktor des Rechenzentrums der Universität Karlsruhe (TH), feierte am 4. April seinen 80. Geburtstag. In seiner Amtszeit von 1972 bis 1998 entwickelte er das URZ zu einem der größten und leistungsfähigsten Rechenzentren in der Bundesrepublik. Bereits Anfang der 80er Jahre verfügte das Karlsruher Universitätsrechenzentrum als eines der ersten über einen Supercomputer, und über viele Jahre gab es in Karlsruhe den größten Supercomputer an europäischen Hochschulen.

Prof. Schreiner zählte auch zu den Pionieren der lokalen Hochgeschwindigkeitsglasfaser-Vernetzung in Europa und führte bundesweit als erster Computer-Hörsäle großen Stils ein. Als Mitglied der Kommission für Rechenanlagen der Deutschen Forschungsgemeinschaft gestaltete er die Entwicklung der deutschen Informationstechnologie maßgeblich mit. Der „vernetzte Campus“, die „informatisierte Universität“ waren in den 80er Jahren zu prägenden Begriffen für die Förderprogramme in der ganzen Bundesrepublik geworden. Das Kooperationsprojekt „HECTOR“ mit IBM, zu dessen beiden Leitern Prof. Schreiner gehörte, brachte nicht nur Hunderte von PCs an die Universität, sondern war auch die Grundlage für das heute flächendeckende Campus-Netz.

Mit der Gründung der Akademischen Software Kooperation (ASK) 1989 trug er der unbefriedigenden Versorgung deutscher Hochschulen mit Lehrsoftware Rechnung. Heute ist die asknet AG ein weltweit erfolgreich operierendes Unternehmen im Bereich Online-Shop-Lösungen. Das Rechenzentrum baute Prof. Schreiner kontinuierlich zu einem überregionalen, hochqualifizierten Dienstleistungs- und Kompetenzzentrum aus, das nicht nur den einzelnen universitären Institutionen und einer externen Nutzerschaft Spitzentechnologie und Spezialservices bedarfsorientiert anbot, sondern auch Vorreiterfunktionen im Hinblick auf neue Technologien übernahm.

Seine Kollegen und Freunde sowie alle Mitarbeiterinnen und Mitarbeiter des SCC wünschen ihm und seiner Familie noch viele glückliche und erfüllte Lebensjahre.

Prof. Dr. Wilfried Juling

Notepad++ statt UltraEdit für Windows-Umgebungen

Das SCC-Süd hat seit etlichen Jahren über die asknet AG eine Campuslizenz für den Texteditor UltraEdit im Angebot. Allerdings hatte sich die Herstellerfirma bisher dagegen gewehrt, diese Software im Rahmen der Campuslizenz auch für Studierende und Mitarbeiter auf deren Privatrechnern zur Verfügung zu stellen. Bei den jüngsten Verhandlungen konnte in diesem Punkt zwar ein Fortschritt erzielt werden, jedoch nur zu im Voraus definierten Stückzahlen, nicht in Richtung einer unbeschränkten Campuslizenz zu einem Pauschalpreis. Bei einem solchen Abschluss hätten sich im Vergleich zu bisher deutlich höhere Jahresgebühren ergeben.

Das SCC hat sich daher nach einem alternativen System umgesehen, das einheitlich auf allen Rechnern von Campus-Nord und -Süd, in den Ausbildungspools und auf den Privatrechnern von Studierenden und Mitarbeitern eingesetzt werden kann und einen in etwa vergleichbaren Funktionsumfang wie UltraEdit bietet. Als Ergebnis dieser Suche schlägt das SCC seinen Kunden jetzt den Text- und Programmeditor Notepad++ zur Nutzung für Windows-Umgebungen vor. Dabei handelt es sich um eine bei einem Sourceforge-Projekt unter GPL (GNU General Public License) entstandene Software, die für kleinere Entwicklungsprojekte sehr verbreitet eingesetzt und auch stetig weiter entwickelt wird. Zufriedene Benutzer haben natürlich die Möglichkeit, dem Hauptentwickler eine kleine Spende zukommen zu lassen.

Wolfgang Preuß

Weitere Informationen und Download
http://notepad-plus.sourceforge.net/de/site.htm

IT-Sicherheitsexperte der Bundeswehr hielt Vortrag am SCC

Der Gruppe IT-Sicherheit der SCC-Abteilung IT Security and Service Management (ISM) ist es im September letzten Jahres gelungen, den international sehr gefragten Redner Oberstleutnant Volker Kozok vom Bundesministerium der Verteidigung für einen zweistündigen Vortrag an das KIT einzuladen.

Kozok ist derzeit Beauftragter für den Datenschutz der Bundeswehr. Vor dieser Tätigkeit hatte er das Computer Emergency Response Team (CERT) der Bundeswehr konzipiert, aufgebaut und jahrelang geleitet.

In seinem interessanten Vortrag präsentierte Kozok einen Streifzug durch die gesamte Welt der aktuellen IT-Bedrohungen im Internet. Einschlägige Beispiele für schwerste Verletzungen von Persönlichkeitsrechten wurden ebenso gezeigt und erläutert wie aktuelle Bedrohungen im Bereich der IT-Spionage durch Viren, trojanische Pferde und andere Schadsoftware. Der Vortrag endete in einer lebhaften Diskussion über verschiedene Aspekte der IT-Sicherheit.

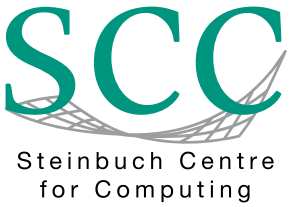
Tobias Dussa

Stand des SCC auf der SC08 in Austin/Texas.
Foto: SCA

SCC auf der Internationalen Supercomputing Conference SC2008 in Austin/Texas

Die jährlich stattfindende Konferenz ist eine der renommiertesten Veranstaltungen im Bereich „High Performance Computing“ (HPC) und ermöglicht Spitzenwissenschaftlern aus Forschung, Industrie und Wirtschaft, ihre Erfahrungen und Visionen auszutauschen. Aber auch Themen wie Grid und Cloud Computing sowie Storage und Netzwerkumgebungen bildeten Schwerpunkte. Mit insgesamt etwa 11.000 Teilnehmern zählte die Veranstaltung im November letzten Jahres zu den Höhepunkten in der 21-jährigen Geschichte der SC (http://www.supercomp.org/). Das SCC war zum siebten Mal auf der Supercomputing Conference in den USA vertreten und präsentierte innovative Projekte und Infrastrukturlösungen aus dem HPC-Bereich.

(red)



Steinbuch Centre for Computing (SCC)
76128 Karlsruhe
Tel: 0721/608-3754 oder 07247/82-5601
E-Mail: scc@kit.edu

www.scc.kit.edu