

ÄNDERUNG BEIM SSH-ZUGANG IN DAS FZK-INTRANET

SSH (Secure Shell) ist ein Programm und Protokoll, mit dessen Hilfe man sich als Benutzer auf einem entfernten Computer anmelden und dort Programme ausführen kann. Mit dem zur SSH-Protokollfamilie gehörenden Programm SCP (Secure Copy) können Dateien zu oder von einem entfernten Computer kopiert werden. Der Namenszusatz „Secure“ rührt daher, dass die gesamte Datenübermittlung (insbesondere auch Benutzername und Passwort beim Anmeldevorgang) verschlüsselt erfolgt.

Ein Rechner bietet den SSH-Dienst standardmäßig auf Port 22 des Netzwerkprotokolls an. Im Rahmen des virtuellen Rechenzentrums wurde zwischen Forschungszentrum und Universität Karlsruhe zusätzlich Port 24 als weiterer SSH-Port vereinbart. Bei der Einführung der zentralen Firewall zwischen Internet und FZK-Intranet wurden diese beiden Zugänge generell, das heißt von jedem Rechner weltweit auf jeden an das FZK-LAN angeschlossenen Rechner, offen gelassen. Als Reaktion auf die Zunahme von Angriffen aus dem Internet mit dem Ziel, über SSH unberechtigten Zugang zu Rechnern zu erlangen, wurde aber 2002 der Zugang über Port 22 gesperrt. Die generelle Zugangsmöglichkeit über Port 24 blieb bestehen, da sich die Angriffe auf den Standard-Port 22 konzentrierten.

Wegen der weiter stetig steigenden Zahl von automatisierten Angriffen aus dem Internet sehen wir in der generellen Öffnung von Port 24 mittlerweile ebenfalls ein großes Gefahrenpotential. **Daher wurde mit Zustimmung des IT-Expertenkreises beschlossen, die generelle Öffnung der Firewall für Zugriffe auf Port 24 am 26. März 2007 zu entfernen und durch eine bedarfsgerechte Freischaltung einzelner Rechner zu ersetzen.**

Zur Beantragung einer solchen Freischaltung genügt eine E-Mail mit Kenntnisnahme des zuständigen LAN-Koordinators, in der Sie die IP-Adresse Ihres Rechners und den gewünschten SSH-Port (22 oder 24) angeben. Dabei empfehlen wir Ihnen, nach Möglichkeit weiterhin Port 24 zu verwenden, da er wesentlich seltener angegriffen wird. Falls der Zugang nur für wenige bekannte Rechner im Internet bestimmt ist (z.B. für eine Partneereinrichtung), lässt sich die Freischaltung entsprechend einschränken. Voraussetzung zur Durchführung der Freischaltung ist, dass der Rechner eine feste IP-Adresse besitzt und der SSH-Dienst sicher konfiguriert ist. Hierzu führen wir Sicherheitstests durch, in denen wir gängige Angriffe aus dem Internet simulieren. Hinweise zum sicheren Betrieb des SSH-Dienstes haben wir unter <http://iwr-sicherheit.fzk.de/html/Dienste/SSH> zusammengestellt.

Eine Alternative zur Freischaltung Ihres Rechners in der Firewall ist die Nutzung unseres Dienstes „Citrix Web Access“. Er bietet den SSH-Zugang über einen Browser an, der daher praktisch von jedem Internet-

DER IWR-SERVICE-KATALOG FÜR 2007

Der Service-Teil des IWR, der für die OEs des Forschungszentrums vielfältige IT-Dienste bereit hält, unterliegt der Budgetierung. Das bedeutet, dass die OEs mit Mitteln aus ihrem Budget die jeweils benötigte IT-Infrastruktur bedarfsgerecht im IWR beziehen können. Das IWR hat alle angebotenen IT-Services in einem Katalog zusammengefasst, der auch für alle Services die zugehörigen Preise ausweist.

Grundsätzlich orientieren sich die vom IWR für das Erbringen der Services verrechneten Preise an den Kosten, die das IWR für das Vorhalten und Erbringen dieser Dienste aufwenden muss. In den allermeisten Fällen ergeben sich so Preise, die günstiger sind als vergleichbare Marktpreise außerhalb des Zentrums. Für 2007 konnten wir die Preise an einigen Stellen deutlich senken, nur bei den IP-Adressen ließ sich eine Preiserhöhung leider nicht vermeiden.

CPU-Leistung: Eine CPU-Stunde des Ende 2006 neu beschafften Vektorrechners NEC-SX8-8R kostet 14,- €, ab der 41. CPU-Stunde pro Benutzer und Monat nur noch 6,- €. Die bisherigen Vektorrechner VPP5000 und NEC-SX5 werden voraussichtlich Ende Februar stillgelegt.

IP-Adressen: Pro IP-Adresse und Monat werden 20,- € berechnet. Hier wurde eine moderate Preiserhöhung erforderlich, um die im FZK extrem gute und hochverfügbare Verbindung zum Internet auch weiterhin sicherzustellen. Außerdem wurde das FZK-Datennetz zur Erhöhung der Ausfallsicherheit redundant ausgelegt, was mit zusätzlichen Kosten verbunden ist. Großverbraucher erhalten bei den IP-Adressen einen Rabatt von 10 Prozent.

Datenarchivierung: Hier wurden alle Preise gegenüber 2006 um 50 Prozent gesenkt. Sie liegen nun – je nach Datenmenge – zwischen 0,75 € / GB / Monat und 0,05 € / GB / Monat.

WWW-Portale: Das Bereitstellen eines Portals im Share Point Portal Service kostet ab 2007 nur noch 50,- € / Monat; dieser Preis konnte gegenüber dem Vorjahr um zwei Drittel gesenkt werden.

Der ausführliche [IWR-Service-Katalog](#) (1), der alle Services des IWR und alle Preise enthält, ist im IWR-Sekretariat erhältlich und auch im Internet verfügbar (www.fzk.de/iwr)

Klaus - Peter Mickel, ☎ 5600

Anschluss aus möglich ist. Dabei verbleibt Ihr Rechner vollständig geschützt hinter der Firewall.

Anträge und Fragen betreffend der Firewall richten Sie bitte an Firewall@iwr.fzk.de.

Norbert Lehmann, ☎ 6586

SX-8R VEKTORRECHNER LÖST DIE SYSTEME FUJITSU/SIEMENS VPP5000 UND NEC SX-5 AB

Anfang Februar ist es soweit! Der SX-8R Vektorrechner kann in den Produktionsbetrieb übernommen werden. Da alles etwas anders ist als beim VPP5000 wird es vom 5.2.-7.2.2007 eine Benutzerschulung mit praktischen Übungen geben. Anmeldungen zur Schulung bitte an Frank.Schmitz@iwr.fzk.de. Sinnvollerweise sollte vorher eine Benutzernummer eingetragen sein. Falls noch kein Account für SX-5 oder VPP5000 existiert, diesen bitte mit dem entsprechenden [Formular](#) (2) beantragen.

Agenda	
Monday (5.2.)	
14:00 – 16:00	Theory I (SX architecture overview and basics on vectorization)
<i>coffee break</i>	
16:30 – 18:00	Theory II (Vectorization and optimization examples, libraries)
Tuesday (6.2.)	
9:00 – 10:30	Theory III (Indirect addressing, performance analysis/tools, tuning your code)
<i>coffee break</i>	
10:45 – 12:15	Practice I (Optimization example, work on user codes)
<i>lunch break (local arrangements)</i>	
13:00 – 14:30	Theory IV (Most important compiler switches)
<i>coffee break</i>	
15:00 – 18:00	Practice II (Optimization example, continue work on user codes)
Wednesday (7.2.)	
09:00 – 10:30	Theory V (Parallelization – OMP and MPI)
<i>coffee break</i>	
11:00 – 12:30	Practice III (Final work on user codes)

Frank Schmitz, ☎ 5632

NEUER SPAMFILTER IM FZK?

Im Dezember informierten wir Sie, dass zum Jahreswechsel die neue Version unseres Spamfilters installiert wird. Im Vorfeld zur Versionsänderung wurde die Software von uns auf Herz und Nieren geprüft und für gut befunden.

Soweit die Theorie... Die Software, die uns dann geliefert wurde, entsprach nun leider nicht in allen Punkten der getesteten, so dass es nach dem Einspielen der Software zu massiven Leistungseinbußen kam.

Diesen Zustand wollten wir natürlich so nicht lassen. Aus diesem Grund sind wir vorerst auf die bisherige Softwareversion zurückgegangen und stehen nun mit der Lieferfirma in engem Kontakt, damit die nachgebesserte Version unseren Anforderungen wieder genügt.

Wir bedauern diesen Umstand und hoffen, Ihnen die versprochenen Funktionalitäten bald zur Verfügung stellen zu können.

Kerstin Schmidt, ☎ 4501

SPYBOT WURMPROBLEMATIK IM FORSCHUNGSZENTRUM

Seit dem 11. Dezember letzten Jahres kursiert im Intranet des Forschungszentrums eine Variante des Spybot Wurmes. Nachdem klar wurde, dass sich die Wurmproblematik nicht auf einzelne Systeme beschränkt, sondern sich im Netzwerk schnell verbreitet, haben wir sofort reagiert und am gleichen Tag

die Personenkreise informiert, die mit der Systemadministration im Zentrum betraut sind (NT-Koordinatoren, LAN-Koordinatoren ...). Nach Vorankündigung haben wir am gleichen Abend die auffälligen Geräte vom Netzwerk und/oder vom Backbone getrennt. Auffällig bedeutet, dass der Netzwerkverkehr, der von diesen Geräten ausgelöst wurde, auf die Verteilung des Wurmes hinwies. Am folgenden Tag wurde klar, dass bei Windows-NT Systemen die Entstörung nicht nachhaltig war. Die zur Verfügung stehenden Patches und Service Packs schützten vor **dieser** Variante des Wurmes nicht. Die Entwicklung eines entsprechenden Updates vom Hersteller Microsoft hätte das Forschungszentrum 80.000 € gekostet. Dies wurde am 13. Dezember im Expertenkreis vorgetragen, diskutiert und verworfen. Diese Lösung wäre nicht nachhaltig, lediglich gegen diese Angriffsvariante wäre Schutz geboten.

Daraufhin haben wir die NT-Koordinatoren, LAN-Koordinatoren etc. sowie auch den OE-Leitern unsere Hilfe beim Upgrade der Systeme angeboten. Eine schnelle Projektierung und Unterstützung für die Active Directory-Integration der OEs mit Ablösung der NT-Domänen war ebenfalls Bestandteil dieses Angebotes, welches derzeit aus vielen Bereichen in Anspruch genommen wird. Zusätzlich konzipierten wir eine Zwischenlösung, die wir wenige Tage später anbieten konnten. Die NT4-Server aus den OEs konnten mit jeweils einem Domänencontroller des zentralen Active Directory-Services und der BK-Domäne kommunizieren, welche dann weitere Clients in ihrem Subnetz bedienen konnten. Die Netzwerknamensdienste DNS und WINS standen ebenfalls in diesem (Quarantäne)-Netz zur Verfügung. Ein Notbetrieb war möglich, ohne den Betrieb der sicheren Systeme zu gefährden.

Es ist klar, dass nicht alle NT4-Systeme auf ein sichereres Betriebssystem gehoben werden können. Dafür bieten wir schon seit geraumer Zeit eine Technik an, wie potentiell unsichere oder besonders schutzbedürftige Geräte auf sicherem Weg an das FZK-Intranet angeschlossen werden können (siehe [Infoblatt 9/2006](#) (3)). Sprechen Sie uns an - selbstverständlich auch dann, wenn es um die Integration in den zentralen Antivirenschutz oder das Security Update Management geht.

Im IT-Expertenkreis wurde darüber hinaus am 24. Januar 2007 beschlossen, das Thema Angriffsfrüherkennung und -schutz erneut zu beleuchten und entsprechende finanzielle Mittel dafür zu beantragen. Es sollen ebenso die Endgeräte im FZK klassifiziert werden (z.B. nach Sicherheitskriterien) und dann gezielt für Anwendungen in unserem Netzwerk freigegeben werden. Hierzu wird im Rahmen des IT-Expertenkreises eine Konzeption entwickelt.

Andreas Lorenz, ☎ 4500

(1) <http://www.fzk.de/fzk/idcplg?ldcService=FZK&node=2523>

(2) <http://hikwww2.fzk.de/hik/orga/hlr/Allgemein/benutzeranmeldung.html>

(3) <http://hikwww2.fzk.de/hik/info/infoblatt/infoblatt092006.pdf>