URZ 1/09 – Aktuelles, Tipps und Tricks

In eigener Sache

Liebe Leserinnen und Leser,

wir hoffen, dass Ihnen dieses neue Exemplar von *ATT* zusagt; über jede Anregung und jeden interessanten Tipp von Ihrer Seite freuen wir uns.

Arno Spieth, 30. 01. 2009

Infoservice Altstadt: neue Öffnungszeiten

Peter Stede

Ab 2.2.2009 ändern sich die Öffnungszeiten des Infoservice in der UB/Altstadt wie folgt:

montags - donnerstags	11.00 – 12.30 Uhr und 13.00 – 16.00 Uhr
freitags	11.00 – 12.30 Uhr und 13.00 – 15.00 Uhr

Die Zeiten des Infoservice im URZ ändern sich nicht.

TEAM Sicherheit

Virus *Downadup* breitet sich derzeit massiv aus

Joachim Lammarsch

Zur Zeit greift der Internetwurm *Downadup* bzw. *Conficker* weltweit massiv Windows-Rechner an. Er verbreitet sich über eine Schwachstelle in Windows-Betriebssystemen, für die bereits (man glaubt es kaum) seit Ende Oktober ein Sicherheitsupdate von Microsoft bereit steht. Ebenso vermehrt wird er auch über die Autorun-Funktion der Wechsel-Laufwerke beispielweise beim Einstecken eines USB-Sticks verbreitet. Hier wird beim Anschließen des Sticks automatisch das darauf befindliche Schadprogramm gestartet und installiert.
Es ist daher wichtig, dass auf Ihrem Rechner das Sicherheitsupdate von Microsoft MS08-067 installiert ist, das unter folgendem Link erhältlich ist.

http://www.microsoft.com/germany/technet/sicherheit/bulletins/ms08-067.mspx

Dieses Sicherheitsupdate wird für alle unterstützten Editionen von Microsoft Windows als kritisch/hoch eingestuft.
Ebenso ist wichtig, dass Ihr PC durch eine aktive Firewall geschützt ist. Achten Sie ferner auf die regelmäßige Aktualisierung Ihres Virenschutzprogramms.
An diesem Wurm zeigt sich wieder einmal, dass die alte Masche, Schadsoftware über Wechsel-Medien zu verbreiten, auch heutzutage immer noch funktioniert. Beim Umgang mit Wechsel-Laufwerken ist daher immer eine große Vorsicht angebracht.
Bei weiteren Fragen wenden Sie sich bitte an den Infoservice des URZ.

Microsoft: 3 Sicherheitslücken behoben

Kerstin Zapf

Insgesamt drei Sicherheitslücken schließt der *Microsoft Patch Day* im Januar 2009 mit nur einem herausgegebenen Patch. Dabei wird das Risiko zweier Fehler als gefährlich eingestuft, da hier das Einschleusen von Schadcode möglich ist. Das Einspielen des Patches wird daher dringend empfohlen. Sofern nicht über die automatische Microsoft Update-Funktion bezogen, kann es über folgende Webseite heruntergeladen werden:

http://windowsupdate.microsoft.com

Alle drei Fehler betreffen das SMB-Protokoll von Windows Vista, XP und 2000 sowie von Windows Server 2003 und 2008. Die zwei gefährlichen Fehler erlauben Angreifern von außen, durch Manipulation Schadcode einzuschleusen und Kontrolle über den betroffenen Rechner zu erlangen. Beim dritten Fehler ist dies immerhin nicht möglich; allerdings kann durch seine Ausnutzung ein *Denial-of-Service*-Angriff ausgeführt werden, der das System zum Neustart zwingt. Anders als bei den zwei schwerwiegenden Fehlern ist hierzu außerdem eine vorhergehende Anmeldung beim System notwendig.
Eine ausführliche Beschreibung der Fehler und des Patches findet sich auf dem Link zu den *Security Bulletins*:

http://www.microsoft.com/germany/technet/sicherheit/bulletins/ms09-001.mspx

TEAM Windows-Systeme

Verbesserung der Erreichbarkeit

Rolf Bogus

Nach drei Wochen gespickt mit Feiertagen, Urlaubszeit und Grippewelle mussten wir feststellen, dass leider nicht jeder Hilfesuchende rechtzeitig seinen Wunsch erfüllt bekommen konnte. Warum kam es zu dieser Verzögerung? Das Hauptproblem war oft der schnelle Telefonanruf, der in die Leere führte, oder die E-Mail an den vermeintlich Zuständigen. Das Rechenzentrum versucht immer – trotz seiner angespannten Personaldecke – auch in Ferienzeiten einen Notdienst anzubieten, der den Großteil der Anfragen bearbeiten kann. Das funktioniert aber nur, wenn der Notdienst auch Kenntnis vom Problem erhält. Damit das sichergestellt ist, hat das Rechenzentrum die E-Mail-Adresse infoservice@urz.uni-heidelberg.de eingerichtet, die alle eingehenden Anfragen an die richtige Stelle weiterleitet. Sie können auch, falls bekannt, direkt die E-Mail-Adresse des zuständigen Teams benutzen. Anfragen per E-Mail sorgen nicht nur in problematischen Zeiten, sondern auch im Normalfall für eine schnelle und zuverlässige Abarbeitung der Anfragen.

Zugriffsrechte im Home-Ordner

Rolf Bogus

Das Rechenzentrum stellt seinen Benutzern auf den zentralen File-Servern Speicherplatz zur Verfügung. Diese sogenannten Home-Ordner sind so mit Zugriffsrechten ausgestattet, dass jeder Benutzer selbst lesend und schreibend darauf zugreifen kann. Alle anderen Benutzer haben zunächst keine Rechte auf diesem Speicherplatz. Sie können anderen Benutzern Zugriffsrechte einräumen, sollten allerdings die vorab eingestellten Rechte nicht einschränken. Sie riskieren sonst, dass Sie anschließend nicht mehr auf ihre Daten zugreifen können und sich sogar nicht einmal mehr mit Ihrer Benutzerkennung anmelden können.
Sollten Sie unsicher sein, ob die eingetragenen Zugriffsrechte korrekt gesetzt sind, oder haben Sie Fragen zu den gesetzten Rechten, wenden Sie sich bitte an:

Team-Windows-Systeme@urz.uni-heidelberg.de

Termine

Kurse im URZ

Edith Pokrandt

In diesem und dem folgenden Monat beginnen bzw. finden am URZ folgende, chronologisch aufgeführte Kurse statt:

2-Tageskurs: Excel 2007 für Fortgeschrittene
Michaela Wirth, 05.–06.02.09, 9.15–16.00 Uhr
Linux-Treff am URZ
Joachim Lammarsch, 16.02.09, 15.15–17.00 Uhr
Blockkurs: InDesign für angehende Journalisten
Dr. Reinhard Mayer, 23.–27.02.09, 9.30–12.00 Uhr
Linux-Treff am URZ
Joachim Lammarsch, 16.03.09, 15.15–17.00 Uhr
3-Tageskurs: Einführung in das Datenanalysesystem SPSS
Dr. Carina Ortseifen, 25.–27.03.09, 13.00–17.00 Uhr

Genauere Informationen und Anmeldung unter:

http://www.urz.uni-heidelberg.de/Ausbildung/Kurse/

Tipps und Tricks

Drucken über den Terminalserver (TS)

Ingo Schmidt

Von unserem Terminalserver (`ts.ad.uni-heidelberg.de`) ist es möglich so zu drucken, als ob man in einem unserer PC-Pools sitzt. Diese Möglichkeit wird auch gelegentlich genutzt. Auf unseren Servern werden regelmäßig Updates eingespielt, um das Betriebssystem und die Software auf dem aktuellen Stand zu halten. Dies ist unbedingt notwendig, um die Sicherheit zu gewährleisten. Ein solches Systemupdate hat leider ein – handhabbares – Problem beim Drucken geschaffen. Dieses Problem tritt auf, weil das URZ ein ausgeklügeltes Verfahren entwickelt hat, und auch nutzt, um eine seitengenaue Abrechnung der Ausdrucke für Institute und Studenten zu gewährleisten. Leider hat eine Änderung der zum Drucken relevanten Systemdateien von Microsoft zu diesem Fehler geführt. Der Fehler äußert sich – beim Versuch zu drucken – in einer Meldung, dass keine Drucker vorhanden seien. Es gibt aber eine einfache Prozedur, um diesen Fehler zu umgehen und trotzdem zu drucken.

Machen Sie bitte folgendes: Falls geöffnet, schließen Sie das Programm, mit dem Sie drucken wollten. Wählen Sie START und DRUCKER UND FAXGERÄTE. Machen Sie ein Doppelklick auf den Drucker, mit dem Sie drucken wollen. Schließen Sie das dadurch geöffnete Fenster. Jetzt starten Sie das Programm, mit dem Sie drucken wollen und drucken Ihr Dokument aus. Übrigens stehen nach diesem Doppelklick auf den Drucker sämtliche Drucker zur Verfügung. Wir bedauern sehr, dass wir Ihnen im Moment keine andere Lösung anbieten können. Seien Sie aber gewiss, dass wir an der Lösung des durch ein MS-Systemupdate verursachten Problems arbeiten.

Windows-Kennwort vergessen?

Timm Schenker

Ein vergessenes Windows 2000/XP/Vista-Kennwort des Administrators kann „idiotensicher“ mit dem Freeware-Tool *Offline NT Password & Registry Editor* zurückgesetzt werden. Ein downloadbares ISO-Image brennt man einfach auf eine CD und bootet davon. Das Freeware-Tool ist ein menügeführtes Linux-Livesystem, von dem aus die Installation auf der Festplatte, sozusagen „offline“, mit den integrierten Tools bearbeitet werden kann. Das Ganze ist, wie gesagt, menügeführt, d. h. man muss keine Ahnung von Linux haben, sondern man gibt im automatisch gestarteten Menü immer nur *yes* oder *no* ein, und am Ende ein neues (oder leeres) Passwort, rebootet nochmal und fertig.

Zurücksetzen des Kennworts der URZ-Benutzer-ID

Arno Spieth

Frage:

Leider habe ich mal wieder mein Kennwort vergessen. Könnten Sie mir das bitte zurücksetzen?

Antwort:

Unsere Benutzeridentifikation ist an die Person gebunden und nicht nur an die E-Mail-Adresse. Im Internet ist letzteres heute öfter zu finden. Wegen der höheren Ansprüche können wir Ihre Bitte nicht erfüllen. Um sich ein neues Kennwort setzen zu lassen, müssen Sie mit einem Lichtbildausweis in unserem Infoservice vorbeikommen. Für Mitarbeiter und Projektnummern kann auch der EDV-Beauftragte die Kennwortänderung durchführen. Für Studierende der Medizin in Mannheim erledigt dies auch Herr Schoppmann und Frau Schwarz im Sekretariat der Medizinischen Fakultät in Mannheim.

SAS: Erzeugung von kleinen Grafiken

Dr. Carina Ortseifen

Grafiken, die für den Ausdruck auf Papier gedacht sind, eignen sich selten für die Veröffentlichung im Internet. Entweder sie wurden im falschen Dateiformat angelegt (`.cgm` statt `.gif`) oder sie sind zu groß und müssen verkleinert werden. Zu große Grafiken lassen sich in SAS mit GIF-Treibern verkleinern, sodass sie in schmalere Textspalten passen. Eine Anleitung hierzu mit Beispiel anhand eines Streudiagramms finden Sie unter folgendem Link:

http://www.urz.uni-heidelberg.de/imperia/md/content/urz/programme/statistik/sas/tipps_zu_sas_-_kleine_grafiken.pdf

Weitere Beispiele und Erläuterungen zu verschiedenen GIF-Treibern finden Sie im Paper „Controlling Graph Size: Building Thumbnails and GIF Files Using SAS/GRAPH“” von Arthur L. Carpenter und Richard O Smith unter folgendem Link:

http://www.caloxy.com/papers/50-TT05.pdf

Firefox: Änderung der Farbeinstellungen

Marion Lammarsch

Problem:

Sie surfen mit Firefox im Netz und landen auf einer Seite mit gräßlichen Farben, können Sie das ändern?

Lösung:

Nehmen Sie beispielsweise

http://www.opensuse-forum.de

– der Hintergrund ist schwarz, die Schrift weiß, nicht gerade augenfreundlich für längeres Lesen. Im Firefox kann man unter EINSTELLUNGEN -> INHALT -> FARBEN vorgeben, welche Farben man haben möchte, meistens Hintergrund weiß und Schrift schwarz. Außerdem gibt es da ein Kästchen mit der Beschriftung *Seiten das Verwenden von eigenen statt der oben gewählten Farben erlauben*. Wenn man den Haken aus dem Kästchen entfernt, dann gelten nur noch die selbst gewählten Farben und voila, die Seite ist angenehm lesbar. Dasselbe gilt natürlich auch, wenn man in den Menüpunkt SCHRIFTEN hineinschaut. Damit kann man sich seine Lieblingsschriftart und -größe so voreinstellen, dass normale Html-Seiten gut lesbar sind. Alles, was mit PHP, ASP oder ähnlichem programmiert ist, ignoriert diese Einstellungen leider häufig.

Die SAS-Prozedur SQL – Ressourcen im Internet

Dr. Carina Ortseifen

SQL steht für *Structured Query Language* und ist eine Datenbank-Abfrage-Sprache, die nicht nur von Datenbanken verwendet werden kann, sondern auch in einer SAS-Prozedur implementiert ist. Damit arbeitet z. B. die SAS/Enterprise-Guide-Software an allen Stellen, wo der „normale“ Programmierer Datenschritte einsetzen würde.

Eine Einführung zum Einsatz der Prozedur findet man im SAS-Anwenderhandbuch im Netz unter http://www.urz.uni-heidelberg.de/statistik/sas-ah/, (Kapitel 1, Abschnitt 1.6). Darüber hinaus gehende Links werden in der SAS Note 20783 unter http://support.sas.com/kb/20/783.html zusammengefasst, mit Links auf Internet-Seiten von *SAS Institute* selbst, aber auch von Anwendern, die auf SAS-Konferenzen gesprochen haben.

Das gab es auch noch

In dieser Rubrik sind Informationen aufgeführt, die sich nicht auf die EDV-Anwendung in dem Universitäts-Netz beziehen, von denen wir jedoch glauben, dass sie von allgemeinem Interesse bzw. für die private EDV-Nutzung wichtig sein können.

Google: Internet Explorer 6 nicht mehr unterstützt

Jana Motzet

Google wird künftig Nutzern des *Internet Explorer 6* raten, auf *Firefox 3* oder den Google-Browser *Chrome* umzusteigen, da dieser doppelt so schnell wie IE6 sei. Für die Zukunft vorgesehene Google-Mail-Funktionen seien außerdem nicht mehr im IE6 realisierbar. So ist es auch im Hilfe-Center von google auf folgendem Link nachzulesen:

http://mail.google.com/support/bin/answer.py?answer=78161

Während nur Firefox 3 und Chrome bei dem Hinweis direkt zum Download verlinkt werden, sind weiterhin auch *Safari* und *Internet Explorer 7* unterstützt. Eine Umstellung bedeutet dies, da IE6 trotz seines 8-jährigen Alters immer noch ca. 20-25% Marktanteil besitzt. Es wird geschätzt, dass vor allem viele Firmen den veralteten Browser wegen speziell eingerichteter Anwendungen weiter benutzen.

Internet Explorer: Marktanteil unter 60%

Jana Motzet

Im August letzten Jahres sank der Anteil der Internetbenutzer, die den *Internet Explorer* als Browser benutzten, erstmals unter 60%. Dieser Trend setzte sich, trotz eines kurzen Anstiegs im Folgemonat, dann im Oktober und November weiter fort. Im November lag der Marktanteil nur noch bei 59,5%. Auch die Zahl der Firefox-Nutzer sank. Allerdings: Im Gegensatz zum Wert von 33% im August 2008 liegt der Anteil im November nur bei 31,1% – dem tiefsten Wert seit Mai 2008.

Auch die US-Firma *Net Applications Inc.* stellte ein Absinken des Firefox-Anteils im September fest und führte dieses auf die Einführung des Google-Browsers *Chrome* zurück, der zu dieser Zeit veröffentlicht wurde. Die Anzahl der Netzanwendungen von Firefox sank weltweit nur leicht: 0,2% unter den Anteil des Vormonats. Obwohl die Statistiken von Net Applications zeigen, dass Firefox Rückschläge durch Chrome schnell wieder gutmachte, zeigen XiTi-Messungen für Europa (*AT Internet* (http://www.xitimonitor.com), dass Firefox´s Wachstum im Wesentlichen stagniert.

Storm-Botnet beim 25C3 gekapert

Jana Motzet

Auf dem 25. *Chaos Communication Congress* (25C3) in Berlin wurde im Dezember die Übernahme des Storm-Botnet präsentiert. Durch dieses von Spammern errichtete Botnet werden momentan von mehr als 100.000 Windows-Rechner weltweit mit Schadcode versehene Mails versendet. Das Problem hierbei ist, dass die Besitzer meist nichts davon wissen, dass der eigene PC in dieses Netzwerk integriert ist und ebenso solche Mails weiterverbreitet. Beim 25C3 wurde nun gezeigt, wie man Kontrolle über Rechner, die in dieses Botnet eingegangen sind, übernehmen kann. Die Experten schleusten eigene Server in das Netzwerk ein, die die vom Botnet befallenen Systeme als *Command-and-Control*-Server akzeptierten. Dadurch war es möglich, dem Botnet über diese Server Befehle zu erteilen. So könnte man laut den Referenten des Kongresses dem Botnet das Herunterladen bestimmter Software befehlen. Würden diverse betroffene Rechner also Software herunterladen, die zunächst den Botnet-Client und dann sich selbst löscht, so könnten alle befallenen PCs weltweit von ihrer Botnet-Verbindung bereinigt werden.

Die Schwierigkeit besteht allerdings darin, dass eine solche Aktion von mehreren Netzknoten aus koordiniert gestartet werden müsste, da die Entwickler des Botnet sonst die Möglichkeit hätten, diese Attacke leicht unwirksam zu machen. Auch juristisch wirft der Lösungsversuch Schwierigkeiten auf, da es sich trotz des guten Willens um einen unrechtmäßigen Zugriff auf fremde Rechner handeln würde.

Impressum

Herausgeber: Rechenzentrum der Universität Heidelberg
Redaktion: Dr. Carina Ortseifen, Arno Spieth, Joachim Lammarsch, Leif Enzmann, Jana Motzet, Johannes Bätz
Verteiler: `ATT-URZ@urz.uni-heidelberg.de`
Layout: Luzia Dietsche, Joachim Lammarsch
Produktion: TEXlive 2007, LATEX 2ε und pdfTEXk Vers. 3.141592-1.40.3

Namentlich gekennzeichnete Beiträge geben die Meinung der Schreibenden wieder; eine weitere uneingeschränkte Veröffentlichung im WWW ist nicht erlaubt. Die Texte sind nach bestem Wissen erstellt, jedoch kann für die sachliche Richtigkeit keine Garantie übernommen werden. Anregung oder Kritik sowie interessante Beiträge sind jederzeit willkommen. Bitte schicken Sie sie an die Adresse `ATT@urz.uni-heidelberg.de`. Sie können sich bei ATT-URZ durch eine Mail an `listserv@listserv.uni-heidelberg.de` mit dem Inhalt `sub att-urz` einschreiben, oder via:

http://listserv.uni-heidelberg.de/cgi-bin/wa?SUBED1=att-urz&A=1

ATT ist nicht als Alternative zu den BenutzerNachrichten gedacht; vielmehr werden wichtige Artikel in die BN übernommen. Unser Ziel ist lediglich, Ihnen wichtige Informationen möglichst zeitnah zu vermitteln. Zusätzlich fügen wir Tipps und Tricks hinzu, die wir bei unserer Arbeit erfahren haben. Gerne dürfen Sie uns auch Ihre Tipps und Tricks zusenden, die wir dann veröffentlichen.