URZ 01/07 – 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.

Joachim Lammarsch, 31. Januar 2007

TEAM Sicherheit

Gefälschte E-Mail vom BKA im Umlauf

Joachim Lammarsch

Seit heute, dem 31. Januar 2007, werden gefälschte E-Mails verbreitet, die angeblich vom Bundeskriminalamt (BKA) stammen. Darin wird behauptet, dass gegen den Adressaten eine Strafanzeige gestellt wurde wegen illegalem Herunterladen von Musik, Filmen und Software.
Der Empfänger soll den Anhang der E-Mail ausdrucken und eine Stellungnahme auf Grund des laufenden Ermittlungsverfahrens zum BKA via FAX senden. Auf diese Weise sollen unkundige Anwender dazu verleitet werden, den Anhang zu öffnen und dadurch die darin enthaltene Schadsoftware zu aktivieren.
Die Firma TrendMicro hat den Anhang analysiert und bestätigt, dass es sich bei der Schadsoftware in der gefälschten E-Mail um ein Trojanisches Pferd handelt. Seine Aufgabe ist vor allem, sich auf dem betreffenden Rechner zu installieren und weitere Software aus dem Netz nachzuladen. Des weiteren spioniert der Trojaner vertrauliche Daten wie Kennwörter und PINs aus.
Das Bundeskriminalamt weist ausdrücklich darauf hin, dass E-Mails mit dem Betreff „Ermittlungsverfahren Nr. X“ nicht von seinen Ermittlern stammen. Es warnt nachdrücklich davor, den mitgeschickten Dateianhang zu öffnen und die darin enthaltene Schadsoftware zu aktivieren.
Vorhandene Virenscanner sollten dringend aktualisiert werden.

Schwachstelle in Microsoft Word 2000

Joachim Lammarsch

Unter Microsoft Word 2000 wurde eine Schwachstelle entdeckt, durch die ein Angreifer mittels einer speziellen Word-Datei die Speicherstrukturen gefährden kann. Dies ermöglicht ihm beliebige Befehle mit den Rechten des Benutzers auszuführen. Die Datei kann auf einer WWW-Seite verlinkt oder als Attachment an einer E-Mail angehängt sein.
CERT warnt vor bereits verwendeten Exploits, mit deren Hilfe Viren und trojanische Pferde installiert werden. Bereits betroffene Systeme mit Microsoft Word 2000 sind

- Windows 2000
- Windows 95, 98 und Me
- Windows NT
- Windows Server 2003
- Windows XP

Bisher konnte diese Schwachstelle durch kein Update geschlossen werden. Daher empfiehlt Microsoft nur Dokumente aus vertrauenswürdigen Quellen zu öffnen.

http://www.microsoft.com/technet/security/advisory/932114.mspx

Firefox 1.5.0.9/2.0.0.1 – Thunderbird 1.5.0.9

Joachim Lammarsch

Die Entwickler von Mozilla gaben erneut neue Versionen von Firefox und Thunderbird frei. Die neuen Versionen sollen für mehr Sicherheit und Stabilität sorgen. Wie schon bei den letzten Versionen dienen diese der Behebung von Sicherheitsproblemen und der Korrektur von Fehlern.
Es wird allen Firefox-/Thunderbird-Anwendern empfohlen, auf die neue Version zu wechseln. Mozilla kündigte an, dass es nur noch bis zum April Sicherheits-Updates für Firefox 1.5.0.9 geben wird. Es wird daher empfohlen, zügig auf Firefox 2 umzustellen.
Weitere Informationen zu Firefox 1.5.0.9/2.0.0.1 – Thunderbird 1.5.0.9 siehe:

http://www.mozilla.com/firefox/releases/1.5.0.9.html

http://www.mozilla.com/en-US/firefox/2.0.0.1/releasenotes/

http://www.mozilla.com/thunderbird/releases/1.5.0.9.html

Das Herunterladen und Installieren der Updates kann auch automatisiert geschehen. Die Einstellungen dazu finden sich im Menü `Extras`.

Verlängerung der Campuslizenz für Sophos-Antivirus

Ingo Schmidt

Der Lizenzvertrag über eine Campuslizenz für Sophos-Antivirus ist um weitere 5 1/2 Jahre, also bis zum 31.08.2012, verlängert worden. Die Software kann über den Link

http://www.urz.uni-heidelberg.de/Security/nutzer/virusinst.shtml

heruntergeladen und installiert werden, wozu eine Anmeldung mit Benutzername (URZ-Kennung) und Passwort erforderlich ist. Auf dieser Seite ist auch eine Konfigurationsanleitung zu finden. Sophos-Antivirus darf auf allen Rechnern der Universität Heidelberg kostenlos eingesetzt werden. Ebenso dürfen alle Mitarbeiter und Studierende, solange sie in der Universität angestellt sind bzw. studieren, die Software zu Hause nutzen.

TEAM Anwendungssoftware

SelfPHP 4.2

Dan Popović

Die aktuelle Version 4.2 von SelfPHP erklärt rund 600 Befehle der Programmiersprache PHP ausführlich und stellt diese an praktischen Beispielen anschaulich dar. Auch ein über 1000 Seiten umfassendes Tutorial und ein PHP-Kochbuch sind in der Software enthalten. Die Befehlsreferenz ist in 23 Kategorien gegliedert, in denen die am häufigsten verwendeten PHP-Befehle ausführlich dargestellt werden. Dabei bieten die jeweiligen Beispiele die entsprechende Ausgabe des Befehls als Text oder Grafik, sodass dieser selbst für Einsteiger gut verständlich ist.
Im Tutorial werden die grundlegenden Sprachelemente von PHP beschrieben. Darüber hinaus vermittelt es Kenntnisse, die zur Entwicklung anspruchsvoller Programmierlösungen mit PHP erforderlich sind. Das PHP-Kochbuch behandelt schließlich anhand konkreter Programmier-Problemstellungen mögliche Lösungsansätze. Insgesamt stellt SelfPHP somit ein hilfreiches Nachschlagewerk und eine Lernhilfe dar und ist sowohl für PHP-Anfänger als auch für professionelle Webdesigner, Internet- und Datenbankentwickler von Interesse.

http://www.selfphp.info

TEAM Windows-Systeme

Einsatz von Windows Vista

Rolf Bogus

Das Team Windows-Systeme hat sich in den letzten Monaten ausgiebig mit Microsoft Windows Vista beschäftigt. Zur Zeit wird davon abgeraten, Windows Vista produktiv einzusetzen. Zu viel Software ist für Windows Vista bisher nicht angepasst (Virenscanner, VPN-Klient, SAS, Treiber, ...). Das Team Windows-Systeme wird Windows Vista weiterhin testen und darüber berichten.

Drei wichtige Vista-Updates

Kerstin Zapf

Bereits am ersten Verkaufstag der Version für die Endnutzer hat Microsoft drei als *wichtig* klassifizierte Updates veröffentlicht. Diese sollen Fehler bei der Berichterstattung, bei Signaturen der Sicherheitsfunktionen und bei der Aktivierungsfunktion beseitigen.
Insgesamt bietet Microsoft neun Updates für Vista an, drei werden hierbei als *wichtig* eingestuft:

- Signaturen für den *Windows Defender*,
- Entfernen bösartiger Software,
- ein Problem mit dem Datenschutz bei Vista (hier soll der Fehlerberichterstattungsdienst Daten auch ohne Zustimmung der Nutzers an Microsoft verschickt haben).

Daneben gibt es noch weitere Updates, die lediglich als *empfohlen* eingestuft sind. Dazu gehören:

- Eigenheiten bei der Produktaktivierung,
- ein Update, das die Kompatibilität mit nicht für Vista empfohlenen Anwendungen verbessert. (Interessanterweise laufen auch Produkte wie Photoshop 7.0 und Outlook 2003 nur nach diesem Update stabil.)

Alle Aktualisierungen werden über die automatische Update-Funktion von Vista bezogen und bringen zusammen über 15 MByte auf die Platte.

TEAM Unix-Systeme

openSUSE 10.2 als Live-DVD

Joachim Lammarsch

Das openSUSE-Projekt hat nun den letzten fehlenden Teil von openSUSE 10.2 herausgegeben: Das Image einer Live-DVD mit einem Umfang von 1,7 GB. Für das Testen der openSUSE-Distribution ohne Installation und Systemänderung ist die Live-CD auf jedem x86-System anwendbar, sofern es sich um einen Rechner mit mehr als 512 MB RAM handelt. Auf der Live-DVD ist ein Desktopsystem mit KDE und Gnome sowie mit weiteren Anwendungen für Multimedia, Office und Internet enthalten. Als Image steht die Live-DVD unter

http://download.opensuse.org/distribution/10.2/iso/dvd/openSUSE-10.2-GM_LiveDVD.iso

zur Verfügung.
Die Distribution openSUSE 10.2 wird mit dem Kernel 2.6.18.2, GNOME 2.16.1, KDE 3.5.5, glibc 2.5 und X.Org 7.2rc2 geliefert. Gegenüber der älteren Version openSUSE 10.1 enthält sie zahlreiche Änderungen wie zum Beispiel einen neuen Bluetooth-Stack, native 64-Bit-Unterstützung für OpenOffice.org und OpenSync statt MultiSync, ein *ZMD-freies* Update-Tool namens Zypper und eine schnellere Paketverwaltung. Außerdem wurde das *Powersave-Management* vollständig erneuert und interne SD-Kartenleser und Xen 3 werden nun unterstützt.

TEAM Internetdienste

WWW-Seiten unter Firefox archivieren

Leif Enzmann

Der Gewinner des letztjährigen Extend Firefox Contests ist ein Archivierungs-*Add-on* namens Scrapbook. Mit dieser in der Version 1.2.0.8 vorliegenden Erweiterung können Seiten *offline* abgespeichert, mit Notizen versehen und weiter bearbeitet werden. Das Speichern der Seite erfolgt im HTML-Format und speichert die Links bis zur eingestellten Tiefe. Automatisch wird zur besseren Übersicht eine Sitemap erstellt, die die Navigation im Archiv erleichtert. Ebenso kann man alle geöffneten Tabs mit einem Klick archivieren und gegebenenfalls Elemente der Seite vor dem Speichern entfernen, die nicht benötigt werden. Eine einblendbare Seitenleiste erleichtert die Bedienung.
Im integrierten Scrapbook-Manager können die gespeicherten Archive dann weiterhin mit Notizen versehen, unterstrichen, verschiedenen WWW-Seiten zusammengefügt oder im Volltext durchsucht werden. Wer also WWW-Seiten offline verfügbar machen will oder für seine Recherchen Veränderungen im WWW dokumentieren muss, der sollte sich diese Erweiterung für Firefox einmal genauer ansehen.

Termine

SPSS-Treff – Präsentation von SPSS Inc.

Dr. Carina Ortseifen

Am 16. Februar 2007 werden Herr Bohnenstengel, Frau Anja Burghardt und Herr Markus Eberl von der Fa. SPSS aus München am URZ zu Gast sein und u. a. über folgende Themen sprechen:

1. SPSS Family
   - Grundlagen
   - Neuerungen (Datenmanagement, Reporting/Grafikengine, Statistikfunktionalitäten: Verallgemeinerte lineare Modelle/GZLM und GEE, ordinale Regression in komplexen Stichproben, Programmierbarkeit/Python)
   - Live Demo
   - Diskussion/Fragen und Antworten
2. Statistik vs. Data Mining – eine kurze Abgrenzung
3. Data Mining mit SPSS Clementine
   - Grundlagen
   - Beispielhafte Modellierungsalgorithmen (Entscheidungsbäume, Assoziationsanalysen, etc.)
   - Live Demo
   - Diskussion/Fragen und Antworten
4. Vorstellung und Diskussion SPSS Lizenzmodelle

Den Teilnehmern wird dabei sowohl Raum für Diskussion der Vorträge gegeben als auch eigene Fragen und Themen anzusprechen. Bei Bedarf können Sie Themen, die Ihnen wichtig sind, vorab übermitteln, damit sich die Referenten entsprechend vorbereiten können.
Die Veranstaltung beginnt um 13:30 Uhr und findet im Raum 119 des URZ statt.
Aus organisatorischen Gründen werden Interessierte um Anmeldung gebeten bis 13.2.2007 per Mail an

carina.ortseifen@urz.uni-heidelberg.de

Kurse im URZ

Edith Pokrandt

Im aktuellen und den nächsten beiden Monaten beginnen bzw. finden am URZ folgende, chronologisch aufgeführte Kurse statt:

2-Tageskurs: Das Datenanalysesystem SAS
Dr. Carina Ortseifen, 15.2.+16.2.07, V+Ü 9.15–18/13 Uhr
Linux-Treff am URZ
Joachim Lammarsch, 15.2.07, 15.15–17.00 Uhr
SPSS-Treff am URZ: Präsentation von SPSS Inc.
Dr. Carina Ortseifen, 16.2.07, 13.30—17.00 Uhr
2-Tageskurs: Tabellenkalkulation mit Excel
Michaela Wirth, 22.2 + 23.2.07, V+Ü 9.15–16.00 Uhr
Einführung in die Programmierung mit SAS: Teil 1
Dr. Carina Ortseifen, 14.–16.3.07, V+Ü 9.15–16.00 Uhr
Linux-Treff am URZ
Joachim Lammarsch, 15.3.07, 15.15–17.00 Uhr
Einführung in die Programmierung mit SAS: Teil 2
Dr. Carina Ortseifen, 19.–21.3.07, V+Ü 9.15–14.00 Uhr
1-Tageskurs: Einführung in das Betriebssystem Linux II
Joachim Lammarsch, 22.3.07, 15.15–17.00 Uhr

Genauere Informationen und Anmeldung unter:

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

Tipps und Tricks

Ubuntu GNU/Linux

Leif Enzmann

Die 2. Auflage von Marcus Fischers *Ubuntu GNU/Linux* steht als HTML-Version bei

http://www.galileocomputing.de/openbook/ubuntu/

zum Download bereit.

Das Buch beschreibt die einzelnen Funktionen der Distribution, darunter die Paketverwaltung, Programmierung, Kernelkompilierung und Netzwerktechnik. Der 30 MB große Download des über 900 Seiten starken Buches soll Einsteigern und Fortgeschrittenen den Wechsel zu Ubuntu erleichtern. Eine gedruckte Version ist seit Dezember für 39,90 € ebenfalls bei Galileo Computing erhältlich.

Linux Kernel in a Nutshell

Joachim Lammarsch

Das Buch des Novell-Angestellten Greg Kroah-Hartman über die Steuerung des Kernels steht nun unter

http://www.kroah.com/lkn/

zum Download bereit.

Unter Anderem geht es um die Kompilierung und Konfiguration der Quellen, sowie die Möglichkeiten, den Kern zu aktualisieren.

Die fast 200 Seiten behandeln die Kernel-Version 2.6.18 und stehen unter der Creative-Commons-Attribution-ShareAlike-2.5-Lizenz. Der Download erfolgt entweder im PDF- oder DocBook-Format, die gedruckte Version kann jedoch auch im Handel gekauft werden.

Open Book Sicherheit im Internet freigegeben

Marion Lammarsch

Im O'Reilly- Verlag wurde ein neues deutschsprachiges OpenBook *Sicherheit im Internet* freigegeben. Dieses ist über den Link

http://www.oreilly.de/german/freebooks/sii2ger/

zugänglich. Das Buch behandelt diverse Internet-Dienste unter dem Aspekt des Schutzes vor Viren, Würmern, Phishing und Dialern. Zum Einen klärt es die Frage, welche Techniken diesbezüglich beim Surfen, bei WWW-Accounts, Online-Banking und E-Mail-Verschlüsselung vertrauenswürdig sind und vermittelt somit Informationen zur richtigen Einschätzung und Minimierung der Sicherheitsrisiken im Internet. Zum Anderen enthält das OpenBook zahlreiche Tipps zur effektiven Nutzung von Sicherheitstools und Hinweise zur Konfiguration der geläufigsten Mail-Clients und Browser. Ebenso ist ein Kapitel zur Ersten Hilfe beim erfolgten Einbruch ins System enthalten.

Serienbrief umleiten in eine Datei

Henriette Höhle

Nachdem die Serienbriefe nicht auf einen Drucker sondern in eine Datei umgeleitet wurden, wird eine Druckdatei erstellt (.prn Datei). Danach auf `Individuelle Briefe bearbeiten` im Arbeitsbereich klicken, die fertigen Briefe sollten nun angezeigt werden. Diese können nun als Word-Datei abgespeichert werden.

Befehlszeilenergänzung unter Windows

Leif Enzmann

Nutzer von Linux und Windows XP kennen die Erweiterung einzelner Befehle und Pfade mit der Tabulator-Taste schon lange. Man gibt beispielsweise als Pfad nur `C:\Win` ein, drückt `Tab` und der Computer erweitert den Pfad automatisch zu `C:\Windows`. Mit derselben Taste kann man in Ordnern auch alphabetisch durch alle verfügbaren Dateien schalten, mit `Shift+Tab` geht es zurück.

Um diese Funktion auch unter Windows 2000 verfügbar zu machen ist nur eine kleine Änderung in der *Registry* nötig. Diese erreicht man unter `Ausführen` durch die Eingabe von `regedit`. Im folgenden Fenster geht man den Pfad

```
HKEY_CURRENT_USER\Software\Microsoft\
                    CommandProcessor\CompletionChar
```

und setzt hier den Wert auf 9. Danach ist auch unter Windows 2000 die Tabulator-Taste zur Vervollständigung der Kommandozeilenbefehle konfiguriert.

Viren manuell löschen

Ingo Schmidt

Problem:

Ein Virus hat sich im Speicher eingenistet und eine manuelle Bereinigung ist unter Sophos erforderlich.

Lösung:

Der erste Weg den Virus zu entfernen ist, diesen Prozess aus der Prozessliste zu entfernen und dann noch einmal eine Bereinigung mit Sophos zu starten:

- Merken oder notieren Sie sich den Namen der Datei.
- Drücken Sie in der Taskleiste, am unteren Bildschirmrand, die rechte Maustaste und wählen *Taskmanager*.
- wählen Sie das Register *Prozesse*.
- klicken Sie den *viruellen* Prozess an und wählen `Prozess beenden`.
- Starten Sie dann noch mal einen ausführlichen Scan Ihres PC durch Sophos.

Starten Sie den Scan vom Taskleisten-Symbol mit der rechten Maustaste und wählen `Meinen Computer überprüfen`. Nur dann werden auch der Hauptspeicher und die Registry durchsucht.

Sophos kann jetzt den Virus entfernen, da er nicht als Prozess läuft. Wenn ein Virus als Prozess im Hauptspeicher läuft, ist die Datei *offen* und kann von keinem Antivirenprogramm entfernt werden.

Proxy-Einstellungen

Leif Enzmann

Bei der nicht nur großen Auswahl an WWW-Browsern, sondern auch an Versionen derselben ist es schwer, den Überblick über die Funktionen zu behalten. Deshalb haben wir uns den Pfad zu den Proxy-Einstellungen im aktuellen Microsoft Internet Explorer 7, im Firefox 2.0, sowie im älteren Internet Explorer 6 und Firefox 1.5.0.9 einmal genauer angesehen.

Bei Microsoft hat sich zwischen den zwei Versionen nur die Lage des `Extras`-Buttons verändert, der Weg bleibt absolut gleich. Nämlich über die `Internetoptionen`, dann `Verbindungen` und hier dann in den `LAN-Einstellungen` unter `Erweitert`. Der neue Firefox hat seinen Proxy-Einstellungen einen neuen Platz gegeben. Schon der Zugang zu den `Einstellungen` wurde in der Taskbar von `Bearbeiten` in die `Extras` verschoben. Fand man die `Verbindungs-Einstellungen` in der alten Version noch unter `Allgemein`, wurde für 2.0 das Ganze nach `Erweitert` verschoben und ein neuer Reiter `Netzwerk` spendiert. Hier kann man genau wie im Vorgänger den Proxy mit wenigen Klicks einstellen.

Interessante Programme

Lohnrechner für 2007 vorgestellt

Joachim Lammarsch

Das Programm *Lohnrechner* von Sascha Wilde steht nun – den Bedingungen des Jahres 2007 angepasst – in der neuen Version 20070126 zum Download zur Verfügung.

http://wald.intevation.org/projects/lohnrechner/

Es steht unter der GNU General Public License (GPL) und ist für die Lohn- oder Gehaltsberechnung nützlich, wenn man sich bei dieser nicht einem Online-Rechner anvertrauen möchte.

Der mit Python geschriebene Lohnrechner bietet eine übersichtliche graphische Oberfläche (plattformunabhägig mit TkInter) und ist durch seinen modularen Aufbau einfach in eigene Anwendungen integrierbar. Für die internen Berechnungsgrundlagen nutzt die Software das Python-Modul LST2007, das alle Berechnungen des offiziellen Programmablaufplans des Bundesfinanzministeriums implementiert. Außerdem ermöglicht das Programm auch die Berechnung der nach diesem Plan anfallenden Steuern.

Impressum

Herausgeber:	Rechenzentrum der Universität Heidelberg
Redaktion:	Dr. Carina Ortseifen, Joachim Lammarsch (verantwortlich), Leif Enzmann, Paulina von Mirbach, Jana Motzet, Dan Popović
Verteiler:	`ATT-URZ@urz.uni-heidelberg.de`
Layout:	Luzia Dietsche, Joachim Lammarsch
Produktion:	TEXlive 11/2005, LATEX 2_ε und pdfTEXk Vers. 3.141592-1.40.0

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.