URZ 5/09 – 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, 2. 6. 2009

Mac-Pool im URZ: Neue Apple-Mac-Pro-Rechner

Klaus Kirchner

Das Medienzentrum des URZ wurde mit neuen Rechnern ausgestattet.Es handelt sich dabei um Mac-Pro-Rechner von Apple mit 8 Intel-Xeon-Prozessorkernen vom Typ *Nehalem*. Jeder Rechner besitzt 6 GB RAM sowie ein Festplatten-RAID mit 2,4 TB Speicherplatz und einen DVD-Brenner für Single- und Double-Layer-Medien. Gleichzeitig wurde die Videoschnitt-Software auf den neusten Stand gebracht. *FinalCut Studio 2* ist optimiert für die Arbeit mit Mehrkern-Prozessoren und ermöglicht das optimale Arbeiten mit der neuen Rechnertechnik. Auch die neuste Version von *iLife Version 09* ist jetzt auf den Rechnern installiert (iMovie, iDVD,...), Weiterhin verfügbar sind die *Adobe Creative Suite Premium 3*, *Roxio Toast* sowie *Microsoft Office für den Mac 2008*. Des Weiteren wurden die Scanner und Analog-Digital-Wandler auf den neusten Software-Stand gebracht.
Mehr Details gibt es auf unserer Webseite über folgenden Link:

http://www.urz.uni-heidelberg.de/mac/leopard.html

TEAM Sicherheit

Internetbetrug: Mahnungen ohne Vertragsabschluss

Arno Spieth

Immer wieder treten Fälle von Internetbetrug auf, wobei eine besonders heimtückische Falle die Verunsicherung der Betroffenen mit Mahnungen per E-Mail ist. Erst kürzlich erreichte das URZ wieder eine Anfrage, was zu tun sei, wenn man eine dubiose Mahnung per E-Mail erhalte. Das betroffene Universitätsmitglied war auf der Suche nach einer aktuellen Version von *Adobe Reader* auf die gefälschte Webseite von *Belleros Premium Media Limited* gestoßen. Nach dem irrtümlichen Download der dort angebotenen Software erschien sofort eine Rechnungsaufforderung, ohne dass eine Aktivierung der Software stattgefunden hatte. Einige Wochen später folgte eine „anwaltliche Mahnungszahlung“ per E-Mail, in der ein Rechnungsbetrag von 70,50 Euro zuzüglich ca. 40 Euro Anwaltskosten eingefordert wurde. Aus der besuchten Internet-Seite sei ersichtlich, „dass es sich bei der erbrachten Dienstleistung um ein kostenpflichtiges Angebot handelt.“ Im Falle der Nichtzahlung drohte die E-Mail mit der unverzüglichen Einleitung eines gerichtlichen Mahnverfahrens.
Betrugsversuche dieser Art sind bereits seit Längerem bekannt und auch schon häufig in Verbindung mit der Seite von *Belleros Premium Media Limited* aufgetreten. Hier ist also Vorsicht geboten. Generell sollte man dubiose Mahn-E-Mails ignorieren, da in Fällen wie dem oben beschriebenen kein wirklicher Vertrag zustande gekommen ist. Alternativ kann man die Mail auch beantworten, indem man um Informationen bittet, wie ein solcher Vertrag zustande gekommen sei, da die Daten nicht verifiziert worden seien.
Hier liegt nämlich die Schwachstelle, an der man Rechtanwälte greifen kann, da sie keine wissentlich falsche Antwort geben dürfen. Wichtig zu wissen ist aber vor allem, dass der wirkliche *gerichtliche* Mahnbescheid immer per Post kommt und man erst auf diesen reagieren *muss*, indem man ihm binnen 14 Tagen widerspricht. Ein solcher wird aber wohl nie kommen, da auch diese dubiosen Anwälte natürlich wissen, dass sie derartige Fälle vor Gericht nicht durchbekommen.
Weitere Informationen zu Internetbetrug und Hinweise, wie man sich als Betroffener verhalten soll, finden sich auf folgender Seite:

http://www.computerbetrug.de/abzocke-im-internet/abofallen-und-abzocke-im-internet-das-muessen-sie-wissen/

MacOS X: Update auf Version 10.5.7

Arno Spieth

Mit dem Update auf Version 10.5.7 schließt MacOS X jetzt über 50 Sicherheitslücken im Betriebssystem. Bei vielen der Fehler in verschiedenen Komponenten kann es zur Einschleusung von Schadcode kommen, sofern manipulierte Websites besucht werden bzw. in anderen Fällen bearbeitete Dokumente geöffnet werden. Die Aktualisierung mit den Patches ist daher dringend anzuraten. Das Update ist auf folgender Seite erhältlich:

http://support.apple.com/downloads/

Neben diesen Sicherheitspatches sind aber auch einige Aktualisierungen für verschiedene Anwendungen enthalten, zum Beispiel für die Druck- und Kindersicherungsfunktion, iCal und Mail. Außerdem sind Videowiedergabe und Cursorbewegung für Macs mit NVIDIA-Grafik verbessert worden und es werden jetzt weitere Kameras und das RWA-Bildformat unterstützt.
Ausführliche Informationen zu allen Änderungen finden sich auf folgender Seite im Changelog:

http://support.apple.com/kb/HT3397?viewlocale=de_DE&locale=de_DE

Microsoft Patch Day: 14 Lücken in Powerpoint geschlossen

Kerstin Zapf

Am *Microsoft Patch Day* im Mai wurde nur ein einziges Update (MS09-017) veröffentlicht, das jedoch gleich 14 Sicherheitsmängel behebt. Diese betreffen alle *Powerpoint* in den Versionen 2000, 2002, 2003, 2007 und die *Powerpoint-Viewer 2003* und *2007*.
Bei einer der Lücken handelt es sich um die bereits seit Anfang April bekannte und mehrfach aktiv ausgenutzte Schwachstelle. Jedoch werden auch noch 12 der anderen Fehler von Microsoft als kritisch eingestuft und es ist mit zukünftigen Ausnutzungen zu rechnen. Da in diesen Fällen das Einschleusen von Schadcodes möglich ist, ist es dringend zu empfehlen, das Update schnellstmöglich einzuspielen.
Sofern nicht über die automatische *Microsoft Update*-Funktion bezogen, kann es über folgende Webseite heruntergeladen werden:

http://windowsupdate.microsoft.com

Auch die *Office*-Versionen für Mac 2004 und 2008 sind von den Lücken betroffen, jedoch liegen hierfür noch keine Updates vor. Eine ausführliche Beschreibung der Fehler findet sich auf dem Link zu den *Security Bulletins*:

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

Neues aus dem Spionage-Handbuch

Arno Spieth

Die seit einem Monat kursierenden Gerüchte, dass sich mit einem alten Nokia-Handy, für das Kriminelle bis 25.000 Euro geboten hatten, SMS anderer Rufnummern abhören lassen, hat das niederländische Sicherheitsunternehmen *Ultrascan Knowledge Process Outsourcing* bestätigt. Damit ist es potentiell möglich, mTANs abzufangen und sie für Banktransaktionen zu benutzen. Was noch fehlt, sind die Zugangsdaten zu den Bankkonten.
Diesbezüglich gibt es inzwischen natürlich auch die geeigneten Maßnahmen. Die Universität des Saarlandes hat schon im letzten Jahr gezeigt, sauberes Geschirr in der Nähe eines Bildschirms lässt sich mit Hilfe eines Teleskops als hervorragender Spiegel benutzen, der den Bildschirminhalt den Mitmenschen vertraut macht.
Sie werden einwenden, das nützt nichts, denn auf dem Bildschirm ist zumindest das Kennwort ja glücklicherweise nur als Sternchen-Reihe sichtbar. Aufwendige Maßnahmen, wie Key-Logger oder Trojaner lassen wir mal beiseite. Auf der Sicherheitskonferenz *CanSecWest* hat die britische Sicherheitsfirma *Inverse Path* gezeigt, dass es auch einfacher geht. Mit einem geeigneten Mikrofon lassen sich, so unglaublich es sich anhört, die Tastenklicks belauschen und mit einer Software ähnlich einem Texterkennungsprogramm auswerten. Hierzu siehe folgenden Spiegel-Artikel:

http://www.spiegel.de/netzwelt/tech/0,1518,614887,00.html

Mikrofone hat der vor kurzem mit dem *IBM Faculty Award* ausgezeichnete Professor Backes wieder von der Universität des Saarlandes jetzt auch benutzt, um Nadeldrucker abzuhören. Das ist einfach, da diese häufig noch in Arztpraxen anzutreffenden altmodischen Geräte ja schließlich genug Lärm machen. Interessant ist jetzt wieder, dass es ihm gelungen ist, aus dem Lärm den Text zu entschlüsseln, den diese Drucker gedruckt haben – siehe:

http://www.uni-saarland.de/de/aktuelles/presse/news-lesen/datum/2009/05/27/druckergeraeusche-verraten-patientenakten-und-kontodaten.html

Damit klappen wir das Handbuch lieber wieder zu.

TEAM Drucken

FollowMe-Drucklösung von Ricoh in Betrieb genommen

Rolf Bogus

Die Druckerfirma Ricoh, die die öffentlichen Kopierer in der Universität betreibt, bietet inzwischen auch eine Drucklösung auf ihren öffentlichen Kopierern an. Druckfertige Dokumente vom Typ Postscript (Endung `.ps`), PDF (Endung `pdf`) oder TIFF (Endung `tif`) können Sie direkt über die Webseite

http://ricohsrv1.urz.uni-heidelberg.de:8080

auf den Ricoh-Druckserver übertragen. Dabei müssen Sie sich mit Ihrer Uni-ID (oder Ihrer URZ-Kennung) anmelden.
Der Ausdruck kann dann an jedem öffentlichen Kopierer, der schon mit der nötigen Druckerschnittstelle ausgerüstet ist, erfolgen. Nachdem Sie sich wieder mit Ihrer Uni-ID bzw. URZ-Kennung mit Kennwort angemeldet haben, können Sie dann aus einer Liste Ihrer auf den Ricoh-Druckserver übertragenen Druckaufträge die auszudruckenden Aufträge auswählen. Es ist darauf zu achten, dass beim Ausdrucken die Campus-Karte eingeschoben wird, sonst wird kein Papier bedruckt.

Aus einer Anwendung (z.B. Word oder Powerpoint) auf dem Rechner, auf dem Sie arbeiten, können Sie nur dann drucken, wenn der Rechner den erforderlichen Ricoh-Drucker installiert hat. Näheres und eine Beschreibung der Ricoh-Drucklösung finden Sie auf den URZ-Webseiten unter

http://www.urz.uni-heidelberg.de/drucken/

in den Unterpunkten „Dezentrale Drucksysteme“.
Das URZ weist darauf hin, dass die Ricoh-Drucklösung völlig unabhängig von dem vom URZ betriebenen Drucksystem (zentral oder in den über das URZ angesteuerten Pooldruckern) läuft. Insbesondere gibt es beim Drucken über die Ricoh FollowMe-Drucklösung kein Freikontingent.

TEAM Anwendungssoftware

PDF schlägt DOC-Format

Arno Spieth

Immer wieder haben wir in der letzen Zeit darauf hingewiesen, dass nicht nur Patches und Updates von Betriebssystemen und Office-Programmen eingespielt werden sollen, sondern auch die Patches einer Anwendung, des Acrobat Readers, erwähnt, der sich im Internet zunehmender Beliebtheit erfreut. PDF-Dateien, deren Druckbild sich im Gegensatz zu HTML-Dateien nicht sehr von der Bildschirmausgabe unterscheidet, verbreiten sich dank großzügiger Bandbreiten schneller als ein Schweinegrippe-Virus.
Sie werden vielleicht fragen: Ein Textformat, wo soll da die Gefahr herkommen? Wenn Sie ein PDF-Formular vorgelegt bekommen, dann können Sie es Ausdrucken oder Sie können es online ausfüllen. Und wenn Sie bei der Telefonnummer Buchstaben eingeben, dann bekommen Sie eine Fehlermeldung. Trivial, aber wie geht das? Im PDF-Format ist nicht nur Text enthalten, sondern auch Programmcode, der via Javascript ausgeführt wird. So wird Ihr scheinbarer Text zu einer ausführbaren Datei.
Man kennt das schon länger von Word und seiner großzügigen Macro-Programmierung. Deshalb sollte sich langsam bei jedem eingeprägen, dass man bevor man auf eine DOC-Datei klickt, kurz darüber nachdenkt, ob dem Verfasser zu trauen ist. Sei es ein Mail-Anhang, ein Link auf einer Internetseite oder der Inhalt eines Speichermediums.
Das wäre noch keine 100%-ige Sicherheit, doch ein erster Schritt, aber wer verschwendet einen Gedanken bei einem Klick auf eine PDF-Datei? Wenn Sie vorsichtig sind, dann haben Sie im Browser Javascript deaktiviert. Aber haben Sie auch im Acrobat Reader von Adobe dieses Feature ausgeschaltet oder haben Sie sich einen alternativen PDF-Reader zugelegt, der nicht so erfolgreich angegriffen wird? Vermutlich nicht.
Der Vergleich der Überträger von Schadprogrammen aus 2008 und dem Anfang von 2009 weist in eine unheilvolle Richtung. Wurden 2008 bei knapp 2000 als schädlich identifizierten Dateien in 34,55% der Fälle MS-Word infiziert und „nur“ in 28,61% der Fälle der Acrobat Reader, so konnten im ersten Vierteljahr 2009 bei 663 Malware-Dateien als Zielprogramm in fast 50% der Fälle der Acrobat-Reader erkannt werden sowie bei weiteren 40% der Fälle das Zielprogramm MS-Word. Von Entwarnung beim DOC-Format kann also keine Rede sein.
Auch im diesem Monat wurden wieder Updates von Adobe herausgebracht, die zwei Sicherheitslücken stopfen. Auch wenn bisher noch keine Dateien gefunden wurden, die diese Sicherheitslöcher ausnutzen, sollten Sie die Patches zeitnah einspielen.

TEAM Unix-Systeme

Studie zum Einsatz von Linux auf dem Desktop

Jana Motzet

Eine im Auftrag von IBM vorgestellte Studie von *Freeform Dynamics* untersuchte den Status des Einsatzes von Linux auf dem Desktop im geschäftlichen Rahmen. Die Studie befragte international über 1200 IT-Spezialisten zum Einsatz von Linux auf dem Desktop im Geschäftsumfeld. Hierbei gaben 70% der Befragten an, ihr Umstieg auf Linux sei aus Gründen der Kostenreduktion motiviert gewesen. Die beiden nächst häufig genannten Gründe waren Stabilität und Sicherheit. Laut Angaben der Befragten wird Linux bisher auf weniger als 20% der Geschäfts-Desktops verwendet, wobei sich jedoch die meisten eine Migration weiterer Desktops vorstellen können.
Zu den möglichen Einsatzgebieten von Linux-Desktops stellte die Studie fest, dass sich die Migration meist als weniger problematisch als angenommen erweise und die Anwendungen für grundlegende Büroanwendungen gut handhabbar seien. So seien auch weniger technisch versierte Nutzer in der Lage auf dieser Ebene mit Linux umzugehen, da sich auf Office-Anwendungen, E-Mails und andere Äquivalente zu den üblichen Windows-Anwendungen gut unter Linux bedienen lassen. Hier setzen laut Studie allerdings bisher wenige Unternehmen Linux ein. Probleme hingegen, mit Linux-Desktops auszukommen stellen sich vielmehr in einer anderen Zielgruppe dar, nämlich bei Power-Usern, sehr mobilen und kreativ anspruchsvollen Nutzern.
Alle Ergebnisse der Studie können in der kostenlosen Online-Version unter folgendem Link nachgelesen werden:

http://www.freeformdynamics.com/fullarticle.asp?aid=678

Termine

Kurse im URZ

Edith Pokrandt

Im kommenden Monat beginnen bzw. finden am URZ folgende, chronologisch aufgeführte Kurse statt:

2-Tageskurs: Das Datenanalysesystem SPSS
Dr. Carina Ortseifen, 08.06.+09.06.09, 13.00–17.00 Uhr
Bewerbungsunterlagen umwandeln für die Online-Bewerbung
Ingo Schmidt, 09.06.09, 15.00–17.00 Uhr
Linux-Treff am URZ
Kirsten Glöer, Venelin Petkov, 15.06.09, 15.15–17.00 Uhr
4-Tageskurs: Fortgeschr. Videobearbeitung mit Finalcut Pro
Klaus Kirchner, mo., 15.06.–06.07.09, 15.15–18.00 Uhr
2-Tageskurs: PowerPoint für Anfänger (Version 2007)
Henriette Höhle, 16.+17.06.09, 9.15–16.00 Uhr
2-Tageskurs: Einführung in die Videobearbeitung am Mac
Michaela Wirth, 18.+19.06.09, 15.15–18.00 Uhr
2-Tageskurs: Tabellenkalulation mit Excel 2007
Michaela Wirth, 18.+19.06.09, 9.15–16.00 Uhr
1-Tageskurs: Einführung in EndNote
Michaela Wirth, 24.06.09, 9.30–12.00 Uhr
2-Tageskurs: PowerPoint für Anfänger (Version 2007)
Henriette Höhle, 29.+30.06.09, 9.15–16.00 Uhr

Genauere Informationen und Anmeldung unter:

http://www.urz.uni-heidelberg.de/ausbildung/kurse.html

Impressum

Herausgeber: Rechenzentrum der Universität Heidelberg
Redaktion: Dr. Carina Ortseifen, Arno Spieth, Joachim Lammarsch, Jana Motzet
Verteiler: ATT-URZ@urz.uni-heidelberg.de
Layout: Luzia Dietsche, Joachim Lammarsch
Produktion: TeXlive 2007, LaTeX 2_ε und pdfTeXk Vers. 3.141592-1.40.3