GWDG
Nachrichten

für die Benutzerinnen und Benutzer des Rechenzentrums

GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Ausgabe 3/2012

Inhalt

IMPRESSUM

GWDG-Nachrichten für die Benutzerinnen und Benutzer des Rechenzentrums
ISSN 0940-4686
35. Jahrgang, Ausgabe 3/2012 **Erscheinungsweise: monatlich**
www.gwdg.de/gwdg-nr **Auflage: 500**

Titelfoto: Blick in die GWDG-Bibliothek, für die das Bibliothekssystem Aleph genutzt wird

Herausgeber:	**Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen**		
	Am Faßberg 11		
	37077 Göttingen	**Tel.: 0551 201-1510**	**Fax: 0551 201-2150**
Redaktion:	**Dr. Thomas Otto**	**Tel.: 0551 201-1828**	**E-Mail: Thomas.Otto@gwdg.de**
Herstellung:	**Maria Geraci**	**Tel.: 0551 201-1804**	**E-Mail: Maria.Geraci@gwdg.de**
Druck:	**GWDG / AG H**	**Tel.: 0551 201-1523**	**E-Mail: printservice@gwdg.de**

Tipps für Datennomaden – Dateiverschlüsselung

Die Verschlüsselung von Dateien ist eine effektive Methode, Dateien dauerhaft vor fremdem Zugriff zu schützen, auch wenn diese über unsichere Wege übertragen werden oder der Zugriff auf die Dateien nicht kontrolliert werden kann. Verschlüsselung muss nicht schwierig oder umständlich sein und ist sicher, wenn ein paar Regeln beachtet werden. Im Folgenden werden zunächst ein paar grundsätzliche Informationen zur Sicherheit gegeben, anschließend ein paar Herangehensweisen an Dateiverschlüsselung erklärt und diese dann an Beispielen gezeigt. Die dabei verwendete Software ist frei und kostenlos.

Warum Dateien verschlüsseln?

Wer viel unterwegs ist und seine Daten und Dateien mit sich führt oder zumindest seine Dateien über unsichere Wege auf die Reise schickt, ist gut beraten, sich über die Sicherheit dieser Informationen Gedanken zu machen. Dies betrifft Dateien, die auf mobilen PCs liegen, welche man auf der Reise mit sich führt, genauso wie Dateien, die über unbekannte Netze gesendet werden, wie sie das Internet bilden, z. B. per E-Mail-Anhang oder über einen Dienst als Download für Dritte.

Banale und an sich harmlose Anlässe können dazu führen, dass man die Kontrolle darüber verliert, wer Zugriff auf die eigenen Daten – oder schlimmer die des Arbeitgebers – hat, z. B. wenn ein Laptop defekt ist und zur Reparatur gesendet wird. Wer direkten Zugang zum PC hat, erlangt normalerweise auch direkten Zugang zu den darauf gespeicherten Daten, trotz einer durch ein Passwort geschützten Anmeldung am Betriebssystem. Außer: die sensiblen Daten sind selber verschlüsselt.

Werden Daten und Dateien über ein Netzwerk gesendet, kann prinzipiell jeder, der die Kontrolle über Teile des genutzten Netzwerks hat, diese Daten mitschneiden und analysieren. Viele Programme und Dienste im Internet setzten aus diesem Grund auf eine Verschlüsselung bei der Datenübertragung, worauf man als Benutzer auch immer achten sollte. Existiert keine oder ist diese nicht vertrauenswürdig, ist man als Benutzer auf der sicheren Seite, die zu übertragenen Dateien und Daten selber zu verschlüsseln.

Grundsätzlich sollte eine Dateiverschlüsselung so sicher sein, dass die Informationen auch dann noch sicher sind, wenn die Personen oder Parteien, vor denen die Informationen verborgen werden sollen, sehr einfach Zugriff auf die verschlüsselten Dateien haben.

Im Folgenden sollen praxisnah und mit Beispielen einige Anwendungsfälle und die genutzten Werkzeuge erklärt werden. Gute Verschlüsselung ist technisch und konzeptionell sehr komplex und ein weites Feld, auf dem oft die besten Mathematiker tätig sind. Glücklicherweise haben sich einige Standards und Strategien herausgebildet, an denen sich jeder Benutzer leicht orientieren kann und die hier aufgegriffen werden sollen.

Was macht eine Verschlüsselung sicher?

Es gibt grundsätzlich zwei Punkte, in denen der Schutz einer Verschlüsselung versagen kann: technisch/konzeptionell und beim verwendeten Schlüssel (meistens ein Passwort).

Gilt ein Verschlüsselungsalgorithmus allgemein als sicher in seinem Konzept und der Umsetzung, muss man als Benutzer nur darauf achten, dass die angedachte Software diesen auch verwendet. Ein Blick in die Dokumentation, Hilfetexte oder auf die Internetseite der Software gibt dabei meist schon Aufschluss. Sind die dort genannten Verschlüsselungen einem nicht bekannt oder werden nicht kurz erläutert, hilft oft eine Suche im Internet oder direkt ein Blick bei Wikipedia.

Ein Punkt, der leider häufig nicht beachtet wird, ist das Vertrauen in die Umsetzung der Verschlüsselung. Verspricht ein Hersteller in einer Software eine bestimmte Funktion, kann man als Anwender diese häufig einfach ausprobieren und so feststellen, ob der Anbieter das Versprochene hält. Bei Verschlüsselungen ist das schwierig, da dazu eine Kryptoanalyse [1] durchgeführt werden müsste, was eine Aufgabe für Fachleute ist, und Hersteller zudem meist nicht bereit sind, Informationen

über ihre Implementierung preiszugeben. Und blindes Vertrauen ist eine schlechte Grundlage für die sichere Aufbewahrung und Übermittlung von Informationen. Ein möglicher Ausweg ist hierbei der Einsatz von Software, deren Quellcode offen zugänglich ist [2] und die bereits von vielen Benutzern verwendet wird. Dies reduziert die Wahrscheinlichkeit, dass z. B. eine an sich sichere Verschlüsselung eingesetzt wird, aber aufgrund von schlechter Implementierung die erzeugten Schlüssel leicht vorhersagbar sind. Auch wenn es nicht offensichtlich scheint, ist eine Software, deren Aufgabe das Verstecken von Informationen ist, trotzdem und gerade deshalb sicher, obwohl alle Details ihrer Funktionsweise bekannt sind, weil das verwendete Konzept sicher ist. Bei einem sicheren Konzept und der guten Implementierung gibt es keinen „geheimen Trick" oder eine „versteckte Hintertür", die Zugang zu den Informationen ohne den richtigen Schlüssel ermöglicht.

Das Gegenstück ist die (vermeintliche) „Sicherheit durch Verschleierung" („Security by obscurity" [3]). Ist die Funktionsweise einer Verschlüsselung nicht überprüfbar, kann man sich nur auf die Aussagen des Herstellers verlassen. Im Zweifelsfall sind dann Schwachstellen dem Angreifer, aber nicht dem Benutzer bekannt. Dieser verlässt sich weiter auf das System, obwohl der Schutz bereits nicht mehr existiert.

Die beste Verschlüsselung nutzt aber leider nichts, wenn der Schlüssel in Form eines Passworts nicht sicher ist oder – schlimmer noch – dem Angreifer bereits bekannt ist. Letzteres kann passieren, wenn das Passwort an einem PC eingegeben wurde, der mit einem Trojaner infiziert ist, welcher die Eingabe von Passwörtern mitschneidet. Oder der Angreifer erlangt Zugriff auf einen Ort, wo Passwörter gespeichert sind, z. B. in den Einstellungen eines Browsers. Bei der Arbeit mit Passwörtern sollte ein Benutzer diese Punkte immer im Hinterkopf haben.

Ist das Passwort sehr schwach, kann es dem Angreifer unter u. U. sogar gelingen, das Passwort durch Ausprobieren herauszufinden. Man kann sich dies am Beispiel einer ec-Karte und deren PIN deutlich machen. Ist ein Angreifer im Besitz der ec-Karte (analog zu der verschlüsselten Datei), kann er immer noch nicht am Geldautomaten das Geld des zugehörigen Kontos abheben (analog zu den enthaltenen Informationen der verschlüsselten Datei), weil eine PIN benötigt wird (analog zum Passwort für die Entschlüsselung). Dass bei einer ec-Karte Bezahlungen gegen eine leicht zu fälschende Unterschrift möglich sind, sei hier außer acht gelassen. Die PIN einer ec-Karte besteht aus vier Stellen der Ziffern 0 - 9 und damit 10.000 möglichen Kombinationen [4]. Ein Angreifer muss lediglich alle Kombinationen ausprobieren, um garantiert die richtige, funktionierende PIN zu finden. Aus der Praxis wissen wir, das nach drei falschen Eingaben die Karte gesperrt ist und nur durch die Bank wieder freigegeben werden kann. Dies ist in dem Fall ec-Karte ein guter Schutz und macht ec-Karten relativ sicher. In der Datenverarbeitung und so auch bei vielen Diensten der GWDG wird ähnlich verfahren; mehrere Fehlversuche beim Anmelden führen zur Sperrung eines Benutzerkontos.

Im Falle von verschlüsselten Dateien kann es aber Situationen geben, in denen der Angreifer im Besitz der Datei ist und automatisiert beliebig viele Versuche durchführen kann. In einem solchen Szenario ist es nur eine Frage der Zeit, bis das richtige Passwort gefunden wurde, und die Zeitdauer ist nur abhängig von der Rechenleistung des Angreifers. Abgesehen von einigen besonderen Fällen kann der zeitliche Aufwand des Angreifers nur erhöht werden, indem ein langes und komplexes Passwort [5] gewählt wird, das keine bekannten Begriffe enthält. Theoretisch gesehen ist ein Passwort damit immer nur ein Schutz auf Zeit. In der Praxis werden Versuche, ein Passwort alleine durch Ausprobieren zu ermitteln, aber meistens uninteressant, wenn z. B. mehrere Monate oder gar Jahre an Rechenzeit investiert werden müssten.

Wer also als Benutzer in der Praxis für seine Anwendung eine bekannte, sichere Verschlüsselung mit einem Passwort verwendet, das den empfohlenen Regeln entspricht, und etwas Vorsicht walten lässt, wo er dieses Passwort eingibt, speichert und notiert, der kann seine Informationen effektiv schützen.

Ein Tipp für weitere Informationen: In dem Artikel „Sicherheit und Vertraulichkeit: Grundlagen der Verschlüsselung" in den GWDG-Nachrichten 9/2011 [6] wird genauer auf die theoretischen Grundlagen von Verschlüsselungstechniken eingegangen und eine Reihe von verwendeten

Verfahren und Prinzipien erläutert.

Die Anwendung

Was wird verschlüsselt?

Will man nun Informationen verschlüsseln, eignen sich für den jeweiligen Anwendungsfall unterschiedliche Werkzeuge unterschiedlich gut. Im Folgenden soll es nur um Dateiverschlüsselung gehen. In den GWDG-Nachrichten 10/2011 im Artikel „Sicherheit und Vertraulichkeit: Authentifizierung und Verschlüsselung im Internet“ werden detailliert die Funktion, Beantragung, Installation und Verwendung von Zertifikaten für das Signieren und Verschlüsseln von E-Mails beschrieben. Diese gut funktionierende Methode wird jedem Benutzer zum Versenden von besonders schützenswerten Informationen per E-Mail sehr empfohlen. Verschlüsselte Protokolle, z. B. SSL bei Verwendung von HTTPS [7], sichern Informationen aber nur während einer Übertragung ab. Bei Dateiverschlüsselung geht es um das sichere Aufbewahren von Informationen, also um das Speichern der Informationen in einem verschlüsselten Zustand. Sollen diese Dateien in ihrem verschlüsselten Zustand übertragen werden, kann das auch über ein unsicheres, offenes Protokoll geschehen, da die Informationen geschützt und nicht ohne den zugehörigen Schlüssel lesbar sind.

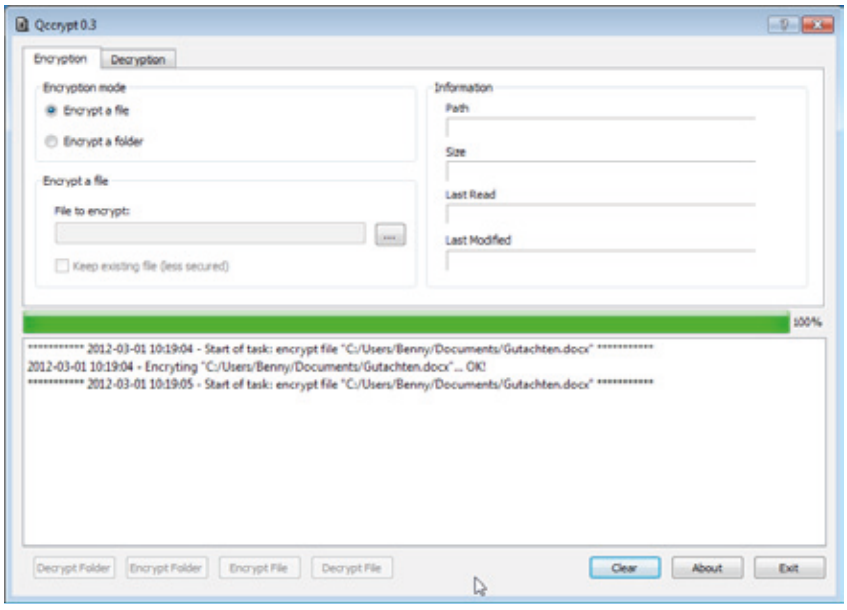
Bei der konkreten Verschlüsselung der Dateien kann man nun wählen, ob man die einzelne Datei selber verschlüsselt, eine Art Container nimmt, in dem Dateien abgelegt werden, und diesen dann verschlüsselt, oder ob man ein ganzes Dateisystem mit allen enthaltenen Dateien verschlüsselt, z. B. einen USB-Stick oder die Partition einer Festplatte.

Verschlüsselung einer Datei

Eine einzelne Datei zu verschlüsseln, ist besonders praktisch für E-Mail-Anhänge und ähnliche, dateibasierte Datentransfers, wo sonst keine weitere Absicherung in Form einer Verschlüsselung zur Verfügung steht. Will man also z. B. zwei Kollegen ein Gutachten als Word-Datei per E-Mail schicken, E-Mail-Verschlüsselung aber nicht zur Verfügung steht, kann man die Word-Datei verschlüsseln, versenden und den beiden Kollegen z. B. per Telefon das Passwort mitteilen.

Ein Programm, welches diese Aufgabe einfach und unkompliziert lösen kann, ist „**ccrypt**“ [8]. Der Programmcode ist offen und frei zugänglich, womit er dem Anspruch an Transparenz genügt. Laut dem Autor setzt es für die Verschlüsselung den Standard „AES“ [9] ein, der allgemein als sehr sicher gilt. Da der Standard und der Programmcode von ccrypt offen ist, wäre dieser Umstand z. B. für jeden Benutzer nachprüfbar. Damit genügt das Programm dem gewünschten Sicherheitsanspruch. Das Programm ist nicht nur Open Source, sondern auch noch kostenlos. Zudem bietet der Autor Versionen für Windows, Mac OS X, Linux und verschiedene Server-Betriebssysteme an. Dies sind wichtige Punkte für die Praxis, da so sichergestellt ist, das alle Empfänger die zu sendende Datei verarbeiten können, unabhängig vom verwendeten System. Einziger praktischer Nachteil ist, dass es ein Programm nur für die Kommandozeile/das Terminal [10] ist, was viele Benutzer als umständlich empfinden. Glücklicherweise wurden für das Programm von Dritten auch zwei Programmoberflächen geschrieben, z. B. „**Qccrypt**“ [11]. Für Qccrypt gelten die gleichen, vorher genannten Bedingungen, womit nichts gegen den Einsatz spricht.

Im Download-Bereich gibt es ein „Windows Installer Package“ zum Herunterladen und Installieren. Nach der Installation steht das Programm „Qccrypt“ im Startme-



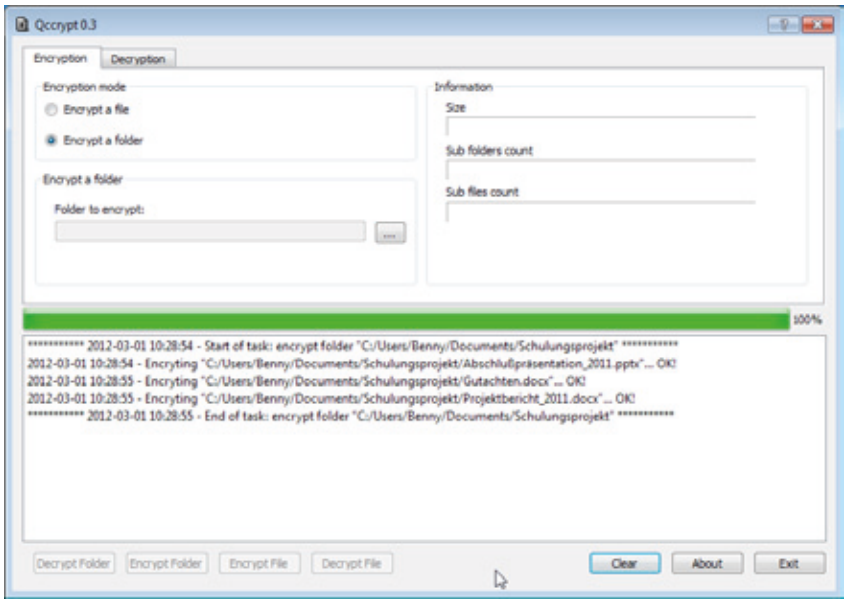
1 *Qccrypt nach der Verschlüsselung einer Datei*

nü unter „Alle Programme“ zur Verfügung und kann gestartet werden. Die Programmoberfläche hat zwei Registerkarten, eine stellt die Optionen für Verschlüsselung (encryption) und eine für Entschlüsselung (decryption) dar. Außerdem kann ausgewählt werden, ob eine einzelne Datei oder alle Dateien in einem Ordner verschlüsselt werden sollen sowie die zu bearbeitende Datei bzw. den Ordner (siehe Abb. 1).

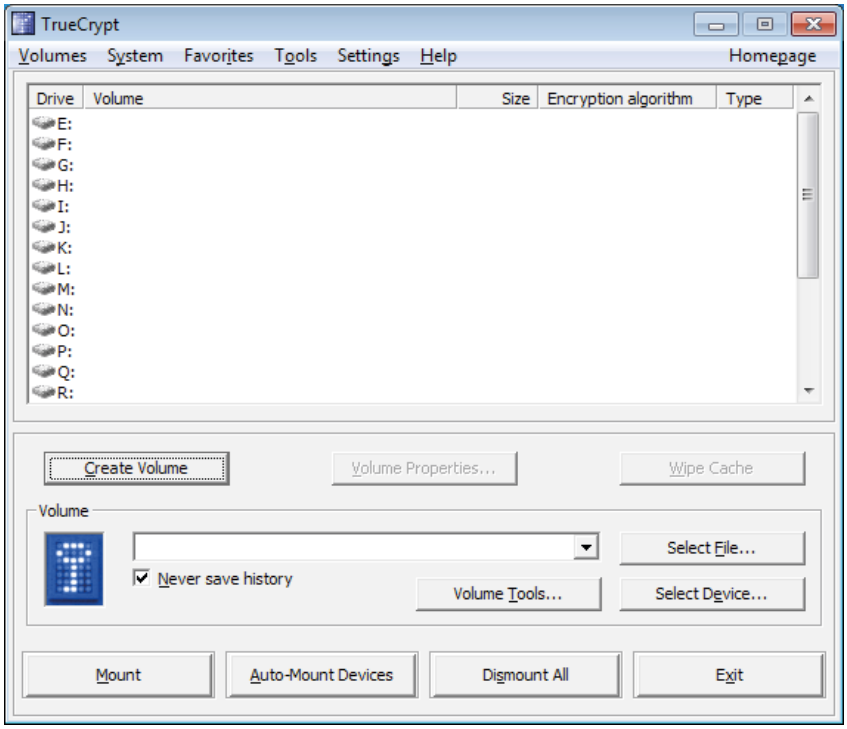
Um nun eine wichtige Datei zu verschlüsseln, wird unter „Encrypt a file“ eine Datei über die „...“-Schaltfläche ausgewählt, der Knopf „Encrypt file“ gedrückt, ein Passwort zweimal eingetippt und mit „ok“ der Vorgang gestartet. Ein Dialog bestätigt, dass die Datei erfolgreich verschlüsselt wurde, und in der unteren Hälfte des Programms werden ein paar Informationen zu dem Vorgang dargestellt. Damit sind die Datei erfolgreich verschlüsselt und der Inhalt durch eine starke Verschlüsselung mit einem sicheren Passwort geschützt.

Zur Entschlüsselung wird zur Registerkarte „Decryption“ gewechselt, wie vorher die nun verschlüsselte Datei ausgewählt und mit dem Drücken von „Decrypt file“ die Entschlüsselung gestartet. Nach Eingabe des richtigen Passworts ist die Entschlüsselung abgeschlossen und mit der Datei kann wieder normal gearbeitet werden.

Bei der Funktion „Encrypt a folder“ wird statt einer einzelnen Datei ein Dateiordner angegeben. Qccrypt verschlüsselt dann jede enthaltene Datei nacheinander. In dem Infofeld in der unteren Hälfte des Programms findet man die



2 *Qccrypt nach der Verschlüsselung von Dateien in einem Ordner*



3 *TrueCrypt-Programmoberfläche*

Meldungen aller verarbeiteten Dateien (siehe Abb. 2). Die Entschlüsselung eines ganzen Dateiordners funktioniert analog.

Sollen mehrere Dateien aufbewahrt oder versendet werden, ist es auch eine gute Idee, diese vorher in einer Zip-Datei [12] zusammenzufassen und ihre Größe zu reduzieren und die dann entstandene Datei zu verschlüsseln. Zur Wiederherstellung werden die Schritte einfach in umgekehrter Reihenfolge rückgängig gemacht.

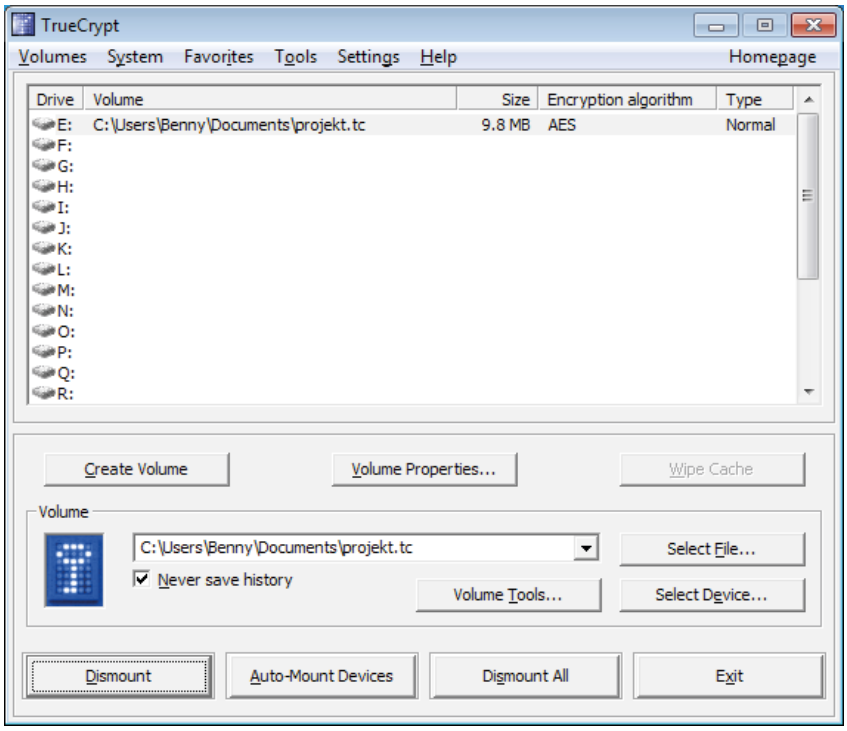
Verschlüsselung mehrerer Dateien in einem Container

Es kann Anwendungsfälle geben, in denen mit verschlüsselten Dateien häufig gearbeitet werden soll, so dass diese immer wieder entschlüsselt und wieder verschlüsselt werden müssten.

Steigt die Anzahl der betroffenen Dateien, erhöhen sich auch jedes Mal die Arbeitsschritte. Hier kann es praktisch sein, mit einer Software eine größere, verschlüsselte Container-Datei anzulegen und einzelne Dateien darin zu speichern. Dieser Container kann wie ein Laufwerk – ähnlich einem USB-Stick – behandelt werden. Dateien können darin abgelegt, geöffnet, bearbeitet und davon gelöscht werden. Die Verschlüsselung übernimmt die Software und sobald die Container-Datei geschlossen wird, sind die Informationen sicher.

Eine bekannte Software (siehe Abb. 3), die diese Möglichkeiten bietet, ist „**TrueCrypt**“ [13]. Der Programmcode ist offen und frei zugänglich, womit die Software transparent ist. TrueCrypt unterstützt die Verschlüsselung nach AES, Serpent und Twofish [14] bzw. Kombinationen aus diesen, welche als sehr sicher gelten. Die verwendeten Standards sind sicher und ihre Implementierungen bekannt; einem Einsatz steht also nichts entgegen. Zusätzlich gibt es die Software für die drei bekanntesten Desktop-Betriebssysteme Windows, Mac OS X und Linux, wobei die erzeugten Container untereinander kompatibel sind, wenn ein gemeinsam unterstütztes Dateisystem für den Container gewählt wird. Damit ist die Möglichkeit, mit den Containern und den enthaltenen Informationen in unterschiedlichen Umgebungen zu arbeiten, gewährleistet. Für die Grundfunktionen steht ein „Beginner's Tutorial“ [15] zur Verfügung.

Nach der Installation von TrueCrypt steht es unter „Alle Programme“ zur Verfügung. Um den



4 *Geöffneter Dateicontainer in TrueCrypt*

beschriebenen Fall umzusetzen, klickt man auf „Create Volume“, wählt „Create an encrypted file container“ aus, „Standard TrueCrypt volume“ im nächsten Schritt, dann einen Speicherort und Dateinamen für die Container-Datei, dann die vorgegebenen Verschlüsselungstechniken, danach die Größe des Containers und das Passwort für die Verschlüsselung. Im letzten Schritt wird dann im Container eine Dateisystem angelegt, worin Dateien gespeichert werden können. Soll der Container sehr große Dateien von 2 GByte und mehr aufnehmen können oder Dateien und Ordner mit sehr langen Namen, sollte als Dateisystem NTFS gewählt werden, das Standarddateisystem von Windows. In den meisten Fällen kann Linux damit ebenfalls umgehen, Max OS X kann es lesen und mit zusätzlicher Software auch schreiben [16]. Wird der Container nur mit Windows-Systemen genutzt, ist NTFS die bessere Wahl. Bestehen Zweifel, aber sehr große Dateien oder sehr lange Dateinamen werden nicht benötigt, ist FAT die bessere Wahl. Mit einem Klick auf „Format“ wird die Erstellung abgeschlossen.

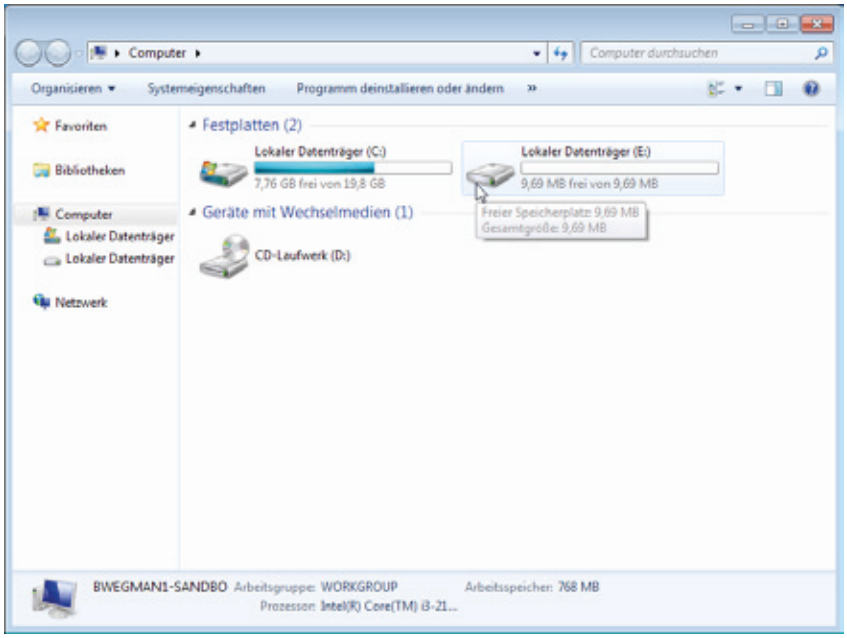
Um nun mit dem Container arbeiten zu können, muss er geöffnet werden, analog zu einem USB-Stick, der erst angeschlossen werden muss. Dazu wählt man in der Oberfläche von TrueCrypt (unter Windows) einen Laufwerksbuchstaben aus der Liste aus und mit einem Klick auf „Select file“ die zuvor erstellte Container-Datei (siehe Abb. 4). Der Container wird nun unter dem ausgewählten Laufwerksbuchstaben geöffnet, wenn man auf den Knopf „Mount“ klickt und das richtige Passwort angibt.

Nun findet sich der Container geöffnet als Laufwerk unter der Liste der Laufwerke im Explorer wieder (siehe Abb. 5). Dateien können nun beliebig hinein verschoben

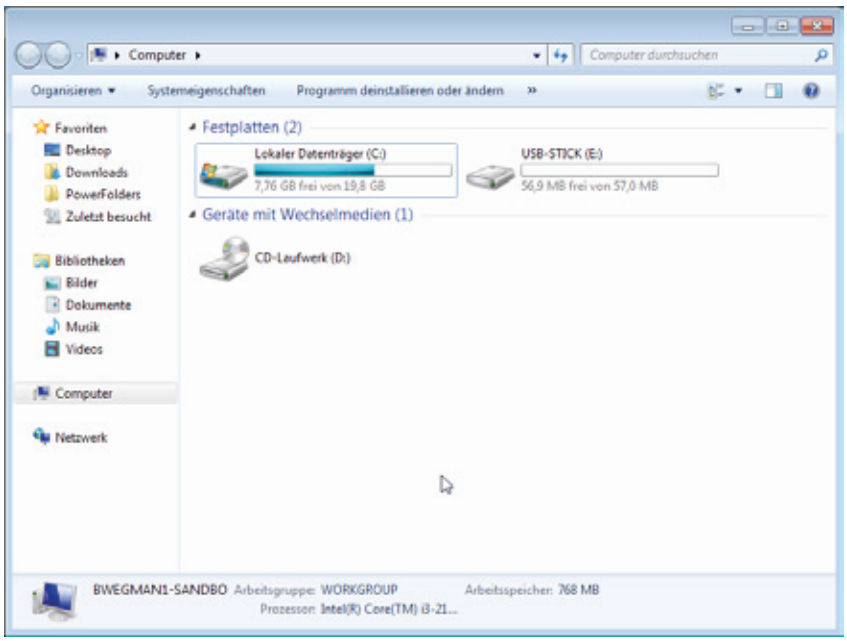
oder darin erstellt werden. Der Container steht allen Anwendungen wie jedes andere Laufwerk zur Verfügung. Die TrueCrypt-Oberfläche kann nun mit einem Klick auf „Exit“ in den Hintergrund gebracht werden und ist über das Schlüsselsymbol in der Symbolleiste neben der Uhr wieder erreichbar.

Ist die Arbeit mit dem Container abgeschlossen, kann und sollte dieser über die TrueCrypt-Oberfläche geschlossen werden. Dazu ruft man die Oberfläche über das Schlüsselsymbol auf, wählt den Laufwerksbuchstaben aus und schließt den Container mit einem Klick auf „Dismount“. Wenn es zu einer Fehlermeldung kommt, dass der Container nicht geschlossen werden kann, sind darin enthaltene Dateien wahrscheinlich noch von einer Anwendung geöffnet. Sind alle entsprechenden Anwendungen beendet, kann der Container geschlossen werden.

Wichtig ist, dass die Verschlüsselung nur Schutz bietet, wenn der Container geschlossen ist. Ist er geöffnet, kann auf den entschlüsselten Inhalt genauso zugegriffen werden, wie auf alle übrigen Dateien. Im geschlossenen Zustand sind die Informationen aber auch dann geschützt, wenn jemand vollen Zugriff auf den Inhalt der Festplatte oder anderer Datenträger erlangt, auf denen der Container gespeichert ist. Geschlossen ist dieser eine normale Datei, die zum Versenden z. B. auch mit Zip komprimiert werden oder an beliebige Stellen verschoben und kopiert werden kann.



5 *Geöffneter Dateicontainer im Explorer als Laufwerk E:*



6 *USB-Stick vor der Verschlüsselung*

Verschlüsselung von Laufwerken

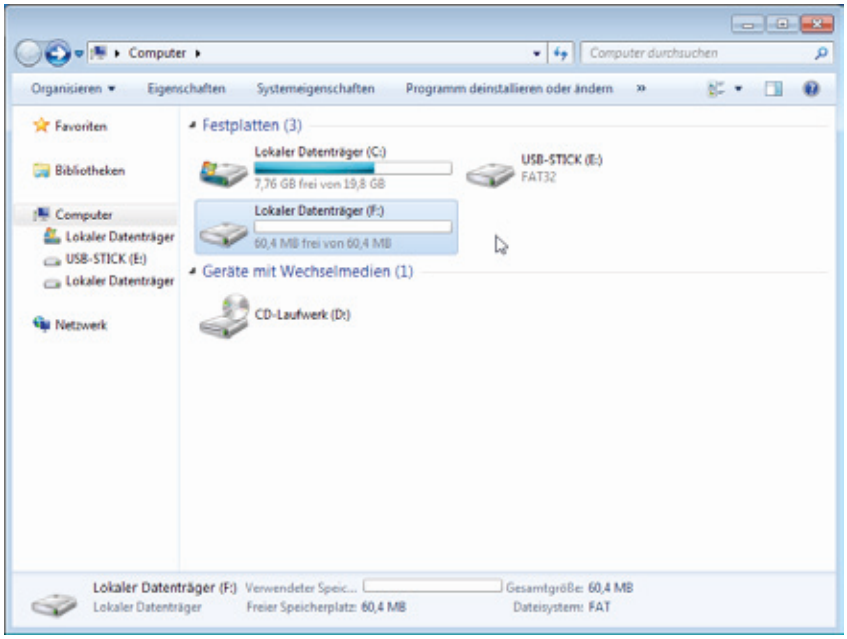
Die oben beschriebene Vorgehensweise mit Containern bietet den Vorteil, dass diese recht mobil sind, da sie im geschlossenen Zustand weitgehend wie jede andere Datei auch behandelt werden können. Nachteilig ist, dass die Container in ihrer Größe nicht mehr verändert werden können und in Einzelfällen die Geschwindigkeit geringer ist, als wenn direkt auf dem Laufwerk des Containers gearbeitet werden würde.

Mit TrueCrypt ist es aber auch möglich, ganze Geräte bzw. einzelne Partitionen zu verschlüsseln. Dabei wird eine Verschlüsselung über einen ganzen Datenträger oder seine Partition gelegt, dieser dann als neues Laufwerk geöffnet, in dem sich dann ein Dateisystem befindet, mit welchem wieder wie im obigen Beispiel gearbeitet

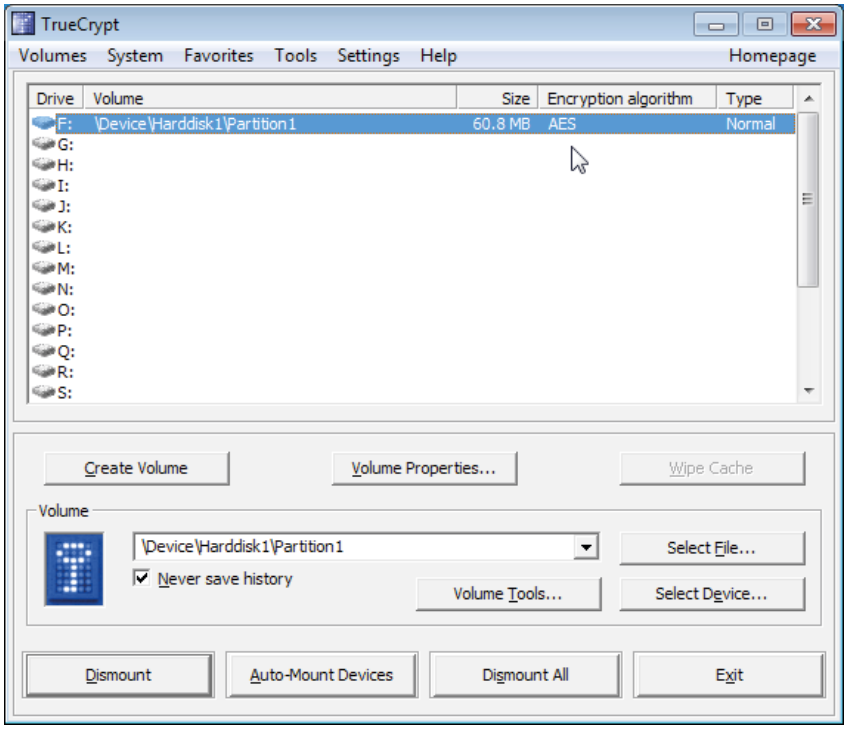
werden kann. Wird ein USB-Stick auf diese Weise verschlüsselt und dann geöffnet, erscheint er in der Übersicht der Laufwerke unter „Computer“ zwei Mal. Einmal der Stick selber, scheinbar ohne Inhalt und unformatiert, und einmal unter einem eigenen Laufwerksbuchstaben der entschlüsselte Inhalt (siehe Abb. 6 und 7).

Die Verschlüsselung eines ganzen Datenträgers ist nicht grundsätzlich schwierig oder sehr anders als die Vorgehensweise bei einem Container. Bei der Angabe des zu verschlüsselnden Datenträgers muss aber vorsichtig vorgegangen und die Hinweise in TrueCrypt genau beachtet werden. Würde der falsche Datenträger ausgewählt, wird das Dateisystem darauf gelöscht und alle enthaltenen Dateien gehen verloren. Normalerweise werden bei der Einrichtung alle auf dem USB-Stick gespeicherten Daten gelöscht. Es ist mit TrueCrypt unter bestimmten Voraussetzungen auch möglich, einen Datenträger zu verschlüsseln, auf dem sich Daten befinden und diese dabei zu erhalten [17], worauf im Folgenden aber nicht weiter eingegangen wird.

Um einen USB-Stick zu verschlüsseln, sollte man sich erst einmal Gewissheit über den zugeordneten Laufwerksbuchstaben machen, z. B. anhand der Größe des Laufwerks, des Gerätenamens oder bereits enthaltener Dateien. In der TrueCrypt-Oberfläche beginnt man die Erstellung wieder mit einem Klick auf „Create Volume“. Nun wird „Create a non-system partition/drive“ ausgewählt, „Standard TrueCrypt volume“, dann mit einem Klick auf „Select device“ anhand der aufgelisteten Laufwerksbuchstaben der USB-



7 *Der Inhalt des USB-Stick E: steht entschlüsselt als Laufwerk F: zur Verfügung*



8 *Ein verschlüsselter USB-Stick wurde als Laufwerk F: geöffnet*

Stick, danach die Option „Create encrypted volume and format it“ auswählen. Danach wird das Verschlüsselungsverfahren gewählt, die Laufwerksgröße überprüft und ein Passwort angegeben. Abschließend wird noch das zu erzeugende Dateisystem – für Hinweise zu den Dateisystemen siehe den Abschnitt „Verschlüsselung mehrerer Dateien in einem Container“ – ausgewählt und die Formatierung durchgeführt. Die Hinweise am Ende des Prozesses sind sehr wichtig für den Erhalt der verschlüsselten Daten und sollten gelesen und beachtet werden. Danach steht der Datenträger zur Verfügung. Mit einen Klick auf „Auto-Mount Devices“ und Eingabe des richtigen Passworts wird der verschlüsselte In-

halt des Sticks unter einem neuen Laufwerksbuchstaben geöffnet und kann verwendet werden. Alternativ kann mit „Select device“ der USB-Stick auch gezielt ausgewählt und geöffnet werden (siehe Abb. 8).

Ist die Arbeit mit dem verschlüsselten Inhalt des Sticks beendet und soll er entfernt werden, muss zunächst die Verschlüsselung gestoppt werden. Hierzu wird in der TrueCrypt-Oberfläche der Stick ausgewählt und mit einem Klick auf „Dismount“ die Verschlüsselung beendet. Kommt es zu einer Fehlermeldung, sind wahrscheinlich enthaltene Dateien noch von einer Anwendung geöffnet, die zuerst beendet werden muss. Ist der Laufwerksbuchstabe, unter dem der entschlüsselte Inhalt dargestellt wurde, verschwunden, kann der USB-Stick wie gewohnt sicher entfernt werden.

Analog zu dem Beispiel mit dem USB-Stick kann auch eine Speicherkarte (SD-Karte [18], Memory Sticks [19] etc.) oder die Partition einer USB-Festplatte verschlüsselt werden.

Verschlüsselung des Betriebssystems oder aller Laufwerke

Möchte man den Schutz der Daten eines Computers durch Verschlüsselung der Laufwerke auf das gesamte System ausdehnen, ist dies grundsätzlich auch möglich, erhöht aber den Installationsaufwand, ist teilweise nur unter bestimmten Voraussetzungen möglich und bringt ein paar Nachteile mit sich. Der Vorteil ist, dass das gesamte System dadurch weitgehend geschützt bleibt, auch wenn jemand Zugriff auf das ausgeschaltete System hat. Selbst Informationen, die in Anwendungen ohne besondere Schutzmaßnahmen gespeichert sind, wie z. B. Passwörter in E-Mail-Programmen, Cookies und Browser-Historie in Internetbrowsern, Chat-Protokolle etc., können so vor unbeabsichtigtem Zugriff bei Verlust des Gerätes geschützt werden.

Mögliche Nachteile können sein, dass für den Zugang beim Systemstart ein Passwort eingegeben werden muss, das bei einem Mehrbenutzersystem dann allen Benutzern mitgeteilt werden muss. Da dass Passwort üblicherweise Bestandteil der Verschlüsselung ist und vor dem eigentlichen Systemstart benötigt wird, kann an dieser Stelle noch nicht mit Benutzerkonten gearbeitet werden. Da durch eine Systemverschlüsselung sich auch die Komplexität eines Systems erhöht, ist eine Reparatur im Fehlerfall komplexer und sie muss beim Backup von Daten oder dem ganzen System berücksichtigt werden. Der Sicherheitsgewinn wird in Frage gestellt, wenn die zu schützenden Daten bei einem Backup dann doch in an einem ungeschützten Ort hinterlegt werden. Zusätzlich sollte man bedenken, das die Echtzeitver- und -entschlüsselung von Daten immer etwas CPU-Zeit in Anspruch nimmt. Wenn also maximaler Datendurchsatz für ein Laufwerk wichtig ist oder nur sehr begrenzte CPU-Leistung zur Verfügung steht, ist die Verschlüsselung eines kompletten Systems keine gute Wahl.

Eine Beschreibung der Methoden für die komplette Systemverschlüsselung von Windows, OS X und Linux ginge über den Rahmen dieses Artikels hinaus. Die Möglichkeiten sollen aber zumindest erwähnt werden. In jedem Fall sollten bei einem bestehenden System diese Maßnahme gut geplant und vorher ein Backup erstellt werden. Es wird unbedingt empfohlen, sich an eine Anleitung zu halten, die für den eigenen Einsatzzweck passt, da sonst Datenverlust sehr wahrscheinlich ist.

Das hier beschriebene TrueCrypt ist mittlerweile in der Lage, auch die Systempartition einer Windows-Installation komplett zu verschlüsseln [20]. Zusätzlich bietet Microsoft in den Windows-Versionen Ultimate und Enterprise/Professional die Software BitLocker [21] an. Diese ermöglicht ebenfalls eine komplette Verschlüsselung der Festplatten. Unter Mac OS X kommt FileVault [22] zum Einsatz, das ab OS X 10.7 (Lion) auch die Verschlüsselung des gesamten Systems ermöglicht. Unter Linux kann dies mit dm-crypt/LUKS [23] erreicht werden.

Wegmann

Kontakt:
Benedikt Wegmann
Benedikt.Wegmann@gwdg.de
0551 201-1870

Fußnoten

[1] *http://de.wikipedia.org/wiki/Kryptoanalyse*
[2] *http://de.wikipedia.org/wiki/Open_source*
[3] *http://de.wikipedia.org/wiki/Security_by_obscurity*
[4] *http://de.wikipedia.org/wiki/Pers%C3%B6nliche_Identifikationsnummer#Sicherheit*
[5] *http://de.wikipedia.org/wiki/Passwort#Wahl_von_sicheren_Passw.C3.B6rtern*
[6] *http://www.gwdg.de/index.php?id=2277*
[7] *http://de.wikipedia.org/wiki/Https*
[8] *http://ccrypt.sourceforge.net/*
[9] *http://de.wikipedia.org/wiki/Advanced_Encryption_Standard*
[10] *http://de.wikipedia.org/wiki/Kommandozeile*
[11] *http://qccrypt.free.fr/*
[12] *http://de.wikipedia.org/wiki/ZIP_%28Dateiformat%29*
[13] *http://www.truecrypt.org/, http://de.wikipedia.org/wiki/Truecrypt*
[14] *http://www.truecrypt.org/docs/?s=encryption-algorithms*
[15] *http://www.truecrypt.org/docs/?s=tutorial*
[16] *http://de.wikipedia.org/wiki/NTFS#Zugriff_mit_Unix-basierten_Betriebssystemen*
[17] *http://www.truecrypt.org/faq*
[18] *http://de.wikipedia.org/wiki/SD-Karte*
[19] *http://de.wikipedia.org/wiki/Memory_Stick*
[20] *http://www.truecrypt.org/docs/?s=system-encryption*
[21] *http://windows.microsoft.com/de-DE/windows7/products/features/bitlocker*
[22] *http://de.wikipedia.org/wiki/FileVault*
[23] *http://de.wikipedia.org/wiki/Linux_Unified_Key_Setup*

Aufgabenverwaltung mit dem iPhone/iPad

Moderne Smartphones bieten sich bekanntermaßen bestens dazu an, die alltäglichen Abläufe gerade auch im wissenschaftlichen Umfeld zu organisieren. Sie empfangen E-Mails, koordinieren Termine, speichern Adressen und verstehen sich auf die Verwaltung von Aufgaben. Seit iOS 5 gelingt Letzteres beim iPhone/iPad nun endlich auch mit Bordmitteln.

Programme für das Aufgabenmanagement

Weil Apple ursprünglich keine eigene Anwendung für das Aufgabenmanagement und selbst nicht einmal für die Verwaltung einfacher ToDo-Listen mitlieferte, führte dies zu einer schier unüberschaubaren Zahl entsprechender Angebote im AppStore. Inzwischen kristallisierte sich eine Art Anforderungskatalog für eine ideale ToDo-App heraus. Sie sollte nicht nur auf den mobilen Geräten, sondern auch auf dem Desktop präsent sein, die dafür erforderliche Synchronisation cloud-basiert erledigen, günstigenfalls ortsabhängige Aufgaben ermöglichen und unbedingt leicht zu bedienen sein, da sie anderenfalls einfach nicht genutzt wird. Gerade wegen des letzten Aspekts hat das ansonsten sehr leistungsfähige Produkt „**Omnifocus**“ nach wie vor Akzeptanzprobleme, da es einfach eine längere Einarbeitungszeit erfordert. Dem wegen seiner geradezu „Apple-artig“ eingängigen Bedienoberfläche beliebten Programm „**Things**“ fehlte der zentrale Abgleich über die Cloud, der jetzt endlich in einer ersten Beta-Version nachgeliefert wird. Das kostenlose „**Wunderlist**“ glänzt durch seine Präsenz auf zahlreichen Plattformen (iPhone, iPad, Mac, Windows und Android), lässt aber noch einige wichtige Funktionen vermissen, die jetzt offenbar durch das Nachfolgeprodukt „**Wunderkit**“ abgedeckt werden sollen.

Aufgabenverwaltung in iOS

Mit dem Erscheinen von iOS 5 hat nun auch Apple selbst eine Aufgabenverwaltung mit dem Namen „**Erinnerungen**“ (engl.: **Reminder**) mitgeliefert, die zwar recht spartanisch wirkt, dennoch die wichtigsten Funktionen anbietet:

- Synchronisationmöglichkeit über die iCloud zeitnah (Push-Dienst) mit allen iOS-Geräten, **iCal** auf dem Mac und über das „**iCloud Control Panel**“ auch auf Outlook 2007/2010 unter Windows.

- Zusätzliche Synchronisationmöglichkeit mit den auf einem Exchange-Server verwalteten Aufgaben und damit automatisch der Zugriff über Outlook (Windows und Mac) und natürlich dem Web-Interface „**OWA**“. Um dies zu erreichen, muss bei der Konfiguration des Exchange-Kontos auf dem iPhone/iPad „Erinnerungen“ und unter Mac OS X „Kalender“ aktiviert werden.

  Auf diese Weise könnten übrigens die Aufgaben auch gleichzeitig auf anderen Smartphones bearbeitet werden: unter Windows Phone 7 mit der mitgelieferten Kalenderanwendung und unter Android unter Zuhilfenahme entsprechender Apps wie beispielsweise „**TouchDown**“ von NitroDesk.

- Verwaltung ortsgebundener Aufgaben, auf die der Nutzer beim Verlassen oder Eintreffen einer vorher festgelegten Adresse hingewiesen wird. Dies funktioniert allerdings nur bei Erinnerungen und auch nur auf dem iPhone, bei dem natürlich die Ortungsdienste aktiviert sein müssen. So könnte man sich an dienstliche Aufgaben genau dann erinnern lassen, sobald man das Büro betreten hat.

- Das Sprachassistenzsystem „**Siri**“ auf dem iPhone 4S ermöglicht ein komfortables Aufsprechen der Erinnerungen. Verwendet man ein entsprechendes Bluetooth-Headset, dann muss man dafür noch nicht einmal das iPhone in die Hand nehmen.

- Natürlich bieten auch die „Erinnerungen“ die üblichen Funktionen wie die Erstellung immer wiederkehrender Aufgaben, die Vergabe von Prioritäten, die Einrichtung zusätzlicher eigener Listen und die Sortierungsmöglichkeit nach Terminen.

- Und schließlich kann man sich über die Mitteilungszentrale

stets über fällige Aufgaben benachrichtigen lassen.

„Erinnerungen“ unter Mac OS X

Leider wird es erst in „OS X Mountain Lion“ – dem voraussichtlich im Sommer 2012 erscheinenden Nachfolger von „OS X Lion“ – eine dedizierte Anwendung „Erinnerungen“ geben, die in etwa dem Aussehen und dem Funktionsumfang der entsprechenden iOS-Anwendungen gleichkommt. Bis dahin muss man sich mit der rudimentären Repräsentation in iCal in Form der rechten „Erinnerungen“-Spalte begnügen. Wem das für die Eingabe zu umständlich ist, der kann sich mit Hilfe des „**Automators**“ – ein Programm, das es erlaubt, unter Mac OS X Routineaufgaben zu automatisieren, – ein kleines Eingabeformular basteln, welches sich jederzeit über eine selbstgewählte Tastenkombination auf dem Desktop öffnet. Eine leichtverständliche Anleitung hierzu findet sich im folgenden Artikel auf „Mac OS X Tips“:

http://www.macosxtips.co.uk/index_files/add-to-do-items-ical-reminders-keyboard-shortcut.php

Nachdem es nun Apple nach vier Jahren endlich geschafft hat, auf seinen iOS-Geräten auch eine Aufgabenverwaltung mitzuliefern, die sich gut in die jeweiligen verwendeten Umgebungen (iCloud und Exchange) einfügt, ist man zur erfolgreichen Selbstorganisation nicht mehr zwingend auf Fremdprodukte angewiesen. Hat man aber andererseits bereits seit längerem Produkte wie „Omnifocus“ oder „Things“ im Einsatz, so muss man diese jetzt nicht etwa deswegen aufgeben, denn die Hersteller zeigen sich durchaus bestrebt, Schnittstellen zu den Apple-eigenen Funktionen anzubieten, um so beispielsweise auch „Siri“ zur vereinfachten Eingabe einzuspannen.

Reimann

Kontakt:
Michael Reimann
Michael.Reimann@gwdg.de
0551 201-1826

Apple veröffentlicht iOS 5.1

Zeitgleich mit der Ankündigung des neuen iPads am 07.03.2012 hat Apple auch die lange erwartete Betriebssystemversion iOS 5.1 für das iPad und iPhone freigegeben.

Das Update zielt auf die Geräte **iPhone** (ab 3GS), **iPad** (alle Modelle) und **iPod touch** (ab dritter Generation) und kann nun erstmalig auch direkt vom Gerät aus (OTA: over the air) angestoßen werden (Menü: Einstellungen > Allgemein > Softwareaktualisierung). Die bekannte Installation über iTunes ist natürlich weiterhin möglich, nur wird dann stets das komplette Betriebssystem aufgespielt. Bei der OTA-Methode werden hingegen nur die Änderungen geladen, was weniger als 200 MByte ausmacht, gegenüber den mehr als 800 MByte bei einer vollständigen Installation über iTunes.

Neuerungen

Im Folgenden sollen die wichtigsten Änderungen in iOS 5.1 aufgeführt werden:

- Die wichtigste Neuerung zuerst: Die Probleme mit den ständig zu kurzen Batterielaufzeiten besonders beim iPhone 4S scheinen nun endlich behoben worden zu sein.

- In diesem Zusammenhang kehrt nun auf dem iPhone 4S endlich wieder der bekannte Schalter „3G aktivieren“ (Einstellungen > Allgemein > Netzwerk) zurück, über den die Nutzer UMTS (3G) in den Gegenden ausschalten können, in denen es nicht verfügbar ist. Das hilft, Strom zu sparen.

- Eine Veränderung bei der Geolokation trägt ebenfalls zur Einsparung der kostba-

ren Akku-Energie bei. So wird beim Zugriff auf den Standort erstmals unterschieden zwischen einer kontinuierlichen Abfrage der Position, wie sie von Navigations-Anwendungen vorgenommen werden, und der Geofence-Funktion, bei der nur das Erreichen oder Verlassen eines vorher definierten Ortes von Bedeutung ist, wie z. B. bei den ortsabhängigen Erinnerungen. Erkennbar ist letzteres jetzt an einer lilafarbenen Kompassnadel in der oberen Menüleiste, die als Kontur erscheint.

- Über den iCloud-Dienst „**Fotostream**“ lassen sich mit einem iPhone aufgenommene Bilder auf ausgewählte Geräte über den Online-Dienst von Apple verteilen. Bislang konnte man nur alle Bilder auf einmal serverseitig entfernen. Ungewollte Bilder lassen sich nun endlich auch selektiv löschen, allerdings immer nur von dem jeweiligen Gerät aus, nicht direkt vom Server. Damit dieser Vorgang auch vom Mac aus gelingt, gab es dort ein entsprechendes Update für iPhoto.

- Die beste Kamera nutzt bekanntlich nichts, wenn es einfach zu lange dauert, bis sie ausgelöst ist. Deshalb lässt sich jetzt der Kamera-Schnellzugriff im Sperrbildschirm noch schneller bedienen. Statt wie bislang zweimal auf den Home-Knopf zu drücken, genügt jetzt ein einfacher Knopfdruck mit gleichzeitigem Schieben nach oben, und schon ist die Kamera schussbereit.

- Die Kamera-Anwendung für das iPad 2 und seinen Nachfolger wurde neu gestaltet.

- Eine verbesserte Gesichtserkennung im iPhone 4S und im neuen iPad hebt die erkannten Gesichter mit einem grünen Rahmen hervor und erleichtert es dem Fotografen, die Kamera auf die richtige Position zu fokussieren.

- Optimierte Audio-Funktionen beim iPad führen zu verbesserter Lautstärke und Tonqualität bei TV-Sendungen und Filmen. Zudem wurde auch die Wiedergabegeschwindigkeit u. a. bei Podcasts verbessert und um den beim iPhone bekannten 30-Sekunden-Rücklauf erweitert.

- Ein Hauptgrund für dieses Update dürfte neben dem nicht unerheblichen Funktionsgewinn letztlich auch das Schließen von zahlreichen Sicherheitslücken sein, von denen sich viele potenziell zum Einschleusen von Schadcode eignen. Die meisten davon befinden sich erwartungsgemäß im Browser Safari.

iTunes 10.6

Gleichzeitig mit iOS 5.1 veröffentlichte Apple auch die aktuelle Version 10.6 seines Multimedia-Verwaltungsprogramms **iTunes**. Neben der Unterstützung für das neuen iPad und den damit verbundenen Full-HD-Filmen im 1080p-Format flossen hier auch zahlreiche Verbesserungen und vor allem Sicherheitskorrekturen mit ein. Einige der Sicherheitslücken des Safari-Browsers fanden sich nämlich auch in dem rudimentären Browser-Kern von iTunes wieder.

Fazit

Bei dem gewaltigen Funktionsumfang heutiger Smartphones werden zunehmend die Begehrlichkeiten der Angreifer geweckt, diese leistungsfähigen Geräte und die darauf befindlichen, teils sehr persönlichen Daten unter ihre Kontrolle zu bringen. Um so wichtiger ist es daher, dass offene Sicherheitslücken schnell geschlossen werden. Hier haben die Anwender von iPhone und iPad den leichten Vorteil, dass der Hersteller aufgrund der weitgehenden Gleichförmigkeit der Hardware-Plattformen relativ schnell mit Updates reagieren kann. Dieses Angebot sollte daher auch möglichst zeitnah wahrgenommen werden.

Reimann

Kontakt:
Michael Reimann
Michael.Reimann@gwdg.de
0551 201-1826

Cloud Plugfest in Düsseldorf

Dieses Jahr fand bereits zum vierten Mal das von der Storage and Network Industry Association (SNIA) ins Leben gerufene Cloud Plugfest statt. Ziel des Plugfestes ist es, Mitglieder von Standardisierungsgremien und Entwickler von Cloud Frameworks zusammenzubringen, um über Cloud-Schnittstellen und deren Implementierung zu diskutieren und das Zusammenspiel verschiedener Implementierungen zu testen.

Nachdem das Cloud Plugfest mehrere Male in den USA stattfand, war es der GWDG in Kooperation mit der Firma NetApp in diesem Jahr zum ersten Mal möglich, die Veranstaltung nach Deutschland zu holen. Sie fand vom 28.02. bis 01.03.2012 in Düsseldorf statt. Besonders im Fokus standen dieses Mal das Open Cloud Computing Interface (OCCI), welches vom Open Grid Forum spezifiziert wird, sowie das Cloud Data Management Interface (CDMI), welches von der SNIA spezifiziert wird. Daneben wurde auch über Cloud-Standards wie das Cloud Information Model Interface (CIMI) sowie das Open Virtual Format (OVF) diskutiert und insbesondere die Möglichkeiten beleuchtet, wie diese verschiedenen Standards zu interoperablen Cloud-Lösungen kombiniert werden können.

Die Teilnehmer des Cloud Plugfestes waren überwiegend Entwickler oder Wissenschaftler und sie kamen zum größten Teil aus der EU, den USA und Indien. Auch einige Studierende und Promovierende waren anwesend, um ihre Arbeiten beim Plugfest vorzustellen und über diese zu diskutieren. Unter den teilnehmenden Firmen befanden sich unter anderem große Firmen wie IBM, Intel, NetApp, Oracle und Bull sowie Teilnehmer von großen EU-Projekten (Venus-C, SAIL und FI-Ware) und von mehreren internationalen Universitäten.

Teilnehmer des Cloud Plugfestes testen und diskutieren die Implementierung von Cloud-Schnittstellen

In kleinen, wechselnden Gesprächsrunden wurden die besten Vorgehensweisen für Implementierungen sowie die Auslegung der Schnittstellenspezifikationen diskutiert. Hierbei wurde insbesondere über die kompakte Darstellung und einfache Verarbeitung von Nachrichten über Cloud-Schnittstellen gesprochen.

Während des gesamten Plugfestes wurden die verschiedenen Implementierungen getestet und die Ergebnisse in einer Testmatrix festgehalten. Diese zeigt an, welche Anforderungen der verschiedenen Schnittstellen durch die vorhandenen Implementierungen erfüllt werden und ob hierbei noch Probleme auftreten. Diese Probleme wurden dann im Teamwork bearbeitet und konnten in den meisten Fällen gelöst werden.

Immer wieder wurden spontane Präsentationen zu unterschiedlichen Themen gehalten, welche nachmittags durch vorab geplante und über ein Konferenzsystem an Teilnehmer aus aller Welt übertragene Präsentationen ergänzt wurden. Themen waren hierbei unter anderem die Einbindung von OCCI in die Cloud Frameworks OpenNebula und Openstack, eine Übersicht zu Open Source CDMI-Implementierungen sowie die Nutzung von standardisierten Schnittstellen in der European Grid Infrastructure (EGI) Federated Cloud.

Besonders intensiv wurde über die Kombination von verschie-

denen proprietären und offenen Cloud-Standards diskutiert, welche am Ende des Cloud Plugfest zusammengefasst wurde und als Basis für weitere Arbeiten in den Standardisierungsgremien dient.

Die Resultate des Cloud Plugfestes werden u. a. vom 12. - 15. März 2012 beim Open Grid Forum 34 in Oxford präsentiert und weiter vertieft.

Insgesamt war die Resonanz auf die Durchführung und inhaltliche Gestaltung sehr positiv und es wurde angeregt, die Veranstaltung noch stärker zu bewerben und in einigen Monaten erneut durchzuführen. Während des Cloud Plugfestes hat das European Telecommunications Standards Institute (ETSI) das Interesse geäußert, sich an der Organisation der nächsten Cloud Plugfestes zu beteiligen und nach Möglichkeit auch die Finanzierung zu unterstützen.

Weiterführende Informationen sind unter *http://www.snia.org/cloud/cloudplugfest* zu finden.

Feldhaus

Kontakt:
Florian Feldhaus
florian.feldhaus@gwdg.de
0551 39-20364

FreeBSD 9.0 verfügbar

Vor einigen Wochen wurde die neueste FreeBSD-Produktionsversion 9.0 freigegeben, welche mit einigen Überraschungen aufwartet. So sind nach vielen Jahren das Installationsprogramm sowie die Festplatten-Partitionierung komplett überarbeitet worden. Das neue Installationsprogramm **bsdinstall** ist zwar nicht mit einer grafischen Oberfläche versehen, aber dennoch für weniger versierte Anwender leichter bedienbar als die alte **sysinstall**-Software.

Unterstützt werden auf Intel-Hardware im Standardfall MBR- und GPT-Partitionen; das klassische zusätzliche BSD-Disklabel-Verfahren ist nur noch mit Handarbeit durchführbar. Im Normalfall wird auch nur eine Dateisystempartition angelegt, um FreeBSD-Installationen in virtuellen Umgebungen pflegeleichter zu machen. Das UFS-Dateisystem bietet neben Softupdates jetzt ein Journal, so dass selbst ein verdeckter Dateisystemcheck im Hintergrund obsolet wird; ZFS wird immer mehr zum Dateisystem der Wahl.

Ein ausführlicherer Bericht ist für eine der nächsten Ausgaben der GWDG-Nachrichten geplant.

Heuer

Kontakt:
Dr. Konrad Heuer
kheuer@gwdg.de
0551 201-1540

Drei zusätzliche Kurse

Kurzfristig wurde folgende drei Kurse in das Kursangebot der GWDG aufgenommen:

- 19.04.2012:
  Outlook – E-Mail und Groupware
- 26.04.2012:
  Die IT-Sicherheitsrichtlinien der Universität Göttingen
- 12.06. – 13.06.2012:
  InDesign – Aufbaukurs

Ausführliche Informationen zu diesen Kursen sind unter dem URL *http://www.gwdg.de/index.php?id=1403* zu finden.

Otto

Kontingentzuweisung für das zweite Quartal 2012

Die nächste Zuweisung von Institutskontingenten für die Inanspruchnahme von Leistungen der GWDG erfolgt am Montag, dem 2. April 2012. Die Höhe der Kontingente wird den Instituten per Brief oder per E-Mail mitgeteilt. Die Bemessung der Institutskontingente erfolgte nach den Vorläufigen Richtlinien des Beirats der GWDG und den Ergänzungen der Beiratskommission für die Verteilung von IT-Leistung entsprechend dem Verbrauch im Zeitraum vom 01.09.2011 bis 29.02.2012. Nicht verbrauchte Kontingente werden zu 50 % in das nächste Quartal übertragen. Negative Verbrauchswerte werden zu 100 % mit dem neuen Institutskontingent verrechnet.

Jeder Benutzer kann den aktuellen Stand des Institutskontingents durch die Eingabe des Kommandos *kontingent* auf einer Workstation des UNIX-Clusters oder im WWW unter dem URL *http://www.gwdg.de/index.php?id=1678* abfragen. Dort besteht auch die Möglichkeit, Informationen über den Stand des separaten Druckkontingents abzurufen.

Falls in Ausnahmefällen das Institutskontingent nicht ausreichen sollte, können begründete Anträge an die Beiratskommission für die Verteilung von IT-Leistung über den URL *http://www.gwdg.de/index.php?id=799* gestellt werden. Solche Anträge sollen bis zum 18.05.2012 eingereicht werden.

Glässer

Kontakt:
Renate Glässer
renate.glaesser@gwdg.de
0551 201-1883

Öffnungszeiten des Rechenzentrums um Ostern 2012

Das Rechenzentrum der GWDG ist vom **06.04.2012, Karfreitag, bis zum 09.04.2012, Ostermontag, geschlossen**.

Falls Sie sich zu der Zeit, an der das Rechenzentrum geschlossen ist, in dringenden Fällen an die GWDG wenden wollen, schicken Sie bitte eine E-Mail an *support@gwdg.de*. Das dahinter befindliche Ticketsystem wird auch während dieser Zeit von Mitarbeiterinnen und Mitarbeitern der GWDG regelmäßig kontrolliert.

Wir bitten alle Benutzerinnen und Benutzer, sich darauf einzustellen.

Grieger

Personalia

Neue wissenschaftliche Hilfskraft in der AG O

Seit dem 15. Februar 2012 arbeitet Herr **Kay Servatius** in der Arbeitsgruppe „Basisdienste und Organisation“ (AG O).

Sein Aufgabenbereich umfasst den Support im Göttinger Funk-LAN „GoeMobile“ und im „eduroam“, für den bisher Herr Stephan Hilker zuständig gewesen ist, der innerhalb der GWDG andere Aufgaben übernommen hat. Unterstützt wird er dabei, wie bisher auch Herr Hilker, von Herrn Albert Hartmann und Herrn Kai-Uwe Mather. Die Beratungszeiten von Herrn Servatius zum GoeMobile und zum eduroam finden Sie unter *http://www.gwdg.de/index.php?id=777*.

Herr Servatius studiert zurzeit an der HAWK Göttingen im Masterstudiengang Elektrotechnik. Per E-Mail ist er unter *Kay.Servatius@gwdg.de* und telefonisch unter der Nummer 0551 201-1877 zu erreichen.

Grieger

Neue Aleph-Version (V20) in den Produktionsbetrieb übernommen

Am 13. Februar 2012 schaltete die GWDG eine neue Aleph-Version (Version 20) für den Produktionsbetrieb der Aleph-nutzenden MPG-Bibliotheken frei. Die neue Programmversion hält nicht nur für die Bibliothekare viele neue Funktionalitäten bereit, sondern bietet auch den Bibliotheksnutzern einen moderneren, von den MPG-Bibliothekaren und der GWDG weiterentwickelten Online-Katalog.

Seit 2001 betreibt die GWDG für Institutsbibliotheken der Max-Planck-Gesellschaft (MPG) einen Server für das Bibliothekssystem Aleph500, eine Software für Katalogisierung, Erwerbung und Ausleihe von Büchern und Zeitschriften. Aleph500 bietet sowohl den Bibliothekaren ein Arbeitsinstrument für den gesamten bibliothekarischen Geschäftsgang, als auch den Wissenschaftlerinnen und Wissenschaftlern an den Instituten mit dem Online-Katalog (OPAC) ein weltweit zugängliches Instrument für die Recherche in den Beständen ihrer Institutsbibliothek. Als zentrale Kataloge der MPG stehen auf dem Göttinger Aleph-Server das Zeitschriftenverzeichnis und das Verzeichnis der e-Books zur Verfügung. Alle Bibliotheken der MPG können darüber hinaus auf dem Aleph-Server die Normdaten der Personennamendatei (PND), der Gemeinsamen Körperschaftsdatei (GKD) und der Schlagwortnormdatei (SWD) nutzen.

31 Bibliotheken, die insgesamt 36 Max-Planck-Institute versorgen, nutzen derzeit das Aleph-System. Auch die GWDG selbst setzt dieses System für ihre Bibliothek ein. Seit August 2011 beherbergt das System außerdem den Verbundkatalog des Kunstbibliotheken-Fachverbundes Florenz - München - Rom - Paris „kubikat". Im Kunstbibliotheken-Fachverbund haben sich zwei Max-Planck-Institute (das Kunsthistorische Institut Florenz und die Bibliotheca Hertziana in Rom) sowie das Zentralinstitut für Kunstgeschichte in München und das Deutsche Forum für Kunstgeschichte in Paris zusammengeschlossen. Durch die Integration der Kunstbibliotheken ist der Aleph-Datenbestand auf über drei Millionen Titelsätze angewachsen. In der Aleph-Entwicklungsumgebung ist im Oktober 2011 der Katalog der Bibliothek des Forschungszentrums Caesar eingerichtet worden, der produktive Betrieb dieser Bibliothek wurde nun zeitgleich mit dem Versionswechsel aufgenommen.

Für die Bibliothekssoftware Aleph500, die auf einer Oracle-Datenbank (Oracle Version 11) basiert, werden bei der GWDG zwei SunFire M4000-Server betrieben; der eine beherbergt die Entwicklungsumgebung, der andere die Produktionsumgebung. Die M4000-Server (4 x 2,53 GHz Quad-Core CPUs SPARC64 VII, 64 GByte RAM), sind über FC-Adapter an das (virtualisierte) Storage Area Network (SAN) der GWDG angeschlossen. Eingesetzt wird das Betriebssystem Solaris 10, ZFS, LifeUpgrade und die Partitionierungstechnologie „Solaris Zones", die der Virtualisierung von Betriebssystemservices dient und es erlaubt, verschiedenen Anwendungen eine isolierte und sichere Umgebung zu bieten.

Bereits im März 2011 wurde die Aleph-Entwicklungsumgebung von Version 18 nach Version 20 migriert, dann folgten im Laufe des Jahres zahlreiche Anpassungen durch die Systembibliothekare und das GWDG-Aleph-Team. So wurden zum Beispiel ein neues Design und neue Funktionalitäten für die Online-Kataloge der Bibliotheken (*http://aleph.mpg.de/F*) erstellt und es wurde aus den zahlreichen Neuerungen der Version 20 ein MPG-Standard entwickelt und eingepflegt. Hiermit steht den MPG-Aleph-Bibliotheken und ihren Nutzern nun ein verbessertes und moderneres Bibliothekssystem zur Verfügung.

Weitere Informationen finden Sie unter *http://www.gwdg.de/index.php?id=353*

Bost

Kontakt des Aleph-Teams der GWDG:
aleph500@gwdg.de

Regina Bost
rbost@gwdg.de; 0551 201-1831
Anke Bruns
abruns1@gwdg.de; 0551 201-1519
Benjamin Tetzlaff
btetzla@gwdg.de; 0551 201-1821

Stellenangebote

Die GWDG sucht ab sofort zur Unterstützung der Arbeitsgruppe „Nutzerservice und Betriebsdienste“ zwei

Studentische Hilfskräfte

mit bis zu 68 Stunden Beschäftigungszeit pro Monat. Die Vergütung erfolgt entsprechend den Regelungen für Studentische/Wissenschaftliche Hilfskräfte.

Aufgaben:

1. Mitarbeit bei der Beantwortung von Support-Anfragen, sowohl im Telefondienst oder per E-Mail als auch über das bei der GWDG eingesetzte Ticketsystem, vor allem in den Themenfeldern Windows-Arbeitsplatzrechner und E-Mail-Bearbeitung mit Microsoft Outlook

2. Mitarbeit bei Erstellung und Pflege entsprechender Dokumentation im Internet-Auftritt der GWDG

3. Bereitschaft zur Mitarbeit bei der Systemüberwachung und Peripheriebetreuung im Schichtdienst im Bedarfsfall

Diese Aufgaben, die unter der Anleitung wissenschaftlicher Mitarbeiter zu bearbeiten sind, bieten viele interessante Möglichkeiten zur Weiterentwicklung eigener Kenntnisse.

Anforderungen:

- Gute Kenntnisse in Windows-Betriebssystemen
- Schnelle Lernfähigkeit
- Gute Kommunikations- und Teamfähigkeit

Die GWDG will den Anteil von Frauen in den Bereichen erhöhen, in denen sie unterrepräsentiert sind. Frauen werden deshalb ausdrücklich aufgefordert, sich zu bewerben. Die GWDG ist bemüht, mehr schwerbehinderte Menschen zu beschäftigen. Bewerbungen Schwerbehinderter sind ausdrücklich erwünscht.

Wir bitten interessierte Damen und Herren um schriftliche **Bewerbung bis zum 10. April 2012** über unser Online-Formular unter *http://www.gwdg.de/index.php?id=2573*

Fragen zur ausgeschriebenen Stelle beantworten Ihnen Herr Eric Helmvoigt (Tel.: 0551 201-1845, E-Mail: *ehelmvo@gwdg.de*) oder Herr Dr. Konrad Heuer (Tel.: 0551 201-1540, E-Mail: *kheuer@gwdg.de*).

Die GWDG sucht ab sofort zur Unterstützung der Arbeitsgruppe „Nutzerservice und Betriebsdienste“ eine

Studentische Hilfskraft

mit bis zu 68 Stunden Beschäftigungszeit pro Monat. Die Vergütung erfolgt entsprechend den Regelungen für Studentische/Wissenschaftliche Hilfskräfte.

Aufgaben:

1. Mitarbeit bei der Installation und Betreuung von Windows-Arbeitsplatzrechnern in den Instituten
2. Mitarbeit bei der Dokumentation der zentralen Dienste im Active Directory der GWDG
3. Mitarbeit bei der Systemüberwachung und Peripheriebetreuung im Schichtdienst

Diese Aufgaben, die unter der Anleitung wissenschaftlicher Mitarbeiter zu bearbeiten sind, bieten viele interessante Möglichkeiten zur Weiterentwicklung eigener Kenntnisse.

Anforderungen:

- Gute Kenntnisse in Windows-Betriebssystemen
- Schnelle Lernfähigkeit
- Gute Kommunikations- und Teamfähigkeit

Die GWDG will den Anteil von Frauen in den Bereichen erhöhen, in denen sie unterrepräsentiert sind. Frauen werden deshalb ausdrücklich aufgefordert, sich zu bewerben. Die GWDG ist bemüht, mehr schwerbehinderte Menschen zu beschäftigen. Bewerbungen Schwerbehinderter sind ausdrücklich erwünscht.

Wir bitten interessierte Damen und Herren um schriftliche **Bewerbung bis zum 10. April 2012** über unser Online-Formular unter *http://www.gwdg.de/index.php?id=2574*

Fragen zur ausgeschriebenen Stelle beantworten Ihnen Herr Eric Helmvoigt (Tel.: 0551 201-1845, E-Mail: *ehelmvo@gwdg.de*) oder Herr Dr. Konrad Heuer (Tel.: 0551 201-1540, E-Mail: *kheuer@gwdg.de*).

Kurse von April bis Dezember 2012

Allgemeine Informationen zum Kursangebot der GWDG

Teilnehmerkreis

Das Kursangebot der GWDG richtet sich an die Mitarbeiterinnen und Mitarbeiter aus den Instituten der Universität Göttingen und der Max-Planck-Gesellschaft sowie aus anderen wissenschaftlichen Einrichtungen, die zum erweiterten Benutzerkreis der GWDG gehören. Eine Benutzerkennung für die Rechenanlagen der GWDG ist nicht erforderlich.

Anmeldung

Anmeldungen können schriftlich per Brief oder per Fax unter der Nummer 0551 201-2150 an die GWDG, Kursanmeldung, Postfach 2841, 37018 Göttingen oder per E-Mail an die Adresse *support@gwdg.de* mit dem Betreff „Kursanmeldung" erfolgen. Für die schriftliche Anmeldung steht unter *http://www.gwdg.de/antragsformulare* ein Formular zur Verfügung. Telefonische Anmeldungen können wegen der Einbeziehung der Kurse in die interne Kosten- und Leistungsrechnung der GWDG nicht angenommen werden. Aus diesem Grund können Anmeldungen auch nur durch den Gruppenmanager – eine der GWDG vom zugehörigen Institut bekannt gegebene und dazu autorisierte Person – oder Geschäftsführenden Direktor des Instituts vorgenommen werden. Die Anmeldefrist endet jeweils sieben Tage vor Kursbeginn. Sollten nach dem Anmeldeschluss noch Teilnehmerplätze frei sein, sind auch noch kurzfristige Anmeldungen in Absprache mit der Service-Hotline bzw. Information (Tel.: 0551 201-1523, E-Mail: *support@gwdg.de*) möglich.

Kosten bzw. Gebühren

Die Kurse sind – wie die meisten anderen Leistungen der GWDG – in das interne Kosten- und Leistungsrechnungssystem der GWDG einbezogen. Die bei den Kursen angegebenen Arbeitseinheiten (AE) werden vom jeweiligen Institutskontingent abgezogen. Für die Institute der Universität Göttingen und der Max-Planck-Gesellschaft erfolgt keine Abrechnung in EUR.

Rücktritt und Kursausfall

Absagen durch die Teilnehmer oder die zugehörigen Gruppenmanager bzw. Geschäftsführenden Direktoren können bis zu acht Tagen vor Kursbeginn erfolgen. Bei späteren Absagen durch die Teilnehmer oder die zugehörigen Gruppenmanager bzw. Geschäftsführenden Direktoren werden die für die Kurse berechneten Arbeitseinheiten vom jeweiligen Institutskontingent abgebucht. Sollte ein Kurs aus irgendwelchen Gründen, zu denen auch die Unterschreitung der Mindestteilnehmerzahl bei Anmeldeschluss sowie die kurzfristige Erkrankung des Kurshalters gehören, abgesagt werden müssen, so werden wir versuchen, dies den betroffenen Personen rechtzeitig mitzuteilen. Daher sollte bei der Anmeldung auf möglichst vollständige Adressangaben inkl. Telefonnummer und E-Mail-Adresse geachtet werden. Die Berechnung der Arbeitseinheiten entfällt in diesen Fällen selbstverständlich. Weitergehende Ansprüche können jedoch nicht anerkannt werden.

Kursorte

Alle Kurse finden in Räumen der GWDG statt. Der Kursraum und der Vortragsraum der GWDG befinden sich im Turm 5 bzw. 6, UG des Max-Planck-Instituts für biophysikalische Chemie, Am Faßberg 11, 37077 Göttingen. Die Wegbeschreibung zur GWDG bzw. zum Max-Planck-Institut für biophysikalische Chemie sowie der Lageplan sind im WWW unter dem URL *http://www.gwdg.de/lageplan* zu finden.

Ausführliche und aktuelle Informationen

Ausführliche Informationen zu den Kursen, insbesondere zu den Kursinhalten und Räumen, sowie aktuelle kurzfristige Informationen zum Status der Kurse sind im WWW unter dem URL *http://www.gwdg.de/kurse* zu finden. Anfragen zu den Kursen können an die Service-Hotline bzw. Information per Telefon unter der Nummer 0551 201-1523 oder per E-Mail an die Adresse *support@gwdg.de* gerichtet werden.

Kurs	Vortragende/r	Termin	Anmeldeschluss	AE
UNIX für Fortgeschrittene	Dr. Sippel	16.04. – 18.04.2012 9:15 – 12:00 und 13:15 – 15:30 Uhr	09.04.2012	12
Outlook – E-Mail und Groupware	Helmvoigt	19.04.2012 9:15 – 12:00 und 13:00 – 16:00 Uhr	12.04.2012	4
Smartphones und Tablets (iPad) für den wissenschaftlichen Einsatz	Reimann	18.04.2012 9:00 – 12:00 und 13:00 – 16:00 Uhr	11.04.2012	4
UNIX/Linux-Arbeitsplatzrechner – Installation und Administration	Gerdes, Dr. Heuer, Körmer, Dr. Sippel	23.04. – 24.04.2012 9:15 – 12:00 und 13:30 – 16:00 Uhr	16.04.2012	8
UNIX/Linux-Server – Grundlagen der Administration	Gerdes, Dr. Heuer, Körmer, Dr. Sippel	25.04. – 26.04.2012 9:15 – 12:00 und 13:30 – 16:00 Uhr	18.04.2012	8
Die IT-Sicherheitsrichtlinien der Universität Göttingen	Dr. Beck	26.04.2012 10:15 – 11:30 Uhr ZHG 006	19.04.2012	0
UNIX/Linux – Systemsicherheit für Administratoren	Gerdes, Dr. Heuer, Körmer, Dr. Sippel	27.04.2012 9:15 – 12:00 und 13:30 – 15:00 Uhr	20.04.2012	4
Einführung in die Statistische Datenanalyse mit SPSS	Cordes	08.05. – 09.05.2012 9:00 – 12:00 und 13:00 – 15:30 Uhr	01.05.2012	8
PDF-Dateien: Erzeugung und Bearbeitung mit Adobe Acrobat	Dr. Baier	05.06. – 06.06.2012 9:15 – 12:00 und 13:00 – 15:30 Uhr	29.05.2012	8
InDesign – Aufbaukurs	Töpfer	12.06. – 13.06.2012 9:30 – 16:00 Uhr	05.06.2012	8
PDF-Formulare mit Adobe Acrobat und Adobe Designer erstellen	Dr. Baier	14.06.2012 9:15 – 12:00 und 13:00 – 15:30 Uhr	07.06.2012	4
Angewandte Statistik mit SPSS für Nutzer mit Vorkenntnissen	Cordes	19.06. – 20.06.2012 9:00 – 12:00 und 13:00 – 15:30 Uhr	12.06.2012	8
Datenschutz – Verarbeitung personenbezogener Daten auf den Rechenanlagen der GWDG	Dr. Grieger	04.07.2012 9:00 – 12:00 Uhr	27.06.2012	2
Einführung in das IP-Adressmanagement-System der GWDG für Netzwerkbeauftragte	Dr. Beck	05.07.2012 10:00 – 12:00 Uhr	28.06.2012	2
Grundlagen der Bildbearbeitung mit Photoshop	Töpfer	28.08. – 29.08.2012 9:30 – 16:00 Uhr	21.08.2012	8
InDesign – Grundlagen	Töpfer	04.09. – 05.09.2012 9:30 – 16:00 Uhr	27.08.2012	8

Kurs	Vortragende/r	Termin	Anmeldeschluss	AE
Einführung in die Bedienung eines Windows-PCs	Becker, Nolte, Quentin	10.09.2012 9:00 – 12:30 und 13:30 – 15:30 Uhr	03.09.2012	4
Grundkurs UNIX/Linux mit Übungen	Hattenbach	11.09. – 13.09.2012 9:15 – 12:00 und 13:30 – 16:00 Uhr	04.09.2012	12
Installation und Administration eines Windows-Arbeitsplatz-rechners	Becker, Nolte, Quentin	17.09.2012 9:00 – 12:30 und 13:30 – 15:30 Uhr	10.09.2012	4
Photoshop für Fortgeschrittene	Töpfer	18.09. – 19.09.2012 9:30 – 16:00 Uhr	11.09.2012	8
Administration von PCs im Active Directory der GWDG	Buck, Hast	25.09.2012 9:00 – 12:30 und 13:30 – 15:30 Uhr	18.09.2012	4
Outlook – E-Mail und Group-ware	Helmvoigt	27.09.2012 9:15 – 12:00 und 13:00 – 16:00 Uhr	20.09.2012	4
UNIX für Fortgeschrittene	Dr. Sippel	15.10. – 17.10.2012 9:15 – 12:00 und 13:15 – 15:30 Uhr	08.10.2012	12
Smartphones und Tablets (iPad) für denwissenschaftli-chen Einsatz	Reimann	17.10.2012 9:00 – 12:00 und 13:00 – 16:00 Uhr	10.10.2012	4
SharePoint-Umgebung in der GWDG	Hast, Helmvoigt, Rosenfeld	13.11.2012 9:00 – 12:30 und 13:30 – 15:30 Uhr	06.11.2012	4
Einführung in die Statistische Datenanalyse mit SPSS	Cordes	21.11. – 22.11.2012 9:00 – 12:00 und 13:00 – 15:30 Uhr	14.11.2012	8
Angewandte Statistik mit SPSS für Nutzer mit Vorkenntnissen	Cordes	04.12. – 05.12.2012 9:00 – 12:00 und 13:00 – 15:30 Uhr	27.11.2012	8
UNIX/Linux-Arbeitsplatzrech-ner – Installation und Adminis-tration	Gerdes, Dr. Heuer, Körmer, Dr. Sippel	10.12. – 11.12.2012 9:15 – 12:00 und 13:30 – 16:00 Uhr	03.12.2012	8
UNIX/Linux-Server – Grundla-gen der Administration	Gerdes, Dr. Heuer, Körmer, Dr. Sippel	12.12. – 13.12.2012 9:15 – 12:00 und 13:30 – 16:00 Uhr	05.12.2012	8
UNIX/Linux – Systemsicherheit für Administratoren	Gerdes, Dr. Heuer, Körmer, Dr. Sippel	14.12.2012 9:15 – 12:00 und 13:30 – 15:00 Uhr	07.12.2012	4