GWDG NACHRICHTEN 06|14

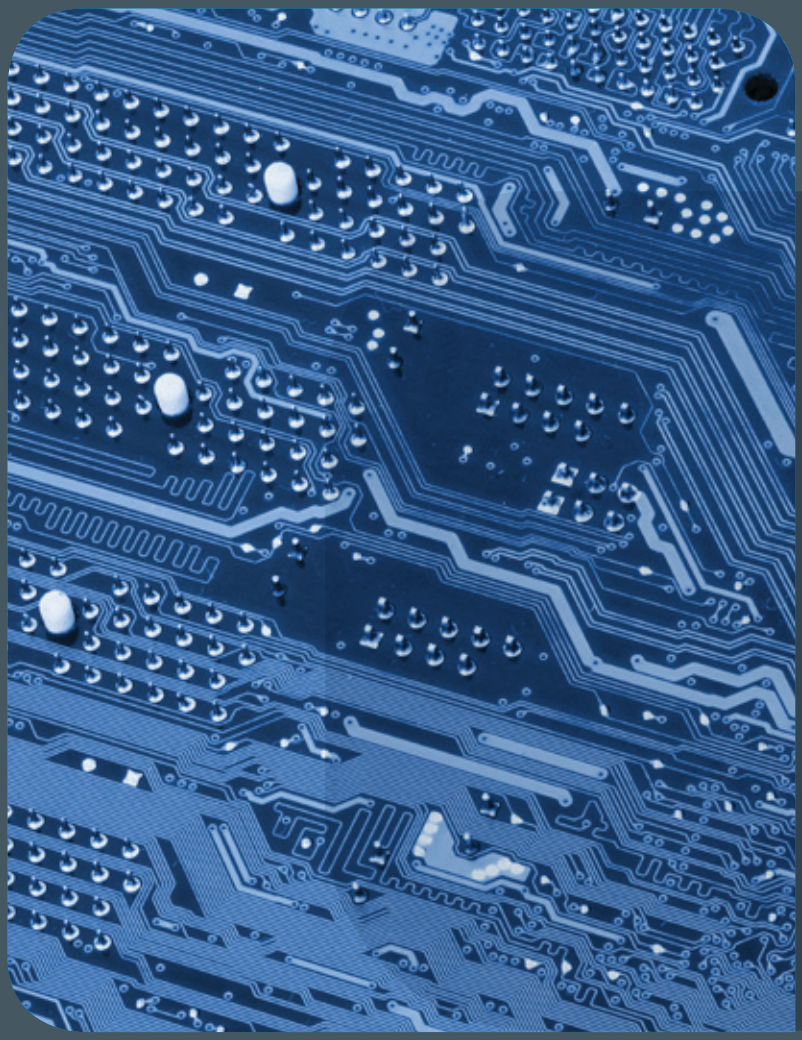
Online-Umfragen mit LimeSurvey

„Heartbleed“ Bug – Der Super-GAU für OpenSSL und HTTPS

Microsoft Campus Agreement für die Universität Göttingen

ZEITSCHRIFT FÜR DIE KUNDEN DER GWDG

GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen



GWDG
NACHRICHTEN

06|14

Inhalt

Impressum

Zeitschrift für die Kunden der GWDG

ISSN 0940-4686
37. Jahrgang
Ausgabe 6/2014

Erscheinungsweise:
monatlich

www.gwdg.de/gwdg-nr

Auflage:
500

Herausgeber:

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen
Am Faßberg 11
37077 Göttingen
Tel.: 0551 201-1510
Fax: 0551 201-2150

Redaktion:
Dr. Thomas Otto
E-Mail: thomas.otto@gwdg.de

Herstellung:
Maria Geraci
E-Mail: maria.geraci@gwdg.de

Druck:
GWDG / AG H
E-Mail: printservice@gwdg.de

Prof. Dr. Ramin Yahyapour
ramin.yahyapour@gwdg.de
0551 201-1545

Liebe Kunden und Freunde der GWDG,

die durch die Medien weltweit bekannt gewordene Sicherheitslücke „Heartbleed" hat abermals gezeigt, wie verwundbar unsere technische Informationsinfrastruktur ist. Der angebliche Programmierfehler betraf die häufig benutzte Open-Source-Softwarebibliothek OpenSSL, die für verschlüsselte Verbindungen zwischen Computer verwendet wird: eine Technik, die praktisch ständig und überall benötigt wird.

Der Vorfall zeigt zum einen, dass uns leider auch Open-Source nicht vor solchen Sicherheitsproblemen schützt. Zum anderen wird deutlich, dass es kritisch ist, wenn eine einzige Software-Implementierung die weltweite Grundlage für viele Systeme ist. Eine höhere Diversifikation durch unterschiedliche Implementierungen von wichtigen Kerntechnologien könnte das Risiko einer globalen Sicherheitslücke minimieren. Doch ein solcher Ansatz kostet Ressourcen, wobei bezweifelt werden kann, dass diese in multiple, redundante Software-Entwicklungen investiert werden.

So bleibt vielleicht nur das Warten auf die nächste Sicherheitslücke mit dem folgenden Wettlauf, diese kurzfristig zu schließen. Sicherlich kein zufriedenstellender Gedanke, wenn man berücksichtigt, wie abhängig wir von der IT-Infrastruktur geworden sind.

Ramin Yahyapour

GWDG – IT in der Wissenschaft

Neuer Dienst: Online-Umfragen mit LimeSurvey

Text und Kontakt:
Dr. Roland Baier
roland.baier@gwdg.de
0551 201-1822

Anke Bruns
anke.bruns@gwdg.de
0551 201-1519

Sie möchten für ein wissenschaftliches Projekt oder eine Prüfungsarbeit eine Datenerhebung per Online-Befragung durchführen und suchen nach einer geeigneten Softwarelösung? Die GWDG bietet ihren Kunden sowie den Studierenden der Universität Göttingen die weithin bekannte Open-Source-Software LimeSurvey (*http://www.limesurvey.org/de/*) zur Nutzung auf einem GWDG-eigenen Server an.

LimeSurvey ist eine webbasierte Umfrage-Anwendung, die mit jedem gebräuchlichen Webbrowser verwendet werden kann. Sie zeichnet sich durch eine intuitive Benutzeroberfläche aus und bietet u.a. die folgenden Funktionen und Merkmale:

- Keine Programmierkenntnisse für die Erstellung einer Umfrage erforderlich
- Rund 30 verschiedene Fragetypen stehen zur Verfügung
- Fragebedingungen lassen sich definieren.
- Umfragen können vorab getestet werden.
- Umfragen können öffentlich oder nur innerhalb eines begrenzten Teilnehmerkreises durchgeführt werden, mit anonymen oder nicht-anonymen Teilnehmern.
- Export der Umfrage-Ergebnisse in diverse Formate (z. B. Excel, CSV, SPSS)
- Umfragen können kopiert, exportiert und importiert werden.
- Gruppenarbeit möglich: ein Umfrageadministrator kann Bearbeitungsrechte an andere registrierte Benutzer geben, auch kann man Benutzer in einer Gruppe zusammenfassen und der Gruppe Berechtigungen für eine Umfrage übertragen.
- Mehrsprachigkeit
- Fristenkontrolle
- Integrierte Auswertungsfunktionen

SICHERHEIT

Die GWDG betreibt eine eigene Installation der Software, alle Daten der Umfragen bleiben vollständig „inhouse“ und werden nicht auf externe Server hochgeladen.

Die Datenübertragung zwischen dem GWDG-Server und den Web-Clients (Browsern) erfolgt verschlüsselt, der Zugang zu den LimeSurvey-Administrationsseiten ist passwortgeschützt.

Nach Abschluss einer Umfrage und einer Übergangszeit von sechs Monaten werden die Umfragen und Ergebnisse bei der GWDG gelöscht. Damit sind bewährt gute Rahmenbedingungen für Sicherheit und Datenschutz bei Umfragen gegeben.

NUTZUNG VON LIMESURVEY

Die Nutzung von LimeSurvey wird im Rahmen des Kontingentierungssystems der GWDG in Arbeitseinheiten (AE) abgerechnet. Voraussetzung für die Nutzung ist die Zugehörigkeit zur Universität Göttingen (Mitarbeiter oder Studierende), zu einer Max-Planck-Einrichtung oder zu einer anderen Forschungseinrichtung. Sie benötigen:

- Ein Benutzerkonto bei der GWDG. Dies kann auf folgender Webseite beantragt werden: *http://www.gwdg.de/index.php?id=antragsformulare*. Es entstehen dadurch keine Kosten.

ODER:

- Eine dienstliche E-Mail-Adresse oder eine studentische E-Mail-Adresse der Universität Göttingen bzw. eine E-Mail-Adresse bei einer Einrichtung der Max-Planck-Gesellschaft.

Bei Interesse an der Nutzung oder diesbezüglichen Fragen schreiben Sie bitte an *support@gwdg.de*. Geben Sie dabei Ihren Namen, Ihr GWDG-Benutzerkonto und/oder Ihre dienstliche E-Mailadresse an, und teilen Sie uns mit, für welchen Zeitraum bzw. ab wann Sie LimeSurvey nutzen möchten.

Preparing and conducting surveys with LimeSurvey

You plan to conduct an online survey for a scientific project or an examination paper and are looking for an appropriate software tool? GWDG offers its customers and the students of the university of Göttingen the use of the Open Source software LimeSurvey on a GWDG server. LimeSurvey is a web-based, user-friendly tool. The surveys and results stay completely inhouse on GWDG premises so that a maximum of data protection and security is provided.

If you are interested in using LimeSurvey or have a question please contact *support@gwdg.de*.

Sie erhalten automatisch eine E-Mail mit den Zugangsdaten für LimeSurvey, sobald ein Account für Sie eingerichtet wurde.

Wenn mehrere registrierte Benutzer gemeinsam Umfragen bearbeiten möchten, können auf Wunsch Benutzer-Gruppen eingerichtet und dann Gruppenrechte für Umfragen festgelegt werden.

DATENSCHUTZ UND VERANTWORTLICHKEIT

Umfragen werden eigenverantwortlich von den Umfrage-Administratoren erstellt. Diese dürfen ihre Zugangsdaten nicht anderen zugänglich machen. Der Veranstalter einer Umfrage ist für die Einhaltung der Datenschutzgesetze bei der Verarbeitung personenbezogener Daten verantwortlich.

In jeder Umfrage müssen Angaben zum Veranstalter (Name, Adresse, E-Mail-Adresse) gemacht werden (Impressum). Bei Umfragen innerhalb eines Unternehmens oder Instituts sind ggf. die Mitbestimmungsrechte des zuständigen Betriebsrats bzw. Personalrats zu beachten. Das Urheberrecht ist bei Text-, Bild- oder Tonmaterial einzuhalten.

Umfragedaten sollten von den Umfrageadministratoren gelöscht werden, sobald sie nicht mehr benötigt werden. Die GWDG behält sich vor, die Daten aller Umfragen, deren Abschlussdatum länger als sechs Monate zurück liegt, zu löschen. Wenn Sie die Daten über einen längeren Zeitraum für den Zweck der Umfrage benötigen, exportieren Sie diese bitte rechtzeitig vorher. Umfragedaten mit personenbezogenen und/oder sensiblen Daten müssen gegen unerlaubten Zugang gesichert aufbewahrt werden. Bitte beachten Sie, dass Sie personenbezogene Daten, auch exportierte, löschen müssen, sobald sie nicht mehr für den angegebenen Zweck gebraucht werden.

AUSWERTUNG UND ARCHIVIERUNG

Die Auswertung einer Umfrage ist direkt in LimeSurvey möglich. Ferner lassen sich die Umfrageergebnisse aus LimeSurvey in verschiedene Formate exportieren, z. B. für Excel oder SPSS, oder als „Tab-getrennte Werte". Damit stehen die Daten auch außerhalb von LimeSurvey für Auswertungen zur Verfügung.

Auch die Umfrage-Struktur kann aus LimeSurvey exportiert werden, und zwar wahlweise nur die Struktur und die Fragen oder auch die komplette Umfrage inkl. Antworten. Dies ermöglicht die Archivierung einer Umfrage. Auch kann eine Umfrage wieder in LimeSurvey importiert werden, z. B. um sie später erneut durchzuführen.

WEITERFÜHRENDE INFORMATIONEN ZUR NUTZUNG VON LIMESURVEY

Wissenswertes über den Service und die Nutzungsbedingungen für LimeSurvey bei der GWDG finden Sie unter *http://www.gwdg.de/index.php?id=2991*.

Erster Anlaufpunkt bei Fragen zum Arbeiten mit LimeSurvey ist das umfangreiche Online-Handbuch *http://manual.limesurvey.org/LimeSurvey_Manual/de*. Lösungen zu vielen Problemen gibt es in den LimeSurvey Support-Foren *http://www.limesurvey.org/de/community/hilfe-foren*.

Darüber hinaus findet man im World Wide Web zahlreiche weitere Anleitungen und Ratgeber, und nicht zuletzt berät auch die GWDG bei Fragen oder Problemen mit LimeSurvey.

Informationen zu Online-Umfragen generell findet man z.B. in Wikipedia *http://de.wikipedia.org/wiki/Online-Umfrage*.

Wenn Sie LimeSurvey einfach nur ausprobieren möchten, dann können Sie dazu die Demo-Installation auf *http://www.limesurvey.org/de/demo* nutzen.

Ein „eigenes" LimeSurvey zur Selbstinstallation für Testzwecke lässt sich leicht beschaffen. Man besorgt sich dazu eine XAMPP-Entwicklungsumgebung, *https://www.apachefriends.org/de/index.html*, und installiert darin LimeSurvey. Für Windows gibt es auch ein Komplettpaket „LimeSurvey on XAMPP" *http://www.limesurvey.org/en/stable-release*.

Kurz & knapp

Öffnungszeiten des Rechenzentrums um Himmelfahrt und um Pfingsten 2014

Das Rechenzentrum der GWDG ist sowohl Himmelfahrt, 29.05.2014, als auch an beiden Pfingstfeiertagen, 08.06. und 09.06.2014, 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 Ticket-System wird auch während dieser Zeit von Mitarbeiterinnen und Mitarbeitern der GWDG regelmäßig kontrolliert.

Wir bitten alle Benutzerinnen und Benutzer, sich darauf einzustellen.

Grieger

„Heartbleed“-Bug – Der Super-GAU für OpenSSL und HTTPS

Text und Kontakt:
Dr. Daniel Adler
daniel.adler@gwdg.de
0551 201-2134

Thorsten Hindermann
thorsten.hindermann@gwdg.de
0551 201-1837

Anfang April 2014 wurde eine kritische Sicherheitslücke in der OpenSSL-Bibliothek gemeldet – viele Sicherheitsexperten bewerteten die Meldung als den Super-GAU für sichere Kommunikation im World Wide Web. Daher ist es nun Zeit für eine technische Nachbetrachtung.

OpenSSL ist eine der weit verbreiteten open-source Implementierungen für das SSL/TLS Protokoll zur sicheren Kommunikation im Internet und wird bei vielen Web-Servern wie Apache, nginx oder lighttpd zur Unterstützung von HTTPS-Verbindungen eingesetzt.

Die Sicherheitslücke in OpenSSL ermöglicht einem Angreifer, eine Anfrage an den Webserver zu stellen, womit er knapp 64 Kilobyte große Speicherblöcke pro Anfrage aus dem Hauptspeicher der Gegenstelle an einer äußerst sensiblen Stelle im Kontext der Verschlüsselung mit OpenSSL auslesen kann. Sie kann u.a. dafür verwendet werden, verschlüsselte Kommunikation von Dritten auf dem selben Server „mitzulesen“, um z. B. Session-Schlüssel, Benutzernamen und Passwörter unverschlüsselt abzufangen oder aber auch um den privaten Schlüssel eines Server-Zertifikats auszulesen.

Die Sicherheitslücke entstand als Seiteneffekt während der Implementierung der „Heartbeat”-Erweiterung von TLS - welche im Februar 2012 veröffentlicht wurde (siehe [1]). Die Implementierung wurde einen Monat später eingepflegt. Damit klaffte diese Lücke seit März 2012 in vielen Produkten mit aktuelleren OpenSSL-Versionen 1.0.1 bis 1.0.1f.

Aufgrund der Brisanz wurde die Sicherheitslücke im Rahmen einer medienwirksamen Web-Kampagne mit dem Spitznamen „Heartbleed“ und einem passenden Logo publik gemacht. Offiziell ist der Bug als CVE-2014-0160 registriert (siehe [2]). Dazu gibt es zahlreiche Websites und Online-Tools mit denen man seinen eigenen Webserver überprüfen kann (siehe [3]).

Schätzungen zur Folge waren zum Zeitpunkt des Vorfalls etwa eine halbe Million HTTPS-Server betroffen (etwa 17% der weltweit verfügbaren HTTPS-Webserver) [4]. Zahlreiche Linux-Distributionen (Ubuntu, Debian, Fedora, CentOS, Suse, NetOS) und BSD-basierte Betriebssysteme (NetBSD, FreeBSD, OpenBSD), Webseiten (Yahoo, GitHub, Ars Technica, Stack Overflow, DuckDuckGo) und Anwendungen (LibreOffice, FileMaker, WinSCP

„Heartbleed“ Bug – the worst case scenario for OpenSSL

In April a critical security vulnerability in OpenSSL was reported.OpenSSL is the most commonly used HTTPS protocol engine - responsible for managing secure connections in major open-source web servers. The security bug „Heartbleed“ allows an attacker to read random server memory, including username and password credentials or even private keys of server certificates. Since „Heartbleed“ remained undiscovered for about the last two years, security experts were talking about one of the worst security bugs of our times.

5.5.2) waren betroffen. Auch einige Web-Dienste der GWDG (Cryptshare, VMware vSphere, GWDG Compute Cloud, virtuelle Web-Server) waren nicht verschont worden, wurden aber sofort nach Erscheinen der Sicherheitswarnungen gepatcht und mit neuen Server-Zertifikaten versorgt. Wir haben keinerlei Anzeichen dafür, dass die Schwachstelle genutzt wurde, um Datenübertragungen der GWDG zu entschlüsseln.

WAS IST ZU TUN?

Die Konsequenzen aus dieser fatalen Schwierigkeit mit OpenSSL können in zwei Bereiche aufgeteilt werden. Ein Bereich ist für die Verwalter der betroffenen Betriebssysteme und Dienste. Der zweite Bereich ist für Anwender, die zentral bereitgestellte Dienste nutzen.

SERVER-BETRIEBSSYSTEME

Als Verwalter eines Systems oder Dienstes, sollten Sie prüfen, ob ihr Betriebssystem die betroffene OpenSSL-Version noch einsetzt oder in dem genannten Zeitraum diese Version im Einsatz war. Die meisten Betriebssysteme haben inzwischen mittels Software-Aktualisierung die betroffene Version gegen die neueste, korrigierte OpenSSL-Version ausgetauscht. Aber zu Ihrer eigenen (System-)Sicherheit und der Ihrer Anwender sollten Sie überprüfen, ob die neueste OpenSSL-Version im Einsatz ist, und als weiteren Schritt sollten Sie für Ihr System oder Ihren Dienst ein neues Zertifikat mit der neuesten OpenSSL-Version beantragt haben. Das ausgestellte Zertifikat sollten Sie dann auch schnellst möglich in den Einsatz bringen.

Die Informationen darüber, ob Ihr System betroffen war oder noch ist, finden Sie unter dem URL *https://portal.cert.dfn.de/adv/DFN-CERT-2014-0420/*.

ANWENDER

Benutzern von zentralen Systemen und Diensten, an denen sie sich anmelden müssen, wird empfohlen, die Kennwörter für die Systeme in regelmäßigen Abständen zu ändern. Wichtig ist hier der Hinweis, dass das neue Kennwort eine Zeichenlänge von mindestens 10 Zeichen oder mehr hat. Wahlweise können ein oder mehrere Zeichen Großbuchstaben, Zahlen oder Sonderzeichen sein.

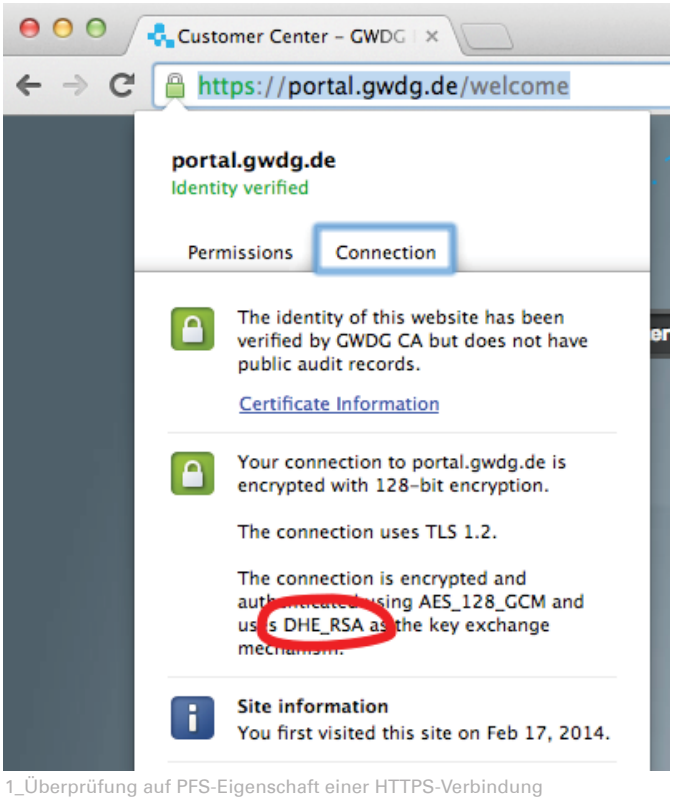
Aber am wichtigsten ist die regelmäßige Änderung des Kennworts, unabhängig vom Bekanntwerden einer Sicherheitslücke! Dies ist der beste Schutz gegen den Zugriff Dritter auf ihre Daten.

Alle Anwender von GWDG-Systemen und -Diensten können sich unter dem URL *http://www.gwdg.de/heartbleed* über deren fehlerbereinigten Zustand informieren. Bei allen dort aufgeführten Systemen und Diensten sind die Zertifikate für die Verschlüsselung der Kommunikation ausgetauscht worden. Damit sind alle eingegebenen und abgerufenen Informationen wieder abgesichert, verschlüsselt und können nicht mehr mittels präparierter Web-Seiten attackiert werden, um unberechtigter Weise an sensible Informationen zu gelangen.

ZUSÄTZLICHE MASSNAHMEN FÜR BETREIBER VON WEB-SERVERN MIT HTTPS-UNTERSTÜTZUNG

Verschlüsselte Kommunikation nutzt einen gemeinsam bekannten zufällig ausgehandelten Session-Schlüssel. Typischerweise generiert der Browser (Client) diesen Schlüssel und verschlüsselt diesen mit dem öffentlichen Schlüssel des Server-Zertifikats. Dieses Verfahren hat allerdings einen Haken.

Für den Fall, dass der private Server-Schlüssel kompromittiert wurde, können aufgezeichnete verschlüsselte Nachrichten aus der Vergangenheit rückwirkend offline entschlüsselt werden. Deshalb wird spätestens seit der NSA-Abhöraffäre, und nun auch nach "Heartbleed", Betreibern von SSL/TLS Servern eine Konfiguration des Schlüsselaustausch-Verfahren nach dem Prinzip von "Perfect Forward Secrecy" (PFS) empfohlen. Hier wird der gemeinsame Schlüssel über ein verbessertes mathematisches Verfahren (Diffie-Hellman) unter den Beteiligten bekannt gemacht und hängt nicht mehr direkt vom privaten Schlüssel des Server-Zertifikats ab. Viele gängige Web-Browser und Server unterstützen dieses Verfahren. Eine Überprüfung, ob eine HTTPS-Verbindung nach „PFS" arbeitet, kann u.a. im Google-Chrome-Browser eingesehen werden, wie in Abbildung 1 gezeigt ist. Folgende Schlüsseltausch-Verfahren funktionieren nach PFS: DHE-RSA, ECDHE-RSA oder ECDHE-ECDSA.



1_Überprüfung auf PFS-Eigenschaft einer HTTPS-Verbindung

Um einen PFS-basierten Schlüsselaustausch anzubieten, muss die SSL-Konfiguration des Webservers gegebenenfalls konfiguriert werden. Auszüge aus der SSL Konfiguration für Apache 2.2/2.4, nginx und lighttpd sind hier gezeigt:

Apache 2.2/2.4

```
SSLProtocol all -SSLv2 -SSLv3 +TLSv1.2 +TLSv1.1 +TLSv1 SSL-
Compression off
SSLHonorCipherOrder on
SSLCipherSuite "EECDH+ECDSA+AESGCM:EECDH+aRSA+AES
GCM:EECDH+ECDSA+SHA384:EECDH+ECDSA+SHA256:EECD
H+aRSA+SHA384:EECDH+aRSA+SHA256:EECDH+aRSA+RC4:
EECDH:EDH+aRSA:RC4:!aNULL:!eNULL:!LOW:!3DES:!MD5:!EX
P:!PSK:!SRP:!DSS"
```

nginx 1.4

```
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
ssl_prefer_server_ciphers on;
ssl_ciphers „EECDH+ECDSA+AESGCM EECDH+aRSA+AESGCM
EECDH+ECDSA+SHA384 EECDH+ECDSA+SHA256
EECDH+aRSA+SHA384 EECDH+aRSA+SHA256
EECDH+aRSA+RC4 EECDH EDH+aRSA RC4 !aNULL !eNULL
!LOW !3DES !MD5 !EXP !PSK !SRP !DSS";
```

lighttpd 1.4

```
ssl.use-sslv2 = „disable"
ssl.use-compression = „disable"
ssl.honor-cipher-order = „enable"
ssl.cipher-list = „ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-
RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-
SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECD-
SA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-
SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-
AES128-SHA256:ECDHE-RSA-AES256-SHA"
```

DETAILS DES „HEARTBLEED"-BUGS UND EINES ANGRIFFS

Die „Heartbeat"-TLS-Erweiterung ist dazu gedacht, um eine bestehende, aber vielleicht gerade inaktive Verbindung längerfristig aufrecht zu erhalten. Hierbei wird eine „Herzschlag"-Anfrage mit zufälligen Dummy-Daten vom Client oder Server an die Gegenstelle geschickt. Das Protokoll sieht vor, dass die Gegenstelle die Dummy-Daten aus dem empfangenen Paket in ein Antwort Paket umkopiert und zurücksendet.

Grund für das Sicherheitsleck war ein Programmierfehler in der Routine zur Generierung des Antwortpakets. Es wurde versäumt zu überprüfen, ob die Größenangabe *„payload_length"* mit der tatsächlichen Größe des gesendeten Pakets übereinstimmt (C Datenstruktur des Pakets ist abgebildet in Listing 1).

Listing 1:

```
struct {
  HeartbeatMessageType type;
  uint16 payload_length;
  opaque payload[HeartbeatMessage.payload_length];
  opaque padding[padding_length];
} HeartbeatMessage;
```

Ein Angreifer kann somit eine Heartbeat-Anfrage mit einer sehr kleinen payload allerdings einer payload_length von 65535 schicken, sodass die Gegenstelle über das empfangene kleine Paket hinaus weitere Daten aus dem Heap-Speicher in das große Antwort-Objekt kopiert und an den Angreifer zurückschickt. (Siehe Listing 2 und originalen GIT commit unter [5])

Listing 2: Auszug aus OpenSSL GIT Repo, File t1_lib.c ab Zeile 2404 (Stand vom 01.01.2012).

```
int  tls1_process_heartbeat(SSL *s)
{
  unsigned char *p = &s->s3->rrec.data[0], *pl;
  unsigned int payload;
  unsigned int padding = 16; /* Use minimum padding */

  /* Read type and payload length first */

  hbtype = *p++;
  n2s(p, payload);
  pl = p;

  /* Allocate memory for the response, size is 1 bytes
   * message type, plus 2 bytes payload length, plus
   * payload, plus padding
   */

  buffer = OPENSSL_malloc(1 + 2 + payload + padding);
  bp = buffer;
  *bp++ = TLS1_HB_RESPONSE;
  s2n(payload, bp);
  pl = p;
  memcpy(bp, pl, payload); /* <-- *BAM* */
```

Chronologie der Ereignisse

2011	Seggelmann begann mit Arbeiten an der Heartbeat-Erweiterung.
31.12.2011	OpenSSL-Entwickler Henson pflegte den Patch von Seggelmann ein.
02/2012	TLS/DTLS-Heartbeat Extension wurde veröffentlicht als RFC 6520.
14.03.2012	OpenSSL 1.0.1 inkl. Heartbeat-Implementierung und Bug wurde released.
01.04.2014	Codedenomicon Security Company und Neel Mehta von Google's Security Team haben „Heartbleed" gemeldet.
07.04.2014	„Heartbleed" wurde unter CVS-2014-0160 offiziell gemeldet.

Referenzen (Alle Links vom 16.05.2014)

[1] Details über CVE-2014-0160: *http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160*

[2] RFC 6520 - TLS/DTLS Heartbeat Extension: *https://www.rfc-editor.org/rfc/rfc6520.txt*

[3] Heartbleed Website Testing Tool: *https://filippo.io/Heartbleed/*

[4] Half a million widely trusted websites vulnerable to Heartbleed bug: *http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html*

[5] GIT commit des Heartbeat Bugs in den OpenSSL Source: *http://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=4817504*

Microsoft Campus Agreement für die Universität Göttingen

Text und Kontakt:
Dr. Wilfried Grieger
wilfried.grieger@gwdg.de
0551 201-1512

Nach dem beabsichtigten Beitritt der Universität Göttingen zum Campus Agreement der Firma Microsoft wird den Instituten Desktop- und Server-Software ohne weitere Zusatzkosten zur Verfügung stehen.

Das Präsidium der Universität hat auf seiner Sitzung am 13.05.2014 beschlossen, dass die gesamte Universität Göttingen, einschließlich Universitätsmedizin, dem Bundesrahmenvertrag über ein Campus Agreement der Firma Microsoft beitreten soll.

AUSSCHREIBUNG

Aufgrund des finanziellen Volumens des Campus Agreements muss der Vertrag europaweit ausgeschrieben werden, und zwar bezüglich des Händlers, der nach Abschluss des Vertrags die Software sowie die zugehörigen Lizenzen liefern wird. Wir rechnen damit, dass der Vertrag danach zum 01.08.2014 oder zum 01.09.2014 in Kraft treten kann.

SOFTWARE

Da die Kosten des Campus Agreements lediglich nach der Anzahl der Beschäftigten und nicht nach der Anzahl der eingesetzten Systeme berechnet werden, steht nach Abschluss des Vertrags u. a. die folgende Software ohne Zusatzkosten in beliebiger Anzahl für die Rechner der Institute und der Verwaltung zur Verfügung:

- Windows Upgrade
- Office Professional Plus
- Windows Server
- SharePoint Server
- Exchange Server
- alle Standard-Zugriffslizenzen (CALs) (sowohl für Beschäftigte als auch für Studierende) auf diese Server

„Windows Upgrade" bedeutet dabei, dass Sie für einen Rechner, auf dem ein Windows-Betriebssystem lizenziert ist (beispielsweise mitgekauft bei der Anschaffung des Rechners, OEM-Lizenz) ein beliebiges „höheres" Windows-Betriebssystem einsetzen dürfen. Es ist also weiterhin erforderlich, dass Sie mit einem neuen Rechner, der für den Einsatz von Windows vorgesehen ist, ein Windows-Betriebssystem (Basis-Lizenz) z. B. über den Dell-Rahmenvertrag mitbeschaffen. Für Rechner ohne Windows-Betriebssystem kann auch nachträglich beispielsweise bei der Firma asknet eine Basis-Lizenz(natürlich kostenpflichtig) erworben werden. Dadurch ist sichergestellt, dass genügend viele Basis-Lizenzen vorhanden sind, die als Grundlage für den Upgrade dienen können.

In allen anderen oben genannten Software-Produkten ist die Basis-Lizenz enthalten.

Falls Sie andere Software von Microsoft benötigen, kann diese nach wie vor über den Microsoft Select Plus Vertrag bei der Firma asknet in Karlsruhe erworben werden. Dieser Vertrag wird unabhängig vom Campus Agreement weiterhin bestehen bleiben.

UPGRADE DER WINDOWS-XP-LIZENZEN

Diejenigen von Ihnen, die wegen der Sicherheitsproblematik in Windows XP dringend auf ein neueres Betriebssystem upgraden müssen, können das nun im Rahmen von Testlizenzen kostenlos tun. Diese Testlizenzen werden dann nach dem Abschluss des Campus Agreements automatisch in diesen Vertrag überführt.

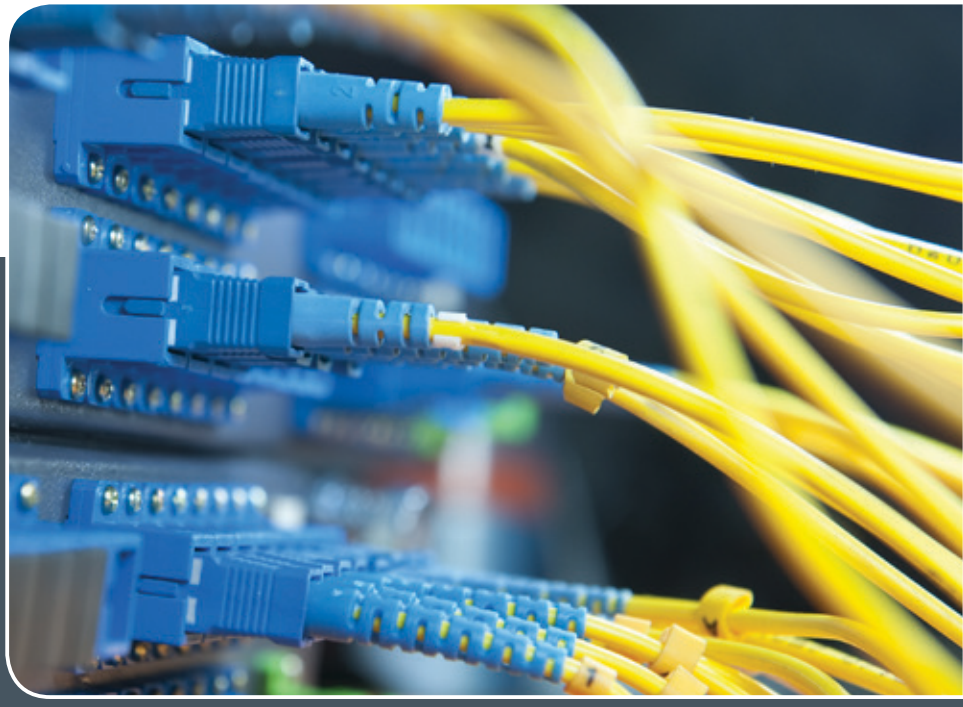
FINANZIERUNG

Von der Universität wird es demnächst noch Informationen über die Verteilung der Kosten zur Finanzierung des Campus Agreements geben.

Microsoft Campus Agreement for the University of Göttingen

After the proposed accession of the University of Göttingen for Microsoft´s Campus Agreement the institutes will have access to desktop and server software without additional fees.

GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen



IP-Adress-Managementsystem

IP-ADRESS-VERWALTUNG LEICHT GEMACHT!

Ihre Anforderung

Sie möchten Ihre IP-Adressvergabe, DNS- und DHCP-Dienste (IPv4 und IPv6) zentral und professionell verwalten. Sie möchten die Pflege der IP-, DNS- und DHCP-Daten an eigene Administratoren delegieren. Sie möchten DNS- und DHCP-Dienste über Appliance-Technologie hochverfügbar realisieren.

Unser Angebot

Wir bieten Ihnen die Mitnutzung unseres mandantenfähigen IP-Adress-Managementsystems (IPAM-Systems) an. Die Adressbestände und DNS-Namensräume können dabei von einem Administrator oder mehreren gepflegt werden. Die Synchronisation der Daten in den zugehörigen DNS- und DHCP-Diensten erfolgt periodisch oder unmittelbar auf Anforderung. DNS- und DHCP-Dienste können über zentral verwaltete Appliances lokal erbracht werden. Wir bieten Schulung Ihrer Administratoren durch GWDG-Spezialisten an.

Ihre Vorteile

> Die IPv4- und IPv6-Adressbestände werden professionell verwaltet.

> Die Konsistenz der Daten im Adress- und Namensraum wird sichergestellt.

> Die Pflege über die WWW-Schnittstelle ist ohne große Einarbeitung und ohne großes Expertenwissen über DNS- und DHCP-Dienste sowie Betriebssysteme seitens Ihrer Mitarbeiter möglich.

> Die Delegation der Verwaltung von Teilbereichen des Adress- und Namensraums an verschiedene Sub-Administratoren wird ermöglicht.

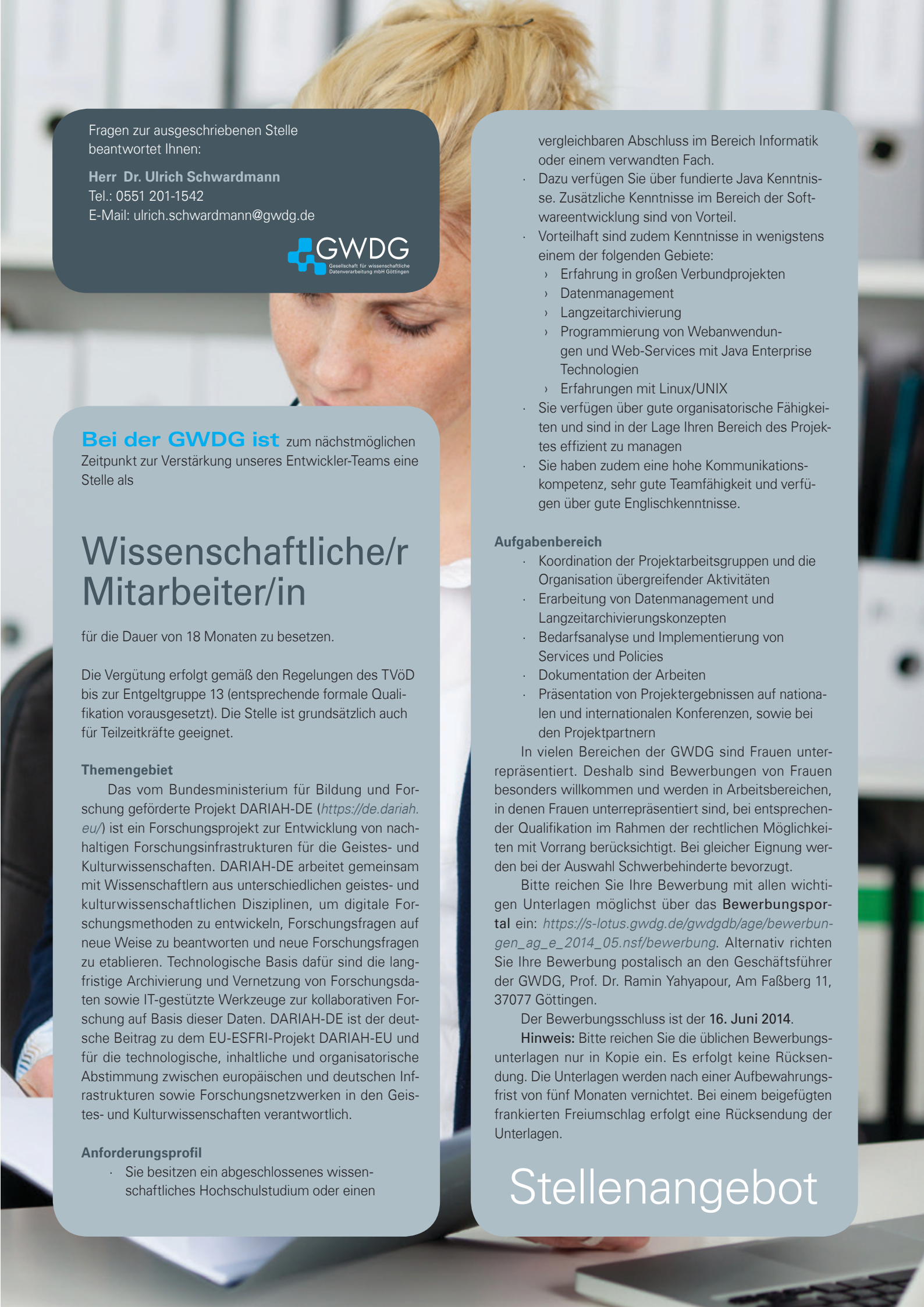
> DNS- und DHCP-Dienste können bei Einsatz von Appliance-Systemen vor Ort hochverfügbar erbracht werden (optional).

> Nutzung der DNS-Server der GWDG für öffentliche DNS-Datenbestände (ohne Notwendigkeit, dafür einen eigenen Server zu betreiben; optional)

Interessiert?

Wenn Sie unser IPAM-System nutzen möchten, werfen Sie bitte einen Blick auf die u. g. Webadresse. Ihr Institut muss einen oder mehrere erforderliche Administratoren benennen. Für DNS-Dienste ist die Integration vorhandener DNS-Server oder der Einsatz einer lokalen Appliance nötig. DHCP-Dienste erfordern immer eine lokale Appliance. Lokale Appliances müssen vom Institut beschafft werden (optional; abhängig von den Anforderungen des Instituts).

www.gwdg.de/ipam



Fragen zur ausgeschriebenen Stelle beantwortet Ihnen:

Herr Dr. Ulrich Schwardmann
Tel.: 0551 201-1542
E-Mail: ulrich.schwardmann@gwdg.de

Bei der GWDG ist zum nächstmöglichen Zeitpunkt zur Verstärkung unseres Entwickler-Teams eine Stelle als

Wissenschaftliche/r Mitarbeiter/in

für die Dauer von 18 Monaten zu besetzen.

Die Vergütung erfolgt gemäß den Regelungen des TVöD bis zur Entgeltgruppe 13 (entsprechende formale Qualifikation vorausgesetzt). Die Stelle ist grundsätzlich auch für Teilzeitkräfte geeignet.

Themengebiet

Das vom Bundesministerium für Bildung und Forschung geförderte Projekt DARIAH-DE (*https://de.dariah.eu/*) ist ein Forschungsprojekt zur Entwicklung von nachhaltigen Forschungsinfrastrukturen für die Geistes- und Kulturwissenschaften. DARIAH-DE arbeitet gemeinsam mit Wissenschaftlern aus unterschiedlichen geistes- und kulturwissenschaftlichen Disziplinen, um digitale Forschungsmethoden zu entwickeln, Forschungsfragen auf neue Weise zu beantworten und neue Forschungsfragen zu etablieren. Technologische Basis dafür sind die langfristige Archivierung und Vernetzung von Forschungsdaten sowie IT-gestützte Werkzeuge zur kollaborativen Forschung auf Basis dieser Daten. DARIAH-DE ist der deutsche Beitrag zu dem EU-ESFRI-Projekt DARIAH-EU und für die technologische, inhaltliche und organisatorische Abstimmung zwischen europäischen und deutschen Infrastrukturen sowie Forschungsnetzwerken in den Geistes- und Kulturwissenschaften verantwortlich.

Anforderungsprofil

- Sie besitzen ein abgeschlossenes wissenschaftliches Hochschulstudium oder einen vergleichbaren Abschluss im Bereich Informatik oder einem verwandten Fach.
- Dazu verfügen Sie über fundierte Java Kenntnisse. Zusätzliche Kenntnisse im Bereich der Softwareentwicklung sind von Vorteil.
- Vorteilhaft sind zudem Kenntnisse in wenigstens einem der folgenden Gebiete:
  - Erfahrung in großen Verbundprojekten
  - Datenmanagement
  - Langzeitarchivierung
  - Programmierung von Webanwendungen und Web-Services mit Java Enterprise Technologien
  - Erfahrungen mit Linux/UNIX
- Sie verfügen über gute organisatorische Fähigkeiten und sind in der Lage Ihren Bereich des Projektes effizient zu managen
- Sie haben zudem eine hohe Kommunikationskompetenz, sehr gute Teamfähigkeit und verfügen über gute Englischkenntnisse.

Aufgabenbereich

- Koordination der Projektarbeitsgruppen und die Organisation übergreifender Aktivitäten
- Erarbeitung von Datenmanagement und Langzeitarchivierungskonzepten
- Bedarfsanalyse und Implementierung von Services und Policies
- Dokumentation der Arbeiten
- Präsentation von Projektergebnissen auf nationalen und internationalen Konferenzen, sowie bei den Projektpartnern

In vielen Bereichen der GWDG sind Frauen unterrepräsentiert. Deshalb sind Bewerbungen von Frauen besonders willkommen und werden in Arbeitsbereichen, in denen Frauen unterrepräsentiert sind, bei entsprechender Qualifikation im Rahmen der rechtlichen Möglichkeiten mit Vorrang berücksichtigt. Bei gleicher Eignung werden bei der Auswahl Schwerbehinderte bevorzugt.

Bitte reichen Sie Ihre Bewerbung mit allen wichtigen Unterlagen möglichst über das **Bewerbungsportal** ein: *https://s-lotus.gwdg.de/gwdgdb/age/bewerbungen_ag_e_2014_05.nsf/bewerbung*. Alternativ richten Sie Ihre Bewerbung postalisch an den Geschäftsführer der GWDG, Prof. Dr. Ramin Yahyapour, Am Faßberg 11, 37077 Göttingen.

Der Bewerbungsschluss ist der **16. Juni 2014**.

Hinweis: Bitte reichen Sie die üblichen Bewerbungsunterlagen nur in Kopie ein. Es erfolgt keine Rücksendung. Die Unterlagen werden nach einer Aufbewahrungsfrist von fünf Monaten vernichtet. Bei einem beigefügten frankierten Freiumschlag erfolgt eine Rücksendung der Unterlagen.

Stellenangebot

Personalia

NEUE MITARBEITERIN NOA CAMPOS LÓPEZ

Seit dem 15. April arbeitet Frau Noa Campos López für die Arbeitsgruppe eScience und unterstützt dort das PERICLES-Projekt. Frau Campos Lopéz besitzt einen Masterabschluss in Signalverarbeitung und Kommunikation und einen Ingenieurabschluss in Telekommunikation. Danach arbeitete sie mehr als drei Jahre am Institut für organische Chemie an der Univesität Vigo. Dort war sie Softwareentwicklerin für die Verarbeitung von Kernspinresonanzspektren und 3D-Visualisierungswerkzeugen. Hierbei begleitete sie u.a. die Implementierung für die mobile Visualisierung auf Tablets und Smartphones. Im Anschluss wechselte sie in die Arbeitsgruppe für Inverse Probleme am Institut für Numerische und Angewandte Mathematik in Göttingen und arbeitete dort an der Verarbeitung von Magnetresonanztomographie-Daten und deren Visualisierung.

Since April 2014 Noa Campos López is working at the „eScience" Arbeitsgruppe, supporting the PERICLES project. She is a Telecommunications engineer with a Master's degree in Signal Theory and Communications. She was working during more than three years at the Department of Organic Chemistry, University of Vigo. Her contribution was to provide the software development for the scientific needs of the group. This leads to the active development of NMR (Nuclear magnetic resonance) processing and 3D molecular visualization tools, as well as a mobile platform oriented application for displaying and processing NMR spectra. After that, she joined the Inverse Probleme Arbeitsgruppe at the Institut für Numerische und Angewandte Mathematik in Göttingen, where she collaborated in an MRI (Magnetic resonance imaging) processing and visualization project.

Wieder

INFORMATIONEN:
support@gwdg.de
0551 201-1523

Juni bis
Dezember 2014

Kurse

KURS	VORTRAGENDE/R	TERMIN	ANMELDEN BIS	AE
ANGEWANDTE STATISTIK MIT SPSS FÜR NUTZER MIT VORKENNTNISSEN	Cordes	18.06. – 19.06.2014 9:00 – 12:00 und 13:00 – 15:30 Uhr	11.06.2014	8
DATENSCHUTZ – VERARBEITUNG PERSONENBEZOGENER DATEN AUF DEN RECHENANLAGEN DER GWDG	Dr. Grieger	25.06.2014 9:00 – 12:00 Uhr	18.06.2014	2
MAC OS X IM WISSENSCHAFTLICHEN ALLTAG	Bartels	25.06. – 26.06.2014 9:30 – 16:30 Uhr	18.06.2014	8
EINFÜHRUNG IN WINDOWS 8	Buck	02.07.2014 9:00 – 12:30 und 13:30 – 15:30 Uhr	25.06.2014	4
QUICKSTARTING R: EINE ANWENDUNGSORIENTIERTE EINFÜHRUNG IN DAS STATISTIKPAKET R	Cordes	08.07. – 09.07.2014 9:00 – 12:00 und 13:00 – 15:30 Uhr	01.07.2014	8
HIGH-LEVEL, HIGH-PERFORMANCE TECHNICAL COMPUTING WITH JULIA	Chronz	22.07.2014 9:15 – 16:30 Uhr	15.07.2014	4
INSTALLATION UND ADMINISTRATION VON WINDOWS 8	Buck	30.07.2014 9:00 – 12:30 und 13:30 – 15:30 Uhr	23.07.2014	4
GRUNDLAGEN DER BILDBEARBEITUNG MIT PHOTOSHOP	Töpfer	15.09. – 16.09.2014 9:30 – 16:00 Uhr	08.09.2014	8
INDESIGN – GRUNDLAGEN	Töpfer	23.09. – 24.09.2014 9:30 – 16:00 Uhr	16.09.2014	8

KURS	VORTRAGENDE/R	TERMIN	ANMELDEN BIS	AE
OUTLOOK – E-MAIL UND GROUPWARE	Helmvoigt	29.09.2014 9:15 – 12:00 und 13:00 – 16:00 Uhr	22.09.2014	4
GRUNDKURS UNIX/LINUX MIT ÜBUNGEN	Hattenbach	30.09. – 02.10.2014 9:15 – 12:00 und 13:30 – 16:00 Uhr	23.09.2014	12
PHOTOSHOP FÜR FORTGESCHRITTENE	Töpfer	06.10. – 07.10.2014 9:30 – 16:00 Uhr	29.09.2014	8
DIE SHAREPOINT-UMGEBUNG DER GWDG	Buck	09.10.2014 9:00 – 12:30 und 13:30 – 15:30 Uhr	02.10.2014	4
INDESIGN – AUFBAUKURS	Töpfer	13.10. – 14.10.2014 9:30 – 16:00 Uhr	16.10.2014	8
ADMINISTRATION VON PCS IM ACTIVE DIRECTORY DER GWDG	Buck	16.10.2014 9:00 – 12:30 und 13:30 – 15:30 Uhr	09.10.2014	4
WINDOWS-CLIENT-MANAGEMENT MIT BARAMUNDI	Becker, Körmer, Quentin, Rosenfeld	16.10.2014 9:00 – 12:30 und 13:30– 15:30 Uhr	09.10.2014	4
HIGH-LEVEL, HIGH-PERFORMANCE TECHNICAL COMPUTING WITH JULIA	Chronz	20.10.2014 9:15 – 16:30 Uhr	13.10.2014	4
EINFÜHRUNG IN DIE STATISTISCHE DATENANALYSE MIT SPSS	Cordes	29.10. – 30.10.2014 9:00 – 12:00 und 13:00 – 15:30 Uhr	22.10.2014	8
UNIX FÜR FORTGESCHRITTENE	Dr. Sippel	10.11. – 12.11.2014 9:15 – 12:00 und 13:15 – 15:30 Uhr	03.11.2014	12
ANGEWANDTE STATISTIK MIT SPSS FÜR NUTZER MIT VORKENNTNISSEN	Cordes	19.11. – 20.11.2014 9:00 – 12:00 und 13:00 – 15:30 Uhr	12.11.2014	8
EINFÜHRUNG IN DAS IP-ADRESSMANAGEMENTSYSTEM DER GWDG FÜR NETZWERKBEAUFTRAGTE	Dr. Beck	26.11.2014 10:00 – 12:00 Uhr	19.11.2014	2
DIE SHAREPOINT-UMGEBUNG DER GWDG	Buck	04.12.2014 9:00 – 12:30 und 13:30 – 15:30 Uhr	27.11.2014	4
QUICKSTARTING R: EINE ANWENDUNGSORIENTIERTE EINFÜHRUNG IN DAS STATISTIKPAKET R	Cordes	10.12. – 11.12.2014 9:00 – 12:00 und 13:00 – 15:30 Uhr	03.12.2014	8

Teilnehmerkreis
Das Kursangebot der GWDG richtet sich an alle Mitarbeiterinnen und Mitarbeiter aus den Instituten der Universität Göttingen und der Max-Planck-Gesellschaft sowie aus einigen anderen wissenschaftlichen Einrichtungen.

Anmeldung
Anmeldungen können schriftlich per Brief oder per Fax unter der Nummer 0551 201-2150 an die GWDG, Postfach 2841, 37018 Göttingen oder per E-Mail an die Adresse *support@ gwdg.de* erfolgen. Für die schriftliche Anmeldung steht unter *http://www.gwdg.de/antragsformulare* ein Formular zur Verfügung. Telefonische Anmeldungen können leider nicht angenommen werden.

Kosten bzw. Gebühren
Unsere Kurse werden wie die meisten anderen Leistungen der GWDG in Arbeitseinheiten (AE) vom jeweiligen Institutskontingent abgerechnet. Für die Institute der Universität Göttingen und der Max-Planck-Gesellschaft erfolgt keine Abrechnung in EUR.

Absage
Sie können bis zu acht Tagen vor Kursbeginn per E-Mail an *support@gwdg.de* oder telefonisch unter 0551 201-1523 absagen. Bei späteren Absagen werden allerdings die für die Kurse berechneten AE vom jeweiligen Institutskontingent abgebucht.

Kursorte
Alle Kurse finden im Kursraum oder Vortragsraum der GWDG statt. Die Wegbeschreibung zur GWDG sowie der Lageplan sind unter *http://www.gwdg.de/lageplan* zu finden.

Kurstermine
Die genauen Kurstermine und -zeiten sowie aktuelle kurzfristige Informationen zu den Kursen, insbesondere zu freien Plätzen, sind unter *http://www.gwdg.de/kurse* zu finden.


GWDG
Gesellschaft für wissenschaftliche
Datenverarbeitung mbH Göttingen