MITTEILUNGSBLATT
DER
KARL-FRANZENS-UNIVERSITÄT GRAZ

www.uni-graz.at/zvwww/miblatt.html

15. SONDERNUMMER

.

Studienjahr 2007/08 | Ausgegeben am 7. 5. 2008 | 31.a Stück

Das Rektorat hat am 24. April 2008 folgende Richtlinie erlassen:

Security Policy für Computer und Netze

1. Präambel

Die Universität Graz möchte allen Benutzer/inne/n effizientes und ungestörtes Arbeiten ermöglichen. Daher ist in der Security Policy eine Liste von nicht zulässigen Verhaltensweisen (siehe Pkt. 5, regelwidrige Benutzung) festgelegt, deren Unterlassung jede/r Benutzer/in einfordern kann, um sich vor Belästigungen und Bedrohungen zu schützen und in Folge die Universität Graz und ihre Organisationseinheiten vor Schäden und rechtlichen Konsequenzen zu bewahren. Um den einwandfreien Betrieb zu gewährleisten, werden in der Security Policy der Universität Graz Standards für die Sicherheit von Computern, Netzen und Daten festgelegt.
Die Universität Graz erwartet von den Benutzer/inne/n der Computer und der Netze der Universität Graz verantwortungsbewussten Umgang bei deren Gebrauch. Als Reaktion auf Verstöße gegen die Security Policy oder gegen gesetzliche Bestimmungen sind die Universität Graz und ihre Organisationseinheiten berechtigt, Benutzer/inne/n Zugangsberechtigungen zu IT-Services zeitweise oder auf Dauer zu entziehen, bei Bedarf Daten von Computern der Universität Graz zu löschen und Computer bzw. Systeme aus dem Netz zu entfernen.

1.1. Sicherheitskultur

Absolute Sicherheit ist bei möglichst flexibler und offener Nutzung von IT-Infrastruktur und -Diensten nicht erreichbar. Vielmehr wird mit der Security Policy die höchstmögliche Sicherheitsstufe für die Universität unter Bedachtnahme auf Kosten, Funktionalität, Akzeptanz und juristische Anforderungen angestrebt. Dabei steht die Sicherstellung des IT- und Informationsangebotes in der aktuellen Kommunikationslandschaft im Internet an oberster Stelle.
Die Security Policy bietet die Möglichkeit zur Kommunikation zwischen IT-Fachkräften, den Manager/inne/n und Benutzer/inne/n an der Universität. Sie soll alle Unterstützung bieten, die für sicherheitsrelevante Entscheidungen nötig ist. Insbesondere soll das Verständnis für eine aktive Sicherheitsvorsorge gefördert werden. Da die IT-Sicherheit in den Köpfen beginnt, soll unter Einbeziehung aller Beteiligten durch gezielte Information über Sicherheitsprobleme, Angebote zur Weiterbildung und sonstige Maßnahmen (Merkblätter, Checklisten etc.) eine Kultur zur IT-Sicherheit nachhaltig gefördert werden.

1.2. Richtlinien für den sicheren Betrieb von Systemen und IT-Infrastrukturen im Universitätsnetzwerk

Der Gebrauch von Computern und Netzen ist für die Angehörigen der Universität Graz zur alltäglichen Routine geworden. Bei ordnungsgemäßer Benutzung erleichtern Computersysteme viele Tätigkeiten,

manche Arbeiten wären ohne ihren Einsatz gar nicht denkbar. Fahrlässige oder gar gesetzwidrige Verwendung hingegen kann die Rechte anderer Benutzer/innen verletzen. Die Universität Graz verlangt daher von allen Benutzer/inne/n sorgfältigen und verantwortungsvollen Umgang beim Gebrauch von Systemen und Netzen.
Grundsätzlich bleibt es dem Ermessen jeder/s einzelnen Benutzer/in/s bzw. der Institute und Universitätseinrichtungen der Universität Graz überlassen, in welcher Art und Weise Systeme und Netze verwendet werden, sofern dies nicht gesetzlichen Bestimmungen oder Regelungen der Universität widerspricht. Der über die Jahre praktizierte und bewährte Ansatz - es ist alles erlaubt, was nicht „verboten" ist - soll beibehalten werden. Dabei sind jedenfalls alle Gesetze, sowie die Satzung der Universität Graz, die Betriebsvereinbarungen, die Betriebs- und Benutzungsordnung des ZID (EDV- Ordnung), die Vorschriften des ZID zur Einbindung in das Universitätsnetz, sowie die Vorgaben der Security Policy und den daraus abgeleiteten Strategien, Verordnungen, Checklisten und Richtlinien einzuhalten.

1.3. Prozeduren und Vorgangsweise bei Sicherheitsproblemen

Zweck der Security Policy ist es, die Mindeststandards für den sicheren Betrieb eines Computer-Systems und Konsens darüber, wann eine regelwidrige Benutzung vorliegt, zu formalisieren und allen Benutzer/inne/n eine einheitliche Grundlage zu bieten, anhand derer entschieden werden kann, welche Benutzung konform ist.
Auf Grund einer gewünschten maximalen Offenheit kann Missbrauch a priori nicht ausgeschlossen werden. Durch die Security Policy soll das Erkennen von Sicherheitsproblemen beschleunigt werden, um den Schaden für jeden Einzelnen und die Universität Graz gering zu halten. Damit verringert sich auch die Wahrscheinlichkeit, dass Verstöße ohne Konsequenzen bleiben.

2. Gültigkeitsbereich

Die Security Policy ist verbindlich für alle Angehörigen der Universität Graz sowie für alle Personen, denen durch Vereinbarungen der Zugang zu und die Benutzung von Computern, Systemen und Netzen der Universität Graz möglich ist.
Die Security Policy dient der Datensicherheit und dem besonderen Schutz der Privatsphäre der Benutzer/innen von Computern und Netzwerken vor ungerechtfertigten Angriffen. Um dieses Ziel zu erreichen, werden einerseits jene Maßnahmen festgelegt, die von Benutzer/inne/n jedenfalls zu unterlassen sind (regelwidrige Benutzung) und andererseits jene Anforderungsprofile definiert, die beim Betrieb von Computern und Netzen jedenfalls gewährleistet sein müssen (Anforderungen für den Betrieb von Computern und Netzwerken).
Die Security Policy ist durch den Zentralen Informatikdienst alle 2 Jahre auf ihre Aktualität zu überprüfen. Schwerwiegende Veränderungen der verwendeten Technologien, organisatorischer Art oder die Veränderung der gesetzlichen Lage können eine Überarbeitung auch außerhalb dieses Intervalls bedingen.

3. Organisation

Zur Wahrnehmung der IT-Sicherheit an der Universität Graz sieht die Security Policy ein Zusammenwirken der Benutzer/innen, der in der IT-Administration operativ tätigen Personen und der zentralen Koordination vor, um die IT-Sicherheit zu fördern und sicherzustellen. In allen Einrichtungen der Universität Graz haben die jeweiligen Vorgesetzten auf die Einhaltung der einschlägigen Regelungen sowie der Security Policy zu achten. Die Universität Graz ist darauf angewiesen, dass die Benutzer/innen Mängel auf Institutsebene entweder selbst oder mit Unterstützung des ZID beheben. Vorfälle, welche die Sicherheit der System- und Netzinfrastruktur betreffen, sind ohne Verzug dem ZID zu melden. Die zentrale Koordination der notwendigen Maßnahmen ist dann Aufgabe der/s Security Manager/in/s im Zentralen Informatikdienst.

3.1. Security-Manager/in am ZID

Die/der Security Manager/in wird durch die ZID-Leitung besetzt und ist ihr direkt zugeordnet. Zu ihren/seinen Aufgaben gehören insbesondere:

- die Koordination der Aktivitäten zur Aufrechterhaltung der Sicherheit der Daten und der Systeme im Universitätsnetzwerk

- die Sicherstellung der Einhaltung der Security Policy
- die Untersuchung von Verstößen gegen die Security Policy

Sie/er entscheidet bei Unklarheiten oder Streitfällen in Angelegenheiten der IT-Sicherheit, in zweiter Instanz entscheidet die ZID-Leitung.
Die/der Security Manager/in hat für die regelmäßige Aktualisierung der Arbeit zugrunde liegenden Dokumente und Vereinbarungen zu sorgen, alle getroffenen Maßnahmen zu dokumentieren und über ihre/seine Tätigkeit in regelmäßigen Abständen einen Bericht an die ZID- Leitung zu erstellen. Sie/er hat den Netz- und Systemadministrator/innen die für die Wahrnehmung ihrer/seiner Aufgaben notwendigen sicherheitsrelevanten Informationen zu übermitteln.
Sie/er wird in ihrer/seiner Arbeit von den Abteilungen des ZID unterstützt, welche die vorliegenden Informationen sammeln und dokumentieren. Ihre/Seine Vertretung wird von der Leitung des ZID wahrgenommen.

3.2. Kompetenzen der Rektorin/des Rektors
In schwerwiegenden Problemfällen trifft die/der Rektor/in die Entscheidungen über die Vorgehensweise der Universität, insbesondere über

- Berufungen oder Beschwerden über Prozeduren und Vorgangsweisen bei Sicherheitsproblemen
- die Weitergabe von Informationen an die Polizei und andere Behörden
- Anzeige des Sachverhaltes an die zuständigen Behörden, wenn der dringende Verdacht besteht, dass durch die Verletzung der Security Policy auch eine in die Zuständigkeit dieser Behörden, insbesondere der Gerichtsbehörden, fallende strafbare Handlung gesetzt worden ist
- Einschaltung von weiteren Organen der Universität zur Durchführung disziplinärer Maßnahmen.

3.3. Netz- und Systemadministratoren
An allen Einrichtungen der Universität Graz, die Computersysteme und/oder Netze betreiben, sind verantwortliche System- bzw. Netzadministrator/inn/en zu benennen.
Systemadministrator/inn/en sind Personen, die autorisiert sind, festzulegen, wer Zugang zu Diensten, Systemen und Datenbeständen im oder in Verbindung mit dem Universitätsnetz hat.
Netzadministrator/inn/en sind Personen, die autorisiert sind, festzulegen, wer Zugang zu Netzwerken mit Verbindung zum Universitätsnetz hat. Aufgabe dieser Personen ist es, die Verantwortung für von ihnen verwaltete Datenbestände, Dienste und Systeme wahrzunehmen. Insbesondere sind sie befugt, bei regelwidriger Benutzung den Zugang zu verwehren und alle Maßnahmen zu setzen, die zur Aufrechterhaltung der Dienste notwendig sind.
Die Kenntnis dieser Netz- und Systemadministrator/inn/en ist wichtig, weil bei Attacken (z.B. Hacker) die schnelle Kontaktaufnahme unumgänglich ist. Außerdem können gewisse Services wie z.B. die Sicherheitsüberprüfung eines Computers nur auf Anfrage der/s Systemadministrator/in/s bzw. der/s Institutsleiter/in/s oder der/s Leiter/in/s einer Universitätseinrichtung geleistet werden.
Die Netz- und Systemadministrator/inn/en sind von der Leitung der jeweiligen Einrichtung an der Universität Graz für jeden Computer und jedes Netzwerk-Service im Netzwerk festzulegen und an den ZID zu melden. Die Funktion einer/s Netz- und Systemadministrator/in/s kann auch von der/m EDV-Beauftragten der Organisationseinheit wahrgenommen werden. Der ZID stellt eine Datenbank im Intranet zur Verfügung, über die Änderungen der Systemadministration bekannt gegeben und von Verantwortlichen in Störfällen aufgefunden werden können.

3.4. Informations- und Mitwirkungspflicht
Die Weitergabe von bekannten Informationen ist wesentlicher Bestandteil der gegenseitigen Unterstützung und Hilfestellung. Die nachfolgenden Punkte sollen aber nicht als eine Aufforderung zur generellen Sammlung und Beschaffung von Informationen missverstanden werden. Die Regelungen aus dem Datenschutzgesetz sind auch bei Verstößen uneingeschränkt gültig.
Falls einer/m Benutzer/in eines Computers Sicherheitsmängel auffallen, so ist sie/er verpflichtet, die/den Systemadministrator/in davon zu informieren und sie/ihn zur Behebung derselben aufzufordern.

Bei allen absichtlichen und grob fahrlässigen Verstößen muss von der/m System- oder Netzwerkverantwortlichen unverzüglich ein Protokoll angelegt werden. Die/der Security Manager/in am ZID ist über jeden der vorher genannten Verstöße zu informieren. Diese/r entscheidet über die weitere Vorgangsweise.
Bei schweren Verstößen bildet die/der Security Manager/in am ZID ein Team mit Personen aus den betroffenen Bereichen, das sich mit der Behebung des Störfalles beschäftigt. Alle in den Vorfall involvierten Personen sind zur uneingeschränkten Informationsweitergabe verpflichtet und können von der/vom Security Manager/in am ZID zu weiteren Tätigkeiten (z.B. Sicherstellung von Userdaten) autorisiert werden.

3.5. Sicherheitsmanagement

Für ein erfolgreiches Sicherheitsmanagement sind Systeme von Nöten, die an zentraler Stelle im Netzwerk der Universität Graz folgende spezielle Aufgaben erfüllen

- email Filter an der Grenze zum Internet zur Abwehr von Viren und SPAM
- Firewall Systeme an der Grenze zum Internet und an den Grenzen von Arbeitsbereichen (organisatorische Subeinheiten)
- Systeme für Intrusion Detection und Prevention an der Grenze zum Internet und zu Extranets
- Systeme zu Traffic Shaping zum zeitweiligen Einschränkung von Diensten des privaten Gebrauchs
- Systeme zur aktiven Überprüfung des Sicherheitszustandes der im Netzwerk der Universität Graz betriebenen Systemen

Die angeführten Systeme werden nach einer innerhalb der Universität abgestimmten Konfiguration vom Zentralen Informatikdienst betrieben.
Der ZID behält sich zur Sicherstellung eines einheitlichen Sicherheitsstandards das Recht vor, in Abstimmung mit den betroffenen Personen und Einrichtungen punktuelle und generelle Sicherheitsüberprüfungen (Audit) selbst durchzuführen oder Dritte damit zu beauftragen.

4. Anforderungen für den Betrieb von Computern oder Netzwerken

Einrichtungen und Angehörige der Universität Graz können in begründeten Fällen für ihre jeweiligen Aufgabenbereiche Services und Computersysteme im Netz der Universität Graz anbieten.
Bei nicht entsprechender Wartung kann ein Computer den Betrieb von Teilen der IT- Infrastruktur der Universität Graz gefährden (z.B. Hacker, Spam-Mail, Viren).
Um den ordnungsgemäßen Betrieb eines Computers oder einer aktiven Netzkomponente zu gewährleisten, sind die dem Stand der Technik entsprechenden Vorkehrungen zu treffen. Dazu werden von der/dem Security Manager/in Strategien entwickelt und in entsprechenden Richtlinien veröffentlicht. Darunter fallen insbesondere:

- Softwareinstallation und Wartung
- System- oder Netzwerkadministration
- Zugang und Authentifizierung
- Datensicherheit und Backup
- Email- und Webdienste (nur im Einklang mit der IT- Architektur)

Darüber hinaus können vom Netzbetreiber an ausgewählten Netzübergabepunkten Sperren (Firewall, Access Lists, ...) errichtet werden, um die Betriebssicherheit in speziellen Netzbereichen oder im Gesamtnetz der Universität Graz zu erhöhen.

5. Regelwidrige Benutzung

Eine regelwidrige Benutzung von Computersystemen, Diensten und Netzen liegt dann vor, wenn die einschlägigen gesetzlichen Bestimmungen oder Regelungen der Universität Graz nicht eingehalten werden.

Unzulässige Verwendungen sind insbesondere:

1. eine Verwendung, wenn sie andere Benutzer/innen in ihrer Arbeit behindert oder wenn es das gute Funktionieren der Dienste der Netze unserer Universität oder der angeschlossenen Netze stört, sowie
2. eine Verwendung im Sinne von Cyberkriminalität, Erstellung von Kopien von urheberrechtlich geschützten Inhalten (Raubkopien) und deren Verwendung, Datenmissbrauch und Missbrauch von Geschäfts- und Betriebsgeheimnissen, insbesondere der Weitergabe von Identitäten (z.B. Passwort), die den folgende gesetzliche Bestimmungen widerspricht:

[UrhG]	Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte, StF: BGBl. Nr. 111/1936 i.d.F. BGBl I Nr. 32/2003, 22/2006 und 81/2006
[TKG]	Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird - BGBl I Nr. 70/2003, idF BGBl I Nr. 178/2004 und BGBl I 133/2005 (ab 1.3.2006)
[DSG]	Bundesgesetz über den Schutz personenbezogener Daten - DSG 2000 StF: BGBl. I Nr. 165/1999, idF: BGBl. I Nr. 136/2001 und BGBl I 13/2005
[VbVG]	Bundesgesetz über die Verantwortlichkeit von Verbänden für Straftaten, BGBl I 151/2005
[StGB]	Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch - StGB) StF: BGBl. Nr. 60/1974 i.d.F. BGBl. I Nr.15/2004, 136/2004, 152/2004, 68/2005 und 56/2006
[UWG]	Bundesgesetz gegen den unlauteren Wettbewerb 1984 - UWG, BGBl. Nr. 448/1984 (WV) idF BGBl. I Nr. 136/2001, 106/2006

Die angeführten Gesetzestexte können auch online über das Rechtsinformationssystem des Bundes unter folgender URL abgerufen werden: http://www.ris.bka.gv.at oder zusammengefasst unter http://www.internet4jurists.at/gesetze/gesetze.htm.

5.1. Angriffe auf Computer, Netzwerke und Services

Alle Angriffe auf Computer, Netzwerke und Services gelten als regelwidrige Benutzung und sind daher zu unterlassen. Dazu gehören insbesondere:

Portscans	automatisiertes Ausforschen von Servern und Services (Ausnahme: Sicherheitstests nach Absprache mit der/dem Systemadministrator/in)
Hacken	Unerlaubte Aneignung von Ressourcen oder der Versuch einer solchen Aneignung (Ausnahme: Sicherheitstests nach Absprache mit der/dem Systemadministrator/in)
Denial of Service Attacken	Beschädigung oder Störung von elektronischen Diensten
Viren	Verbreitung oder In-Umlauf-Bringen von Virenprogrammen, Computer-Würmern, Trojanischen Pferden oder anderen schädlichen Programmen
Passwort Sniffer	Ausspähen von Passwörtern oder auch der Versuch des Ausspähens, z.B. Passwort Sniffer, Netzwerksniffer etc.
Netzwerksniffer	Ausspähen von Informationen zu Netzwerken und Diensten oder auch der Versuch des Ausspähens
Spoofing	Manipulation oder Fälschung von Mail- oder Newsheadern, elektronischer Verzeichnisse oder anderer elektronischer Information, insbesondere Vorgabe einer falschen Identität wie IP-Spoofing etc. (Ausnahme: IP-Umsetzung durch gemeldete Masquerading Firewalls)
Exploiting	Ausnützung von erkannten Sicherheitsmängeln bzw. administrativen Mängeln

5.2. Fahrlässige Gefährdung der Sicherheit

Im Sinne der Security Policy ist auch die fahrlässige Gefährdung der IT-Sicherheit als regelwidriges Verhalten anzusehen. Diese besteht insbesondere in der Verwendung unsicherer Passwörter und oder unsicherer Software oder dem Betrieb unsicherer IT- Systeme.

5.3. Physische Verstöße

Jegliche unautorisierte Manipulation an IT-Einrichtungen der Universität Graz ist zu unterlassen. Dazu zählen insbesondere:

- Veränderungen am Netzwerk und seinen Komponenten
- nicht autorisierter Aufenthalt in Räumen mit Zutrittskontrolle
- Diebstahl von IT-Komponenten und Installation und Betrieb von unautorisierten Computersystemen (Bots) im Universitätsnetzwerk, was die unmittelbare Einschaltung der Polizei durch die/den Security Manager/in am ZID zur Folge hat
- Sachbeschädigung

6. Folgen bei Nichteinhaltung der Security Policy

Erfahrungsgemäß geschehen die meisten Verstöße gegen die Security Policy unwissentlich oder fahrlässig und ohne nachweisbare böse Absichten. Daher können Aufklärung und Ermahnungen den Schwerpunkt der hier aufgelisteten Aktivitäten bilden:

- Vorbereitung der möglichen Anzeige bei Gesetzesverletzungen
- Hinweis auf die Netiquette
- Aufklärung bei Unkenntnis der Security Policy oder technischer Unzulänglichkeit
- Einfordern der schriftlichen Zurkenntnisnahme der Security Policy und der daraus abgeleiteten Richtlinien durch die/den Verursacher/in
- Bei Verstößen gegen die Netiquette oder gegen Lizenzvereinbarungen muss gegebenenfalls die Löschung von Daten auf Servern verlangt werden.

Falls eine direkte Aufforderung ohne Erfolg bleibt, können durch die/der Security Manager/in am ZID folgende Maßnahmen (Eskalation) ergriffen werden:

- Aufforderung an die/den Netz- und Systemadministrator/in zur Unterbindung der Regelverstöße mit bindender Zeitvorgabe
- Aufforderung an die/den EDV- Beauftragte/n und an den Institutsvorstand bzw. die/den Leiter/in der Universitätseinrichtung
- Sperren von Zugängen zu Systemen und Netzen: bei Gefahr im Verzug oder im Wiederholungsfall unmittelbar nach Information der Betroffenen

Wenn anzunehmen ist, dass erkannte Verstöße auch andere Institute, Universitätseinrichtungen, Organisationen (auch außerhalb der Universität Graz) oder die gesamte Universität betreffen, hat der Netzbetreiber alle Maßnahmen zu setzen, um möglichst rasch einen reibungslosen Betrieb wieder herzustellen.
Einrichtungen, die die Mindeststandards für einen sicheren Betrieb nicht einhalten, können vom Netzbetreiber vom Netzzugang ausgeschlossen werden. Nach der Wiederherstellung der Netz- und Systemsicherheit kann die/der Security Manager/in am ZID den dokumentierten Vorfall abschließen:

- Entsperren von Zugangsberechtigungen zu Systemen und Netzen erfolgen nach Wiederherstellung der Mindestanforderungen für den sicheren Betrieb von Systemen und IT- Infrastrukturen im Universitätsnetzwerk und nach unmittelbarer Information an die/den Betroffene/n

7. Definitionen

aktive Netzwerkkomponente	Router, Switch, Firewall, Wireless LAN Access Point etc.
Backup	Kopie von Daten, besonders hilfreich bei technischen Defekten in Verbindung mit Datenverlust
Benutzer/in	Endbenutzer/in
Bot	Computersystem, das maliziöse Aufgaben automatisiert ausführt
elektronische Kommunikation	Verwendung von Computern, Netzen (Universitätsnetz, Telefon etc.) und deren Services
IDS/IPS	Einbruchserkennungs- und Einbruchsverhinderungssysteme
Masquerading Firewall	Aktive Netzkomponente die öffentliche auf private Adressen abbildet und v.v.
Netiquette	Etikette im Netzwerk
Netze	alle Kommunikationsnetze (z.B. Universitätsnetz, Telefonnetz, Novell/Microsoft-Netzwerk)
Netzadministrator/in	Personen mit der Autorität festzulegen, wer Zugang zu Netzwerken mit Verbindung zum Universitätsnetz hat
Service	Jedes Service, das von einem Dienstleister zur Verfügung gestellt oder weitergeleitet wird
Systemadministrator/in	Personen mit der Autorität festzulegen, wer Zugang zu Diensten, Systemen und Datenbeständen im oder in Verbindung mit dem Universitätsnetz hat
Traffic shaping	Servicebezogene Regelung der Netzwerkbandbreite
Universitätsnetz	Netz-, Kommunikations- und Rechnerinfrastruktur für die Informations- und Datenverarbeitung an der Karl-Franzens-Universität Graz
Verwendung	Verwendung eines von einer Dienstleistungseinrichtung zur Verfügung gestellten Services sowie der Kommunikationseinrichtungen (z.B. Leitungen, Geräte) der Dienstleistungseinrichtungen (egal ob betrieben, gemietet oder deren Eigentum), der von Dienstleistungseinrichtungen betriebenen oder gewarteten Software und aller Informationen, die verfügbar gemacht werden
ZID	Zentraler Informatikdienst, IT Services

Der Rektor:
Gutschelhofer

Kontakt bzw. Autoren: Dr. Günther Berthold, Heinrich Grillhofer, Karl-Franzens-Universität Graz, Zentraler Informatikdienst, Universitätsstraße 15/G, A-8010 Graz, Telefon: +43 316 380 2230, Fax: +43 316 380 9180, email: zid@uni-graz.at , url: http://www.uni-graz.at/zid

Impressum: Medieninhaber, Herausgeber und Hersteller: Karl-Franzens-Universität Graz, Universitätsplatz 3, 8010 Graz. Verlags- und Herstellungsort: Graz.
Anschrift der Redaktion: Administration und Dienstleistungen, Universitätsplatz 3, 8010 Graz.
E-Mail: mitteilungsblatt@uni-graz.at