stiftung secure information and communication

Jahresbericht 2009

Zusammenfassender Bericht über die Aktivitäten der
Stiftung Secure Information and Communication Technologies SIC

Die *Stiftung Secure Information and Communication Technologies SIC* wurde vom Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK) der Technischen Universität Graz (TU Graz) als gemeinnützige Stiftung gegründet und mit Bescheid der Stiftungsbehörde vom 5. Februar 2003 für zulässig erklärt. In diesem Jahresbericht wird über die Aktivitäten der Stiftung im Geschäftsjahr 2009 berichtet.

Inhaltsverzeichnis

Inhaltsverzeichnis 1
Executive Summary 2
1 Einleitung 3
1.1 Stiftungszweck 3
1.2 Forschungsschwerpunkte 3
1.3 Zur Lage der Stiftung 4
1.4 Hilfsbetrieb JCE Toolkit 4
1.5 Stiftungsorgane und Organisationsstruktur 5
2 Leistungen im Sinne des Stiftungszwecks 7
2.1 Förderung von Forschung und Lehre, Wissenstransfer 7
2.1.1 Stiftungsprofessur Informationssicherheit 7
2.1.2 Best Project Award 9
2.1.3 Vorlesung Kritische Informationsinfrastrukturen 9
2.1.4 E-Government 9
2.2 Organisatorisches und Sonstiges 9
2.2.1 Technische Infrastruktur 9
2.2.2 Entwicklungsaktivitäten JCE Toolkit 10

Auskünfte

Stiftung Secure Information and Communication Technologies SIC
Inffeldgasse 16a
8010 Graz
Tel.: (0316) 873-5513 / 5521 Fax.: (0316) 873-5520

Impressum

Medieninhaber, Herausgeber und Verleger
Stiftung Secure Information and Communication Technologies SIC, Inffeldgasse 16a, 8010 Graz

Redaktion und für den Inhalt verantwortlich
Dipl.-Ing. Herbert Leitold, Dr. Peter Lipp *(Vorstand der Stiftung)* Graz, am 28. April 2010

Executive Summary

Die **Stiftung Secure Information and Communication Technologies SIC** wurde im Februar 2003 gegründet und mit einem Stammvermögen von € 2.320.000 ausgestattet. Der Zweck der Stiftung ist „*die Förderung und eigenständige Durchführung von wissenschaftlicher Forschung und Entwicklung sowie der Lehre und des Wissenstransfers in den Bereichen Angewandte Informationsverarbeitung und Kommunikationstechnologie sowie Informationssicherheit*". Satzungsgemäß kann dies durch „*... Vergabe von Forschungsaufträgen, die Vergabe von Beiträgen für wissenschaftliche Arbeiten, sowie Zuwendungen an Personen oder Institutionen ...*" erfolgen.

Dieser Jahresbericht 2009 stellt die Leistungen der Stiftung nach dem Stiftungszweck im Zeitraum 1.1. – 31.12.2009 dar. Der Bericht behält die Struktur der bisherigen Berichte.

Im Berichtszeitraum konnte die Stiftung in allen Bereichen des Stiftungszwecks wertvolle Beiträge leisten:

- Die „*Stiftungsprofessur Informationssicherheit*", die von der Stiftung SIC 2004 initiiert wurde und seit 2006 als permanente Professur besteht, wurde 2009 weiter getragen (Gesamtkosten bis September, ab dann zu 50%).
- Vier Studenten wurden mit einem Best Project Award ausgezeichnet. Zwei weiteren Studenten, die in einem internationalen Wettbewerb den zweiten Platz belegten, wurden Sonderpreise verliehen.
- Aus dem Bereich Lehre wurde die Lehrveranstaltung „*Kritische Informations-infrastrukturen*" an der TU Graz weiterhin finanziert.
- Aus dem Hilfsbetrieb JCE Toolkit konnten wiederum Gewinne erzielt werden, die dem gemeinnützigen Forschungsbereich zufließen.

1 Einleitung

Die „*Stiftung Secure Information and Communication Technologies SIC*“ – in diesem Bericht in Folge als „*die Stiftung*“ bezeichnet – wurde vom Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK) der Technischen Universität Graz (TU Graz) im Jahr 2003 gegründet. Rechtliche Grundlage ist das *Steiermärkische Stiftungs- und Fondsgesetz, LGBl. Nr. 69/1988* – in Folge als *StSFG* abgekürzt. Mit Bescheid der Stiftungsbehörde vom 5. Februar 2003 wurde die Stiftung für zulässig erklärt. In diesem Jahresbericht wird die Tätigkeit der Stiftung im Jahr 2009 dargestellt. Es stellt dies auch den Bericht über die im Sinne des Stiftungszwecks erbrachten Leistungen gemäß StSFG § 14 (3) dar (Abschnitt 2 „Leistungen im Sinne des Stiftungszwecks“). In den Anhängen sind die weiteren nach StSFG § 14 (3) definierten Berichte an die Aufsichtsbehörde angefügt.

Entsprechend einem Beschluss des Kuratoriums vom 28. April 2010 ist dieser Bericht im Internet zu veröffentlichen (ohne Finanzdaten, Bilanz und Rechnungsabschluss).

In diesem einleitenden Abschnitt werden die Grundlagen der Stiftung zusammengefasst.

1.1 Stiftungszweck

Der gemeinnützige Stiftungszweck ist in Artikel III. der Satzung wie folgt definiert:

> *Zweck der Stiftung ist die Förderung und eigenständige Durchführung von wissenschaftlicher Forschung und Entwicklung sowie der Lehre und des Wissenstransfers in den Bereichen Angewandte Informationsverarbeitung und Kommunikationstechnologie sowie Informationssicherheit durch Vergabe von Forschungsaufträgen, die Vergabe von Beiträgen für wissenschaftliche Arbeiten, sowie Zuwendungen an Personen oder Institutionen, die zur Erreichung des Stiftungszweckes beitragen. Diese stellen den begünstigten Personenkreis gemäß § 10 Abs. 2 Z 3 des Steiermärkischen Stiftungs- und Fondsgesetzes dar.*
>
> *Die Leistungen der Stiftung erfolgen aus den Erträgnissen des Stiftungsvermögens bzw. aus dem Stiftungsvermögen selbst. Sämtliche Leistungen der Stiftung sind freiwillig und begründen keinen Rechtsanspruch gegen die Stiftung. Über die Gewährung von Leistungen der Stiftung entscheiden die Organe der Stiftung.*

Die gesamte Satzung ist in der Willbriefsammlung des Steiermärkischen Landesarchivs unter LReg. Vertrag Nr. 5509 hinterlegt bzw. auch im Internet unter der Adresse http://sic.iaik.tugraz.at/sic/about_us/stiftung/satzung veröffentlicht.

1.2 Forschungsschwerpunkte

Die allgemeine Formulierung des Stiftungszwecks soll dem in der Informations-verarbeitung, der Kommunikationstechnologie und der Informationssicherheit immens schnelllebigen technologischen Fortschritt begegnen, wo einzelne Forschungsgebiete sich laufend wandeln, jedoch in der auf Dauer eingerichteten Stiftung auf lange Sicht ein entsprechend vitales Betätigungsfeld anzunehmen ist.

Um die Leistungen der Stiftung dennoch der aktuellen technologischen und wissen-schaftlichen Situation angepasst gestalten zu können, wurden Schwerpunkte definiert.

Als aktuelle Forschungsschwerpunkte sind festgelegt:

- Sicherheitsaspekte der Informationsgesellschaft, insbesondere E-Commerce und E-Government
- Kryptographie und Kryptoanalyse
- Hardware- und Software-Umsetzung kryptographischer Verfahren
- Public Key Infrastrukturen und elektronische Signaturen
- Netzwerksicherheit
- Radio Frequency Identification - RFID
- Beiträge zur Standardisierung in obgenannten Bereichen

Diese Forschungsschwerpunkte schließen andere, im Rahmen des Stiftungszwecks rechtfertigbare Leistungen nicht aus, sondern geben eine grobe Richtlinie zu besonders förderungswürdigen Themen. Die Schwerpunkte sollen auch laufend an aktuelle Gegebenheiten angepasst werden.

1.3 Zur Lage der Stiftung

Seit Bestehen der Stiftung wurde über Forschungsförderungen, Zuwendungen, Kooperationen und Gewinne des Hilfsbetriebs Toolkit ein Vermögensstand aufgebaut, der über das gewidmete Stammkapital hinausgeht. Die in den Jahren 2008 und 2009 erfahrene Finanzkrise hat dies durch die auf Werterhalt und geringes Risiko ausgerichtete Veranlagung nicht geändert. Im Gegenteil konnten die Leistungen uneingeschränkt beibehalten werden. Durch die Rücklagen ist in absehbarer Zukunft auch mit keiner Änderung dieser Situation zu rechnen, sodass für Leistungen weiterhin nicht auf das Stammvermögen zurückgegriffen werden wird müssen.

Die gemeinnützigen Leistungen kamen im Berichtszeitraum 2009 über die Stiftungsprofessur Kryptographie (seit Oktober 2008 in Teilfinanzierung), die Lehrveranstaltung kritische Informationsinfrastrukturen, sowie Best Project Awards vor allem Studierenden der Technischen Universität Graz zugute und stärken damit Ausbildung im Wirkungsbereich der Stiftung. Aus der Stiftungsprofessur wurden wieder exzellente, international beachtete Forschungsleistungen in der Steiermark unterstützt.

Der Hilfsbetrieb „*JCE Toolkit*“ konnte einen Gewinn erwirtschaften, der gänzlich dem gemeinnützigen Stiftungszweck zufließt. Der Personalstand in der Stiftung wurde etwas erhöht.

Es bestehen also Reserven, um die Leistungen auf hohem Niveau zu halten.

1.4 Hilfsbetrieb JCE Toolkit

Mit Übertragung des „*JCE Toolkit*“ durch das IAIK Ende 2003 besteht ein Hilfsbetrieb, über den die Stiftung Zuflüsse über die Erträgnisse aus dem pekuniären Stammvermögen bzw. aus der Veranlagung der Rücklagen hinausgehend erzielen kann.

Mit Bescheid der Finanzlandesdirektion aus 2003 wurde festgestellt, dass der Vertrieb des JCE Toolkit keine Begünstigung auf abgaberechtlichem Gebiet zukommt, jedoch die Begünstigung in den gemeinnützigen Bereichen weiterhin erhalten bleibt. Es wurde hier die Auflage erteilt, die Gewinne aus der kommerziellen Verwertung den gemeinnützigen Aktivitäten zuzuführen. Diese auch im Übertragungsvertrag des IAIK gegebene Maßgabe ist seit 2004 in der Satzung verankert.

Die Abgrenzung zwischen gemeinnützigem und gewerblichem Bereich erfolgt über getrennte Kostenrechnung der Bereiche „Forschung“ (gemeinnützige Aktivitäten), „Toolkit“ (gewerblicher Hilfsbetrieb) und „Overheads“ (Gemeinkosten, die anteilig den Bereichen Toolkit und Forschung zugeordnet werden).

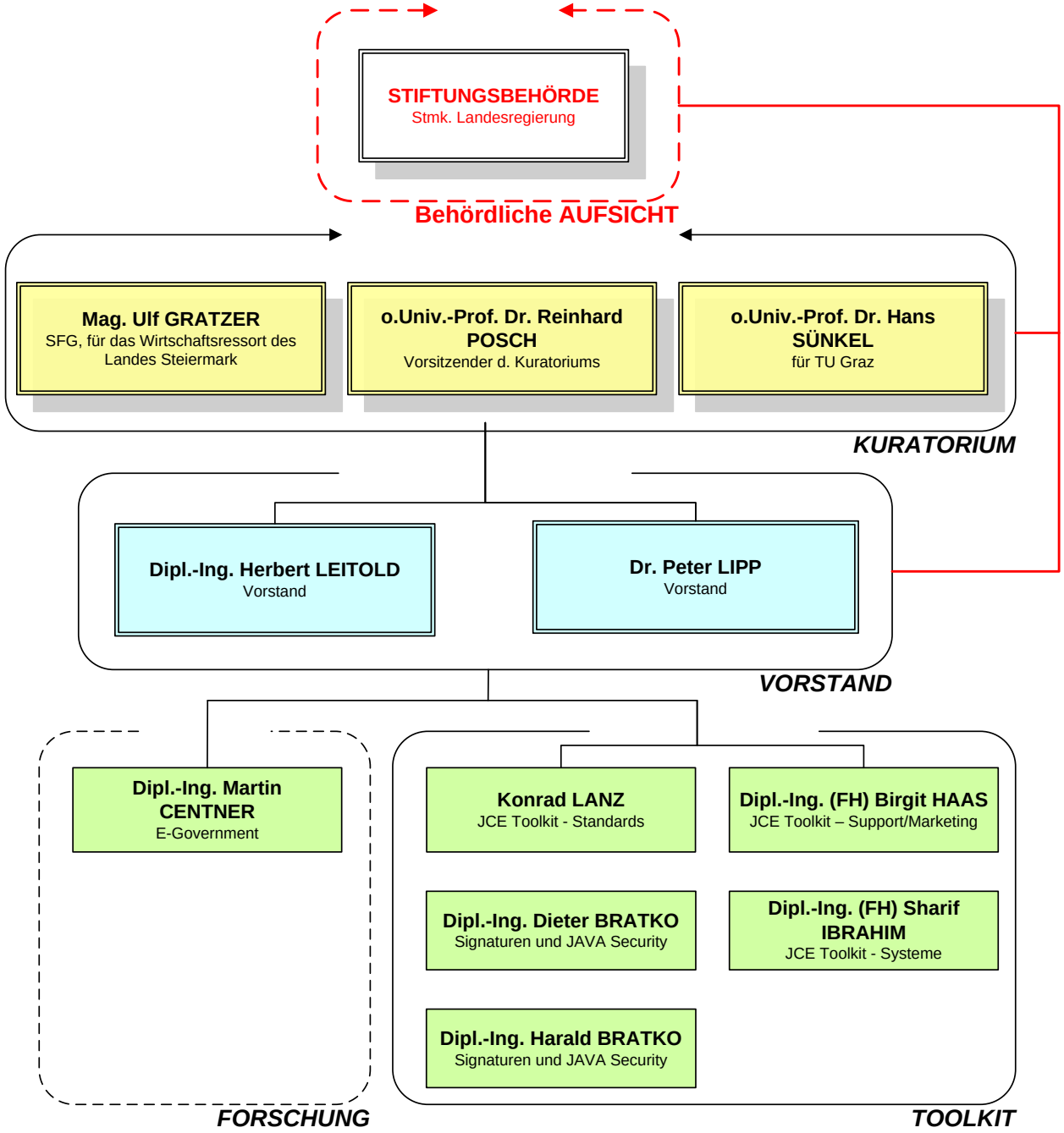
1.5 Stiftungsorgane und Organisationsstruktur

Die Organisationsstruktur der Stiftung teilt sich in drei Ebenen:

- Die Kontrollebene wird durch das Kuratorium und die staatliche Aufsicht gebildet.
  - Das Kuratorium besteht aus drei Personen. Im Geschäftsjahr 2009 waren dies:
    - Mag. Ulf Gratzer (für das Wirtschaftsressort des Landes Steiermark)
    - o.Univ.-Prof. Dr. Reinhard Posch (Vorsitzender des Kuratoriums)
    - o.Univ.-Prof. Dr. Hans Sünkel (für die TU Graz)
  - Staatliche Aufsicht ist die Stiftungsbehörde FA7C der Steiermärkischen Landesregierung
- Die Führungsebene bildet der Vorstand
  - Dipl.-Ing. Herbert Leitold
  - Dr. Peter Lipp
- Die operative Ebene wird durch zwei Säulen gebildet:
  - Der Bereich *Forschung* umfasst die mit eigenständiger Durchführung von Forschung und Entwicklung befassten MitarbeiterInnen der Stiftung.
  - Der Bereich *Toolkit* ist als Hilfsbetrieb vom gemeinnützigen Bereich *Forschung* abgegrenzt, unterstützt diesen jedoch über Gewinne und in der nicht-kommerziellen Forschung kostenlos verwendbare Werkzeuge.

Diese Struktur ist im folgenden Organigramm dargestellt. Dabei wird der Stand an Mitarbeiterinnen und Mitarbeitern der Stiftung per 31.12.2009 dargestellt. Administration und

technische Infrastruktur wird gegen Kostenersatz vom IAIK der TU Graz gestellt.



Organigramm und Personalstand per 31.12.2009

2 Leistungen im Sinne des Stiftungszwecks

Über die Leistungen der Stiftung wird dem in der Satzung der Stiftung definierten *Stiftungszweck* entsprechend in „*Förderung von Forschung und Lehre*“ berichtet.

2.1 Förderung von Forschung und Lehre, Wissenstransfer

2.1.1 Stiftungsprofessur Informationssicherheit

Seit 1.10.2004 ist die Stiftungsprofessur Informationssicherheit mit Prof. Dr. Vincent Rijmen besetzt. Dabei finanziert die Stiftung die Personalkosten von Prof. Rijmen, die TU Graz stattet die Stiftungsprofessur mit Räumlichkeiten, Assistenten und Sekretariat aus.

Seit 2006 ist die Professur an der TU Graz permanent eingerichtet. Die Stiftung hat eine Finanzierungszusage bis September 2009 bzw. eine Teil-Finanzierungszusage bis 2012 gegeben.

Seit Oktober 2008 ist die Stiftungsprofessur an der TU Graz nur mehr zu 30 % besetzt, die Initiative besteht jedoch weiter und 2009 konnte die Gruppe zahlreiche wissenschaftliche Schriften veröffentlichen oder war Co-Autor von wissenschaftlichen Publikationen:

Es wurde eine Dissertation abgeschlossen:

1. Christian Rechberger - "Cryptanalysis of Hash Functions"

Prof. Rijmen war Autor bzw. Co-Autor von zwei Büchern:

1. Stefan Dodunekov, Svetla Nikova, Bart Preneel, Vincent Rijmen - "Enhancing cryptographic primitives with techniques from error correcting codes" (IOS Press Amsterdam - ISBN: 978-1-60750-002-5)

2. Vincent Rijmen - "Selected Areas in Cryptography (SAC 2009)" (Springer - ISBN: 978-3-642-05443-3)

Es wurden fünf Artikel in wissenschaftlichen Journalen veröffentlicht:

1. Vincent Rijmen, Justin Troutman - "Green cryptography: cleaner engineering through recycling, Part 2" - IEEE security & privacy buildings confidence in a networked world (Volume: 7 5)

2. Joan Daemen, Vincent Rijmen - "New criteria for linear maps in AES-like ciphers" - Cryptography and communications discrete structures, boolean functions and sequences (Volume: 1)

3. Vincent Rijmen, Justin Troutman - "Green cryptography: cleaner engineering through recycling" - IEEE security & privacy buildings confidence in a networked world (Volume: 7 4)

4. Joan Daemen, Mario Lamberger, Norbert Pramstaller, Vincent Rijmen, Frederik Vercauteren - "Computational aspects of the expected differential probability of 4-round AES and AES-like ciphers" - Computing archives for informatics and numerical computation (Volume: 85 1-2)

5. Tomislav Nad, Mario Lamberger, Vincent Rijmen - "Numerical solvers and cryptanalysis" - Journal of mathematical cryptology (Volume: 3 3)

Weiters wurden elf Artikel in Tagungsbänden wissenschaftlicher Konferenzen veröffentlicht.

1. Florian Mendel, Martin Schläffer - "On Free-Start Collisions and Collisions for TIB3" - Information Security

1. Florian Mendel, Tomislav Nad, Martin Schläffer - "Collision Attack on Boole" - Applied Cryptography and Network Security

2. Florian Mendel, Christian Rechberger, Martin Schläffer, Søren Steffen Thomsen - "The Rebound Attack: Cryptanalysis of Reduced Whirlpool and Grøstl" - Fast Software Encryption

3. Lars R. Knudsen, Florian Mendel, Christian Rechberger, Søren Steffen Thomsen - "Cryptanalysis of MDC-2" - Advances in Cryptology - EUROCRYPT 2009

4. Mario Lamberger, Florian Mendel - "Structural Attacks on Two SHA-3 Candidates: Blender-n and DCH-n" - Information Security

5. Florian Mendel, Christian Rechberger, Martin Schläffer - "MD5 is Weaker than Weak: Attacks on Concatenated Combiners" - Advances in Cryptology - ASIACRYPT 2009

6. Mario Lamberger, Florian Mendel, Christian Rechberger, Vincent Rijmen, Martin Schläffer - "Rebound Distinguishers: Results on the Full Whirlpool Compression Function" - Advances in Cryptology - ASIACRYPT 2009

7. Florian Mendel, Christian Rechberger, Martin Schläffer - "Cryptanalysis of Twister" - Applied Cryptography and Network Security

8. Christian Rechberger - "Wie lange halten die SHA-2 Hashfunktionen kryptanalytischen Angriffen noch stand?" - Tagungsband 11. Deutscher IT-Sicherheitskongress (Note: to appear)

9. Florian Mendel - "Two Passes of Tiger are not One-Way" - Progress in Cryptology - AFRICACRYPT 2009

10. Florian Mendel, Tomislav Nad - "A Distinguisher for the Compression Function of SIMD-512" - Progress in Cryptology - INDOCRYPT 2009

11. Florian Mendel, Thomas Peyrin, Christian Rechberger, Martin Schläffer - "Improved Cryptanalysis of the Reduced Grøstl Compression Function, ECHO Permutation and AES Block Cipher" - Selected Areas in Cryptography

In der Lehre wurden von der Gruppe unter anderem die Vorlesungen „Angewandte Kryptographie“ und „Angewandte Kryptographie 2“, „Einführung in die Informations-sicherheit“ „Cryptanalysis of symmetric cryptographic primitives (PV)“ und „IT-Sicherheit“ betreut. Das Angebot wird mit Seminaren, Projekten und Diplomarbeiten ergänzt.

Die von der Stiftung finanzierte Professur ist also als Nukleus erstklassischer Forschung im Bereich der Kryptographie anzusehen. Es hat sich daraus eine Gruppe an Forschern in der Steiermark etabliert, die mittlerweile internationales Ansehen genießt.

2.1.2 Best Project Award

Bereits 2008 wurde ein Best Project Award ausgeschrieben. Dieser wurde 2009 an vier Bakkalaureats-Studierende der TU Graz vergeben:

1. Christoph Nagl für seine Arbeit „Elliptic Curve Cryptography on the IAIK DemoTag - An Implementation of ECSchnorr“

2. Christian Pendl für seine Arbeit „Implementation of the ISO/IEC 18888-6B Standard on a Semi-Passive RFID-Tag Prototype“

3. Günther A. Roland für seine Arbeit „Efficient Implementation of the Grøstl-256 Hash Function on an ATmega163 Microcontroller“ und

4. Michael Schwarz für seine Arbeit „Word Sense Disambiguation“

Zusätzlich wurde Paul Rouschal und Erich Wenger ein Anerkennungspreis dafür verliehen, dass sie am internationalen Design Contest der *7th ACM-IEEE International Conference on Formal Methods and Models for Codesign MEMOCODE 2009* den zweiten Platz erzielt haben.

2.1.3 Vorlesung Kritische Informationsinfrastrukturen

Die Vorlesung zu kritischen Informationsinfrastrukturen an der TU Graz wurde von der Stiftung zum dritten Mal finanziert. Die Vorlesung wurde wieder von Dr. Otto Hellwig gehalten.

2.1.4 E-Government

Mitarbeiter des Bereichs Forschung der Stiftung unterstützen das E-Government Innovationszentrum (EGIZ). EGIZ ist eine Initiative des Bundeskanzleramts und der TU Graz zur wissenschaftlichen Weiterentwicklung des E-Government in Österreich. Experten der Stiftung werden zu Projekten beigezogen.

2.2 Organisatorisches und Sonstiges

In diesem Abschnitt werden Aktivitäten berichtet, die zwar nicht in ursächlichem Zusammenhang mit dem gemeinnützigen Stiftungszweck stehen, jedoch als Hilfsbetrieb den gemeinnützigen Bereich fördern, oder als administrative und organisatorische Infrastruktur erforderlich sind, um die Stiftungsaktivitäten effizient durchzuführen.

2.2.1 Technische Infrastruktur

Die technische Infrastruktur der Stiftung wurde weiterhin vor allem vom IAIK der TU Graz getragen. Darüber hinausgehend wurde keine Infrastruktur angeschafft, da hier die qualitativ hochwertigen Ressourcen des IAIK die Anschaffung eigener teurer Anlagen nicht rechtfertigt. Die Nutzung der Infrastruktur wird an das IAIK abgegolten.

2.2.2 Entwicklungsaktivitäten JCE Toolkit

Die Umsatzerlöse aus dem Verkauf des JCE Toolkits im Hilfsbetrieb waren 2009 den Erwartungen entsprechend, Es wurden wiederum Entwicklungen teilweise von eigenem Personal der Stiftung, teilweise durch Forscher des IAIK übernommen. Durch die Erweiterung des Personalstands in der Stiftung selbst wurde dies in geringerem Ausmaß als in Vorjahren bezogen.