stiftung secure information and communication

Jahresbericht 2005

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 als gemeinnützige Stiftung gegründet und mit Bescheid der Stiftungsbehörde vom 5. Februar 2003 für zulässig erklärt. In diesem Jahresbericht werden die Aktivitäten der Stiftung im Geschäftsjahr 2005 berichtet.

Inhaltsverzeichnis

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 07. Mai 2006

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 2005 stellt die Leistungen der Stiftung nach dem Stiftungszweck im Zeitraum 1.1.2005 – 31.12.2005 dar. In diesem Zeitraum konnte die Stiftung in allen Bereichen des Stiftungszwecks entscheidende Beiträge leisten:

- In der Förderung von Forschung und Lehre ist ein wesentlichstes Element die „*Stiftungsprofessur Informationssicherheit*“ an der TU Graz. Hier wird die Stelle von Prof. Dr. Vincent Rijmen von der Stiftung SIC finanziert.

- Im Berichtszeitraum ist es gelungen, unter dem Titel „*Programme for Advanced Contactless Technology*“ (PROACT) eine Initiative mit der Firma Philips zu starten. Es werden dabei von Philips Aktivitäten im Bereich Radio Frequency Identification (RFID) gefördert. Die Stiftung SIC wird die Mittel zur Förderung von Forschungs- und Ausbildungsmaßnahmen an der TU Graz verwenden.

- Darüber hinaus hat sich die Stiftung SIC zusammen mit der TU Graz an einer Ausschreibung des Landes Steiermark zu Wissenstransfer und Koordination im Bereich E-Government beworben. Der Zuschlag dieses Angebots erfolgte Anfang 2006.

- Zur Förderung der Studierenden in Bereichen des Stiftungszwecks wurde zum dritten Mal ein Best Student Paper Award zur Informationssicherheit ausgeschrieben und der Gewinner zur Teilnahme an einer wissenschaftlichen Konferenz in den USA eingeladen. Dies soll die intensive Beschäftigung mit dem Thema Informationssicherheit anregen.

- Das von der EU geförderte Projekt POSITIF, an dem die Stiftung SIC beteiligt ist, wurde im seinem zweiten Projektjahr erfolgreich weitergeführt. Es handelt sich dabei um eigenständige Forschung der Stiftung SIC im Bereich Intrusion Detection.

- Im Bereich der Awareness wurden Veranstaltungen zum Thema Informationssicherheit (mit-)organisiert.

Mit Beschluss des Stiftungskuratoriums vom 25. April 2006 wird der Jahresbericht ohne Bilanz und Rechnungsabschluss im Internet veröffentlicht.

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 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 2005 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 Beschluss des Kuratoriums der Stiftung vom 25. April 2006 ist dieser Bericht im Internet zu veröffentlichen (ohne 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 wissenschaftlichen Situation angepasst gestalten zu können, wurden aktuelle 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 Allgemeines zur Lage der Stiftung

Das Jahr 2005 stellt das zweite, voll operative Jahr der Stiftung seit der Gründung 2003 dar. Es wurden hier die bereits im Vorjahr erfolgreichen Leistungen fortgeführt. Dies sind vor allem die Stiftungsprofessur an der TU Graz und das EU Forschungsprojekt POSITIF, die beide über das Berichtsjahr 2005 hinausgehende Verbindlichkeiten finanzieller oder inhaltlicher Natur darstellen.

Im Jahr 2005 konnten mit der erfolgreichen Beteiligung an einer Ausschreibung des Landes Steiermark zusammen mit der TU Graz das Aktivitätsfeld um konkrete Elemente aus dem Bereich E-Government erweitert werden. Insbesondere wurde aber über die Initiative PROACT ein wesentliches weiteres Element im Förderungsportefeuille der Stiftung akquiriert. Beide Aktivitäten – Ausschreibung Land und PROACT – werden erst 2006 anlaufen.

Es wurde 2005 wieder eine Reihe von Leistungen im Stiftungszweck finanziert. Dies waren zusammengefasst:

- Die Finanzierung einer *„Stiftungsprofessur Informationssicherheit“* an der TU Graz, über die die Forschung und Lehre in den Fachgebieten des Stiftungszwecks in Graz nachhaltig gestärkt wurde.

- Die dritte Ausschreibung eines Studentenwettbewerbs „*Best student paper award*“, über den Studierende bereits in ihrer Ausbildung angeregt werden, sich mit den Fachgebieten des Stiftungszwecks auseinanderzusetzen. Der Gewinner wurde zur Teilnahme an einer renommierten wissenschaftlichen Fachtagung eingeladen.

- Wissenschaftliche Weiterentwicklung durch „*Entwicklungsaktivitäten JCE Toolkit*“ durch Forscher an der TU Graz. Damit bezieht der Hilfsbetrieb direkt wissenschaftliche Tätigkeit und fördert damit auch aus dem Stiftungszweck, da das Toolkit weiterhin für die öffentliche Verwaltung in Österreich sowie für nationale und internationale Forschung frei verfügbar bleibt.

- Zusätzlich wurde ein Teil des Toolkits – die so genannten „*MOA-Lizenzen*“– neben der öffentlichen Verwaltung auch der Wirtschaft kostenlos zur Verfügung gestellt. Dies fördert die Umsetzung von E-Government und elektronischer Signatur vor allem bei Klein- und Mittelbetrieben.

- Akquisition der RFID Initiative PROACT und des Auftrags des Landes Steiermark zu Wissenstransfer und Koordination im Bereich E-Government. Beide Aktivitäten werden erst 2006 operativ.

- Das zweite Jahr des dreijährigen, EU-geförderten Forschungsprojekts POSITIF wurde erfolgreich abgeschlossen. Die Stiftung beschäftigt sich hier in einem internationalen Konsortium vor allem mit Intrusion Detection.

  Es bestehen mit der Rücklage aus 2003 Reserven, um die eingegangenen Verpflichtungen (vor allem Stiftungsprofessur bzw. Erfüllungsrisiken in Projekten wie POSITIF oder dem Hilfsbetrieb) zu bedecken und weiterhin entsprechend aktive Gestaltung aus dem Stiftungszweck zu ermöglichen.

1.4 Hilfsbetrieb JCE Toolkit

Mit Übertragung des „*JCE Toolkit*“ durch das IAIK Ende 2003 besteht ein Hilfsbetrieb, über den die Stiftung 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 wurde bereits 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). Zusätzlich wurde 2005 ein Bereich „PROACT“ angelegt, um die Gebarung dieser gemeinnützigen Aktivität gegenüber dem Kooperationspartner Philips gesondert dokumentieren zu können.

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:

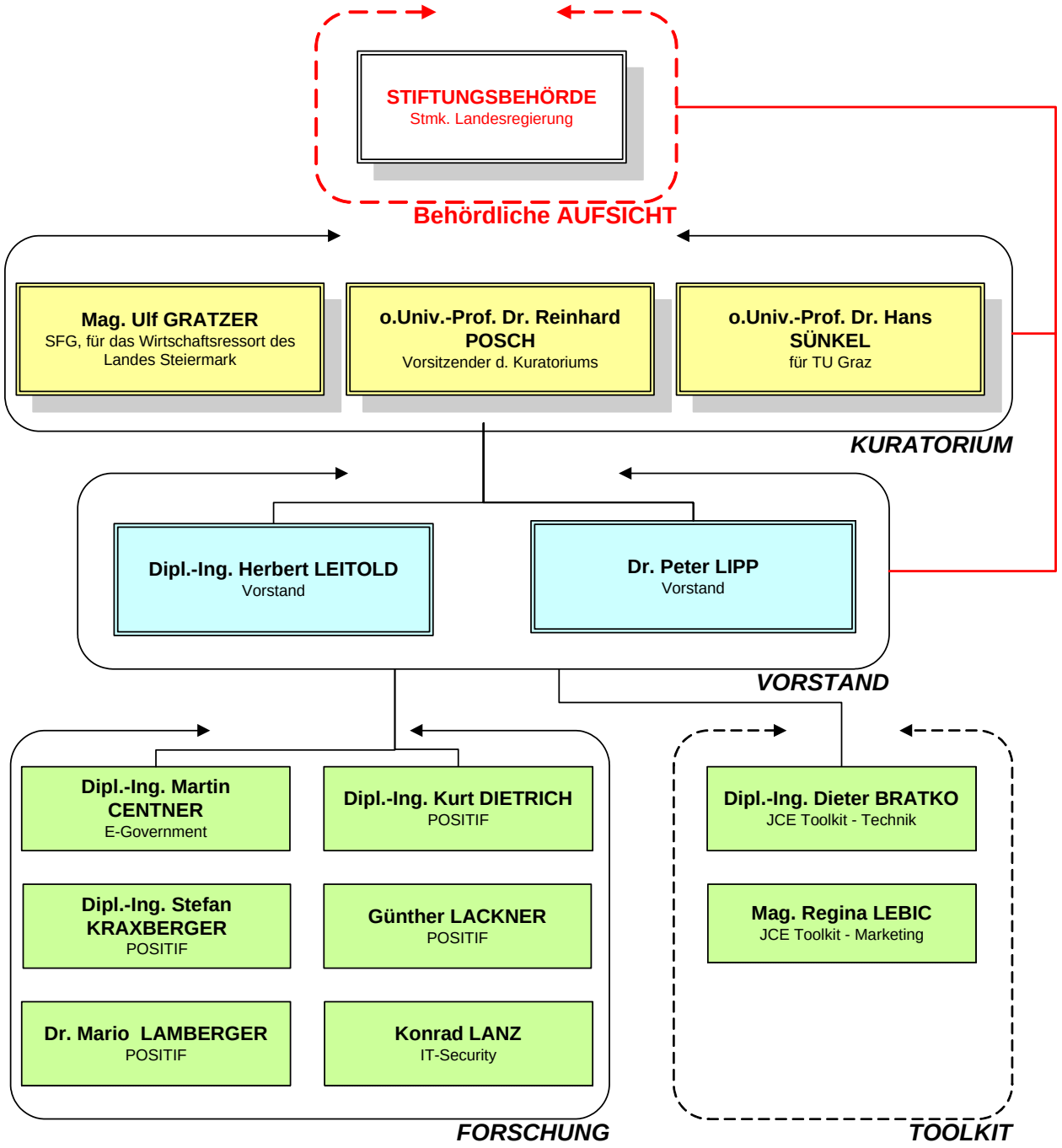
    - Mag. Ulf Gratzer (für das Wirtschaftsressort des Landes Steiermark)
    - o.Univ.-Prof. Dr. Reinhard Posch (Vorsitzender des Kuratoriums)
    - o.Univ.-Prof. Dr. Hans Sünkel (für die TU Graz)

  - 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 Mitarbeiter der Stiftung.
  - Der Bereich *Toolkit* ist als Hilfsbetrieb vom gemeinnützigen Bereich *Forschung* abgegrenzt, unterstützt diesen über Gewinne und in der Forschung verwendete Werkzeuge.

Diese Struktur ist im folgenden Organigramm dargestellt. Dabei wird der Stand an Mitarbeiterinnen und Mitarbeitern der Stiftung per 31.12.2005 dargestellt, der Bereich Administration ist wie die technische Infrastruktur vom IAIK der TU Graz gestellt – die Kosten werden von der Stiftung ersetzt.



Organigramm und Personalstand per 31.12.2005.

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*“ und „*Eigenständige Forschung und Entwicklung*“ strukturiert berichtet.

2.1 Förderung von Forschung und Lehre, Wissenstransfer

2.1.1 Stiftungsprofessur Informationssicherheit

Die im Jahr 2004 an der TU Graz am IAIK eingerichtete Stiftungsprofessur Informationssicherheit ist seit 1.10.2004 mit Prof. Dr. Vincent Rijmen besetzt. Dabei finanziert die Stiftung die Personankosten von Prof. Rijmen, die TU Graz stattet die Stiftungsprofessur mit Räumlichkeiten, zwei Assistentenstellen und Sekretariat aus.

Aus der Gruppe um Prof. Rijmen entstanden 2005 sechs wissenschaftliche Publikationen vor allem aus dem Bereich der Hash-Funktionen, die einen wesentlichen wissenschaftlichen Schwerpunkt der Gruppe darstellt:

1. Krystian Matusiewicz, Josef Pieprzyk, Norbert Pramstaller, Christian Rechberger, and Vincent Rijmen, "*Analysis of simplified variants of SHA-256*". In WEWoRC 2005 - Western European Workshop on Research in Cryptology, LNI P-74, Gesellschaft für Informatik, 2005.

2. Norbert Pramstaller, Christian Rechberger, and Vincent Rijmen, “*Exploiting Coding Theory for Collision Attacks on SHA-1*”. In Proceedings of 10th IMA International Conference on Cryptography and Coding, Royal Agricultural College, Cirencester, UK , December 19-21, 2005, pp 78-95, LNCS 3796

3. Norbert Pramstaller, Christian Rechberger, and Vincent Rijmen, "*Breaking a new Hash Function Design Strategy called SMASH*", Selected Areas in Cryptography (SAC 2005), Kingston, Ontario, Canada, to appear in LNCS.

4. Norbert Pramstaller, Christian Rechberger, and Vincent Rijmen, "*Impact of Rotations in SHA-1 and Related Hash Functions*", Selected Areas in Cryptography (SAC 2005), Kingston, Ontario, Canada, to appear in LNCS.

5. Rijmen, V.; Bechlaghem, M.: “*Proving key usage*”. - in: WISA 2004, Lecture notes in computer science 3325 (2005) , S. 68-75.

6. Rijmen, V.; Oswald, M. E.: “*Update on SHA-1*”. - in: CT-RSA 2005, Lecture notes in computer science 3376 (2005) , S. 58-71.

Weiters bereichert Prof. Rijmen die Lehre an der TU Graz mit einer Reihe von Lehrveranstaltungen wie „*Einführung in das wissenschaftliche Arbeiten*“ (Seminar), „*Angewandte Kryptografie 1 und 2*“ (Vorlesung und Übungen), Seminare in Kryptographie und „*Cryptanalysis of symmetric cryptographic primitives*“ (Privatissimum).

Es konnte durch Prof. Rijmen damit der Bereich Kryptographie in der Steiermark deutlich gestärkt werden. Mit der Organisation einer KinderUni konnte Prof. Rijmen selbst Volksschüler für die Kryptographie begeistern.

2.1.2 Best student paper award

Zur Förderung von Lehre und Wissenstransfer in der Informationssicherheit wurde zum dritten Mal ein Best Student Paper Award ausgeschrieben. Dies soll Studentinnen und Studenten anregen, sich mit dem Thema Informationssicherheit bereits während ihrer Ausbildung intensiv zu befassen.

Um ein breites studentische Feld zu erreichen, wurde der Wettbewerb nicht nur auf Studierende beschränkt, die im Studium unmittelbar mit Informationstechnologien befasst sind, sondern der Preis wurde auf alle Studierende der TU Graz ausgeschrieben.

Als Gewinner ging der Beitrag „*High Speed Elliptic Curve Cryptography Processor for GF(p)*“ von Christian Pühringer hervor. Als attraktiver Preis wurde die Teilnahme (Flug, Hotel und Konferenzgebühr) an der renommierten Fachkonferenz „ACSAC'2005; Tucson, AZ, Dezember 2005“ finanziert.

2.1.3 MOA-Lizenzen

Das JCE Toolkit wird im Rahmen des österreichischen E-Government in der Entwicklung der so genannten Module für Onlineanwendungen (MOA) verwendet. Dazu stand das Toolkit der öffentlichen Verwaltung seit jeher kostenlos zur Verfügung und wurde in bekannten Anwendungen wie FinanzOnline eingesetzt.

Ende 2005 hat sich die Stiftung entschlossen, das Toolkit auch der Wirtschaft dann kostenlos zur Verfügung zu stellen, wenn es zusammen mit diesen MOA-Modulen zum Einsatz kommt. Damit unterstützt die Stiftung die Entwicklung im Umfeld der österreichischen Bürgerkarte und des E-Government unabhängig davon, ob diese Entwicklung durch die öffentliche Verwaltung selbst oder durch die Wirtschaft erfolgt.

Dies ergab eine öffentlichkeits-wirksame Reihe von Nennungen in der Presse, vor allem auch in Online-Medien. Bekannte Nennungen sind:

- APA Meldung (23.12.2005)
- ORF – Futurezone (23.12.2005)
- Kleine Zeitung Online (23.12.2005)
- Der Standard Online (23.12. 2005)
- Wiener Zeitung (28.12. 2005)
- Kurier Online (23.12. 2005)
- Computerwelt (23.12. 2005)

Beispiele der Presseresonanz werden in „*Anhang: Pressemeldungen*“ gegeben.

2.1.4 E-Government

Die Stiftung hat zusammen mit der TU Graz an einer Ausschreibung des Landes Steiermark zu Wissenstransfer und Koordination zu E-Government angeboten[1] und den Zuschlag erhalten.

Diese Aktivität wird erst 2006 operativ starten.

2.1.5 PROACT

Es ist gelungen, in einer Kooperation mit Philips Gratkorn und der TU Graz eine Initiative „Programme for Advanced Contactless Technology“ (PROACT) zu gründen. Dabei unterstützt Philips mit dem Hauptaugenmerk in der Förderung von Forschung und Lehre der RFID Technologie an der TU Graz.

Diese Aktivität wird erst 2006 operativ starten.

2.1.6 Veranstaltungen

Im Berichtszeitraum 2005 hat die Stiftung zwei Veranstaltungen in der Steiermark mitorganisiert:

- Der „*Workshop on RFID and Lightweight Crypto*“ wurde zusammen mit dem EU Projekt ecrypt am 14. und 15. Juli in Graz organisiert. Es waren hier internationale Experten im Bereich der RFID Sicherheit vertreten.

- Der „*2. Österreichische Sicherheitstag*“ fand am 9. November 2005 in Graz statt und wurde zusammen mit der Universität Klagenfurt organisiert. Die Veranstaltung hat sich an Entscheider und Mitarbeiter von kleinen und mittleren Unternehmen gerichtet, denen IT-Sicherheitsfragen ein Anliegen sind.

2.2 Eigenständige Forschung und Entwicklung

2.2.1 Forschungsprojekt POSITIF

Das im 6. EU Rahmenprogramm geförderte Projekt „*Policy-based Security Tool and Framework (POSITIF)*“ war 2005 im zweiten von drei Projektjahren. Das Projekt betreibt Forschung im Bereich Policy-orientierter Methoden zu Netzwerksicherheit und entwickelt Werkzeuge der Informationssicherheit.

Die Stiftung beschäftigt sich dabei vor allem mit Erkennungsmethoden von Angriffen in Intrusion Detection Systemen. Es wurden Forschungsergebnisse in internationalen Konferenzen präsentiert. Unter anderem erfolgten 2005 folgende wissenschaftliche Publikationen:

1. S. Kraxberger, U. Payer, "*Polymorphic Code Detection with GA optimized Markov Models*" CMS 2005, 9th IFIP TC-6, TC-11 Conference on Communications and Multimedia Security, 19-21 September 2005, Salzburg, Austria.

[1] Teil 1 der Ausschreibung „GZ FA1B B1.40-5688/2005 Ressourcen für die Konzeption und Umsetzung von E-Government“

2. M. Lamberger, U. Payer, P. Teufl, "*Massive Data Mining for Polymorphic Code Detection*" MMM 2005, International Workshop on "Mathematical Methods, Models and Architectures for Computer Networks Security", 24 - 28 September 2005, St. Petersburg, Russia.

3. M. Lamberger, U. Payer, P. Teufl, "*Hybrid Engine for Polymorphic Code Detection*" DIMVA 2005 GI SIG SIDAR Conference on Detection of Intrusions and Malware & Vulnerability Assessment, 07 - 08 July 2005, Vienna, Austria.

4. M. Lamberger, U. Payer, P. Teufl, "*Traffic Classification using Self-Organizing Maps*" INC 2005 Fifth International Networking Conference Workshops, 05 - 07 July 2005, Samos Island, Greece.

5. S. Kraxberger, U. Payer, "*Markov Model for Polymorphic Shellcode Detection*" INC 2005 Fifth International Networking Conference Workshops, 05 - 07 July 2005, Samos Island, Greece.

2.3 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.

2.3.1 Technische Infrastruktur

Die technischen Anlagen der Stiftung, wie PCs, wurden nur in geringem Maße ausgeweitet. 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 der TU Graz und des IAIK die Anschaffung eigener teurer Anlagen nicht rechtfertigt. Die Nutzung der Infrastruktur wird an das IAIK abgegolten.

2.3.2 Entwicklungsaktivitäten JCE Toolkit

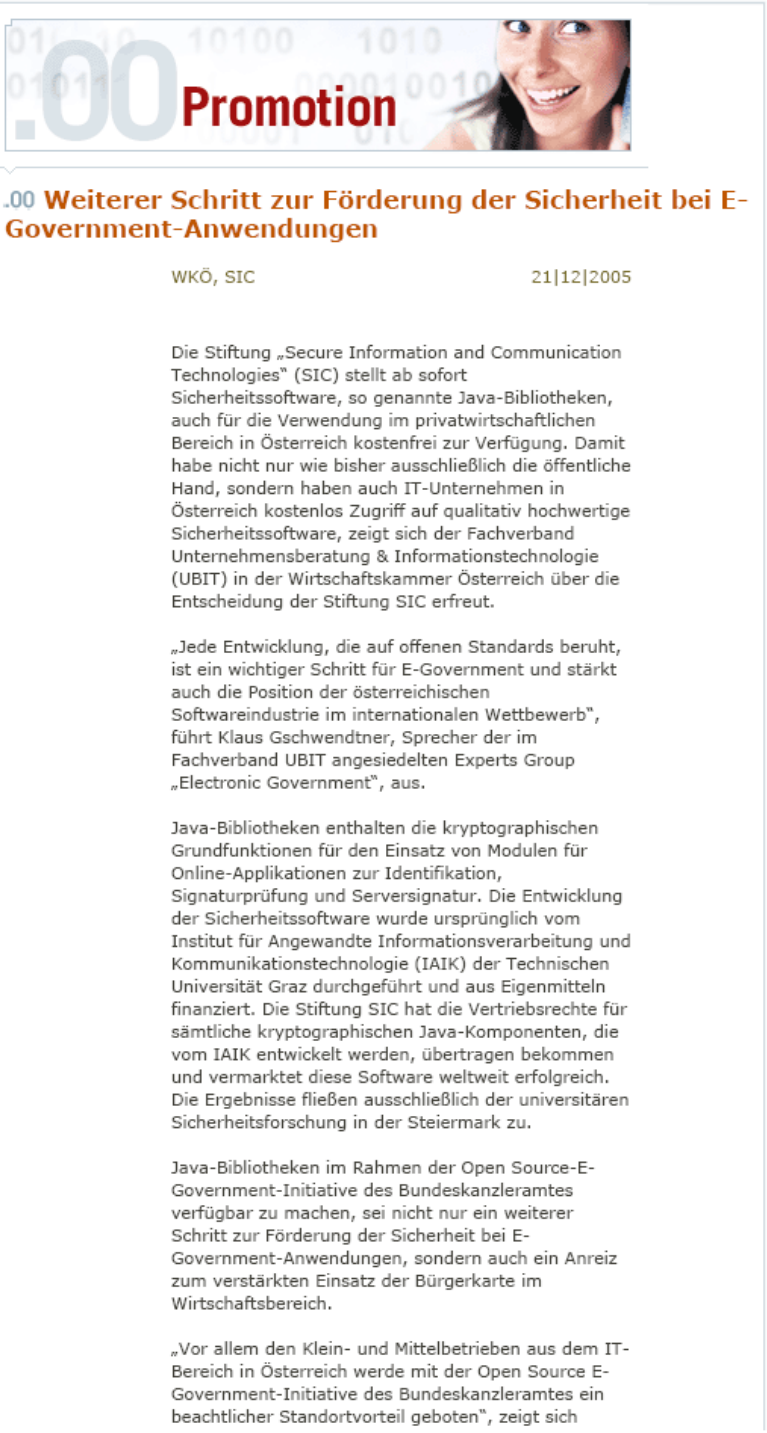
Im Hilfsbetrieb Toolkit wurden durch das Personal der Stiftung vor allem das Management, technische Wartung, Weiterentwicklung und Support, sowie das Marketing durchgeführt. Wissenschaftliche Weiterentwicklungen wurden auch an das IAIK der TU Graz vergeben. Dies insbesondere auch deshalb, als Umsatzrückgänge es erforderlich machten, den Personalstand im Bereich Toolkit zu reduzieren, um den Umsatzrückgang nicht zu Lasten der gemeinnützigen Aktivitäten kompensieren müssen. Die notwendigen Weiterentwicklungen konnten so von der TU Graz flexibler an die Geschäftslage angepasst beauftragt werden, als dies mit Fixpersonal möglich ist.

Es wurde die inhaltliche Trennung, konventionelle Entwicklungen in der Stiftung durchzuführen und wissenschaftliche Entwicklungen zu vergeben, weitergeführt, um damit Erlöse aus der kommerziellen Verwertung im Hilfsbetrieb der universitären Forschung zufließen lassen zu können. Die Gemeinnützigkeit in der wissenschaftlichen Weiterentwicklung des Produkts JCE Toolkit definiert sich daraus, dass dieses Produkt für Forschung und öffentliche Einrichtungen kostenlos zur Verfügung steht, teilweise auch der Wirtschaft wie in „*2.1.3 MOA-Lizenzen*“ dargestellt.

Anhang: Pressemeldungen

Es folgen Beispiele der Presseresonanz zur Freigabe der MOA-Lizenzen des Toolkits:

COMPUTERWELT



.00 Promotion

.00 Weiterer Schritt zur Förderung der Sicherheit bei E-Government-Anwendungen

WKÖ, SIC 21|12|2005

Die Stiftung „Secure Information and Communication Technologies" (SIC) stellt ab sofort Sicherheitssoftware, so genannte Java-Bibliotheken, auch für die Verwendung im privatwirtschaftlichen Bereich in Österreich kostenfrei zur Verfügung. Damit habe nicht nur wie bisher ausschließlich die öffentliche Hand, sondern haben auch IT-Unternehmen in Österreich kostenlos Zugriff auf qualitativ hochwertige Sicherheitssoftware, zeigt sich der Fachverband Unternehmensberatung & Informationstechnologie (UBIT) in der Wirtschaftskammer Österreich über die Entscheidung der Stiftung SIC erfreut.

„Jede Entwicklung, die auf offenen Standards beruht, ist ein wichtiger Schritt für E-Government und stärkt auch die Position der österreichischen Softwareindustrie im internationalen Wettbewerb", führt Klaus Gschwendtner, Sprecher der im Fachverband UBIT angesiedelten Experts Group „Electronic Government", aus.

Java-Bibliotheken enthalten die kryptographischen Grundfunktionen für den Einsatz von Modulen für Online-Applikationen zur Identifikation, Signaturprüfung und Serversignatur. Die Entwicklung der Sicherheitssoftware wurde ursprünglich vom Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK) der Technischen Universität Graz durchgeführt und aus Eigenmitteln finanziert. Die Stiftung SIC hat die Vertriebsrechte für sämtliche kryptographischen Java-Komponenten, die vom IAIK entwickelt werden, übertragen bekommen und vermarktet diese Software weltweit erfolgreich. Die Ergebnisse fließen ausschließlich der universitären Sicherheitsforschung in der Steiermark zu.

Java-Bibliotheken im Rahmen der Open Source-E-Government-Initiative des Bundeskanzleramtes verfügbar zu machen, sei nicht nur ein weiterer Schritt zur Förderung der Sicherheit bei E-Government-Anwendungen, sondern auch ein Anreiz zum verstärkten Einsatz der Bürgerkarte im Wirtschaftsbereich.

„Vor allem den Klein- und Mittelbetrieben aus dem IT-Bereich in Österreich werde mit der Open Source E-Government-Initiative des Bundeskanzleramtes ein beachtlicher Standortvorteil geboten", zeigt sich

DER STANDARD

derStandard.at/Web

23.12.2005 12:18

TU Graz bietet kostenlose Kryptografie-Software für Unternehmen

Sicherheit für E-Government-Anwendungen für Österreichs Wirtschaftsbetriebe - TU-Stiftung SIC bietet Programm an

Die Technische Universität Graz hält rechtzeitig zu Weihnachten ein Software-Präsent an die österreichischen Unternehmen bereit: Die gemeinnützige Stiftung "Secure Information and Communication Technologies" (SIC) an der TU Graz stellt allen österreichischen Unternehmen Sicherheits-Software für E-Government-Anwendungen kostenfrei zur Verfügung - zum Download

Schutz

Sensible Kundendaten müssen vor Fälschung und Missbrauch bewahrt werden. Entsprechenden Schutz bieten so genannte Java-Bibliotheken, wie sie die Stiftung SIC an der TU Graz entwickelt wurden und von dieser nun auch weltweit vermarktet werden. Diese auf der Java-Programmiersprache basierenden Bibliotheken enthalten die Grundfunktionen zur Verschlüsselung von Daten (Kryptografie). Sie wiederum können mit den vom Bundeskanzleramt (BKA) zur Verfügung gestellten "Modulen für Online-Applikationen für Identifikation, Signaturprüfung und Serversignatur" verknüpft werden, um der Verwaltung die Umsetzung von sicheren Online-Verfahren zu ermöglichen. Auch diese Module waren bisher nur für den Einsatz von Behörden kostenfrei. Nun können auch österreichische Unternehmen diese Produkte für Verwaltungsverfahren kostenlos nutzen.

Gemeinnützig

"Wir sind eine gemeinnützige Einrichtung, die es sich zum Ziel gesetzt hat, Datenübertragung in Österreich sicherer zu machen", begründete SIC-Vorstand Peter Lipp vom Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK) den Schritt, diese Sicherheits-Software für österreichische Wirtschaftsbetriebe bis auf weiteres kostenfrei zur Verfügung zu stellen. Begrüßt wird diese Entscheidung vom Fachverband Unternehmensberatung & Informationstechnologie (UBIT) der Wirtschaftskammer: Damit habe nicht nur wie bisher ausschließlich die öffentliche Hand, sondern auch IT-Unternehmen in Österreich kostenlos Zugriff auf qualitativ hochwertige Sicherheitssoftware. Durch die Initiative des BKA werde vor allem den Klein- und Mittelbetrieben in der IT-Branche ein beachtlicher Standortvorteil geboten.

Die Stiftung SIC wurde im Jahr 2003 vom Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK) der TU Graz gegründet. Sie hat die Vertriebsrechte für sämtliche kryptographischen Java-Komponenten, die vom IAIK entwickelt werden, übertragen bekommen und vermarktet diese Software weltweit erfolgreich. Die Erlöse fließen ausschließlich der Sicherheitsforschung in der Kommunikationstechnologie und Angewandten Informationsverarbeitung in der Steiermark zu.(APA)

Link zum Artikel:TU Graz bietet kostenlose Kryptografie-Software für Unternehmen