Jahresbericht 2019

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 werden die Aktivitäten der Stiftung im Geschäftsjahr 2019 dargestellt.

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 15. April 2020

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 „*…eigenständige Durchführung von Forschungsaufgaben und -projekten, Förderung anderer Einrichtungen, Personen und Institutionen, die zur Erreichung des Stiftungszweckes beitragen, Vergabe von Forschungsaufträgen, Vergabe von Beiträgen für wissenschaftliche Arbeiten, Durchführung von Veranstaltungen zur Bekanntmachung der Forschungsergebnisse, Publikation und Dokumentation der im Rahmen des Stiftungszwecks durchgeführten Forschungstätigkeiten*“ erfolgen.

Dieser Jahresbericht 2019 stellt die Leistungen der Stiftung nach dem Stiftungszweck im Zeitraum 1.1. - 31.12.2019 dar. Der Bericht behält die Struktur der bisherigen Berichte.

2019 konnte die Stiftung in allen Bereichen des Stiftungszwecks Beiträge leisten:

- Die Stiftungsprofessur „*Cloud Computing Security*“ – besetzt mit Prof. Mangard – wurde weiter mit Beteiligung an den Kosten der Professur zu einem Drittel und einer Assistentinnen-Stelle zu zwei Drittel finanziert.
- Zur Professur „*Kryptographie*“ von Prof. Christian Rechberger wurde eine Assistentinnenstelle zu zwei Drittel finanziert.
- 14 Studierende wurden mit einem Research Excellence Award ausgezeichnet.
- 9 Studierende erhielten ein Stipendium zur Teilnahme an einer Summer School
- Die Stiftung ist Partner im EU Forschungsprojekt KRAKEN
- Der Hilfsbetrieb JCE Toolkit hat wiederum Gewinne erwirtschaftet, 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 2019 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 16. April 2020 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 (aktuelle Version vom 7.11.2013) wie folgt definiert:

> *Zweck der Stiftung, die nicht auf Gewinn gerichtet ist, 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.*
>
> *Das Ziel der Stiftung ist die Erweiterung des menschlichen Wissens in den oben genannten Bereichen im Interesse der österreichischen Allgemeinheit.*

Die gesamte Satzung ist in der Willbriefsammlung des Steiermärkischen Landesarchivs unter LReg. Vertrag Nr. 5509 hinterlegt bzw. auch im Internet unter der Adresse https://jce.iaik.tugraz.at/sic/About_Us/Stiftung/Satzung veröffentlicht.

1.2 Forschungsschwerpunkte

Die allgemeine Formulierung des Stiftungszwecks soll dem in der Informationsverarbeitung, 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 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
- Cloud Computing
- 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. Trotz seit längerem anhaltend geringen Zinsniveaus konnten die Leistungen vor allem über Rücklagen uneingeschränkt beibehalten werden. Es ist in absehbarer Zukunft nicht damit zu rechnen, dass für Leistungen auf das Stammvermögen zurückgegriffen werden wird müssen.

Die gemeinnützigen Leistungen kamen im Berichtszeitraum 2019 über die Stiftungsprofessur Cloud Computing und die Stiftungsprofessur Kryptographie, sowie Research Excellence Awards und Stipendien vor allem Studierenden der Technischen Universität Graz zugute und stärken damit Ausbildung im Wirkungsbereich der Stiftung.

Über die Stiftungsprofessuren „*Kryptographie*“ und „*Cloud Computing Security*“ werden exzellente, international beachtete Forschungsleistungen in der Steiermark unterstützt. Mit Anstoßfinanzierung der Laufbahnprofessur „*Cybersecurity*“ wurde dies 2018 erweitert.

Die Stiftung nimmt am EU Projekt „KRAKEN“ teil, das Ende 2019 gestartet ist, womit sie auch in internationalen Forschungsaktivitäten verankert ist.

Der Hilfsbetrieb „*JCE Toolkit*“ konnte einen Gewinn erwirtschaften, der gänzlich dem gemeinnützigen Stiftungszweck zufließt. Der Personalstand ist gleich geblieben.

Es bestehen also Reserven, um die Leistungen der Stiftung weiterhin auf hohem Niveau halten zu können.

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 abgabenrechtlichem 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.

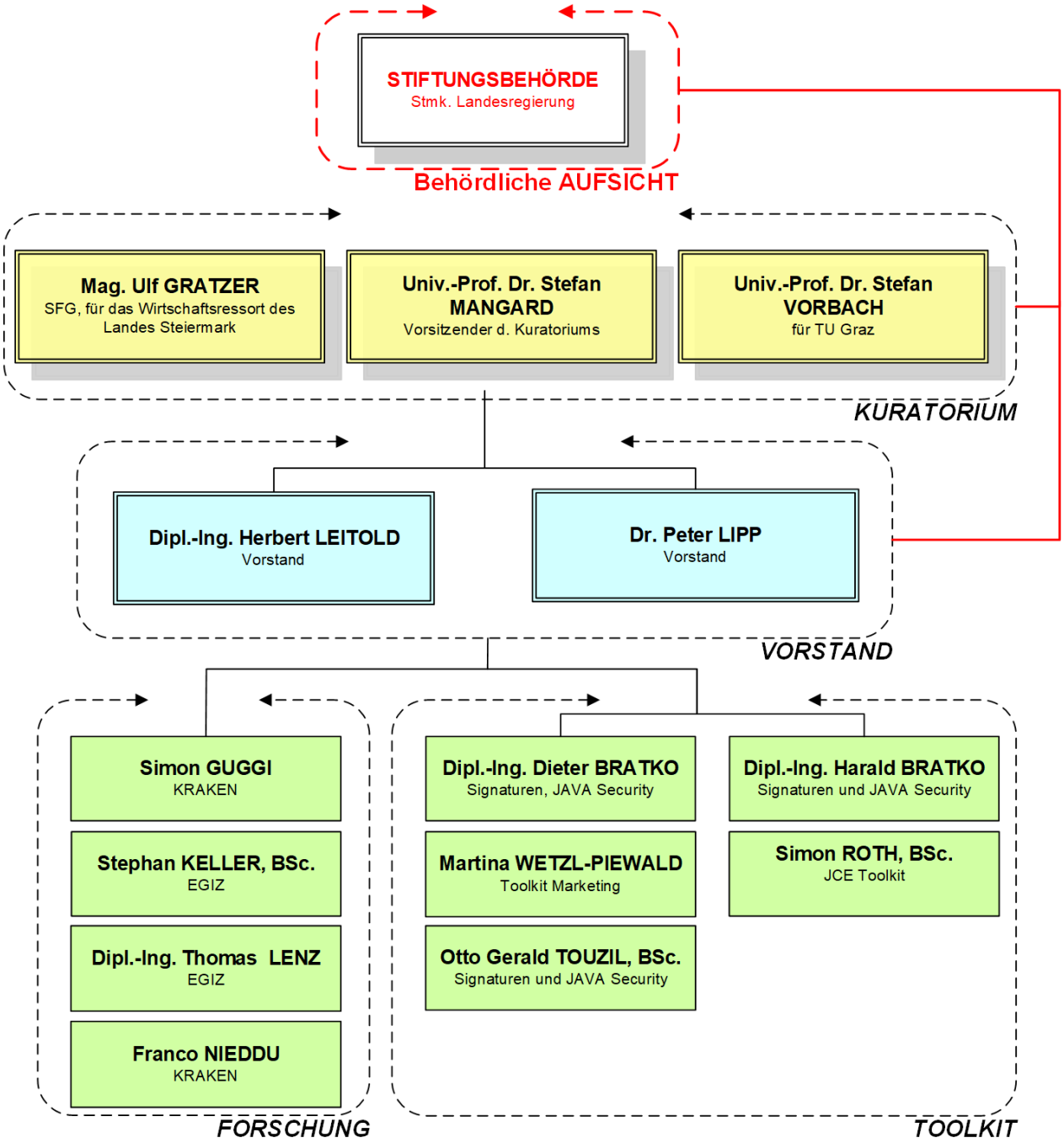
Die Abgrenzung zwischen gemeinnützigem und gewerblichem Bereich erfolgt über getrennte Kostenrechnung der Bereiche „Forschung“ (gemeinnützige Aktivitäten), „Toolkit“ (gewerblicher Hilfsbetrieb) und „Overheads“ (Gemeinkosten, die anteilig den Bereichen Toolkit und Forschung zugeordnet werden).

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 2019 waren dies:
    - Mag. Ulf Gratzer (für das Wirtschaftsressort des Landes Steiermark)
    - Univ.-Prof. Dr.-Ing. Detlef Heck (bis 1.10.2019 für die TU Graz)
    - Univ.-Prof. Dr. Stefan Vorbach (ab 1.10.2019 für die TU Graz)
    - o.Univ.-Prof. Dr. Reinhard Posch (bis 4.6.2019 Vorsitzender Kuratorium)
    - Univ.-Prof. Dr. Stefan Mangard (ab 4.6.2019 Vorsitzender Kuratorium)
  - 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 31.12.2019 dargestellt. Administration und technische Infrastruktur wird gegen Kostenersatz vom IAIK der TU Graz gestellt.



Organigramm und Personalstand per 31.12.2019

2 Leistungen im Sinne des Stiftungszwecks

Über die Leistungen der Stiftung wird nach dem in der Satzung der Stiftung definierten Zweck „Förderung von Forschung und Lehre“ berichtet.

2.1 Förderung von Forschung und Lehre, Wissenstransfer

2.1.1 Stiftungsprofessur Kryptographie

Diese Stiftungsprofessur wurde 2004 eingerichtet und von der Stiftung durchgängig co-finanziert. Nach Wechsel von Prof. Vincent Rijmen 2012 nach Leuven wurde als Überbrückung eine Gastprofessur von Florian Mendel finanziert. Seit 2017 ist die Professur mit Prof. Christian Rechberger besetzt. Die Stiftung hat eine vorgezogene Bestellung 2017 mit einer Überbrückungsfinanzierung unterstützt.

Die Stiftung bekennt sich weiter zu der von ihr 2004 initiierten Professur, es besteht die Finanzierungszusage einer AssistentInnenstelle. Diese wurde Mitte 2017 besetzt.

Die Gruppe um Prof. Rechberger konnte 2019 ihre Ergebnisse an namhaften und auch erstklassigen wissenschaftlichen Tagungen und Journalen veröffentlichen. Eine Auswahl an solchen Veröffentlichungen ist in Folge gegeben und soll zeigen, dass sich aus der von der Stiftung zusammen mit der TU Graz initiierten Professur eine Gruppe entwickelt hat, die erstklassige wissenschaftliche Forschung in der Steiermark betreibt:

1. Algebraic Cryptanalysis of STARK-Friendly Designs: Application to MARVELlous and MiMC: Albrecht, M. R., Cid, C., Grassi, L., Khovratovich, D., Lüftenegger, R., Rechberger, C. & Schofnegger, M., Advances in Cryptology - ASIACRYPT 2019.

2. Linear Equivalence of Block Ciphers with Partial Non-Linear Layers: Application to LowMC: Dinur, I., Promitzer, A., Kales, D., Ramacher, S. & Rechberger, C., Advances in Cryptology - EUROCRYPT 2019.

3. Feistel Structures for MPC, and More: Albrecht, M. R., Grassi, L., Perrin, L., Ramacher, S., Rechberger, C., Rotaru, D., Roy, A. & Schofnegger, M., ESORICS 2019.

4. Analyzing the Linear Keystream Biases in AEGIS: Eichlseder, M., Nageler, M. & Primas, R., In: IACR Transactions on Symmetric Cryptology. 2019

5. Mobile Private Contact Discovery at Scale: Kales, D., Rechberger, C., Schneider, T., Senker, M. & Weinert, C., 28th USENIX Security Symposium 2019.

In der Lehre wurden von der Gruppe unter anderem die Vorlesungen „*IT Sicherheit*“, „*Cryptography*“, „*Applied Cryptography*“ und „*Applied Cryptography 2*“ gehalten, wie auch Seminare, Bakkalaureats- und Master-Arbeiten, sowie Dissertationen betreut werden.

2.1.2 Stiftungsprofessur Cloud Computing Security

Die Stiftungsprofessur *Cloud Computing* wurde mit November 2013 mit Prof. Stefan Mangard besetzt. Die Stiftung hat diese Professur auf drei Jahre bis November 2016 zu 67% finanziert, sowie auf weitere drei Jahre bis Oktober 2019 zu 33%. Zusätzlich übernimmt die Stiftung 67% der Stelle einer Universitätsassistentin auf sechs Jahre.

Die Gruppe um Prof. Mangard konnte 2019 wieder an teils erstklassigen Konferenzen und Journalen veröffentlichen. Auch hier wird nur eine kleine Auswahl gegeben um zu zeigen,

wie die von der Stiftung und der TU Graz gestartete Professur nachhaltig wissenschaftliche Exzellenz in der Steiermark etabliert:

1. Spectre Attacks: Exploiting Speculative Execution: Kocher, P., Horn, J., Fogh, A., Genkin, D., Gruss, D., Haas, W., Hamburg, M., Lipp, M., Mangard, S., Prescher, T., Schwarz, M. & Yarom, Y., 40th IEEE Symposium on Security and Privacy 2019.

2. ScatterCache: Thwarting Cache Attacks via Cache Set Randomization: Werner, M., Unterluggauer, T., Giner, L., Schwarz, M., Gruß, D. & Mangard, S., 28th USENIX Security Symposium 2019.

3. ZombieLoad: Cross-Privilege-Boundary Data Sampling: Schwarz, M., Lipp, M., Moghimi, D., Bulck, J. V., Stecklina, J., Prescher, T. & Gruss, D., CCS 2019.

4. Page Cache Attacks: Gruss, D., Kraft, E., Tiwari, T., Schwarz, M., Trachtenberg, A., Hennessey, J., Ionescu, A. & Fogh, A., CCS 2019.

5. NetSpectre: Read Arbitrary Memory over Network: Schwarz, M., Schwarzl, M., Lipp, M., Masters, J. & Gruß, D., Computer Security - ESORICS 2019.

In der Lehre wurden von der Gruppe unter anderem die Vorlesungen „Computer Organization and Networks", „*IT Security*", "*Embedded Security*" und „*System-on-Chip Architectures and Modelling*" betreut. Das Angebot wird mit Seminaren, Bakkalaureats- und Master-Arbeiten, sowie Dissertationsbetreuungen ergänzt.

2.1.3 Research Excellence Awards

Die Prämierung ausgezeichneter studentischer Leistungen wurde 2008 begonnen und seither jährlich fortgeführt. 2019 wurden Preise an vierzehn Studierende der TU Graz vergeben, die bereits im Zuge ihrer studentischen Tätigkeiten Ergebnisse wissenschaftlich veröffentlichen konnten. Es waren dies:

- Benjamin Berg für das Paper "A Systematic Evaluation of Transient Execution Attacks and Defenses"
- Lukas Bodner für das Paper "Big Numbers - Big Troubles: Systematically Analyzing Nonce Leakage in (EC)DSA Implementations"
- Erik Kraft für das Paper "Page Cache Attacks"
- Florian Lackner für das Paper "JavaScript Template Attacks: Automatically Inferring Host Information for Targeted Exploits"
- Benedikt Maderbacher für das Paper "Bounded Synthesis of Register Transducers"
- Luca Mayr für das Paper "SGXJail: Defeating Enclave Malware via Confinement"
- Marcel Nageler für das Paper "Analyzing the Linear Keystream Biases in AEGIS"
- Lukas Neugebauer für das Paper "Mind the Gap: Finding what Updates have (really) changed in Android Applications"
- Franco Nieddu für das Paper "Cloud Data Sharing and Device-Loss Recovery with Hardware-Bound Keys"
- Philipp Ortner für das Paper "A Systematic Evaluation of Transient Execution Attacks and Defenses"

- Stefan Pranger für das Paper “Run-Time Optimization for Learned Controllers Through Quantitative Games”
- Angela Promitzer für das Paper “Linear Equivalence of Block Ciphers with Partial Non-Linear Layers: Application to LowMC
- Martin Schwarzl für das Paper “NetSpectre: Read Arbitrary Memory over Network”
- Roman Walch für das Paper “Efficient FPGA Implementations of LowMC and Picnic”

Die prämierten Studierenden erhielten jeweils Bluetooth-Lautsprecher.

2.1.4 Stipendien Summer School

Anlässlich der Graz Security Week fand eine Summer School „Security & Correctness" vom 16.-20. September 2019 statt. Über Stipendien der Stiftung wurde Studierenden der TU Graz die kostenlose Teilnahme ermöglicht. Vergeben wurden diese an neun Studenten und Studentinnen.

2.1.5 KRAKEN

Als EU Forschungsprojekt mit Beteiligung der Stiftung ist im Dezember 2019 das Projekt KRAKEN (broKeRage And marKEt platform for persoNal data) gestartet. Ziel dieses Projekts mit zehn Partnern in sechs Ländern ist es, Lösungen zu datenschutzkonformem Teilen personenbezogener Daten unter Kontrolle der Betroffenen zu erforschen.

2.1.6 E-Government

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

2.1.7 Eigene Forschungsleistungen

Mitarbeiter der Stiftung haben eigenständige Forschung im Bereich elektronischer Identität und Signaturen fortgesetzt.

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.

2.2.3 Technische Infrastruktur

Die technische Infrastruktur der Stiftung wurde weiterhin vor allem vom IAIK der TU Graz getragen. Darüber hinaus gehend 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.

2.2.4 Entwicklungsaktivitäten JCE Toolkit

Die Umsatzerlöse aus dem Verkauf des JCE Toolkits im Hilfsbetrieb waren 2019 sehr gut. Dies wurde über Aufträge zu elektronischen Signaturen sowie Lizenzierung von Software für Vertrauensdienstanbieter ergänzt.