secure
sba-research.org

Wissensbilanz

Leistungsbericht

Research Report 2012

www.sba-research.org

COMET

Competence Centers for
Excellent Technologies

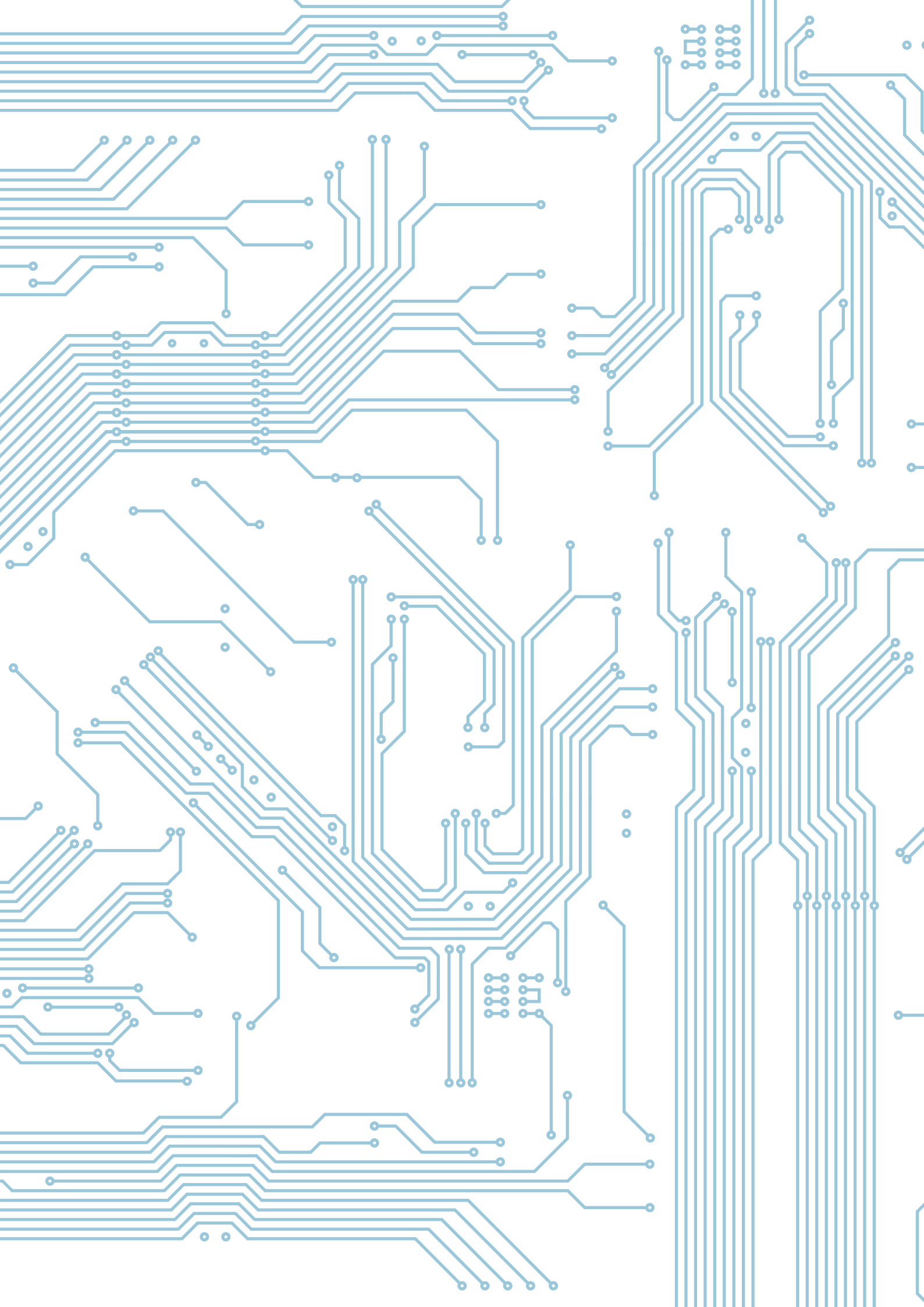
secure
sba-research.org

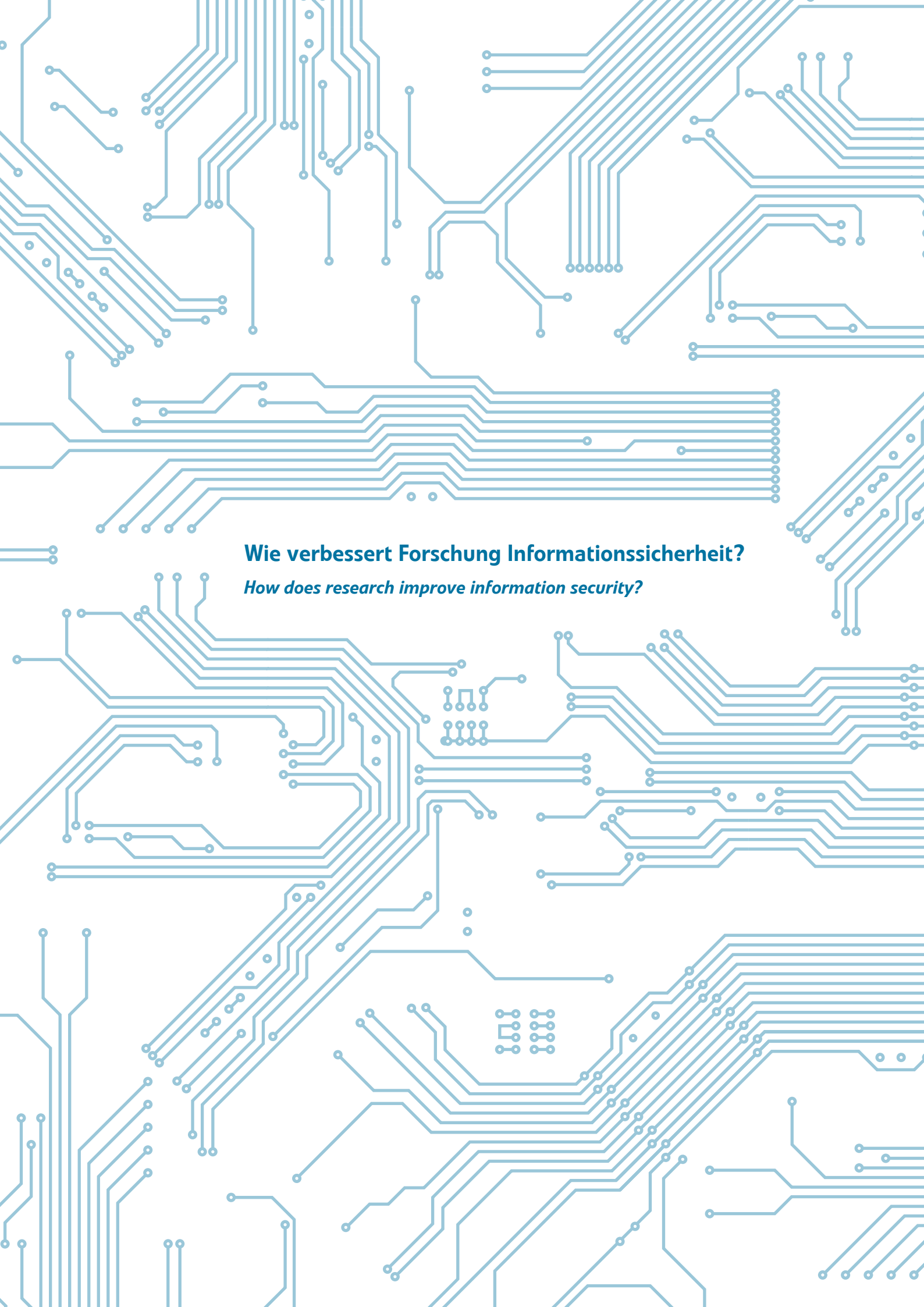
Wissensbilanz

Leistungsbericht

Research Report 2012

www.sba-research.org





Wie verbessert Forschung Informationssicherheit?

How does research improve information security?

#01 Über SBA Research

Daten mobil und sicher

Schutz von
IT-Infrastruktur & Daten

Protecting
IT infrastructure & data

Es ist noch nicht lange her, da wurden vertrauliche Informationen, Verträge oder Pläne zu Papier gebracht und im Tresor gesichert. Wer sich diese Information widerrechtlich aneignen wollte, musste vor Ort einen Aktenordner kopieren oder unbemerkt hinaustragen. Im Zeitalter vernetzter Informationsströme, globaler Geschäftsbeziehungen und mobiler MitarbeiterInnenstäbe können Unternehmen, Verbände und Rechenzentren ihre Daten nicht mehr wie Fort Knox abschotten, ohne den Anschluss zu verlieren. Die digitale Revolution entfaltet ihren Nutzen nur, wenn Daten zugänglich sind und nicht weggesperrt werden.

SBA Research, das nationale Kompetenzzentrum für Informationssicherheit, hilft, sensible Informationen beweglich und dennoch sicher zu halten. Organisatorische und technische Informationssicherheitslösungen ermöglichen es autorisierten Personen, mobil zu arbeiten und sich dabei nicht über die Schulter schauen zu lassen.

„Wir forschen und entwickeln Lösungen im Bereich Informationssicherheit."

Informationssicherheit umfasst den Schutz von IT-Infrastruktur und Daten vor unabsichtlicher oder mutwilliger Schädigung durch Personen oder Ereignisse. „Wir forschen und entwickeln Lösungen im Bereich Informationssicherheit. So stellen wir die Verfügbarkeit, Vertraulichkeit und Integrität von digital gespeicherten Daten sicher", erläutert Edgar Weippl, wissenschaftlicher Leiter bei SBA Research. Betriebsspionage und Datendiebstahl verlagern sich zunehmend ins Internet. Betroffen von Cyber-Attacken sind sowohl große als auch

About SBA Research

Mobile and secure data management

Not too long ago, confidential information, contracts and plans were written on paper and kept in a safe. If someone wanted to misappropriate this information, they had to copy the files on site or physically remove them without anyone noticing. In the age of networked information flows, global business contacts and mobile employees, businesses, institutions and computing centers can no longer seal off their data from the outside world without falling behind. Companies can use the full potential of the digital revolution only if their data are accessible instead of locked away in a strongbox.

SBA Research, the Austrian competence center for information security, helps to keep sensitive information mobile but still secure. Organizational and technical information security solutions allow authorized users to be mobile and work without anyone reading their data.

Information security is the protection of IT infrastructure and data from accidental or intentional damage by persons or events. "We research and develop solutions in the field of information security. With our work, we ensure the accessibility, confidentiality and integrity of digitally stored data," says Research Director Edgar Weippl. Industrial espionage and data theft are shifting online. Both large and small organizations can be affected by cyber attacks. There have been media reports of attacks on the US Army, Sony and VISA Card as well as on the Tyrol Health Insurance Fund, the Austrian radio and TV license fee management (GIS) and the Austrian Economic Chamber.

kleine Organisationen. Medien berichten dabei von Fällen in der US-Armee, bei Sony oder VISA Card ebenso wie bei der Tiroler Gebietskrankenkasse, dem Rundfunk-Gebühren Info Service (GIS) oder der Wirtschaftskammer Österreich.

Die Fachleute von SBA Research schützen Hardware, Prozesse und Infrastruktur forschungsbasiert und fundiert. An der Schnittstelle von Unternehmen und Universitäten arbeitet das Forschungszentrum projektorientiert und in enger Koppelung mit den wirtschaftlichen Erfordernissen. Sämtliche Mitarbeiterinnen und Mitarbeiter sind akademisch ausgebildet und an der Praxis geschult. Sie erweitern ständig ihr Know-how durch Austausch auf nationalen und internationalen Fachkonferenzen. Übernimmt man die Metapher von Schild und Speer für das Wettrüsten im Bereich Informationssicherheit, so verbessert SBA Research den Schild (Datenschutz), indem es die Prinzipien des Speers (Datenraub) gründlich auskundschaftet. Das COMET-Forschungszentrum beteiligt sich an nationalen und internationalen Forschungsprogrammen der EU (FP7), und österreichischer Ministerien etwa den BMVIT-Programmen KIRAS und FIT-IT. Der wissenschaftliche Erfolg offenbart sich in Top-Publikationen und in zunehmender internationaler Sichtbarkeit. Das Vertrauen der Industrie wird aus 25 langfristigen Partnerschaften offenkundig.

The experts at SBA Research use well-founded scientific findings to protect hardware, processes, and infrastructure. The research center is at the interface of business and academia. It works in a project-oriented and strongly business need-oriented way. All employees have a university education and hands-on experience. They are constantly expanding their knowledge by exchanging experiences with other experts at national and international conferences. If we adapt the metaphor of the shield and the spear to the arms race in IT security, SBA Research can be seen as strengthening the shield (data protection) by gaining in-depth information on how the spear (data theft) operates. The COMET research center is involved in a number of national and international research programs, such as the European Union FP7, the KIRAS program of the Austrian Ministry for Transport, Innovation and Technology, and FIT-IT. The center's scientific success is reflected in top publications and increasing international visibility. The confidence of the industry in the research center is evident in 25 long-term partnerships.

Hardware, Prozesse & Infrastruktur schützen

Protecting hardware, processes & infrastructure

Forschung zu aktuellen IT-Problemen

Prinzipiell kann jede technische Neuerung zum Einfallstor für Datendiebstahl oder Cyber-Attacken werden. SBA Research klopft aktuelle technische Trends auf ihr Bedrohungspotenzial für die Informationssicherheit ab. „Prävention von Datendiebstahl durch Klassifizierung, Beratung und das Aufdecken von Sicherheitslücken – ganz aktuell bei Cloud Computing, Sicherheit von SMS oder Social Media sowie Secure Coding – gehört zu unseren Spezialgebieten“, erläutert Markus Klemen, Geschäftsführer von SBA Research. Dass Mitarbeiterinnen und Mitarbeiter nicht nur im Büro, sondern auch via Smartphone oder Laptop von zu Hause, beim Kunden, mit weit entfernten KollegInnen oder unterwegs arbeiten können, hat Unternehmen viele Vorteile gebracht. „Dem Bild vom gut gepanzerten Tresor für die Aufbewahrung sensibler Daten stehen Cloud Computing oder WLAN-Hot Spots allerdings diametral entgegen“, weiß Klemen. Nicht zuletzt ist jeder Mitarbeiter, jede Mitarbeiterin auch eine Privatperson, die vielleicht eine Netzpräsenz auf Google+, Facebook & Co pflegt und dabei vielleicht sogar im Namen der Firma auftritt.

„Wir erforschen keine praxisfernen theoretischen Probleme, sondern suchen gemeinsam Lösungen für die Probleme unserer Partner.“

Beim Secure Coding fließt der Sicherheitsgedanke schon in die Planung und Architektur von Software ein und macht so das Endprodukt sicherer. „Wir erforschen keine praxisfernen theoretischen Probleme, sondern suchen gemeinsam Lösungen für die Probleme unserer Partner – so profitieren beide

Research on current IT problems

Generally speaking, any technical innovation can become an attack vector for data theft or cyber attacks. SBA Research scrutinizes new technical trends to evaluate their threat potential for information security. “Preventing data theft through classification, consulting and the detection of vulnerabilities – in cutting-edge areas such as cloud computing, security of text messaging and social media, as well as secure coding – is one of our specialties”, Managing Director Markus Klemen says. Companies benefit greatly from employees being able to work not only in their office, but also from home, a client’s office, or on the road using their smartphone or laptop, which allows them to cooperate with colleagues in other locations. “However, cloud computing and wireless hotspots are diametrically opposed to the image of keeping your data in an armored safe,” Klemen explains. After all, every employee is also a private individual who may have an online presence on Google+, Facebook or elsewhere – sometimes even as a representative of the company.

Secure coding means making the product secure from the ground up, starting with the initial planning and software architecture. “We don’t study theoretical problems that are far removed from practice. Instead, we work with our partners to find solutions to their problems – and both sides benefit,” says Edgar Weippl. For good research in applied informatics, results must be validated. The center’s partners and clients are companies that have an inherent need for high security, such

Seiten“, erläutert Edgar Weippl. Um in der angewandten Informatik sinnvoll forschen zu können, müssen die Forschungsergebnisse validiert werden. Partner und Kunden sind Unternehmen, die aus ihrem Wesen heraus hohe Sicherheitsanforderungen haben: Banken, der Medizin- und Pharmabereich oder Hersteller von Fertigungsanlagen.

„Unser Informationsvorsprung kommt aus dem breiten thematischen Überblick und dem guten Zugang zum akademischen Netzwerk. “

Zum anderen unterstützt SBA Research als spezialisierte Forschungseinrichtung Firmen, die selbst Sicherheitslösungen entwickeln. „Unser Informationsvorsprung kommt aus dem breiten thematischen Überblick und dem guten Zugang zum akademischen Netzwerk. Wir unterstützen unsere Partner dabei, neue Märkte zu erschließen. Wer einen Virenscanner für Browser hat, braucht künftig vielleicht einen für Mobiltelefone oder will den Mechanismus für Virenerkennung auf Spam-Erkennung umbauen“, ergänzt Markus Klemen.

as banks, medical and pharmaceutical companies, and manufacturers of production lines. As a specialized research center, SBA Research also supports companies that develop their own security solutions. “We have an information edge thanks to our broad scope of topics and good academic connections. We support our partners in developing new markets. A company with a virus scanner for browsers might need one for mobile phones some day, or might want to change the mechanism from virus to spam detection“, Markus Klemen adds.

Vom Versuchsballon zum Kometen

Gegründet wurde SBA Research 2006 von A Min Tjoa, Professor an der Fakultät für Informatik der TU Wien, und seinen Mitarbeitern Markus Klemen und Edgar Weippl im K-ind-Programm der österreichischen Forschungsförderungsgesellschaft (FFG). Eine Handvoll Unternehmenspartner der ersten Stunde – wie Raiffeisen IT oder die Sozialversicherungsanstalt der Gewerblichen Wirtschaft – gewährten dem Gründungsteam einen enormen Vertrauensvorschuss. Die sensible Forschungsmaterie rund um IT-Infrastruktur verlangt nach einem landeseigenen, langfristig geförderten Forschungszentrum für Informationssicherheit.

From trial balloon to comet

A Min Tjoa, Professor at the Informatics Department at the Vienna University of Technology (TU Vienna), and his colleagues Markus Klemen and Edgar Weippl founded SBA Research in 2006 within the framework of the K-ind program of the Austrian Research Promotion Agency (FFG). A handful of companies – including Raiffeisen IT and the Austrian Social Insurance Authority for Business (SVA) – trusted the vision of the founders from day one and became their first partner companies. The sensitive research area of IT infrastructure requires a national research center for information security with long-term funding.

Firmen profitieren von Forschung

Companies benefit from research

Seit 2006 hat sich die Belegschaft verzehnfacht und der Erfolg des Informationssicherheitszentrums wurde nach vier Jahren Laufzeit mit der Aufnahme ins Förderprogramm COMET bestätigt. 2010 wurde das Zentrum zudem in eine gemeinnützige Gesellschaft mit beschränkter Haftung (gGmbH) umgewandelt. 2014 findet die nächste Evaluierung durch die FFG und internationale ExpertInnen statt. SBA Research finanziert sich durch nationale und internationale Firmen über drei Säulen. COMET fördert die langjährige Zusammenarbeit mit Unternehmen. Mit Partnerunternehmen stellt SBA Research Anträge auf nationaler (FFG, FWF) und internationaler (EU) Ebene und übernimmt auch die Förderabwicklung. Zudem werden am Markt für Informationssicherheit Beratungsdienstleistungen und Softwareentwicklungen angeboten.

Since 2006, the number of employees has increased tenfold and the success of the research center for information security was confirmed after four years when it was accepted into the research promotion program COMET. In 2010, the legal form of the center was changed to non-profit limited liability company (gGmbH). The next evaluation by the FFG and international experts will take place in 2014. The funding of SBA Research by Austrian and international companies is built on three pillars. COMET promotes long-term cooperation with companies. SBA Research submits funding proposals for joint projects with partner companies at the national (FFG, Austrian Science Fund FWF) and the international (EU) levels and is also in charge of processing the grants. Finally, it also offers consulting services and software development on the information security market.

Privatdozent Dr. Edgar Weippl

Jahrgang 1975, ist wissenschaftlicher Direktor und Gründer von SBA Research und an der Technischen Universität Wien habilitiert. Sein Forschungsschwerpunkt liegt auf Konzepten für angewandte IT-Security und E-Learning. Nach dem Studium an der TU Wien arbeitete er in einem Start-up und unterrichtete am Beloit College (Wisconsin). 2002 bis 2004 war er als Berater für ein Software-Unternehmen in den USA und Deutschland tätig.

Born in 1975, Edgar R. Weippl is Research Director and one of the co-founders of SBA Research as well as Associate Professor at the Vienna University of Technology. His research interests are concepts for applied IT security and e-learning. After receiving a PhD and a Habilitation degree (venia docendi) from the Vienna University of Technology, he worked in a start-up and taught at Beloit College in Wisconsin. From 2002 to 2004 he worked as a consultant for a software company in the US and Germany.

„Wir überlegen uns keine theoretischen Probleme, sondern suchen gemeinsam Lösungen für die Probleme unserer Partner – so profitieren beide Seiten."

Mag. Markus Klemen

Jahrgang 1973, ist Lektor an der TU Wien sowie Geschäftsführer und Gründer von SBA Research mit Spezialgebiet angewandte Konzepte für IT-Security und Semantic-Database-Lösungen. In zehn Jahren als IT-Sicherheits-Berater und Software-Projektmanager setzte er zahlreiche Kundenprojekte um. Markus Klemen war verantwortlich für IT-Management am Institut für Softwaretechnik und Interaktive Systeme der TU Wien und entwickelte dort diverse Vorlesungen zum Thema IT-Security.

Born in 1973, Markus Klemen is a lecturer at the Vienna University of Technology and Managing Director and co-founder of SBA Research. He specializes in applied concepts for IT security and semantic database solutions. In ten years of working as an IT security consultant and software project manager, he carried out various projects for customers. Markus Klemen was responsible for IT management at the Institute of Software Technology and Interactive Systems at the Vienna University of Technology, where he developed a number of lecture series on IT security.

„Unser Informationsvorsprung kommt aus dem breiten thematischen Überblick und dem guten Zugang zum akademischen Netzwerk."

#02 „Privacy ist unsere Mission“

Noch immer erhöhen sich Datenvolumina, Rechenleistungen und die Anzahl weltweiter Computersysteme exponentiell, dem Grundsatz von Moore’s Law folgend. Bleibt dabei die IT-Sicherheit auf der Strecke? Fünf Fragen an Informatik-Professor A Min Tjoa, Gründer von SBA Research.

> Wie sind Sie zum Thema IT-Sicherheit gekommen?

Die Informatik hat zwei zentrale Elemente: Daten und Algorithmen. Datenbanken sind daher das Herzstück der Informatik. Seit meiner Dissertation beschäftige ich mich damit. Mit Zugangsregelungen für Datenbanken (Access Control) fing unsere Security-Forschung an. Die Idee, sich mit dem Thema eingehend zu befassen, hatte damals ein Dissertant von mir an der Universität Wien, der heute Professor in Regensburg ist. Der Schutz der Privatsphäre und der kritischen Informationsinfrastruktur blieb ein wichtiges Forschungsthema nach meinem Wechsel an die TU.

> Wieso haben Sie neben der universitären Forschung auch ein Kompetenzzentrum gegründet?

Ich war sogar an der Gründung von zwei Kompetenzzentren beteiligt. Ich mache das nicht zuletzt aus Gestaltungslust. Als Forscher möchte ich wissen, ob meine Konzepte in der Praxis funktionieren. Unser Institut war immer mit einem Bein in der angewandten Forschung tätig. Im Jahr 2000, in den Boomzeiten des Electronic Commerce, haben wir das Electronic Commerce Competence Center (EC3) gegründet. Viele der damaligen Themen dieses

“Privacy is our mission”

Data volumes, computing power and the number of computer systems worldwide are still growing exponentially as predicted by Moore’s Law. Can IT security keep up with this or will it fall behind? Five questions for informatics professor A Min Tjoa, co-founder of SBA Research.

> What got you started in IT security?

There are two central elements to informatics: data and algorithms. This makes databases a core feature of informatics. I have been interested in them since my dissertation. Our security research started with access control for databases. The idea to study this topic in depth came from a PhD student of mine at the University of Vienna, who is now a professor in Regensburg. Protection of privacy and critical information infrastructure remained an important topic for me when I came to the Vienna University of Technology.

> Why did you found a competence center in addition to your academic research?

Actually, I was involved in the founding of two competence centers. One of the reasons is that I enjoy the creative, hands-on process. As a researcher, I want to know whether my concepts work in practice. Our institute was always half-rooted in applied research. In 2000, during the e-commerce boom, we founded the Electronic Commerce Competence Center (EC3). Many of the topics we dealt with there are also relevant for security: preventing payment system fraud, creating ontologies and protecting personal data in the use of smart phones. This inspired us to found a competence center with a focus on information security.

Zentrums sind auch in der Security-Welt wichtig: Schutz vor Betrug bei Bezahlsystemen, Ontologien oder der Schutz personenbezogener Daten bei Nutzung von Smartphones. Dies bewog uns zur Gründung des Kompetenzzentrums mit dem Fokus Informationssicherheit.

> Wie ist die Stellung Österreichs in diesem Bereich?

In der Informatik-Community gibt es im Unterschied zu vielen anderen Disziplinen keine Ellbogen-Rangeleien. Vielleicht weil die junge Disziplin immer unter Druck von den klassischen Wissenschaften war. Die TU Graz hat einen hervorragenden Ruf im Bereich Verschlüsselung und beim E-Government. Der Kollege Reinhard Posch ist Vorstand des Institute for Applied Information Processing and Communications der TU Graz und CIO der Bundesregierung. Er hat die elektronische Signatur vorangetrieben. Die TU Wien hat sich mit Ontologien profiliert und mit den „schmutzigen Sachen" wie „intrusion detection and prevention".
Die Universität Wien und die Wirtschaftsuniversität Wien beschäftigen sich traditionell mit Geschäftsprozessen und Autorisierungen im Sinne der Zugangssicherheit von Daten. Diese vier Universitäten sind heute wissenschaftliche Partner des Kompetenzzentrums.

> Wie stehen Sie zu Hypes in der IT-Welt?

Man braucht sich vor neuen Entwicklungen niemals zu fürchten. Viele Sicherheitspannen passieren, weil die Regeln für einen sorgfältigen Umgang mit Daten nicht eingehalten werden.

> What is Austria's status in this field?

The informatics community differs from many other fields in that there isn't a ruthless scramble for positions. Maybe this is because the young discipline was always under pressure from the traditional sciences. The Graz University of Technology has an excellent reputation in cryptography and e-government. My colleague Reinhard Posch is Chair of the Institute for Applied Information Processing and Communications at the Graz University of Technology and CIO of the Austrian Federal Government. He has also contributed greatly to the development and introduction of electronic signatures. The Vienna University of Technology, in turn, is well known for its ontological developments and its focus on the 'dirty work', such as intrusion detection and prevention.
The University of Vienna and the Vienna University of Economics and Business have always had their focus on business processes and authentication in data access security. All four universities are scientific partners of the competence center.

> What do you think about IT hypes?

We should never be afraid of new development. Many security breaches are the result of people not sticking to the basic rules for careful treatment of data.

> Is complete IT security an illusion?

There is technology and then there is the human factor. Software can only be as good as the people who code and use it. Even if a software has been tested, it is not necessarily without errors or vulner-

> Ist hundertprozentige IT-Sicherheit eine Illusion?

Es gibt die Technik und den „human factor". Software kann nur so gut sein wie die Menschen, die sie schreiben und benutzen. Getestete Software bedeutet nicht, dass sie fehlerfrei ist oder keine Sicherheitslücken aufweist. Es bräuchte die mathematische Verifikation der Prozesse. Aber so weit sind wir in vielen Bereichen noch nicht. Secure Coding, das Schreiben von Software nach bestimmten Prinzipien, die Sicherheitslücken vermeiden, ist daher äußerst wichtig und wird bei uns auch gelehrt und praktiziert. Das erhöht in signifikanter Weise die Zuverlässigkeit von Systemen. Neue Konzepte bringen in der IT-Welt stets neue Chancen, aber auch neue Gefahren. Ein gutes Beispiel hierfür ist das Auslagern von Rechnerkapazitäten via Cloud Computing. Den Schutz vertraulicher Daten haben wir immer im Blick. Privacy ist unsere Mission.

abilities. This would require a mathematical verification of the processes. However, in many areas this is not yet the norm. Secure coding – following certain principles to avoid security issues when writing software – is, therefore, very important and is something we teach and practice. It significantly increases the reliability of systems. New concepts in IT always bring about new opportunities, but also new risks. A good example of this is the outsourcing of computing capacities via cloud computing. The protection of confidential data is always in our focus. Privacy is our mission.

„Es gibt die Technik und den „human factor". Software kann nur so gut sein wie die Menschen, die sie schreiben und benutzen."

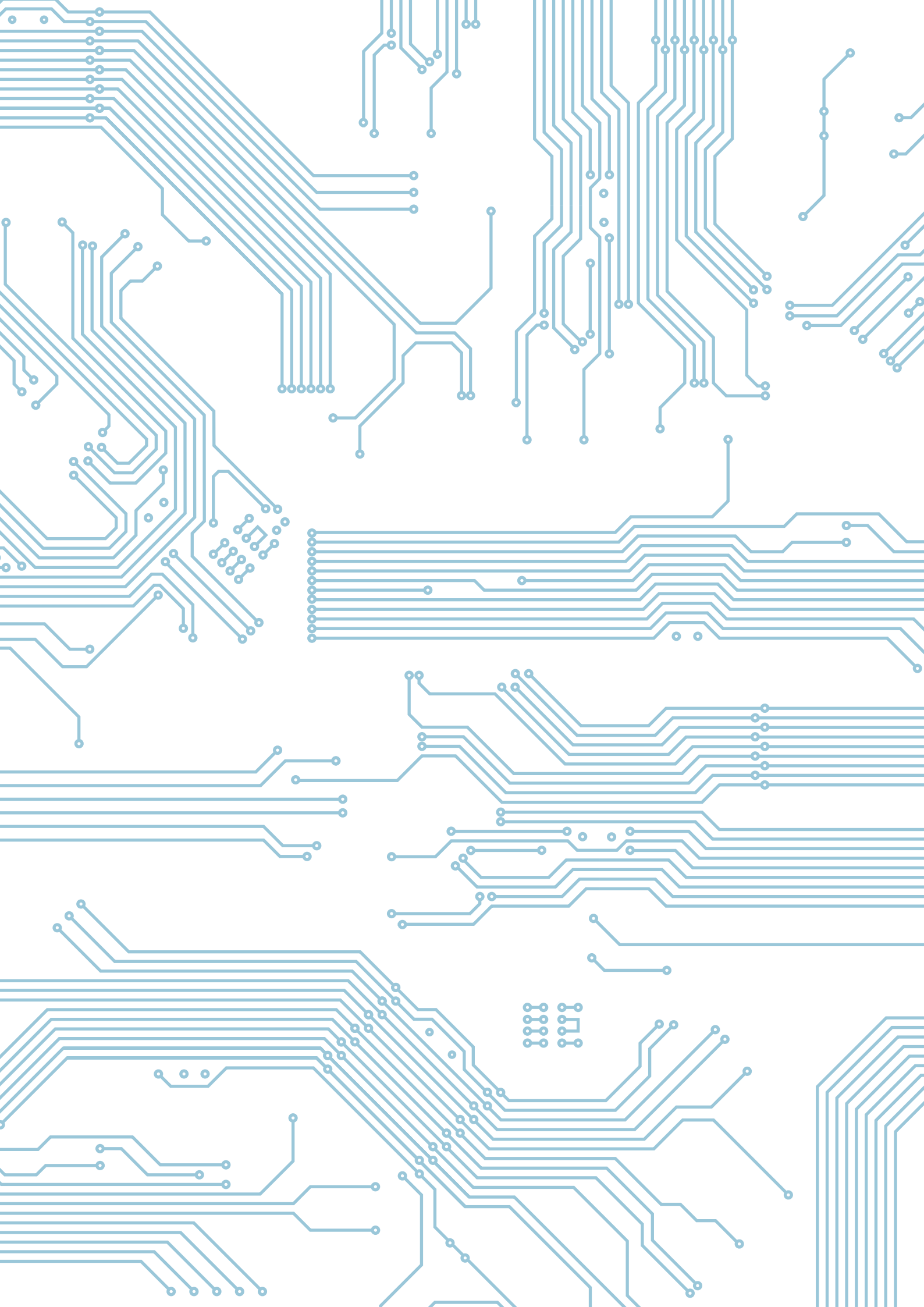
Univ.- Prof. DI Dr. A Min Tjoa

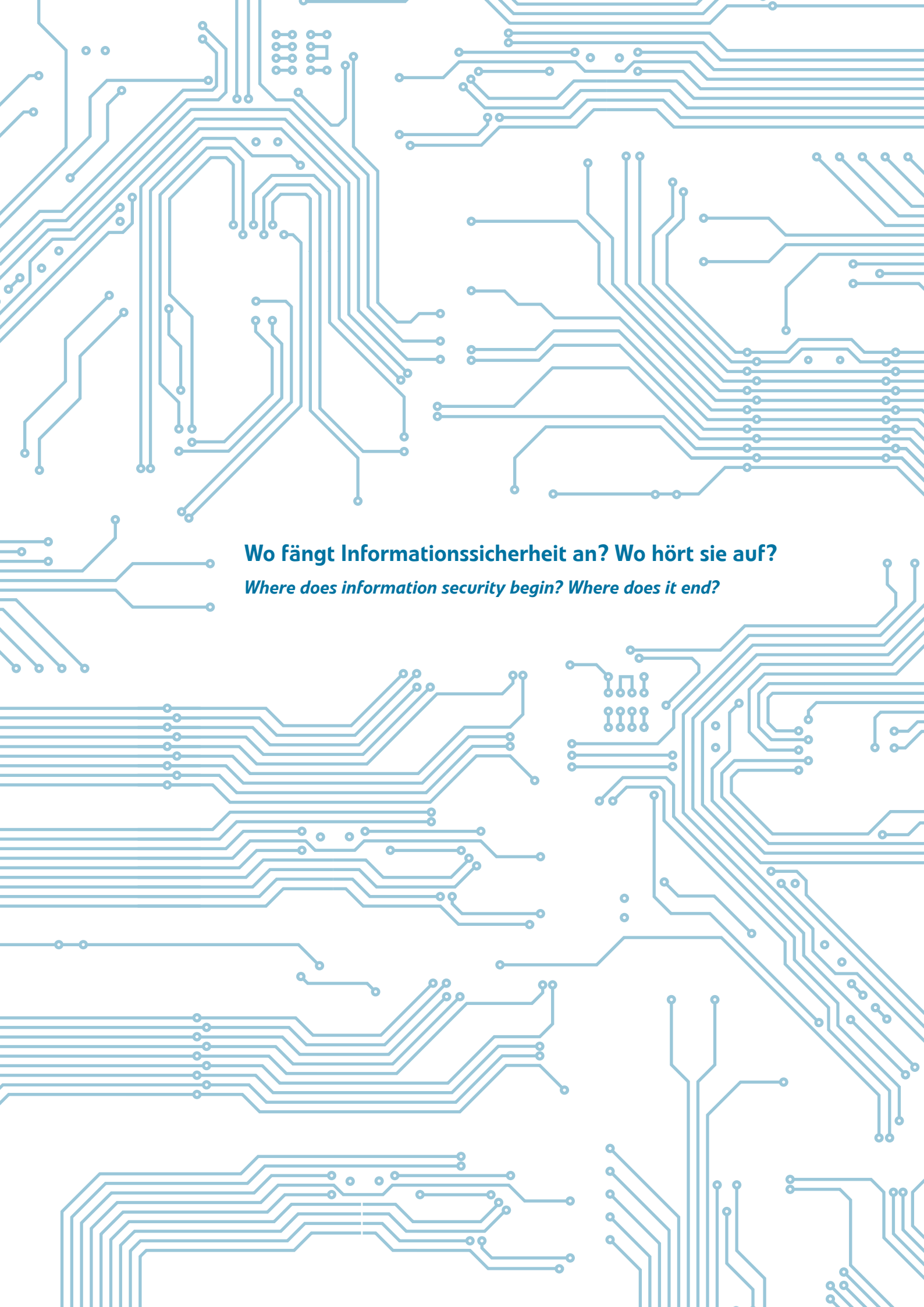
Jahrgang 1952, ist seit 1994 Vorstand des Instituts für Softwaretechnik und Interaktive Systeme der TU Wien, Obmann von SBA Research, 1982–1994 Professor an der Universität Wien, 1985–1987 Vorstand des Instituts für Statistik und Informatik der Uni Wien, 1999–2003 Präsident der Österreichischen Computergesellschaft, gründete das Electronic Commerce Competence Center (EC3) und das Kompetenzzentrum für IT-Sicherheit.

Born in 1952, A Min Tjoa has been Head of the Institute of Software Technology and Interactive Systems at the Vienna University of Technology since 1994. He is also the Chairman of SBA Research. From 1982 to 1994, he was professor at the University of Vienna, serving as Head of the Institute of Statistics and Computer Science at the University of Vienna from 1985 to 1987. He was President of the Austrian Computer Society from 1999 to 2003 and co-founded the Electronic Commerce Competence Center (EC3) and the Competence Center for IT Security.

The SBA Research team

The founders (from left to right): Edgar Weippl, A Min Tjoa, Markus Klemen





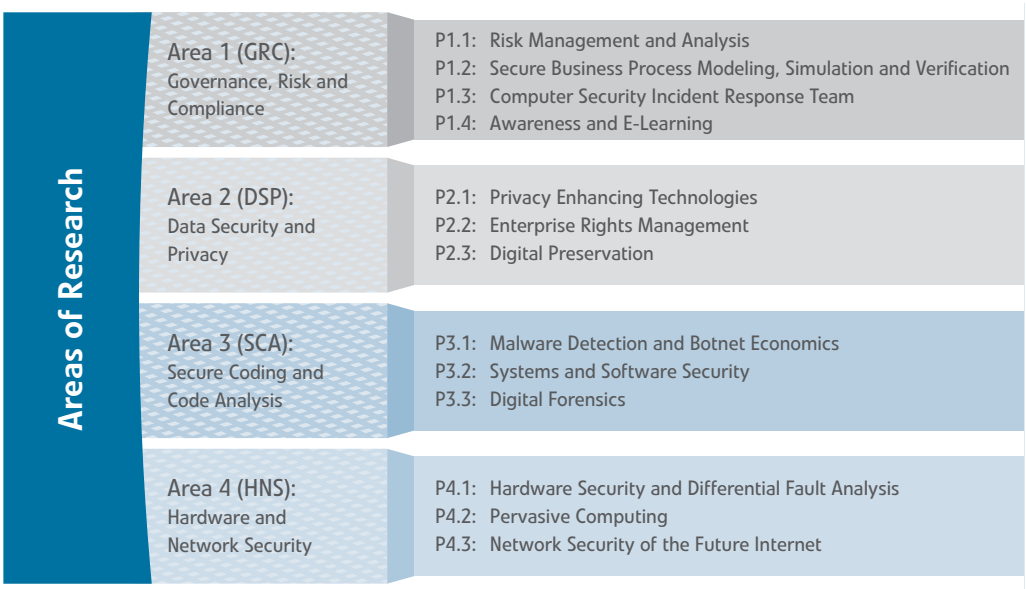
Wo fängt Informationssicherheit an? Wo hört sie auf?

Where does information security begin? Where does it end?

Die vier Forschungsbereiche von SBA Research auf einen Blick
Our four areas of research at a glance

#03 Die vier Forschungsbereiche auf einen Blick

Our four areas of research at a glance



Die vier Schwerpunkte von SBA Research repräsentieren die vier Ebenen der IT-Sicherheit:

Area 1 beleuchtet die Organisation und ihre Geschäftsprozesse.
Area 2 widmet sich der Datensicherheit, dem Rechtemanagement von Daten sowie der Problematik der digitalen Langzeitarchivierung.
Area 3 stellt die Sicherheit von Software ins Zentrum.
Area 4 behandelt die Hardware, die IT-Infrastruktur sowie die Sicherheit zukünftiger Internetstandards.

The four main research areas of SBA Research represent the four levels of IT security:

***Area 1** deals with organizations and business processes.*
***Area 2** addresses questions of data security, data rights management, and questions of long-term digital preservation.*
***Area 3** focuses on software security.*
***Area 4** deals with hardware, IT infrastructure, and the security of future Internet protocol standards.*

Die vier Forschungsbereiche im Detail

Our four areas of research in detail

#04

Area 1: Governance, Risk and Compliance (GRC)

„Geschäftsprozesse und Produkte sind zwei Seiten derselben Medaille – gemeinsam bilden sie den Unternehmenskern."

– Stefanie Rinderle-Ma, SBA Key Researcherin und Informatikprofessorin an der Uni Wien

Nahezu jedes Geschäftsmodell beruht heute auf der Verfügbarkeit von zuverlässiger und sicherer Informationstechnologie.
Risk Management & Analysis behandelt IT-Sicherheits-relevante Schwachstellen: Risiko-Management und -Analyse unterstützen Entscheidungsträger bei der Kosten-Nutzen-Abwägung von Investitionen in die IT-Sicherheit.
Secure Business Process Modeling, Simulation & Verification: Die Modellierung sicherer Geschäftsprozesse, ihre Simulation und Verifikation zeigen Schwachstellen auf und machen Systeme hinsichtlich bestehender Gesetze und Richtlinien sicher.
Computer Security Incident Response Team: Die schnelle Eingreiftruppe ermöglicht den Aufbau einer Organisationsstruktur, die Gefahren identifiziert und IT-Sicherheitslösungen, abgestimmt auf die Risiko-Analyse, rasch einführt.
Awareness & E-Learning: richtet sich an die zentralen Akteure eines ganzheitlichen IT-Security-Konzepts: die Nutzerin und den Nutzer. Neuartige Methoden erlauben es Organisationen, die UserInnen zu schulen und Lösungen effizient und Nutzen stiftend einzuführen.

Area 1: Governance, Risk and Compliance (GRC)

"Business processes and products are two sides of the same coin – together, they form the core of a business."

– Stefanie Rinderle-MA, SBA Key Researcher and Professor of Informatics at the University of Vienna

Nearly every business model today is based on the availability of reliable and secure information technology.
***Risk Management & Analysis** deals with weaknesses that are relevant to IT security. Risk management and analysis support decision-makers in weighing the costs and benefits of IT security investments.*
***Secure Business Process Modeling, Simulation & Verification:** Modeling, simulating and verifying secure business processes helps identify their weaknesses and makes systems secure and compliant with legal norms and guidelines.*
***Computer Security Incident Response Team:** This quick response team allows an organization to create a structure that identifies threats, performs a risk analysis and rapidly implements appropriate IT security solutions.*
***Awareness & E-Learning** is directed at the central players in a holistic IT security concept: the users. Novel methods allow organizations to train users and introduce solutions in an efficient and effective way.*

Area 2: Data Security and Privacy (DSP)

„Privacy ist unsere Mission!“

– A Min Tjoa, Informatikprofessor und Obmann von SBA Research

Privacy – also der Schutz personenbezogener Daten – ist ein zentrales Thema der heutigen Informationsgesellschaft, ein fundamentales Recht des Einzelnen, das verteidigt werden muss. Heute erzeugt jede und jeder Datenspuren, die von Firmen und Behörden aufgespürt, gespeichert und verwendet werden können. Verteilte und eingebettete Systeme bergen das Risiko, dass jeder Anwender überwacht werden kann. Ziel ist Schutz und Sicherstellung von Daten und Privacy durch:

Enterprise Rights Management: Schutz von unternehmensrelevanten Daten vor unbefugtem Zugriff.

Privacy: Schutz von Daten und Aktivitäten von Privatpersonen.

Digital Preservation: Methoden zur Langzeitspeicherung von Daten und Prozessen, bei denen die Lesbarkeit und Verarbeitung der Daten und die Nachvollziehbarkeit von Prozessen in Zukunft garantiert werden können.

Area 2: Data Security and Privacy (DSP)

“Privacy is our mission!”

– A Min Tjoa, Professor of Informatics and Chairman of SBA Research

Privacy – the protection of personal data – is an important issue in our modern information society. It is a fundamental right of each individual and must be protected. Today, everyone leaves data traces that businesses or government agencies can find, store and use. In distributed and embedded systems, it is possible to monitor all users. The objective of SBA Research is the protection and securing of data and privacy through:

Enterprise Rights Management: Protecting critical company data from unauthorized access.

Privacy: Protection of data and activities of private individuals.

Digital Preservation: Methods for the long-term archiving of data and processes in order to ensure that data remains accessible and usable and processes remain reproducible in the future.

Area 3: Secure Coding and Code Analysis (SCA)

„Das Wettrüsten zwischen Malware-Autoren und Analysten geht weiter."

– Martina Lindorfer, Doktorandin bei SBA Research und an der TU Wien

In den letzten Jahren war IT-Sicherheit für viele Unternehmen gleichbedeutend mit Virenscannern und Firewalls. Dieser Ansatz ist pragmatisch, aber zu wenig umfassend. Wer die Firewall durchdringt, kann sensible Daten weiterverbreiten und widerrechtlich Zugriff auf Informationen erlangen.
SBA Research erforscht neue Erkennungsmethoden, um böswillige Angriffe wirksam eindämmen zu können. Hierfür sind wir in folgenden Forschungsfeldern tätig:
Secure Coding: Das Berücksichtigen von Sicherheitsaspekten schon beim Programmieren zählt zu den wichtigsten Maßnahmen zur Erhöhung der Gesamtsicherheit eines Systems.
Malware Detection und Botnet Economics: Sicherheitsmechanismen können durch Bots/Malware umgangen oder aufgebrochen werden. Derartige Angriffe müssen erkannt und verhindert werden. Ein permanenter Wettlauf, da die Angreifer ihre Methoden laufend verfeinern, neue Lücken finden und Angriffsmethoden entwickeln.
Digitale Forensik: Beweissicherung in der digitalen Welt ist eine besondere Herausforderung, da – anders als in der physischen Beweissicherung – digitale Spuren leicht verwischt werden können. Durch die Zunahme von Cyberkriminalität erhält dieser Forschungsbereich langfristig eine große Bedeutung.

Area 3: Secure Coding and Code Analysis (SCA)

"The arms race between malware authors and analysts continues."

– Martina Lindorfer, PhD student at SBA Research and at the Vienna University of Technology

In the past, many companies equated IT security with virus scanners and firewalls. While this approach may be pragmatic, it does not go far enough. If someone gets through the firewall, they can gain unauthorized access to information and spread sensitive data. SBA Research develops new ways of intrusion detection in order to mitigate malicious attacks successfully. To do so, we focus on the following research areas:
Secure Coding: Taking security aspects into account already in the programming phase is one of the top measures for increasing the overall security of a system.
Malware Detection and Botnet Economics: Security mechanisms can be circumvented or breached by bots or malware. Such attacks must be recognized and prevented. It is a constant race with attackers, who keep refining their methods, finding new vulnerabilities and developing new attacks.
Digital Forensics: Securing digital evidence is a special challenge, as digital traces are much easier to hide than in traditional forensics. The increase in cyber crime gives this research field an enormous long-term significance.

Area 4: Hardware and Network Security (HNS)

„Wo eine technische Komponente eine Entscheidung für uns trifft, müssen vertrauenswürdige und sichere IT-Komponenten stehen."

– Philipp Tomsich, Gründer von Theobroma Systems und Partner von SBA Research

Da jede Softwarelösung auf sicherer Hardware und sicheren Netzwerken basieren sollte, sollten diese Systeme durch Forschung auf folgenden Gebieten möglichst sicher gestaltet werden:

Hardware-Security und Fehleranalyse: Ein Missbrauch von Hardware kann sehr großen Schaden anrichten, da sie nicht so leicht ausgetauscht werden kann. Entsprechende Potenziale für Sicherheitslücken sind weit weniger erforscht als bei Softwarekomponenten.

Pervasive Computing: SBA Research beschäftigt sich mit den Sicherheitsproblemen, welche aus dem stärker werdenden Einsatz von Mikroelektronik und Netzwerktechnologie in Alltagsgegenständen erwachsen.

Netzwerksicherheit im „Future Internet": Durch die Bedeutung von Web 2.0 und Cloud Computing gewinnen neuartige Sicherheitsproblematiken – wie verteilte Datenspeicherung und Zugriffssicherung auf externen Systemen – an Bedeutung. Hierfür werden Security-Konzepte entwickelt, neuartige Systeme analysiert und getestet sowie neue Architekturvorschläge erarbeitet.

Area 4: Hardware and Network Security (HNS)

"Wherever a technical component makes a decision for us, we must make sure it is a trustworthy and secure IT component."

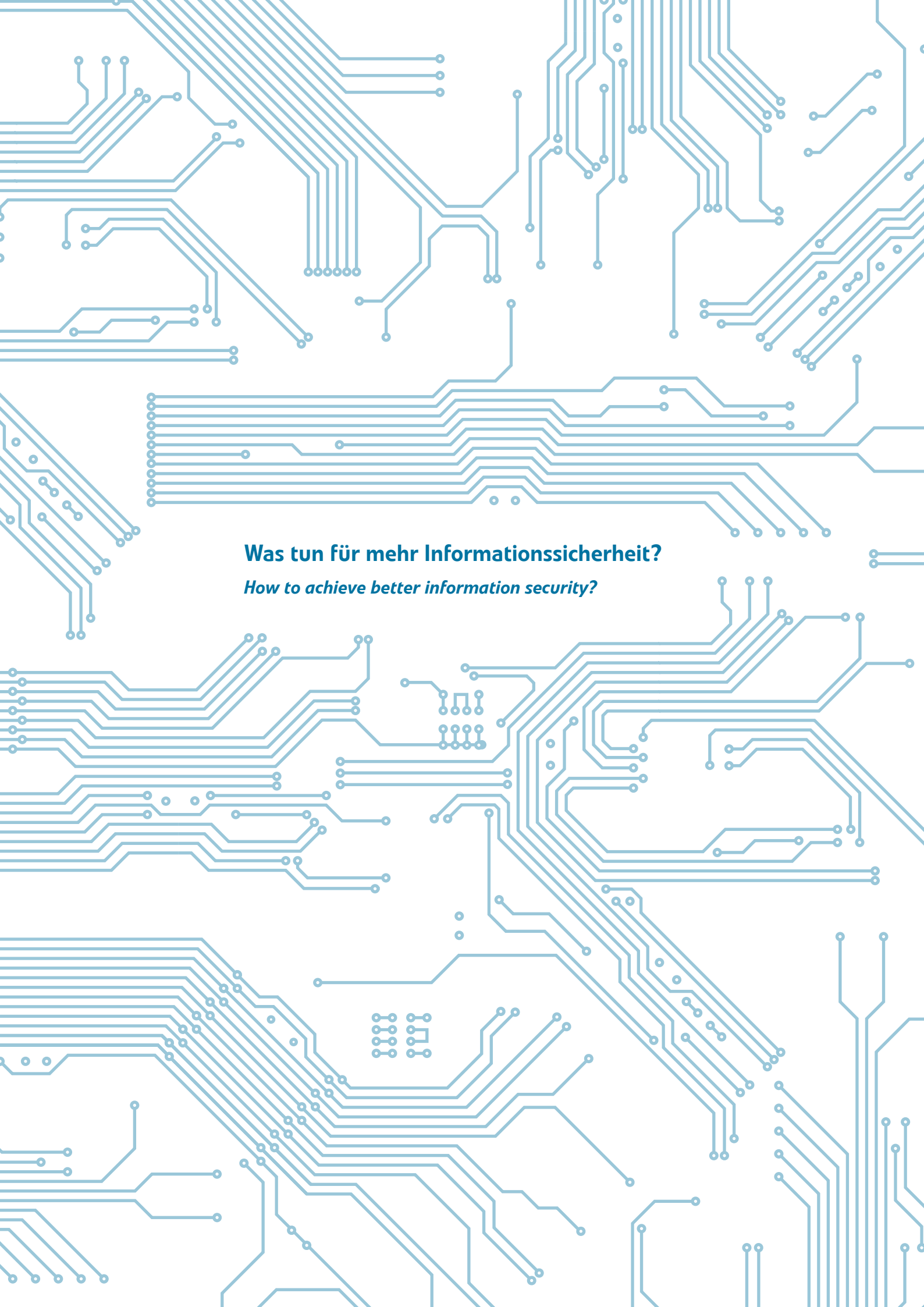
– Philipp Tomsich, founder of Theobroma Systems and partner of SBA Research

Because every software solution should be based on secure hardware and networks, we aim to increase the security of these systems with research in the following areas:

Hardware Security and Fault Analysis: The malicious use of hardware can cause great damage, as it is hard to switch out the components. There is much less research into potential vulnerabilities than with software components.

Pervasive Computing: SBA Research researches security issues that result from the increased use of microelectronics and network technology in everyday objects.

Network Security of the Future Internet: With the growing significance of Web 2.0 and cloud computing, new security issues emerge, such as distributed data storage and access control on external systems. We develop security concepts, analyze and test new systems, and develop recommendations for system architecture.



Was tun für mehr Informationssicherheit?

How to achieve better information security?

#05 Area 1: Governance, Risk und Compliance (GRC)

Systematische Dokumentation macht IT-Sicherheit erst möglich

„Geschäftsprozesse und Produkte sind zwei Seiten derselben Medaille – gemeinsam bilden sie den Unternehmenskern", meint Stefanie Rinderle-Ma, Informatikprofessorin an der Uni Wien: Die Spitalsbehandlung eines Patienten von der Diagnose bis zur Nachbetreuung, die Fertigung eines Produkts von Zulieferern bis zum Qualitätsmanagement, der Verkauf einer Dienstleistung samt Kundenbetreuung.

„Es ist falsch zu glauben, dass IT-Sicherheit nur ein technisches Thema ist."

„Wenn es in der eigenen Organisation zu wenig Informationen darüber gibt, wie Geschäftsprozesse genau ablaufen und welche sicherheitskritischen Stellen es gibt, ist eine professionelle Analyse und Modellierung dieser Sachverhalte sinnvoll", ergänzt Mark Strembeck, Associate Professor an der Wirtschaftsuniversität Wien. Prozesse sind für ihn die höchste Ebene der IT-Sicherheit: „Es ist falsch zu glauben, dass IT-Sicherheit nur ein technisches Thema ist. Über sicherheitskritische Tätigkeiten, Daten und Geschäftsprozesse kann nicht der IT-Administrator entscheiden, sondern nur die Unternehmensleitung."

Area 1: Governance, Risk and Compliance (GRC)

Systematic documentation is a prerequisite for IT security

"Business processes and products are two sides of the same coin – together, they form the core of a business," says Stefanie Rinderle-Ma, Professor of Informatics at the University of Vienna. Be it the hospital treatment of a patient from diagnosis to aftercare, the manufacturing of a product from suppliers to quality assurance, or the sale of a service with customer support: "If an organization has too little information about how its business processes work and which parts are security critical, professional analysis and modeling is a good idea," adds Mark Strembeck, Associate Professor at the Vienna University of Economics and Business. He considers processes the highest level of IT security: "It is a mistake to think that IT security is only a technical issue. It is not the IT administrator who can make decisions about security-critical measures, data or business processes – these can only be made by the management."

Today, compliance with legal norms in businesses (e.g., in the financial, automotive or medical industry) is monitored by auditors. In the future, intelligent software will help automate these checks as much as possible and give alerts in case of problems. Available GRC software products generally have a lower performance than the state of the art

Bisher wurde die Compliance, also die Einhaltung gesetzlicher Vorgaben in Unternehmen (Finanz-, Automobil-, Medizinbereich etc.), von Auditoren überwacht. Künftig soll intelligente Software helfen, diese Checks (soweit möglich) zu automatisieren und auf Probleme aufmerksam machen. Verfügbare GRC-Softwareprodukte leisten in der Regel deutlich weniger, als nach dem Stand der Forschung möglich wäre. Mark Strembeck und Stefanie Rinderle-Ma beschäftigen sich als Key Researcher von SBA Research damit, Lösungen für die große Zahl komplexer Fragestellungen in diesem Bereich zu erarbeiten. Als Teil ihrer Arbeit machen sie Vorschläge für adaptierte Vorgehensweisen und die Umsetzung von sicherheitstechnischen Maßnahmen.

Im Alltag ist kaum Zeit, Anweisungen schriftlich zu dokumentieren, aktuell zu halten und Wissen aus den Köpfen für alle zugänglich zu machen.

Geschäftsprozesse sind meist nicht ausreichend dokumentiert. Im Alltag ist kaum Zeit, Anweisungen schriftlich zu dokumentieren, aktuell zu halten oder Wissen aus den Köpfen der Mitarbeiterinnen und Mitarbeiter für alle zugänglich zu machen. Erstes Ergebnis und Mehrwert ist eine systematische Dokumentation, die organisationsweite IT-Sicherheitsmaßnahmen oft erst möglich macht. Jeder Geschäftsprozess hat einen Beginn und ein Ende,

would allow. As Key Researchers at SBA Research, Mark Strembeck and Stefanie Rinderle-Ma develop solutions for the large number of complex questions in this area. Part of their work is to make suggestions for adapting methods and for the implementation of security measures.

Business processes are generally not documented sufficiently. There is little time for documenting instructions in writing, for updating, or for making the knowledge of individual employees available to everyone. The first result of an analysis is a systematic documentation, which is often the prerequisite for developing organization-wide IT security measures. Every business process has a beginning and an end, with several steps in between and branches where decisions are made. These are translated into a standardized, graphical language for modeling. Each symbol represents an activity, a person, a role or location. The use of a symbol language allows an intuitive approach to the problems and is a starting point for translating a process into software.

Business process analysis starts by examining written process descriptions that are already available and with questionnaires, workshops or interviews with the employees. This analysis often leads to surprising realizations when the main processes of an organization are modeled visually for the first time. "The statements range from 'so that's what it looks like' to 'that's the way things were five years

mehrere Schritte und Verzweigungen bei Entscheidungen. Diese werden für die Modellierung in standardisierte, grafische Sprachen übersetzt. Jedes Symbol steht für Tätigkeiten, Personen, Rollen oder auch Orte. Der Kunstgriff über die Symbolsprache macht Probleme intuitiv zugänglich und bildet gleichzeitig die Grundlage, um einen Prozess auch in Software umzusetzen.

Compliance rechnergestützt umsetzen

Computer-assisted compliance

Die Basis einer Geschäftsprozessanalyse sind bereits existierende schriftliche Prozessbeschreibungen, Fragebögen, Workshops oder Gespräche mit MitarbeiterInnen. Eine solche Analyse sorgt immer wieder für Aha-Erlebnisse, wenn zentrale Prozesse einer Organisation zum ersten Mal grafisch modelliert werden. „Statements reichen von ‚So sieht das also aus' bis ‚so war das vor fünf Jahren'. Erst wenn man die Prozesse kennt, kann man systematisch vorgehen und Richtlinien in die IT integrieren", weiß die Key Researcherin. Es werden allgemeingültige Konzepte und Vorgehensweisen entwickelt, wie Compliance rechnergestützt umzusetzen ist. Im Modell können zum Beispiel Algorithmen für die Erkennung von Konflikten entwickelt werden. In Pilotprojekten und Fallstudien mit Partnerunternehmen – etwa mit dem Rechenzentrum der Stadt Wien oder dem Anlagenbauer ABB – wird geprüft, wie gut diese Ansätze funktionieren. „Man muss ein kommunikativer Typ sein. Oft treten in Unternehmen Ängste auf, die eigene Expertise oder das Ausmaß der Arbeitsbelastung preiszugeben", so Rinderle-Ma. „Es hilft uns, dass wir nicht als kommerziell orientierte Unternehmensberater auftreten, sondern als Wissenschaftler mit dem Anliegen des Erkenntnisgewinns. Wir haben zum Beispiel kein Interesse daran, Menschen wegzurationalisieren", ergänzt Key Researcher Mark Strembeck.

ago'. Only if you know how the processes work can you work systematically and integrate guidelines into IT," Key Researcher Rinderle-Ma explains. She develops general concepts and approaches for computer-assisted compliance. In the model, individual algorithms can be developed, e.g., for recognizing conflicts. The approaches are tested in pilot projects and case studies with partner companies – e.g., the Computing Centre of the City of Vienna or the plant manufacturer ABB. "In this job, you have to be a communicative person. When we go into companies, people are often hesitant about sharing their own expertise or telling us how large their workload is," she says. Key Researcher Mark Strembeck adds, "It helps that we are not seen as profit-oriented business consultants but as scientists looking to gain new insights. We aren't there to make people redundant."

Univ.- Prof. Dipl.-Math. Dr. Stefanie Rinderle-Ma

Jahrgang 1976, Head of Research Group Workflow Systems and Technology, seit 2010 Professorin für Informatik an der Uni Wien.
Studierte Wirtschaftsmathematik in Augsburg, ab 2000 wissenschaftliche Mitarbeiterin an der Uni Ulm, Post-Doc-Aufenthalte an den Universitäten Twente und Eindhoven (Niederlande) sowie der University of Ottawa/Telfer School of Management (Kanada), seit Mai 2010 Key Researcher bei SBA Research.

Born in 1976, Stefanie Rinderle-Ma is the Head of the Research Group Workflow Systems and Technology and Professor of Informatics at the University of Vienna.
She studied business mathematics in Augsburg and began working as a research assistant at the University of Ulm in 2000. She had postdoc research stays at the Universities of Twente and Eindhoven (Netherlands) and the University of Ottawa/Telfer School of Management (Canada). She has been Key Researcher at SBA Research since May 2010.

„Erst wenn man die Prozesse kennt, kann man systematisch vorgehen und Richtlinien in die IT integrieren."

Prof. Dr. Mark Strembeck

Jahrgang 1974, Associate Professor und stellvertretender Institutsvorstand am Institut für Wirtschaftsinformatik und Neue Medien der Wirtschaftsuniversität Wien.
Studierte Wirtschaftsinformatik in Essen, Schwerpunkt Software Engineering und Informationssicherheit, kam 2001 nach Wien für die Promotion, habilitierte an der WU Wien und ist seit 2009 Key Researcher bei SBA Research.

Mark Strembeck was born in 1974 and is Associate Professor and Vice Institute Head of the Institute for Information Systems and New Media at the Vienna University of Economics and Business.
He studied business informatics in Essen with a focus on software engineering and information security. In 2001, he came to Vienna to get a doctoral degree and went on to receive a Habilitation degree (venia docendi) at the Vienna University of Economics and Business. He has been Key Researcher at SBA Research since 2009.

„Es ist falsch zu glauben, dass IT-Sicherheit nur ein technisches Thema ist. Über sicherheitskritische Tätigkeiten, Daten und Geschäftsprozesse kann nicht der IT-Administrator entscheiden, sondern nur die Unternehmensleitung."

#06 Area 2: Data Security und Privacy (DSP)

Aus der Kultur in die Unternehmen

Datenformate veralten rasant

Data formats rapidly become obsolete

Während die IT voranschreitet, veralten hinter ihr die Datenformate der gespeicherten Informationen. Bibliotheken, Archive und Museen haben die Aufgabe, analoge und digitale Wissens- und Kulturschätze zu sammeln, aufzubewahren und verfügbar zu machen. Entsprechend intensiv beschäftigen sie sich mit digitaler Langzeitarchivierung (digital preservation). Das Thema betrifft aber auch die Industrie. Sie muss Daten benutzbar halten, um damit arbeiten zu können. Was heute problemlos mit einem weit verbreiteten Programm aufzurufen ist, könnte in wenigen Jahren unlesbar geworden sein. „Der Bedarf für digitale Langzeitarchivierung ist bereits da, das Bewusstsein dafür ist aber erst im Kommen", meint Andreas Rauber, der in Österreich die Brücke von den ArchivierungsexpertInnen aus den Kulturwissenschaften zu den InformatikerInnen gebaut hat.

Flugzeugbauer und Kraftwerksbetreiber haben Anlagen, Infrastruktur und Produkte lange in Betrieb. Typische Beispiele für bits und bytes in Formaten, die vielleicht nicht mehr zuverlässig ausgeführt werden können, sind Prozesssteuerungen (Automobil, Pharma), Baupläne, Verzeichnisse, Berechnungen mit eingespeisten Sensordaten, Kontobewegungen, Kundendaten oder Lohnabrechnungen. Sie sollten auch nach einem Vierteljahrhundert Fortschritt fehlerfrei aufgerufen werden können. Produktrückrufe, Gerichtsprozesse, Audits, Übernahmen, internationale Kooperationen – die Anlässe sind mannigfaltig. Viele Unternehmen arbeiten zudem mit EDV-Lösungen, die speziell auf ihre Bedürfnisse zugeschnitten und so zu Insellösungen geworden sind.

Area 2: Data Security and Privacy (DSP)

From culture to business

As information technology progresses, data formats of stored information become obsolete. Libraries, archives and museums have the responsibility to collect and preserve analog and digital treasures of art and science and make them available to the public. As a result, they are strongly involved in digital preservation. However, the issue also concerns the world of business. Companies have to keep their data accessible in order to work with them. Information that might be readily accessible with a widely-used program today may become unreadable in a few years. "The need for digital preservation is already here, but the awareness for it is only now emerging", says Andreas Rauber, who has managed to bridge the gap between the arts and computing by connecting Austrian archiving experts with informatics experts.

Aircraft companies and power plant operators, for example, use their plants, infrastructure and products for a long time. Typical examples of bits and bytes in formats that may no longer be retrievable in the future are process control (automotive industry, pharmaceutical industry), blueprints, directories, calculations using sensor data, account movements, customer data, or payroll accounting. These should be retrievable without errors even after twenty-five years of technological advances. Product recalls, lawsuits, audits, takeovers, international cooperation – there are countless situations where those data could be needed. As an added difficulty, many businesses use customized IT solutions, which become isolated applications.

Digitale Langzeitarchivierung bedeutet, Datenverarbeitungssysteme
- langfristig
- beim Wechsel zu anderen IT-Systemen
- bei Ergänzungen
- oder Erneuerungen/Austausch

arbeiten zu lassen.

Besonders interessant sind Archivierungslösungen für Anbieter von Backup-Lösungen, Cloud Storage oder Virenschutzprogrammen. Rechenzentren können ihren Kundinnen und Kunden die „Nutzbarkeit von Informationen" als Zusatzleistung anbieten, Daten also nicht nur speichern, sondern auch langfristig verfügbar halten.
„Digitale Langzeitarchivierung ist keine einmalige Aktivität", warnt der Associate Professor an der TU Andreas Rauber. Ihre Strategien helfen aber schon in der Gegenwart. Eine saubere Dokumentation, klare Strukturen der Decodierung von Nullen und Einsen und die Verwendung offener Standards als Strukturprotokoll sind empfehlenswert.

Zwei Strategien und Lösungswege kommen zum Einsatz: Bei der Migration werden die Daten immer weiter umgewandelt, um verwendbar zu bleiben. Emulation versucht das System und die Umgebung zu erhalten, in denen die Daten ursprünglich verarbeitet wurden.

Bisherige Forschungsergebnisse wurden am „lebenden Objekt" mit großen Kulturinstitutionen erarbeitet. Mit diesen Erfahrungen hat SBA Research eine automatisierte Digital-Preservation-Lösung für den kommerziellen Bereich entworfen. Vorgehensweisen, Referenzmodelle sowie Tools zur Analyse und Verifizierung der Dokumente werden entwickelt und als Programm prototypisch für KMUs umgesetzt.

Digital preservation means ensuring that data processing systems can work
- *in the long term*
- *when IT systems are changed*
- *when things are added*
- *or renewed/replaced.*

Archiving solutions are particularly interesting for providers of backup services, cloud storage or antivirus programs. Computing centers can offer their clients the 'usability of information' as an added service, ensuring that data is not only stored but also accessible in the long term.
"Digital preservation is not something you do only once", Andreas Rauber, Associate Professor at the Vienna University of Technology, points out. However, the strategies are useful in the present as well. Good documentation, clear structures for decoding zeroes and ones, and the use of open standards as structural protocols are recommended.

There are two different strategies and solutions: In migration, data are converted with every system change to keep them useable. Emulation, on the other hand, seeks to preserve the system and environment in which the data were originally processed.

The research results so far were gained in a real-world environment together with large cultural institutions. Based on these experiences, SBA Research has developed an automated digital preservation solution for commercial applications. Procedures, reference models, and document analysis and verification tools are developed and implemented in a prototype for SMEs.

Programm für KMUs

Program for SMEs

SBA Research ist Partner im EU-Projekt Timeless Business Processes (TIMBUS) und erforscht mit Unternehmen wie SAP, Intel oder SQS wie dynamische, rechnergestützte Geschäftsprozesse bewahrt und langfristig ausgeführt werden können. Alliance for Permanent Access to the Records of Science Network (APARSEN) ist ein europäisches Netzwerk mit rund 30 Partnern, das den Wissensaustausch, die Standardisierung und die Ausbildung im Bereich digitale Langzeitarchivierung fördert. Das Thema soll gemeinsam mit der Herausforderung, entsprechende rechtliche Standards zu schaffen, in der Öffentlichkeit thematisiert und weitergetrieben werden.

www.timbusproject.at

www.alliancepermanentaccess.org

SBA Research is involved in the EU project Timeless Business Processes (TIMBUS), where it cooperates with businesses such as SAP, Intel or SQS to research how dynamic, computer-assisted business processes can be preserved and performed in the long term. The Alliance for Permanent Access to the Records of Science Network (APARSEN) is a European network with around 30 partners that promotes knowledge exchange, standardization, and training in digital preservation. The goal is to publicize and promote the issue and the challenge of creating legal norms.

www.timbusproject.at

www.alliancepermanentaccess.org

„Der Bedarf für digitale Langzeitarchivierung ist bereits da, das Bewusstsein dafür ist aber erst im Kommen."

ao. Univ.- Prof. DI Dr. techn. Andreas Rauber

Leiter der TU-Forschungsgruppe Digital Preservation an der Fakultät für Informatik.
Jahrgang 1973, studierte Informatik an der TU Wien, forschte ab 2001 am National Research Council of Italy (CNR) und am French National Institute for Research (INRIA) in Computer Science and Control, seit 2004 Associate Professor am Institut für Softwaretechnik und Interaktive Systeme, Präsident der Austrian Association for Research in IT (AARIT), seit 2007 Key Researcher bei SBA Research.

Andreas Rauber is head of the Research Group on Digital Preservation at the Department of Informatics at the Vienna University of Technology.
He was born in 1973 and studied informatics at the Vienna University of Technology. In 2001, he joined the National Research Council of Italy (CNR) as a researcher and then worked at the French National Institute for Research in Computer Science and Control (INRIA). He became Associate Professor at the Institute of Software Technology and Interactive Systems at TU Vienna in 2004. He is president of the Austrian Association for Research in IT (AARIT) and has been a Key Researcher at SBA Research since 2007.

Area 3: Secure Coding und Code Analysis (SCA)

Ferngesteuert unter einer Tarnkappe

In Botnetzen kann jeder mit seinem Rechner unwissentlich Teil einer E-Mail-Massenversand-Aktion (Spam) werden. Der „Bundestrojaner", eine Software des Deutschen Bundeskriminalamts zur unbemerkten Online-Überwachung von Computern verdächtiger Personen, sorgte für intensive Debatten. Und der Stuxnet-Wurm in Steuerungssystemen legte unter anderem Anlagen zur Anreicherung von atomarem Material im Iran lahm. Für Martina Lindorfer sind diese Fernsteuerungsmechanismen Teil der Ausbildung und Forschung, spezialisiert sich die junge Informatikerin doch auf die Analyse von Malware.

Mit Malware werden bösartige Programme wie Viren, Würmer und Trojaner bezeichnet, hinter deren Entwicklung handfeste finanzielle oder politische Motivation steckt. Schaden entsteht dabei direkt oder indirekt durch den Diebstahl wertvoller Informationen bis zum unbrauchbar machen oder der missbräuchlichen Verwendung von Infrastruktur. Nützliche und schädliche Programme wurden immer parallel entwickelt: „In den vergangenen Jahren ist Malware jedoch durch die große Verbreitung von Computern mit Internetverbindung besonders lukrativ geworden", weiß Martina Lindorfer.

Im September 2011 präsentierte die Malware-Spezialistin auf der RAID-Konferenz (Recent Advances in Intrusion Detection) in Kalifornien ihre Arbeit über die Erkennung von Anti-Analyse-Mechanismen:

Area 3: Secure Coding and Code Analysis (SCA)

#07

Remote-controlled and cloaked

Anyone can unwittingly become part of a spam campaign if their computer becomes part of a botnet. In the last years, there have been heated debates about a Trojan developed by the German Federal Criminal Police Office for the purpose of monitoring computers of suspects. The Stuxnet worm hit control systems, bringing, among others, Iran's nuclear enrichment facilities to a standstill. For Martina Lindorfer, these remote-control mechanisms are part of her training and research. The young informatics expert specializes in malware analysis.

Malware refers to malicious programs such as viruses, worms and Trojans, whose development is financially or politically motivated. Damage is caused directly or indirectly by actions ranging from the theft of valuable information to sabotaging infrastructure or using it for malicious purposes. Useful and harmful programs have always been developed in parallel. "However, in recent years malware has become very lucrative due to the large number of computers connected to the Internet," says Martina Lindorfer.

In September 2011, the malware specialist presented her work on the recognition of anti-analysis mechanisms at the RAID (Recent Advances in Intrusion Detection) conference in California: "Malware attempts to detect and circumvent the analysis to remain hidden for longer," she explains. Martina

Diebstahl wertvoller Informationen

Theft of valuable information

„Malware versucht die Analyse zu erkennen und zu umgehen, um länger unerkannt zu bleiben", beschreibt sie. Bereits in ihrer Masterarbeit hat Martina Lindorfer dynamische Analysesysteme erforscht: „Dabei führen wir Malware in einer geschützten Umgebung – wir nennen es Sandbox – aus und beobachten das Verhalten der Malware." Die „infizierten Proben" für ihre Versuche in der Sandkiste beinhalten ganz aktuelle Schadprogramme, die sich im Internet in großem Ausmaß in Umlauf befinden.

Das Wettrüsten zwischen Malware-Autoren und Analysten geht weiter.

Insgesamt ein Jahr dauerte die Analyse von 1700 Proben für ihre Diplomarbeit am Secure Systems Lab der TU Wien. Bestimmte Schadprogramme können erkennen, ob sie sich in einer Analyseumgebung befinden oder auf einem Rechner eines „echten" Benutzers. Wenn sie ein „nicht produktives System" erkennen, bleiben sie inaktiv. Ein großer Teil der Arbeit war die Implementierung eines Systems, in dem eine Malware aktiv wird. „Ich habe mein Referenzsystem möglichst einfach gehalten und so umgebaut, dass Unterschiede im Verhalten der Malware feststellbar sind. Es ist für die Zukunft erweiterbar, denn das Wettrüsten zwischen Malware-Autoren und Analysten geht weiter", erklärt die Doktorandin. Geduldig hat sie Proben in verschiedenen Analyseumgebungen verglichen, bis die Schadprogramme nicht mehr erkennen konnten, ob sie gerade analysiert wurden. Ihnen wurden die „Tarnkappen" abgezogen und so ihre Anti-Analyse-Mechanismen erkennbar gemacht.

Lindorfer's research into dynamic analysis systems began with her Master's thesis. "We execute malware in a safe environment – we call this a sandbox – and observe its behavior." The 'infected samples' for her sandbox experiments include some very current malicious programs that are widely spread on the Internet.

It took a year to analyze the 1,700 samples for her Master's thesis at the Secure Systems Lab at TU Vienna. Some malware programs can detect whether they are in an analysis environment or on the computer of a 'real' user. If they recognize that they are on a non-productive system, they remain inactive. A large part of Martina Lindorfer's work was to implement a system in which malware would activate. "I tried to keep my reference system as simple as possible and modified it to find differences in malware behavior. The system can be expanded at any time, for the arms race between malware authors and analysts continues," the PhD student adds. She compared samples in different analysis environments until the malicious programs were no longer able to detect that they were being analyzed. 'Uncloaking' them in this way made their anti-analysis mechanisms visible.

For her dissertation, which is supervised by Edgar Weippl, she examines trends in malware development. She enjoys the input from various sources that she gets at SBA Research, where cooperation between different areas is encouraged. The evolution of malware is generally tied to the spread in the use of devices and applications. One aim of

Für ihre Dissertation, betreut von Edgar Weippl, beschäftigt sie sich mit Trends in der Malware-Entwicklung und freut sich auf vernetzte Inputs, denn bei SBA Research wird viel Wert auf die Kooperation verschiedener Bereiche gelegt. Die Evolution von Malware folgt dabei generell der Verbreitung von Geräten und Anwendungen. In ihren Forschungsarbeiten wird sie entsprechende Prognosen erstellen und aufzeigen, wie finanzielle Motivation die Weiterentwicklung steuert – etwa bei mobilen Geräten wie Smartphones oder Tablets. Sie sucht Antworten auf die Fragen: Wie wird Malware im Laufe der Zeit weiterentwickelt und wie kann man sich davor schützen?

Der große Freiraum bei der Forschung an der Front fasziniert die Linzerin. Die Computer-Spätzünderin – sie bekam den ersten Rechner mit 15 Jahren – ist Hackerin im ursprünglichen Sinn: „Man muss verstehen, wie man Systeme angreifen kann, um sie zu schützen. Das ist abwechslungsreich und kreativ und reizt mich!"

her research is to predict future developments and show how financial motivation guides development – e.g., with mobile devices such as smartphones and tablets. She focuses on how malware evolves over time and how we can protect ourselves against it.

Martina Lindorfer is fascinated by the countless possibilities of front-line research. She did not get her first computer until she was 15, but the researcher from Linz is a 'hacker' in the original sense: "To protect systems you have to know how they can be attacked. That's interesting and creative work, I enjoy it!"

DI Martina Lindorfer

Jahrgang 1984, Projektassistentin am Institut für Rechnergestützte Automation der TU Wien, absolvierte an der FH Hagenberg den Bachelor-Lehrgang Computer- und Mediensicherheit, wechselte zum Master-Studium in Software Engineering und Internet Computing an die TU Wien und macht ihr Doktorat am Secure Systems Lab der TU Wien, betreut von Edgar Weippl (SBA Research) und Paolo Milani (TLLOD.com, Partner von SBA Research).

Born in 1984, Martina Lindorfer is a project assistant at the Institute of Computer Aided Automation at TU Vienna. She received her Bachelor's degree in computer and media security at the University of Applied Sciences in Hagenberg, got a Master's degree in Software Engineering and Internet Computing at TU Vienna, and is now working on her PhD at the Secure Systems Lab of TU Vienna, supervised by Edgar Weippl (SBA Research) and Paolo Milani (TLLOD.com, partner of SBA Research).

„Man muss verstehen, wie man Systeme angreifen kann, um sie zu schützen."

#08 Area 4: Hardware and Network Security (HNS)

Sicherheit ist eine Zwiebel

Produktsicherheit auf allen Ebenen

Die Entwicklungsabteilungen der Hardwarehersteller stehen vor großen Herausforderungen. Es müssen Zeit und Kosten gespart und zum anderen die Zahl der Funktionen und die Leistungsparameter gesteigert werden. Wer mit einem Datenleck oder einem Sicherheitsproblem nicht in die Schlagzeilen geraten möchte, setzt dabei besser auf sicheres Design, integriert also Sicherheitsüberlegungen schon in die Architektur- und Planungsphase eines Projekts. Produktsicherheit hat mehrere Ebenen. Die erste ist Betriebsspionage, wenn die Konkurrenz aufwendige Eigenentwicklungen anbietet. Die zweite sind Fälschungen, die günstig in Asien produziert werden, und die dritte Haftungsfragen, wenn jemand z. B. mit Chip-Tuning die Funktion verändert und diese Modifikation einen Schaden auslöst. Theobroma entwickelt gemeinsam mit SBA Research „Blueprints". Diese Blaupausen für sichere Hardware, Prozesse und Netzwerke betrachten Informationssicherheit wie eine Zwiebel. In allen Schichten muss Sicherheit und Vertrauenswürdigkeit gewahrt sein. Die beste Software nützt nichts, wenn die Datenübermittlung, die Authentifizierung oder die Hardware fehlerhaft und unsicher sind.

„Theobroma ist ein Designhaus – ähnlich wie ein Architekturbüro. Wir planen und beschreiben ein System, suchen Bauteile und Hersteller aus, kümmern uns um Zulassung und Zertifizierung bis hin zu Fertigungs- und Wartungsabläufen. Wir beziehen den gesamten Lebenszyklus und Bedienungsaspekte mit ein", erklärt Geschäftsführer und Gründer Philipp Tomsich. Sicherheit in der IT ist immer ambivalent:

Area 4: Hardware and Network Security (HNS)

Security is like an onion

Product security at all levels

The development divisions of hardware producers face great challenges. They are supposed to save time and money while increasing the number of functions and the performance parameters. Companies that do not want to be in the headlines with a data breach or security issue should invest in secure design, i.e., integrate security considerations early in the architecture and planning phase of a project. Product security has many levels. The first is industrial espionage when the competition develops complex, high-profile products. The second are counterfeit products that are manufactured cheaply in Asia, and the third level are liability questions, e.g., if someone uses chip tuning to change the functionality and this modification causes damage. Theobroma cooperates with SBA Research in the development of blueprints for secure hardware, processes and networks. They approach security like an onion: every layer must be secure and reliable. The best software is useless if the data transfer, authentication or hardware are faulty and not secure.

"Theobroma is a design house – similar to an architect's office. We plan and describe a system, we find the right components and suppliers, and take care of everything from validation and certification to production and maintenance processes. We consider the entire life cycle and all operation aspects," explains Philipp Tomsich, CTO and founder of the company. Security in IT is always ambivalent: Too much security can hinder the use of a product, while too little security can cause dramatic vulner-

Zu viel Sicherheit steht der Nutzung im Weg, zu wenig Sicherheit kann zu fatalen Lücken führen. In unserem Alltag werden viele Vorgänge durch Software, die auf eingebetteten Mikrocontrollern und Rechnern abläuft, unterstützt, ohne dass wir dies bewusst wahrnehmen. Embedded Systems, also eingebettete Systeme, steuern und kommunizieren im Lift, im Fahrkartendrucker, im Festplattenrekorder, in der Klimaanlage, der Mautabrechnung, dem E-Card-Terminal. „Wo eine technische Komponente eine Entscheidung für uns trifft, müssen vertrauenswürdige und sichere IT-Komponenten stehen", fügt Tomsich hinzu.

Der intelligente Stromzähler (Smart Meter) ist ein gutes Beispiel. Er hängt beim Verbraucher und kommuniziert automatisch mit dem Energieversorger. Er soll korrekte Daten für die Abrechnung übermitteln. Der Fantasie potenzieller Angreifer sind ebenso wenig Grenzen gesetzt wie der Kreativität der Verbraucher, wenn es um die eigene Haushaltskasse geht. Ein Zähler gibt bei Stillstand indirekt über unsere Abwesenheit Auskunft. Es braucht also einen sicheren Übertragungsweg und verschlüsselte Zählerwerte. Zudem müssen sich Zähler und Zentrale vor der Übermittlung authentifizieren. Dafür haben beide einen Schlüssel, eine Art Parole, die sie gegenseitig austauschen, um aus der Entfernung die Identität des jeweils anderen festzustellen. Diese Schlüssel müssen wiederum gegen unerlaubtes Ablesen und missbräuchliche Verwendung geschützt sein. Zum Manipulationsschutz des Zählers gehört, dass der Schlüssel in der Hardware nicht mehr zugänglich ist, wenn das Gerät geöffnet wird. Ein Erfolgsfaktor dafür ist, die Software so an die Hardware zu koppeln, dass sie nur auf dem Gerät läuft.

abilities. Software on embedded microcontrollers or computers influences many processes in our daily life without us always being aware of it. Embedded systems control and communicate in elevators, ticket vending machines, DVRs, air conditioning systems, tollbooths, or electronic health card terminals. "Wherever a technical component makes a decision for us, we must make sure it is a trustworthy and secure IT component", Tomsich adds.

Sichere Übertragung & Verschlüsselung

Secure transmission & encryption

Smart meters are a good example. The electricity meter is installed in the customer's home and communicates automatically with the energy company. It is supposed to transmit correct data for billing. The creativity of potential attackers is as limitless as the resourcefulness of consumers trying to save on utilities. If the meter is not counting, it indirectly shows that we are not at home. Therefore, data from the meter must be encrypted and transmitted via a secure channel. Both the meter and the central system also have to identify themselves before transmitting. Each has a key, a kind of passphrase that they exchange to verify each other's identity remotely. These keys must, in turn, be protected against unauthorized reading and misuse. One of the meter's protection measures against manipulations is that the key is no longer accessible in the hardware if the device is opened. For this to be successful, the software must be coupled with the hardware so that it can only run on the device.

Together with SBA Research, Theobroma develops blueprints for secure systems and implements the plans so that a tested reference design can be adapted to the individual specifications of the client. Thanks to its international academic network,

Gemeinsam mit SBA Research erarbeitet Theobroma „Baupläne“ für sichere Systeme bis zum getesteten Referenzdesign aus, das auf kundenspezifische Bedürfnisse angepasst werden kann. Durch das internationale akademische Netzwerk ist SBA Research nah an aktuellen Entwicklungen und Best-Practice-Lösungen. „Im Team von SBA Research sitzen unsere Fühler, um akademische Entwicklungen in industrielles Know-how zu überführen“, sagt der Kooperationspartner. Dafür kennt Theobroma die realen Probleme und Anforderungen der Kunden. Gemeinsam gelingt es, die „trade offs“ gut abzuschätzen: Was ist sicher genug? Und auf welche Trends muss man sich vorbereiten?

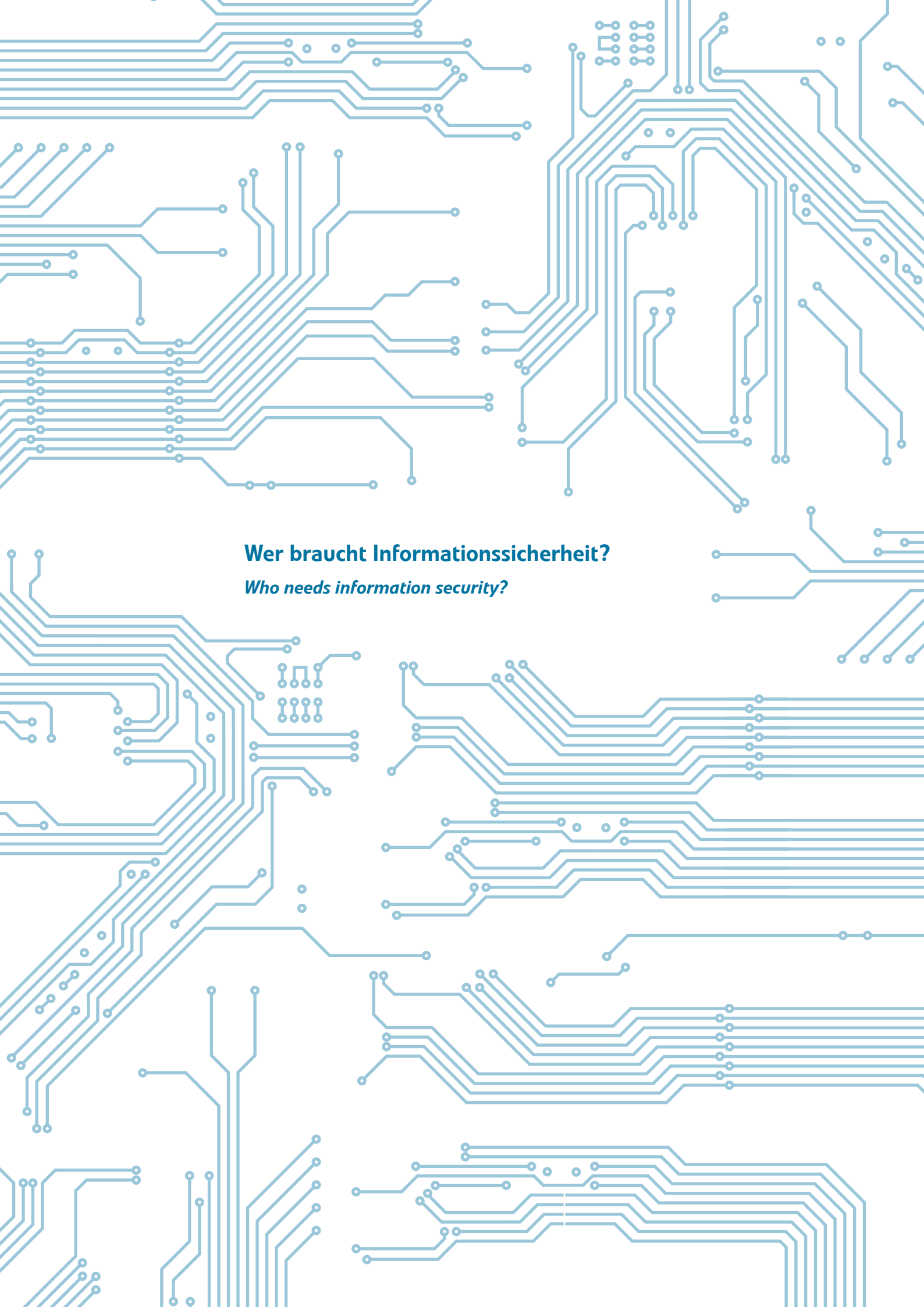
SBA Research is always up to date on new developments and best practices. “The team of SBA Research is our finger on the pulse when it comes to incorporating academic developments into industrial know-how”, Tomsich adds. Theobroma, in turn, is familiar with real-world problems and customer requirements. Together, both successfully evaluate trade-offs: What is secure enough? And which trends should we prepare for?

„Der Schlüssel zur Systemsicherheit ist immer die durchgängige und konsistente Lösung der Sicherheitsanforderungen, weshalb auch Endgerät und Laufzeitumgebung betrachtet werden müssen.”

Dr. DI Philipp Tomsich

Jahrgang 1978, Absolvent der TU Wien, Assistent am Institut für Softwaretechnik und Interaktive Systeme bis 2001, danach im Bereich Engineering für einen Hochleistungscomputerhersteller in den USA, Consulting im Bankbereich und zur sicheren Datenübermittlung im Gesundheitswesen in Österreich und Deutschland tätig, „Vater“ der GINA-Box für die E-Card, gründete 2006 Theobroma Systems mit dem Ziel, die Entwicklung zuverlässiger und vertrauenswürdiger Embedded-Systems-Anwendungen zu vereinfachen.

Born in 1978, Philipp Tomsich studied at TU Vienna and worked as an assistant at the Institute of Software Technology and Interactive Systems until 2001. He then worked in engineering for a high-performance computing manufacturer in the US, in consulting for the banking sector, and as a consultant for secure data transmission in health care in Austria and Germany. He created the ‘GINA box’ for the Austrian electronic health insurance certificate and founded Theobroma Systems in 2006 with the goal of making the development of reliable and trustworthy embedded systems applications easier.



Wer braucht Informationssicherheit?

Who needs information security?

#09 Partner von SBA Research

Partners of SBA Research

Industriepartner

In den Projekten arbeiten Partnerunternehmen gemeinsam mit SBA Research an konkreten Forschungsfragen, Problemstellungen oder neuen Produktideen. So können branchen- oder themenrelevante Lösungen, basierend auf Forschungsergebnissen, entwickelt werden. Wir teilen unsere Partner grob in zwei Kategorien ein:

Security Consumers: Diese müssen ihre sensiblen Daten schützen und haben einen sehr hohen Sicherheitsbedarf.

Andritz Hydro

Die Sparte Hydro der ANDRITZ AG liefert elektromechanische Systeme und Services für Wasserkraftwerke und ist Weltmarktführer für hydraulische Energiegewinnung. SBA Research hat Andritz Hydro bei der Entwicklung einer Sicherheitsarchitektur für ein kritisches Anwendungsfeld unterstützt.

www.andritz.com/hydro

Braincon

Die Braincon Handels GmbH vereint zwei Geschäftsbereiche: Braincard Systems ist ein IT- und Serviceprovider für Chipkarten-Systeme. Der Fokus von ams-braincon Medizintechnik liegt auf digitaler Aufnahmetechnik, Bildbearbeitung und Befundung von Röntgenaufnahmen. Das Chipkarten-System wurde mit SBA Research durch einen neuartigen Architekturansatz zum Schutz von Patientendaten

Research Partners

In our projects, partner companies and SBA Research work together on concrete research questions, issues and new product ideas. This allows us to develop solutions for specific topics or branches of industry that are based on scientific research. We divide our partners into two general categories:

Security Consumers: These need to protect their sensitive data and have a very high security demand.

Andritz Hydro

Andritz Hydro, a part of the ANDRITZ AG group, is a supplier of electro-mechanical systems and services for hydropower plants and is one of the world's leading suppliers for hydraulic power generation. SBA Research assisted Andritz Hydro in developing a security architecture for a critical area of application.

www.andritz.com/hydro

Braincon

Braincon Handels GmbH has two business units: Braincard Systems is an IT and service provider for smartcard systems, while ams-braincon Medizintechnik is a specialist for digital radiography, image processing and x-ray diagnostics. The smartcard system was expanded considerably together with SBA Research with a new design approach for the protection of patient data, increasing the security

wesentlich erweitert, wodurch das Auslesen bzw. Verschlüsseln der gespeicherten Informationen noch sicherer gemacht werden konnte. Die Medizintechnik hält gemeinsam mit SBA Research ein Patent auf eine Pseudonymisierungslösung. Identifizierende Daten von Patienten werden getrennt von Befunden, Behandlungsschemata und Bilddaten elektronisch aufbewahrt, um für Forschung oder Statistik verwendet werden zu können. Diese Anwendungen sind abgewandelt auch für Cloud-Service-Anbieter interessant, damit die Kundin bzw. der Kunde nicht gleich komplett gläsern wird, wenn ein Datenleck auftritt.

www.bct.co.at

Bravestone

Die Bravestone Information-Technology GmbH entwickelt und betreut webbasierte Systeme zur raschen Interaktion von MitarbeiterInnen an verschiedenen Orten. Auf der Plattform können Texte, Grafiken, Bilder etc. gemeinsam bearbeitet werden. Eine kritische Kernfunktionalität der Datenbanklösung ist die verlässliche Nachvollziehbarkeit der Aktionen verschiedener BenutzerInnen.
In einem gemeinsamen Projekt arbeitet Bravestone mit SBA Research an einem automatisierten Textanalyseprogramm für Ermittlungsbehörden. SBA Research zeichnet für die Verbesserung der Funktionalität des Programms als Vorbereitung für tiefer gehende forensische Analysen verantwortlich.

www.bravestone.at

of readout and encryption of the stored information. The medical technology unit and SBA Research hold a joint patent for a pseudonymization solution. Identifying patient data is stored electronically separately from diagnostic findings, treatment plans and images so that these can be used for research or statistics. With some modifications, these applications are also useful for cloud service providers to prevent all customer data being compromised in the event of a data leak.

www.bct.co.at

Bravestone

Bravestone Information Technology GmbH develops and supports Web-based systems that allow employees at different locations to interact fully. On the platform, they can work on texts, graphics, images, etc. together. A critical core functionality of the database solution is that every user's actions are documented.
In a joint project with SBA Research, Bravestone is working on an automated text analysis program for investigative authorities. SBA Research was in charge of improving the functionality of the program as preparation for deeper forensic analyses.

www.bravestone.at

Bundesrechenzentrum

Die Bundesrechenzentrum GmbH ist der IT-Dienstleister der Österreichischen Bundesverwaltung. Sie verfügt über eines der größten Rechenzentren Österreichs und entwickelt, implementiert und betreibt erfolgreich E-Government-Lösungen. Zentrale Aufgabe ist der Schutz der Vertraulichkeit und Integrität sowie die Sicherstellung der Verfügbarkeit der ihr anvertrauten Verwaltungsdaten.

www.brz.gv.at

Factline

factline beschäftigt sich mit dem Potenzial des Internets als verlässliches Aktionsmedium für verteiltes Arbeiten und E-Learning. Das Unternehmen arbeitet an der umfassenden Referenzierbarkeit, Integration und Unveränderbarkeit von Online-Inhalten. Für den Baubereich hat factline gemeinsam mit SBA Research und anderen Partnern einen Prototypen entwickelt, mit dem zeitkritische Veränderungen im Bereich Projektstruktur und –planung verlässlich ausgesandt und die Kenntnisnahme durch die Partnerunternehmen nachvollziehbar aufgezeichnet werden. So bleiben ineinandergreifende und aufeinanderfolgende Bauphasen bei Umplanungen beherrschbar und etwaige Schuldfragen sind bei Verzug eindeutig beantwortbar. Nach Ende des Bauprojekts halten die künftigen Mieter gleich eine Dokumentation des Bauwerks in Händen, in die die letztgültigen Pläne eingespeist sind.

www.factline.com

Bundesrechenzentrum

Bundesrechenzentrum GmbH, the Austrian Federal Computing Centre, is the IT service provider for the Austrian federal administration. It is one of the largest computing centers in Austria and successfully develops, implements, and operates e-government solutions. Their core responsibilities are protecting the confidentiality and integrity and ensuring the availability of administrative data entrusted to them.

www.brz.gv.at

Factline

Factline's focus is the potential of the Internet as a reliable medium for distributed working and e-learning. The company focuses on comprehensive referenceability, integration and on making online content unchangeable. Factline, along with SBA Research and other partners, developed a prototype for the building sector that reliably mails out time-critical changes in project structure and project planning and records that the partner companies have read the information. This allows the management of interdependent and consecutive construction phases in the event of changes and clearly shows who is responsible should there be delays. After construction is completed, the future tenants receive a documentation of the building that contains the final plans.

www.factline.com

Gekko it-solutions GmbH

Gekko ist ein 1997 gegründetes IT-Dienstleistungs- und -Beratungsunternehmen und entwickelt im Rahmen einer Forschungskooperation mit SBA Research für klein- und mittelständische Unternehmen eine Lösung auf Basis von Microsofts „Azure"- Cloud-Technologie. Dabei sind die Erarbeitung eines adäquaten Sicherheitskonzepts sowie die Überprüfung der Lösungsansätze in Bezug auf die Informationssicherheit zentrale Aspekte. SBA Research trägt Expertise in den Bereichen Cloud-Sicherheit und System- und Softwaresicherheit zur gemeinsamen Forschung bei.

www.gekko.at

GIBODAT

GIBODAT hat sich auf EDV-Lösungen für die Sozialwirtschaft spezialisiert. Mit dem Produkt CareCenter wird eine Software-Gesamtlösung für stationäre Einrichtungen, Behinderteneinrichtungen, Reha- und Kureinrichtungen sowie ambulante Dienste angeboten. SBA Research hat GIBODAT bei der Implementierung einer SmartCard-Lösung für ein E-Health-System unterstützt.

www.gibodat.at

Gesundheit Österreich GmbH

Die Gesundheit Österreich GmbH (GÖG) wurde als nationales Forschungs- und Planungsinstitut für das Gesundheitswesen sowie Kompetenzzentrum und Förderstelle zur Gesundheitsförderung errichtet. Die GÖG entwickelte ein Informationssystem für gesundheitsrelevante Planung. SBA Research hat sich mit

Gekko it-solutions GmbH

Gekko was founded in 1997. It is an IT service and consulting company and is currently developing a solution for small and medium-sized enterprises based on Microsoft's 'Azure' cloud technology in a research cooperation project with SBA Research. Core aspects of this solution are the development of an adequate security concept and the examination of possible solutions with regard to information security. SBA Research contributes its expertise in the areas of cloud security and systems as well as software security to the joint research project.

www.gekko.at

GIBODAT

GIBODAT specializes in IT solutions for the social sector. Their CareCenter product is a one-stop package solution for in-patient facilities, facilities for people with disabilities, medical and physical rehabilitation facilities and out-patient services. SBA Research supported GIBODAT in the implementation of a smartcard solution for an e-health system.

www.gibodat.at

Gesundheit Österreich GmbH

Gesundheit Österreich GmbH (GÖG) was established as a national research and planning institute for health care and as a competence and funding center for health promotion. GÖG developed an information system for health planning.

Visualisierungs- und Standardisierungskompetenz eingebracht, da das Produkt auch in andere Länder verkauft werden soll. Sensible Register der Gesundheit Österreich wurden architektonisch und konzeptionell völlig neu entworfen, um noch höheren Sicherheitsanforderungen zu genügen.

www.goeg.at

SBA Research contributed its visualization and standardization expertise, as the product is designed to be marketed in other countries as well. Sensitive registers of Gesundheit Österreich were completely re-designed in terms of architecture and concept in order to meet even higher security requirements.

www.goeg.at

Hewlett-Packard

HP Österreich, Tochter des globalen Technologieunternehmens, hat mit banqpro/ eine Branchenlösung für Finanzunternehmen im Programm. Als Generalunternehmer liefert HP Software, Hardware, Implementierung, Schulung und Wartung des Kernbankensystems. Die Lösung umfasst Module für diverse Geschäftsbereiche (Wertpapiere, Zahlungsverkehr, Auslandsgeschäft, Spareinlagen, Rechnungswesen) und Customer Relationship Management. Dem Privatbankenbereich steht damit ein individuelles Paket zur Verfügung, das sich in die Aufgabenlandschaft einbettet, ohne Ballast mitzuführen. banqpro/ wurde anlässlich eines neuen Architekturentwurfs der Gesamtlösung gemeinsam mit SBA Research auf Herz und Nieren geprüft und zu einem noch zuverlässigeren integrierten Front- und Backofficesystem ausgebaut.

www.hp.com/at

Hewlett-Packard

HP Austria, a subsidiary of the global technology company, offers a solution for the financial sector, banqpro/. As general contractor, HP provides software, hardware, implementation, training and maintenance of the core banking system. The solution includes modules for various business areas (securities, payments, foreign operations, personal savings, accounting) and customer relationship management. It provides a tailored package for private banking, which meets the needs without providing unnecessary functionalities. In the process of a new architecture concept for the overall solution, SBA Research was involved in testing banqpro/ extensively and making it an even more reliable and integrated front and back office system.

www.hp.com/at

LG Nexera Business Solutions AG

LG Nexera entwickelt Softwarelösungen für Unternehmen mit MitarbeiterInnen im Außendienst via BlackBerry und anderen mobilen Geräten. Nach dem Motto „immer und überall" werden Lösungen

LG Nexera Business Solutions AG

LG Nexera develops software solutions for companies with field employees to communicate via BlackBerry and other mobile devices. This includes solutions for time management, activity recording, photo documentation, task scheduling, project management, dispatching, work schedules, cloud

für die Bereiche Zeit- und Leistungserfassung, Fotodokumentation, Auftragsvergabe, Projektmanagement, Disposition, Dienstpläne, Cloud Working und Lohnverrechnung erstellt. Da Produkte in verschiedene Länder verkauft werden, stellte SBA Research sicher, dass Funktionalitäten des Programms je nach Gesetzeslage zuverlässig aktiviert oder deaktiviert werden können. Da die Daten mehrerer Kunden über LG-Nexera-Systeme laufen, muss sichergestellt werden, dass beim Login nur Daten des eigenen Unternehmens einsehbar sind. Die ordnungsgemäße Datentrennung ist für alle Firmen, die Cloud Services anbieten, ein wichtiges Thema.

www.lgsoft.at

Österreichische Computer Gesellschaft (OCG)

Die Österreichische Computer Gesellschaft (OCG) ist ein 1975 gegründeter gemeinnütziger Verein zur Förderung der Informationstechnologie unter Berücksichtigung ihrer Auswirkungen auf Mensch und Gesellschaft. Der Verein unterstützt die Arbeit von Informatikerinnen und Informatikern u. a. mit fachlichem Austausch und Publikationen, Förderung des wissenschaftlichen Nachwuchses, Weiterbildung, internationalen Forschungs- und Lehraufträgen und internationaler Vernetzung (z. B. ERCIM). Für die OCG hat SBA Research das OCG-Security-Zertifikat – eine Schulung zum Thema IT-Sicherheit nach dem Muster des ECDL-Computerführerscheins – entwickelt und sorgt so für eine weitere Verbreitung von Basiswissen über Informationssicherheit.

www.ocg.at

working, and payroll accounting. As the company sells its products internationally, SBA Research ensured that individual functions of the program can be reliably activated or deactivated depending on local laws. As LG Nexera systems host the data of multiple customers, it is crucial to ensure that each customer can only see their own company's data when they log in. Keeping customer data separate is an important issue for all cloud service providers.

www.lgsoft.at

Austrian Computer Society (OCG)

The Austrian Computer Society (OCG) was founded in 1975 and is a non-profit association for the promotion of information technology with due regard for its effects on humans and society. The association supports the work of computer scientists through forums for exchange of knowledge and publications, the promotion of young scientists, training courses, international research and teaching positions, and its international ties (e.g., ERCIM). SBA Research developed the OCG Security Certificate with OCG, which is an IT security training and certification measure similar to the European Computer Driving Licence (ECDL), contributing to the dissemination of basic IT security knowledge.

www.ocg.at

Parlamentsdirektion

Die Mitarbeiterinnen und Mitarbeiter der Parlamentsdirektion garantieren den reibungslosen Ablauf des parlamentarischen Geschehens und unterstützen die gesetzgebenden Organe des Bundes sowie die österreichischen Abgeordneten zum Europäischen Parlament. Dazu gehört die IT-Bereitstellung und die umfangreiche Webseite des Parlaments. SBA Research unterstützt die IT-Fachleute in spezifischen Informationssicherheitsfragen.

www.parlament.gv.at

ProCom Strasser – Werner Strasser e.U.

ProCom Strasser entwickelt Software für die Bereiche Textsuche und Analyse, zum Steuern von Geschäftsprozessen, dem Teilen/Bearbeiten/Verwalten von Dokumenten sowie für Telekonferenzen und virtuelle Besprechungs- und Konferenzräume. In den letzten Jahren wurden gemeinsam sehr spezielle Sicherheitsfragen bearbeitet. Für eine patentierte Biodieselanlage, die auch ohne autonome Stromversorgung und Netzwerkverbindung funktionieren soll, hat SBA Research gemeinsam mit ProCom Strasser eine Steuerungssoftware mit kombiniertem Software- und Hardware-Kopierschutz konzipiert und prototypisch entwickelt.

www.procom-strasser.com

SVA

Die Sozialversicherungsanstalt der gewerblichen Wirtschaft ist die Sozialversicherung für Unternehmerinnen und Unternehmer in Österreich. 2007 durchleuchtete die SVA mit SBA Research ausgesuchte Geschäftsprozesse auf ihre Sicherheits-

Austrian Parliamentary Administration

The staff of the Parliamentary Administration ensures the smooth running of parliamentary business and supports the federal legislative bodies and the Austrian Members of the European Parliament. This includes providing IT and managing the large website of the Austrian Parliament. SBA Research supports the in-house IT specialists with specific information security questions.

www.parlament.gv.at

ProCom Strasser – Werner Strasser e.U.

ProCom Strasser develops software for text retrieval and analysis, management of business processes, document sharing, processing and management, remote conferences and virtual meeting and conference rooms. In the last years, SBA Research and ProCom Strasser cooperated on some very specific security questions. Together, they designed and prototyped a control program with a combined software and hardware copy protection for a patented biodiesel plant that will work with autonomous power supply, without access to the grid.

www.procom-strasser.com

SVA

The Austrian Social Insurance Authority for Business (SVA) is the insurance provider for entrepreneurs. In 2007, SBA Research assisted SVA in analyzing selected business processes to determine their security relevance. We were able to develop the best-suited organizational principles with the help of models and simulations. The objective was to find the right balance between the cost of security measures and possible financial damage.

relevanz. Mit Hilfe von Modellen und Simulationen konnten die am besten geeigneten organisatorischen Prinzipien entwickelt werden. Es ging um die richtige Balance zwischen den Kosten der Sicherheitsmaßnahmen und denen eines möglichen finanziellen Schadens selbst. Sicherheitsrelevante Prozesse in Geschäftsprozesse zu integrieren ist eine Kernberatungstätigkeit von SBA Research. Jede eingeführte Regelung – etwa zur Vertraulichkeit von Informationen im E-Mail-Verkehr – hat Auswirkungen, die vorher abgeschätzt und abgewogen werden sollten.

esv-sva.sozvers.at

Theobroma Systems

Theobroma Systems ist Anbieter für Embedded Systems. Das Unternehmen entwickelt und designt schlüsselfertige, individuelle Lösungen mit Hardware, Software und Serververwaltung für Hochsicherheits-Anwendungen (E-Card, Smart Meter, Verkehrssteuerung ...). Mit Beratung und Prüfung durch SBA Research werden Hardware, Datenbanken und Kommunikationswege fit für den Austausch in einer Umgebung gemacht, in der Missbrauch oder Manipulation stattfinden kann. Des Weiteren unterstützt SBA Research Theobroma bei verschiedenen speziellen Sicherheitsfragen. SBA Research kann im Gegenzug auf ein exzellentes Hardware-Spezialwissen für die gemeinsame Forschungsarbeit zurückgreifen.

www.theobroma-systems.com

Integrating security-critical processes into business processes is one of the core consulting activities of SBA Research. Every new regulation – such as confidentiality of information in e-mails – has consequences that should be assessed and calculated in advance.

esv-sva.sozvers.at

Theobroma Systems

Theobroma Systems is a provider of embedded systems solutions. The company develops and designs tailored turnkey solutions with hardware, software and server administration for high-security applications (e-card, smart meters, traffic control, etc.). SBA Research provides consulting and checks systems to prepare hardware, databases and communication channels for environments where misuse or manipulation can take place.
SBA Research also supports Theobroma in dealing with various specialized security questions. In return, SBA Research benefits from Theobroma's excellent hardware knowledge in our joint research work.

www.theobroma-systems.com

UC4 (vormals Senactive)

UC4 ist ein Software-Provider für Automatisierungstechnologie. In den Systemen werden sämtliche Vorfälle in der Steuerung von Ventilen, Alarmanlagen oder auch Freigabeprozeduren in Logfiles abgespeichert. Die systematische Auswertung der aufgezeichneten Vorfälle ermöglicht das Aufspüren von Anomalien, die für IT-Sicherheit relevant sein können. Mit einem eigenen Programm wird die Suche nach Fehlern und Zusammenhängen oder Abfolgen von Vorfällen grafisch aufbereitet. So können falsche Einstellungen rasch korrigiert oder Neudefinitionen von Prozessen übernommen werden. SBA Research war an den Forschungs- und Entwicklungsarbeiten des Event-Management-Systems federführend beteiligt. UC4 und SBA Research konnten hervorragende gemeinsame Publikationen zu diesem Thema herausbringen.

www.uc4.com

Vertretungsnetz

Der überparteiliche und gemeinnützige Verein Vertretungsnetz stellt den Bezirksgerichten ausgebildete SachwalterInnen, PatientInnenanwälte und BewohnerInnenvertreter zur Verfügung. Diese VertreterInnen sind in ganz Österreich unterwegs und greifen bei der Arbeit auf zentrale Daten zu. Die Dokumentationen und Begründungen der Vertretungsfälle sind als sensible Daten einzustufen. SBA Research verbessert die Archivierung, den Zugriff, die Verschlüsselung und den Datenaustausch.

www.vsp.at

UC4 (formerly Senactive)

UC4 is a provider of automation technology software. The systems log any incidents with valve control, alarm systems or enable signals. The systematic analysis of the logged incidents makes it possible to detect anomalies that might be relevant for IT security. The errors, correlations and sequences of incidents found in the analysis are visualized with a special program so that wrong settings can be corrected or new process definitions can be applied. SBA Research was heavily involved in the research and development of the event management system. UC4 and SBA Research have written excellent joint publications on the topic.

www.uc4.com

Vertretungsnetz

The nonpartisan not-for-profit association Vertretungsnetz provides professional legal guardians, patient advocates and nursing home residents' advocates at district courts. These advocates travel across Austria and need to access data on a central server for their work. The documentations and statements of grounds for their cases are considered sensitive data. SBA Research improves archiving, access control, encryption and data exchange for Vertretungsnetz.

www.vsp.at

Security Providers: Entwickeln selbst IT-Security-Dienstleistungen oder -Produkte und haben auf dem Weg zu neuen Märkten noch Forschungsbedarf.

A1 Telekom

Die Tochter der Telekom Austria Group stellt Sprachtelefonie, Daten- & IT-Lösungen, Internet und Media sowie Lösungen für Home & Office zur Verfügung. SBA Research hat für das führende Telekommunikationsunternehmen im CEE-Raum die Entwicklung von Sicherheitsarchitekturen für innovative Anwendungsbereiche unterstützt.

www.a1.net

anovis IT-Security

Anovis IT-Security bietet die Betreuung von Firewalls von der Architektur bis zum 24-Stunden-Managed-Service an. Die installierten Firewalls bei den Firmenkunden liefern große Datenmengen zu den Verbindungen, deren Analyse und Auswertung gemeinsam mit SBA Research echtzeitnah umgesetzt wurde. So kann Anovis sich schnell einen Überblick über den Status seiner Dienste verschaffen und rasch reagieren.

www.anovis.com

avedos™ business solutions

avedos™ bietet Lösungen im Bereich Governance, Risk und Compliance Management (GRC). Die Softwareprodukte ermöglichen es, die Anforderungen gegenüber Aufsichtsbehörden, KundInnen, Arbeit-

Security Providers: These partners develop IT security services or products and have a need for research to help them enter new markets.

A1 Telekom

The subsidiary of Telekom Austria Group provides voice telephony, data and IT solutions, Internet and media, and home & office solutions. SBA Research supported this leading telecommunications company of the CEE area in the development of security architectures for innovative application areas.

www.a1.net

anovis IT-Security

Anovis IT security provides support for firewalls from architecture to 24/7 managed services. The firewalls installed at the client companies provide a large amount of data on the connections, whose near real-time analysis and evaluation SBA Research implemented together with anovis. This shows anovis the status of its services at a glance, allowing it to respond quickly.

www.anovis.com

avedos™ business solutions

avedos™ provides solutions for governance, risk and compliance management (GRC). The software products allow clients to manage and synchronize the requirements of regulatory bodies, customers, employees, etc. In 2009, we fully revised the organizational and technological aspects of the main project 'risk2value' together. Avedos tightened the

nehmerInnen etc. geordnet einzuhalten und abzugleichen. Das Hauptvorhaben „Risk2value“ wurde 2009 gemeinsam organisatorisch und technologisch vollständig überarbeitet. Avedos schärfte die Programmanforderungen in Einklang mit den Bedürfnissen der Kunden nach. SBA Research sorgte mit einer runderneuerten Programmierung und Konzeption im Bereich GRC-Management in Zusammenarbeit mit anderen Forschungspartnern für einen neuen Prototypen, der auch für zukünftige Anwendungserweiterungen ideal vorbereitet ist.

www.avedos.com

CYAN Networks Software GmbH

CYAN Networks Security kümmert sich mit Proxy Technology und Web Filtering Solutions um Web-Security für Unternehmen. Mit SBA Research arbeitet die Firma daran, Technologien für neue Herausforderungen, die sich durch die intensive Nutzung von Smartphones sowie durch Social-Media-Inhalte ergeben, zu entwickeln.

www.cyan-networks.com

nic.at/CERT.at

nic.at ist die zentrale Registrierungs- und Verwaltungsstelle der österreichischen Top-Level-Domain (.at) und vertritt die Interessen der österreichischen Internet-Community in internationalen Gremien. Das nationale Computer Emergency Response Team (CERT) ist eine Initiative von nic.at. Als Ansprechpartner für IT-Sicherheit im nationalen Umfeld gibt es

program requirements in keeping with its customers' needs. Together with other research partners, SBA Research completely overhauled the programming approach and GRC management concept to create a new prototype that is also ideally suited for possible future expansions of its applications.

www.avedos.com

CYAN Networks Software GmbH

CYAN Networks Security uses proxy technology and Web filtering solutions to provide Web security for businesses. With SBA Research, the company develops technologies for new challenges that arise from the widespread use of smartphones and from social media content.

www.cyan-networks.com

nic.at/CERT.at

nic.at is the central registry operator and administrator of the Austrian top-level domain (.at) and represents the Austrian Internet community in international bodies. The national Computer Emergency Response Team (CERT) is an initiative of nic.at. It is the primary contact partner for IT security in Austria and issues warnings, alerts and advice for SMEs. In the case of attacks against infrastructure, CERT.at will provide information and coordinate the response at national level. SBA Research staff frequently support CERT.at with their expert knowledge on current topics of IT security, networking and the exchange of know-how between stakeholders.

Warnungen, Alerts und Tipps für KMUs heraus. Bei Angriffen auf Rechner koordiniert und informiert CERT.at auf nationaler Ebene. SBA Research-MitarbeiterInnen unterstützen CERT.at laufend als Fachleute bei aktuellen Themen der IT-Sicherheit, bei Vernetzung und beim Austausch von Know-how unter den Betroffenen. Nach der raschen CERT.at-Warnung vor Phishing-Attacken, Schadprogrammen etc. werden deren technische Hintergründe aufgearbeitet, um sie kurzfristig zu beseitigen und langfristig zu verhindern.

www.cert.at

R-IT

Raiffeisen Informatik verfügt als IT-Dienstleister einer großen österreichischen Bankengruppe über mehr als 40 Jahre Erfahrung. IT- und Software-Dienstleistungen werden vor diesem fachlichen Hintergrund auch für andere Großkunden erbracht. SBA Research arbeitet seit mehr als fünf Jahren intensiv mit dem Security Competence Center (SCC) der R-IT in Zwettl zusammen. Gemeinsam wurden spannende Forschungsthemen im Informationssicherheitsbereich adressiert und bearbeitet. Z. B. hat SBA Research mit R-IT einen Softwareprototypen für die automatische Verarbeitung und Reihung von Hersteller-Warnmeldungen (Advisories) erarbeitet. Wenn ein Hersteller oder Institutionen wie etwa CERT.at eine Schwachstelle für ein Produkt finden und melden, wird vom Programm abgeglichen, ob das betreffende Produkt in den betroffenen

Following a rapid CERT.at warning about phishing attacks, malware, etc., their technical features are examined in order to remove them in the short term and prevent them in the long term.

www.cert.at

R-IT

Raiffeisen Informatik is the IT service provider of a large Austrian banking group and has over 40 years of experience in the field. Due to this background, it also provides IT and software services for other major customers. For over five years, SBA Research has been cooperating closely with the Security Competence Center (SCC) of R-IT in Zwettl. Together, we have addressed interesting topics in information security research. One example is a software prototype for the automated processing and sequencing of product advisories that SBA Research developed with R-IT. When software providers or institutions like CERT.at find and report a vulnerability in a product, the program analyses whether that product and the affected versions are in use in the system. Subsequently, it evaluates and orders the messages by status and sends an automatic notice to the administrators in charge. Thanks to this system, the administrators no longer need to evaluate each advisory individually and can instead focus on the truly relevant problems and their solutions.

www.raiffeiseninformatik.at

Versionen verwendet wird. Anschließend werden die Meldungen nach ihrem Status beurteilt und gereiht sowie automatisch eine Verständigung an die zuständigen Administratoren verschickt. Diese müssen nicht mehr jedes Advisory einzeln studieren, sondern können sich auf die für sie wirklich relevanten Probleme und deren Lösung konzentrieren.

www.raiffeiseninformatik.at

Security Research Sicherheitsforschung GmbH

Security Research arbeitet forschungsnah in den Bereichen IT-Sicherheitsberatung, Schulung, Prozessberatung sowie kontrollorientiertes Prozessdesign in Unternehmen. Der mit SBA Research designte IS-Control-Point-Prototyp unterstützt die Dokumentation von Compliance-Prozessen im Rahmen von ISO-27001-Zertifizierungen und -Audits. So bleiben Protokolle, Updates, Zuständigkeiten und Checklisten stets aktuell und abrufbar und der Prozess der beständigen Erneuerung nach Audits wird nachvollziehbar.

www.securityresearch.at

The Last Line of Defense (TLLOD)

The Last Line of Defense wurde als Spin-off von TU-Absolventen in den USA gegründet. Im Austausch mit SBA Research entwickelt die Firma eine Art umgekehrte Firewall. Sie konzentriert sich auf ausgehende Verbindungen und prüft, ob Kontakte zu Botnets aufgebaut werden. Es wird eine Liste

Security Research Sicherheitsforschung GmbH

Security Research provides research-oriented services in IT security consulting, training, process consulting, and control-oriented process design in businesses. SBA Research was involved in designing the IS Control Point prototype, which supports the documentation of compliance processes in ISO 27001-certification processes and audits. This keeps protocols, updates, responsibilities and checklists up to date and accessible and documents the process of continuous renewal after audits.

www.securityresearch.at

The Last Line of Defense (TLLOD)

The Last Line of Defense is a spin-off founded by TU Vienna graduates in the US. In constant exchange with SBA Research, the company is developing a kind of reverse firewall. It monitors outgoing traffic and checks whether the computer connects to botnets. It assembles a list of target IPs and defines behaviors of botnet connections. While this does not prevent infection, data can no longer be sent outside and new commands from a command and control server cannot get into the company network.

www.tllod.com

von Zieladressen (IP-Adressen) erstellt bzw. werden Verhaltensmuster für Botnet Connections definiert. So wird zwar nicht die Infizierung verhindert, Daten können aber nicht nach außen geschickt und neue Befehle von einem Command-and-Control-Server nicht in das Firmennetzwerk abgesetzt werden.

www.tllod.com

XiTrust

XiTrust, mit Sitz in Graz und Wien, strafft Unternehmensprozesse durch den Einsatz von Spezial-Software. Zeitstempel, Verschlüsselung, Signaturen, Archivsignaturen oder E-Government-Anwendungen können als Module über den Business-Server punktgenau in bestehende IT-Landschaften integriert werden. Die Kombination zu sinnvollen Workflows sowie Erweiterungen sind jederzeit möglich. Mit SBA Research wurde das Produkt verbessert, indem die Protokolle und Umgebungen der sicherheitsrelevanten Anwendungen durchleuchtet und aufeinander abgestimmt wurden. Die Verbesserung muss an beiden Positionen erfolgen: Eine gute Information in einer schlechten Umgebung ist ebenso ungünstig wie ein schlechter Input in einer guten Umgebung. Wer Rechtsverbindlichkeit und Authentizität gewährleisten will, sichert sich in jede Richtung ab.

www.xitrust.com

XiTrust

XiTrust, which has offices in Graz and Vienna, streamlines business processes through the use of special software. Time stamps, encryption, signatures, archive signatures and e-government applications are available as modules that can be integrated in a precise manner into existing IT environments via the business server. Clients can combine several modules to create workflows or expand their system at any time. Together with SBA Research, the product was improved by examining and harmonizing the protocols and environments of the security-relevant applications. Improvements are always necessary on both sides: Good information in a bad environment is just as problematic as bad input in a good environment. If you want to guarantee legal force and authenticity, it is best to protect yourself in every aspect.

www.xitrust.com

Universitäre Partner

Mit dem Forschungszentrum für IT-Sicherheit bearbeiten ForscherInnen von verschiedenen Fakultäten in Österreich gemeinsam grundlegende Fragestellungen und veröffentlichen die Ergebnisse in wissenschaftlichen Journalen und Konferenzbeiträgen. Mit Universitäten im Ausland wird der internationale Transfer von Know-how durch Summer Schools, Fachkonferenzen und Austauschprogramme bewerkstelligt.

TU Wien / ISIS

Das Institut für Softwaretechnik und Interaktive Systeme (ISIS) der Technischen Universität Wien rund um den SBA Research-Gründer Prof. A Min Tjoa forscht zu den Themen Informations- und Software-Engineering, Quality Engineering, IT-Security und Prozess-Management.

www.isis.tuwien.ac.at

TU Graz / IAIK

Die Technische Universität Graz mit ihrem Institut für angewandte Informationsverarbeitung und Kommunikation (IAIK) konzentriert sich auf die Bereiche Kryptografie, sichere Transport- und Kommunikationsprotokolle und Hardwaresicherheit. Entwicklungen der TU Graz trugen zum Spitzenplatz Österreichs in der Verbreitung von E-Government-Lösungen bei.

www.iaik.tugraz.at

University Partners

Together with the research center for IT security, researchers from different university departments in Austria jointly research fundamental questions and publish their results in scientific journals and conference proceedings. We cooperate with universities abroad to facilitate international knowledge transfer through summer schools, conferences and exchange programs.

TU Vienna / ISIS

The Institute of Software Technology and Interactive Systems at the Vienna University of Technology, headed by SBA Research co-founder A Min Tjoa, researches information and software engineering, quality engineering, IT security, and process management.

www.isis.tuwien.ac.at

TU Graz / IAIK

The Institute for Applied Information Processing and Communications (IAIK) at the Graz University of Technology focuses on cryptography, secure transport and communication protocols, and hardware security. Solutions developed at TU Graz contributed to Austria's top position in a benchmarking report on the availability of e-government services.

www.iaik.tugraz.at

WU Wien / NM

Das Institut für Informationssicherheit und neue Medien (NM) der Wirtschaftsuniversität Wien stellt die Architektur von Informationssystemen, Software Engineering und Application Engineering in den Mittelpunkt. Der Fokus liegt auf flexiblem Security and Workflow Management, skalierbaren Frameworks und webbasierten Systemen für E-Learning und Information Retrieval.

nm.wu-wien.ac.at

Uni Wien / DKE

Das Department of Knowledge Engineering (DKE) der Universität Wien beschäftigt sich mit IT-vermitteltem Prozess-Management und Optimierung sowie Wissens-Management-Lösungen.

www.dke.univie.ac.at

WU Wien / NM

The Institute for Information Systems and New Media (NM) at the Vienna University of Economics and Business focuses on information systems, software engineering, and application engineering. The main emphasis is on flexible security and workflow management, scalable frameworks and Web-based systems for e-learning and information retrieval.

nm.wu-wien.ac.at

University of Vienna / DKE

The Department of Knowledge Engineering (DKE) at the University of Vienna researches IT-mediated process management and optimizations and devel-ops knowledge management solutions.

www.dke.univie.ac.at

Akademische Kooperationen *Academic Cooperation*

Purdue University

Gene Spafford gründete 1999 das weltweit anerkannte Security-Ausbildungs- und Forschungszentrum CERIAS (Center for Education and Research in Information Assurance and Security) am Campus der Purdue University (Indiana). Spafford war auch im Organisationskomitee der ARES-Konferenz aktiv. Das Zentrum wirbt Gelder ein und bündelt und koordiniert Forschungsaktivitäten zum Thema Informationssicherheit quer über alle Fachrichtungen der Universität. Mit CERIAS wird der fachliche Austausch auch über SBA-Nachwuchswissenschaftlerlnnen gepflegt.

www.cerias.purdue.edu

Purdue University

In 1999, Gene Spafford founded the internationally recognized Center for Education and Research in Information Assurance and Security (CERIAS) on the campus of Purdue University, Indiana. Spafford was a member of the organizing committee of the ARES conference.

The center secures funding and coordinates research activities in information security across all departments of the university. In addition to other information exchange with CERIAS, young SBA researchers also have the opportunity to conduct research there.

www.cerias.purdue.edu

TU Darmstadt / Security Engineering Group (SecEng)

Die Security Engineering Group von Professor Stefan Katzenbeisser will die Lücke zwischen theoretischen Ansätzen von Informationssicherheit (Kryptografie, Software Engineering oder Zugangskontrollen) zu realen Systemen überbrücken. Die Fachleute entwickeln Methoden für Design und Analyse von sicheren Systemen anhand einfacher technischer Elemente und Bausteine. Prof. Katzenbeisser betreut SBA-Nachwuchswissenschaftlerlnnen.

www.seceng.informatik.tu-darmstadt.de

TU Darmstadt / Security Engineering Group (SecEng)

Professor Stefan Katzenbeisser's Security Engineering Group aims at bridging the gap between the theoretical approaches to information security (such as cryptography, software engineering, access control) and real-world systems. The experts develop methods for the design and analysis of secure systems using primitives and building blocks. Professor Katzenbeisser also mentors young SBA researchers in research projects.

www.seceng.informatik.tu-darmstadt.de

Uni Regensburg / Lehrstuhl Wirtschaftsinformatik I – Informationssysteme

Professor Günther Pernul von der Fakultät für Wirtschaftswissenschaften stellt Informationssysteme in den Mittelpunkt von Lehre und Forschung. Ihr Einsatz bringt gesteigerte Komplexität, die Abhängigkeit vom einwandfreien Funktionieren und das Bedürfnis nach Sicherheit und Verlässlichkeit mit sich. Prof. Pernul arbeitet zum Thema Zugriffskontrolle und ist Mitglied des wissenschaftlichen Rats von SBA Research, der die wissenschaftliche Qualität überwacht und den Austausch über aktuelle Forschungsfelder fördert. Er ist Gründer und Mitorganisator der IPICS-Schools (Intensive Program on Information Communication Security).

www-ifs.uni-regensburg.de

Eurecom

Das Eurecom-Foschungszentrum in der Technopole Sophia Antipolis (Frankreich) verfolgt die Themen Networking and Security, Multimedia Communications und Mobile Communications. Die Ausrichtung der kleinen, dynamischen Ausbildungsstätte für Ingenieurinnen und Ingenieure ist international, industrienah und hat einen hervorragenden Ruf. Assistant Professor Davide Balzarotti ist Mitglied des wissenschaftlichen Rats von SBA Research. Engin Kirda, heute an der Northeastern University in Boston, ist Key Researcher für den Bereich Malware und betreut einige Dissertationen bei SBA Research.

www.eurecom.fr

University of Regensburg / Chair of Information Science I – Information Systems

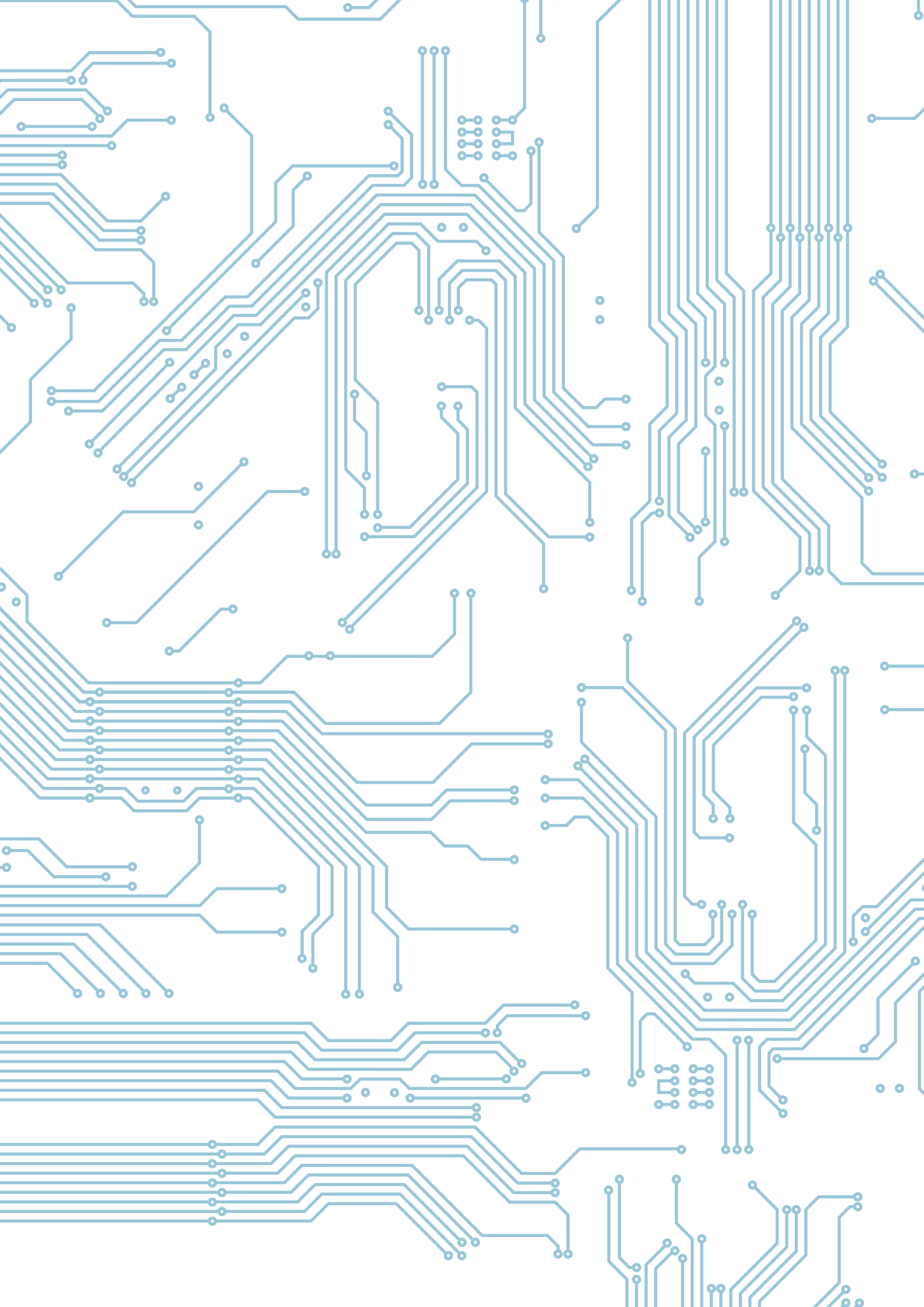
Professor Günther Pernul at the Department of Business focuses on information systems both in teaching and in research. Their use increases the level of complexity and creates a dependence on their flawless functioning and a need for security and reliability. Professor Pernul's research interest is access control and he is a member of the Scientific Board of SBA Research, which reviews the quality of the center's scientific work and promotes exchange on current research topics. He is the founder and co-organizer of the IPICS schools (Intensive Program on Information Communication Security).

www-ifs.uni-regensburg.de

Eurecom

The main fields of research of the Eurecom research center in the technopolis Sophia Antipolis (France) are networking and security, multimedia communications, and mobile communications. This small and dynamic engineering school is very international, has good industry ties and an excellent reputation. Assistant Professor Davide Balzarotti is a member of the Scientific Board of SBA Research. Engin Kirda, who is currently at Northeastern University, Boston, is Key Researcher for malware and the supervisor of several dissertations at SBA Research.

www.eurecom.fr



Wie kann Informationssicherheit gelingen?

How can information security be achieved?

#10 Datenschutz und was jede/r selbst dafür tun kann

SBA Research-Team gibt auf dem Forschungsfest und im ORF-TV konkrete Tipps zum Datenschutz

Die Angst ist groß, der Grad der Aufklärung gering. Gebeutelt von Schlagzeilen über gestohlene Daten, Cyber-Mobbing und Hacker-Attacken, sorgen sich Privatpersonen wie Unternehmen um den Schutz ihrer Daten. SBA Research leistete beim Wiener Forschungsfest 2010 anschauliche Aufklärungsarbeit. Das Thema: Informationssicherheit und was jede und jeder selbst dafür tun kann.

Kontrolle der eigenen Daten

Controlling your personal data

Rund 20.000 Wienerinnen und Wiener nutzten Mitte September 2010 die Gelegenheit, forschenden Unternehmen über die Schulter zu schauen. Am Stand von SBA Research im Prater drehte sich alles um die Kontrolle über die eigenen Daten. Das zweiköpfige Team hatte ein unverschlüsseltes WLAN-Testnetz aufgebaut, um zu zeigen, wie leicht dieses abgehört werden kann. „Wir haben uns für WLAN und Facebook entschieden, weil beides bekannt und weit verbreitet ist. Auf einem Rechner hatten wir eine Identität angelegt und auf dem anderen Rechner lasen wir mit. Anschließend haben wir die Gäste mit den abgehörten Daten konfrontiert", erläutert Manuel Leithner.

Der SBA Research-Stand war an den zwei Tagen gut besucht. Die häufigste Frage? „Wie kann ich mich schützen? Wobei wir die Erklärungen an das Vorwissen der Besucherinnen und Besucher anpassen

Data security and what everyone can do to protect themselves

SBA Research Team gives useful advice on data protection at the Research Festival and on national TV

When it comes to data protection, there are many fears but little information. In view of headlines about stolen data, cyber-bullying and hackers, both individuals and companies are concerned about the security of their data. At the 2010 Vienna Research Festival, SBA Research provided hands-on awareness training. The topic was information security and what everyone can do to protect themselves.

Some 20,000 Viennese visited the festival in mid-September 2010 to find out what research companies do. At the SBA Research booth in Vienna's Prater park, it was all about controlling your personal data. The two researchers had set up an unencrypted WLAN test network to show how easy eavesdropping is. "We chose WLAN and Facebook because they are widely known and used. We set up a test profile on one computer and used the other one to read the data. Then we showed our guests the data we had gained by eavesdropping," Manuel Leithner explains.

The booth of SBA Research attracted many visitors during the two days. What was the most common question? "'How can I protect myself?' Of course, we had to adapt our explanations to each visitor's level of knowledge. It was quite difficult at first to express it in clear and simple terms," the SBA researcher

mussten. Gar nicht leicht, sich auf Anhieb klar und einfach auszudrücken", so der SBA-Mitarbeiter. Ein gutes Training ist unumgänglich, denn „es gehört zu unseren Aufgaben als Kompetenzzentrum, die Öffentlichkeit zu unterrichten und aufzuklären. Sie fördert uns mit Steuergeld und wir müssen zeigen, was wir tun", schildert der Security-Experte.

Das Ziel war, Basiswissen und Bewusstseinsbildung zum Thema vertrauliche Daten und unverschlüsselte Übermittlung zu vermitteln. Wer sich im unverschlüsselten Hot Spot auf Facebook einloggt, gibt leicht seine Zugangsinfos preis. Fremde Personen im gleichen Netz können sich so der Identität bemächtigen und im Namen der ahnungslosen NutzerInnen in den sozialen Netzwerken agieren und spionieren. Dasselbe gilt für den Zugriff auf ein Firmennetzwerk vom Computer eines Internetcafés aus. Auf der Hardware installierte Programme können unbemerkt mitlesen und so finden sensible Informationen den Weg in falsche Hände.

Einen ähnlichen Zweck erfüllte der Auftritt von SBA-Researcher Manuel Leithner in „direkt – das Magazin" auf ORFeins im Oktober 2011. Aufgeschreckt durch aufeinanderfolgende Attacken von AnonAustria wurde ein Beitrag zum Thema „Datenleck Österreich – Wie gläsern sind wir bereits?" gestaltet. Gemeinsam mit Redakteurin Elisabeth Hötzl zeigte Leithner auf, wie leicht Informationen im Internet gefunden werden können und wie sorglos junge Österreicherinnen und Österreicher mit ihren Daten umgehen. Mediengerecht prägnant vermittelte Leithner, selbst im Alter der Zielgruppe, Basisinfor-

adds. Good training is essential, for "it is one of our duties as a competence center to inform and educate the public. They support us with their taxes and we must show what we do," says the security expert.

The objective was to convey basic information and raise awareness for the issue of confidential data and unencrypted connections. Someone who logs into Facebook at an unencrypted hotspot can easily divulge their account information. Other people in the same network could take over their identity and act in their name in social networks or collect information about them. The same is true for accessing a company network from an Internet café. Programs installed on the computer could read everything and sensitive information could get into the wrong hands.

Manuel Leithner also appeared on the Austrian TV channel ORFeins in October 2011 in the information program 'direkt – das Magazin'. Alarmed by several consecutive attacks by AnonAustria, the program ran a report titled 'Data leak Austria – are we already transparent citizens?' Together with reporter Elisabeth Hötzl, Manuel Leithner showed how easy it is to find information on the Internet and how careless young Austrians are with their data. Manuel Leithner, who is in the same age group as the target group, succinctly provided basic information on the careful use of personal data. With Elisabeth Hötzl's permission, the security expert hacked her smartphone and gained access to photos, contacts, text messages, etc. within seconds. The two also

Basiswissen
& Bewusstseinsbildung

Basic information
& awareness raising

mationen zum bewussten Umgang mit den eigenen Daten. Mit Erlaubnis der Redakteurin knackte der Fachmann für Datensicherheit ihr Smartphone und verschaffte sich binnen Sekunden Zugang zu Fotos, Adressbuch, SMS etc. Beim gemeinsamen Besuch in einem Café mit offenem WLAN-Netz konfrontierte die Redakteurin ahnungslose Social-Media-NutzerInnen mit Informationen aus ihrem Facebook-Account, die mit einem frei verfügbaren Programm eingesehen und manipuliert werden konnten. Das Einverständnis der „Opfer" dazu wurde vorab eingeholt. Im Anschluss gab Leithner konkrete Tipps zur Verbesserung, die unmittelbar umgesetzt werden können.

went to a café with an open WLAN network, where the reporter confronted users of social media with information from their Facebook accounts, which she and the security expert were able to read and manipulate with a freely available program. They obtained permissions from the 'victims' in advance. Finally, Manuel Leithner gave practical advice for improving security that can be implemented immediately.

„Es ist spannend, zu wissen, wie man in Systeme eindringen kann. Noch spannender ist es, dieses Wissen dazu zu verwenden, die Systeme sicherer zu machen."

Manuel Leithner

Jahrgang 1989, wurde schon in der HTL für EDV und Organisation in St. Pölten von einem SBA-Mitarbeiter und -Vortragenden angeworben. Nach einem Praktikum 2009 wurde er fix ins Team übernommen. Seine Spezialgebiete sind soziale Netzwerke, Cloud Computing und Mobile Security.

Born in 1989, Manuel was recruited when he was still in school by an SBA researcher who was holding a lecture at the Upper Secondary School for IT and Organization in St. Pölten. After an internship in 2009, he became a permanent team member. His areas of expertise are social networks, cloud computing, and mobile security.

ARES-Konferenz für die Security-Fachwelt

Erstklassige Vortragende in IT-Sicherheit und ihr Publikum finden mitten in Europa zusammen

Die Idee für eine eigene europäische Security-Konferenz wurde zeitgleich mit der Gründung des Kompetenzzentrums SBA Research geboren. Viele Forschungszentren liegen in den USA und Asien, weshalb die Fachwelt nur alle 10 bis 15 Jahre in einer europäischen Hauptstadt Halt macht. Zu selten für einen Bereich, in dem sich so viel bewegt. Bei jeder neuen Konferenz stellt sich die Frage: Wozu braucht es die noch? Für ARES kann das seit 2006 klar beantwortet werden: Eine eigenständige europäische Konferenz ist ein erstklassiger Ort, um hochklassige Forschungsarbeiten zu präsentieren, regelmäßig ein europäisches Fachpublikum anzusprechen und sich zu vernetzen.

„Die Hauptarbeit bei der Organisation ist die Sicherstellung einer hohen inhaltlichen Qualität. Unsere Keynote Speaker nutzen die Gelegenheit, vor europäischem Publikum zu sprechen, und unser Publikum nutzt die Gelegenheit, mit einem vertretbaren Reisebudget diese Forschungsgrößen zu hören“, betont der wissenschaftliche Leiter von SBA Research Edgar Weippl. Junge, noch unbekannte Konferenzen haben das Problem, dass die Community nicht die besten Ergebnisse schickt. Da kann leicht eine Negativspirale entstehen. Durch den internationalen Reviewprozess und ein strenges Programm-Komitee, das nur die besten und relevantesten Beiträge zulässt, hatte sich die ARES-Konferenz schon nach zwei Jahren einen sehr guten Ruf erarbeitet. 60 Personen

ARES Conference for security experts

Top-level speakers from the field IT security and their audience meet in the heart of Europe

The idea for a European security conference was born when the competence center SBA Research was founded. Many research centers are located in the US and Asia, and so the experts meet in a European capital perhaps every ten to fifteen years. That is far too little for such a dynamic field. With every conference, the question arises for what it is still needed. For ARES, there is a clear answer since 2006: A separate European conference is an excellent opportunity to present high-quality research and to regularly speak to and connect with a European expert audience.

“The main effort in organizing this conference goes into ensuring the high quality of the program. Our keynote speakers use the opportunity to speak to a European audience, and our audience enjoys the opportunity to hear these top researchers speak with reasonable travel expenses”, Edgar Weippl, Research Director of SBA Research, notes. Young conferences that have not made a name for themselves yet have the problem that the community does not always submit the best papers. This can easily turn into a downward spiral. Thanks to an international reviewing process and a program committee that only accepts the best and most relevant submissions, the ARES conference had already earned a very good reputation after just two years. 60 people from 40 different institutions ensure a top-class program with approximately

#11

Hohe Qualität, internationale Forschungsgrößen & Vernetzung

High quality, top international researchers & networking

The ARES Conference team (from left to right): A Min Tjoa, Edgar Weippl, Yvonne Poul, Simon Tjoa, Stefan Jakoubi

aus 40 verschiedenen Institutionen wachen über ein hochkarätiges Programm mit circa 25 Full Papers bei rund 120 Beiträgen insgesamt. „Das Finanzielle steht für die Vortragenden sicher nicht im Vordergrund, weil nur Reisespesen abgegolten werden. Wohl eher Wertschätzung und eine gute Plattform", ist sich der Organisator sicher.

ARES, kurz für Availability, Reliability and Security, ist zum Thema Informationssicherheit ebenso breit aufgestellt wie SBA Research. Rund 150 Gäste besuchen jedes Jahr die dreitägige Konferenz mit dem Namen eines listigen griechischen Kriegsgottes. Es sind dies Studierende und Wissenschaftler ab PhD-Level aus dem Securitybereich aus Europa und dem asiatischen Raum, schwerpunktmäßig aus Deutschland, Italien, Frankreich, Spanien und Japan.

Aufkeimende Themen & neue Ideen

Emerging topics & new ideas

Parallel zu den Vorträgen werden in Workshops aufkeimende Themen und neue Ideen aufbereitet und diskutiert. „Das ist unsere aktuelle Schiene mit Work in Progress. Für junge Forscherinnen und Forscher gibt es Poster-Präsentationen und auf

25 full papers and 120 contributions in total. "I am sure the financial aspect is not the main reason for speakers to come, since we only cover their travel expenses. It is more likely due to appreciation and the good platform we provide", the organizer says.

ARES is an acronym for Availability, Reliability and Security, and the conference has as broad a range of information security topics as SBA Research. Some 150 participants come every year to the three-day conference, which is named after a Greek god of war. They are PhD students and scientists from the security field from Europe and Asia, mainly from Germany, Italy, France, Spain and Japan.

In addition to the presentations, there are workshops where emerging topics and new ideas are discussed. "That is our current Work in Progress Track. Young researchers can present posters, and in the Industrial Track, companies can present their newest developments", Edgar Weippl explains. The most successful workshop is the Secure Software Engineering (SECSE) workshop, which is organized

dem Industrial Track stellen Firmen ihre neuesten Entwicklungen vor“, steckt Edgar Weippl den Rahmen ab. Der erfolgreichste Workshop ist der zu Secure Software Engineering (SECSE), der von der norwegischen SINTEF organisiert wird. Ende August 2012 findet der nächste auf der ARES-Konferenz in Prag statt.

„Da ist über die Jahre eine gute Community entstanden“, freut sich der wissenschaftliche Leiter. SBA Research verankert mit der Konferenz Österreich auf der Forschungslandkarte. „Weil man unseren Namen von der ARES kennt, fallen unsere Publikationen auch bei Top-Konferenzen in den USA mehr auf und es können neue Partnerschaften und Austauschprogramme etabliert werden.“ Das lässt das wissenschaftliche Netzwerk weiter wachsen.

www.ares-conference.eu

by the Norwegian research organization SINTEF. The next one will be held at the ARES conference in Prague in late August 2012.

“Over the years, a really good community has developed”, Weippl says with a smile. With this conference, SBA Research has positioned Austria on the research map. “People know our name from ARES, and so our publications also get more attention at top conferences in the US, which helps establish new partnerships and exchange programs.” And with each of these, the research network grows.

www.ares-conference.eu

#12 Eine Partnerschaft auf Augenhöhe

Gesundheit Österreich und SBA Research sorgen für mehr Sicherheit bei gesundheitsbezogenen Daten

Die Gesundheit Österreich GmbH ist eine Gesellschaft mbH, die zu 100 Prozent im Eigentum des Bundes steht. Sie verfasst Berichte, führt Register, erstellt Pläne für Gesundheitsmaßnahmen und sammelt Daten. Otto Postl, Leiter Finanz, Organisation und Personal, erinnert sich an den Beginn der Zusammenarbeit mit SBA Research. Eine für das Unternehmen sehr ernste Situation trat ein: der Ausfall des IT-Leiters. „Er war ein genialer Programmierer und außer dieser Person hatte niemand Einblick in die Entwicklungsarbeiten und das IT-System. In dieser Situation hat uns SBA Research geholfen und in kürzester Zeit die komplette Systemlandschaft erneuert und auf stabile Füße gestellt."

Neue Forschungsansätze für die tägliche Praxis

New research approaches for daily business

Seit diesem „Erste-Hilfe-Einsatz" hat sich die Partnerschaft zum beiderseitigen Nutzen weiterentwickelt. Die GÖG profitiert im täglichen Geschäft von neuartigen Ansätzen aus der Sicherheitsforschung. SBA Research bekommt umgekehrt Wissen aus dem Gesundheitsbereich und einen umfassenden „reality check". „Wir können unsere Ideen für den E-Health-Bereich umsetzbar, gesetzeskonform und praxisnah gestalten", erklärt Gernot Goluch von SBA Research, ebenfalls von Anfang an dabei. Otto Postl schätzt zudem die geringen Reibungsverluste: „Bei einfachen Problemen könnte der EDV-Support sogar aus einem anderen Land kommen, aber hier geht es um hoch spezialisierte wissensbasierte Leistungen."

A balanced partnership

Gesundheit Österreich and SBA Research make health data more secure

Gesundheit Österreich GmbH (GÖG) is a limited liability company that is 100 percent state owned. It writes reports, manages registers, creates plans for health promotion measures, and collects data. Otto Postl, Head of Finance, Organization and Personnel, remembers how the cooperation with SBA Research began. The Head of IT was suddenly gone – a very serious situation for the company. "He was a programming genius, and nobody else knew what he had been developing and how the IT system worked. SBA Research helped us out in this situation and renewed and stabilized the entire IT environment in a brief period of time."

Since that 'first aid' mission, the partnership has evolved to everyone's benefit. GÖG profits from the newest results of security research in their daily business, while SBA Research gains knowledge about the health sector and can check their work against reality. "This allows us to design our ideas for e-health so that they can be implemented, meet the legal requirements and are in step with current practice", explains Gernot Goluch of SBA Research, who was there from the start. Otto Postl also appreciates the good cooperation: "For simple problems, IT support could even be from abroad, but we are dealing with highly specialized, knowledge-based services here."

Der größte gemeinsame Entwicklungserfolg war die Optimierung des Softwarepaketes zum österreichischen Gesundheitsinformationssystem. Dieses komplexe zentrale Informationssystem wurde über viele Jahre von der GÖG entwickelt und ist europaweit eine der besten Anwendungen auf diesem Gebiet. Auch der österreichische „Strukturplan Gesundheit" basiert darauf. Mit verschiedenen Modulen können Daten zu Sterblichkeit, Gesundheit, Krankenhausplanung, Gesundheitsversorgung etc. statistisch ausgewertet, georeferenziert und grafisch dargestellt werden. SBA Research hat sich den Datenimport angesehen und für einige neue Module die Sicherheitsarchitektur mitgestaltet. Daten-Lieferungen haben manchmal personenbezogene Elemente, die für die Statistik nicht benötigt werden und gar nicht gespeichert werden dürfen. „Es geht darum, genug Informationen zu bekommen, aber nicht zu viele. Ein intelligenter Filter ist der Anfang von Datensicherheit", erklärt Gernot Goluch. Es ist etwa für die Auswertung von Stellungsdaten egal, wie die Rekruten heißen. Wichtig ist die Verteilung der Körpergröße oder die Tauglichkeit.

„Wir definieren anwendungsorientierte Anforderungen", schildert Otto Postl seine Kundenperspektive: „SBA Research versteht und durchdringt unsere Anliegen und setzt die Problematik programmiertechnisch um." Ein Stab IT-Betreuer bei der GÖG und SBA Research als Supervisor und Helping Hand mit Spezialwissen sind für einen Mittelbetrieb eine extrem wertvolle Kombination. „Wir geben unsere Leistungen z. B. an den Bund weiter, ein anspruchsvoller Auftraggeber. Bei SBA Research

The largest joint development success was the optimization of the software package for the Austrian health information system. This complex centralized information system was developed by GÖG over the course of many years and is one of the best applications in this field in Europe. The Austrian 'Structural Health Sector Plan' is based on it as well. With a number of modules, data on mortality, health, hospital planning, health care, etc. can be analyzed statistically, geo-referenced and shown as graphs. SBA Research examined how the data are imported, and contributed to the design of a security architecture for several new modules. Data sets sometimes contain personal elements that are not needed for statistic analyses and that are not allowed to be stored. "The point is to get enough information but not too much. An intelligent filter is the first step towards data security", Gernot Goluch explains. For example, the names of new recruits are irrelevant when evaluating data from military medical exams. What is relevant is the distribution of height among recruits or whether they were fit for service.

"We define our requirements depending on what they will be used for", Otto Postl describes the customer perspective. "SBA Research understands what we want and puts it into code." A group of IT support staff at GÖG and SBA Research as supervisor and helping hand with expert knowledge is a very valuable combination for a medium-sized enterprise. "We also provide our services to the federal state, a very demanding client. With SBA Research, the quality-cost ratio is always good. And the way in which SBA Research is rooted in

Sicherheitsarchitektur für neue Module

Security architecture for new modules

war die Relation von Qualität zu Kosten immer in Ordnung. Ihre Entstehungsgeschichte aus Forschung und Lehre passt sehr gut mit uns zusammen", so Otto Postl. Projektmanager Gernot Goluch nennt die Arbeitsbeziehung partnerschaftlich, vertraulich und unbürokratisch. „Wir arbeiten an einem stetigen Verbesserungsprozess im Bereich IT-Sicherheit und werden dabei nicht als Kassandra gesehen", freut sich der SBA-Projektleiter.

Als nächsten Meilenstein plant die GÖG, im EDV-Bereich einen Risk-Management-Prozess einzuleiten. Otto Postl ist überzeugt: „Das muss bei allen Mitarbeiterinnen und Mitarbeitern wirken und sickern, sonst ergibt es keinen Sinn. SBA Research wird realistische Szenarien liefern, was passieren kann, wenn man bestimmte Standards nicht einhält. So werden wir das erforderliche Bewusstsein bilden können."

research and teaching is a good fit for us as well", Postl adds. Project manager Gernot Goluch appreciates that the working relationship is cooperative, confidential and unbureaucratic: "We are constantly working on improving IT security and they still don't dismiss us as doomsayers."

As its next milestone, GÖG is planning to introduce a risk management process in its IT division. Otto Postl knows: "This is something where we need all employees on board, otherwise there is no point. SBA Research will deliver realistic scenarios that show what can happen if you do not observe certain standards. With their help, we will be able to raise awareness among our employees."

„Wenn Informationssicherheit bei jedem IT-Projekt mitgedacht wird, ist sie der Schlüssel zu einer sicheren Lösung. Sie ist kein Zauberpulver, das über ein IT-System verstreut wird und dieses sofort sicherer macht."

Mag. Gernot Goluch

Jahrgang 1981, Master in Economics and Computer Science an der TU Wien, Certified Information Systems Security Professional-CISSP (ISC)² und Certified Secure Software Lifecycle Professional-CSSLP (ISC)².
Gernot Goluch verfügt über viel Erfahrung in der IT-Sicherheitsprüfung und Softwareentwicklung, die er laufend mit Referenzprojekten, Publikationen und Fachvorträgen praxisorientiert vertieft. Bei SBA Research leitet er das Softwareentwicklungsteam sowie das eigens auf Software- und Informationssicherheitsüberprüfungen spezialisierte SSG-Team (Software Security Group).

Born in 1981, Gernot Goluch holds a Master in Economics and Computer Science from TU Vienna and is a Certified Information Systems Security Professional-CISSP (ISC)² and Certified Secure Software Lifecycle Professional-CSSLP (ISC)².
He has extensive experience in IT security reviews and software development, which he expands continuously with reference projects, publications and presentations. At SBA Research, he is the team leader of both the software development team and the Software Security Group (SSG), which was developed specifically for software and information security reviews.

Im Wettrüsten einen Wimpel voraus

A step ahead in the arms race

#13

Das Team der TU Wien gewann 2011 das internationale Capture-the-Flag (iCTF) der Universität von Santa Barbara, die akademische Hacker-WM. Mit auf der Trainerbank: das COMET-Kompetenzzentrum SBA Research.

Vienna University of Technology team wins the 2011 international Capture the Flag Contest (iCTF) at the University of Santa Barbara – the world championship of hacking for academic institutions. On the coach's bench: the COMET competence center SBA Research.

Die akademische Hacker-WM der Universität von Santa Barbara (UCSB) gewannen 2011 Studierende der Technischen Universität Wien. Ausgebildet und rekrutiert wurde das Team in der Lehrveranstaltung „Advanced Internet Security", veranstaltet von der TU Wien und SBA Research. Weltweit wird an Universitäten im Bereich Datenschutz und Internetsicherheit geforscht. Der „International Capture the Flag" (iCTF) Wettbewerb bietet akademischen Datendieben und Strukturssprengmeistern eine völlig legale Möglichkeit, ihr Können unter Beweis zu stellen. Das heimische Team „We_0wn_You" setzte den Lehrstoff erfolgreich in die Praxis um und trat gegen 87 exzellente Teams an.

Thema der von der UCSB organisierten und über das Internet ausgetragenen Hacker-WM 2011 war Geldwäsche. Jedes Team erhielt einen virtuellen Server mit zehn verschiedenen Diensten samt Sicherheitslücken. Wer es schaffte, ins gegnerische System einzudringen und Aufgaben zu lösen, holte sich eine „Flag" und punktete bei der Jury. Ein hohes Maß an Koordination und Geschicklichkeit war gefragt. Gleichzeitig galt es, das eigene System vor Angriffen zu schützen. Stärkster Konkurrent der Wiener war ein Team aus Russland. Die Entscheidung über den Sieg fiel erst in den letzten zehn Minuten, nach neun Stunden Wettkampf, kurz vor zwei Uhr Früh.

„Entscheidend für den Erfolg waren die gemeinsame Vorbereitung samt eigener Strategie, hierar-

The 2011 world champions of hacking for academic teams are students of TU Vienna. The team was recruited and trained in the course 'Advanced Internet Security', which is organized jointly by TU Vienna and SBA Research. Universities around the world conduct research on data protection and online security. The International Capture the Flag Contest at the University of Santa Barbara (UCSB) is a legal way for academic hackers to show off their skills. The members of the Austrian team 'We_0wn_You' were able to put the things they learned into practice and were victorious over 87 excellent teams.

The topic of iCTF 2011, which is held online, was money laundering. Each team received a virtual server with ten services with vulnerabilities. The team that managed to compromise their opponents' system and solve tasks captured a 'flag', gaining them points from the jury. The competition required a high degree of coordination and skill. At the same time, they had to protect their own system from attacks by other teams. The Viennese team's strongest rival was a Russian team. The game was decided in the last ten minutes, after nine hours of competition, just before 2 am.

"The key factors for their success were preparing together and developing their own strategy, a

Hacker-WM zu aktuellen Sicherheitsthemen wie Geldwäsche

World championship of hacking on current security topics such as money laundering

Teilnahme am wichtigsten Bewerb weltweit

Participation in the world's most important hacking contest

chischer Organisation und das genaue Umsetzen der Spielregeln", ist Sebastian Schrittwieser, einer der „Trainer" und Forscher am COMET Kompetenzzentrum SBA Research, überzeugt. Das Team der TU Wien darf sich über 2000 Dollar Preisgeld freuen und über eines der begehrten Tickets für den „Capture the Flag"-Wettbewerb während der DefCon in Las Vegas, dem wichtigsten Hackerwettbewerb weltweit. Dort wird es etwas härter zugehen. „Während die UCSB als Veranstalter festlegt, was erlaubt ist und was als Punkt gewertet wird, ist bei der DefCon fast alles erlaubt. Der Wettbewerb dauert mehrere Tage und man kann nicht sicher sein, ob nicht gerade die Anzeigetafel mit dem Punktestand manipuliert wurde", weiß Martin Mulazzani, Vortragender für IT-Security und digitale Forensik. Auch er ist „Trainer" des TU-Teams und Forscher bei SBA Research.

Nach fünf Jahren Aufbauarbeit hat sich das COMET-Kompetenzzentrum SBA Research Österreich 2011 auf der internationalen Landkarte für IT-Sicherheits-Forschung verankert. „Wir kooperieren österreichweit mit jeder Hochschule, die einen Security-Schwerpunkt anbietet und sorgen so für kompetenten Nachwuchs", freut sich der wissenschaftliche Leiter Edgar Weippl. Forscherinnen und Forscher von SBA Research präsentierten 2011 Arbeiten zu „Alltags-Anwendungen als IT-Sicherheitsfallen" – wie es etwa Cloud Computing, soziale Netzwerke oder Textnachrichten auf Smartphones sein können – auf fast allen großen internationalen Konferenzen. Durch erfolgreiche wissenschaftliche Vernetzung kommen 2012 auch die internationalen Konferenzen TrustBus (Trust, Privacy & Security in Digital Business) und Trust (Trust and Trustworthy Computing) nach Wien.

ictf.cs.ucsb.edu

hierarchical organization, and following the rules exactly", says Sebastian Schrittwieser, one of the 'trainers' and researcher at the COMET competence center SBA Research. The team of TU Vienna won $ 2000 in prize money and one of the sought-after tickets for the 'Capture the Flag' contest at DefCon in Las Vegas, the most important hacking contest worldwide. There, the gloves will come off. "UCSB has clear rules on what is permitted and what counts as a point, but at DefCon, almost everything is allowed. The competition takes several days and you can never be sure if the scoreboard hasn't just been manipulated," says Martin Mulazzani, lecturer for IT security and digital forensics. He is another 'trainer' of the TU Vienna team and researcher at SBA Research.

After five years, the COMET competence center SBA Research finally put Austria on the international map of IT security research in 2011. "We cooperate with every Austrian university that has a focus on IT security and ensure that we have capable new researchers," Research Director Edgar Weippl says. The researchers of SBA Research presented their work on everyday applications as IT security risks, such as cloud computing, social networks, or text messages on smartphones, at nearly all large international conferences in 2011. Thanks to successful scientific networking, the international conferences TrustBus (Trust, Privacy & Security in Digital Business) and Trust (Trust and Trustworthy Computing) will be held in Vienna in 2012.

ictf.cs.ucsb.edu

DI Martin Mulazzani

Jahrgang 1983, Studium „Computer- und Datensicherheit" an der TU Wien und seit 2009 Dissertant bei SBA Research. Mehrere Semester verbrachte er an der Purdue University und der Reykjavik University. Seine Forschung beschäftigt sich mit digitaler Forensik und Cloud Computing. Die Herausforderung im jungen Forschungsfeld Forensik liegt darin, dass Computer an den unterschiedlichsten Stellen Daten speichern. An der TU Wien und an verschiedenen FHs unterrichtet er Kurse darüber und zum Thema Security.

Born in 1983, Martin Mulazzani studied computer and data security at TU Vienna and has been working as a PhD student at SBA Research since 2009. His research interests are digital forensics and cloud computing. The challenge in the still young research area of forensics is that computers store data in various locations. He teaches courses on security and digital forensics at TU Vienna and several Austrian universities of applied sciences, and spent several semesters at Purdue University and Reykjavik University.

„Nach einem Hackerangriff oder bei der zeitlichen Reihung von Ereignissen geht es nicht um die Frage, ob der Computer Hinweise gespeichert hat, sondern wo."

DI Sebastian Schrittwieser

Jahrgang 1983, Studium der Wirtschaftsinformatik an der TU Wien, Schwerpunkt IT-Sicherheit, Diplomarbeit zu Enterprise Rights Management (ERM) mit Schwerpunkt sicheres Drucken, derzeit Dissertation im Informatikstudium, seit Jänner 2010 bei SBA Research. Seine Schwerpunkte: Digitale Forensik im Bereich Datenbanken, Sicherheit von Smartphones und Enterprise Rights Management. Während Digital Rights Management zu Recht einen schlechten Ruf hat, ergibt ERM Software in Unternehmen sehr wohl einen Sinn.

Born in 1983, Sebastian Schrittwieser studied informatics at TU Vienna with an emphasis on IT security and wrote his MA thesis on Enterprise Rights Management (ERM) with a focus on secure printing. He is currently working on his PhD in informatics and joined SBA Research in January 2010. His main research interests are digital forensics in databases, security of smartphones, and Enterprise Rights Management. While Digital Rights Management has a bad reputation – and rightly so – ERM makes sense in an enterprise context.

„Ein Mitarbeiter ist nicht wie ein Kunde, der Musik gekauft hat. Firmendokumente gehören ihm nicht, und durch den Einsatz wird niemand eingeschränkt oder benachteiligt."

#14 Praxisnahe Ausbildung und internationaler Austausch

Allianzen mit internationalen Forschungszentren und starke nationale Partner

Bei SBA Research wird die praxisnahe Aus- und Weiterbildung der Mitarbeiterinnen und Mitarbeiter ernst genommen. Der ForscherInnennachwuchs kommt oft – wie die drei Gründer des Forschungszentrums selbst – von der TU Wien. Wer in das Berufsfeld IT-Security hineinwachsen möchte, kommt an dem COMET-Kompetenzzentrum kaum vorbei. Edgar Weippl, wissenschaftlicher Leiter des Kompetenzzentrums, ist stolz auf die Kooperation mit den Hochschulen, die in diesem Bereich tätig sind. Dazu gehören die Fachhochschulen Hagenberg, St. Pölten, Technikum Wien und Campus Wien, die Donau Universität Krems und die Institute an den Partnerunis TU Wien, TU Graz, Uni Wien und

Practically oriented education and international exchanges

Ties to international research centers and strong national partners

SBA Research places great importance on the practical education and further training of its employees. The young researchers often come from the Vienna University of Technology, just like the three founders of the research center. Students aiming to work in IT security can hardly avoid hearing about the COMET competence center. Research Director Edgar Weippl is proud of the center's cooperation with all Austrian universities with an IT security focus. This includes the universities of applied sciences Hagenberg, St. Pölten, Technikum Wien and Campus Wien, the Danube University Krems, and the departments at the partner universities, the Technical Universities of Vienna and Graz, the University of Vienna and the Vienna University of Economics and Business.

International exchange

WU Wien. Als Vortragende und BetreuerInnen für Studierende, ForscherInnennachwuchs und Industrie geben die Mitarbeiterinnen und Mitarbeiter von SBA Research die gesammelte IT-Security-Erfahrung weiter. Bei internationalen Konferenzen werden Kontakte mit Kolleginnen und Kollegen in Spitzen-Arbeitsgruppen weltweit gepflegt.

As lecturers and mentors for students, young researchers, and the industry, the staff of SBA Research share their collective IT security experience. At international conferences, they refresh their contacts with colleagues from all over the world in top-level working groups.

SBA Research-Gründer und Informatikprofessor A Min Tjoa sieht es mit einem lachenden und einem weinenden Auge: „Die KollegInnen vom Kompetenzzentrum sind in die Lehre eingebunden und halten schon bei den Erstsemestrigen Ausschau nach Talenten. Wir rekrutieren gute junge Leute, die uns aber oft an Unis auf der ganzen Welt ‚wegberufen' werden." Sie bleiben SBA Research jedoch meist mit Ausbildungskooperationen an ihren Universitäten und Forschungszentren gewogen.

Founder of SBA Research and professor of informatics A Min Tjoa sees it as a mixed blessing: "The colleagues at the competence center teach courses and look for promising people even among first year students. We recruit talented young people, but universities from all over the world often end up recruiting them away from us." However, they usually maintain good contacts with SBA Research through training exchanges at their universities and research centers.

Austausch über Ideen & Arbeitsweisen

Exchanging ideas & working methods

Eine intensive Zeit verbrachte SBA-Researcher Martin Mulazzani an der Purdue University in den Arbeitsgruppen von Professor Elisa Bertino, Leiterin des US-Forschungszentrums für Computersicherheit (CERIAS), und Professor Cristina Nita-Rotaru, Leiterin des Dependable and Secure Distributed Systems Laboratory (DS2). Er arbeitete insgesamt sechs Monate mit, nahm an den Treffen der Forschungsgruppen teil und stand im intensiven wechselseitigen Austausch über Ideen und Arbeitsweisen. Bertino und Nita-Rotaru arbeiten unter anderem mit Sensornetzwerken, die in sensiblen Bereichen Daten autonom messen können und untereinander kommunizieren. Im Grenzschutz, bei der Energiegewinnung oder in abgelegenen Schutzgebieten können solche Netze gute Dienste leisten, wobei natürlich

SBA Researcher Martin Mulazzani spent six busy months in the working groups of Professor Elisa Bertino, Research Director of CERIAS, the Center for Education and Research in Information Assurance and Security, and of Professor Cristina Nita-Rotaru, Director of the Dependable and Secure Distributed Systems Laboratory (DS2), at Purdue University. He worked in their teams, participated in research group meetings and exchanged ideas and knowledge about working methods. One of the research areas of Elisa Bertino and Cristina Nita-Rotaru are sensor networks that can read data in sensitive areas autonomously and communicate with each other. Such networks can be useful in border control, energy generation or remote conservation areas. Of course, it is vital to ensure that the systems are secure and cannot be manipulated.

die Sicherheit gewährleistet werden muss. Manipulationen müssen ausgeschlossen werden können. Ein weiteres Betätigungsfeld war die Sicherheit von intelligenten Zählern (sogenannte Smart Meter), die auch innerhalb der EU in den nächsten Jahren flächendeckend eingesetzt werden sollen. „Informationssicherheit ist ein sehr kleines Spezialgebiet in der Informatik, das an dieser Uni disziplinenübergreifend gepflegt und auf hohem Niveau betrieben wird", berichtet SBA-Forscher Martin Mulazzani, der in Purdue vielleicht die gleiche Schulbank drückte wie Neil Armstrong.

Themenübergreifende Teamarbeit

Interdisciplinary teamwork

Themenübergreifend und im Team zu arbeiten ist die Maxime bei SBA Research. Im ursprünglichen Sinn zeigt ein Hacker Schwachstellen auf, ohne Schaden anzurichten. Er ist ein kreativer Einbrecher, der einen Brief hinterlegt. Darin steht dann: Das Fenster war offen oder das Schloss schließt schlecht. Bitte schalten Sie das nächste Mal die Alarmanlage ein. „Wir bei SBA Research sind ‚white hats'", erzählt der wissenschaftliche Leiter, Edgar Weippl. „Wir brechen nur mit Genehmigung des Hauseigners ein. Unsere Widersacher sind ‚black hats': Malware, Botnetze, Datendiebe, Viren, Würmer, Sicherheitslücken und Co."

Sebastian Schrittwieser forscht mit Professor Stefan Katzenbeisser, Leiter der Security Engineering Group der TU Darmstadt, zum Thema Code Obfuscation als Teil des Bereichs Enterprise Rights Management (ERM). „Ein ausgefeiltes Programm kann ein Wettbewerbsvorteil gegenüber anderen Herstellern sein. Wenn ich ein Feature schützen will, muss ich es sichern, damit Kopierschutz-Überprüfungen

Another research area is the security of smart meters, which will become widely used in the EU in the coming years. "Information security is a very small specialized area of informatics, and this university researches it at a high level across all departments," says Martin Mulazzani, who may have sat on the very same chair in Purdue as Neil Armstrong.

Interdisciplinary teamwork is the rule at SBA Research. Hackers in the original sense highlight security flaws without doing damage. They are like a creative burglar who leaves behind a note that says, "Your window was open / your door does not lock well. Please switch on the alarm system next time." "We at SBA Research are 'white hats'", says Research Director Edgar Weippl. "We only break in if the house owner allows it. Our opponents are 'black hats': the ones with malware, botnets, data theft, viruses, worms, security breaches, etc."

Sebastian Schrittwieser's research with Professor Stefan Katzenbeisser, head of the Security Engineering Group of TU Darmstadt, focuses on code obfuscation as part of Enterprise Rights Management (ERM). "A sophisticated program can give you a competitive edge over other software providers. To protect a feature, you have to secure it so that copy protection mechanisms cannot be circumvented or the code copied", Schrittwieser explains. Enterprise Rights Management systems control the access to and use of documents in enterprises. The documents are generally encrypted and are only decrypted by the ERM system after validating

nicht einfach umgangen oder der Code kopiert werden kann", erläutert Schrittwieser. Enterprise Rights Management-Systeme überwachen den Zugriff auf und die Nutzung von Dokumenten in Unternehmen. Dabei sind Dokumente prinzipiell verschlüsselt und werden vom ERM-System erst nach Überprüfung der Zugriffsrechte des Benutzers entschlüsselt. Der Schlüssel zur Freigabe liegt meist in der Software versteckt. Hier gilt: Wer suchet, der findet auch irgendwann. In seiner Dissertation will Schrittwieser einfache Hardware-Bausteine nützen, um Software zu schützen. Mittel zum Zweck sind sogenannte Physically Uncloneable Functions (PUF). Die TU Darmstadt prüft rund ein Dutzend verschiedene Ansätze und rankt sie nach Eignung: Was ist praktikabel, wie stabil sind die PUF, wie robust, wie schnell und wie leicht zu knacken. „Die Grundidee ist, dass die Software ein Signal aussendet, das aufgrund der spezifischen physikalischen Eigenschaften der Hardware unverwechselbar beantwortet wird. Erst dann wird überhaupt ein Schlüssel erzeugt und ausgehändigt", erläutert der Doktorand und SBA Researcher. So sieht trotz Serienfertigung jede Platine etwas anders aus. Wenn Leiterbahnen und ihre Abweichungen bekannt sind, werden Abfragen von einem fremden Rechner falsch beantwortet und der kryptografische Schlüssel kann somit nicht berechnet werden.

Mit dem European Research Consortium for Informatics and Mathematics (ERCIM) wird der europaweite Austausch von Post Docs organisiert. Im September 2012 wird das Wiener Forschungszentrum für IT-Sicherheit einen Fellow aus Griechen-

a user's access rights. The decryption key is usually hidden in the software. And if you search long enough, you will find it eventually. In his dissertation, Sebastian Schrittwieser plans to use simple hardware building blocks to protect software. This is done using so-called Physically Uncloneable Functions (PUF). TU Darmstadt examines about a dozen different approaches and ranks them by suitability: what is feasible, how stable are the PUF, how robust, how fast and how easy to crack? "The basic idea is that the software sends out a signal and receives a response that is unmistakable due to the specific physical attributes of the hardware. Only then is a key created and used," the PhD student and SBA researcher explains. Despite serial production, each circuit board is a little different. If the circuit paths and their deviations are known, requests from another computer will receive a false response and the cryptographic key cannot be created.

Programm-Features & Code schützen

Protecting program features & code

Together with the European Research Consortium for Informatics and Mathematics (ERCIM), SBA Research organizes exchanges of postdocs in Europe. In 2012, a Fellow from Greece will join the Viennese research center for information security. He is currently familiarizing himself with cryptography in France. SBA Research selected Dimitris Simos for cooperation in projects on coding theory and digital forensics.

In 2009, SBA Research organized an IPICS summer school in Vienna and will do so again in 2012. In the Intensive Program on Information Communication Security (IPICS), Master's and PhD students from the

land aufnehmen. Der Kollege arbeitet sich derzeit in Frankreich in den Bereich Kryptografie ein. SBA Research hat sich Dimitris Simos vorab für die Einbindung in Projekte zu Codierungstheorie und digitaler Forensik ausgesucht.

Uni-Netzwerk für Studierende zu Informationssicherheit

2009 organisierte SBA Research in Wien eine IPICS Summer School und wird das auch 2012 wieder tun. Bei dem Intensive Program on Information Communication Security (IPICS) tauschen sich Master-Studierende und DoktorandInnen der Informatik, Wirtschaftsinformatik und IT-Engineering aus ganz Europa über Informationssicherheit aus. In dem Netzwerk haben sich Universitäten aus ganz Europa zusammengeschlossen: Stockholm University und Karlstads Universitet (Schweden), Katholieke Universiteit Leuven (Belgien), Kingston University, University of Bristol, University of Plymouth, University of Kent, Royal Holloway und University of London (UK), University of Piraeus und University of the Aegean (Griechenland), Universidad de Málaga (Spanien), Università Degli Studi Di Milano (Italien), Universität Regensburg (Deutschland), Universität Wien und die Technischen Universitäten in Wien und Graz. In einer Art Entwicklungszusammenarbeit hat 2012 auch erstmals eine IPICS Winter School an der University of Havana auf Kuba stattgefunden.

www.ercim.eu
www.cerias.purdue.edu
www.ipics-school.eu
www.seceng.informatik.tu-darmstadt.de

University network for students on information security

fields of informatics, business informatics, and IT engineering from across Europe will meet to discuss information security. Universities from all over Europe have joined the network: Stockholm University and Karlstads Universitet (Sweden), Katholieke Universiteit Leuven (Belgium), Kingston University, University of Bristol, University of Plymouth, University of Kent, Royal Holloway and University of London (UK), University of Piraeus and University of the Aegean (Greece), Universidad de Málaga (Spain), Università Degli Studi Di Milano (Italy), Universität Regensburg (Germany), the University of Vienna and the Universities of Technology in Vienna and Graz. As a kind of development cooperation, the first IPICS Winter School was held at the University of Havana in Cuba in 2012.

www.ercim.eu
www.cerias.purdue.edu
www.ipics-school.eu
www.seceng.informatik.tu-darmstadt.de

Impressum

Herausgeber und Medieninhaber:

SBA Research gGmbH

Sommerpalais Harrach

Favoritenstr. 16, 2. Stock

1040 Wien

Telefon: +43 (1) 505 36 88

E-Mail: office@sba-research.org

Web: www.sba-research.org

Text: Astrid Kuffner, www.astroid.at, Sylvi Rennert (Übersetzung)

Layout: Nora Swoboda, www.goldmaedchen.at

Print: druckwerker, 1020 Wien, www.druckwerker.at

Bundesministerium für Verkehr, Innovation und Technologie

Bundesministerium für Wirtschaft, Familie und Jugend

FFG

wirtschaftsagentur wien zit Die Technologieagentur der Stadt Wien

Christian Doppler Forschungsgesellschaft

FWF Der Wissenschaftsfonds.

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.

SBA Research gGmbH
Favoritenstraße 16, 2. Stock
A-1040 Wien
Telefon: +43 1 505 36 88
www.sba-research.org