HTWG

Hochschule Konstanz
Fakultät Informatik

Jahrestagung des Fachbereichs Sicherheit –
Schutz und Zuverlässigkeit

SICHERHEIT 2018

25.-27.04.2018

Veranstaltungsprogramm

Stand 2018-04-19

GESELLSCHAFT
FÜR INFORMATIK

Gastzugang zum Internet

Alternative 1: Eduroam

Alternative 2: HTWG-Guests

1. Verbinden Sie Ihr Gerät mit dem WLAN „HTWG-Guests“, starten Sie Ihren Web-Browser und rufen Sie die Startseite der Hochschule http://www.htwg-konstanz.de auf.
2. Sie werden vom System automatisch auf die Anmeldeseite umgeleitet, auf der Sie bitte Ihren Zugangscode **`DICKK-QDSEQ`** eingeben. Nach der Annahme der Nutzungsbedingungen zeigt Ihnen das System die Gültigkeitsdauer Ihres Zugangs an und aktiviert Ihre Anmeldung.
3. Die Zugangsdaten können während der Gültigkeitsdauer beliebig oft dazu verwendet werden, sich erneut am System anzumelden.

Bitte beachten Sie: Mit dem Gastzugang erhalten Sie einen ungesicherten Zugang zum Internet, eine Verschlüsselung Ihrer übertragenen Daten erfolgt hierbei nicht. Wir empfehlen zur Absicherung der Übertragung die Nutzung eines VPN-Dienstes.

Dienstag, 24.04.2018

14:30-17:30 Sitzung Leitungsgremium des Fachbereichs [O-202]

14:00-15:30 Doktorandenforum Session A [P-001]

Chair: Prof. Dr. Delphine Reinhardt, Universität Göttingen

- *My Data is Mine – Users' Handling of Personal Data in Everyday Life*
  Sven Bock, TU Berlin

  This experimental study is about investigating users' handling of personal data and their awareness of data collection. A deception experiment was designed to let the subjects believe that they are participating in a decision-making experiment. Only after the experiment, they were informed about the actual aim of examining their behaviour towards their personal data. Before the deception experiment either a printed or a digital version of the terms and conditions was handed out. The reading time and the willingness to accept the terms and conditions was measured in order to find significant differences. For the deception, a program was implemented which simultaneously presents two terms including sensitive data like religious and political orientation. The subject should choose the favoured term. Afterwards, subjects were asked whether and to what extent they agree to hand out their collected data to third parties in exchange for financial gain. After the experiment the participants were asked about their usual behaviour regarding their personal data.

- *Bounded Privacy: Formalising the Trade-Off Between Privacy and Quality of Service*
  Lukas Hartmann, Universität Regensburg

  Many services and applications require users to provide a certain amount of information about themselves in order to receive an acceptable quality of service (QoS). Exemplary areas of use are location based services like route planning or the reporting of security incidents for critical infrastructure. Users putting emphasis on their privacy, for example through anonymization, therefore usually suffer from a loss of QoS. Some services however, may not even be feasible above a certain threshold of anonymization, resulting in unacceptable service quality. Hence, there need to be restrictions on the applied level of anonymization. To prevent the QoS from dropping below an unacceptable threshold, we introduce the concept of Bounded Privacy, a generic model to describe situations in which the achievable level of privacy is bounded by its relation to the service quality. We furthermore propose an approach to derive the optimal level of privacy for both discrete and continuous data.

- *Towards a Differential Privacy Theory for Edge-Labeled Directed Graphs*
  Jenni Reuben, Karlstad University [Skype]

  Increasingly, more and more information is represented as graphs such as social network data, financial transactions and semantic assertions in Semantic Web context. Mining such data about people for useful insights has enormous social and commercial benefits. However, the privacy of the individuals in datasets is a major concern. Hence, the challenge is to enable analyses over a dataset while preserving the privacy of the individuals in the dataset. Differential privacy is a privacy model that offers a rigorous definition of privacy, which says that from the released results of an analysis it is *difficult* to determine if an individual contributes to the results or not. The differential privacy model is extensively studied in the context of relational databases. Nevertheless, there has been growing interest in the adaptation of differential privacy to graph data. Previous research in applying differential privacy model to graphs focuses on unlabeled graphs. However, in many applications graphs consist of labeled edges, and the analyses can be more expressive, which now takes into account the labels. Thus, it would be of interest to study the adaptation of differential privacy to edge-labeled directed graphs. In this paper, we present our foundational work towards that aim. First we present three variant notions of an individual's information being/not being in the analyzed graph, which is the basis for formalizing the differential privacy guarantee. Next, we present our plan to study particular graph statistics using the differential privacy model, given the choice of the notion that represent the individual's information being/not being in the analyzed graph.

Kommunikationspause

15:45-17:15 Doktorandenforum Session B

Chair: Prof. Dr. Delphine Reinhardt, Universität Göttingen

- *Turning the Table Around: Monitoring App Behavior*
  Nurul Momen, Karlstad University

  Since Android apps receive whitecard access through permissions, users struggle to understand the actual magnitude of app access to their personal data. Due to unavailability of statistical or other tools that would provide an overview of data access or privilege use, users can hardly assess privacy risks or identify app misbehavior. This is a problem for data subjects. The presented PhD research project aims at creating a transparency-enhancing technology that helps users to assess the magnitude of data access of installed apps by monitoring the Android permission access control system. This article will present how apps exercise their permissions, based on a pilot study with an app monitoring tool. It then presents a prototypical implementation of a networked laboratory for crowdsourcing app behavior data. Finally, the article presents and discusses a model that will use the collected data to calculate and visualize risk signals based on individual risk preferences and measured app data access efforts.

- *Usability von Security-APIs für massiv-skalierbare vernetzte Service-orientierte Systeme*
  Peter Leo Gorski, TH Köln

  Kontemporäre Service-orientierte Systeme sind hochgradig vernetzt und haben zudem die Eigenschaft massiv-skalierbar zu sein. Diese Charakteristiken stellen im besonderen Maße Anforderungen an die Datensicherheit der Anwender solcher Systeme und damit primär an alle Stakeholder der Softwareentwicklung, die in der Verantwortung sind, passgenaue Sicherheitsmechanismen effektiv in die Softwareprodukte zu bringen. Die Effektivität von Sicherheitsarchitekturen in service-orientierten Systemen hängt maßgeblich von der richtigen Nutzung und Integration von Security-APIs durch eine heterogene Gruppe von Softwareentwicklern ab, bei der nicht per se ein fundiertes Hintergrundwissen über komplexe digitale Sicherheitsmechanismen vorausgesetzt werden kann. Die Diskrepanz zwischen komplexen und in der Anwendung fehleranfälligen APIs und einem fehlenden Verständnis für die zugrundeliegenden Sicherheitskonzepte auf Seiten der Nutzer begünstigt in der Praxis unsichere Softwaresysteme. Aus diesem Grund ist die Gebrauchstauglichkeit von Security-APIs besonders relevant, damit Programmierer den benötigten Funktionsumfang effektiv, effizient und zufriedenstellend verwenden können. Abgeleitet von dieser Problemstellung, konzentriert sich das Dissertationsvorhaben auf die gebrauchstaugliche Ausgestaltung von Security-APIs und den Herausforderungen die sich aus den Methoden zur Evaluation der Usability in typischen Umgebungen der Softwareentwicklung ergeben.

- *I Did a Ph.D. in Computer Science – Lessons Learned & Some Advice*
  Prof. Dr. Andreas Heinemann, Hochschule Darmstadt

Platz für Ihre Notizen

Mittwoch, 25.04.2018 [Raum P-001]

09:00-09:15 Eröffnung

09:15-10:00 Keynote Prof. Dr. Marc Strittmatter, HTWG Konstanz: Die EU Datenschutz Grundverordnung - neue Anforderungen an IT-Sicherheit durch einen risikobasierten Ansatz?

Die EU Datenschutz GVO intensiviert die Vereinheitlichung des Datenschutzrechts in Europa. Sie führt neben einigen neuen Konzepten robuste Bußgeldtatbestände ein. Technisch-organisatorische Maßnahmen zur Datensicherung müssen nun risikoangemessen beschaffen sein. Je höher die Risiken, desto höher müssen die zu treffenden datenschutzrechtlichen Vorkehrungen ausfallen. Der Vortrag geht der Frage nach, was sich durch dieses Konzept im Vergleich zur Richtlinie EWG 95/46 bzw. dem BDSG ändert.

Prof. Dr. Marc Strittmatter ist in Deutschland als IT-Rechtler bekannt. Er berät als Of Counsel der Kanzlei Unternehmen, die sich Technologie-Einführungsprojekte im Bereich ERP, Cloud, Outsourcing oder Unternehmensvernetzung (Industrie 4.0) und der regulatorischen Compliance, insb. im Datenschutz vorgenommen haben. Seine langjährige Erfahrung in einem der größten IT Konzerne der Welt, zuletzt als Leiter der Rechtsabteilung von IBM Deutschland, als Rechtsanwalt in der IT-Kanzlei Bartsch und Partner und aus internationalen Tätigkeiten kombiniert er mit der angewandten Wissenschaft, die er als ordentlicher Professor für Wirtschaftsrecht an der HTWG Konstanz lehrt. Seine Forschungsschwerpunkte sind rechtliche Bedingungen der Digitalisierung, Verhandlungstheorie, technische Konzepte im Datenschutz und die Risikosteuerung von Unternehmen mithilfe rechtlicher Instrumente. Marc Strittmatter ist Mitglied der Deutschen Institution für Schiedsgerichtsbarkeit, für die er auch Mandate in Schiedsgerichtsverfahren als Richter betreut. Er wurde vom Handelsblatt in die Liste der „Best Lawyers“ im Bereich Informationstechnologierecht für die Jahre 2014, 2015, und 2016 gewählt, für das Jahr 2017 zum Lawyer des Jahres Informationstechnologierecht.

Kommunikationspause

10:15-11:15 Session 1: Privacy I

Session Chair: Sandra Ringmann

- *Towards an Architecture for Pseudonymous E-Commerce - Applying Privacy by Design to Online Shopping*
  Sebastian Pape, Goethe-Universität Frankfurt
  Daniel Tasche, Hochschule Zittau/Görlitz
  Iulia Bastys, Goethe-Universität Frankfurt & Chalmers University of Technology
  Akos Grosz, Goethe-Universität Frankfurt
  Jörg Lässig, Hochschule Zittau/Görlitz
  Kai Rannenberg, Goethe-Universität Frankfurt

  In this paper we apply privacy by design in e-commerce. We outline the requirements of a privacy-aware online shopping platform that satisfies the principle of data minimization and we suggest several architectures for building such a platform. We then compare them according to four dimensions: privacy threats, transparency, usability and compatibility with existing business models. Based on the comparison, we aim to build the selected platform in the next step.

- *Anreize und Hemmnisse für die Implementierung von Privacy-Enhancing Technologies im Unternehmenskontext*
  David Harborth, Maren Braun, Akos Grosz, Sebastian Pape, Kai Rannenberg, Goethe-Universität Frankfurt

  Wir untersuchen in diesem Artikel mögliche Anreize für Firmen Privacy-Enhancing Technologies (PETs) zu implementieren, und damit das Privatsphäre- und Datenschutzniveau von Endkonsumenten zu erhöhen. Ein Großteil aktueller Forschung zu Privatsphäre- und Datenschutz (im Weiteren Privacy) wird aktuell aus Nutzersicht, und nicht aus der Unternehmensperspektive geführt. Um diese bislang relativ unerforschte Lücke zu füllen, interviewten wir zehn Experten mit einem beruflichen Hintergrund zum Thema Privacy. Die Resultate unserer qualitativen Auswertung zeigen eine komplexe Anreizstruktur für Unternehmen im Umgang mit PETs. Durch das sukzessive Herausarbeiten zahlreicher Interdependenzen der gebildeten Kategorien leiten wir externe sowie unternehmens- und produktspezifische Anreize und Hemmnisse zur Implementierung von PETs in Firmen ab. Die gefundenen Ergebnisse präsentieren wir anschließend in einer Taxonomie. Unsere Ergebnisse haben relevante Implikationen für Organisationen und Gesetzgeber sowie die aktuelle Ausrichtung der Privacyforschung.

- *Ein Werkzeug zur automatisierten Analyse von Identitätsdaten-Leaks*
  Timo Malderle, Universität Bonn
  Matthias Wübbeling, Universität Bonn & Fraunhofer FKIE
  Sven Knauer, Universität Bonn
  Michael Meier, Universität Bonn & Fraunhofer FKIE

  Schon vor den Leaks von Dienstleistern wie last.fm, Playstation-Network oder Ashley Madison war Identitätsdiebstahl ein relevantes Thema im Bereich IT-Sicherheit. Die deutsche Gesetzgebung fordert zumeist eine Veröffentlichung der Umstände in relevanten Medien. Trotz öffentlicher Bekanntgabe und Präsenz in einschlägigen Medien erreichen relevante Informationen oft nur wenige Betroffene. Durch solche Veröffentlichungen lässt sich der Missbrauch von personenbezogenen und persönlichen Daten durch Kriminelle weder verhindern noch kontrollieren. Individuelle Benachrichtigungen von Betroffenen können die Folgen von Identitätsdiebstahl abschwächen. Dabei sollten die Benachrichtigungen weiterführende Informationen über den Umfang des Leaks beinhalten, welche die Kritikalität der betroffenen Merkmale darstellen und auch über mögliche Maßnahmen informieren. Um eine individuelle Information auf Basis verfügbarer Identitätsdaten-Leaks zu gewährleisten, müssen diese normalisiert und analysiert werden. Aufgrund der großen Menge kursierender Identitätsdatensammlungen ist eine Automatisierung notwendig. Diese Arbeit dokumentiert eine Implementierung zur automatisierten syntaktisch-, semantischen Analyse und Normalisierung relevanter Merkmale öffentlich verfügbarer Identitätsdaten als Vorbereitung zur individuellen Benachrichtigung von Betroffenen.

Kommunikationspause

11:30-12:30 Session 2: Privacy II

Session Chair: Prof. Dr. Dieter Hutter

- *Hashing of personally identifiable information is not sufficient*
  Matthias Marx, Ephraim Zimmer, Tobias Mueller, Maximilian Blochberger, Hannes Federrath, Universität Hamburg

  It is common practice of web tracking services to hash personally identifiable information (PII), e. g., e-mail or IP addresses, in order to avoid linkability between collected data sets of web tracking services and the corresponding users while still preserving the ability to update and merge data sets associated to the very same user over time. Consequently, these services argue to be complying with existing privacy laws as the data sets allegedly have been pseudonymised. In this paper, we show that the finite pre-image space of PII is bounded in such a way, that an attack on these hashes is significantly eased both theoretically as well as in practice. As a result, the inference from PII hashes to the corresponding PII is intrinsically faster than by performing a naive brute-force attack. We support this statement by an empirical study of breaking PII hashes in order to show that hashing of PII is not a sufficient pseudonymisation technique.

- *Improving Anonymization Clustering*
  Florian Thaeter, Rüdiger Reischuk, Universität Lübeck

  Microaggregation is a technique to preserve privacy when confidential information about individuals shall be used by third parties. A basic property to be established is called k-anonymity. It requires that identifying information about individuals should not be unique, instead there has to be a group of size at least k that looks identical. This is achieved by clustering individuals into appropriate groups and then averaging the identifying information. The question arises how to select these groups such that the information loss by averaging is minimal. This problem has been shown to be NP-hard. Thus, several heuristics called MDAV, V-MDAV,… have been proposed for finding at least a suboptimal clustering. This paper proposes a more sophisticated, but still efficient strategy called MDAV* to construct a good clustering. The question whether to extend a group locally by individuals close by or to start a new group with such individuals is investigated in more depth. This way, a noticeable lower information loss can be achieved which is shown by applying MDAV* to several established benchmarks of real data and also to specifically designed random data.

- *Verbesserung der Syndrome-Trellis-Kodierung zur Erhöhung der Unvorhersagbarkeit von Einbettpositionen in steganographischen Systemen*
  Olaf Markus Köhler, Universität Innsbruck
  Cecilia Pasquini, Rainer Böhme, Universität Innsbruck & Universität Münster

  Beim Einbetten einer versteckten Nachricht in ein Trägermedium wählen adaptive steganographische Systeme die Einbettpositionen abhängig von der erwarteten Auffälligkeit der Änderungen. Die optimale Auswahl kann statistisch modelliert werden. Wir präsentieren Ergebnisse einer Reihe von Experimenten, in denen untersucht wird, inwiefern die Auswahl durch Syndrome-Trellis-Kodierung dem Modell unabhängiger Bernoulli-verteilter Zufallsvariablen entspricht. Wir beobachten im Allgemeinen kleine Näherungsfehler sowie Ausreißer an Randpositionen. Bivariate Abhängigkeiten zwischen Einbettpositionen ermöglichen zudem Rückschlüsse auf den verwendeten Kode und seine Parameter. In Anwendungen, welche die Ausreißer nicht mithilfe zufälliger Permutationen verstecken können, kann die hier vorgeschlagene „outlier corrected“-Variante verwendet werden um die steganographische Sicherheit zu verbessern. Die aggregierten bivariaten Statistiken sind dahingegen invariant unter Permutationen und stellen, unter der Annahme mächtiger Angreifer, ein bisher nicht erforschtes Sicherheitsrisiko dar.

12:30 – 14:00 Kommunikationspause

Buffet [Sponsor des Mittagessens: DB Systel GmbH]

14:00-16:00 Vorträge Promotionspreis

Session Chair: Prof. Dr. Andreas Heinemann

- *Characterizing the Strength of Software Obfuscation Against Automated Attacks*
  Sebastian Banescu, TU München

  In this thesis, we develop a framework for the characterization of software obfuscation strength against automated analysis attacks. We do this by formulating automated analysis as search problems, whose complexities depend on various software characteristics. These characteristics become apparent after an attack is formulated using our framework. This helps developers to choose obfuscating transformations, which change those software characteristics, such that heuristics are no longer applicable or to increase the search effort to an extent that it is no longer economically attractive. We present multiple experiments involving various software applications, obfuscating transformations and an automated attack based on symbolic execution, whose results support our hypothesis. Using the insights gained from this approach towards obfuscation strength characterization, we are able to improve the state of the art of obfuscating transformations.

- *Generating and Managing Secure Passwords for Online Accounts*
  Moritz Horsch, TU Darmstadt

  In this thesis, we introduce the Password Assistance System (PAS). It makes secure passwords usable for users. This is achieved by automation and comprehensive support. PAS covers all aspects of passwords. It generates, preserves, and changes passwords for users as well as ensures the confidentiality, availability, recoverability, and accessibility of the preserved passwords. This reduces the efforts and activities of users to deal with passwords to a minimum and thus enables users to practically realize secure passwords for their online accounts for the first time.

16:15-17:15 Vergleichende Diskussion und Stimmabgabe

Der CAST e.V. und der Fachbereich "Sicherheit – Schutz und Zuverlässigkeit" der Gesellschaft für Informatik e.V. (GI) vergeben einen Preis für eine hervorragende Leistung im Bereich der IT-Sicherheit. Die Dissertation muss in einem Themengebiet des Fachbereichs Sicherheit bzw. seiner Fachgruppen angesiedelt sein. Preiswürdig sind Arbeiten, die einen Fortschritt für die IT-Sicherheit bedeuten, und solche, die einen Zugewinn von Sicherheit in IT-Anwendungen ermöglichen. Der Preis ist mit 3.000,- Euro dotiert.

Bewerber(innen) sollten die Promotion abgeschlossen haben oder kurz vor dem Abschluss stehen. Die Arbeit darf zum Zeitpunkt der Einreichung nicht länger als 24 Monate abgeschlossen sein. Die Arbeit darf bereits für andere Preise nominiert worden sein.

Die anwesenden Fachexpert(inn)en wählen den einen Preisträger (Publikumsaward).

17:30 Verleihung CAST/GI-Promotionspreis

Empfang

Donnerstag, 26.04.2018 [Raum P-001]

09:00-10:00 Keynote Marina Krotofil, FireEye:

'Race-to-the-Bottom': Evolution of the ICS Threat Landscape

Industrial Control Systems (ICS) threat landscape has changed dramatically over the past few years. New threats have emerged to challenge the shock created by Stuxnet. This talk will present the evolution of the ICS exploits and tactics to picture ongoing „race-to-the-bottom“ situation between ICS threat actors and defenders. Special attention will be given to the relationship between security and safety, and how current cyber threats may undermine traditional safety design decisions. The discussion will “descend” all the way to the physical process, showing that cyber-physical systems cannot be secured only by the means of canonical IT security approaches. Physical world can be exploited by unconventional methods and therefore needs to be taken into consideration when securing ICS.

Marina Krotofil is a Principal Analyst at FireEye (USA). Previously she worked as a Lead Cyber Security Researcher at Honeywell (USA), a Senior Security Consultant at the European Network for Cyber Security (The Netherlands) and as a Research Assistant at Hamburg University of Technology (Germany). She spent almost a decade on discovering unique attack vectors, engineering damage scenarios and understanding attacker techniques when exploiting industrial control systems. In 2017, Ms. Krotofil was involved in investigation of both publicly known ICS attacks associated with the Industroyer and Triton attack frameworks. She authored more than a dozen academic and white papers on industrial security and is a frequent speaker at leading security events around the world (4xBlack Hat, DefCon, CCC, 3xSAS, HITB, Zero Nights, etc.). Ms. Krotofil holds a MBA in Technology Management, M.Sc. in Telecommunication and M.Sc. in Information and Communication Systems.

Kommunikationspause

10:15-11:15 Session 4: Software

Session Chair: Vincent Haupert

- *SDN Ro2tkits: A Case Study of Subverting Closed Source SDN Controllers*
  Christian Röpke, Ruhr-Universität Bochum

  An SDN controller is a core component of the SDN architecture. It is responsible for managing an underlying network while allowing SDN applications to program it as required. Because of this central role, compromising such an SDN controller is of high interest for an attacker. A recently published SDN rootkit has demonstrated, for example, that a malicious SDN application is able to manipulate an entire network while hiding corresponding malicious actions. However, the facts that this attack targeted an open source SDN controller and applied a specific way to subvert this system leaves important questions unanswered: How easy is it to attack closed source SDN controllers in the same way? Can we concentrate on the already presented technique or do we need to consider other attack vectors as well to protect SDN controllers? In this paper, we elaborate on these research questions and present two new SDN rootkits, both targeting a closed source SDN controller. Similar to previous work, the first one is based on Java reflection. In contrast to known reflection abuses, however, we must develop new techniques as the existing ones can only be adopted in parts. Additionally, we demonstrate by a second SDN rootkit that an attacker is by no means limited to reflection-based attacks. In particular, we abuse aspect-oriented programming capabilities to manipulate core functions of the targeted system. To tackle the security issues raised in this case study, we discuss several countermeasures and give concrete suggestions to improve SDN controller security.

- *Source Code Patterns of Buffer Overflow Vulnerabilities in Firefox*
  Felix Schuckert, Max Hildner, HTWG Konstanz
  Basel Katt, NTNU
  Hanno Langweg, HTWG Konstanz & NTNU

  We investigated 50 randomly selected buffer overflow vulnerabilities in Firefox. The source code of these vulnerabilities and the corresponding patches were manually reviewed and patterns were identified. Our main contribution are taxonomies of errors, sinks and fixes seen from a developer’s point of view. The results are compared to the CWE taxonomy with an emphasis on vulnerability details. Additionally, some ideas are presented on how the taxonomy could be used to improve the software security education.

- *Is MathML dangerous?*
  Christopher Späth, Ruhr-Universität Bochum

  HTML5 forms the basis for modern web development and merges different standards. MathML is an example for this. It is used to express and display mathematical statements. However, with more standards being natively integrated into HTML5 the processing model gets inherently more complex. In this paper, we evaluate the security risks of MathML. We created a semi-automatic test suite and studied the JavaScript code execution and the XML processing of MathML. We added also the Content-Type handling of major browsers to the picture. We found two novel ways to execute JavaScript code, with which we were able to bypass several sanitizers. The fact, that JavaScript code embedded in MathML can access session cookies worsens matters even more. Furthermore, we discovered a novel way to manipulate the browser's status line without JavaScript.

Kommunikationspause

11:30-12:30 Session 5: Kritische Infrastrukturen, Policies und Digitale Forensik

Session Chair: Prof. Dr. Thomas Kemmerich

- *Harmonizing physical and IT security levels for critical infrastructures*
  Vanessa Chille, Sybille Mund, Andreas Möller, Siemens AG

  We present a concept for finding an appropriate combination of physical security and IT security measures such that a comprehensive protection is provided. In particular, we consider security for critical infrastructures, such as railway systems. For classifying physical security measures, the so-called Protection Classes from the standard EN 50600 are used in our approach. To provide comprehensive protection for a system under consideration, these sets of explicit physical security measures need to be combined with other kinds of security, such as IT security and organizational security. We present a new classification approach named 'Type of Attack(er)' that allows for taking all aspects of security into joint consideration, and harmonizes physical and IT security levels by creating a link between EN 50600 and IEC 62443.

- *On the possible impact of security technology design on policy adherent user behavior - Results from a controlled empirical experiment*
  Sebastian Kurowski, Fraunhofer IAO
  Nicolas Fähnrich, Universität Stuttgart
  Heiko Roßnagel, Fraunhofer IAO

  This contribution provides results from a controlled experiment on policy compliance in work environments with restrictive security technologies. The experimental setting involved subjects forming groups and required them to solve complex and creative tasks for virtual customers under increasing time pressure, while frustration and work impediment of the used security technology were measured. All subjects were briefed regarding existing security policies in the experiment setting, and the consequences of violating these policies, as well as the consequences for late delivery or failure to meet the quality criteria of the virtual customer. Policy breaches were observed late in the experiment, when time pressure was peaking. Subjects not only indicated maximum frustration, but also a strong and significant correlation (.765, $p<.01$) with work impediment caused by the security technology. This could indicate that user-centred design does not only contribute to the acceptance of a security technology, but may also be able to positively influence practical information security as a whole.

- *Towards Forensic Exploitation of 3-D Lighting Environments in Practice*
  Julian Seuffert, Marc Stamminger, Christian Riess, Friedrich-Alexander-Universität Erlangen-Nürnberg

  The goal of image forensics is to determine authenticity and origin of a digital image or video without an embedded security scheme. Among the existing methods, the probably most well-known physics-based approach is to validate the distribution of incident light on objects of interest. Inconsistent lighting environments are considered as an indication of image splicing. However, one drawback of this approach is that it is quite challenging to use it in practice. In this work, we propose several practical improvements to this approach. First, we propose a new way of comparing lighting environments. Second, we present a factorization of the overall error into its individual contributions, which shows that the biggest error source are incorrect geometric fits. Third, we propose a confidence score that is trained from the results of an actual implementation. The confidence score allows to define an implementation- and problem-specific threshold for the consistency of two lighting environments.

12:30 – 14:00 Kommunikationspause

Buffet [Sponsor des Mittagessens: DB Systel GmbH]

Donnerstagnachmittag mit zwei parallelen Tracks

- Track A SICHERHEIT 2018 [P-001] +SIDAR oder CUES im Anschluss
- Track B Workshop eVoting in der Praxis [P-004]

Track A SICHERHEIT 2018 [P-001]

14:00-15:30 Session 6: Practitioners Track

Session Chair: Bernhard C. Witt

- *Ein integriertes Vorgehensmodell zur Planung und Umsetzung eines ISMS am Beispiel der Pharmaproduktion*
  Robert Geiger, M+W Central Europe GmbH
  Sabrina Krausz, Hochschule Neu-Ulm
  Holger Mettler, M+W Central Europe GmbH

  Der Beitrag stellt ein integriertes Vorgehensmodell zur Planung und Umsetzung eines Informationssicherheitsmanagementsystems (ISMS) für KRITIS Betreiber im pharmazeutischen Produktionsumfeld vor. Es soll Betreibern kritischer Infrastrukturen helfen diese zu schützen und kann einen Beitrag zu einem branchenspezifischen Sicherheitsstandard (B3S) für den Sektor Gesundheit leisten. Es soll mögliche Synergien zu vorhandenen Systemen und Prozessen der pharmazeutischen Qualitätssicherung aufzeigen und zusätzliche Anforderungen der automatisierten Produktion berücksichtigen.

- *Fallstricke bei der Inhaltsanalyse von Mails: Beispiele, Ursachen und Lösungsmöglichkeiten*
  Steffen Ullrich, genua GmbH

  E-Mail ist eine der Hauptangriffswege zur Infektion mit Malware und zum Phishing von Zugangsdaten. Waren Mails vor 1996 auf ASCII-Zeichen und eine Zeilenlänge von 1000 Zeichen beschränkt, so ermöglicht die Nutzung der MIME-Standards heute die Abbildung beliebiger Zeichenkodierungen und binärer Anhänge innerhalb der ursprünglichen Beschränkungen. Die durch die Komplexität und Flexibilität dieser Standards bedingten Implementationsdifferenzen ermöglichen jedoch die Konstruktion von Mails, welche unterschiedlich in Sicherheits- und Endsystemen interpretiert werden. Wir haben exemplarisch untersucht, wie dadurch die Analyse in existenten Sicherheitsprodukten umgangen werden kann und welche Möglichkeiten es gibt, dieses Problem in der Praxis zu addressieren.

- *Introducing DINGfest: An architecture for next generation SIEM systems*
  Florian Menges, Fabian Böehm, Manfred Vielberth, Universität Regensburg
  Alexander Puchta, Nexis GmbH
  Benjamin Taubmann, Noëlle Rakotondravony, Universität Passau
  Tobias Latzo, Friedrich-Alexander-Universität Erlangen-Nürnberg

  Isolated and easily protectable IT systems have developed into fragile and complex structures over the past years. These systems host manifold, flexible and highly connected applications, mainly in virtual environments. To ensure protection of those infrastructures, Security Incident and Event Management (SIEM) systems have been deployed. Such systems, however, suffer from many shortcomings such as lack of mechanisms for forensic readiness. In this extended abstract, we identify these shortcomings and propose an architecture which addresses them. It is developed within the DINGfest project, on which we report and for which we seek initial feedback from the community.

Kommunikationspause

15:45-17:15 Fachgruppensitzung SIDAR Security Intrusion Detection and Response [Raum O-202 im Nachbargebäude]

Die Fachgruppe beschäftigt sich mit der Erkennung und Beherrschung von Sicherheitsvorfällen im Bereich der Informationstechnik. Mehr Informationen: https://fg-sidar.gi.de/

15:45-17:15 Workshop CUES Computerunterstütztes Entwicklungstool für sichere benutzerfreundliche und marktkonforme Sicherheitslösungen [Raum F-007 im F-Gebäude]

Im Forschungsprojekt CUES (siehe http://www.cues-projekt.de/) wurde ein smarter Softwareassistent (Wizard) zur Entwicklung sicherer, benutzerfreundlicher und marktkonformer Sicherheitslösungen umgesetzt. Der Wizard unterstützt Softwareentwickler von Sicherheitslösungen während des gesamten Entwicklungsprozesses anhand von Fragen und darauf basierenden Empfehlungen (Methoden, Best Practices, etc.), um einen ganzheitlichen Softwareentwicklungsansatz zu schaffen. Die vom Empfehlungssystem des Wizards vorgeschlagenen Lösungen stammen aus den Bereichen IT-Sicherheit, Usability und Sozioökonomie. Ziel des Workshops ist das Einholen von Rückmeldungen und Verbesserungsvorschlägen.

17:30 Abfahrt Bus zur Mainau (siehe Seite 20)

Track B Workshop eVoting in der Praxis [P-004]

Workshop Chairs: Prof. Dr. Melanie Volkamer und Prof. Dr. Rüdiger Grimm

14:00-14:05 – Welcome and basic information

14:05-15:05 – Session 1: Polyas, Scytl, Artologik

- Polyas (Germany): **Tomasz Truderung** (Head of Research)
- Scytl (Spain): **Mr. Jordi Puiggalí** (Scytl's CSO and SVP Research & Security), **Mr. Onno van Dommelen** (Scytl's VP Strategic Accounts)
- Artologik Software (Sweden): **Mrs. Linda Braunias** (International Sales Manager)

Kommunikationspause

15:15-16:15 – Session 2: BFH, Smartmatic, Bluekrypt

- BFH (Switzerland): **Prof. Dr. Rolf Haenni**
- Smartmatic-Cybernetica Centre of Excellence for Internet Voting (Estonia): **Sven Heiberg, Jan Willemson**
- Bluekrypt: **Damien Giry** CEO

16:15-16:45 – Open questions for all the presenters

16:45-17:15 Fachgruppensitzung ECOM E-Commerce und E-Government [Raum P-004]

Zwei Aspekte der Sicherheit sind im E-Commerce und E-Government besonders eingehend zu behandeln: erstens die Gefahrenabwehr (von Viren, Datendiebstahl und -verlust, Maskeraden u.a.m bestehender Anwendungen und zweitens die Ermöglichung neuer, sicherheitskritischer Anwendungen. Neue Anwendungen werden ermöglicht durch die Definition und Umsetzung von Sicherheitseigenschaften auf Protokoll- und Anwendungsebene als eine der wesentlichen Voraussetzungen für jegliche E-Anwendungen. Die Fachgruppe E-Commerce & E-Government befasst sich vor allem mit dieser zweiten ("enabling") Rolle von Sicherheit für E-Commerce und E-Government.

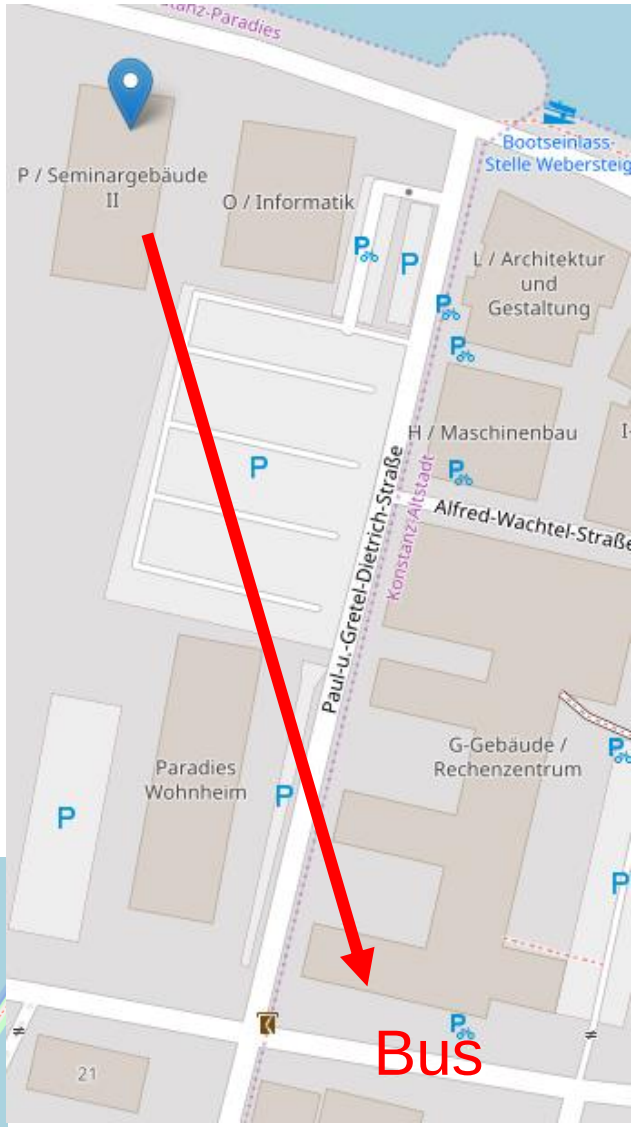
https://fg-ecom.gi.de/

17:30 Abfahrt Bus zur Mainau (siehe Seite 20)

Konferenz-Dinner

17:30 Abfahrt Bus zur Mainau

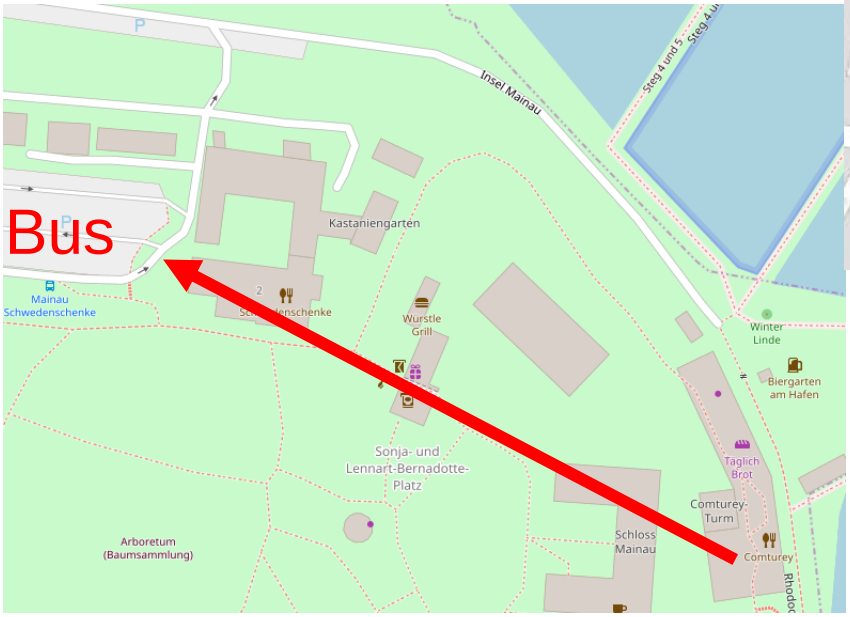
Bus verpasst? Bus „4/13“ ab Bahnhof 00/15/30/45, ab 18:30 alle 30‘, Fahrtzeit 16‘ bis Mainau
Am Mainau-Eingang auf Gruppenzugehörigkeit SICHERHEIT 2018 hinweisen.



ca. 19 Uhr Eröffnung Buffet, Restaurant Comturey

22:30 Rückfahrt Bus ab Mainau,
Parkplatz Schwedenschenke

Bus fährt über Ibis (Benediktinerplatz) und Marktstätte



Freitag, 27.04.2018

09:00-10:00 Keynote Dirk Fox, Secorvo Security Consulting: 10 Schritte zur digitalen Souveränität

Angesichts der wachsenden Komplexität von IT-Systemen, dem Eindringen der IT in immer mehr Lebensbereiche und der Zunahme der Verarbeitung personenbezogener Daten ist „digitale Souveränität" nicht mehr lediglich von mangelnder Medienkompetenz bedroht. Der Vortrag zeichnet die Entwicklung des Internet vom „Schaufenster" zu einer Überwachungsinfrastruktur nach und zeigt auf, welche Verantwortung für die Erhaltung (oder womöglich die Wiederherstellung) von digitaler Souveränität auf die Informatiker von heute und morgen zukommt – und welche Schritte dafür erforderlich sind.

Dirk Fox ist Diplom-Informatiker und Gründer und Geschäftsführer der Secorvo Security Consulting GmbH in Karlsruhe. Er beschäftigt sich seit mehr als 30 Jahren mit Fragen der Informationssicherheit und des Datenschutzes in Forschung, Entwicklung und Beratung. Seit 1997 ist er Herausgeber der Fachzeitschrift „Datenschutz und Datensicherheit" (DuD), seit 2008 Vorstand des IT-Unternehmernetzwerks „CyberForum" in Karlsruhe.

Herr Fox ist Autor von mehr als 150 Veröffentlichungen zur Informationssicherheit und externer Datenschutzbeauftragter mehrerer Unternehmen. Sein Unternehmen wurde mit dem „Landespreis Baden-Württemberg für Junge Unternehmen" (2002), dem „Sicherheitspreis Baden-Württemberg" (2007), dem Preis „Best of Consulting" der WirtschaftsWoche in der Kategorie IT-Strategie (2010) und dem Qualitätssiegel „Top Consultant" (2015) ausgezeichnet.

Kommunikationspause

10:15-11:15 Session 7: Authentisierung und eVoting

Session Chair: Prof. Dr. Rüdiger Grimm

- *Ich sehe was, das du nicht siehst - Die Realität von Mobilebanking zwischen allgemeinen und rechtlichen Anforderungen*
  Vincent Haupert, Gaston Pugliese, Friedrich-Alexander-Universität Erlangen-Nürnberg

  Kürzlich hat die Europäische Kommission die Technischen Regulierungsstandards im Rahmen der Zahlungsdiensterichtlinie II vorgelegt. Sie regeln unter anderem auch die Anforderungen an die starke Kundenauthentifizierung, die für digitale Zahlungsvorgänge zumindest eine Zwei-Faktor-Authentifizierung vorschreiben. Der Beitrag setzt sich mit den rechtlichen Vorgaben auseinander, indem zunächst allgemeine Anforderungen formuliert werden, ehe darauf eingegangen wird, ob und wie Transaktionen auf nur einem mobilen Endgerät diesen Anforderungen genügen können. Hierbei wird die Transaktionssicherheit

der Ein-Gerät-Authentifizierung anhand von smsTAN- und App-basierten Mobilebankingverfahren mittels allgemeiner wie auch rechtlicher Anforderungen bewertet. Es zeigt sich, dass die vorherrschenden Plattformen Android und iOS die Anforderung an ein unkopierbares Besitzelement bereits heute erfüllen können, während eine sichere Anzeige weiter eine Zukunftsaufgabe bleibt, gerade auch, weil der Gesetzgeber klare Anforderungen versäumt hat.

- *Auf dem Weg zu sicheren abgeleiteten Identitäten mit Payment Service Directive 2*
  Daniel Träder, Alexander Zeier, Andreas Heinemann, Hochschule Darmstadt

  Online-Dienste erfordern eine eindeutige Identifizierung der Benutzer und somit eine sichere Authentisierung. Insbesondere eGovernment-Dienste innerhalb der EU erfordern eine starke Absicherung der Benutzeridentität. Auch die mobile Nutzung solcher Dienste wird bevorzugt. Das Smartphone kann hier als einer der Faktoren für eine Zwei-Faktor-Authentifizierung dienen, um eine höhere Sicherheit zu erreichen. Diese Arbeit schlägt vor, den Zugang und die Nutzung einer abgeleiteten Identität mit einem Smartphone zu sichern, um es dem Benutzer zu ermöglichen, sich auf sichere Weise gegenüber einem Online-Dienst zu identifizieren. Dazu beschreiben wir ein Schema zur Ableitung der Identität eines Benutzers mithilfe eines Account Servicing Payment Service Provider (ASPSP) unter Verwendung der Payment Service Directive 2 (PSD2) der Europäischen Union. PSD2 erfordert eine Schnittstelle für Dritte, die von ASPSPs implementiert werden muss. Diese Schnittstelle wird genutzt, um auf die beim ASPSP gespeicherten Kontoinformationen zuzugreifen und daraus die Identität des Kontoinhabers abzuleiten. Zur Sicherung der abgeleiteten Identität ist der Einsatz von FIDO (Fast Identity Online) vorgesehen. Wir bewerten unseren Vorschlag anhand der Richtlinien von eIDAS LoA (Level of Assurance) und zeigen, dass für die meisten Bereiche das Vertrauensniveau substantiell erreicht werden kann. Um diesem Level vollständig gerecht zu werden, ist zusätzlicher Arbeitsaufwand erforderlich: Zunächst ist es erforderlich, Extended Validation-Zertifikate für alle Institutionen zu verwenden. Zweitens muss der ASPSP sichere TAN-Methoden verwenden. Schließlich kann derWiderruf einer abgeleiteten Identität nicht erfolgen, wenn der Benutzer keinen Zugriff auf sein Smartphone hat, das mit der abgeleiteten ID verknüpft ist. Daher ist ein anderes Widerrufsverfahren erforderlich (z. B. eine Support-Hotline).

- *Comparative Usability Evaluation of Cast-as-intended Verification Approaches in Internet Voting*
  Karola Marky, Oksana Kulyk, TU Darmstadt
  Melanie Volkamer, TU Darmstadt & Karlstad University

  Internet Voting promises benefits like the support for voters from abroad and an overall improved accessibility. But it is accompanied by security risks like the manipulation of votes by malware. Enabling the voters to verify that their voting device casts their intended votes is a possible solution to address such a manipulation – the so-called cast-as-intended verifiability. Several different approaches for providing cast-as-intended verifiability have been proposed or put into practice. Each approach makes various assumptions about the

voters‘ capabilities that are required in order to provide cast-as-intended verifiability. In this paper we investigate these assumptions of four chosen cast-as-intended approaches and report the impact if those are violated. Our findings indicate that the assumptions of cast-as-intended approaches (e.g. voters being capable of comparing long strings) have an impact on the security the Internet Voting systems. We discuss this impact and provide recommendations how to address the identified assumptions and give important directions in future research on usable and verifiable Internet Voting systems.

11:30-12:30 Session 8: Cloud

Session Chair: Peter Leo Gorski

- *Secure Remote Computation using Intel SGX*
  David Übler, Johannes Götzfried, Tilo Müller, Friedrich-Alexander-Universität Erlangen-Nürnberg

  In this paper, we leverage SGX to provide a secure remote computation framework to be used in a cloud scenario. Our framework consists of two parts, a local part running on the user’s machine and a remote part which is executed within the provider’s environment. Users can connect and authenticate themselves to the remote side, verify the integrity of a newly spawned loading enclave, and deploy confidential code to the provider’s machine. While we are not the first using SGX in a cloud scenario, we provide a full implementation considering all practical pitfalls, e.g., we use Intel’s Attestation Services to prove the integrity of the loading enclave to our users. We also take care of establishing a secure bidirectional channel between the target enclave and the client running on the user’s machine to send code, commands, and data. The performance overhead of CPU-bound applications using our framework is below 10% compared to remote computation without using SGX.

- *Homomorphe Verschlüsselung für Cloud-Datenbanken: Übersicht und Anforderungsanalyse*
  Lena Wiese, Daniel Homann, Tim Waage, Universität Göttingen
  Michael Brenner, Universität Hannover

  Auslagerung von Daten in Cloud-Datenbanken verspricht eine Reihe von Vorteilen wie reduzierte Wartungskosten, Flexibilität der Ressourcenverteilung und einfache Zugreifbarkeit von nahezu überall. Diese Datenbanken bieten dabei eine Vielzahl von Funktionalitäten, um Berechnungen auf Daten auszuführen. Datensicherheit (einschließlich dem Schutz persönlicher Daten) ist in Cloud-Datenbanken jedoch noch nicht angemessen umgesetzt worden. Konventionelle Verschlüsselungsverfahren garantieren zwar hohe Sicherheit, verhindern aber auch weitere Berechnungen auf den Daten. Modernere homomorphe Verschlüsselungsverfahren versprechen dagegen sowohl Datensicherheit als auch die Möglichkeit, auf verschlüsselten Daten zu rechnen. Das bestehende System FamilyGuard kombiniert bisher eigenschaftsbewahrende Verschlüsselungsverfahren. Um

die Funktionalität auf Aggregationsfunktionen zu erweitern, soll in Zukunft auch homomorphe Verschlüsselung eingesetzt werden. In diesem Artikel geben wir eine Übersicht über diverse Kategorien homomorpher Verschlüsselungsverfahren und ihre Sicherheitsgrundlagen. Im Anschluss stellen wir Anforderungen für den Einsatz homomorpher Verfahren in Cloud-Datenbanken auf.

- *Informationssicherheitskonzept nach IT-Grundschutz für Containervirtualisierung in der Cloud*
  Erik Buchmann, Andreas Hartmann, Hochschule für Telekommunikation Leipzig
  Stephanie Bauer, T-Systems International GmbH

  Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt mit dem IT-Grundschutz eine sichere und wirksame Schutzvorkehrung vor den stetig steigenden Bedrohungen im Kontext der Digitalisierung zur Verfügung. Zwar sind die behandelten BSI-Bausteine herstellerneutral definiert. Gleichwohl beziehen sich die Bausteine auf die sich ändernden Technologien, was eine entsprechende Anpassung erforderlich macht. Mit dem Hintergrund von Cloud basierten IT-Infrastrukturen findet aktuell ein massiver Wandel hinsichtlich eingesetzter Servertechnologien und –dienste hin zu Containervirtualisierung in der Cloud statt. Unternehmen, die ihre IT-Landschaften diesbezüglich transformieren, müssen darum mehr denn je die Sicherheit ihrer Daten gewährleisten. Wir zeigen am Beispiel von Docker Containern, wie der IT-Grundschutz auf diese neuen Herausforderungen anzupassen ist. Wir gehen dabei insbesondere auf die Gefährdungsanalyse, Docker-spezifische Gefährdungen sowie entsprechende Maßnahmen ein.

12:30-13:00 Abschluss SICHERHEIT 2018

Kommunikationspause

Mittagessen auch zum Mitnehmen [Sponsor des Mittagessens: DB Systel GmbH]

Züge: ’03 Zürich (Flughafen), ’22/’52 Singen (Umstieg für Stuttgart), ’40 Offenburg/Karlsruhe

Die nächste GI SICHERHEIT findet 2020 statt

14:00-17:30 Normung zu IT Sicherheit und Datenschutz in Deutschland, Österreich und der Schweiz als Spiegelung der Arbeiten bei ISO/IEC und CEN/CENELEC [P-004]

14:00 Einführung (Kai Rannenberg, Goethe-Universität Frankfurt)

14:10 Spiegelung der ISO/IEC-Normung zu IT Sicherheit und Datenschutz bei JTC 1/SC 27: Thematische Schwerpunkte und Arbeitsweise der Gremien

- 14:10 Schweiz: Das SNV Komitee INB/NK 0149/UK 07 (Markus Soland, SBB AG, Bern)
- 14:40 Österreich: Die AG 001.27 (Stephan Krenn, AIT, Wien)
- 15:10 Deutschland: Der NA 043-01-27 AA (Kai Rannenberg, Goethe-Universität Frankfurt)
- 15:40 Österreich: Die AG 001.18 (Datenschutz) mit in Österreich initiierten Projekten (Ingrid Schaumüller-Bichl, FH Oberösterreich, Linz)

16:10-16:25 Kommunikationspause

16:25 Europäische Aspekte, etwa das neue CEN/CLC/JTC 13 „Cybersecurity and Data Protection“ und seine Spiegelung

16:50 Querbezüge und verwandte Themen

17:30 Abschluss

<kes>/Microsoft-Sicherheitsstudie 2018 gestartet

Die Fachzeitschrift <kes> führt seit 1986 alle zwei Jahre eine Studie durch, um neutrale Zahlen und Fakten zur Lage der Informations-Sicherheit im deutschsprachigen Raum zusammenzutragen.

Um eine möglichst aussagekräftige Basis zu erhalten, bittet die Redaktion der <kes> um Ihre Mithilfe in Form der Teilnahme an der Fragebogenaktion, die auch für Sie selbst einige Vorteile bedeutet:

- Teilnehmer der Studie erhalten die Ergebnisse unmittelbar nach ihrem Erscheinen kostenlos – exklusiv auch in tabellarischer Form.
- Wer seine eigenen Erkenntnisse beisteuert, profitiert von einer erhöhten "Passgenauigkeit" der Ergebnisse durch den Datenanteil des eigenen Hauses.
- Schon das Ausfüllen des Fragebogens dient idealerweise als Möglichkeit zur Reflexion und zum Self-Assessment der eigenen Sicherheitslage.
- Für den Ausfüller gibt es ein kleines persönliches Dankeschön.

Uns ist bewusst, dass Ressourcen knapp sind und das Ausfüllen eines umfassenden Fragebogens nicht "mal eben schnell" nebenher erfolgen kann. Auf der anderen Seite eröffnen gerade die Breite und Tiefe der Fragen erst die gewohnte Qualität der Ergebnisse sowie die Chance zur Selbsteinschätzung.

Die Erhebung zur <kes>/Microsoft-Sicherheitsstudie läuft noch bis zum 16. Mai 2016. Interessierte finden den Fragebogen und weitere Informationen auf www.kes.info/studie2018 – die Teilnahme ist sowohl mit einem ausgedruckten Fragebogen als auch über eine Online-Plattform möglich. Selbstverständlich erfolgt die Auswertung der Fragebögen nur nach vollständiger Anonymisierung – Kontaktdaten werden ausschließlich zur Abwicklung des Versands von Ergebnissen und Geschenken sowie ggf. für eine Einladung zur Teilnahme an Folgestudien genutzt.