

Agenda 2022

Dienstag, 21. Juni 2022

13:45 Kick-Off-Meeting

14:30 Kommen Sie entspannt im Palace Hotel an und begrüßen Sie Ihre Fachkolleg:innen. Nach einem Kaffee oder Tee steigen Sie ein in die ersten Agendapunkte der OMNISECURE 2022.

14:30 DIGITALE VERTRAULICHKEIT / VS



15:30

FORUM 1-A | LECTURES

VS-Anforderungsprofile - Standard des BSI für VS-verarbeitende Systeme

VS-Anforderungsprofile sind seit 2017 Jahren ein unverzichtbarer Teil der Zulassungsstrategie geworden. Diese Session zeigt ausgehend von den Erfahrungen der letzten 4 Jahre die immer besser werdende Einbettung in das weiterentwickelte, regulatorische Umfeld und gibt Einblicke in die strategische Weiterentwicklung der Standards.



Thomas Borsch (Moderation)

Referent im Referat KM 12 - Zulassung von VS-Produkten / Abteilung KM - Krypto-Technik und IT-Management, Bundesamt für Sicherheit in der Informationstechnik (BSI)



Ingo Hahlen

Referent im Referat KM 12, Bundesamt für Sicherheit in der Informationstechnik BSI



Daniel Janiszczak

Referat KM 12 - Zulassung von VS-Produkten, Bundesamt für Sicherheit in der Informationstechnik BSI



Dr. Bertolt Krüger

Leiter der Common Criteria Prüfstelle, SRC Security Research & Consulting GmbH



Basicwissen: Quantensichere Kryptografie

Die Entwicklung leistungsfähiger Quantencomputer bedroht die heute eingesetzte Public-Key-Kryptografie. Zurzeit wird entsprechend an der Entwicklung, Standardisierung und Implementierung von quantensicheren Alternativen gearbeitet. Hierfür gibt es im Wesentlichen zwei Ansätze: Post-Quanten-Kryptografie und Quantum Key Distribution. Diese beiden Ansätze sollen in dem Tutorial vorgestellt werden.

Einführung in die Post-Quanten-Kryptografie (Dr. Heike Hagemeyer)

Als Post-Quanten-Kryptografie bezeichnet man kryptografische Verfahren, von denen man annimmt, dass sie auch mit einem Quantencomputer nicht gebrochen werden können. Im Vortrag soll die Notwendigkeit für den Wechsel motiviert, einige grundlegende Begriffe erläutert und die wesentlichen Entwicklungen im Bereich Post-Quanten-Kryptografie in den letzten Jahren vorgestellt werden.

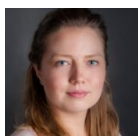
Einführung in die Quantum Key Distribution (Stephanie Reinhardt)

Quantum Key Distribution (kurz QKD) umfasst Protokolle zur Schlüsseleinstellung, deren Sicherheit zumindest theoretisch auf den Gesetzmäßigkeiten der Quantenmechanik beruht und die resistent gegen Angriffe mit klassischen und Quanten-Computern sein sollen. Aktuell wird QKD viel Aufmerksamkeit gewidmet und es gibt zahlreiche Aktivitäten zur Entwicklung und Implementierung auf nationaler, europäischer und internationaler Ebene. In diesem Vortrag wird erklärt, wie QKD funktioniert und einige wichtige Sicherheitsaspekte werden diskutiert.



Dr. Heike Hagemeyer

Referat KM 21 - Vorgaben an und Entwicklung von Kryptoverfahren, Bundesamt für Sicherheit in der Informationstechnik BSI



Stephanie Reinhardt

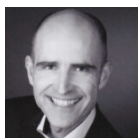
Referentin im Referat KM 21 Vorgaben an und Entwicklung von Kryptoverfahren, Bundesamt für Sicherheit in der Informationstechnik BSI



FORUM 1-C | LECTURES

Überblick zur Entwicklung von Satellittensicherheit

Öffentliche Nutzer wie Such- und Rettungsdienste, Polizei oder Feuerwehren benötigen eine hohe Verfügbarkeit ihrer digitalen Infrastrukturen wie Kommunikation oder Navigation, zu jeder Zeit und an jedem Ort. Um dieses Ziel zu erreichen, sind satellitengestützte Dienste ein wesentlicher Bestandteil der gesamten Kommunikationsszenarien und bedürfen daher eines ausreichenden Schutzniveaus, Deutschland treibt diese Entwicklung voran. Die Session liefert einen Überblick über die aktuelle Situation der Entwicklung von sicheren GNSS-Empfängern.



Frank Christophori

Referatsleiter KM 16 - Sichere IT-Systeme für Luft-und Raumfahrt, Bundesamt für Sicherheit in der Informationstechnik (BSI)



Alexander Rügamer

Gruppenleiter Spezialisierte SatNav-Empfänger, Fraunhofer-Institut für Integrierte Schaltungen IIS

Kaffeepause | Lobby + Ausstellung



FORUM 2-A | TUTORIAL

Die Smartcard ist tot – lang lebe das integrierte Secure Element!

Smartcard-basierte Identitätslösungen werden zunehmend durch Secure Elements ersetzt, die fest an Mobiltelefonen, IoT-Geräte, oder Fahrzeuge gebunden sind. Ein entscheidender neuer Trend ist die Integration von Sicherheitsprozessoren in komplexe System-on-Chip Designs. Dieses Tutorial diskutiert die sich daraus ergebenden Herausforderungen für effiziente Sicherheitsevaluierungen.



Dr. Karsten Klohs

achelos GmbH, Director Business Development Security Engineering

15:50
16:30

DIGITALE INTELLIGENZ



FORUM 2-C | TUTORIAL

Integration und Einbettung von Hochgeschwindigkeitsverschlüsslern in bestehende Netzwerke und Arbeitsumgebungen

Der Einsatz von Krypto-Lösungen im Bereich der Netzwerkverschlüsselung kann viel Einfluss auf Netzwerkarchitektur und Management-Systeme mit sich bringen, zudem gibt es möglicherweise Auswirkungen auf das Betriebskonzept von Netzwerken. Der Vortrag erläutert wie mit „Security Made in Germany“ sensible Netzwerke abgesichert werden können mit dem Ziel der möglichst einfachen Einbindung in vorhandenen Strukturen und effizientem Betrieb.



Martin Wilske

Director R&D Network Encryption, Rohde & Schwarz Cybersecurity GmbH

16:30
17:00

Kaffeepause | Lobby + Ausstellung



FORUM 3-A | TUTORIAL

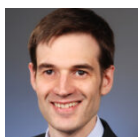
Basicwissen: Seitenkanalangriffe - Praxis und Theorie

Seitenkanalangriffe spielen bei der Evaluierung von IT-Sicherheitsprodukten eine wichtige Rolle. Dieses Tutorial führt in die Thematik ein, indem praktische Angriffe demonstriert und Auswertungsmethoden vorgestellt werden, um z.B. aus dem Stromverbrauch den geheimen Schlüssel zu bestimmen. Dabei finden Ansätze aus der Stochastik, aber auch aus dem Bereich der künstlichen Intelligenz Anwendung.



Prof. Dr. Werner Schindler

Referatsleiter KM 22 - Prüfung von Kryptoverfahren, Bundesamt für Sicherheit in der Informationstechnik BSI



Dominik Klein

Referent, Referat TK11 Sichere Halbleiter-Technologien, Bundesamt für Sicherheit in der Informationstechnik BSI



Dr. Friederike Laus

Referentin im Referat KM 22 - Prüfung von Kryptoverfahren, Bundesamt für Sicherheit in der Informationstechnik BSI



FORUM 3-B | TUTORIAL

Codyze - ein Schritt zur automatisierten Nachweisführung

Durch den Trend agiler Entwicklungsprozesse und der steigenden Komplexität von IT-Sicherheitsprodukten wächst auch der Evaluierungsaufwand auf Seiten des BSI und beauftragter Prüfstellen im Kontext der Zulassung und Zertifizierung. In diesem Vortrag soll das vom BSI beauftragte und von dem Fraunhofer AISEC entwickelte Codeanalysewerkzeug „Codyze“ als Gegenmaßnahme vorgestellt werden.



Christian Banse

Abteilungsleiter des Bereichs Service und Application Security, Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC

17:00

17:40

DIGITALE IDENTITÄT



FORUM 3-C | WORKSHOP

Gemeinsame Entwicklung einer europäischen Perspektive für digitale Identität

Die Verwendung der elektronischen Identifikation (eID) variiert in Europa mit entwickelten Pionierländern in den nordischen Ländern, Schwellenländern wie BeNeLux sowie Nachzüglern in Mittel- und Südeuropa. Gleichzeitig wird mit der eIDAS-Verordnung ein europaweiter Rahmen geschaffen, und die Europäische Kommission hat die Einführung einer digitalen Geldbörse angekündigt. Gemeinsam untersuchen wir die Gründe für das unterschiedliche Nutzungsverhalten von eIDs und entwickeln Zukunftsszenarien vor dem Hintergrund aktueller Markt- und Regulierungsentwicklungen.



Frank Wunderlich

Partner, Arkwright Consulting AG

17:40

18:00

Kaffeepause | Lobby + Ausstellung



ERÖFFNUNGSREDE DES BEAUFTRAGTEN DER BUNDESREGIERUNG FÜR INFORMATIONSTECHNIK

Nutzerzentrierung und neue föderale Kooperation: Bausteine für eine zukunftsfähige Verwaltung

Die Digitalisierung ist Treiber des größten Transformationsprozesses der deutschen Verwaltung – dessen Herzstück ist das OZG. Sein transformativer Charakter bezieht sich dabei nicht nur auf die Übertragung von Verwaltungsleistungen in das Internet, sondern zeigt sich auch in einer neudefinierten föderalen Zusammenarbeit und gesteigener Bedeutung gemeinsamer Standards.

In den vergangenen zwei Jahren ist es so gelungen, erste Erfolge zu erzielen. Ein Grundstein dafür war es, landesübergreifende Qualitätsprinzipien transparent festzulegen, welche die nutzerzentrierte Gestaltung sowie hohe Zuverlässigkeit und IT-Sicherheit digitaler Verwaltungsservices sicherstellen.

Die Nutzerzentrierung wird weiter wichtigste Leitplanke der immer schneller voranschreitenden OZG-Umsetzung sein. Nur wenn die Angebote einfach und nutzerfreundlich sind, werden Bürgerinnen und Bürgern sie auch nutzen.



Dr. Markus Richter

Staatssekretär im Bundesministerium des Innern, für Bau und Heimat und Beauftragter der Bundesregierung für Informationstechnik



FORUM 5-A | PANEL

Endspurt Onlinezugangsgesetz

Das Onlinezugangsgesetz setzt eine Frist bis Ende 2022 für das Angebot von 575 durchgehend digitalisierten Verwaltungsprozessen. Wie ist der Umsetzungsstand beim Bund, in den Ländern und vor allem bei den Kommunen?

Noch sind ganz wesentliche Teilprojekte in Arbeit, wie beispielsweise das einheitliche Unternehmenskonto oder das Datenschutz-Cockpit. Wie realistisch ist die Umsetzung bis Jahresende?



Dr. Stephan Klein (Moderation)

CEO, Governikus KG



Dr. Markus Richter

Staatssekretär im Bundesministerium des Innern, für Bau und Heimat und Beauftragter der Bundesregierung für Informationstechnik

Come Together

Der erste Networking Abend der OMNISECURE 2022

Die Netzwerke rund um die digitale Identität bewegen und verändern sich kontinuierlich. Neue Impulse und lange Erfahrung brauchen sich gegenseitig – und müssen zueinander gebracht werden. Auch der Vorabend des Kongresses dient ganz dieser Aufgabe: In Kooperation mit dem Digital Society Institut DSI sind Sie eingeladen zum ersten Come Together der Referenten und Teilnehmenden.

Der Abend wird musikalisch begleitet von KellerJazz + Guests.

Hotel Palace

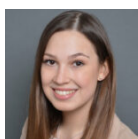
Budapester Straße 45 – 10787 Berlin

Mittwoch, 22. Juni 2022



Schaufenster Sichere Digitale Identitäten

Digitale Identitäten sind das Schlüsselement einer sicheren und nachhaltigen Digitalisierung. Mit dem Schaufensterprogramm „Sichere Digitale Identitäten“ fördert das Bundesministerium für Wirtschaft und Energie (BMWi) Projekte, die herausragende Ansätze für offene, interoperable und einfach nutzbare ID-Ökosysteme in Modellregionen in ganz Deutschland entwickeln und anwendungsnah erproben. In der 60-minütigen Vortragssession werden die Referent:innen eine erste Zwischenbilanz ziehen und einen Ausblick geben.



Franziska Granc (Moderation)

Projektmanagerin Sichere Digitale Identitäten, Nimbus Technologieberatung GmbH



Dr. Stefan Afting

Referent KI 3, Bundesministerium für Wirtschaft und Energie BMWi



Prof. Dr.-Ing. Jürgen Anke

Professur für Softwaretechnologie und Informationssysteme, Hochschule für Technik und Wirtschaft Dresden



Peter Eisenhofer

Product Manager, yes IDP GmbH



Walter Landvogt

Projektkoordinator ONCE, Bundesdruckerei GmbH



Richard Wacker

Innovation Manager, CAS Software AG



FORUM 6-B | PANEL

Hinein in viele Branchen: E-Justice auf Erfolgsspur

Früher ein Thema ausschließlich für Justiz und Verwaltung, weitet sich nun auf nahezu alle Rechtsabteilungen von Unternehmen und Organisationen aus: der elektronische Rechtsverkehr. Das sog. eJustice-Gesetz sieht für die Kommunikation mit der Justiz zwingend neben der (gescheiterten) De-Mail nur noch eigene Lösungen vor, auch für Bürger:innen. Wie gehen Banken, Sparkassen oder Versicherungen damit um?



Dr. Stephan Klein (Moderation)

CEO, Governikus KG



Matthias Drefs

Bereichsleiter Business Development | Forschung und Entwicklung, S-Markt & Mehrwert GmbH & Co. KG



Thomas Lämmrich

Abteilungsleiter Rechtsschutz, Gesamtverband der Deutschen Versicherungswirtschaft e.V. GDV



Dr. Martin Wachter

Ministerialrat, Bayerisches Staatsministerium der Justiz

09:00
10:00

DIGITAL PAYMENT



FORUM 6-C | LECTURES

Wo stehen wir mit dem Rollout von «Click to Pay»

Verschiedene E-Commerce Prozesse wurden in den letzten Jahren verbessert – EMV 3DS löst 3DS 1.0 ab, die E-Commerce Tokenisierung löst Card-on-File ab. Bis jetzt blieb aber der sogenannte Guest Checkout, bei dem die Kartendaten jeweils in Gänze neu eingetippt werden müssen, unberührt. Hier greift «Click to Pay» ein und soll Abhilfe schaffen.



Dr. Thomas Fromherz (Moderation)

Chief Strategy Officer, Payments, Netcetera AG

10:00
10:20

Kaffeepause | Lobby + Ausstellung

10:20
11:00

DIGITALE INTELLIGENZ



FORUM 7-A | TUTORIAL

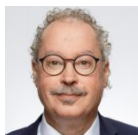
Künstliche Intelligenz und Verbraucherinformation

KI-Systeme finden zunehmend im Verbraucherkontext Anwendung, zum Beispiel bei Bewerbungsverfahren, im Gesundheitssektor oder in sozialen Netzwerken. Im Tutorial wird das vom BMVI geförderte „Zentrum für vertrauenswürdige Künstliche Intelligenz“ (ZVKI) vorgestellt, das an den Schnittstellen zu Wissenschaft, Wirtschaft, Politik und Zivilgesellschaft zu Verbraucherschutz und KI forscht und informiert.



Dr. Wiebke Glässer

Geschäftsführerin, iRights.Lab GmbH



Prof. Dr. Christian Kastrop (angefragt)

Staatssekretär im Bundesministerium der Justiz und für Verbraucherschutz

10:20
11:00

DIGITALE IDENTITÄT



FORUM 7-B | TUTORIAL

Elektronische Identitäten als Schlüssel für die Netze der Zukunft

Der Netzwerkperimeter als Stelle für die Durchsetzung von Zugriffsrechten hat zwar noch nicht ausgedient, verliert aber an Bedeutung. Rechte können nicht mehr zuverlässig auf Basis von Zugehörigkeit zu einem Netzwerk vergeben werden, sondern sollten abhängig von der Identität eines Nutzers oder Geräts sein. Diese Sicherheitsarchitektur wird unter dem Begriff „Zero-Trust“ zusammengefasst. Im Tutorial geben wir einen Überblick über bestehende Ansätze, zu erwartende Herausforderungen und berichten von ersten praktischen Erfahrungen.



Claas Lorenz

Senior Technology Analyst und stellv. Forschungsleiter, genua GmbH



Dr. Moritz Schmitt

Software-Entwickler in der Gruppe Intrapreneurship (IPS), genua GmbH

10:20
11:00

DIGITALE VERTRAULICHKEIT / VS



FORUM 7-C | TUTORIAL

Einführung in die VS-NfD-konforme E-Mail- und Datei-Verschlüsselung

Die VS-NfD-konforme E-Mail- und Datei-Verschlüsselung, wie zahlreiche Behörden sie benötigen, stellt hohe Sicherheitsanforderungen, muss aber dennoch benutzerfreundlich sein. Dieser Vortrag stellt die wichtigsten Lösungen vor. Hierbei kommen auch die unterschiedlichen Formate (S/MIME und OpenPGP) zur Sprache, die idealerweise beide unterstützt werden.



Marco Smeja

CEO, cv cryptovision GmbH

11:00
11:20

Kaffeepause | Lobby + Ausstellung



FORUM 8-A | PANEL

Demokratie in Gefahr - Wie gefährlich ist die Mehrheit?

Das Zeitalter der Informationstechnologie vernetzt Millionen von Menschen. Der Fortschritt führt auch zur Überforderung, die viele Benutzer des Systems im Sinne einer Entlastung in Gruppierungen mit Alternativ-Realitäten bis hin zur Verschwörungstheorien lockt. Die verlockend „einfache Weltsicht“ wird bereits erfolgreich zur Manipulation der angeschlossenen Benutzer verwendet. Der „mündige Bürger“ steht dabei auf dem Prüfstand – ist er wirklich der Täter oder eher das Opfer?

Die Podiumsdiskussion mit Experten auf den Gebieten der Medienwissenschaften, Ethik, Politik und Netzwerktechnologie soll Impulse liefern, die im Kontext einer kritischen Masse stehen, die zukünftig mehrheitsentscheidend in einem demokratischen System sein kann. Auch sollen Ideen zur Sprache kommen, die einer möglichen Entwicklung entgegenwirken.



Helmut Scherzer (Moderation)

Security Analyst



Prof. Dr. Michael Zürn

Direktor der Abteilung Global Governance am WZB und Professor für Internationale Beziehungen an der Freien Universität Berlin



FORUM 8-B | PANEL

Cyber Security – An International View

Es ist allgemein bekannt, dass Digitalisierung nicht an den nationalen Grenzen aufhört. Daher ist es heutzutage unabdingbar, europäische und internationale Entwicklungen zu betrachten. In dieser Session schauen wir bewusst über den deutschsprachigen Tellerrand hinaus und betrachten ausgewählte Projekte aus anderen Ländern.



Dr. Silke Bargstädt-Franke (Moderation)

Abteilungsleiterin Cyber-Sicherheit in der Digitalisierung und für elektronische Identitäten, Bundesamt für Sicherheit in der Informationstechnik BSI



N.N., Serbien



N.N., Polen (angefragt)



N.N., Finnland (angefragt)



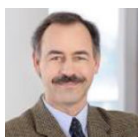
N.N., Singapur (angefragt)



FORUM 8-C | PANEL

Digitale Souveränität am Beispiel Mikroelektronik

Mit Important Project of Common European Interest Microelectronics II (IPCEI-ME II) wird die zweite Phase der Förderung der Halbleiterindustrie in Europa gestartet. Neben Chipdesign und der Entwicklung modernster Fertigungsprozesse stehen auch neue Bauvorhaben von Produktionsstätten in Europa auf dem Programm. Die Panel-Teilnehmer reflektieren die Ziele und Maßnahmen dieses EU- bzw. BMWi-Projekts.



Dr. Detlef Houdeau (Moderation)

Senior Director Digital Security Solution, Infineon Technologies AG



Dr. Christina Schmidt-Holtmann

Leiterin des Referats Ökosystem der Künstlichen Intelligenz, Datenverfügbarkeit, SprinD, Bundesministerium für Wirtschaft und Energie BMWi



Dr. Angelika Iberl

Senior Director Industrial Policy, Infineon Technologies AG

Mittagsbuffet | Lobby + Ausstellung



FORUM 9-A | TUTORIAL

VPN-Lösung für VS-NfD mit BSI-Zulassung: die Zukunft ist Software!

Bei der sicheren Kommunikation von „Verschlusssachen – Nur für den Dienstgebrauch“ (VS-NfD) spielt die Sicherheit aller eingesetzten Hardware- und Softwarekomponenten eine besonders große Rolle. So auch bei der unter anderem für Homeoffice und im mobilen Umfeld eingesetzten VPN-Lösung. Der NCP VS GovNet Connector und der NCP Secure VPN GovNet Server verfügen über eine BSI-Zulassung. Beide Softwarekomponenten können gemeinsam zur sicheren Bearbeitung und Übertragung von VS-NfD eingesetzt werden.



Swen Baumann

Head of Product Management, NCP engineering GmbH

13:40
14:20



FORUM 9-B | WORKSHOP

Von der Produktzulassung zur Herstellerqualifizierung - eine Einführung für Hersteller

Im Rahmen von Zulassungen von Produkten, die für die Verarbeitung von eingestuften Informationen gedacht sind, bietet das BSI seit einiger Zeit die sogenannte ‚Herstellerqualifizierung‘ an. Die Anforderungen im Bereich Lebenszyklusunterstützung (Sicherheit der Entwicklungsumgebung, Auslieferungsprozesse, Konfigurationsmanagement, etc.) sind für die Herstellerqualifizierung allerdings deutlich höher als bei reinen Produktzulassungen. Diese Anforderungen betreffen im wesentlichen Infrastruktur, Tools und Prozesse des Herstellers und können für diesen eine nicht zu unterschätzende Herausforderung darstellen.

Der Workshop erklärt die wesentlichen Aspekte der Herstellererklärung im Vergleich zu Produktzulassungen und skizziert gängige Umsetzungen. Die Session richtet sich in erster Linie an Hersteller von Produkten zur Verarbeitung eingestufte Informationen.

Michael Vogel

atsec information security GmbH, Geschäftsführer

13:40
14:20

DIGITALER BÜRGER & VERWALTUNG



FORUM 9-C | WORKSHOP

Architektur einer selbstverwalteten substantiellen Bürgeridentität für Behörden und Wirtschaft



Thomas Maier

Senior Berater Web- and Application Security, secunet Security Networks AG

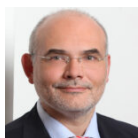
14:20
14:40

Kaffeepause | Lobby + Ausstellung



FORUM 10-A | LECTURES

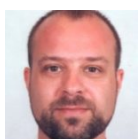
Der beste Weg zum qualifizierten Vertrauensdienst gemäß eIDAS

**Enrico Entschew (Moderation)**

Senior Technical Product Manager PKI, D-Trust GmbH

**Arno Fiedler**

Owner & CEO, Nimbus Technologieberatung GmbH

**Konstantin Götze**

Leiter des Referates Elektronische Vertrauensdienste, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

**Matthias Wiedenhorst**

Leiter Zertifizierungsfachbereich TSP, TÜV Informationstechnik GmbH TÜViT



Kryptografie im Wandel

Quantencomputer haben erhebliche Auswirkungen auf heute eingesetzte kryptografische Verfahren. Ziel der Session ist es, diese Folgen zu erläutern und mögliche Lösungsvorschläge zu diskutieren. Dabei wird auf den aktuellen Stand der Wissenschaft eingegangen, der Standardisierungsprozess in diesem Bereich betrachtet und auch Fortschritte bei der praktischen Umsetzung aufgezeigt.



Prof. Dr. Marian Margraf (Moderation)

Institut für Informatik, Fachbereich Mathematik und Informatik, Freie Universität Berlin



Dr. Heike Hagemeier

Referat KM 21 - Vorgaben an und Entwicklung von Kryptoverfahren, Bundesamt für Sicherheit in der Informationstechnik BSI



Tudor A. A. Soroceanu

Wissenschaftlicher Mitarbeiter Post-Quantum Cryptography, Efficient Cryptographic Algorithms, Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC



Benjamin Zengin

Wissenschaftlicher Mitarbeiter, Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC

14:40

DIGITALE GESUNDHEIT



15:40

FORUM 10-C | LECTURES

Die Digitalisierung des Gesundheitswesens – von digitaler Pandemiebekämpfung bis zur Telematikinfrastruktur 2.0

Vielfältige Themen, wie die Etablierung der Corona-Warn-App als Werkzeug der digitalen Pandemiebekämpfung, des digitalen Impfnachweises als sichere und elektronisch prüfbare Dokumentation eines Impfstatus sowie die Fortentwicklung der Telematikinfrastruktur hin zu einer für die Versicherten offenen Plattform für Gesundheitsanwendungen sind Wegweiser für die Entwicklung der Digitalisierung im Gesundheitswesen. In dieser Vortrags-Session geben Experten einen Überblick über diese Entwicklung und bewerten die sich ergebenden Herausforderungen für die Informationssicherheit.



Thomas Gast (Moderation)

Fachbereichsleiter DI 2 Cyber-Sicherheit in der Digitalisierung, Bundesamt für Sicherheit in der Informationstechnik BSI

15:40

Kaffeepause | Lobby + Ausstellung

16:00

16:00
17:10

DIGITALE IDENTITÄT



FORUM 11-A | PANEL

eIDAS Identifizierungs- und Vertrauensdienste: ein guter Markt?



Arno Fiedler (Moderation)

Owner & CEO, Nimbus Technologieberatung GmbH



Dr. Dirk Woywod

CTO, VERIMI GmbH



Jörg-Matthias Lenz (angefragt)

Direktor Marketing & Kommunikation, Namirial Deutschland GmbH



Sebastian Schulz (angefragt)

Product Manager for Client Certificates, GlobalSign

16:00
17:10

DIGITALE GESUNDHEIT



FORUM 11-B | PANEL

Was bringt Elektronische Patientenakte und Gesundheitskarte tatsächlich dem Bürger?



Christof Basener (Moderation)

Director eHealth Solutions, achelos GmbH



Prof. Dr. Klemens Budde

Leitender Oberarzt der Medizinischen Klinik mit Schwerpunkt Nephrologie und Internistische Intensivmedizin, Charité Universitätsmedizin Berlin



FORUM 11-C | PANEL

Formulare signieren per Online-Banking

Je nach Bundesland erfordern 12% bis 14% der OZG-Leistungen eine Unterschrift. Um auch diese Leistungen durchgehend digital anbieten und bearbeiten zu können, bieten erste Kommunen ihren Bürger:innen das Signieren per Online-Banking an. Denn wer hat schon eine Signaturkarte und einen Kartenleser? Wie gut, dass die EU mit der eIDAS-Verordnung solche qualifizierten Fernsignaturen ermöglicht hat.



Dr. Stephan Klein (Moderation)

CEO, Governikus KG



Gerd Rüter

Leiter Produktmanagement Identity & Trusted Services, Bank-Verlag GmbH



Andreas Hünnebeck

Business Development Digital Identity, Atruvia AG



Yvonne Rowoldt

Koordination E-Government, Landkreis Nordwestmecklenburg



Dr. Karen Verbist

Leitung Fachdienst Digitalisierung, Magistrat der Universitätsstadt Marburg



Annika Biglmaier

Produktmanagerin, Sparkassen-Finanzportal GmbH



FORUM 12-A | KEY NOTE

Digital transformation requires Trust

Industry, public sector, defense and many more domains are facing their digital transformation. Success critically depends on trusted solutions for secure digital interactions. Trust in identity, integrity, communication, data protection, as well as cyber-security and cyber-resilience. Trust in converging solutions across historically separate vertical markets such as telecom, banking, government and mobility. Philippe Vallée's presentation highlights the challenges and opportunities, both globally and specifically in Germany.



Philippe Vallée

Executive Vice President, Digital Identity and Security, Thales Group



FORUM 13-A | PANEL

Digitalization as the Major Transformation Driver for a Wide Range of Domains

Die Digitalisierung ist der wichtigste Transformationsmotor für eine Vielzahl von Bereichen wie Industrie, öffentliche Dienste, Verteidigung. Sie kann nur erfolgreich eingesetzt werden, wenn Mensch und Maschine sicher miteinander kommunizieren können. Dies erfordert Lösungen für Identifikation, Datenschutz sowie Cyber-Security für die zugrunde liegende Infrastruktur. In diesem Zusammenhang konvergieren historisch getrennte Märkte wie Telekommunikation, Bankwesen, Staat und Mobilität zunehmend. Die Nutzer teilen sich digitale Identitäten zwischen diesen Domänen und die gleichen Technologien kommen ins Spiel.

Welche großen Trends sowie Herausforderungen und Chancen sind erkennbar, sowohl global als auch spezifisch in Europa und Deutschland. Wie lässt sich diese Dynamik in den verschiedenen Märkten vergleichen?



Axel Deininger

Vorsitzender des Vorstands, secunet Security Networks AG



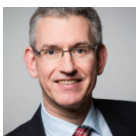
Arne Schönbohm

Präsident des Bundesamtes für Sicherheit in der Informationstechnik BSI



Philippe Vallée

Executive Vice President, Digital Identity and Security, Thales Group



Klaus Lenssen

CSO, Head of Security & Trust Office Germany & Konzern-Sicherheitsbevollmächtigter, Cisco Systems Deutschland GmbH



Carsten Loschinsky

Vice President Marketing Connected Secure System, Infineon Technologies AG

19:00
00:00

Come Together | Lobby + Ausstellung

Willkommen zu unserer Open-End-Kontaktbörse mit großem Buffet. Musikalisch wird der Abend begleitet vom Bad Boys Club 46.



Donnerstag, 23. Juni 2022

09:00
10:00

DIGITALE VERTRAULICHKEIT / VS



FORUM 14-A | LECTURES

Herausforderungen beim Aufbau einer Cloud für die Bundesverwaltung

Wer spricht über was?



Quantentechnologie & QKD

Quantentechnologien haben das Potenzial, diverse Technologiebereiche grundlegend zu verändern und völlig neue Möglichkeiten zu eröffnen. Für die IT-Sicherheit stellen Quantentechnologien sowohl eine Bedrohung als auch eine Chance dar: Durch die Entwicklung hinreichend leistungsfähiger Quantencomputer ist ein großer Teil der heute eingesetzten Public Key-Kryptografie bedroht; gleichzeitig liefert die Quantenkommunikation eine mögliche quantensichere Alternative zu diesen kryptografischen Verfahren. In dieser Session werden die Auswirkungen von Quantentechnologien auf die IT-Sicherheit sowie Forschungs- und Entwicklungsaktivitäten in diesem Bereich thematisiert.



Dr. Manfred Lochter (Moderation)

Referent Abteilung Krypto-Technik und IT-Management, Bundesamt für Sicherheit in der Informationstechnik BSI



Dr. Robert Axmann

Leiter Quantencomputing Initiative, Deutsches Zentrum für Luft- und Raumfahrt e.V. DLR



Dr. Christoph Glingener

Chief Technology Officer, ADVA Optical Networking SE



Dr. Tobias Hemmert

Referent im Referat KM 21 „Vorgaben an und Entwicklung von Kryptoverfahren“, Bundesamt für Sicherheit in der Informationstechnik BSI

09:00
10:00

DIGITALE INTELLIGENZ



FORUM 14-C | LECTURES

Fortschritte & aktuelle Themen in der KI

Die KI-Forschung wird sogar in der Politik als Symbol für Zukunftstechnologie immer wieder genannt und gefördert. Doch wo stehen wir derzeit – Was können wir schon? – Woran arbeiten wir? – Welches sind die wichtigsten Anwendungen?

Die Session beantwortet diese Fragen mit einem Überblick über den heutigen Forschungsstand. Weiterhin wird ein konkretes Projekt vorgestellt, welches einen Einsatz der KI im Bildungssektor umsetzt und verbessertes „Lernen“ verspricht.



Helmut Scherzer (Moderation)

Security Analyst



Barbara Engels

Digital Economist, Institut der deutschen Wirtschaft (IW)



Prof. Dr. Jochen Kuhn

Lehrstuhl für Didaktik der Physik, TU Kaiserslautern

10:00
10:20

Kaffeepause | Lobby + Ausstellung

10:20
11:00

DIGITALE IDENTITÄT



FORUM 15-A | TUTORIAL

Mediale Identitäten: Angriffsmöglichkeiten und Schadenspotentiale

10:20
11:00

DIGITAL PAYMENT



FORUM 15-B | TUTORIAL

QR-Codes in aller Munde – NFC Tags im Hinterkopf

In jüngerer Zeit schießen in Europa QR-Code Lösungen aus dem Boden. Und oft sind es tatsächlich (Zahlungs)Anwendungen, die eine Lücke in den bestehenden Zahlungsmöglichkeiten füllen. Was dabei vergessen geht – es gibt für gewisse (Zahlungs)Situationen eine bessere Alternative: den NFC Tag.



Dr. Thomas Fromherz

Chief Strategy Officer Payments, Netcetera AG

10:20
11:00

DIGITALE VERTRAULICHKEIT / VS



FORUM 15-C | TUTORIAL

Zulassung für VS - Minimierung von Aufwänden durch verkettete Prozesse und optimierten Einsatz von Tools

Bei der Produktzulassung durch das BSI werden nicht nur die Sicherheitsaspekte des Produktes selbst evaluiert, es wird auch ein besonderes Augenmerk auf die dazugehörige Prozesslandschaft gelegt. Durch die Verkettung von verschiedenen Softwaretools kann eine automatisierte und lückenlose Kontrolle des gesamten Produktlebenszyklus sicher und nachvollziehbar abgebildet werden.



Ulrich Schlegel

Product Line Management Director, ADVA Optical Networking SE

11:00
11:10

Kaffeepause | Lobby + Ausstellung

11:20
12:00

DIGITALE WIRTSCHAFT



FORUM 16-A | TUTORIAL

Vertrauensinfrastrukturen im Kontext von Industrie 4.0 – Anforderungen und Lösungsbausteine

Das Tutorial beschäftigt sich mit der Gestaltung automatisierter Geschäftsbeziehungen entlang der Supply Chain. Geschäftspartner müssen ihre Erwartungen und Fähigkeiten verständlich beschreiben und austauschen können. In diesem Zusammenhang müssen die Unternehmen dem Ursprung und der Unveränderbarkeit von Nachweisen vertrauen können. Dabei wird auch Bezug auf dezentrale Identitäten genommen.



Vanessa Bellinghausen

Referat DI 23 - Cyber-Sicherheit für intelligente Transportsysteme und Industrie 4.0 Bundesamt für Sicherheit in der Informationstechnik, Bundesamt für Sicherheit in der Informationstechnik BSI

11:20
12:00

DIGITALER BÜRGER & VERWALTUNG



FORUM 16-B | TUTORIAL

BürgerApp - Lokaldemokratie als Pionier des E-Votings?

E-Voting ist seit Jahren ein heiss umstrittenes Thema. Die weniger verfängliche Variante findet auf Lokalebene statt. Mit der Tübinger „BürgerApp“ werden die Bürger direkt nach ihrer Meinung zu anstehenden Themen befragt. Das Tutorial berichtet über Organisation, Anwendung und Erfahrungen mit diesem Ansatz. Wie hoch ist die typische Wahlbeteiligung? Was geschieht mit den Ergebnissen? Sehen wir hier den Wegbereiter für bürgernahe Entscheidungen?



Ulrich Narr

Fachbereich Kommunales, Universitätsstadt Tübingen



FORUM 16-C | TUTORIAL

Sicherheit ohne Friktion in digitalen Ökosystemen

Digitale Plattformen ermöglichen eine harmonisierte und effiziente Interaktion zwischen allen Ökosystemteilnehmern und sind ein wesentlicher Baustein für die Skalierbarkeit digitaler Geschäftsmodelle. Allerdings ergeben sich aus der Komplexität, Dynamik und notwendigen Geschwindigkeit in digitalen Ökosystemen Herausforderungen, denen sich alle Unternehmen, die ein digitalen Ökosystemen betreiben oder initiieren wollen, stellen müssen. Vor allem das Thema Sicherheit ist in digitalen Ökosystemen absolut erfolgskritisch. Gleichzeitig muss jedoch eine friktionsfreie User Experience gewahrt werden. Innovative Tools können dazu beitragen, Identitäten besser zu bewerten und Identitätsbetrug frühzeitig zu vermeiden. Mastercard stellt zum Beispiel Tools zur Prüfung des Eingabeverhaltens („Wie“) und der Eingaben („Was“) bereit, um entsprechende Identitäten zweifelsfrei festzustellen und so die Sicherheit zu erhöhen und unnötige Friktionen zu vermeiden.

**Carsten Muerl**

Director Product Management, Mastercard Europe SA



FORUM 17-A | LECTURES

Smart Cities und Smart Regions - Eine Herausforderung für die Informationssicherheit

In einer Smart City oder Smart Region werden moderne Informations- und Kommunikationstechnologien eingesetzt, um die Lebensqualität zu verbessern, Transparenz und Demokratie zu fördern und das Umfeld ökologisch, ökonomisch und sozial nachhaltig zu gestalten. Informationssicherheit ist dabei eine tragende Säule auf dem Weg zu einer erfolgreichen Digitalisierung dieser Lebensräume. Anhand einiger Praxisbeispiele wird dies verdeutlicht.



Dr. Silke Bargstädt-Franke (Moderation)

Abteilungsleiterin Cyber-Sicherheit in der Digitalisierung und für elektronische Identitäten, Bundesamt für Sicherheit in der Informationstechnik BSI



FORUM 17-B | LECTURES

VS-NfD geeignete Infrastrukturen

Diese Session wendet sich an Personen, die Bedarf oder Interesse an dem Betrieb VSA-konformer Infrastrukturen haben. Neben einem Einblick in dafür relevante VS-Anforderungsprofile zur Beschreibung der umzusetzenden BSI-Anforderungen zeigen zwei Beispiele aus der Industrie, wie Verschlusssachen in bestimmten Szenarien behandelt werden können.



Ingo Hahlen (Moderation)

Referent im Referat KM 12, Bundesamt für Sicherheit in der Informationstechnik BSI



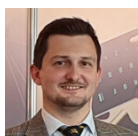
Dr. Elke Dallmer

Common Criteria Prüfstelle , SRC Security Research & Consulting GmbH



Alexander Krähenbühl

Airbus CyberSecurity GmbH



André Gimbut

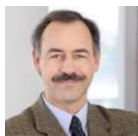
CTO, DIGITTRADE GmbH



FORUM 18-A | PANEL

Die digitale Transformation ruft nach sicheren digitalen Identitäten. Wo steuert die EU hin?

Nach der EU Ankündigung im September 2020 wurde eine neue Experten Gruppe initiiert, die eine Toolbox als Grundlage für die eIDAS 2.0 Regulierung bis zum Oktober 2022 entwickeln und veröffentlichen soll. Off- und Online Anwendungen sollen künftig mit einer Wallet auf dem Smartphone ermöglicht werden. Als Anwendungen sind u.a. Gesundheits-, Reise- und Ausbildungsdaten, sowie Bezahlungsfunktion-Unterstützung in der Diskussion. Das Panel ventiliert den aktuellen Stand der Entwicklungen.

**Dr. Detlef Houdeau (Moderation)**

Senior Director Digital Security Solution, Infineon Technologies AG

**Norbert Sagstetter**

Deputy Head of Unit eGovernment and Trust, European Commission

**Bernd Kowalski**

KI 3 - Entwicklung Digitaler Technologien, Bundesministerium für Wirtschaft und Energie BMWi

**Arno Fiedler**

Owner & CEO, Nimbus Technologieberatung GmbH



FORUM 18-B | PANEL

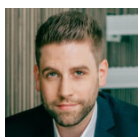
Bank-Identität, Video-Identität oder Ausweis-Identität: wer macht das Rennen?

KYC – also know your customer – beginnt im digitalen Onboardingprozess mit einer Identifikation bzw. Registrierung ohne persönlichen Kontakt. Die sicherste, schnellste und zugleich preiswerteste Identifikation ermöglicht der Online-Ausweis. Aber auch andere Verfahren werden immer besser. Es scheint sich weniger ein Wettbewerb der Verfahren als ein Wettbewerb von Multi-Plattformen zu etablieren.



Dr. Stephan Klein (Moderation)

CEO, Governikus KG



Benny Bennet Jürgens

CEO & Founder, Nect GmbH



Frank S. Jorga

Co-CEO & Founder, WebID Solutions GmbH



Dr. Kim Nguyen

CEO, D-Trust GmbH



Uwe Stelzig

CEO & Co-Founder, identity Trust Management AG



FORUM 18-C | LECTURES

Sichere Schlüsseltechnologie für die Digitalisierung der Energiewende

Im Rahmen der Digitalisierung der Energiewende setzt die stufenweise Weiterentwicklung des intelligenten Messsystems Anreize zur Wertschöpfung und Umsetzung von weiteren Dienstleistungen und Mehrwerten. Dabei werden Themen wie die sichere Anbindung von Ladeinfrastruktur, die Steuerung von dezentralen Verbrauchern und Erzeugern das Mehrsparten- und das Sub-Metering fokussiert. Das Smart-Meter-Gateway bietet dabei die zentrale Kommunikationseinheit des Systems zur sicheren Kommunikation.



Thomas Gast (Moderation)

Fachbereichsleiter DI 2 Cyber-Sicherheit in der Digitalisierung, Bundesamt für Sicherheit in der Informationstechnik BSI



Dr.-Ing. Lutz Martiny (Moderation)

Management Consultant, achelos GmbH



Dennis Laupichler

Referatsleiter DI 21 - Cyber-Sicherheit für die Digitalisierung der Energiewirtschaft, Bundesamt für Sicherheit in der Informationstechnik BSI



Sebastian Schaule

Referent Energie, bitkom Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.



Ingo Schönberg

Gründer & Vorstandsvorsitzender, PPC Power Plus Communications AG