Bundesministerium
des Innern, für Bau
und Heimat

Online Kompendium Cybersicherheit in Deutschland

Online Kompendium Cybersicherheit in Deutschland

Quadrigavertreter für die Zivilgesellschaft

Herr Klaus Müller
Vorstand Verbraucherzentrale Bundesverband e.V.

Quadrigavertreterin für die Wissenschaft

Frau Prof. Dr. Mira Mezini
Professorin für Informatik an der TU Darmstadt

Quadrigavertreterin für die Wirtschaft

Frau Claudia Nemat
Mitglied des Vorstands der Deutschen Telekom

Quadrigavertreter für den Staat

Herr Prof. Dr. Günter Krings
Parlamentarischer Staatssekretär beim Bundesminister des Innern, für Bau und Heimat

Vorwort

Die Analyse des jährlichen Lageberichts zur IT-Sicherheit des Bundesamtes für Sicherheit in der Informationstechnik zeigt, dass Cybersicherheit niemals statisch ist und die Bedrohungen im Netz vielseitig sind. Genauso vielfältig wie die Bedrohungen im Netz sind jedoch auch die Möglichkeiten des Schutzes und damit die in Deutschland derzeit existierenden Akteure und Initiativen zum Thema Cybersicherheit. Bislang fehlt jedoch ein vollumfassendes Bild aller Akteure und Initiativen in Deutschland, die sich tatsächlich mit dem Thema befassen, Informationen, Hilfestellungen, Dienstleistungen und Produkte anbieten oder forschen und entwickeln. Die Weiterentwicklung der Cybersicherheit auf gesamtgesellschaftlicher Ebene erfordert eine Berücksichtigung aller Interdependenzen als Ausgangsposition, welche nur eine ganzheitliche Perspektive liefern kann. Dies ist notwendig, um die Verbraucherinnen und Verbraucher, Wissenschaftlerinnen und Wissenschaftler sowie Entscheiderinnen und Entscheider der Wirtschaft und des Staates zum einen über Cybersicherheitsrisiken und -gefahren aufklären und bei der Prävention unterstützen zu können. Zum anderen um bei der Behebung eingetretener IT-Sicherheitsvorfälle behilflich zu sein oder aber durch Veröffentlichung bestehender Cyberakteure und -initiativen die eigene Vernetzung zu unterstützen.

Cybersicherheit betrifft alle Gesellschaftsbereiche, sowohl Zivilgesellschaft als auch Wissenschaft, Wirtschaft und Staat, und stellt eine digital- und sicherheitspolitische Herausforderung dar, die gemeinsam angegangen werden muss. Eine nachhaltige Stärkung der Cybersicherheit in Deutschland kann daher nur in einem gemeinschaftlichen Schulterschluss zwischen Zivilgesellschaft, Wissenschaft, Wirtschaft und Staat erreicht werden.

Im Rahmen des Nationalen Pakts Cybersicherheit vertreten wir diese Gesellschaftsgruppen und gehen diese Aufgabe gemeinsam an. Im vorliegenden Kompendium ist das Ergebnis der ersten Phase des Nationalen Pakts Cybersicherheit festgehalten. In einer mehrstufigen und strukturierten Erhebung sowie zahlreichen Multiplikator- und Stakeholder-Gesprächen haben wir nahezu jeden Winkel Deutschlands digital erkundet und über mehrere Aufrufe im Internet und in sozialen Medien Unternehmen, Vereine, NGOs und Einzelpersonen aufgerufen, uns online ihre Initiativen oder ihren Beitrag zur Cybersicherheit in Deutschland zu nennen.

Und wie Sie selbst im vorliegenden Kompendium nachlesen können, sind uns dabei viele interessante und spannende Engagements begegnet.

In den letzten Monaten hat die COVID-19 Pandemie Deutschland und die Welt in Atem gehalten. Auch im Nationalen Pakt Cybersicherheit haben wir die Auswirkungen gespürt. Denn zum einem konnten zahlreiche Veranstaltungen und Konferenzen auch im Bereich der Cybersicherheit nicht oder nur eingeschränkt stattfinden. Zum anderen hat aber auch die rasante Geschwindigkeit der Digitalisierung des Arbeits- und Privatalltags von Bürgerinnen und Bürgern aufgrund der notwendigen Kontaktbeschränkungen uns allen vor Augen geführt, wie wichtig und unverzichtbar digitale Lösungen in unserem Lebensalltag geworden sind. Gleichzeitig steigen hierdurch jedoch nochmals die Herausforderungen im Bereich der Cybersicherheit, bspw. durch den vermehrten Einsatz privater Hardware im beruflichen Umfeld.

Liebe Leserinnen und Leser, Sie alle wissen: Cybersicherheit ist kein statischer Zustand, sondern ein Prozess. Dabei geht es auch darum, kontinuierlich die neuen Herausforderungen unserer Zeit zu identifizieren und gemeinschaftlich hierfür neue Lösungen zu finden. In Deutschland ist ein breites Spektrum von Vereinen, Verbänden, NGOs, Unternehmen, Wissenschafts- und Forschungseinrichtungen und Behörden vertreten, die zur Verwirklichung dieses Ziels an einem Strang ziehen.

Das vorliegende Kompendium ist das erste Ergebnis dieses Paktes, gibt der deutschen Cybersicherheits-Landschaft einen strukturierten Überblick und wird im nächsten Schritt durch einen gesamtgesellschaftlichen Zielkanon fortgeschrieben. Dieser soll dann Grundlage für die sich anschließende konkrete Umsetzungsplanung sein.

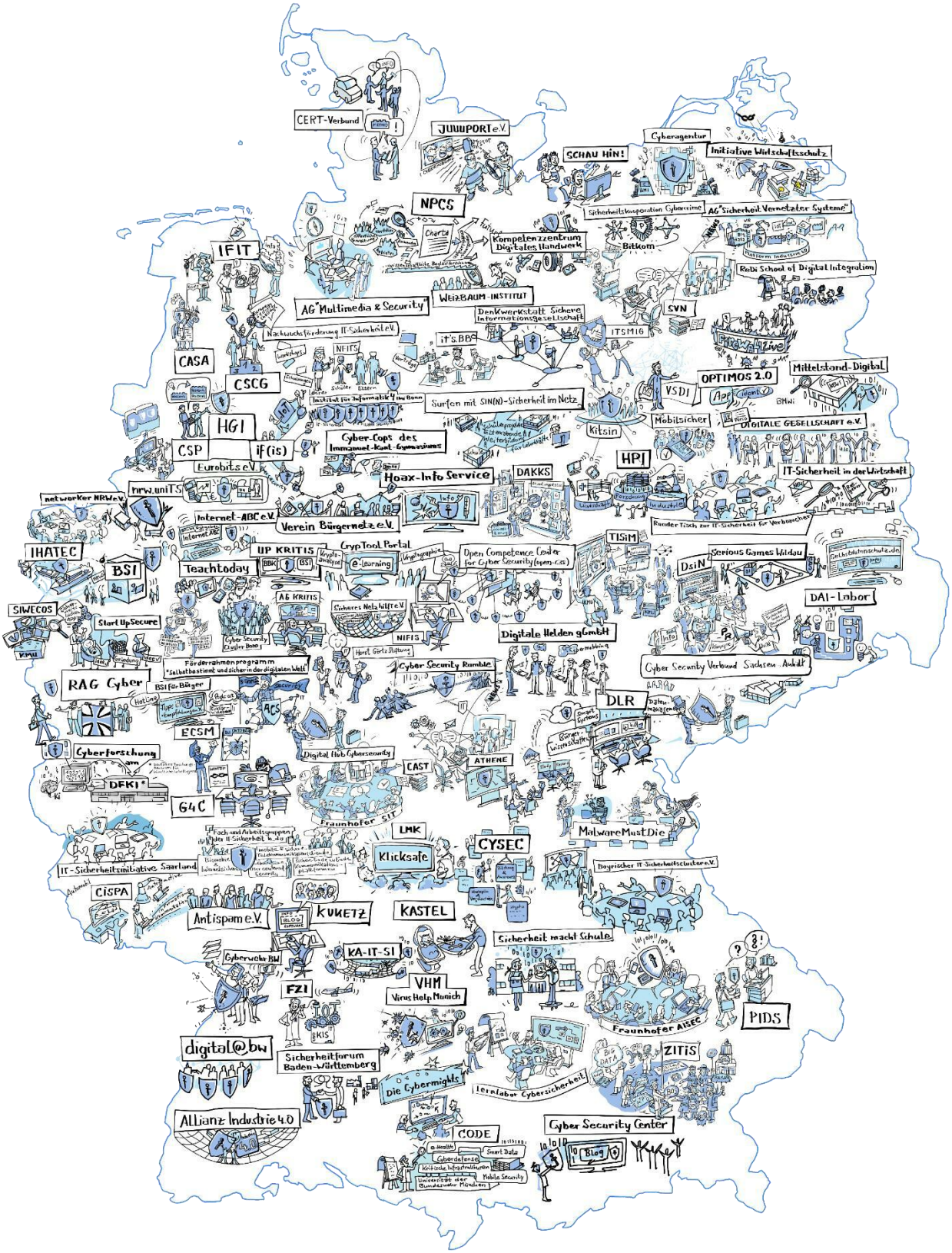
Wir wünschen Ihnen eine spannende Lektüre.

Prof. Dr. Mira Mezini, TU Darmstadt

Claudia Nemat, Deutsche Telekom

Klaus Müller, Verbraucherzentrale Bundesverband

Prof. Dr. Günter Krings, Bundesministerium des Innern, für Bau und Heimat


CERT-Verbund
JUWUPORT e.V.
SCHAU HIN!
Cyberagentur
Initiative Wirtschaftsschutz
NPCS
Sicherheitskooperation Cybercrime
AG "Sicherheit Vernetzter Systeme"
IFIT
Kompetenzzentrum Digitales Handwerk
Bitkom
Rebi School of Digital Integration
AG "Multimedia & Security"
WEIZBAUM-INSTITUT
DenkWerkstatt Sichere Informationsgesellschaft
SVN
Nachwuchsförderung IT-Sicherheit e.V.
it's.BB
ITSMIG
CASA
CSCG
OPTIMOS 2.0
Mittelstand-Digital
Surfen mit SIN(N)-Sicherheit im Netz
VSDI
HGI
Mobilsicher
DIGITALE GESELLSCHAFT e.V.
CSP
if(is)
Cyber-Cops des Immanuel-Kant-Gymnasiums
Kitsin
HPI
Eurobits e.V.
Hoax-Info Service
DAKKS
IT-Sicherheit in der Wirtschaft
nrw.uniTS
Runder Tisch zur IT-Sicherheit für Verbraucher
networker NRW e.V.
Internet-ABC e.V.
Verein Bürgernetz e.V.
TISiM
IHATEC
UP KRITIS
CrypTool Portal
Open Competence Center for Cyber Security (open.ccs)
DsiN
Serious Games Wildau
BSI
Teachtoday
e-Learning
DAI-Labor
SIWECOS
AG KRITIS
Sicheres Netz hilft e.V.
Start Up Secure
NIFIS
Digitale Helden gGmbH
Förderrahmenprogramm "Selbstbestimmt und sicher in der digitalen Welt"
Cyber Security Rumble
Cyber Security Verbund Sachsen-Anhalt
RAG Cyber
BSI für Bürger
DLR
ACS
ECSM
Cyberforschung am DFKI
Digital Hub Cybersecurity
CAST
ATHENE
G4C
Fraunhofer SIT
LMK
MalwareMustDie
CYSEC
Klicksafe
Bayerischer IT Sicherheitscluster e.V.
IT-Sicherheitsinitiative Saarland
CISPA
Antispam e.V.
KUKETZ
KASTEL
Sicherheit macht Schule
Cyberwehr BW
KA-IT-SI
VHM
Virus Help Munich
FZI
PIDS
Fraunhofer AISEC
digital@bw
Sicherheitforum Baden-Württemberg
ZITiS
Die Cybermights
Lernlabor Cybersicherheit
Allianz Industrie 4.0
CODE
Cyber Security Center
Blog

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

ABE	Attribute-based Encryption / Attributbasierte Verschlüsselung
AISEC	Fraunhofer-Institut für Angewandte und Integrierte Sicherheit
AKUS	Arbeitskreis für Unternehmenssicherheit Brandenburg
AOK	Allgemeine Ortskrankenkasse
APT	Advanced Persistent Threats / fortgeschrittene andauernde (Cyber-) Bedrohung
ASW	Allianz für Sicherheit in der Wirtschaft
ATHENE	Nationales Forschungszentrum für angewandte Cybersicherheit
B2B	Business-to-Business / Geschäftsbeziehungen zwischen zwei oder mehr Unternehmen
BDEW	Bundesverband der Energie- und Wasserwirtschaft
BDI	Bundesverband der deutschen Industrie e.V.
BDLI	Bundesverband der Deutschen Luft- und Raumfahrtindustrie e.V.
BDSV	Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e.V.
BDSW	Bundesverband der Sicherheitswirtschaft
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
bff	Bundesverband Frauenberatungsstellen und Frauennotrufe Frauen gegen Gewalt e.V.
BfIT	Beauftragte der Bunderegierung für Informationstechnik
BfV	Bundesamt für Verfassungsschutz
BGP	Border Gateway Protocol
Bitkom	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BITMi	Bundesverband IT-Mittelstand e.V.
BKA	Bundeskriminalamt
BKK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BMFSFJ	Bundesministerium für Familie, Senioren, Frauen und Jugend
BMI	Bundesministeriums des Innern, für Bau und Heimat
BMJV	Bundesministerium der Justiz und für Verbraucherschutz
BMVg	Bundesministerium der Verteidigung
BND	Bundesnachrichtendienst
BOS	Behörden des Bundes mit Sicherheitsaufgaben
BPOL	Bundespolizeipräsidium
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Gesetz
BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz
BSKI	Bundesverband für den Schutz Kritischer Infrastrukturen e.V.
BTU	Brandenburgische Technische Universität
BvD	Berufsverband der Datenschutzbeauftragten Deutschlands e.V.
BVMW	Bundesverband mittelständische Wirtschaft, Unternehmerverband Deutschlands e.V.
BW	Baden-Württemberg, je nach Kontext auch Bundeswehr
C.i.e.S.	Cybercrime im engeren Sinne
CASA	Cyber Security in the Age of Large-Scale Adversaries
CAST	Competence Center for Applied Security Technology
CC	Cybercrime
CC Security	Competence Center Security
CCC	Chaos Computer Club e.V.
CERT	Computer Emergency Response Team / Computersicherheits-Ereignis- und Reaktionsteam,
CHE	Centrum für Hochschulentwicklung
CIO	Chief Information Officer / Leiter Informationstechnik
CIR	Cyber- und Informationsraum
CISPA	Helmholtz-Zentrum für Informationssicherheit gGmbH
CMS	Content Management System
CODE	Forschungsinstitut Cyber Defence
CPS	Cyber-Physical Systems / Cyberphysische Systeme
CRuFz	Cyber-Recherche- und Fahndungszentrum
CSCG	Cyber Security Challenge Germany
CSP	Max-Planck-Institut für Cybersicherheit und Schutz der Privatsphäre
CSS	Cyber-Sicherheitsstrategie
CTF	Capture the Flag
Cyber-AZ	Nationales Cyber-Abwehrzentrum
CyBOK	Cybersecurity Body of Knowledge
CYSEC	Profilbereich für Cybersicherheit an der TU Darmstadt
DAI-Labor	Distributed Artificial Intelligence Laboratory
DAkkS	Deutsche Akkreditierungsstelle GmbH
DDoS	Distributed Denial of Service
DFKI	Cybersicherheitsforschung am Deutschen Forschungszentrum für Künstliche Intelligenz GmbH

DGQ	Deutsche Gesellschaft für Qualität e.V.
DIHK	Deutschen Industrie- und Handelskammertag
DIN	Deutsches Institut für Normung
DiWiSH	Digitale Wirtschaft Schleswig-Holstein
DIZ	Digitales Innovationszentrum
DKG	Deutsche Krankenhausgesellschaft e.V.
DLR	Deutsches Zentrum für Luft- und Raumfahrt e.V.
DNS	Domain Name System
DoS	Denial of Service
DsiN	Deutschland sicher im Netz e.V. (DsiN)
ECSC	European Cyber Security Challenge
ECSM	European Cyber Security Month
ECTEG	European Cybercrime Training and Education Group
eID	elektronische ID
eIDAS	electronic Identification, Authentication and trust Services
ENISA	Agentur der Europäischen Union für Cybersicherheit
EnWG	Energiewirtschaftsgesetz
EU	Europäische Union
EU-NIS Richtlinie	Europäische Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit
F&E	Forschung und Entwicklung
FAQ	Frequently Asked Questions / häufig gestellte Fragen
FAU	Friedrich-Alexander-Universität Erlangen-Nürnberg
FH	Fachhochschule
FHDW	Fachhochschule der Wirtschaft
FIM	Föderales Informationsmanagement
FINSOZ	Fachverband Informationstechnologie in Sozialwirtschaft und Sozialverwaltung e.V.
FinTech	Finanztechnologie
FITKO	Föderale IT-Kooperation
FKIE	Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie
FKIE	Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie
FOKUS	Fraunhofer-Institut für Offene Kommunikationssysteme
FPGA	Field Programmable Gate Array / Integrierter Schaltkreis in der Digitaltechnik
FU	Freie Universität
FZI	Forschungszentrum Informatik
G4C	German Competence Centre against Cyber Crime e. V.
GB BMVg	Geschäftsbereich des Bundesministeriums der Verteidigung
GDV	Gesamtverband der Deutschen Versicherungswirtschaft e.V.
GI	Gesellschaft für Informatik
GIP	German-Israeli Partnership Accelerator
GmbH	Gesellschaft mit beschränkter Haftung
GTAZ	Gemeinsames Terrorismusabwehrzentrum
h_da	Hochschule Darmstadt
HDE	Handelsverband Deutschland e.V.
HGI	Horst Görtz Institut für IT-Sicherheit
HMWK	Hessisches Ministerium für Wissenschaft und Kunst
HPI	Hasso-Plattner-Institut für Digital Engineering gGmbH
HS	Hochschule
IAO	Fraunhofer-Institut für Arbeitswirtschaft und Organisation
ICS	Industrial Control System / Industrielles Kontrollsystem
ICS	Industrielle Steuerungs- und Automatisierungssysteme
if(is)	Institut für Internet-Sicherheit
IFIT	Freies Insititut für IT-Sicherheit e.V.
IHATEC	Innovative Hafentechnologien
IHK	Industrie und Handelskammer
IKT	Informations- und Kommunikationstechnologie
IMK	Innenministerkonferenz
IOSB	Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB
IoT	Internet of Things / Internet der Dinge
ISInet	Initiative Sicheres Internet
ISi-Reihe	BSI-Standards zur Internet-Sicherheit
ISMS	Informationssicherheitsmanagement
IT	Informationstechnologie
it's.BB	IT-Sicherheitsnetzwerk Berlin-Brandenburg
IT-NetzG	Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder
ITSMIG	IT Security made in Germany
ITUJ	Institut für Technik und Journalismus
ITVSH	IT-Verbund Schleswig-Holstein
ITZ-Bund	Informationstechnik Zentrum Bund
IUNO	Nationale Referenzprojekt zur IT-Sicherheit in der Industrie 4.0
KA-IT-SI	Karlsruher IT-Sicherheitsinitiative
KASTEL	Kompetenzzentrum für angewandte Sicherheitstechnologie
KdoCIR	Kommando Cyber- und Informationsraum
KI	Künstliche Intelligenz
KIT	Karlsruher Institut für Technologie

KITS	Kooperative Studiengang IT-Sicherheit bzw. Koordinierungsstelle IT-Sicherheit des DIN e.V.
Kitsin	Kommunales IT-Sicherheitsbündnis
KMU	Kleine und mittelständische Unternehmen
KRITIS	Kritische Infrastrukturen
LfV	Landesbehörden für Verfassungsschutz
LITiF BW	Sicherheitszentrum IT der Finanzverwaltung Baden-Württembergs
LKA	Landeskriminalamt
LLCS	Lernlabor Cybersicherheit
LMK	Landeszentrale für Medien und Kommunikation Rheinland-Pfalz
LTE	Long Term Evolution (Mobilfunkstandard)
LZfD	Landeszentrums für Datenverarbeitung
M2M	Machine-to-Machine / Maschine zu Maschine
MAD	Militärischer Abschirmdienst
MCN	Maritimes Cluster Norddeutschland
MilOrg-Ber	militärischen Organisationsbereichs
MINT	Mathematik, Informatik, Naturwissenschaften und Technik
MIRT	Mobile Incident Response Team
ML	Machine Learning / Maschinelles Lernen
MLU	Luther-Universität Halle-Wittenberg
NAMUR	Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V.
N-CERT	Niedersachsen-CERT
netlab	CyberSecurity-Verbund Sachsen-Anhalt
NGO	Non-governmental organization / Nichtregierungsorganisation
NIFIS	Nationale Initiative für Informations- und Internet-Sicherheit e. V.
NIS	Netzwerk- und Informationssicherheit
NIST	National Institute of Standards and Technology
NMMT	Nationalen Masterplan Maritime Technologien
NPCS	Nationaler Pakt Cybersicherheit
NPSI	Nationaler Plan zum Schutz der Informationsinfrastrukturen
NTP	Network Time Protocol
NYC	New York City
öfftl.	öffentlich
open-c3s	Open Competence Center for Cyber Security
OT	Operational Technology / Betriebstechnologie
OTH	Ostbayerische Technische Hochschule
OVGU	Otto-von-Guericke-Universität Magdeburg
OZG	Onlinezugangsgesetz
PaaS	Platform as a Service
PEASEC	Lehrstuhl Wissenschaft und Technik für Frieden und Sicherheit an der Technischen Universität Darmstadt
PIDS	Passau Institute of Digital Security
PKI	Public Key Infrastructure
priv.	privat
ProPK	Polizeilichen Kriminalprävention
RAG	Reservistenarbeitsgemeinschaft
RWTH	Rheinisch-Westfälische Technische Hochschule
RZ	Rechenzentrum
SaaS	Software as a Service
SEE-MOO	Secure Mobile Networking Lab
SGB V	Fünftes Buch Sozialgesetzbuch
SID	Safer Internet Day
SiKoSH	Sicherheit für Kommunen in Schleswig-Holstein
SIT	Fraunhofer-Institut für Sichere Informationstechnologie
SI-WECOS	Sichere Webseiten und Content Management Systeme
SK IT-IS	Sektorkomitee Informationstechnik / Informationssicherheit
SN4C	Cybercrime Competence Center des LKA Sachsen
SNV	Stiftung Neue Verantwortung e. V.
SOC	Security Operations Centre
sog.	sogenannt
SPoC	Single Point of Contact
SPS	Speicherprogrammierbare Steuerung
SQL	Structured Query Language
ST	Staatsschutz
T.I.S.P.	TeleTrusT Information Security Professional
TeleTrusT	Bundesverband IT-Sicherheit e.V.
TH	technische Hochschule
TI	Telematikinfrastruktur
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
TU	Technische Universität
TÜV	Technischer Überwachungs-Verein
UNESCO	United Nations Educational, Scientific and Cultural Organization / Organisation der Vereinten Nationen für Bildung, Wissenschaft und Kultur
UP-KRITIS	Umsetzungsplan KRITIS
US	United States / Vereinigte Staaten (von Amerika)
VCV	Verwaltungs-CERT-Verbund
VDA	Verband der Automobilindustrie e.V.
VDE	Verband der Elektrotechnik Elektronik Informationstechnik e.V.
VDI	Verein Deutscher Ingenieure e.V.

VdRBw	Verband der Reservisten der Deutschen Bundeswehr e.V.
VEP	Visuell evoziertes Potential
VHM	Virus Help Munich
VKU	Verband kommunaler Unternehmen e.V.
VSDI	Verband Sichere Digitale Identität e. V.
vzbv	Verbraucherzentale Bundesverband e.V.
ZAC	Zentralen Ansprechstelle Cybercrime
ZCB	Zentralstelle Cybercrime Bayern
ZCS	Zentralstelle Cybercrime Sachsen
ZD.B	Zentrum Digitalisierung.Bayern
ZDF	Zweites Deutsches Fernsehen
ZDH	Zentralverband des Deutschen Handwerks e.V.
ZIR	Zentrale Internetrecherche
ZISC	Zentrale Informations- und Servicezentrum Cybercrime
ZIT	Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität
ZKI	Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e.V.
ZVEI	Zentralverband Elektrotechnik- und Elektronikindustrie e.V.

1 Einleitung und Hintergrund

Cybersicherheit stellt eine gesamtgesellschaftliche Herausforderung dar, da sowohl die Zivilgesellschaft als auch die Wissenschaft, die Wirtschaft und der Staat von Cyber-Gefahren bedroht sind. Daher ist in diesen Bereichen eine noch intensivere und effizientere Zusammenarbeit aller Beteiligten sowie eine starke Stellung von Bund und Ländern erforderlich.

Sicheres Leben in Deutschland - auch online

Auf der Grundlage des Koalitionsvertrags der aktuellen Legislaturperiode wurde auf Initiative des Bundesministeriums des Innern, für Bau und Heimat (BMI) der Nationale Pakt Cybersicherheit (NPCS) ins Leben gerufen. Vor dem Hintergrund von Cybersicherheit als gesamtgesellschaftlicher Herausforderung ist es das Ziel dieses Pakts, alle gesellschaftlich relevanten Gruppen, Hersteller, Anbieter und Anwender sowie die öffentliche Verwaltung in gemeinsamer Verantwortung für Cybersicherheit zusammenzubringen.

Die Notwendigkeit der sicheren Nutzung von Internettechnologien hat sich besonders in der „Digitalisierungswelle“ infolge der COVID-19-Pandemie gezeigt. In Zeiten von Social Distancing und Kontaktbeschränkungen stellen digitale Lösungen für Videokonferenzen, kollaboratives Arbeiten oder auch Vorträge und Präsentationen z.B. im Schulunterricht oder der universitären Lehre, in der Arbeitswelt in Behörden und Unternehmen und auch im Privatleben eine unverzichtbare Alternative dar. Aufgrund des hohen Zeitdrucks zur schnellen Einführung digitaler Lösungen in vielen Lebensbereichen wurden aber auch zum Teil Cybersicherheitsrisiken in Kauf genommen. Daher ist es umso wichtiger, die Cybersicherheit in Deutschland wieder verstärkt in den Fokus zu nehmen und dadurch einen bedeutsamen Beitrag für die erfolgreiche Digitalisierung der Gesellschaft zu leisten.

Hierfür übernimmt und betont die Quadriga im Nationalen Pakt Cybersicherheit – stellvertretend für Zivilgesellschaft, Wissenschaft, Wirtschaft und Staat – die gemeinsame Verantwortung für mehr Cybersicherheit in der Gesellschaft.

Die Quadriga steuert hierbei eigenständig aus Sicht ihrer Gesellschaftsgruppe Impulse, Ideen und Handlungsoptionen zur Vernetzung der Cybersicherheitsinitiativen und beteiligt sich an öffentlichkeitswirksamen Kommunikationsformaten. Die Quadriga gibt damit dem Nationalen Pakt Cybersicherheit ein Gesicht nach außen.

Der NPCS besteht aus drei Phasen:

In der ersten Phase werden die in Deutschland im Bereich Cyber- und Informationssicherheit tätigen Akteure und Initiativen und deren Beiträge identifiziert und in einem strukturierten Gesamtbild der Cybersicherheitsaktivitäten in Deutschland, dem Kompendium Cybersicherheit Deutschland, zusammengestellt.

Auf Grundlage der hieraus gewonnenen Erkenntnisse wird die Quadriga in der zweiten Phase eine gesamtgesellschaftliche Erklärung zur Cybersicherheit mit wesentlichen Schlüsselthemen und einer cybersicherheitspolitischen Zielsetzung vorstellen. Dies soll den Nationalen Pakt Cybersicherheit tatsächlich beschließen und die gemeinsame Verantwortung für mehr Cybersicherheit aller Gesellschaftsgruppen unterstreichen. Gleichzeitig ist dies der Startschuss für die dritte Phase, die Umsetzungsphase, des Nationalen Pakts Cybersicherheit.

Aus internationaler Sicht stellt der NPCS den deutschen Beitrag zum „Paris Call for trust and security in cyberspace“ dar. Dieser wurde am 12. November 2018 vom Präsidenten der Französischen Republik, Emmanuel Macron, während des Internet Governance Forums der UNESCO und des Pariser Friedensforums veröffentlicht. Mit der Deklaration des Paris Call wurden neun grundlegende Prinzipien vereinbart, bspw. die Stärkung des "Security by Design" Ansatzes, welche unter der gemeinsamen Verantwortung aller Unterzeichner das Vertrauen, die Sicherheit und die Stabilität im Cyberspace verbessern sollen. Der Aufruf fordert alle Akteure der Cybersicherheit zur Zusammenarbeit auf und ermutigt die Staaten zur Kooperation mit Partnern aus der Zivilgesellschaft, der Wissenschaft und der Wirtschaft. Die Befürworter des Pariser Aufrufs verpflichten sich zur Zusammenarbeit, um verantwortungsbewusstes Verhalten anzunehmen und im Cyberspace die grundlegenden Prinzipien umzusetzen, die in der physischen Welt gelten. Die Bundesrepublik Deutschland ist einer von aktuell 74 Staaten, die den Aufruf unterzeichnet haben und sich dadurch den gemeinsamen Prinzipien des Paris Call verpflichten. Der Nationale Pakt Cybersicherheit bringt sich mit seinen eigenständigen Maßnahmen in diesen Prozess ein.

Erfolgreiche Strategien und Maßnahmen zur Reduzierung von Cyberrisiken setzen das Zusammenwirken sämtlicher Akteure voraus - von den durch den Staat gesetzten Rahmenstrukturen über die Implementierung von IT-Sicherheitsanforderungen durch Hersteller und Anbieter sowie Forschungsaktivitäten bis hin zu Sensibilisierungsmaßnahmen für die Anwender.

Cybersicherheit liegt in der gesamtgesellschaftlichen Verantwortung aller relevanten Akteure. Gleichzeitig existierte bisher kein gesamthafter Überblick zu der Vielzahl an Institutionen, Akteuren und Initiativen und wie diese zusammenwirken bzw. sich ergänzen können. Synergien zwischen einzelnen Stakeholdern werden bisher in der Regel gar nicht adressiert und damit wertvolle Potenziale aus der möglichen Vernetzung von Wissen, Methoden, Kompetenzen etc. dadurch nicht einmal im Ansatz erschlossen. Ebenso blieb der Bereich für die interessierte Öffentlichkeit weitgehend unübersichtlich und vor allem im Hinblick auf „best practice" wenig greifbar.

Das vorliegende Kompendium widmet sich als Ausprägung der ersten Phase des Nationalen Pakt Cybersicherheit dieser Thematik mit der Leitfrage:

„Wer engagiert sich in Deutschland mit welchem Ziel und Beitrag für die Cybersicherheit?".

Im Kompendium werden daher Akteure und Initiativen identifiziert, die sich in einem relevanten Umfang mit Informations- und Cybersicherheit beschäftigen.

Das Kompendium Cybersicherheit Deutschland beschreibt die Struktur und Ausprägung der deutschen Cybersicherheitslandschaft und geht auf ihre Besonderheiten ein. Zu ca. 100 besonderen Akteuren und Initiativen liefert das Kompendium überblicksartige Steckbriefe, welche den besonderen Beitrag zur Cybersicherheitslandschaft würdigen.

Ziel der Erhebung war die Identifikation aller wesentlichen Akteure und Initiativen der Cybersicherheit aus Zivilgesellschaft, Wissenschaft, Wirtschaft und Staat in Deutschland. Akteure sind im Verständnis des Kompendiums Organisationen oder Einzelpersonen aus dem Bereich der Cybersicherheit, die als Entität auftreten, während Initiativen vielmehr die Verkörperungen von Handlungen und Maßnahmen von einem oder mehreren Akteuren darstellen. Aus Datenschutzgründen werden jedoch Einzelpersonen keiner Betrachtung unterzogen, sondern, wenn möglich, deren als Initiative manifestiertes Engagement für Cybersicherheit in Deutschland. Die Akteure und Initiativen des Kompendiums tragen dazu bei, den Standort Deutschland im Hinblick auf dieses Themengebiet zu stärken - sei es durch eigenständige Beiträge, einzigartige Produkte, herausragendes Knowhow oder vernetzende Effekte.

Die Basis der Identifikation jener prägenden Akteure und Initiativen bildete eine Datenerhebung. Dabei kamen drei unterschiedliche methodische Ansätze zur Anwendung:

1. Eine systematische und mehrstufige Internetrecherche,
2. Multiplikatoren- bzw. Stakeholdergespräche mit z.B. Verbänden und Vernetzungsinitiativen
3. eine öffentliche Meldeformularfunktion auf der Webseite des BMI, über welche bestehende Akteure und Initiativen ihre eigenen Beiträge zur Cybersicherheit in Deutschland eigeninitiativ melden konnten.

Entscheidend für die detaillierte Betrachtung im Kompendium war jeweils der konkrete Beitrag des Akteurs bzw. der Initiative für den Themenbereich Cybersicherheit. Dieser musste einen eigenständig generierten Mehrwehrt, wie z.B. die Bündelung und Fokussierung bestehender oder die Schaffung neuer Informationen, darstellen und zudem

- innovative Methoden, Verfahren, Produkte, Umsetzungshilfen, Leitlinien und Technologien bereitstellen, oder
- Grundlagen- und Anwendungsforschung zu Cybersicherheit betreiben, oder
- Vernetzung von Akteuren und Förderung der Aufmerksamkeit für Aspekte der Cybersicherheit fördern, oder
- staatliche bzw. verbandsbezogene Regulierung zu Cybersicherheit vornehmen.

Sind diese Bedingungen, mithin der „besondere Beitrag" erfüllt, wird der Akteur oder die Initiative mit einem eigenen Steckbrief für das Kompendium berücksichtigt. Diese Einschätzung wurde flankierend durch die geführten Stakeholder- bzw. Multiplikatorengespräche bestätigt, da sich gegebenenfalls erst in der Gesamtschau mehrerer bestehender Initiativen und Akteure in einem Bereich der jeweils individuelle Beitrag zur Cybersicherheit offenbarte.

Aus wettbewerbsrechtlichen Gründen wird auf eine explizite Nennung durch eigene Steckbriefe bei wettbewerblich tätigen Akteuren verzichtet. Soweit sich gewerbliche Akteure jedoch in nicht gewinnorientierter Absicht engagieren und das Gemeinwohl im Fokus steht, wurden diese nicht-kommerziellen Initiativen mit Steckbriefen im Kompendium gewürdigt. Um die gesamte deutsche Cybersicherheitslandschaft, einschließlich wettbewerblich tätiger Akteure, angemessen zu berücksichtigen, wird im Anhang dieses Kompendiums eine Auflistung sämtlicher Organisationen, welche

während der Analyse und der Erstellung des Kompendiums betrachtet wurden, eingefügt.

Im Rahmen der Internetrecherche wurden fast 6.000 Webseiten analysiert. Auf dieser Basis sowie in Verbindung mit Erkenntnissen der Multiplikatorengespräche konnten etwa 2.200 Akteure und Initiativen in Deutschland identifiziert werden, die sich thematisch mit Cybersicherheit beschäftigen. Zu davon ca. 300 Akteuren und Initiativen konnten vollständige Beschreibungen zur Zusammensetzung der Initiative und ihren Aktivitäten erhoben werden, die in den Analyseteil des vorliegenden Kompendiums eingeflossen sind.

Hiervon werden ca. 100 Akteure aus Zivilgesellschaft, Wirtschaft, Wissenschaft und Staat, die einen aus gesamtgesellschaftlicher Sicht wesentlichen Mehrwert zur Cybersicherheit generiert haben und nicht wettbewerblich tätig sind, mit einem ausführlichen beschreibenden Steckbrief veröffentlicht.

2 Die deutsche Cybersicherheitslandschaft

Im Rahmen der Arbeiten am NPCS wurde eine Struktur der deutschen Cybersicherheitslandschaft erhoben und anhand definierter Kriterien und verschiedener Dimensionen analysiert. Dabei sollen die identifizierten Akteure und Initiativen zunächst einer gesamtheitlichen Betrachtung als Einstieg in die vertiefende Analyse jeder Gesellschaftsgruppe dienen. Nachfolgend werden die unterschiedlich starken Ausprägungen entlang der gesellschaftlichen Säulen sowie die Schwerpunkte und Sichtbarkeit von Leistungen im Bereich der Cybersicherheit in Deutschland betrachtet.

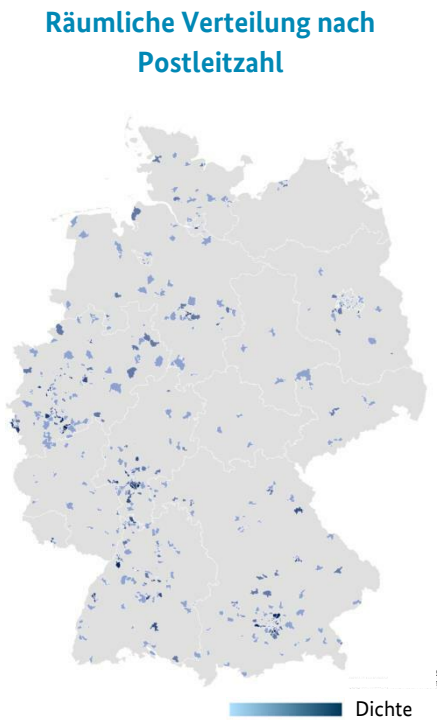


Abbildung 1 Räumliche Verteilung nach Postleitzahl. Quelle: BMI

Die im Rahmen des Nationalen Pakt Cybersicherheit identifizierten Organisationen behandeln das Thema Cybersicherheit unterschiedlich stark. Dadurch decken sie ein breites Spektrum an Hintergründen und Themen ab. Vom „IT-Experten vor Ort“ über Bürgerinitiativen und staatlichen Einrichtungen bis hin zu international geschätzten Forschungsinstituten und Hightech-Firmen.

Räumlich verteilt sind diese Akteure und Initiativen vor allem in oder in der Nähe der großen Ballungsgebiete, wohingegen der ländliche Raum erwartungsgemäß eine geringere Dichte an Ansiedlungen aufweist.

Abbildung 2 Gewichtete Verteilung nach Ländern. Quelle: BMI

Betrachtet man die Verteilung nach Bundesländern und gewichtet nach Bevölkerungszahlen, weisen Sachsen-Anhalt, Mecklenburg-Vorpommern, Thüringen, Sachsen und Rheinland-Pfalz die geringste Dichte an Akteuren und Initiativen auf, welche sich mit Aspekten der Cybersicherheit auseinandersetzen. Die höchste Dichte verzeichnet Berlin, was zum einen durch die ausgeprägte Startup-Kultur der Bundeshauptstadt, aber auch durch die Nähe zur Bundespolitik, bezogen auf dort niedergelassene Verbände, staatliche Einrichtungen und Behörden zurückzuführen ist.

Betrachtet man die jährlichen Neugründungen von Organisationen, die sich in Deutschland mit Cybersicherheit beschäftigen, ist innerhalb der letzten fünf Jahre ein fast exponentieller Anstieg zu beobachten. Erst ab Mitte der 1980er Jahre kann davon gesprochen werden, dass Akteure, allen voran Unternehmen, gezielt mit dem Fokus der IT- und Cybersicherheit gegründet wurden. Zwar existieren vereinzelt wesentlich ältere Akteure, die in der Vergangenheit gegründet wurden und sich nach diversen Neuausrichtungen und technischen Revolutionen heute der Cybersicherheit zuwenden. Jedoch läutet erst die allmähliche Reife der IKT in den 1980ern den signifikanten Gründungszeitraum wesentlicher Akteure der Cybersicherheit in Deutschland ein. Daher beginnt die Skala des nachstehenden Histogramms 1989, mit der Erfindung des World Wide Web durch Timothy Berners-Lee.

Bei der Detailanalyse des genannten Zeitraums fallen fünf Ausschläge des Histogramms auf:

- Ende der 1980er Jahre nehmen die Gründungen zu, zumeist IT-Firmen während der Pionierzeit der IT-Branche aber auch erste explizite IT-Sicherheitsakteure, wie bspw. der Bundesverband IT-Sicherheit (TeleTrusT) 1989 oder das Bundesamt für Sicherheit in der Informationstechnik (BSI) 1991.
- Im Rahmen der New Economy werden Ende der 1990er und Anfang der 2000er Jahre besonders viele IT-Unternehmen, teilweise schon damals mit Schwerpunkt Cybersicherheit, aber auch reine IT-Sicherheitsfirmen gegründet. Außerdem entwickeln sich einschlägige Initiativen. Nach dem Platzen der „Dotcom Blase“ sinkt die Zahl der Neugründungen kurzfristig ab.

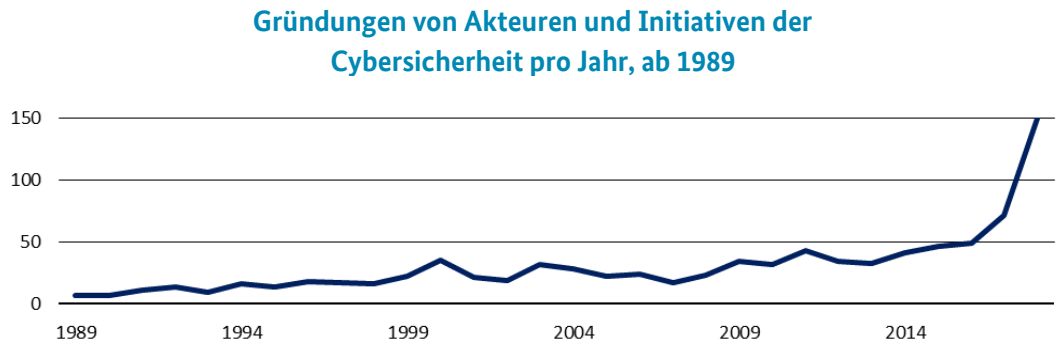


Abbildung 3 Gründungen von Akteuren und Initiativen der Cybersicherheit pro Jahr, ab 1989. Quelle: BMI

- Die einsetzende Weltfinanzkrise 2007 führt zu einem Rückgang an Neugründungen, welcher auch nicht vor Akteuren und Initiativen der Cybersicherheit in Deutschland Halt macht.
- Die gute Arbeitsmarktlage nach der überstandenen Weltfinanzkrise und Änderungen bei Gründungszuschüssen führen Ende 2011 zu einer zeitweisen Senkung der Gründungsaktivitäten. Das gute Angebot an attraktiven und vor allem nach der Krise sicheren Arbeitsplätzen senkt das Interesse an Gründungsvorhaben, die Anzahl der jährlichen Neugründungen nimmt leicht ab.
  Ab 2015 steigt die Anzahl der neu gegründeten Akteure und Initiativen stark an. Das Thema Cybersicherheit gelangt, nach anhaltenden Cyberattacken auf private, wirtschaftliche und staatliche Ziele, in den breiten gesamtgesellschaftlichen Fokus. Mit dem ebenfalls seit 2015 gültigen Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme leistet die Bundesregierung einen wichtigen Beitrag, die IT-Systeme und digitalen Infrastrukturen Deutschlands sicherer zu machen und förderte so die Neugründungen bei den betrachteten Akteuren. Insbesondere wird dem Rechnung getragen, dass im Bereich der Kritischen Infrastrukturen (KRITIS) ein Ausfall oder eine Beeinträchtigung der zunehmend digitalisierten Versorgungsdienstleistungen schwerwiegende Folgen für Gesellschaft, Wirtschaft und Staat in Deutschland haben können. Die Verfügbarkeit und Sicherheit der IT-Systeme spielen somit, speziell im Bereich der Kritischen Infrastrukturen, eine wichtige und zentrale Rolle. Ziel des IT-Sicherheitsgesetzes ist auch, die Verbesserung der IT-Sicherheit bei Unternehmen und in der Bundesverwaltung, sowie einen besseren Schutz der Bürgerinnen und Bürger im Internet anzustreben. Neben o. g. Akteuren gelten einzelne Regelungen des IT-Sicherheitsgesetzes daher auch für Betreiber von kommerziellen Webangeboten, die höhere Anforderungen an ihre IT-Systeme erfüllen müssen.
  Auch Telekommunikationsunternehmen wurden stärker gefordert und verpflichtet, ihre Kunden zu warnen, wenn sie einen Missbrauch eines Kundenanschlusses feststellen. Um diese Ziele zu erreichen, wurden u.a. die Aufgaben und Befugnisse des BSI ausgeweitet.

Von allen identifizierten Akteuren und Initiativen erfüllten insgesamt 374 die im vorherigen Kapitel erläuterte Definition des „besonderen Beitrags“ zur Cybersicherheit in Deutschland, weshalb sich die weiteren Analysen auf diese Grundgesamtheit beziehen. Hiervon haben rund 58% einen wirtschaftlichen Hintergrund, jeweils etwa 15% kommen aus dem wissenschaftlichen und staatlichen Bereich und rund 12 % stammen aus der Zivilgesellschaft. Bezogen auf die gesellschaftliche Herkunft sind auch Kombinationen möglich, da viele Akteure und Initiativen einen interdisziplinären Charakter besitzen, so bspw. Initiativen, die eine Kooperation aus Zivilgesellschaft und dem Staat darstellen.

Die Zielgruppen dieser Akteure und Initiativen sind zu etwa 45% die Wirtschaft, wozu sämtliche Unternehmen unterschiedlichster Branchen zählen. Rund 22 % der erfassten Akteure und Initiativen fokussieren mit ihren Aktivitäten staatliche Zielgruppen, worunter sowohl Ziele auf Bundes-, Landes- als auch Kommunalebene zusammengefasst werden. Bürgerinnen und Bürger verschiedener Altersgruppen, Bürgerinitiativen oder Familien, zusammengefasst unter der Zielgruppe Zivilgesellschaft, werden von rund 20 % der Initiativen und Akteure adressiert. Etwa 13% der Stakeholder auf dem Gebiet der Cybersicherheit in Deutschland sprechen Bildungs- und Forschungseinrichtungen als Repräsentanten der wissenschaftlichen Zielgruppe direkt an. Hieraus lässt sich schließen, dass, neben klassischen wirtschaftlichen B2B-Beziehungen, vor allem die Vernetzung mit anderen Gesellschaftsgruppen im Vordergrund steht.

Abbildung 4 Angebotsverteilung aller Akteure und Initiativen.
Quelle: BMI

Zudem lässt sich das Angebot der Akteure und Initiativen in die drei Kategorien Dienstleistung, Produkt und Information aufteilen. Mit rund 41% stellen Informationen den größten Teil dar, Dienstleistungen werden zu rund 37%, Produkte zu rund 22%, verteilt über alle betrachteten Akteure und Initiativen der vier Gesellschaftsgruppen, angeboten.

3 Cybersicherheit in der Zivilgesellschaft

3.1 Allgemeiner Überblick

Den größten Anteil der Akteure, die sich in Deutschland zivilgesellschaftlich für Cybersicherheit engagieren, stellen gemeinnützige Vereine dar. Von ihnen gehen auch die meisten zivilgesellschaftlichen Initiativen aus. Teilweise werden diese auch durch die öffentliche Hand gefördert. Einzelpersonen oder kleinere Personengruppen, die mit ihrem Engagement die Cybersicherheit in Deutschland stärken, sind seltener in der deutschen Cybersicherheitslandschaft vertreten.

Zielgruppenverteilung zivilgesellschaftlicher Akteure und Initiativen

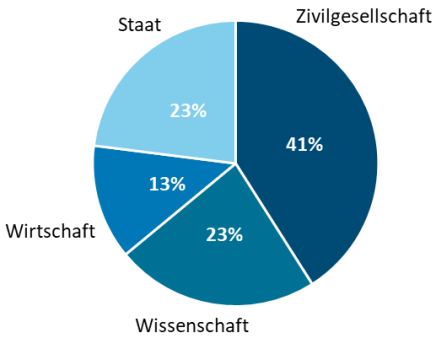


Abbildung 5 Zielgruppenverteilung zivilgesellschaftlicher Akteure und Initiativen. Quelle: BMI

Die Zielgruppe der Zivilgesellschaft ist größtenteils ebenfalls die Zivilgesellschaft; vom Bürger für den Bürger. Die Wirtschaft sowie der Staat werden zu gleichen Teilen, meistens im Rahmen der Interessenvertretung und des Verbraucherschutzes adressiert.

Lediglich 13% der zivilgesellschaftlichen Organisationsformen richten sich an die Wissenschaft. Diese stellen private Stiftungen, meistens zur Förderung der Wissenschaft und der Lehre, sowie gesamtgesellschaftliche Vereinigungen oder Organisationen aus dem wissenschaftsnahen Umfeld dar.

Zahlreiche zivilgesellschaftliche Initiativen bieten Vorträge und Veranstaltungen an, um über Cybersicherheitsthemen sowie Chancen und Risiken von Anwendungen aufzuklären oder den kompetenten und kritischen Umgang mit Medien zu fördern, wie bspw. der Chaos Computer Club e.V.[1] (CCC) oder die Landesverbraucherzentralen und der Verbraucherzentale Bundesverband e.V. (vzbv). Sie behandeln alle Fragen der Cybersicherheit und übernehmen dabei aufklärende, beratende und politisch orientierte Funktionen, bspw. durch Gutachten oder Stellungnahmen zu sicherheitsrelevanten Themen. Mit der Initiative "Chaos macht Schule" unterstützt der CCC Schülerinnen und Schüler, Eltern sowie Lehrerinnen und Lehrer in den Themen Medienkompetenz und Technikverständnis. Die Verbraucherzentralen informieren auf ihren Websites, über sonstige digitale Publikationen und in persönlichen Beratungen über Sicherheitsthemen wie Phishing-Mails. Durch eine Auswertung der von Verbraucherinnen und Verbrauchern geschilderten Probleme sowie durch eine Beobachtung des digitalen Marktes werden strukturelle Probleme aufgedeckt. Dieses zivilgesellschaftliche Engagement stellt einen wichtigen Beitrag für das private und berufliche Miteinander in der digitalen Welt dar.

Ein Anliegen der zivilgesellschaftlichen Stakeholder liegt in den Themen Awareness und Sensibilisierung für Cybersicherheit (39%) sowie in der Vernetzung der verschiedenen Gesellschaftsgruppen (31%). Der gemeinsame Dialog, die gegenseitige Unterstützung, der Erfahrungsaustausch und die Einbindung anderer Akteure und Initiativen in die eigenen Tätigkeiten und Ziele stehen neben der Vermittlung von Medienkompetenz und Technikverständnis im Fokus. Zivilgesellschaftliche Akteure und Initiativen stellen besonders den Verbraucherschutz, d.h. die Bedürfnisse der Bürgerinnen und Bürger, in den Mittelpunkt und setzen sich zusätzlich insbesondere für Themen wie Datenschutz, Informationsfreiheit, Netzzugang und Netzneutralität ein. Hierin werden vor allem Handlungsempfehlungen, Konzepte und konkrete Hilfestellungen thematisiert (16%). Zu den inhaltlichen Themen gehören bspw. Schadsoftware und Gefahren durch vernetzte Geräte im Internet der Dinge (IoT)[2].

[1] Der CCC hat einer Veröffentlichung eines eigenen Steckbriefs innerhalb dieses Kompendiums widersprochen.

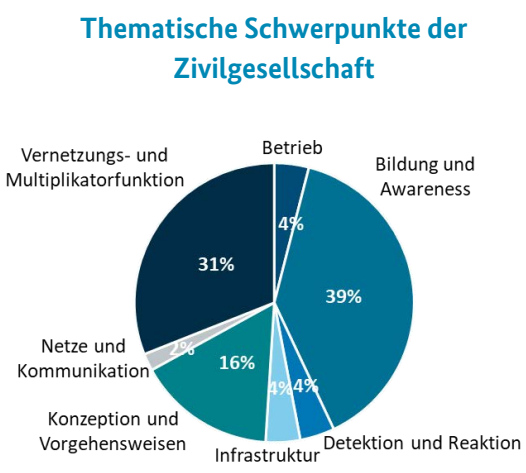


Abbildung 6 Thematische Schwerpunkte der Zivilgesellschaft. Quelle: BMI

Weitere Themen, wie etwa die detaillierte technische Detektion von sicherheitsrelevanten Ereignissen, entsprechende technische Gegenmaßnahmen, und technische Aspekte des sicheren Betriebs von IKT gehen über gängige Awarenessmaßnahmen hinaus und werden seltener durch zivilgesellschaftliche Akteure und Initiativen thematisiert (je 4%). Themen wie infrastrukturelle Aspekte der Cybersicherheit, die Einrichtung und Wartung sicherer (Kommunikations-)Netze scheinen für den Privatanwender wenig relevant zu sein, sodass es kaum Akteure und Initiativen gibt, die sich hiermit beschäftigen.

3.2 Schwerpunktthema: Cybersicherheit in der schulischen Ausbildung

Digitalisierung in Schulen in Zeiten von COVID-19

Die rasante Geschwindigkeit, mit der zu Beginn der COVID-19 Pandemie in Deutschland aufgrund von Kontaktbeschränkungen und Schulschließungen der gesamte Unterricht an Schulen und Universitäten auf digitale Methoden umgestellt werden musste, machte nochmals deutlich, wie wichtig es auch insbesondere im Bereich der Bildung ist, mit technologischen Weiterentwicklungen im digitalen Zeitalter Schritt zu halten. Jedoch offenbarten sich hierbei auch schnell Defizite, die einer effizienten und sicheren Digitalisierung des Bildungsalltags an deutschen Schulen im Wege standen. Hierzu gehören unter anderem die nötige Infrastruktur durch entsprechende Endgeräte wie Laptops und Tablets für Lehrpersonal und Schüler und entsprechende Breitbandzugänge an Schulen. Ebenso jedoch entsprechend einheitliche Lernplattformen zum Datenaustausch und entsprechend sichere Lernumgebungen mit qualitätsgeprüften und unabhängigen Lerninhalten, in denen Schülerinnen und Schüler durch ausgebildete Pädagoginnen und Pädagogen ihre Fertigkeiten im Bereich von Medienkompetenz, Datenschutz und Cybersicherheit schärfen können. Mit dem DigitalPakt Schule gehen Bund und Länder diese Themen derzeit an. Dies muss kontinuierlich fortgeschrieben und mit Qualifizierungsangeboten von unabhängiger Seite unterstützt werden.

Die Digitalisierung führt zu einem stetigen Wandel des Alltags der Menschen und tangiert dabei direkt und indirekt die Interessen der Schülerinnen und Schüler in ihren verschiedenen Rollen als bspw. junge Verbraucherinnen und Verbraucher oder Bürgerinnen und Bürger. Lernen muss verstärkt der zunehmenden Digitalisierung Rechnung tragen und sich an den damit einhergehenden Anforderungen ausrichten. Einerseits sind digitale Techniken und Inhalte zum Bestandteil der Lebens- und Arbeitswelt geworden, so dass Schulabsolventen und -absolventinnen während ihrer Schulzeit die Kompetenzen erwerben müssen, um auf die Anforderungen der digitalen Welt vorbereitet zu sein. Dies erfordert die Aufnahme diesbezüglicher Themen in die Lehrpläne und das Verständnis, dass Themen der Digitalisierung zum Bildungsauftrag der Schulen gehören. Zum anderen verändert die Digitalisierung das schulische Leben, indem digitale Lehr- und Lernprozesse für die Ausgestaltung des Lernorts Schule genutzt werden können und eine Kulturtechnik verändert. Dies erfordert ebenfalls neue Aus- und Weiterbildungsmöglichkeiten für Pädagogen.

Digitalisierung verändert in großem Maß die Möglichkeiten, wie Schülerinnen und Schüler Informationen suchen, verarbeiten und aufbewahren. Aufgabe von Schule muss sein, den Kompetenzerwerb bei Kindern und Jugendlichen zu stärken, um digitale Medien sicher und reflektiert nutzen zu können. Wichtig ist, dass Kompetenzen vermittelt werden und die Grenzen des eigenen Handelns zu erkennen. Denn Mündigkeit in der digitalen Welt ist ein Ideal, das mit der Realität nicht übereinstimmt. Die Vorstellung, dass sich Kinder und Jugendliche über schulische Bildung alle Details der digitalen Technologien und Kulturtechniken aneignen, den stetigen technologischen Wandel bewusst mitvollziehen und die daraus resultierenden Erkenntnisse in Fertigkeiten und Fähigkeiten für rationale Entscheidungen umsetzen können, ist als Anspruch an schulische Bildung nicht realistisch.

Um Digitalisierung an Schulen umzusetzen, ist eine strukturelle Verankerung über Lehrpläne, Aus- und Weiterbildung sowie Qualitätsstandards notwendig, die innerhalb des öffentlichen Bildungssystems verankert sein müssen. Außerschulische externe Partner und Themenverbünde können die öffentlichen Angebote mit ihren verschiedenen Perspektiven ergänzen. Außerschulische Partner können den Unterricht ergänzen, diesen aber nicht ersetzen.

Die Rolle des externen Akteurs muss durch eine Lehrkraft stets eingeordnet werden, um dem „Beutelsbacher Konsens“ gerecht zu werden und auch nur den Anschein der Interessensleitung auszuschließen.

Cybersicherheit im Kontext von Schulen betrifft zum einen den Aufbau diesbezüglicher Kompetenzen bei Schülerinnen und Schüler sowie zum anderen die technische Ausstattung der Institution Schule. Bereits in der Strategie der Kultusministerkonferenz „Bildung in der digitalen Welt“ aus dem Jahr 2016 werden Kompetenzbereiche festgehalten, die für Cybersicherheit relevant sind und eine systematische Umsetzung benötigen. Folgende Schwerpunkte sind hier zu nennen:

- sicherer Umgang mit mobilen Endgeräten und digitalen Umgebungen,
- rechtliche Rahmenbedingungen berücksichtigen (z.B. Cybermobbing, Datenschutz oder Urheberrecht),
- sicherheitsrelevantes Verhalten für persönliche Daten und Privatsphäre (z.B. Passwortsicherheit),
- Verschlüsselung und Signatur,
- aktuelle Bedrohungen im Bezug zu Informationssicherheit.

Damit Schulen sich diesen Aspekten stellen können, müssen Strukturen geschaffen werden, damit diese Themen im Unterricht und ergänzend in begleitenden Projekten aufgegriffen werden. Bundesweit müssen von öffentlicher Seite Qualifizierungsangebote für Lehramtsanwärter und Pädagogen im Schuldienst entwickelt und umgesetzt werden. Lehrkräfte müssen zu diesen Themen in erster Linie von öffentlicher Seite geschult werden. Um dies durch weitere Perspektiven zu unterstützen, können Schulen externe unabhängige Unterstützung und Partnerschaften nutzen. Im Rahmen der Recherchen zum Nationalen Pakt Cybersicherheit sind nur wenige Schulen aufgefallen, die das Thema Medienkompetenz und sicherer Umgang mit digitalen Medien in ihrem Schulleben öffentlich in den Vordergrund stellen und sich im Themenbereich Cybersicherheit stark engagieren. Selbst Schulen, die in Verbünden, Partnerschaften oder Kooperationen an Projekten teilnehmen, bewerben diese Aktivitäten über Kanäle, wie die eigene Internetdarstellung, kaum. Schulen stellen größtenteils nur den Einsatz von IT (z.B. Tablets, Notebooks, interaktive digitale Lernformen) in den Vordergrund, nicht aber den sicheren Umgang mit diesen und den Erwerb von Kompetenzen für die digitale Lebenswelt.

Des Weiteren sind Initiativen und Akteure aufgefallen, die Schulen bei der Umsetzung von Digitalisierungsprojekten unterstützen und als Multiplikatorplattformen für andere Schulen dienen (siehe hierzu die Steckbriefe von Akteuren und Initiativen mit zivilgesellschaftlicher Beteiligung). Zudem sind Akteure hilfreich, die Angebote zur Ausbildung von Lehrerinnen und Lehrer in entsprechenden Themen bieten und Werkzeuge bereitstellen, damit eine Ergänzung des Unterrichts möglich ist und entsprechende Projekte an Schulen durchgeführt werden können.

Bei all diesen Projekten stehen Medienkompetenz und das Verständnis für Technik im Vordergrund. Es geht im Schulkontext weniger um aktuelle Cyber-Technologien oder deren Implementierung in Schulen, sondern um die Vermittlung technisch-organisatorischer Grundkenntnisse durch geeignete Lernumgebungen, erlebnisorientierte Lernszenarien oder Medienkonzepte.

3.3 Schwerpunktthema: Medienkompetenz und Cybermobbing

Neben Schulen setzen sich auch eine Vielzahl zivilgesellschaftlicher Akteure und Initiativen mehrheitlich mit einem bewussten und sicheren Umgang mit dem Internet und IKT auseinander. Medienkompetenz, wie die verantwortungsvolle Nutzung Sozialer Netzwerke oder die Wahrung von Urheberrechten im Cyberspace stellen hierbei häufig einen Schwerpunkt dar. Die soziale Komponente der Cybersicherheit, wie die Verhinderung von Cybermobbing, spiegelt sich in den Initiativen und Akteuren der Zivilgesellschaft wider. Auch wenn Medienkompetenz und die Verhinderung von Gewalt im Internet nur im weiteren Sinne Bezüge zur Cybersicherheit aufweisen, werden nachfolgend, und in Ergänzung zu den Steckbriefen, Akteure und Initiativen aufgeführt, die sich intensiv mit dieser Thematik beschäftigen und somit deren Bedeutung für die Zivilgesellschaft unterstreichen.

Bundesverband Frauenberatungsstellen und Frauennotrufe Frauen gegen Gewalt e.V. (bff) *frauen-gegen-gewalt.de*

Die Initiative "Aktiv gegen digitale Gewalt" des bbf bietet Informationen zur Vermeidung digitaler Gewalt sowie Technik-Sicherheit an. Zudem wird auf weitere ähnliche Projekte oder Unterstützung verwiesen und dabei geholfen, Hilfsangebote vor Ort zu finden.

Bundesverband Gewaltprävention "Selbstbewusst & Stark e.V." *bundesverband-gewaltpraevention.de*

Der Bundesverband "Selbstbewusst & Stark e.V." bietet neben Kursen und Lehrgängen auch Workshops und Schulungen zu Gewaltthemen, darunter auch Cybermobbing, an.

Bündnis gegen Cybermobbing e. V. *buendnis-gegen-cybermobbing.de*

Der Bündnis gegen Cybermobbing e. V. verfolgt das Ziel, die Gesellschaft zum Thema Cybermobbing aufzuklären und zu sensibilisieren. Mitglieder des Bündnisses sind Einzelpersonen aus unterschiedlichen Bereichen; unterstützt wird die Initiative allerdings auch von Unternehmen und verschiedenen Organisationen. Das Bündnis engagiert sich in den Bereichen Prävention, Aufklärung und Forschung zum Thema Cybermobbing. Dabei umfassen die Aktivitäten bspw. die Durchführung von Studien, die Organisation von Fachvorträgen oder Präventionsarbeit an Schulen. Darüber hinaus stellt das Bündnis auf unterschiedliche Zielgruppen ausgerichtete Broschüren zum Cybermobbing zum Download bereit.

Cybermobbing-Prävention e.V. *cybermobbing-praevention.de*

Der "Cybermobbing Prävention e. V." hat das Ziel, die Sensibilisierung im Bereich Cybermobbing mithilfe von Kreativität und Dialog zu fördern. Hierzu bieten Medienpädagogen und Anti-Gewalttrainer verschiedene Workshops und Fortbildungen an. Die Präventionsangebote richten sich dabei an Schülerinnen und Schüler, Lehrkräfte und Eltern. Zur Aufklärung werden Lehrkräftefortbildungen und Elternabende angeboten. Um Schülerinnen und Schüler geeignet zu sensibilisieren stehen kreative Angebote wie bspw. das "Cybermobbing Hip-Hop Projekt" zur Verfügung, bei dem Schülerinnen und Schüler gemeinsam mit den Projektverantwortlichen ihren eigenen Song gegen Cybermobbing produzieren. Neben diesen Präventionsmaßnahmen werden auch Beratung und Interventionshilfe angeboten.

Cybermobbing-Hilfe e.V. *cybermobbing-hilfe.com*

Der Verein Cybermobbing-Hilfe e.V. setzt sich für die Prävention von Cybergewalt, insbesondere aber Cybermobbing, ein. Hierzu werden u.a. Präventionsmaßnahmen, konstante Öffentlichkeitsarbeit und die Zusammenarbeit mit anderen Institutionen eingesetzt. Darüber hinaus wird eine ehrenamtliche Hilfe von Jugendlichen für Jugendliche und Kinder angeboten.

Deutscher Kinderschutzbund Kreisverband Erlangen e.V. *kinderschutzbund-erlangen.de*

Das Medientraining "Medienlöwen" wurde, aufbauend auf dem Modellprojekt "Medienlöwen - Münchner Medientraining", weiterentwickelt, um Prävention im Medienbereich für Kinder in der Grundschule leisten zu können. Ziel des Medientrainings ist es, Kinder in spielerisch gestalteten Unterrichtseinheiten an einen verantwortungsvollen Umgang mit Handys, Computern und Internet heranzuführen.

Europäisches Integrationszentrum Rostock e.V. *eiz-rostock.de*

Das europäische Integrationszentrum Rostock e.V. bietet Informationen zu Cybermobbing, u.a. der Vorbeugung und der Erkennung, an. Dazu werden konkrete Handlungshinweise für den Fall von Cybermobbing geliefert.

FRIEDA-Frauenzentrum e. V. *frieda-frauenzentrum.de*

Das Anti-Stalking-Projekt mit dem Fachbereich Cyberstalking wird vom FRIEDA-Frauenzentrum e.V. getragen. Im Rahmen des Projekts werden zum einen Betroffene und Angehörige beraten und zum Thema Cyberstalking informiert, zum anderen wird die Öffentlichkeit zum Thema informiert und sensibilisiert.

JUUUPORT e.V. *juuuport.de*

Der JUUUPORT e. V. setzt sich für einen respektvollen Umgang im Internet ein. Dazu bietet der Verein eine Online-Beratung von jungen Menschen für junge Menschen an.

Law4school *law4school.de*

Über Infoflyer und Webinare werden im Projekt Law4school, das vom Verein "Prävention 2.0" ins Leben gerufen wurde, Kinder und Jugendliche zum Thema Cybermobbing aufgeklärt. Die Webinare und Vorträge werden in Bildungseinrichtungen gehalten und zeigen anhand praktischer Fälle rechtliche und tatsächliche Folgen auf.

Medien-Leuchtturm *medien-leuchtturm.de*

Das Team des Medien-Leuchtturms ist Ansprechpartner für Fragen zu den Themen Medienbildung und Medienkompetenz für alle Altersklassen. Dabei werden neben Informationsveranstaltungen auch Schulungen und Workshops zum Thema Internet und Smartphone angeboten.

Medienscout e.V. *medienscout.info*

Das Ziel des Medienscout e.V. ist es, Schülerinnen und Schülern den kompetenten, sicheren und werteorientierten Umgang mit Medien zu vermitteln. „Medienscouts“ sind Schülerrinnen und Schüler, die vom Verein Medienscout e.V. ausgebildet werden, um in der Schule einen Beitrag zur Medienkompetenz unter Gleichaltrigen zu leisten.

Sicher-Stark-Stiftung e.V. *sicher-stark-team.de*

Ziel der Sicher-Stark-Stiftung e.V. ist es, Kinder sowohl im Internet als auch auf der Straße sicher und stark zu machen und deren Selbstvertrauen, Selbstbewusstsein und Selbstwertgefühl zu stärken. Hierzu werden zu zahlreichen Themen Kurse angeboten, an denen nicht nur Kinder sondern auch Erzieherinnen und Erzieher, Lehrerinnen und Lehrer sowie Eltern teilnehmen können. Das Kursangebot beinhaltet u.a. auch Angebote zu Computersicherheit und dem Umgang mit neuen Medien und mobilen Geräten.

4 Cybersicherheit in der Wissenschaft

4.1 Allgemeiner Überblick

Die Akteure und Initiativen der Wissenschaft verteilen sich ausgewogen je hälftig auf außeruniversitäre Forschungseinrichtungen bzw. Initiativen und Einrichtungen oder Initiativen von Hochschulen. Im Computer Science Rankingwerden wissenschaftliche Institute anhand ihrer relevanten Veröffentlichungen bewertet. Hiernach sind in den letzten zehn Jahren insgesamt drei wissenschaftliche Einrichtungen der Cybersicherheit aus Deutschland unter den 20 weltweit Besten platziert. Sowohl anwendungsorientierte Forschung wie auch Grundlagenforschung sind in Deutschland ausgewogen verteilt. Die größten Zentren für Cybersicherheit befinden sich in Bochum, Darmstadt und Saarbrücken. Standorte wie bspw. Ansbach, Albstadt-Sigmaringen, Berlin, Bonn, Cottbus, Erlangen, Karlsruhe, Lübeck, Magdeburg, München, Münster und Passau sind ebenfalls wissenschaftlich gut positioniert. Während Deutschland im Bereich der Forschung grundsätzlich gut aufgestellt ist, ist auch die Dichte an Forschungseinrichtungen in diesem Bereich auf gutem internationalem Niveau. Im internationalen Vergleich konzentriert sich der Exzellenzanspruch für Cybersicherheit in Deutschland hauptsächlich auf die oben genannten Zentren. Im direkten Vergleich mit den USA zählt dort fast jede Spitzenuniversität gleichzeitig auch mit zu den Besten im Bereich der Cybersicherheit. Innerhalb Europas ist Deutschland insgesamt qualitativ und quantitativ sehr gut positioniert.

Für die Wissenschaft ist besonders charakteristisch, dass sie ein breites Spektrum an Themen relativ ausgewogen bedient. Die häufigste Gemeinsamkeit wissenschaftlicher Akteure und Initiativen ist die aktiv betriebene Vernetzung. Fast ein Viertel der untersuchten Akteure und Initiativen vernetzt sich öffentlichkeitswirksam. Die Wissenschaft ist in den meisten Verbänden, Netzwerken und Gremien der Cybersicherheit vertreten und wird für ihren fundierten und zukunftsweisenden Input geschätzt.

Die Bedeutung der Vernetzung wird auch in der Praxis der Forschungsförderung deutlich. Grundsätzlich herrscht ein ausgewogenes Verhältnis zwischen Kollaboration und Innovationen schaffendem Wettbewerb. Zum einen wird direkt um finanzielle Förderung für einzelne Forschungsvorhaben konkurriert, zum andern wird durch die Förderung von Verbundprojekten die Kollaboration verschiedener Forschungseinrichtungen aktiv vorangetrieben.

Zudem nimmt die Bedeutung drittmittelgeförderter Forschungsverbünde, bspw. über die Deutsche Forschungsgemeinschaft, zu welchem sich Wissenschaftlerinnen und Wissenschaftler verschiedener Standorte zusammenschließen, immer mehr zu.

Schwerpunkte in der Forschung sind insbesondere Zukunftstechnologien wie kryptographische Verfahren, Quantenkryptographie oder Blockchain, zusammengefasst im Themencluster Konzeption und Vorgehensweisen (16%), aber auch sichere vernetze Systeme und künstliche Intelligenz (7%) spielen eine immer größere Rolle. Die Cybersicherheitsforschung in Deutschland ist besonders ausgeprägt in den Themengebieten der Kryptographie, der System-, Soft- und Hardwaresicherheit, in formalen Methoden zum Beweisen von Systemsicherheit, aber auch im Bereich von Technologien zum Schutz der Privatsphäre. Die Verknüpfung von Künstlicher Intelligenz (KI) oder Machine Learning (ML) mit IT-Sicherheit, um sich KI- bzw. ML-Ansätzen zur Herstellung oder Prüfung von Sicherheit zu bedienen bzw. um KI- und ML-Modelle vor Manipulation abzusichern, sind Zukunftsthemen in der Cybersicherheitsforschung. In Deutschland sind hiermit die wichtigsten Grundlagen im Bereich der Wissenschaft und Forschung zwar gelegt, jedoch ist dieser Themenbereich im internationalen Vergleich und in Anbetracht der wachsenden Bedeutsamkeit der Thematik noch ausbaufähig.

Verteilung behandelter Cyberthemen der Wissenschaft

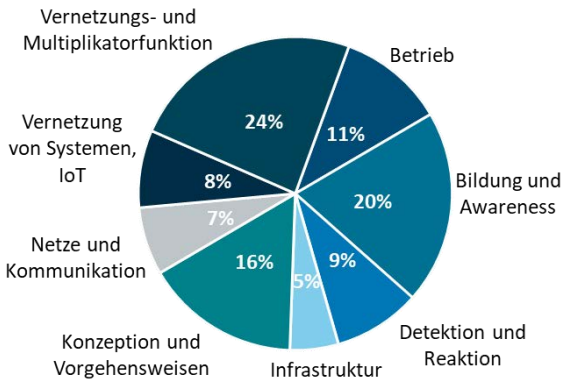


Abbildung 7 Verteilung behandelter Cyberthemen der Wissenschaft. Quelle: BMI

Akteure oder Initiativen aus der Wissenschaft widmen sich in einem großen Umgang auch der Bildung und dem Wissenstransfer von Cybersicherheitsthemen (20%).

Die bereits erwähnte gesamtgesellschaftliche Verflechtung der Wissenschaft zeigt sich auch in der Zielgruppenanalyse. Die größte Zielgruppe der Wissenschaft stellt mit 33% die Wirtschaft dar. Kernthema ist hier vor allem der Wissenstransfer und die gemeinsame Arbeit in Forschung und Entwicklung, aber auch in Initiativen und Netzwerken, welche Veranstaltungen, Foren und Arbeitsgruppen zu IT-Sicherheitsthemen organisieren. Ziele dieser Akteure und Initiativen sind die Steigerung des Informationsaustauschs und die gemeinsame Weiterentwicklung von spezifischen Cybersicherheitsthemen. Auch die Intensität der Beziehungen zu den großen, zumeist US-amerikanischen Internet- und Digitalunternehmen wie Google, Amazon, Facebook oder Intel hat Auswirkungen auf Forschung und Wissenschaft. US-Forschungsinstitute erhalten durch ihre Nähe zu den genannten Unternehmen oftmals einen technologischen Vorsprung.

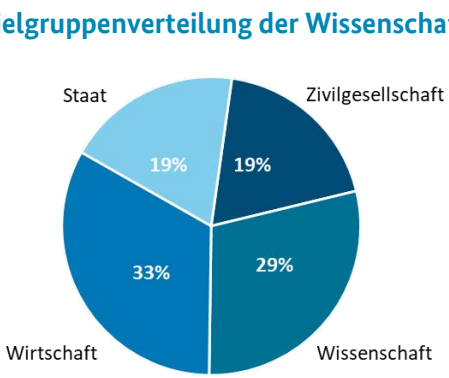


Abbildung 8 Zielgruppenverteilung der Wissenschaft.
Quelle: BMI

Mit dem Ziel, Forschungsergebnisse in die Anwendung zu transferieren, richten sich zahlreiche wissenschaftliche Einrichtungen an Wirtschaftsunternehmen, um diese bei Digitalisierungsmaßnahmen zu unterstützen oder gezielt deren individuelle Probleme zu lösen. Dennoch ist der Wissenstransfer, besonders im Rahmen von wissenschaftlichen Ausgründungen in der Cybersicherheit, noch ausbaufähig. Zwar existieren Gründerzentren an den Hochschulstandorten und spezielle Förderprogramme, jedoch führt die oft fehlende Liquidität, zumeist aufgrund geringerer Risikobereitschaft deutscher Kapitalgeber, in der Wachstumsphase dazu, dass sich neue Akteure am Markt international nicht behaupten können und auch oft von ausländischen Unternehmen oder Kapitalgebern aufgekauft werden, was eine Abwanderung von Know-how zur Folge haben kann.

Mit 29% stellt die Wissenschaft selbst die zweitgrößte Zielgruppe dar, da Forschungsergebnisse, Veröffentlichungen und die Rezeption dieser sich meist direkt an die Wissenschaft richten und wesentlicher Bestandteil wissenschaftlicher Arbeit sind. Staat und Zivilgesellschaft werden jeweils zu 19% direkt durch die Wissenschaft adressiert. Hierbei stehen vor allem der gemeinsame Dialog und der Erfahrungsaustausch, aber auch das Engagement in gesamtgesellschaftlichen Initiativen wie auch die Lehre an Hochschulen im Fokus.

An Hochschulen und außeruniversitären Forschungsinstituten wird angewandte Forschung und Grundlagenforschung betrieben, um intelligente Lösungen für spezifische Fragestellungen zu entwickeln oder theoretische Forschungsergebnisse in die praktische Anwendung zu überführen. Die Akteure und Initiativen forschen an grundlegenden IT-Sicherheitsthemen bis hin zu interdisziplinären Fragestellungen, die ökonomische, soziale und juristische Aspekte der Cybersicherheit betreffen. Die Nähe oder gar Verflechtung wissenschaftlicher Einrichtungen mit der Hochschullehre sorgen zudem für eine Versorgung der Initiativen und Akteure mit Fachkräften.

Das Angebot wissenschaftlicher Akteure und Initiativen besteht zu großen Teilen aus Informationen (47%), wie Studien und Publikationen sowie Lehrinhalten, aber auch konkreten Dienstleistungen wie Forschung und Entwicklung oder Beratung (47%). Das konkrete Angebot von (marktreifen) Produkten, wie Soft- oder Hardware nimmt erwartungsgemäß nur einen geringen Stellenwert ein (7%).

4.2 Schwerpunkthema: Cybersicherheitslehre an Hochschulen

Die gesteigerte Wahrnehmung und Relevanz der Cybersicherheit lässt sich auch an den Hochschulen betrachten. Mittlerweile gibt es an 28 von 68 deutschen Universitäten aus dem Ranking des Centrums für Hochschulentwicklung (CHE), die im Bereich Informatik lehren und forschen, schwerpunktmäßige und spezialisierte Angebote zur Cybersicherheit. An neun der 68 Universitäten werden zudem dedizierte Studiengänge zur IT- und Cybersicherheit angeboten. Diese Studienmöglichkeiten umfassen neun Master- und fünf Bachelor-Studiengänge. Doch auch an Universitäten, die keinen dedizierten Studiengang IT-Sicherheit anbieten, steigt das Angebot an einzelnen Kursen und Forschungsangeboten zur Cybersicherheit merklich. Immer mehr Lehrstühle, bei welchen Cybersicherheit nicht der explizite Schwerpunkt ist, erweitern ihre Aktivitäten in Lehre und Forschung dahingehend, sodass die Thematik einen stetig größer werdenden Stellenwert einnimmt. An heute insgesamt 32 staatlichen und privaten Hochschulen angewandter Forschung bzw. Fachhochschulen existieren einschlägige Einrichtungen zur Forschung und Lehre mit insgesamt 16 Bachelor- und zehn Masterstudiengängen. Damit hat sich das Angebot an Studiengängen im Themenfeld IT-Sicherheit innerhalb der letzten fünf Jahre mehr als verdoppelt. Hochschulen mit starkem Fokus auf Wissenschaft und Lehre in der Informatik tendieren zunehmend dazu, auch ein Grundangebot an cybersicherheitsspezifischen Vorlesungen und Inhalten anzubieten.

Während in den letzten Jahren das Thema Cybersicherheit stetig an Gewicht gewonnen hat, ist auch die Zahl der Professuren an deutschen Hochschulen stark angestiegen, wodurch sich eine für europäische Verhältnisse einzigartige Dichte an wissenschaftlichen Einrichtungen entwickelt hat. Die beiden nachstehenden Tabellen geben einen Überblick über die Zahl der Professuren, welche sich rein bzw. fast ausschließlich mit Cybersicherheit in Lehre und Forschung beschäftigen.

Universität	Professuren	Bachelor	Master
RWTH Aachen	1		
Uni Bamberg	1		
TU Berlin	2		
Uni Bochum	7	1	2
Uni Bonn	2	1	
TU Braunschweig	2		
BTU Cottbus-Senftenberg	3		1
TU Darmstadt	8		1
TU Dresden	1		
Uni Göttingen	2		
Uni Hamburg	2		
Uni Hannover	1		
Karlsruher Institut für Technologie KIT	1		
Uni Kassel	1		
Uni Koblenz-Landau	2		
Uni Lübeck	4	1	1
Uni Magdeburg	2	1	
Uni BW München	10		1
TU München	1		
Uni Münster	4		
Uni Erlangen-Nürnberg	2	2	1
Uni Paderborn	3		
Uni Passau	5		1
Uni Potsdam / H.-Plattner-Inst. (priv.)	3		1
Uni Regensburg	3		
Uni des Saarlandes	13	1	1
Uni Siegen	1		
Uni Stuttgart	5		

Tabelle 1 Übersicht der Professuren und Studiengänge der Cybersicherheit an Universitäten

(Fach-)Hochschule	Professuren	Bachelor	Master	Diplom
FH Aachen	1			
HS Aalen	1	1	1	
HS Albstadt-Sigmaringen	3	1	3	
HS Ansbach	6	1		
SRH Berlin University of Applied Sciences (priv.)	1		1	
TH Brandenburg	4	1	1	
Hochschule des Bundes (Brühl)	4			1
HS Darmstadt	2	1		
TH Deggendorf	1	1	1	
FH Dortmund	2			
FH Erfurt	1			
IUBH Internationale Hochschule (priv.)	1		1	
HS Fulda	1			
Westfälische HS/Gelsenkirchen	2		1	
HS Hannover	2			
Leibniz FH (priv.)		1		
TH Ingolstadt	1			
HS Karlsruhe	2			
HS Kempten	2			
HS Niederrhein/Krefeld		1		
HS Mainz	1			
Duale Hochschule Baden-Württemberg	5	5		
HS Mannheim	1	1		
HS Mittweida	2	2	1	
Hochschule der Bayerischen Wirtschaft (priv.)			1	
FHDW Nordrhein-Westfalen (priv.)	2	1		
HS Offenburg	1	1	1	
HS Schmalkalden	1			
HS Stralsund	3	1	1	
HS Trier	1	1		
FH Wedel (priv.)		1		
HS Wismar	2	1	1	

Tabelle 2 Übersicht der Professuren und Studiengänge der Cybersicherheit an (Fach-)Hochschulen

Ungeachtet der stetig wachsenden Angebote von Universitäten und Hochschulen angewandter Forschung / Fachhochschulen werden mehr Expertinnen und Experten benötigt, als derzeit und wohl auch perspektivisch zur Verfügung stehen. Dadurch wird es für Unternehmen unerlässlich sein, auch im Ausland, insbesondere in den USA und Israel, Fachkräfte zu werben. Auch ein „Training on the Job" ist für die Cybersicherheitsbranche zukünftig umso relevanter zur Rekrutierung neuer Expertinnen und Experten. Neben technischer Expertise ist auch das Interesse an der Wahrung und Schaffung der allgemeinen Sicherheit im Cyberraum unumgänglich. Eine Lösung zum Umgang mit dem Mangel an Fachkräften könnte die feste Verankerung der Cybersicherheit im Curriculum allgemeiner Informatikstudiengänge sein, wie es bspw. von der Gesellschaft für Informatik (GI) für Bachelor und Masterstudiengänge vorgeschlagen wird.

4.3 CyBOK – Schaffung etablierten Grundlagenwissens in der Cybersicherheit

Es gibt eine seit langem anerkannte Qualifikationslücke innerhalb des Cybersicherheitssektors, ein Problem, bei dem sich die Expertinnen und Experten einig sind, dass es durch ein fragmentiertes und inkohärentes Grundlagenwissen für dieses populär gewordene und dynamische Gebiet noch verschärft wird. Ausgereifte wissenschaftliche Disziplinen wie Mathematik, Physik, Chemie und Biologie verfügen über seit langem vorhandenes Grundlagenwissen und klare Lernschritte von Schulen bis hin zu Universitäten.

Hier setzt das Projekt CyBOK – Cybersecurity Body of Knowledge – an. CyBOK ist ein Leitfaden für Grundlagenwissen, welcher anerkannte Literatur wie Lehrbücher, akademische Forschungsartikel, technische Berichte und Standards kodifiziert. Der Schwerpunkt des Projekts liegt auf der Erfassung des vorhandenen Wissens und nicht darauf, alles, was jemals zu diesem Thema geschrieben wurde, vollständig zu reproduzieren. Das CyBOK-Projektteam hat eine umfangreiche Kartierung und Analyse relevanter Texte sowie eine Reihe von Konsultationen der Gemeinschaft, anhand von Workshops, Online-Umfragen, Interviews und Positionspapieren durchgeführt. Diese Aktivitäten ermöglichten ein vertieftes Verständnis der kollektiven Sicht der Wissenschaft auf die Cybersicherheit. CyBOK soll eine international anerkannte Ressource sowohl für die Entwicklung akademischer Curricula als auch für die Einstufung professioneller Fähigkeiten innerhalb der Cybersicherheits-Community werden.

Der Lenkungsausschuss des CyBOK setzt sich aus nationalen wie internationalen Expertinnen und Experten aus Wissenschaft und Wirtschaft zusammen. Gemeinsam stellen sie die international anerkannte wissenschaftliche Qualität der Wissenssammlung sicher und entscheiden über die Aufnahme weiterer Literatur in die bestehende Wissensbasis. Frau Prof. Dr. Mira Mezini vertritt im wissenschaftlichen Beirat des Projektes die deutsche Wissenschaft auf diesem Gebiet.

5 Die Cybersicherheitswirtschaft

5.1 Allgemeiner Überblick

Unternehmen der Privatwirtschaft stellen mit etwa 58% aller Akteure und Initiativen zahlenmäßig den größten Teil derer dar, die sich in Deutschland im Umfeld Cybersicherheit betätigen. Sie sind überwiegend der Branche „Informations- und Kommunikationstechnik“ zuzuordnen (57%) und beraten im Schwerpunkt bei Digitalisierungsprojekten und der Konzeption und Umsetzung von IT-Sicherheitskonzepten inklusive der Einführung von IT-Sicherheitsmanagementsystemen (25%). Neben den Beratungsleistungen stellen diese Unternehmen zum Teil auch entsprechende Hardware- und Software-Lösungen zur Verfügung, um IT-Sicherheitsmaßnahmen zu etablieren. Maßnahmen zur Vermeidung von IT-Sicherheitsangriffen, die Unterstützung bei der Aufklärung und Behebung von Sicherheitsvorfällen oder Sicherheits-Audits und -Zertifizierungen gehören zum Portfolio der meisten Beratungsunternehmen.

Branchenverteilung wirtschaftlicher Akteure und Initiativen

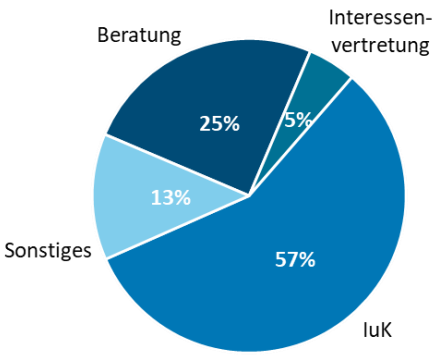


Abbildung 9 Branchenverteilung wirtschaftlicher Akteure und Initiativen. Quelle: BMI

Etwa 13% der Stakeholder der deutschen Cybersicherheitswirtschaft entstammen diversen Branchen, die für sich einen geringen Teil ausmachen und daher zusammengefasst wurden, darunter u.a. die Luft- und Raumfahrt-Branche, Automotive, Baugewerbe, Finanzdienstleistung, Energieversorgung, freie Berufe oder die Rüstungsbranche. Ca. 5% der Akteure und Initiativen stellen Verbände und Interessenvertretungen der Wirtschaft dar. Einen Überblick hierzu bietet vor allem das Kapitel „Verbände und Interessenvertretungen“. Viele Verbände und Interessensvertretungen der Privatwirtschaft setzen sich für die Weiterentwicklung der Qualitätsmaßstäbe und sicherheitsrelevanten Standards und Normen im Bereich der IT-Sicherheit ein. Sie leisten dadurch einen wichtigen Beitrag, nicht nur für die Wirtschaft selbst, sondern auch aus gesamtgesellschaftlicher Perspektive. Durch themenspezifische Arbeitsgruppen liefern sie einen wesentlichen Beitrag, um Vernetzung und Kompetenzerweiterung im Themenfeld Cybersicherheit voranzutreiben oder im Verbund innovative Lösungen zu schaffen. Zudem dienen die Interessensverbände der Vernetzung und dem gegenseitigen Austausch der Akteure und vertreten die Interessen ihrer Mitglieder gegenüber politischen Entscheidungsträgern.

Thematische Schwerpunkte der Wirtschaftsteilnehmer

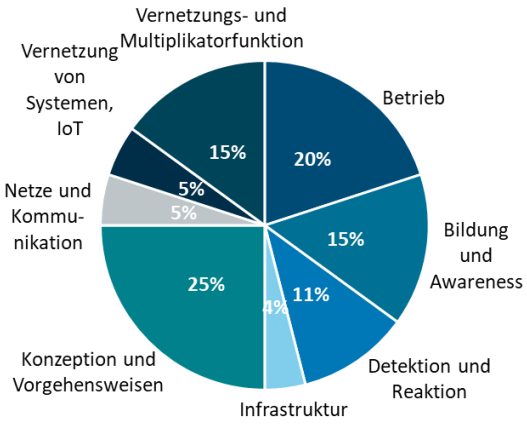


Abbildung 10 Thematische Schwerpunkte der Wirtschaftsteilnehmer. Quelle: BMI

Thematisch befassen sich die Wirtschaftsteilnehmer mit diversen Bereichen. Dabei werden die meisten Themen ähnlich oft abgedeckt, sodass ein deutlich hervorgehobener Schwerpunkt nicht erkennbar ist. Etwa ein Viertel aller Akteure und Initiativen der Wirtschaft setzt sich mit konzeptionellen Themen, u.a. Kryptographie, Authentifizierung, Informationssicherheitsmanagement (ISMS), Endgerätesicherheit, Identitäts- und Berechtigungsmanagement, Datenschutz und IT-Sicherheitsstandards aktiv auseinander und stellt Vorgehensweisen für ihre Kundinnen und Kunden zur Verfügung. Betriebsbezogene Sicherheitsaspekte ist der zweithäufigste vertretene Themenbereich der deutschen Cybersicherheitswirtschaft (20%).

Hierin werden neben dem Schutz vor Cyberangriffen auch Cloudsicherheit, Sicherheitsmonitoring sowie die IT-Administration behandelt. Ein weiterer, häufig behandelter Cybersicherheitsschwerpunkt ist mit 15% die

Schaffung von Awareness und die damit einhergehenden Bildungsangebote wie bspw. Schulungen. Ebenfalls 15% der betrachteten wirtschaftlich tätigen Cybersicherheitsorganisationen betreiben eine aktive Vernetzung, bspw. durch das Engagement in Verbänden, Arbeitsgruppen, Vereinen und Gremien.

Insgesamt 11% widmen ihre Geschäftstätigkeit der Detektion von und Reaktion auf IT-sicherheitsrelevante Ereignisse, wie bspw. im Rahmen der IT-Forensik. Weniger weit verbreitet sind hochspezialisierte Themenkomplexe wie sichere vernetzte Systeme im Internet der Dinge, im Bereich Künstlicher Intelligenz (5%), oder der Netzarchitektur (5%). Infrastrukturelle Sicherheitsaspekte, also Themen wie sichere Betriebs- und Steuerungstechnik, sichere intelligente Messsysteme oder sichere Rechenzentrumsinfrastruktur, werden nur von etwa 4% der wirtschaftlich tätigen Akteure und Initiativen abgedeckt.

Schwerpunkte wirtschaftlicher Betätigung der Cybersicherheitsunternehmen

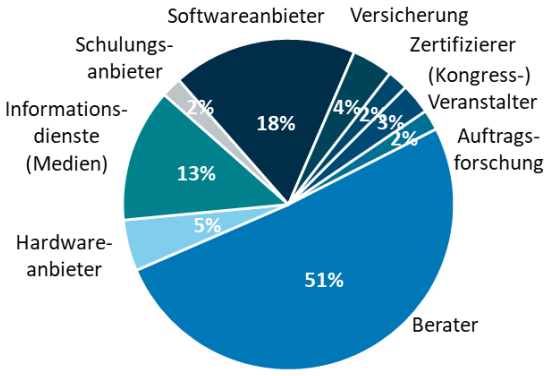


Abbildung 11 Schwerpunkte wirtschaftlicher Betätigung der Cybersicherheitsunternehmen. Quelle: BMI

Unabhängig von Ursprungsbranchen und behandelten Cyberthemen lassen sich bei den Cybersicherheitsunternehmen unter den Akteuren und Initiativen der Wirtschaft die folgenden Schwerpunkte wirtschaftlicher Betätigung betrachten. Bemerkenswert ist, dass rund die Hälfte aller Unternehmen beratend tätig ist, auch, wenn es sich bspw. um ein originäres Softwarehaus oder einen Hardwarehersteller handelt.

Dienstleistungsangebote wirtschaftlicher Akteure und Initiativen

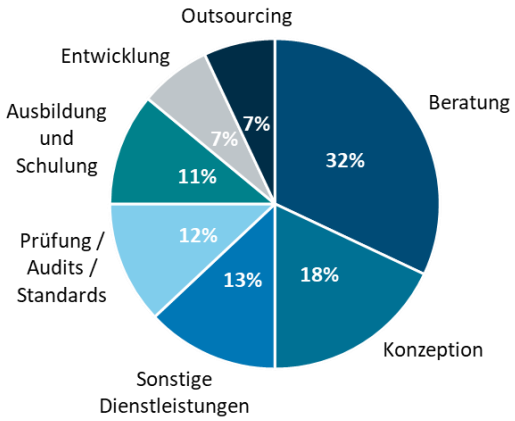


Abbildung 12 Dienstleistungsangebote wirtschaftlicher Akteure und Initiativen. Quelle: BMI

Etwa 18% der Unternehmen stellen Software her oder vertreiben solche. Spezialisierte Anbieter sicherer Software sind hingegen mit 5% seltener. 13% der Unternehmen bieten Beiträge zum Fachthema Cybersicherheit im Rahmen ihrer wirtschaftlichen Tätigkeit an.

Spezialisierte Schulungsanbieter, Eventveranstalter, Zertifizierer und Einrichtungen der Auftragsforschung sind mit unter 5% vertreten. Fast 4% der Unternehmen beschäftigen sich mit dem Vertrieb von Versicherungen gegen Cyberrisiken. Dazu gehören nahezu alle nationalen Versicherer, aber auch FinTech-Startups. Grundsätzlich ist anzumerken, dass die Kombinationen der Branche, Zielgruppe, wirtschaftlicher Schwerpunkte und der behandelten Cybersicherheitsthemen zu einer sehr heterogenen Ausgestaltung der deutschen Wirtschaft führen.

Die wenigsten Akteure stellen ihre Leistungen dedizierten Wirtschaftszweigen zur Verfügung, sondern arbeiten branchenübergreifend. Die Zielgruppe besteht größtenteils ebenfalls aus Wirtschaftsteilnehmern (54%), oft aber auch aus staatlichen Stellen (27%). Seltener wird die Zivilgesellschaft (11%) adressiert. Hier steht besonders die Vermarktung von Verbraucherprodukten der IT-Sicherheit im Fokus, was jedoch, bezogen auf den Gesamtmarkt, einen kleinen Teilbereich ausmacht, der u.a. durch einige wenige internationale Firmen dominiert wird. Die kleinste Zielgruppe stellt die Wissenschaft (8%) dar. Forschungskooperationen sowie spezialisierte Produkte für den Forschungs- und Wissenschaftsbereich bilden hier eine Nische.

Das Angebot wirtschaftlicher Akteure und Initiativen ist einigermaßen ausgewogen verteilt zwischen Produkten (37%), wie Hard- und Software, Dienstleistungen (37%), wie Beratung und Entwicklung sowie Informationen (26%), wie Journalismus, Blogs, Podcasts und andere Informationsaufbereitungen, teilweise auch kostenlos.

Innerhalb der von wirtschaftlichen Akteuren und Initiativen angebotenen Dienstleistungen überwiegen beratende sowie konzeptionelle Dienstleistungen und machen zusammen die Hälfte aller angebotenen Dienstleistungen aus. Angebote bezüglich der Entwicklung von (Software-)Lösungen oder Outsourcing-Angebote bilden innerhalb der Dienstleistungsangebote hingegen nur einen geringen Anteil mit jeweils 7 %. Unter „Sonstige Dienstleistungen“ sind z.B. Cyberversicherungen oder Penetrationstests zusammengefasst.

Die Angebote im Bereich Information setzen sich überwiegend aus aufbereiteten Informationen zusammen, die bspw. auf der Webseite des jeweiligen Akteurs oder der jeweiligen Initiative veröffentlicht werden. Weitere häufige Informationsangebote stellen Newsletter (13 %), Blogs (12 %), Studien (12 %) sowie Informationsangebote im Rahmen von Öffentlichkeitsarbeit (9 %) dar. Der Bereich „Sonstiges Informationsangebot“ (19 %) umfasst z. B. Lernprogramme sowie wissenschaftliche oder journalistische Veröffentlichungen.

Informationsangebote wirtschaftlicher Akteure und Initiativen

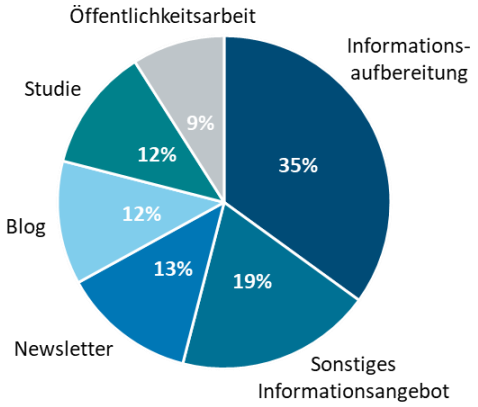


Abbildung 13 Informationsangebote wirtschaftlicher Akteure und Initiativen. Quelle: BMI

Die Produktangebote bestehen hauptsächlich aus Software- und Software as a Service Angeboten (63 %). Clouddienste bzw. Platform as a Service sowie Hardwareangebote bilden jeweils 12 % der Produktangebote wirtschaftlicher Akteure und Initiativen. „Sonstige Produkte“ umfassen bspw. vernetzte Produkte aus dem Bereich IoT oder Infrastructure as a Service.

Ein Vergleich der zahlenmäßig am häufigsten vertretenen Branchen Beratung sowie Information und Kommunikation (vgl. Abbildung 9: Branchenverteilung wirtschaftlicher Akteure und Initiativen) hinsichtlich der verschiedenen Angebote zeigt eine strukturelle Ähnlichkeit beider Branchenausrichtungen. Dies ist vor dem Hintergrund naheliegend, dass Unternehmen aus dem Bereich Information und Kommunikation oft auch beratend tätig sind. In beiden Branchen sind als häufigste Angebotsformen die Softwareangebote, konzeptionellen sowie beratenden Dienstleistungen verzeichnet.

Produktangebote wirtschaftlicher Akteure und Initiativen

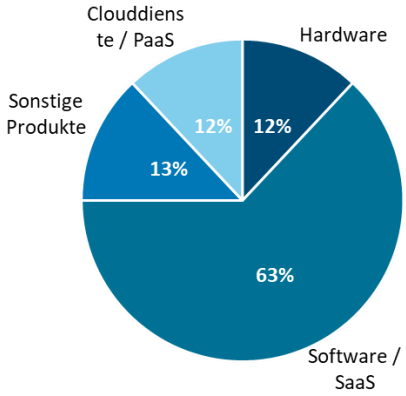


Abbildung 14 Produktangebote wirtschaftlicher Akteure und Initiativen. Quelle: BMI

Dieses Angebot zeigt insbesondere die offenbar vorhandene Nachfrage nach konzeptioneller und beratender Tätigkeit bezüglich Cybersicherheit, aber auch den konkreten Lösungsbedarf, dem bspw. durch Softwarelösungen begegnet wird.

Bei einer Analyse der Zusammenhänge zwischen diesen drei Angebotsformen Beratung, Konzeption und Software zeigt sich, dass das Portfolio von rund 41 % der wirtschaftlichen Akteure und Initiativen, die Softwareprodukte anbieten, auch Beratungsdienstleistungen umfasst. Aus der Perspektive der konzeptionellen Dienstleistungen bieten immerhin 38 % der Akteure und Initiativen auch Software an.

Angebote wirtschaftlicher Akteure aus den Themenbereichen „Bildung und Awareness“ sowie „Vernetzung“

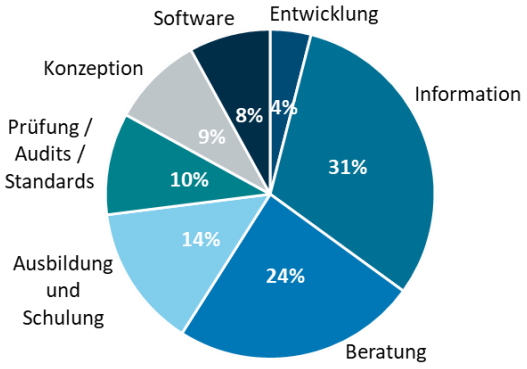


Abbildung 15 Angebote wirtschaftlicher Akteure aus den Themenbereichen „Bildung und Awareness“ sowie „Vernetzung“. Quelle: BMI

Hinsichtlich der Angebotsstruktur lässt sich weiterhin feststellen, dass Unternehmen, deren Cybersicherheits-Aktivitäten in den Bereichen „Netzwerk- und Multiplikatorfunktion“ oder „Bildung und Awareness“ liegen, überwiegend Informationsangebote und beratende Dienstleistungen anbieten. Bei beiden Schwerpunktkategorien stellen Ausbildungs- und Schulungsangebote jeweils das drittgrößte Angebotsfeld dar.

Angebote wirtschaftlicher Akteure aus den Themenbereichen „Konzeption und Vorgehensweisen“ sowie „Betrieb“

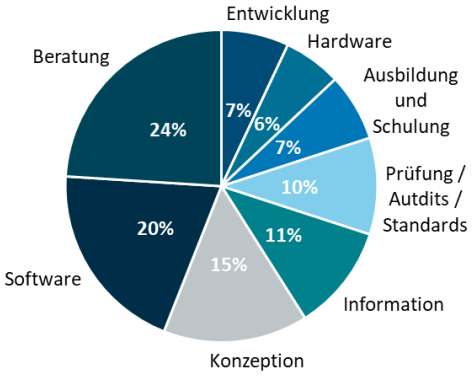


Abbildung 16 Angebote wirtschaftlicher Akteure aus den Themenbereichen „Konzeption und Vorgehensweisen“ sowie „Betrieb“. Quelle: BMI

Das Portfolio von Unternehmen, welche sich vorrangig mit den Cyberthemen „Betrieb“, „Detektion und Reaktion“ sowie „Konzeption und Vorgehensweisen“ beschäftigen, ist deutlich von Dienstleistungen sowie Softwareangeboten geprägt.

5.2 Schwerpunktthema: Fachkräfte und Frauenförderung

Insbesondere in der Informationstechnologie verzeichnet Deutschland einen hohen Bedarf an Fachkräften mit IT-Ausbildung, Akademiker sowie Akademikerinnen aus dem Bereich Cybersicherheit und IT. Der Bedarf an IT-Personal für Cybersicherheitsthemen ist proportional höher und steigt stärker als in anderen IT-Bereichen. Der Anteil von Frauen in der IT-Branche ist in Deutschland allerdings nach wie vor gering. Speziell im Bereich Cybersicherheit dürfte der Frauenanteil sogar noch kleiner ausfallen. Laut einer Umfrage des Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom) aus dem Jahr 2019 ist nur jede siebte Bewerberin auf eine IT-Position weiblich. Auch im Studiengang Informatik sind Frauen unterrepräsentiert. Weitere Studien zeigen, dass der Mangel an weiblichen Vorbildern in der Cybersicherheitsbranche dazu beiträgt, dass sich Frauen nicht für einen Berufsweg im Bereich Cybersicherheit entscheiden. Dies konnte bspw. auch im Rahmen der Multiplikatorengespräche bestätigt werden. 63% der Frauen denken positiver über die Branche, nachdem sie weibliche Personen kennengelernt haben, die in diesem Bereich arbeiten.

Es ist daher ein wichtiges Ziel, den Anteil von Frauen in Berufen im Bereich der Cybersicherheitsbranche zu erhöhen. Zum einen sollten junge Frauen motiviert werden, einen MINT-Beruf zu ergreifen, zum anderen müsste stärker sichergestellt werden, dass entsprechend ausgebildete Frauen im Bereich der Cybersicherheit auch attraktive Bedingungen und interessante Entwicklungs- und Zukunftsaussichten haben. Akteure sollten daher dafür sensibilisiert werden, dass in ihren Unternehmen geschlechterspezifische Vorurteile abgebaut werden und berufliche Möglichkeiten für Frauen in der Cybersicherheit aufgezeigt werden. Obwohl der Fachkräftemangel in IT-Berufen bekannt ist und das Bewusstsein dafür vorhanden ist, dass Frauen als Arbeitskräfte im IT-Bereich benötigt werden, werden Hemmnisse nicht genügend abgebaut. Die Recherche zum Nationalen Pakt Cybersicherheit hat ergeben, dass es im Bereich Cybersicherheit nur wenige Initiativen gibt, die das Thema Frauen und Cybersicherheit explizit aufgreifen (siehe hierzu z. B. den Steckbrief von „Serious Games“ Forschung an der TH Wildau).

Zwar gibt es bereits einige Initiativen in verwandten Themen- und Förderbereichen wie MINT-, Technik oder Informatik generell, der Bereich Cybersicherheit in der Frauenförderung ist jedoch noch nicht ausreichend stark in den Fokus gerückt. Dennoch wachsen die Möglichkeiten der akademischen Ausbildung von Fachkräften der Cybersicherheit stetig (siehe hierzu das Kapitel „Schwerpunktthema: Cybersicherheitslehre an Hochschulen“). In diesem Trend bestehen Chancen durch eine engere Vernetzung wirtschaftlicher, wissenschaftlicher und zivilgesellschaftlicher Akteure und Initiativen auf dem Gebiet der Frauenförderung.

5.3 Schwerpunktthema: Medien und Verbraucherinformation

Der freie Zugang zu Informationen zur Bildung eines eigenen Fachverständnisses und zum autodidaktischen Aufbau von Fähigkeiten ist einer der Grundpfeiler einer Demokratie. Verlage, Medienhäuser und Journalisten leisten hierbei einen wesentlichen Beitrag für mehr Cybersicherheit in Deutschland. Regionale und überregionale Zeitungen, Magazine und Blogs berichten regelmäßig u.a. über aktuelle Hackerangriffe, Sicherheitslücken oder andere Nachrichten aus dem Themenbereich Cybersicherheit. Jedoch haben sich auch Medien gänzlich auf Cybersicherheit spezialisiert und bieten ein breites Angebot an Fach- und Branchenjournalismus. Dies stellt auch einen wichtigen Mehrwert für Verbraucherinnen und Verbraucher da, da diese sich herstellerunabhängig informieren können.

In der nachstehenden Übersicht sind explizit nur Medien und Verbraucherinformationen mit ausschließlichem Fokus auf Cybersicherheit und verwandten Themen aufgeführt. Auch wenn einige der aufgeführten Informationsangebote wettbewerblich agieren, wurden diese mit Blick auf entsprechende frei verfügbare pro bono Angebote berücksichtigt.

AV-TEST GmbH *av-test.org*

Die AV-TEST GmbH hat sich als unabhängiges IT-Sicherheits-Institut auf qualitätssichernde Vergleichs- und Einzeltests international relevanter IT-Sicherheitsprodukte spezialisiert. AV TEST besitzt eine der weltweit größten Sammlungen von Schadsoftware zu Test- und Forschungszecken.
Außerdem werden die Sicherheit von eHealth- und IoT-Produkten, mobilen Anwendungen und der Datenschutz von Anwendungen sowie Dienstleistungen vom Institut erforscht. AV-TEST veröffentlicht aktuelle Produkttests und Forschungsergebnisse kostenlos auf der eigenen Webseite.

datenschutzticker.de *datenschutzticker.de*

datenschutzticker.de ist ein Blog zu Datenschutz und Datensicherheit und wird von der KINAST Rechtsanwaltsgesellschaft mbH betrieben. Auf der Webseite werden regelmäßig Beiträge zu aktuellen, relevanten Themen des Datenschutzes veröffentlicht. Zusätzlich findet im Jahr 2020 zum zweiten Mal eine Datenschutztagung statt, die eine Plattform zum Austausch zwischen Behörden und Wirtschaft bietet.

datensicherheit.de *datensicherheit.de*

Das Online Portal Datensicherheit.de bietet ein Informations- und Schulungsangebot zu vielfältigen Bereichen der Datensicherheit im privaten, beruflichen, geschäftlichen und behördlichen Umfeld. Getragen wird das Portal von der PINNOW & Partner Unternehmens- und Technologieberatungs-gesellschaft mbH.

Golem Media GmbH *golem.de*

Golem Media stellt mit Golem.de eine tagesaktuelle Newsplattform für IT-Themen zur Verfügung und berichtet über alle wesentlichen Neuerungen im IT-Bereich, darunter auch Themen aus dem Bereich Informationssicherheit und Datenschutz. Golem.de berichtet unter dem Schwerpunktthema "Security" über Sicherheitslücken, 0-Days, Angriffsmethoden, Malware und Ransomware und bietet Hintergrundinformationen über Sicherheitsaspekte wie Verschlüsselung, Selbstdatenschutz, Produkttests, aktuelle Updates, Antivirusprodukte, Patches und Entwicklungen.

heise Security *heise.de/security*

Unter dem Schwerpunkt heise Security, einer fachspezifischen Themenseite von heise online, werden sämtliche Artikel des Medienanbieters aus dem Gebiet der IT-Sicherheit gebündelt und mehrmals täglich Beiträge zu aktuellen, relevanten Themen der Cybersicherheit (auch konkrete Warnmeldungen) veröffentlicht. Neben den Beiträgen auf der Webseite werden ein Newsletter, ein Forum sowie verschiedene frei verfügbare Sicherheitschecks angeboten.

identitätsdiebstahl.info *identitaetsdiebstahl.info*

Aufgrund eigener Erfahrung als Opfer von Identitätsdiebstahl im Jahr 2009 ist die Betreiberin seit 2010 als Aktivistin im Bereich Cybersicherheit und Internetkriminalität tätig. In Zusammenarbeit mit einer Rechtsanwaltskanzlei bietet sie Schulungen und Vorträge, u.a. auf Fachtagungen, zu diesem Thema an. Die Domain informiert umfassend über Schutzmaßnahmen und Erste-Hilfe-Maßnahmen als Betroffene oder Betroffener von Identitätsdiebstahl.

Info-Point-Security GmbH *infopoint-security.de*

Infopoint Security ist eine umfassende Fachinformationsplattform zu Themen der IT-Sicherheit. Dabei werden u.a. Nachrichten, Alerts, Analysen und Studien und weitere Beiträge zu innovativen Technologien rund um IT-Sicherheit generiert. Die Plattform bietet auch Expertinnen und Experten die Möglichkeit, Einschätzungen, Bewertungen und Meinungen zu aktuellen Security-Themen zu veröffentlichen.

Kompass Sicherheitsstandards *kompass-sicherheitsstandards.de*

Das Informationsportal "Kompass Informationssicherheit und Datenschutz" von Bitkom und dem deutschen Institut für Normung (DIN) richtet sich als Informationsplattform an alle Gesellschaftsbereiche. Der Kompass Informationssicherheit und Datenschutz klassifiziert einschlägige Standards, sodass Leserinnen und Leser diese für ihre Rolle im Unternehmen bewerten und gegebenenfalls als relevant einschätzen können. Es werden ausgewählte Vorschriften und Gesetze aufgeführt, die im Zusammenhang mit IT-Sicherheit in Medien und Publikationen Erwähnung finden. Die Plattform bietet Nutzerinnen und Nutzern Erläuterungen und Informationen zu den aufgeführten Standards und Vorschriften. Standards spielen im Rahmen des IT-Risikomanagements eine signifikante Rolle. Durch die Informationen der Plattform wird der Einsatz von IT-Sicherheitsstandards für sicherheitsrelevante IT-Prozesse machbarer und transparenter und das Gesamtrisiko somit insgesamt reduziert.

netzpolitik.org e. V. *netzpolitik.org*

Netzpolitik.org ist ein Blog, der zu verschiedenen Fragestellungen im Bereich Internet, Politik und digitale Freiheiten berichtet. Das journalistische Angebot wird durch Spenden finanziert und umfasst Dossiers, Recherchen, einen Podcast sowie weitere Artikel. In den Beiträgen werden unter anderem aktuelle Trends und relevante Themen der IT-Sicherheit kritisch reflektiert und analysiert. Im Fokus der Betrachtung steht die Veränderung des Internets durch politische Regulierung sowie die Veränderung der Politik durch das Netz.

SecuPedia - Die Plattform für Sicherheits-Informationen *secupedia.info*

SecuPedia ist eine Plattform zur Bündelung sämtlicher Informationen rund um die Themen Sicherheit und IT-Sicherheit. Aufgebaut ist die Plattform als Wiki, bei dem jeder Nutzer Inhalte einfügen oder ergänzen kann, die jedoch redaktionell überprüft werden.

Security Insider *security-insider.de*

Security-Insider bietet für IT-Security Professionals Informationen zu aktuellen Bedrohungsmechanismen, erkannten Schwachstellen und Software-Updates. Ebenso werden Whitepaper, Webcasts, Downloads und Fallstudien sowie eine umfangreiche IT-Security-Anbieter- und -Produktdatenbank über security-insider.de zur Verfügung gestellt. Die Plattform bietet ebenfalls Community-Funktionen wie Foren und Expertenblogs zu IT-Sicherheitsthemen.

Sichere Industrie *sichere-industrie.de*

Die "Sichere Industrie" ist ein Projekt der bluecept GmbH und stellt als offene Wissensplattform Tipps und Hilfestellungen zur Industrial Security für Betreiber von Anlagen- und Automatisierungsnetzen zur Verfügung. Autorinnen und Autoren der Plattform sind Expertinnen und Experten aus der IT-Sicherheit, der Automatisierung und der Elektrotechnik. Neben auf der Webseite veröffentlichten Artikeln werden auch Workshops angeboten.

Sicherheit.info *sicherheit.info*

Sicherheit.info ist das Online-Portal der Fachzeitschrift Protector, einer Zeitschrift zu den Themen Sicherheitstechnik und Wirtschaftsschutz. Auch zum Thema IT-Sicherheit veröffentlicht das Portal regelmäßig Beiträge. Neben dem Online-Portal werden ein Newsletter sowie eine Printausgabe des Magazins angeboten.

Verbraucherzentralen *Zivilgesellschaftlicher Akteur*

Die Verbraucherzentralen bieten persönliche Beratungen für Verbraucherinnen und Verbraucher, die von IT-Sicherheitsvorfällen betroffen sind, und nehmen Meldungen über Gefahren im Cyberraum entgegen. Über ihre digitalen Angebote engagieren sie sich aber auch im Bereich der digitalen Bildung und Prävention. So klärt bspw. das Projekt „Phishingradar“ über Risiken in Zusammenhang mit E-Mails auf. Die Verbraucherzentralen und ihr Bundesverband bieten Schulen verschiedene Angebote an, damit sich Kinder und Jugendliche sicher im Netz bewegen können. Im Materialkompass auf verbraucherbildung.de finden Lehrkräfte Lehr- und Lernmaterialien von verschiedenen Anbietern, die von unabhängigen Experten qualitätsgeprüft wurden.

6 Cybersicherheit auf staatlicher Ebene

6.1 Allgemeiner Überblick

Akteure und Initiativen des Staates sind Behörden und Einrichtungen des Bundes (48%), der Länder (40%) und auf kommunaler Ebene (12%).

Staatliche Akteure und Initiativen sind vor allem in der Schaffung von Netzwerken (36%) sowie allgemeiner Sensibilisierung und Awareness für Cybersicherheitsthemen (31%) aktiv. Durch gezielte Förderungen, Kommunikationsmaßnahmen und das Zusammenbringen von Stakeholdern mit Schlüsselfunktionen nimmt der Staat eine allgemeine Rolle als Multiplikator ein. Dabei liefert er über seine diversen Organe auf allen Ebenen auch konkrete Handlungsempfehlungen und Hilfestellungen zum sicheren Umgang mit IKT (11%). Weitere, schwerpunktmäßig technische Themen, wie der sichere Betrieb von IKT, die Detektion von und Reaktion auf sicherheitsrelevante Ereignisse, infrastrukturelle Aspekte der Cybersicherheit, der Aufbau sicherer Kommunikationsnetze sowie die Sicherheit im Internet der Dinge stellen zusammengenommen zwar wichtige Kernthemen des öffentlichen Sektors dar (zusammen 22%), werden jedoch seltener öffentlich und nach außen gerichtet kommuniziert. Die Zielgruppe dieser Themen ist oft spezialisierte Experten.

Der Staat adressiert mit seinen Themen relativ gleichgewichtig alle Gesellschaftsgruppen. Lediglich die Wirtschaft sticht als Zielgruppe mit 39% etwas hervor. Dies ist durch die Schlüsselrolle der Wirtschaft zu erklären. Initiativen, die mit staatlichen Mitteln gefördert werden, richten sich zum überwiegenden Teil an kleine und mittelständische Unternehmen (KMU) mit dem Ziel der Sensibilisierung für Cybersicherheitsthemen und dem Initiieren von Verbundprojekten, damit Teilnehmer vom gegenseitigen Austausch und Best-Practice-Erfahrungen profitieren. Angebote für den Mittelstand zielen darauf ab, geeignete Informationsformate, Demonstrationsmöglichkeiten und Förderangebote zur Verfügung zu stellen, um Unternehmen beim Prozess der Digitalisierung im Sinne der größtmöglichen IT-Sicherheit zu unterstützen. Weitere prominente Initiativen, die von der öffentlichen Hand gefördert werden, richten sich an Verbraucherinnen und Verbraucher sowie Bürgerinnen und Bürger mit dem Ziel der Sensibilisierung im Hinblick auf die Bedeutung von IT-Sicherheitsmaßnahmen und den gezielten Aufbau von Medienkompetenz. Auch die Forschungsförderung spielt auf staatlicher Ebene eine große Rolle. Es existieren zahlreiche Fördermaßnahmen und Förderrichtlinien.

So wurden und werden allein seit 2009 über 175 Projekte im Bereich Kommunikation und Sicherheit digitaler Systeme auf Bundesebene gefördert.

Das Zusammenspiel aus behandelten Themen der Cybersicherheit und zielgruppenspezifischer Ausrichtung spiegelt sich im Angebot staatlicher Akteure und Initiativen wider. Allgemein als Dienstleistungen angesehene Angebote, wie Beratung, Ausbildung und Schulungen sowie konzeptionelle Hilfestellungen (47%) sind ähnlich weit verbreitet wie aufbereitete und veröffentlichte Informationen zur Cybersicherheit (46%). Seltener ist hingegen das konkrete Angebot von Produkten wie Soft- und Hardware, Clouddienste etc. (7%).

6.2 Handlungsfelder, Ziele und Rechtsgrundlagen von Bund und Ländern

Bund und Länder unterscheiden sich bzgl. der Akteure, Initiativen und Handlungsfelder, die sich mit Cybersicherheitsthemen befassen. Sie behandeln das Thema Digitalisierung und die damit einhergehenden Maßnahmen zu Cybersicherheit unterschiedlich intensiv. Manche Länder benennen Digitalisierung und Cybersicherheit als Standortvorteil und informieren aktiv über Akteure sowie Maßnahmen und Fördermöglichkeiten der öffentlichen Hand. Es gibt Bundesländer, die sich im Bereich der Cybersicherheit aufgrund regionaler Anforderungen spezialisieren. Z.B. betreibt das Land Bremen das Thema „IT-Sicherheit in der maritimen Branche (Portsecurity/Hafensicherheit)“. Das Land Hessen hingegen engagiert sich besonders in der Förderung und Ansiedlung von Ausgründungen aus Forschungsprojekten vor Ort.

Es gibt nur einige bundesweit einheitliche Strukturen, bspw. die Zentralen Ansprechstellen Cybercrime (ZAC) der Polizeien, die CERT-Einrichtungen jedes Bundeslandes oder die Kooperationen mit dem BSI in Cybersicherheitsthemen. Unterschiede ergeben sich ebenso darin, wie oder von welcher Stelle die Verantwortung für Cybersicherheitsthemen in Bund und Ländern wahrgenommen und getrieben wird (z.B. Digitalministerium, Innenressort, Wirtschaftsressort).

Die **Handlungsfelder, Maßnahmen und Ziele für Cybersicherheitsthemen** sind für Bund und Länder unterschiedlich verankert. Informationen bieten folgende Strategien, Vorhaben und Rechtsgrundlagen:

- **BSI-Gesetz:** Mit dem Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes, das am 1. Januar 1991 in Kraft getreten ist, wurde der Grundstein für das noch heute geltende BSI-Gesetz gelegt. Um die neuen Bedrohungen der Cybersicherheit zu bekämpfen und der zunehmenden Bedeutung der Informations- und Kommunikationstechnologie Rechnung zu tragen, wurden dem BSI mit dem Gesetz weitergehende Aufgaben und Befugnisse eingeräumt. Nach zwischenzeitlich nur kleineren Änderungen im Gebührenrecht, wurde das BSI-Gesetz mit dem am 25.07.2015 in Kraft getretenen Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) das erste Mal in größerem Umfang ergänzt. Mit dem IT-Sicherheitsgesetz wurden vor allem wesentliche Regelungen KRITIS-Betreiber in das BSI-Gesetz aufgenommen, welche analog auch im Energiewirtschaftsgesetz (EnWG), Telekommunikationsgesetz (TKG) sowie im Fünften Buch Sozialgesetzbuch (SGB V) nachvollzogen wurden. Um Anforderungen im Bereich der IT-Sicherheit insbesondere auch außerhalb der Bundesverwaltung gerecht zu werden, wurde das BSI durch die Ergänzungen mit neuen Aufgaben und Befugnissen ausgestattet.
- **NIS-Richtlinie:** Mit der im August 2016 in Kraft getreten europäischen Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie) wurden Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der europäischen Union definiert. Es wurde ein einheitlicher Rechtsrahmen für den EU-weiten Aufbau nationaler Kapazitäten für die Cybersicherheit, eine stärkere Zusammenarbeit der Mitgliedstaaten der Europäischen Union sowie Mindestsicherheitsanforderungen an und Meldepflichten für Kritische Infrastrukturen, sowie für bestimmte Anbieter digitaler Dienste wie Cloud-Services und Online-Marktplätze geschaffen. Die NIS-Richtlinie ist damit ein wichtiger Schritt für mehr Cybersicherheit in Europa. Die Richtlinie musste von den Mitgliedstaaten der europäischen Union in nationales Recht umgesetzt werden. Mit dem am 29.06.2017 verkündeten Umsetzungsgesetz hat der deutsche Gesetzgeber dies getan. Dabei war die Ausgangsposition hierfür denkbar gut: In Deutschland existierte wie bereits dargestellt seit Juli 2015 mit dem IT-Sicherheitsgesetz bereits ein einheitlicher Rechtsrahmen für die Zusammenarbeit von Staat und Unternehmen für mehr Cybersicherheit bei den Kritischen Infrastrukturen. Völlig neu zu schaffen waren in Deutschland nur noch Regelungen für Anbieter Digitaler Dienste. Diese fanden ab dem 10.05.2018 Anwendung. Das Gesetz zur Umsetzung der NIS-Richtlinie erweiterte die Aufsichts- und Durchsetzungsbefugnisse des BSI gegenüber KRITIS-Betreibern – eine wichtige Voraussetzung, um die Cybersicherheit in Deutschland weiter zu verbessern. Über die reine Umsetzung der NIS-Richtlinie hinaus wird zudem mit dem Umsetzungsgesetz die Zusammenarbeit zwischen den Bundesländern und dem BSI gestärkt. Das BSI hat so die Möglichkeit, Länder noch umfassender zu unterstützen und ihnen seine technische Expertise zur Verfügung zu stellen.
- **Onlinezugangsgesetz (OZG):** Die Interaktion zwischen Bürgerinnen, Bürgern und Unternehmen mit der Verwaltung soll in Zukunft deutlich schneller, effizienter und nutzerfreundlicher werden. Das Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz – OZG) verpflichtet daher Bund und Länder (einschließlich Kommunen), bis Ende 2022 grundsätzlich alle Verwaltungsleistungen über Verwaltungsportale auch digital anzubieten. Im sogenannten OZG-Umsetzungskatalog sind die OZG-Leistungen in 35 Lebens- und 17 Unternehmenslagen gebündelt und 14 übergeordneten Themenfeldern (z.B. "Familie & Kind" und "Unternehmensführung & -entwicklung") zugeordnet. Der OZG-Umsetzungskatalog orientiert sich dabei nicht an behördlichen Zuständigkeiten, sondern an der Nutzerperspektive von Bürgerinnen und Bürgern sowie Unternehmen. Die OZG-Leistungen werden im Rahmen von zwei Digitalisierungsprogrammen online umgesetzt. Im „Digitalisierungsprogramm Bund“ werden alle Leistungen mit Regelungs- und Vollzugskompetenz beim Bund themenfeldübergreifend und in Verantwortung des Bundes digitalisiert. Die Leistungen mit Regelungs- und/oder Vollzugskompetenz bei den Bundesländern bzw. Kommunen werden im „Digitalisierungsprogramm Föderal“ digitalisiert. Für das Digitalisierungsprogramm Föderal haben der Bund und die Länder ein arbeitsteiliges Vorgehen (Ressort-Land-Tandem je Themenfeld) etabliert. Länder, die die Federführung für ein bestimmtes Themenfeld übernommen haben, erarbeiten digitale Lösungen für die hierin enthaltenen OZG-Leistungen mit Unterstützung des federführenden Bundesressorts. Dem arbeitsteiligen Prinzip folgend, werden die Ergebnisse (u.a. Daten des Föderalen Informationsmanagements (FIM)) den anderen Bundesländern zur Nachnutzung bereitgestellt, sodass eine flächendeckende Verfügbarkeit erreicht werden kann – dieses Prinzip nennt sich

„Einer für Alle“. Grundlegend für die Umsetzung des OZG ist der Aufbau des Portalverbunds.

- **Cyber-Sicherheitsstrategie für Deutschland:** Die Bundesregierung hat am 9. November 2016 die vom Bundesminister des Innern vorgelegte "Cyber-Sicherheitsstrategie für Deutschland 2016" beschlossen. Sie schreibt die Cyber-Sicherheitsstrategie aus dem Jahr 2011 fort. Die "Cyber-Sicherheitsstrategie für Deutschland 2016" sieht über 30 strategische Ziele und Maßnahmen zur Verbesserung der Cybersicherheit vor. Dazu gehört unter anderem die Einführung eines IT-Sicherheitskennzeichens, um Cybersicherheit für Anwender transparent zu machen, die Ausweitung der Kooperation zwischen Staat und Wirtschaft sowie die Schaffung von "Mobilen Einsatzteams" für die Unterstützung vor Ort. Die Cybersicherheitsstrategie befindet sich aktuell in einem Evaluierungs- und Fortschreibungsprozess.
- **Digitalstrategien der Länder:** Aufgrund der föderalen Organisation steuern die Länder im Rahmen der Digitalisierung der Wirtschaft Maßnahmen über eigene Digitalisierungsleitlinien, Informationssicherheitsrichtlinien, Vorschriften und Umsetzungsverordnungen. Die Themenbereiche „Digitalisierung“ und „IT-Sicherheit“ sind in den Ländern unterschiedlich verortet: z.B. im Ministerium für Wirtschaft, im Ministerium des Innern oder in Digitalministerien.
- **Koalitionsverträge von Bund und Ländern** enthalten ebenfalls Maßnahmen aus dem Themenbereich IT-Sicherheit.

Die **Digitalstrategien von Bund und Ländern** haben für die Regierungen unterschiedliche Bedeutungen, Handlungsfelder sind ähnlich bzw. gleich:

- **Handlungsfeld „Anwendungen“**, z.B.:
  - E-Government: durch digitalisierte Dienstleistungen für Unternehmen und Bürgerinnen und Bürger die Verwaltung näher, schneller und effizienter zu machen sowie die Verwaltung nach außen zu öffnen.
  - Digitalisierung der Verwaltung: Optimierung der verwaltungsinternen Prozesse durch Digitalisierung.
  - Digitalisierung der Bildung: Digitalisierung der Schulausbildung und dualen Berufsbildung.
- **Handlungsfeld „Technologie“**, z.B.:
  - IT-Sicherheit: Förderung von Präventionstechnologien zur Bekämpfung von Cyberkriminalität.
  - Breitbandausbau: Förderung flächendeckender, breitbandiger und leistungsfähiger Zugangsnetze.
  - Rechenzentren: Ausbau leistungsfähiger Rechenzentren und nachhaltiger Rechenzentrumstechnologien, Förderung von Maßnahmen zur IT-Sicherheit in Rechenzentren und Unterstützung der Vernetzung.
- **Handlungsfeld „Gestaltung“**, z.B.:
  - Bildungswesen: Digitales Wissen in der Hochschulausbildung vermitteln sowie Digitale Kompetenz in der Schulausbildung verankern.
  - Verbraucherinnen und Verbraucher: Datenschutz und die Rechte auf Transparenz der Verbraucherinnen und Verbraucher müssen bei der Teilnahme an digitalen Angeboten gewahrt bleiben. Öffentliche Einrichtungen müssen bzgl. Datenschutz und IT-Sicherheit beraten, informieren, und Kompetenzen bilden.
  - Telekommunikation und Regulierung: Förderung des Wettbewerbs und Schaffung eines einheitlichen Rechtsrahmens für funktional gleiche Dienste.
  - Wissenschaftsförderung: Aufbau digitaler Infrastrukturen, Förderung von Cyber-Forschungsprojekten und Förderung von Gründungsprojekten aus dem universitären Umfeld.
  - Wirtschaftsförderung: Finanzierungs- und Fördermaßnahmen, Transfer- und Netzwerkmaßnahmen, Beratungsleistungen und Clustermanagement.

6.3 Schwerpunktthema: Behörden, Einrichtungen und Initiativen des Bundes

Der Bund mit seinen Institutionen nimmt für die Cybersicherheit in Deutschland eine zentrale und richtungsgebende Funktion ein. Daher bietet die nachfolgende Übersicht, ergänzend zu den Steckbriefen staatlicher Cybersicherheitsakteure und -initiativen, einen Überblick über Stakeholder, die eine bedeutende Rolle für die Cybersicherheit in Deutschland einnehmen.

Bundesregierung *bundesregierung.de*

Digitalisierung umfasst alle Lebensbereiche und demzufolge sind sämtliche Ressorts der Bundesregierung in abgestufter Weise mit Fragen der Digitalisierung beschäftigt. Im Jahr 2018 wurde im Bundeskanzleramt das Amt der Beauftragten der Bundesregierung für Digitalisierung geschaffen.

Der **Kabinettausschuss-Digitalisierung (Digitalkabinett)** ist das zentrale Steuerungsgremium für digitalpolitische Fragen auf höchster politischer Ebene. Im Mittelpunkt stehen die Fragestellungen, was Digitalisierung dem Einzelnen bringt und wie die Werte unserer freiheitlich demokratischen Grundordnung im digitalen Zeitalter erhalten und gestärkt werden können.

6.3.1 Behörden und Einrichtungen des Bundes

Agentur für Innovation in der Cybersicherheit GmbH (Cyberagentur)

Die Cyberagentur ist eine Inhouse-Gesellschaft des Bundes. Die Bundesrepublik Deutschland als Alleingesellschafterin wird durch das BMVg und das BMI gemeinsam vertreten. Die Cyberagentur soll Forschung sowie bahnbrechende und zukunftsgestaltende Innovationen im Bereich der Cybersicherheit und diesbezüglicher Schlüsseltechnologien im Bereich der Inneren und Äußeren Sicherheit anwendungsbezogen vorantreiben, und so einen Beitrag zur Sicherstellung der Technologiesouveränität Deutschland im Cyber- und Informationsraum leisten. Dabei forscht die Cyberagentur nicht selbst, sondern vergibt gezielt Aufträge zu ambitionierten Forschungsvorhaben mit hohem Innovationspotenzial. Die Cyberagentur wurde im Koalitionsvertrag 2018 vereinbart und bettet sich in die Hightech-Strategie 2025 der Bundesregierung ein. Der Gründungsprozess der Agentur konnte im August 2020 abgeschlossen werden. Die Aufstellung der Cyberagentur erfolgte am Standort Halle (Saale).

Beauftragter der Bundesregierung für Informationstechnik (BfIT) *cio.bund.de*

Der Beauftragte der Bunderegierung für Informationstechnik (BfIT) führt den Nationalen Cyber-Sicherheitsrat und ist zentraler Ansprechpartner für Länder und Wirtschaft bei der Zusammenarbeit mit der Bundesregierung in IT-Fragen. Er verantwortet fachlich und politisch die operative Steuerung der Informationstechnik und Digitalisierung der Bundesverwaltung. Die wichtigste Aufgabe des IT-Beauftragten der Bundesregierung ist es, für eine moderne und sichere IT-Landschaft des Bundes und die Herausforderungen des Digitalen Wandels die entscheidenden Bedingungen zu schaffen.

Bundesamt für Sicherheit in der Informationstechnik (BSI) *bsi.bund.de*

Das BSI stellt als Behörde eine unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit in der Informationsgesellschaft für Gesellschaft, Wirtschaft und Staat dar. Das BSI untersucht und bewertet bestehende Sicherheitsrisiken und bietet seinen Kunden Dienstleistungen in den Kernbereichen Information, Beratung, Entwicklung und Zertifizierung an.

Als Unterstützung für Unternehmen und Behörden stellt das BSI ein mobiles Einsatzteam (Mobile Incident Response Team MIRT), das bei IT-Sicherheitsvorfällen vor-Ort unterstützt.
Das BSI erstellt den Lagebericht IT-Sicherheit in Deutschland, der die aktuelle IT-Sicherheitslage unter Bezugnahme konkreter Vorfälle einschließlich einer Beschreibung der Methoden und Mittel der Angreifer analysiert. Es werden konkrete Lösungsansätze zur Verbesserung der IT-Sicherheit in Deutschland sowie Angebote und Maßnahmen des BSI dargestellt. Hierbei wird auf die Adressaten Gesellschaft, Wirtschaft, Staat und Internationales näher eingegangen. Der Lagebericht IT-Sicherheit wird vom BSI online veröffentlicht.

Zusätzliche und detailliertere Informationen können auch dem Steckbrief des BSI entnommen werden.

BSI-Verbindungsbüros

Das BSI als nationale Cybersicherheitsbehörde kann gem. § 3 BSIG die Länder in Fragen der Informationssicherheit beraten und warnen, sowie auf deren Ersuchen bei der Sicherung ihrer Informationstechnik und Abwehr von Gefahren unterstützen. Übergeordnetes Ziel der Bund-Länder-Zusammenarbeit ist es, ein einheitlich hohes IT-Sicherheitsniveau zu schaffen. Angesichts der fortschreitenden Digitalisierung der Verwaltung und einer zunehmenden Vernetzung von IT-Strukturen zwischen Bund und Ländern kommt diesem Ziel eine immer größer werdende Bedeutung zu. Das BSI schließt dazu Kooperationsvereinbarungen mit Ländern auf deren Wunsch. Ziel ist die Stärkung der Zusammenarbeit im Bereich der Informationssicherheit, wobei die Schwerpunkte und Unterstützungsleistungen durch das BSI individuell und bedarfsgerecht angepasst werden. Das Nationale Verbindungswesen des BSI gestaltet darüber hinaus die Beziehungen des BSI zu regionalen Partnern in den Bereichen Gesellschaft, Wirtschaft und Staat in ganz Deutschland und steht als erster Ansprechpartner auf regionaler Ebene für die Bundesländer zur Verfügung. Dazu wurden regionale Verbindungsbüros eingerichtet. Über die Verbindungsbüros wird der Kontakt zu Behörden, Unternehmen, Verbänden, Thinktanks sowie internationalen Organisationen mit Sitz in Deutschland gehalten. Bundesweit existieren fünf Verbindungsbüros (Nord/Hamburg, Ost/Berlin, Rhein-Main, West und Süd/Stuttgart). Diese ermöglichen den Ländern einen schnellen und direkten Zugang zu den Dienstleistungen und Angeboten des BSI, so dass sie vor Ort profitieren können und die Digitalisierung sicher umsetzen können.

Nationales IT-Lagezentrum *bsi.bund.de*

Das Nationale IT-Lagezentrum hat im Rahmen der drei strategischen Ziele Prävention, Detektion und Reaktion folgende Aufgaben:
- Erkennen, Erfassen und Bewerten von Vorfällen,
- Informieren, Alarmieren und Warnen,
- Reagieren bei IT-Sicherheitsvorfällen.

Daraus leiten sich für das Nationale IT-Lagezentrum der Auftrag ab, jederzeit über ein verlässliches Bild der aktuellen IT-Sicherheitslage in Deutschland zu verfügen sowie den Handlungsbedarf und die Handlungsoptionen bei IT-Sicherheitsvorfällen sowohl auf staatlicher Ebene als auch in der Wirtschaft schnell und kompetent einschätzen zu können. Das Nationale IT-Lagezentrum ist zudem organisatorisch und technisch darauf vorbereitet, zum IT-Krisenreaktionszentrum aufzuwachsen.
Das Nationale IT-Lagezentrum hält vorrangig über die Beziehungen von CERT-Bund enge Kontakte zu nationalen und internationalen Partnern. Es stellt dem Nationalen Cyber-Abwehrzentrum Lageberichte, Hintergrundinformationen zu IT-Sicherheitsvorfällen und Schwachstelleninformationen/-warnungen zur Verfügung.

Computer Emergency Response Team der Bundesverwaltung (CERT-Bund) *cert-bund.de*

Das Computer Emergency Response Team der Bundesverwaltung (CERT-Bund) ist dem BSI angegliedert und hat das Ziel, als zentrale Anlaufstelle für präventive und reaktive Maßnahmen mit Bezug auf sicherheits- und verfügbarkeitsrelevante Vorfälle in Computersystemen zu wirken. Zu den Hauptaufgaben von CERT-Bund zählen das Erstellen und Veröffentlichen von präventiven Handlungsempfehlungen zur Schadensvermeidung, das Hinweisen auf Schwachstellen in Hardware- und Softwareprodukten und das Vorschlagen von Maßnahmen zur Behebung von bekannten Sicherheitslücken. Das CERT-Bund warnt und alarmiert bei besonderen Bedrohungslagen (bezogen auf Informationstechnik) und empfiehlt reaktive Maßnahmen zur Schadensbegrenzung oder -beseitigung. Die Dienstleistungen von CERT-Bund stehen in erster Linie den Bundesbehörden zur Verfügung.

Das CERT-Bund betreibt in Zusammenarbeit mit den CERT-Einrichtungen der Länder den Verwaltungs-CERT-Verbund (VCV), der eine Informationsaustauschplattform der CERTs der öffentlichen Verwaltung in Deutschland darstellt. Im Rahmen des VCV sollen so die Verwaltungen entsprechende Informationen und Lösungswege austauschen, um effektiver und schneller auf IT-Angriffe reagieren zu können. Mit einem föderalen, verwaltungsinternen Warn- und Informationsdienst soll eine Verbesserung des Informationsaustausches der bestehenden CERTs des Bundes und der Länder erreicht werden.

Das BSI bietet ebenfalls ein Bürger-CERT an, welches Bürgerinnen und Bürger sowie kleine Unternehmen schnell und kompetent vor Viren, Würmern und anderen Sicherheitslücken warnt. Über das Bürger-CERT werden Empfehlungen zu Maßnahmen ausgegeben, um Bürgerinnen und Bürgern sowie kleinen Unternehmen zu helfen, gegen IT-Sicherheitsvorfälle geschützt zu sein. Ebenso ist das Bürger-CERT die geeignete Anlaufstelle, um einen Sicherheitsvorfall zu melden, sich beraten zu lassen und Verständnisfragen zu stellen. Die Dienstleistung durch das Bürger-CERT erfolgt kostenfrei und neutral. Mit BSI-fuer-Buerger.de wird ein Informationsportal für IT-Sicherheitsthemen zur Verfügung gestellt, um Sicherheitshinweise zu streuen und ein Bewusstsein für die Sicherheitslage im Internet zu schaffen.

Militärischer Abschirmdienst (MAD)

Der MAD nimmt als abwehrender Nachrichtendienst im Geschäftsbereich (GB) des Bundesministeriums der Verteidigung (BMVg) die Aufgaben einer Verfassungsschutzbehörde wahr. Er ist einer der drei Nachrichtendienste des Bundes. Den durch den MAD zu erfüllenden gesetzlichen Abschirmauftrag für den GB BMVg nimmt im Cyber- und Informationsraum (CIR) die Cyberabschirmung des MAD wahr. Sie umfasst alle operativen, reaktiven, aber auch präventiven Maßnahmen des MAD zur Abwehr von nachrichtendienstlichen sowie sicherheitsgefährdenden Tätigkeiten oder extremistischen/ terroristischen Bestrebungen im CIR. Die Cyberabschirmung des MAD trägt damit wesentlich zum Schutz der Dienststellen des GB BMVg im CIR bei. Der MAD ist mit dem Bereich der Cyberabschirmung als Kernbehörde am Nationalen Cyber-Abwehrzentrum vertreten.

Bundesamt für Verfassungsschutz (BfV) *verfassungsschutz.de*

Das BfV dient dem Schutz der inneren Sicherheit und informiert die Bundesregierung über die Sicherheitslage. Es ist zuständig für die Abwehr, einschließlich der Attribution, nachrichtendienstlich gesteuerter sowie extremistisch oder terroristisch motivierter Cyberangriffe. In den Cyber-Briefen berichtet der Verfassungsschutz über Cyberangriffe und gibt Handlungs-empfehlungen ab. Dieses Format, das auch online verfügbar ist, dient zur Unterrichtung von Behörden und Wirtschaftsunternehmen.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) *bbk.bund.de*

Das BBK als Bundesoberbehörde im Geschäftsbereich des BMI ist das zentrales Organisationselement für die Zivile Verteidigung, welches alle einschlägigen Aufgaben an einer Stelle bündelt. Zu seinen Aufgaben gehören u.a. Krisen- und Risikomanagement, Zivilschutz und der Schutz Kritischer Infrastrukturen. Letzteres umfasst auch den Schutz vor Gefahren des Cyberraumes für Kritische Infrastrukturen im Referat II 3, Themenbereich Cyber-Sicherheit KRITIS. Das BBK ist mit der Abteilung II auch im Nationalen Cyber-Abwehrzentrum vertreten.

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI) *bfdi.bund.de*

Zu den Aufgaben des BfDI gehören die Entwicklung datenschutzkonformer Lösungen und die Wahrung der Datenschutzrechte von Personen gegenüber der öffentlichen Verwaltung und Unternehmen. Der BfDI wird von der Bun-

desregierung vorgeschlagen und vom Deutschen Bundestag gewählt. Er ist in der Ausübung seines Amtes völlig unabhängig und nur dem Gesetz unterworfen. Der Bundesbeauftragte ist eine eigenständige und unabhängige oberste Bundesbehörde.

Bundeskriminalamt (BKA) *bka.de*

Das BKA ist ein wichtiger Baustein in der deutschen Sicherheitsarchitektur. In elf Abteilungen arbeiten über 7.000 Mitarbeiterinnen und Mitarbeiter, um den gesetzlichen Auftrag des BKA zu erfüllen.
Das BKA mit seiner im April 2020 neu geschaffenen Abteilung „Cybercrime (CC)" ist ein wesentlicher Bestandteil der Cyber-Sicherheitsarchitektur in Deutschland und gehört weltweit zu den führenden Dienststellen in diesem Phänomenbereich. Der Schwerpunkt liegt auf der Bekämpfung Cybercrime im engeren Sinne (C.i.e.S.). Hierunter werden solche Straftaten subsumiert, die sich gegen das Internet, weitere Datennetze, informationstechnische Systeme oder deren Daten richten. Die Abteilung führt Ermittlungen gegen im Cyberraum aktive Kriminelle und zerschlägt kriminelle Netzwerke und Strukturen, die für die Cyber-Angriffe auf herausgehobene Ziele in Deutschland verantwortlich sind. Sie stellt die Gewinnung, Aufbereitung und Analyse relevanter Informationen als Grundlage von Ermittlungen im Umfeld hochkomplexer Cybertechnologien durch die Polizeien des Bundes und der Länder sicher und unterbindet Cyber-Angriffe auf Bundeseinrichtungen und kritische Infrastrukturen in Deutschland. Die Abteilung berät die Amtsleitung des Bundeskriminalamtes bei kriminalpolitischen Themen im Zusammenhang mit der C.i.e.S. und gestaltet die Weiterentwicklung einschlägiger rechtlicher Bestimmungen z. B. durch Beratungsleistung aktiv mit.

Der Phänomenbereich der Cyber-Spionage wird im BKA in der Abteilung „Staatsschutz (ST)" bearbeitet. Angriffe staatlicher Akteure (insbesondere fremder Nachrichtendienste) erfolgen zumeist in Form von Advanced Persistent Threats (APT). Diese sind eine ernstzunehmende und weiterhin steigende Bedrohung für die Wirtschaft sowie für öffentliche und nicht-öffentliche Stellen und Institutionen. Dies gilt besonders für Unternehmen der KRITIS. Bei APT handelt es sich um zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer dauerhaften Zugriff zu einem Netzwerk verschafft und diesen in der Folge auf weitere Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten auf Seiten der Angreifer aus und sind in der Regel schwierig zu detektieren. Kennzeichnend für APT-Angriffe ist, dass sie sowohl zur Spionage, das heißt zum Ausspähen von Daten, als auch zur Sabotage, also zum Stören von Abläufen, genutzt werden. Cyberspionage gegen Deutschland hat sich als eine wichtige Methode der Informationsgewinnung für ausländische Nachrichtendienste etabliert. Weltweit werden bei Cyberspionage-Angriffen immer wieder dynamisch gestaltete Serverinfrastrukturen sowie hoch professionelle und einer steten Weiterentwicklung unterliegende Schadsoftwarekomponenten verwendet.

Bundesnachrichtendienst (BND) *bnd.bund.de*

Der BND, als deutscher Auslandsnachrichtendienst, hat die Befugnis und die technischen Möglichkeiten zur strategischen Erfassung internationaler Datenverkehre. Cyberangriffe, die sich im Ausland aufbauen und gegen kritische Infrastrukturen in Deutschland gerichtet sind, kann der BND frühzeitig erkennen, indem die Ausbreitung von Schadsoftware im Vorfeld eines Angriffs detektiert wird. Diese Informationen ermöglichen den Inlandsbehörden die Einleitung von Abwehrmaßnahmen, die den Schaden gefährlicher Software begrenzen können. Diese Vorgehensweise wird als „SIGINT Support to Cyber Defense" bezeichnet.

Bundespolizeipräsidium (BPOL) *bundespolizei.de*

Im Rahmen ihrer Aufgaben zur Kriminalitätsbekämpfung ist die Bundespolizei auch im Bereich der Cyber-Kriminalität tätig und dort im Verlauf von Festnahmen an der Beweissicherung beteiligt

Informationstechnik Zentrum Bund (ITZBund) *itzbund.de*

Das ITZBund ist der zentrale IT-Dienstleister der Bundesverwaltung und stellt dieser IT-Infrastruktur und IT-Lösungen zur Verfügung. Es ist im Wege der IT-Konsolidierung des Bundes am 1. Januar 2016 aus dem Zusammenschluss der Bundesstelle für Informationstechnik (Geschäftsbereich des BMI), der Bundesanstalt für IT-Dienstleistungen (Geschäftsbereich des Bundesministeriums für Verkehr und digitale Infrastruktur (BMVI)) und dem Zentrum für Informationsverarbeitung und Informationstechnik (Geschäftsbereich des Bundesministeriums der Finanzen (BMF)) hervorgegangen und wurde als Behörde im Geschäftsbereich des BMF gegründet.

Im Rahmen dieser IT-Konsolidierung des Bundes werden weitere IT-Infrastrukturen von Bundesbehörden zum ITZ-Bund migriert. Durch diese Konsolidierung wird einerseits Know-how zum Vorteil für alle Kunden gebündelt. Andererseits können hierdurch auch Synergieeffekte für die Bundesverwaltung erzielt werden, durch die die Bundesverwaltung dauerhaft in der Lage sein wird, ihre IT-Infrastruktur als Kernelement der Arbeitserledigung zu betreiben

und fortzuentwickeln. Das ITZBund erzeugt Informations-, Kommunikations- und Transaktionsprozesse zwischen unterschiedlichen Adressaten wie z.B. Politik, Verwaltung, Bürgerinnen und Bürgern sowie der Wirtschaft. Zu den Kernaufgaben gehören der hochsichere Betrieb von Fachverfahren, Portalen und Rechenzentren sowie die Gewährleistung von Datenschutz und IT-Sicherheit.

IT-Planungsrat *it-planungsrat.de*

Der IT-Staatsvertrag zur Ausgestaltung von Art. 91c Grundgesetz bildet den rechtlichen Rahmen für den IT-Planungsrat und definiert das Aufgabenspektrum des Gremiums: Koordinierung der Zusammenarbeit von Bund und Ländern in Fragen der Informationstechnik, Beschlussfassung über fachunabhängige und fachübergreifende IT-Interoperabilitäts- und IT-Sicherheitsstandards, Steuerung von E-Government-Projekten sowie Planung und Weiterentwicklung des - vom Bund zu errichtenden und zu betreibenden - Verbindungsnetzes nach Maßgabe des Gesetzes über die Verbindung der informationstechnischen Netze des Bundes und der Länder - IT-NetzG. Ziel des Planungsrates ist es dabei Deutschlands Verwaltung zu einem Spitzenreiter im Bereich der Digitalisierung zu machen. Dieses Ziel erfordert die Zusammenarbeit aller föderalen Ebenen und die Entwicklung neuer Strategien für nutzer- und nutzenorientierte IT-Lösungen. Dazu wurde die Föderale IT-Kooperation, kurz FITKO, als neuer Player gegründet (Januar 2020 als Anstalt des öffentlichen Rechts in Trägerschaft aller Länder und des Bundes mit Sitz in Frankfurt am Main). Die Idee hinter der FITKO ist es, eine kleine, agile Organisation zu schaffen, die die nötigen Ressourcen und Kompetenzen unter einem Dach bündelt und den weiteren Ausbau der Digitalisierung in der öffentlichen Verwaltung im Auftrag des IT-Planungsrates zielgerichtet koordiniert und vorantreibt. Die FITKO bildet als Anstalt des öffentlichen Rechts in Trägerschaft aller Länder und des Bundes den operativen Unterbau für den IT-Planungsrat. Durch dessen Entscheidungen als Bund-Länder-übergreifendes politisches Gremium wurden vielfältige Kooperationen ermöglicht, diverse E-Government-Projekte erfolgreich umgesetzt und gemeinsame Standards entwickelt.

Ziel der FITKO ist es neben der Etablierung eines Informations- und Wissenstransfers neue Formen der Zusammenarbeit beim Austausch und der Kommunikation zu etablieren. Konkret ergeben sich daraus die folgenden Aufgaben:

- Bündelung sämtlicher föderaler Aktivitäten zur Digitalisierung der Verwaltung,
- Erarbeitung und Umsetzung der föderalen IT-Strategie,
- Konzeption und Weiterentwicklung der föderalen IT-Architektur
- Koordinierung und operative Steuerung der Produkte und Projekte des IT-Planungsrates sowie die
- Bewirtschaftung des Digitalisierungsbudgets (Am 1. Oktober 2019 ist der erste IT-Änderungsstaatsvertrag in Kraft getreten. Damit haben sich Bund und Länder verpflichtet, für die Jahre 2020–2022 ein Digitalisierungsbudget im Umfang von 180 Millionen Euro zur Verfügung zu stellen. Mit diesem Budget sollen Projekte und Aktivitäten unterstützt werden, die der Digitalisierung von Verwaltungsleistungen auf allen föderalen Ebenen zugutekommen. Damit leistet das Digitalisierungsbudget auch einen wesentlichen Beitrag zur Umsetzung des OZG.

Ein wichtiger Bestandteil des IT-Planungsrat im Kontext der Cybersecurity ist die Arbeitsgruppe Informationssicherheit.

IT-Rat

Der IT-Rat ist das zentrale politisch-strategische Gremium für übergreifende Themen der Digitalisierung. Er ist für die Steuerung der Informationstechnik in der Bundesverwaltung verantwortlich. Mitglieder sind insbesondere die für Verwaltungsdigitalisierung und Informationstechnik zuständigen beamteten Staatssekretärinnen und Staatssekretäre aller Bundesministerien. Das Gremium tagt unter dem Vorsitz des Chefs des Bundeskanzleramtes.

Kommando Cyber- und Informationsraum (KdoCIR)

Das KdoCIR ist das Führungskommando des militärischen Organisationsbereichs (MilOrgBer) CIR der Bundeswehr. Der MilOrgBer CIR gewährleistet den Schutz und Betrieb der IT-Systeme der Bundeswehr im In- und Ausland und leistet durch die ressortübergreifende Bereitstellung von Lagebildern und Geoinformationen sowie die Mitarbeit im Nationalen Cyber Abwehrzentrum einen bedeutenden Beitrag zur Cybersicherheit in Deutschland. Dem KdoCIR sind das Kommando Strategische Aufklärung, das Zentrum für Geoinformationswesen der Bundeswehr sowie das Kommando Informationstechnik der Bundeswehr unterstellt.

Nationaler Cyber-Sicherheitsrat *cio.bund.de*

Der bereits 2011 eingerichtete Nationale Cyber-Sicherheitsrat organisiert unter dem Vorsitz des BfIT, die Zusammenarbeit im Bereich Cyber-Sicherheit innerhalb der Bundesregierung sowie zwischen Staat und Wirtschaft.
Mitglieder des Cyber-Sicherheitsrats sind:

- Bundeskanzleramt (BKAmt)
- Auswärtiges Amt (AA)
- Bundesministerium des Innern (BMI)
- Bundesministerium der Verteidigung (BMVg)
- Bundesministerium für Wirtschaft und Energie (BMWi)
- Bundesministerium der Justiz und für Verbraucherschutz (BMJV)
- Bundesministerium der Finanzen (BMF)
- Bundesministerium für Bildung und Forschung (BMBF)
- Vertreter der Länder (Niedersachsen und Hessen)

Die Wirtschaft ist durch den Bundesverband der deutschen Industrie (e.V.) (BDI), den Bitkom, den Deutschen Industrie- und Handelskammertag (DIHK), den Bundesverband der Energie- und Wasserwirtschaft (BDEW) sowie durch den UP (Umsetzungsplan) KRITIS als assoziierte Mitglieder vertreten.
Seit Juli 2017 wird der Nationale Cyber-Sicherheitsrat durch einen Fachbeirat unterstützt.

Nationales Cyber-Abwehrzentrum (Cyber-AZ)

Das Cyber-AZ ist ein Kernelement der 2011 ausformulierten Cyber-Sicherheitsstrategie (CSS), die den vorangegangenen "Nationalen Plan zum Schutz der Informationsinfrastrukturen" aus dem Jahr 2005 fortschrieb. Durch die Cyber-Sicherheitsstrategie 2011 wurde das Cyber-AZ unter Federführung des BSI eingerichtet und am 16. Juni 2011 eröffnet.

Das Cyber-AZ dient als Informations- und Koordinierungsplattform zu dessen Kernbehörden derzeit das BBK, das BfV, das BKA, der BND, der MAD, die Bundespolizei (BPOL), das BSI und das Kommando Cyber- und Informationsraum der Bundeswehr (KdoCIR) zählen. Zielsetzung des Cyber-AZ ist der Informationsaustausch zu Cyber-Vorfällen im Rahmen der gesetzlichen Grenzen der teilnehmenden Behörden sowie die Abstimmung von Maßnahmen der Behörden bei Cyber-Vorfällen. Das Cyber-AZ beugt so potentiellen Informationsverlusten bei den Behörden vor und verbessert die Koordination und Abstimmung von Maßnahmen bei Cyber-Vorfällen der teilnehmenden Behörden.
Mit der Verabschiedung einer neuen Geschäftsordnung des Cyber-AZ zum 1. September 2019, wurden wesentliche Änderungen wirksam. Erstmals haben sich alle beteiligten Behörden dazu verpflichtet, Verbindungspersonen vor Ort ins Cyber-AZ zu entsenden. Die neue Vor-Ort-Präsenz erleichtert den Informationsaustausch und die Abstimmung operativer Maßnahmen bei akut zu bewältigenden Sachverhalten. Gleichzeitig wurde die Struktur des Cyber-AZ an die Struktur ähnlicher Kooperationsplattformen angepasst. Nunmehr orientiert sich das Cyber-AZ am Modell des Gemeinsamen Terrorismusabwehrzentrums (GTAZ). Die Funktion des Leiters des Cyber-AZ wurde durch die eines Koordinators ersetzt. Diese Aufgabe wird seit dem 16. Dezember 2019 für die nächsten zwei Jahre durch das BKA wahrgenommen. Unterstützt wird das BKA dabei durch stellvertretende Koordinatoren des BfV und der Bundeswehr bzw. dem KdoCIR. Räumlich bleibt das Cyber-AZ weiterhin im BSI und damit auch in unmittelbarer Nähe des Nationalen IT-Lagezentrums/IT-Krisenreaktionszentrums und des CERT-Bund. Das BSI stellt darüber hinaus wie bisher die IT-Infrastruktur und Mitarbeiter für die Geschäftsstelle des Cyber-AZ zur Verfügung.
Das Cyber-AZ befindet sich in einem kontinuierlichen Fortentwicklungsprozess um neuen technischen Entwicklungen und daraus resultierenden Gefahren zu begegnen. Da bedeutet auch, dass weitere Akteure in die Arbeit Cyber-AZ eingebunden werden sollen. Derzeit wird eine Beteiligung der Länder erarbeitet.

Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) *zitis.bund.de*

ZITiS ist die Forschungs- und Entwicklungsinstanz für innovative, technische Lösungen im Bereich der Cybersicherheit und wurde im Rahmen der Umsetzung der Cybersicherheitsstrategie 2016 gegründet. Die ZITiS gehört zum Geschäftsbereich BMI und hat die Aufgabe, den Behörden des Bundes mit Sicherheitsaufgaben (BOS), insbesondere dem BKA, dem BfV und der BPol sowie BND, Zollkriminalamt (ZKA) und dem MAD technische Werkzeuge und Methoden innerhalb ihres rechtlichen Rahmens zur Verfügung zu stellen, damit sie in die Lage versetzt werden, ihren gesetzlichen Auftrag auch in Zukunft erfüllen zu können. Die ZITiS hat keine eigenen Eingriffsbefugnisse, sondern berät und unterstützt die Sicherheitsbehörden als Forschungs- und Entwicklungsdienstleister in den Themenbereichen: Digitale Forensik, Telekommunikationsüberwachung, Kryptoanalyse und Big Data Analyse. Der Anspruch ist es dabei, im Bereich der Cyberfähigkeiten und nicht zuletzt auch für die Stärkung der digitalen Souveränität der BOS eine Schlüsselrolle zu übernehmen und damit einen wesentlichen Beitrag zur Cybersicherheit bzw. inneren Sicherheit zu leisten. Eine besondere Herausforderung für alle Behörden des Bundes ist die Gewinnung von Personal in technischen Nischen wie z.B. Re-Engineering, Entwicklung von FPGA-Technologie, TKÜ-Technik und Kryptoanalyse. Aus diesem Grund bildet ZITiS in Kooperation mit der Universität der Bundeswehr nicht nur Studenten in den Fachrichtungen „Cybersicherheit“ und „Informatik“ aus, sondern hat mit dem Forschungsinstitut CODE an der Universität der Bundeswehr ein Vertiefungsmodul „Cyber Network Capabilities“ eingerichtet, um Studenten im Studiengang „Cyber-Sicherheit“ Spezialkenntnisse zu vermitteln. Ziel ist es, in Deutschland einzigartige technische und personelle Voraussetzungen zu schaffen, um Forschung und Entwicklung auf Vorreiterniveau betreiben zu können.

6.3.2 Initiativen des Bundes

Bündnis für Cybersicherheit *bmi.bund.de*

Seit 2018 arbeiten BMI und BDI im Bündnis für Cybersicherheit eng und intensiv an Cybersicherheitsthemen. Das Bündnis verfolgt klar definierte Ziele, die das BMI und BDI gemeinsam mit Verbänden, Unternehmen und Bundesbehörden erreichen wollen: eine verbesserte Zusammenarbeit zwischen Staat und Wirtschaft, eine verbesserte Kooperation zwischen Staat und Wirtschaft im internationalen Kontext sowie die Identifikation und Prüfung von Projekten zur Stärkung der digitalen Souveränität des Wirtschaftsstandortes Deutschland.

Digital Hub Initiative de:hub *de-hub.de*

Die Digital Hub-Initiative des BMWi vernetzt an zwölf Kompetenzstandorten in Deutschland gezielt Mittelstand und Corporates mit neuen Innovationspartnern aus Wissenschaft und Gründerszene. Aktuell sind die folgenden zwölf Standorte in Deutschland in der Digital-Hub-Initiative angesiedelt:

- IoT & FinTech (Berlin)
- Smart Systems & Smart Infrastructure (Dresden, Leipzig)
- Logistics (Dortmund)
- FinTech & Cybersecurity (Frankfurt, Darmstadt)
- Logistics (Hamburg)
- Artificial Intelligence (Karlsruhe)
- InsurTech (Köln)
- Digital Health (Nürnberg, Erlangen)
- Digital Chemistry & Digital Health (Mannheim, Ludwigshafen)
- Mobility & InsurTech (München)
- Future Industries (Stuttgart)
- MediaTech (Potsdam)

Die regionalen Digital Hubs sind dabei Kristallisationspunkte für digitale Innovationen und widmen sich verschiedenen branchenspezifischen Schwerpunktthemen. Sie bieten unterschiedlichste Kompetenzen, Disziplinen, Ideen, Technologien und Kreativitätspotential. Die Digital Hubs dienen als regionale Anlaufstelle für kleine und mittlere Unternehmen aller Branchen bei Fragen zur Digitalisierung. Sie sind grundsätzlich branchenoffen konzipiert und bieten die Möglichkeit, sich vor Ort über die Digitalisierung zu informieren, Digitalisierung zu erleben sowie neue Ideen für digitale Projekte in Experimentierräumen zu entwickeln und zu erproben. Einige Schwerpunktthemen der Digital-Hubs stehen in direktem Zusammenhang mit IT-Sicherheit und arbeiten vor diesem Hintergrund an neuen Sicherheitsprodukten und Infrastrukturen für die jeweiligen Märkte, z.B. arbeitet der Digital-Hub in Frankfurt an neuen Sicherheitsprodukten für den Finanzmarkt. Der Digital Hub Darmstadt ist auf Cybersicherheit spezialisiert (siehe hierzu den Steckbrief des Digital Hub Cybersecurity).

Go-Digital *bmwi-go-digital.de*

Das Förderprogramm "go-digital" des BMWi richtet sich mit seinen drei Modulen "Digitalisierte Geschäftsprozesse", "Digitale Markterschließung" und "IT-Sicherheit" gezielt an kleine und mittlere Unternehmen der gewerblichen Wirtschaft und an das Handwerk. Praxiswirksam bietet das Programm Beratungsleistungen, um mit den technologischen und gesellschaftlichen Entwicklungen im Bereich Online-Handel, Digitalisierung des Geschäftsalltags und dem steigenden Sicherheitsbedarf bei der digitalen Vernetzung Schritt zu halten. Zudem unterstützen autorisierte Beratungsunternehmen bei der Umsetzung konkreter Digitalisierungsmaßnahmen im Unternehmen.

Initiative Polizei-Beratung.de *polizei-beratung.de*

Die Aktion „Verklickt!“ dient der polizeilichen Kriminalprävention der Länder und des Bundes. Das Medienpaket kommt an Schulen ab der Klassenstufe 7 zum Einsatz und dient dem Training für einen sichereren Umgang mit digitalen Medien. Es wird ebenso eine Opferberatung bei Cybercrime-Vorfällen angeboten. Das Projekt wird in Zusammenarbeit der Polizeilichen Kriminalprävention (ProPK) und dem BSI betrieben. Alle Länder beteiligen sich an dieser Initiative.

Initiative-S *initiative-s.de*

Die Initiative-S unterstützt Unternehmen bei der Überprüfung des Webauftritts und der Beseitigung von Schadprogrammen, um das IT-Sicherheitsniveau nachhaltig zu verbessern. Träger der Initiative-S ist der eco-Verband der Internetwirtschaft. Die Initiative wird vom BMWi gefördert.

Initiative Wirtschaftsschutz

Die durch das BMI koordinierte Dachinitiative zur Umsetzung der Nationalen Strategie für Wirtschaftsschutz analysiert gemeinsam mit Experten von Sicherheitsbehörden (BfV, BKA, BND und BSI), sowie Spitzenwirtschafts- und Sicherheitsverbänden (BDI, DIHK, ASW Bundesverband und BDSW) die Risikolage und entwickelt tragfähige Handlungskonzepte und Checklisten zu den Themenfeldern

- Ganzheitlicher Wirtschaftsschutz
- Cyber-, hybride und physische Sicherheitsrisiken
- Eigenschutzmaßnahmen von Unternehmen und Forschungseinrichtungen
- Unterstützungsmaßnahmen von Politik und Behörden zum Schutz deutscher Unternehmenswerte.

Mittelstand 4.0 Kompetenzzentren

Die Mittelstand 4.0 Kompetenzzentren unterstützen Unternehmen kostenlos bei Digitalisierungsprojekten, übernehmen das Projektmanagement und begleiten die Unternehmerinnen und Unternehmer von der Ist-Analyse über die Konzeptentwicklung bis zur Auswahl von geeigneten Digitalisierungslösungen. Kompetenzzentren helfen mit Expertenwissen, Demonstrationszentren, Best-Practice-Beispielen sowie Netzwerken, die dem Erfahrungsaustausch dienen. Cybersicherheitsthemen sind in verschiedenen Kompetenzzentren Schwerpunktthemen, die mit der Beratung zu Digitalisierung einhergehen. Das BMWi fördert die Mittelstand 4.0 Kompetenzzentren.

Maritime Forschungsstrategie 2025 *bmwi.de*

Die Maritime Forschungsstrategie 2025 des BMWi umfasst die Ziele und Handlungsfelder der maritimen Industrie im Bereich der vorwettbewerblichen industriellen Forschung. Im Titel „Echtzeittechnologien für die Maritime Sicherheit“ werden Technologieentwicklungen auf den Gebieten der Beobachtung und Überwachung von Seegebieten und Infrastrukturen, der Lagebilderstellung sowie der Assistenz- und Transportleitsysteme gefördert. Neben den technischen Problemstellungen bei der Datenerfassung und -übertragung auf See stehen hierbei insbesondere auch Aspekte der Cybersicherheit im Vordergrund.

Telematikinfrastruktur (TI) *gematik.de*

Die Telematikinfrastruktur (TI) dient der Vernetzung der Akteure der Gesetzlichen Krankenversicherung zum sicheren Informationsaustausch. Die TI gewährleistet einen sicheren Informationsaustausch zwischen Versicherten und Leistungserbringern, wie bspw. Ärztinnen und Ärzten, Zahnärztinnen und Zahnärzte oder Psychotherapeutinnen und Psychotherapeuten. Dadurch ergeben sich besondere Herausforderungen an den Datenschutz und die Informationssicherheit. Neben der Einführung der elektronischen Gesundheitskarte (verpflichtend), sollen Versicherte in Zukunft

weitere, freiwillige Anwendungen zur elektronischen Datenverarbeitung nutzen können, wobei die Datenhoheit stets bei der oder dem Versicherten liegt.

6.4 Schwerpunktthema: Behörden, Einrichtungen und Initiativen auf Länderebene

Die Cybersicherheit auf Länderebene ist vielfältig und facettenreich. Alle Länder verfügen neben gleichartigen Einrichtungen, wie eigene Computer Emergency Response Teams (CERTs), ZAC oder der Cyberabwehr des Verfassungsschutzes, auch über einige besondere und spezialisierte Einrichtungen und Initiativen.

In Ergänzung zu den Steckbriefen der Cybersicherheitsakteure und -initiativen soll die nachstehende Auflistung einen Überblick über die maßgeblichen Player und Aktivitäten auf Ebene der Länder geben, soweit diese über eine Internetrecherche auffindbar waren.

6.4.1 Behörden und Einrichtungen der Länder

Arbeitsgruppe Cyber-Sicherheit der Innenministerkonferenz

Die Innenministerkonferenz (IMK) unterhält eine Länderarbeitsgruppe Cyber-Sicherheit zur Abstimmung der länderübergreifenden fachlichen Zusammenarbeit auf politischer Ebene.

Arbeitsgruppe Cybersicherheit Berlin *berlin.de*

Die Arbeitsgruppe Cybersicherheit in der Senatsverwaltung für Inneres und Sport (Ref III C Abt. III) hat den Schutz Kritischer Infrastrukturen, die Bekämpfung von Computer- und Internetkriminalität sowie die Einbindung von Behörden und Unternehmen in ein umfangreiches Netzwerk als fachliche Schwerpunkte.

Bayrisches Staatsministerium für Digitales *stmd.bayern.de*

Das Bayerische Staatsministerium für Digitales wurde im Zuge der Regierungsbildung im Jahr 2018 neu gegründet. Es ist Denkfabrik der Digitalisierung in Bayern und kümmert sich um Grundsatzangelegenheiten, Strategie und Koordinierung. Das Digitalministerium ist das erste dieser Art in Deutschland. Das Staatsministerium für Digitales sieht Cybersicherheit als Erfolgsfaktor der digitalen Transformation und berücksichtigt das Thema in allen Projekten und Initiativen.

Beratungsstellen Wirtschaftsschutz

Die Beratungsstelle Wirtschaftsschutz als Einrichtung auf Länderebene hat zum Ziel, technologieorientierte und innovative Unternehmen (Großkonzerne sowie klein- und mittelständische Firmen) vor Ausspähversuchen im Sinne der Wirtschaftsspionage durch fremde Nachrichtendienste zu schützen. Zu den Aufgaben der Beratungsstelle Wirtschaftsschutz gehören Beratungsgespräche, Anbieten von Fachvorträgen, Organisation von Fachtagungen, Veröffentlichung von Publikationen und Informationen. Die Beratungsstellen sind bei den jeweiligen Landesämtern für Verfassungsschutz angesiedelt. Für Informationen zur Initiative Wirtschaftsschutz des Bundesamts für Verfassungsschutz wird auf den eigenen Steckbrief verwiesen.

CERT

Alle Länder betreiben ein Computer Emergency Response Team (CERT), das die zentrale Anlaufstelle für alle Maßnahmen der IT-Sicherheit in der Landesverwaltung darstellt. Zu den Aufgaben der CERTs gehören präventive Maßnahmen, um Vorfälle und Sicherheitslücken möglichst früh zu erkennen sowie reaktive Aufgaben, mit dem Ziel auf Angriffe zu reagieren und Schaden gering zu halten oder zu vermeiden. Gemäß der Informationssicherheitsleitlinie in der öffentlichen Verwaltung sind alle Bundesländer verpflichtet, ein CERT aufzubauen, wobei diese in den Ländern in unterschiedlichen Behörden angesiedelt sind.

Das Landes-CERT überwacht ständig die aktuelle Sicherheitslage der Landesverwaltung, um mögliche Bedrohungen aus dem Cyberraum zu erkennen und deren Auswirkungen auf die IT-Systeme der Landesverwaltung zu bewerten.

Im Krisenfall stellt es dem Krisenstab der Landesregierung ein IT-Lagebild zur Verfügung und berät diesen zu Fragen der Informationssicherheit. Das CERT steht in Fragen der Cybersicherheit den Mitgliedern der Landesregierung zur Verfügung und arbeitet im direkten Kontakt mit dem Wirtschaftsschutz im Verfassungsschutz sowie dem LKA (ZAC) zusammen. Das CERT stellt die zentrale Kommunikationsdrehscheibe für den Informationsaustausch über Sicherheitsvorkommnisse innerhalb der Landesverwaltung und auch in Richtung der Kommunen dar.

CERT-kommunal-sal

Die beiden Bundesländer Rheinland-Pfalz und Saarland kooperieren seit 2015 auf dem Gebiet der Informationssicherheit. Ziel dieser Kooperation ist die enge Zusammenarbeit bei der gemeinsamen Abwehr von IT-Angriffen und die Bereitstellung der Dienste des CERT Rheinland-Pfalz auch für das Saarland. Der Zweckverband eGo-Saar dient als Kopfstelle und zentrale Organisationseinheit für die primäre Zielgruppe CERT-kommunal-sal (alle saarländischen Kommunen, Landkreise und Spitzenverbände). Der Zweckverband betreut die CERT-Schnittstellen (Kontaktdaten und redundanzfreie Softwarelisten). Alle relevanten Informationen des CERT werden direkt an die Kommunen geleitet.

Cyber-Allianz-Zentrum Bayern (CAZ) *verfassungsschutz.bayern.de*

Das Bayerische Landesamt für Verfassungsschutz unterstützt mit dem CAZ in Bayern ansässige Unternehmen, Hochschulen und KRITIS-Betreiber bei der Prävention und Abwehr von „elektronischen Angriffen". Das CAZ ist vertraulicher Ansprechpartner und die zentrale staatliche Steuerungs- und Koordinierungsstelle in Bayern. Das CAZ führt für Betroffene forensische Analysen und nachrichtendienstliche Bewertung durch und gibt Handlungsempfehlungen. Informationen zu Angriffen werden in anonymisierter Form anderen Unternehmen und Einrichtungen weitergeleitet.

Digitalagentur Niedersachsen *digitalagentur-niedersachsen.de*

Die Digitalagentur Niedersachsen unterstützt den Mittelstand und das Handwerk in Niedersachsen bei der Identifikation und Umsetzung von wirtschaftlichen Digitalisierungsansätzen. Ihr Arbeitskreis IT-Security beschäftigt sich mit Themen rund um Cybersicherheit; u.a. werden Anlaufstellen und Angebote im Kontext der IT-Sicherheit zentral dargestellt. Die Digitalagentur Niedersachsen ist ein Angebot der Innovationszentrum Niedersachsen GmbH im Auftrag des Niedersächsischen Ministeriums für Wirtschaft, Arbeit, Verkehr und Digitalisierung.

Digitales Innovationszentrum (DIZ) *diz-bw.de*

Das DIZ wurde von der Landesregierung Baden-Württemberg 2016 ins Leben gerufen. Seither bringt das DIZ die Digitale Transformation im Land voran und unterstützt auf der einen Seite insbesondere KMU durch spezifische Angebote in ihren Digitalisierungsbestrebungen. Auf der anderen Seite arbeitet das DIZ eng mit Wirtschaft, Wissenschaft und öffentlicher Hand zusammen in gemeinsamen Projekten wie KI-Transfer BW, Digitales Hubnetzwerk BW und Digital Hub für Angewandte KI um die Digitalisierung in die Fläche zu bringen. Als unabhängige Anlaufstelle begleitet das DIZ den Mittelstand auf dem Weg in die digitale Souveränität und hilft dabei, Wertschöpfungsketten nachhaltig in die digitale Welt zu überführen. Digitalisierung und IT-Sicherheit sind die herausragenden Themenfelder des DIZ. Das DIZ adressiert alle Gesellschaftsgruppen.

Hessisches Ministerium für Digitale Strategie und Entwicklung *digitales.hessen.de*

Das unmittelbar dem Ministerpräsidenten zugeordnete Ressort für Digitale Strategie und Entwicklung wurde 2019 gegründet und steuert die Umsetzung des Masterplans „Digitales Verwaltungshandeln". Im Ressort werden Kompetenzen zum Thema Digitalisierung aus vielen Bereichen der Landesverwaltung gebündelt. Es befasst sich mit Fragen der Künstlichen Intelligenz, den Bedürfnissen von hessischen Unternehmen in Fragen der Digitalisierung sowie gesellschaftlicher Akzeptanz. Die Digitalisierung der Verwaltung zum Nutzen aller hessischen Bürgerinnen und Bürger ist ein sehr wichtiges Handlungsfeld. Die Abteilung Cyber- und IT-Sicherheit verantwortet wichtige Aspekte der Umsetzung, insbesondere des Hauptprojekts „Digitale Modellbehörde".

Hessen Cyber Competence Center (Hessen3C) *hmdis.de und innen.hessen.de*

Hessen3C ist im Bereich Cybersicherheit die zentrale Kompetenzstelle zur interdisziplinären Zusammenarbeit und institutionalisierten Kooperation staatlicher Behörden in Hessen. Das Center hat die Aufgabe, die Sicherheit in der Informationstechnik des Landes zu erhöhen, cyberspezifische Gefahren abzuwehren, die Effizienz der Bekämpfung der Cyberkriminalität zu erhöhen und Synergien zu schaffen. Ein wesentlicher Bestandteil zur Zielerreichung ist der regelmäßige Informationsaustausch zu Cyberthemen zwischen Hessen3C, der Hessischen Polizei und dem Hessischen Verfassungsschutz sowie die Erstellung eines gemeinsamen Lagebildes für Hessen. Dies geschieht unter Beibehaltung der jeweiligen Zuständigkeiten und unter strikter Wahrung des Trennungsgebotes zwischen Polizei und Verfassungsschutz. Im Hessen3C arbeiten Cybersicherheitsspezialisten aus dem CERT des Landes, der Hessischen Polizei und des Landesamtes für Verfassungsschutz Hessen (Bereich digitaler Wirtschaftsschutz) zusammen, um zentral und organisationsübergreifend Expertise und Dienstleistungen im Bereich Cybersicherheit bereitzustellen.

Das Hessen3C vertritt das Land Hessen im Bereich Cybersicherheit in den entsprechenden Bund/Länder-Gremien. Für die hessische Landes- und Kommunalverwaltung sowie für KMU in Hessen steht mit dem Hessen3C ein rund um die Uhr erreichbarer, zentraler Ansprechpartner bei Cybersicherheitsvorfällen im Land Hessen bereit, der mit hoher fachlicher Kompetenz berät. Die Einrichtung des Hessen3C ist bundesweit einzigartig.

Das Hessen3C stellt seine Cybersicherheitswarnung für die Anwendung bzw. App „hessenWARN“ zur Verfügung, die eine Weiterentwicklung der bundesweit bekannten Anwendung „KatWarn“ darstellt und neben Umwelt- und Katastrophenmeldungen auch über Cybersicherheitswarnungen informiert.

Initiativen der Landespolizeien

Die Polizeibehörden aller 16 Bundesländer betreiben jeweils ZACs. Diese wurden für die Wirtschaft und andere öffentliche und nichtöffentliche Stellen eingerichtet, um als kompetente Ansprechpartner für IT-Sicherheitsvorfälle zeitnah polizeiliche Erstmaßnahmen zu veranlassen. Die ZAC-Dienststellen, die bei den Landeskriminalämtern angesiedelt sind, initiieren, koordinieren und beteiligen sich an vielfältigen Cybercrime-Kooperationen mit anderen Behörden, der Wirtschaft und der Wissenschaft auf landes-, bundes- sowie internationaler Ebene. Die ZAC einiger Länder übernehmen zusätzliche Aufgaben und unterscheiden sich im Angebot:

- Die ZAC Baden-Württemberg hat bspw. die Möglichkeit, eine interne Task Force Digitale Spuren aufzurufen, in der Experten aus allen Spezialisierungsbereichen der Abteilung Cybercrime und Digitale Spuren vertreten sind.
- Die Bayerische Kriminalpolizei betreibt spezielle Cybercrime Kommissariate, über die Privatpersonen Cybercrime-Delikte zur Anzeige bringen. Die ZAC im Freistaat Bayern stellt u.a. ihre Leistungen explizit auch Bürgerinnen und Bürgern zur Verfügung und dient ihnen für Hilfestellung als zentrale telefonische Anlaufstelle bei Cybervorfällen.
- Das Landeskriminalamt Brandenburg betreibt die Einrichtung eines Cyber-Competence-Centers in Potsdam, über das eine zentrale Bündelung von personellen und fachlichen Kompetenzen zur Bekämpfung und Aufklärung jeglicher Kriminalitätsbereiche im Zusammenhang mit dem Internet erfolgt. Mit dem Cyber-Competence-Center entsteht eine neue Fachdienststelle, in der die präventiven und repressiven Aufgaben sowie die Ermittlungsunterstützung zur Bekämpfung von Cybercrime zusammengefasst werden. Zu den Aufgaben gehören bspw. die zentralen Ermittlungen im Bereich des qualifizierten Cybercrime, die Zentrale Internetrecherche (ZIR), die Unterstützung der Ermittlungen der Polizeidirektionen und -inspektionen sowie informationstechnische Erhebung und Auswertung von Internetdaten.
- Unter der Leitung der Polizei Hamburg arbeiten Sicherheitsbehörden und Wirtschaft im „Netzwerk Standortsicherheit Hamburg“ zusammen. Das Netzwerk bündelt alle Aktivitäten insbesondere auf den Themenfeldern Wirtschaftskriminalität und Korruption, Wirtschaftsspionage, IT-Sicherheit und Cybercrime, Qualifizierung und Prävention, Sicherheitswirtschaft und Kritische Infrastrukturen. Expertenkreise zu den zentralen Themen gewährleisten einen praktischen Austausch und garantieren kurze Wege und schnelle Entscheidungen.
- In den Polizeipräsidien des Landes Hessen sind seit 2007 Internetkommissariate eingerichtet, in denen Präventionsfachberaterinnen und -berater für den Bereich Cybercrime zur Verfügung stehen. Zusätzlich werden regionale Beraterinnen und Berater für Cybercrime und Internetkriminalität ausgebildet, die in den Dienststellen ansprechbar sind. Die Polizeiakademie Hessen ist Mitglied der ECTEG (European Cybercrime Training and Education Group), die von der Europäischen Kommission zur Förderung der Zusammenarbeit europäischer Strafverfolgungsbehörden, zum Wissensaustausch und der grenzübergreifenden Bearbeitung von Cybercrime-Vorfällen gebildet wurde.
- Das Land Nordrhein-Westfalen betreibt das Zentrale Informations- und Servicezentrum Cybercrime (ZISC), das andere Behörden des Landes und des Bundes bei der Einsatzbewältigung und bei der Ermittlungsführung in Fällen herausragender Cybercrime berät. Dort ist auch die ZAC mit dem Single Point of Contact (SPoC) angesiedelt, die 24x7 erreichbar sind. Staatliche Behörden, Institutionen und Verbände aus Forschung und Lehre oder Wirtschaftsunternehmen erhalten fachkompetente Hilfe. Bei konkreten Cybervorfällen werden vom ZISC aus-

gehend alle wichtigen Sofortmaßnahmen initiiert und koordiniert. Das Cybercrime Kompetenzzentrum Nordrhein-Westfalen geht gezielt im Internet auf Streife, um Straftaten aufzudecken, Gefahren mit Bezug zum Internet abzuwehren und neue Phänomene zu entdecken und zu analysieren. Schwerpunkt der Ermittlungen sind insbesondere die Phänomenbereiche Kinderpornografie, politisch motivierte Kriminalität und illegaler Arzneimittelhandel. Um Straftäterinnen und Straftäter sowie Gefährderinnen und Gefährder im Internet zu identifizieren, entwickelt das Cyber-Recherche- und Fahndungszentrum (CRuFz) immer wieder neue Methoden, die bedarfsweise von anderen Polizeidienststellen genutzt werden können. Darüber hinaus berät und unterstützt das CRuFz Polizei-, Verwaltungs- und Justizbehörden, z. B. bei der Identifizierung von Tatverdächtigen, die versuchen, die Anonymität des Internets für ihre Straftaten zu nutzen.

- Die Polizei Rheinland-Pfalz bietet für Bürgerinnen und Bürger ein Informationsportal (cybersicherheit-rlp.de oder kriminalpraevention.rlp.de), dessen Ziel die Steigerung des Gefahrenbewusstseins sowie die Vermittlung geeigneter Verhaltensweisen zur Gefahrenminimierung ist. Das Präventionsangebot der Polizei für den Bereich der Computer- und Internetkriminalität können Bürgerinnen und Bürger online abrufen. Das Informationsportal informiert anhand konkreter Betrugsszenarien praxisnah über Verhaltensmöglichkeiten und hilfreiche Ansprechpartner. Themen wie Online-Shopping, Schadsoftware, Cloud-Computing, Identitätsdiebstahl, Darknet, Smart Home etc. stehen im Vordergrund des Portals.
- Das Landeskriminalakt Sachsen betreibt ein Cybercrime Competence Center (SN4C), das in herausragenden Cybercrime Fällen ermittelt und eng mit der Zentralstelle Cybercrime Sachsen der Generalstaatsanwaltschaft zusammenarbeitet. Es bietet Ermittlerinnen und Ermittlern hilfreiche Unterstützung, wenn besondere IT-Kompetenz erforderlich ist. In der Zentralstelle der sächsischen Polizei für die Bekämpfung von Cybercrime sind Expertinnen und Experten aus den Bereichen Ermittlung, Massendaten, Telekommunikationsüberwachung und IT-Forensik vereint. Damit ist die Basis für kurze Kommunikationswege, wertvolle Synergieeffekte, gezielte Analyse und deliktspezifische Auswertung geschaffen. Das SN4C bietet mit der ZAC Unterstützung für Unternehmen, Behörden und Verbände des Freistaates Sachsen im Zusammenhang mit Angriffen durch Cyberkriminelle an, indem es Sicherheitsvorfälle mit Bezug zu Cybercrime aufnimmt und polizeiliche Maßnahmen einleitet.
- • Der Ratgeber Internetkriminalität des Landeskriminalamtes Niedersachsen informiert über aktuelle Trends, Gefahren und Prävention im Bereich Cybercrime. Neben aktuellen Warnmeldungen werden Informationen zu verschiedenen relevanten Themen der Internetkriminalität zur Verfügung gestellt und die Möglichkeit gegeben, persönliche Fragen bei Cybersicherheitsvorfällen zu stellen.

IT-Verbund Schleswig-Holstein (ITVSH) *itvsh.de*

Der IT-Verbund Schleswig-Holstein wurde auf Initiative der Landesregierung im Jahr 2019 als kommunales Kompetenzzentrum für die Digitalisierung aller Kommunen gegründet. Der ITVSH unterstützt die Kommunen, indem er die Aufgaben des einheitlichen Ansprechpartners wahrnimmt und kommunale Digitalisierungsprojekte umsetzt. Land und Kommunen finanzieren den ITVSH gemeinschaftlich. Der IT-Verbund Schleswig-Holstein hat zudem die gesetzliche Aufgabe, die Entwicklung einer gemeinsamen IT-Strategie seiner Träger zu fördern. Seit 2019 unterstützt der IT-Verbund mit dem Projekt SiKoSH (Sicherheit für Kommunen in Schleswig-Holstein) Kommunen darin, Grundschutzmaßnahmen nach dem kommunalen Grundschutzprofil des BSI umzusetzen. Der ITVSH unterstützt beim Aufbau eines professionellen ISMS sowie dabei, Sicherheitsmaßnahmen in den Kommunen zu etablieren und damit zusammenhängende Sicherheitsprozesse einzuführen.

Landesamt für Sicherheit in der Informationstechnik *lsi.bayern.de*

Das Landesamt für Sicherheit in der Informationstechnik ist die IT-Sicherheitsbehörde des Freistaats Bayern. Aufgaben sind neben dem aktiven Schutz der staatlichen IT-Systeme die Beratung von Kommunen, öffentlichen Unternehmen als Betreiber kritischer Infrastrukturen und der Staatsverwaltung an sich. Gemeinsam mit den BayernLabs existiert ein Beratungsangebot für Bürgerinnen und Bürger in allen Teilen Bayerns.

Landesbehörden für Verfassungsschutz (LfV)

In sechs Bundesländern ist der Verfassungsschutz als Landesamt organisiert, in den restlichen Bundesländern übernehmen diese Aufgaben eine spezialisierte Abteilung eines jeweiligen Landesinnenministeriums. Zum Aufgabenbereich der LfV gehört neben Spionageabwehr, Wirtschaftsschutz und Terrorismusbekämpfung auch die Cyberabwehr.

Sicherheitszentrum IT der Finanzverwaltung Baden-Württembergs (SITiF BW) *stm.baden-wuerttemberg.de*

Das Sicherheitszentrum IT der Finanzverwaltung Baden-Württembergs hat im Jahr 2020 seine Arbeit aufgenommen. In dieser Einrichtung bündelt das Land Baden-Württemberg IT-Sicherheitsaufgaben, sie ist für die IT-Sicherheit der Finanzämter, der Oberfinanzdirektion, der Landesoberkasse, des Statistischen Landesamtes, des Landesamts für Besoldung und Versorgung und des Landesbetriebs Vermögen und Bau zuständig.

Mitarbeiter überwachen alle Systeme permanent, um Auffälligkeiten schnell erkennen und reagieren zu können. Außerdem soll mit Penetrationstest und Audits die IT-Infrastruktur regelmäßig auf Schwachstellen untersucht werden. Einen weiteren Schwerpunkt stellen die Schulung und Sensibilisierung der Beschäftigten dar. Dazu sind kurzfristig E-Learning-Einheiten und mittelfristig auch Präsenzveranstaltungen vorgesehen. SITiF soll außerdem an sämtlichen IT-Projekten der Finanzverwaltung beteiligt werden. So sollen Sicherheitsvorgaben von vornherein berücksichtigt werden.

Das Sicherheitszentrum IT ist Teil des Landeszentrums für Datenverarbeitung (LZfD) der Oberfinanzdirektion Karlsruhe. Bundesweit nimmt Baden-Württemberg mit dem SITiF eine Vorreiterrolle ein.

Spezialisierte Einrichtungen der Justiz

Deutschlandweit existieren diverse Einrichtungen des Justizsystems, die sich speziell mit der Verfolgung von Straftaten im Cyberspace beschäftigen. Oft übernehmen spezialisierte Staatsanwaltschaften zentral die Strafverfolgung von Straftaten im Internet. Zusätzlich zu den spezialisierten Staatsanwaltschaften übernehmen die nachfolgenden Stellen weitere besondere Aufgaben:

Die Zentralstelle Cybercrime Bayern (ZCB) zur Bekämpfung der Informations- und Kommunikationskriminalität als Einrichtung der Bayerischen Justiz dient dazu, aktuelle Entwicklungen im Bereich der IKT zu sichten, auszuwerten und die Staatsanwaltschaften regelmäßig darüber zu informieren. Die ZCB ist bei der Generalstaatsanwaltschaft Bamberg angesiedelt. Auch die konzeptionelle Planung und Durchführung von Fortbildungsveranstaltungen gehören zu den Tätigkeiten der Zentralstelle. Neue Ermittlungsinstrumente aus dem Bereich der Informations- und Kommunikationstechnologien prüft sie dahingehend, ob sie in rechtlicher Hinsicht für die Strafverfolgung nutzbar gemacht werden können. Zentralstellen sind in der Generalstaatsanwaltschaft angesiedelt.

Die Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität (ZIT) der Staatsanwaltschaft Hessen wurde 2010 als Außenstelle der Generalstaatsanwaltschaft Frankfurt am Main errichtet. Die ZIT ist erster Ansprechpartner des Bundeskriminalamtes für Internetstraftaten bei noch ungeklärter örtlicher Zuständigkeit in Deutschland oder bei Massenverfahren gegen eine Vielzahl von Tatverdächtigen bundesweit. Als operative Zentralstelle bearbeitet die ZIT besonders aufwendige und umfangreiche Ermittlungsverfahren aus den Deliktsbereichen:

- Kinderpornographie und sexueller Missbrauch von Kindern mit Bezug zum Internet,
- Darknet-Kriminalität (Bekämpfung krimineller Darknet-Plattformen sowie des Handels mit Waffen, Drogen und Fälschungsgütern im Darknet),
- Cyberkriminalität im engeren Sinne (Hackerangriffe, Datendiebstahl und Computerbetrug).

Die ZIT ist darüber hinaus für Aus- und Fortbildung von Richtern, Staatsanwälten und Polizeibeamten zuständig und ist zudem Gründungsmitglied im Judicial Cybercrime Network, einem europäischen Netzwerk der Justizbehörden zur Bekämpfung der Internetkriminalität.

Das Land Mecklenburg-Vorpommern hat eine eigene Schwerpunktstaatsanwaltschaft für die Bekämpfung der Informations- und Kommunikationskriminalität in Rostock eingerichtet.

Die Staatsanwaltschaft Saarbrücken im Saarland verfügt über ein Sonderdezernat für „Cybercrime“, um der Kriminalität im Netz zu begegnen. Das Dezernat wird in Zusammenarbeit mit dem Institut für Rechtsinformatik der Universität des Saarlandes und dem CISPA (siehe hierzu den Steckbrief) speziell geschult.

Mit der Zentralstelle Cybercrime Sachsen (ZCS) geht die sächsische Justiz gegen Internetkriminelle vor. Die Expertinnen und Experten der ZCS sind als Berater und Koordinierungsstelle für Ermittler zuständig, die sich mit Internetkriminalität befassen. Zudem übernimmt sie die Aus- und Fortbildung der sächsischen Staatsanwältinnen und -anwälte auf diesem Gebiet. Nur einzelne herausgehobene Verfahren, die sich etwa mit der inneren und äußeren Sicherheit in Deutschland beschäftigen, werden von der ZCS selbst geführt. Neben der Internetkriminalität wie Abzocke und Betrug, Ausspähen oder Sabotage soll sich die Zentralstelle auch um Fälle von Hetze und Bedrohungen im Netz kümmern. Die Zentralstelle kooperiert eng mit dem sächsischen Cybercrime Competence Center (SN4C).

6.4.2 Initiativen der Länder

CyberSecurity Verbund Sachsen-Anhalt *clsa.de*

Der „CyberSecurity Verbund Sachsen-Anhalt“ ist eine gemeinsame Forschungsinitiative der Hoch-schule Harz, der Martin-Luther-Universität Halle-Wittenberg und der Otto-von-Guericke-Universität Magdeburg. Das Gemeinschaftsprojekt wird vom Land Sachsen-Anhalt im Rahmen der Digitalen Agenda sowie über den Europäischen Fonds für regionale Entwicklung gefördert und ist Teil der Digitalisierungsstrategie des Landes. Im Rahmen des Projekts sollen Softwarelösungen im Bereich der IT-Sicherheit für kleine und mittlere Unternehmen sowie öffentliche Einrichtungen im Bundesland Sachsen-Anhalt entwickelt werden. Gemeinsam mit Unternehmen analysieren die beteiligten Hochschulen dazu vorangegangene Cyberangriffe und forschen zu innovativen Lösungen, um solche Angriffe zukünftig zu verhindern.

Deutsches Maritimes Zentrum e.V. *dmz-maritim.de*

Das Deutsche Maritime Zentrum ist ein branchenübergreifender Thinktank mit Sitz in Hamburg, der maritime Querschnittsthemen bearbeitet und koordiniert sowie als Bindeglied zwischen Wirtschaft, Wissenschaft und öffentlicher Hand fungiert. Zu den Mitgliedern des Vereins gehören der Bund (vertreten durch das BMVI) als maßgeblicher Finanzierer, fünf Bundesländer und die großen maritimen Verbände.
Um die Position der deutschen maritimen Wirtschaft nachhaltig zu stärken, sind neue Technologien u.a. aus dem Bereich der Sicherheitssysteme notwendig. Hierbei unterstützt das Deutsche Maritime Zentrum mit der Durchführung von Studien und Analysen zu den Kernthemen Blockchain, Big Data, KI-Anwendungen für die maritime Wirtschaft und autonome Schifffahrt.

Digitalbonus Bayern *digitalbonus.bayern*

Mit dem Förderprogramm Digitalbonus Bayern unterstützt das Bayerische Staatsministerium für Wirtschaft, Landesentwicklung und Energie KMU in Bayern bei der digitalen Transformation. Im Mittelpunkt der Förderung stehen digitale Produkte, Prozesse und Dienstleistungen sowie die Einführung und Verbesserung der IT-Sicherheit. Der Digitalbonus Bayern ist Bestandteil der bayerischen Strategie BAYERN DIGITAL.

Digitale Wirtschaft Schleswig-Holstein (DiWiSH) - Servicepoint Cybersecurity *servicepoint-cybersecurity.de*

Mit insgesamt über 200 Mitgliedern ist die Digitale Wirtschaft Schleswig-Holstein (DiWiSH) das größte Branchennetzwerk für alle kleinen und mittelständischen Unternehmen der IT- und Medienwirtschaft der Region zwischen Nord- und Ostsee. DiWiSH wird teilfinanziert aus Mitteln des Landes Schleswig-Holstein. Der Servicepoint Cybersecurity, betrieben durch die Arbeitsgruppe IT-Security der DiWiSH, dient der Wirtschaft in Schleswig-Holstein als zentrale Anlaufstelle, um Beratung und akute Hilfe zur Prävention und Reaktion bei Cyberangriffen zu erhalten. Jede Anfrage an den Servicepoint wird vertraulich behandelt und entsprechend spezialisierten Cybersecurity-Unternehmen anonymisiert zur Verfügung gestellt, um deren Unterstützungsangebote anzufragen. Diese werden über den Servicepoint dem anfragenden Unternehmen zugeleitet, das somit schnell und unabhängig Lösungsvorschläge bzw. Hinweise zur weiteren Vorgehensweise erhält.

Initiative Sicheres Internet (ISInet) *netzverweis.de*
Kampagne Netzverweis-gemeinsam gegen Internetkriminalität

Mecklenburg-Vorpommern setzt seit dem Jahr 2001 mit der „Initiative Sicheres Internet (ISInet)“ ein deutliches Zeichen gegen Internetkriminalität. Gründungsmitglieder sind das Landeskriminalamt Mecklenburg-Vorpommern und die DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH, deren Gesellschafter das Land Mecklenburg-Vorpommern ist.
Mit der aktuellen Kampagne NETZVERWEIS ruft die Initiative dazu auf, kriminelle Inhalte und Handlungen im Internet nicht länger zu tolerieren und sich interaktiv illegale Handlungen im Internet zur Wehr zu setzen. Zu diesem Zweck hat die ISInet eine Online-Meldestelle eingerichtet. Alle hier eingehenden Hinweise zum Thema Internetkriminalität werden geprüft - auch die anonymen. Gemeldete Inhalte werden von Spezialisten des Landeskriminalamtes Mecklenburg-Vorpommern bearbeitet und bei Verdachtsbestätigung verfolgt. Mit NETZVERWEIS soll der präventive Ansatz weiter verstärkt werden. Ziel ist es, die Bevölkerung des Landes Mecklenburg-Vorpommern über die Gefahren

im Internet aufzuklären, die Internetnutzer für einen sicherheitsbewussten Umgang zu sensibilisieren und für Qualitätskriterien in Verbindung mit dem Angebot kommerzieller Inhalte zu werben. Die Schirmherrschaft über die Kampagne hat das Ministerium für Inneres und Sport Mecklenburg-Vorpommern.

Maritimes Cluster Norddeutschland e. V. (MCN) *maritimes-cluster.de*

Das Maritime Cluster stellt eine länderübergreifende Kooperation als Netzwerk für die maritime Wirtschaft als Schlüsselbranche im Norden dar. Themenfelder aus dem Bereich Cybersicherheit sind: Blockchain für Frachtpapiere, Maritime Sicherheit, autonome Schiffe und Schutz der maritimen (Hafen-) Infrastruktur. Ziel der Fachgruppe "maritime Sicherheit" ist es unter anderem, Themen und zukünftige Hotspots im Bereich maritime Sicherheit zu identifizieren sowie innovative Projekte zu initiieren. Die Länder Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachen und Schleswig-Holstein unterstützen die Clusterbildung der maritimen Branche länderübergreifend durch das Maritime Cluster Norddeutschland. Eingebettet ist dies im Nationalen Masterplan Maritime Technologien (NMMT) der Bundesregierung.

Sicherheitspartnerschaften der Länder

Als wirksames Mittel für den dauerhaften Erhalt und die Steigerung der Sicherheitsstandards informiert die Sicherheitspartnerschaft u.a. zur Gefährdung durch Wirtschaftsspionage, Wirtschaftskriminalität sowie IT-Sicherheit und sensibilisiert im Rahmen von Fachtagungen, öffentliche Veranstaltungen zu aktuellen Entwicklungen und unternehmensbezogenen Gegenstrategien. In insgesamt acht Bundesländern existieren Sicherheitspartnerschaften oder ähnliche Initiativen:

- Sicherheitsforum Baden-Württemberg
- Sicherheitspartnerschaft Berlin
- Arbeitskreis für Unternehmenssicherheit Brandenburg (AKUS)
- Kooperation gegen Wirtschaftskriminalität und Wirtschaftsspionage Hamburg
- Sicherheitspartnerschaft Mecklenburg-Vorpommern
- Sicherheitspartnerschaft gegen Wirtschaftskriminalität Niedersachsen
- Kooperation gegen Wirtschaftsspionage und Wirtschaftskriminalität Nordrhein-Westfalen
- Sicherheitspartnerschaft Rheinland-Pfalz

Zentrum Digitalisierung.Bayern (ZD.B) *zentrum-digitalisierung.bayern*

Das Zentrum Digitalisierung.Bayern (ZD.B) vernetzt etablierte bayerische Unternehmen und Gründerinnen und Gründer, Hochschulen sowie außeruniversitäre Forschungseinrichtungen im Rahmen interdisziplinärer Themenplattformen sowie durch Maßnahmen zur Innovations-, Nachwuchs und Gründungsförderung und koordiniert die bayernweiten Maßnahmen. Das ZD.B betreibt eine Themenplattform Cybersecurity zu deren Projekten gehört die Organisation und Fortentwicklung des Sicherheitsnetzwerks München im Auftrag des Bayerischen Staatsministeriums für Wirtschaft und Medien, Energie und Technologie (siehe unten). Das Sicherheitsnetzwerk München ist an das Zentrum Digitalisierung.Bayern angegliedert und dient der Vernetzung von IT-Sicherheitsunternehmen und Forschungseinrichtungen mit dem Ziel des Wissenstransfers innerhalb der Mitglieder und nach außen. Im Rahmen des Sicherheitsnetzwerkes werden Forschungsprojekte initiiert und durchgeführt. Das Netzwerk dient dem Aufbau von Kontakten zu Partnern und arbeitet über diverse Arbeitskreise mit direktem Bezug zu Cybersicherheitsthemen, insbesondere zu den Themen Sichere Industrie 4.0, Services für KMU, Sichere Smart Grids, Smart Data, Bewertung von Cyberrisiken und Krisenmanagement, Internet der Dinge.

7 Verbände und Interessenvertretung

Der Zusammenschluss natürlicher und juristischer Personen zur Verfolgung gemeinsamer Interessen hat in Deutschland eine lange Tradition. Obgleich sich die Verbandsthemen, die verfolgten Interessen und Ziele sowie die Mitgliederherkunft oft stark unterscheiden, sind die Verbände in Themen mit gesamtgesellschaftlicher Relevanz vereint. Cybersicherheit ist solch ein Thema, unabhängig von Branche oder Couleur. Fast jeder Verband oder Interessenvertretung ist im Bereich der Cybersicherheit aktiv, ob nur im Innenverhältnis oder öffentlichkeitswirksam nach außen.

Im Zuge der Recherchen im Rahmen des NPCS und in der Erstellung dieses Kompendiums wurden 34 Organisationen mit Verbandscharakter identifiziert, welche sich besonders im Bereich der Cybersicherheit engagieren und damit einen wichtigen Beitrag zur Stärkung der Cybersicherheit in Deutschland leisten. Gerade die Diversität der thematischen Hintergründe der vielen Verbände hilft, Cybersicherheit mit all seinen Facetten und Perspektiven gesamtgesellschaftlich zu begreifen.

Bundesverband der Deutschen Luft- und Raumfahrtindustrie e.V. (BDLI) *Wirtschaftlicher Akteur*

Der BDLI unterstützt durch seinen Fachausschuss Cybersicherheit alle BDLI-Mitglieder zum Themenkomplex Cybersicherheit. Durch die Bündelung der Kompetenzen des durch den Verband entstehenden Netzwerkes bietet der BDLI einiges an Knowhow im Bereich der Absicherung von cyber-physischen Systemen.

Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (BvD) *Wirtschaftlicher Akteur*

Der BvD vertritt die Anliegen betrieblicher und behördlicher Datenschutzbeauftragter sowie Beraterinnen und Beratern und bringt sich in diesem Zuge auch bei der Förderung von mehr Cybersicherheit im öffentlichen Diskurs ein. Des Weiteren engagiert sich der BvD für die Steigerung der Cybersicherheitsawareness in der Zivilgesellschaft. Im Rahmen der Initiative „Datenschutz geht zur Schule“ bspw. führen Dozentinnen und Dozenten des BvD am Safer Internet Day 2019 bundesweit Sensibilisierungsveranstaltungen für Schülerinnen und Schüler der Sekundarstufen I und II an Berufsschulen durch. Dabei wird unter anderem zu den Themen Passwortschutz, soziale Netzwerke und Selbstdarstellung im Netz aufgeklärt.

Blockchain Bundesverband e.V. *Wirtschaftlicher Akteur*

Der Blockchain Bundesverband vertritt die Interessen der deutschen Blockchain Community. Die Arbeit des Vereins basiert auf der Überzeugung, dass Blockchain und ähnliche dezentrale Technologien auf Basis von Kryptographie für die Innovation digitaler Infrastrukturen von grundlegender Bedeutung sind. Aus diesem Grund arbeitet der Verband an der Bildung sowohl von Entscheidungsträgern in der Politik und branchenführenden Unternehmen als auch der breiten Öffentlichkeit, um die notwendige rechtliche sowie gesellschaftliche Anerkennung der Technologie zu schaffen.

Bundesverband der Deutschen Industrie e.V. (BDI) *Wirtschaftlicher Akteur*

Der BDI ist die Dachorganisation der deutschen Industrie und der industrienahen Dienstleister und ist für die Wahrnehmung und Förderung aller Anliegen der zusammengeschlossenen Industriezweige verantwortlich. Im Bereich der Cybersicherheit bringt sich der Bundesverband der Deutschen Industrie (BDI) in der Gruppe der B20 (Wirtschaftsdialog der G20-Mitglieder) für die Themen freie Datenflüsse, internationale Cybersicherheitskooperation und ein Künstliche Intelligenz-Ökosystem ein. Zusammen mit dem BMI engagiert sich der BDI im Bündnis für Cybersicherheit zwischen Staat und Wirtschaft für Cybersicherheit als Gemeinschaftsaufgabe von Unternehmen und Staat.

Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e.V. (BDSV) *Wirtschaftlicher Akteur*

Der BDSV ist die Interessenvertretung der deutschen Sicherheits- und Verteidigungsindustrie und verknüpft in einem Ausschuss "Digitale Konvergenz" die Verteidigungsindustrie mit der Cybersicherheitsindustrie. Der Verband stärkt mit seinen Aktivitäten das Bewusstsein für Zukunftstechnologien, aber auch damit verbundene Herausforderungen, bei Kunden, Politik, Gesellschaft und seinen Mitgliedern. Der BDSV veröffentlicht hierzu verschiedene Informationsangebote.

Bundesverband der Energie- und Wasserwirtschaft e.V. (BDEW) *Wirtschaftlicher Akteur*

Der BDEW vertritt ca. 1.900 Unternehmen der Sektoren Energie und Wasser/Abwasser in Deutschland, darunter ca. 900 Betreiber Kritischer Infrastrukturen. Im BDEW sind lokale, kommunale, regionale und überregionale Unternehmen vertreten. Der BDEW ist hierbei auch Ansprechpartner und Vertreter dieser Branchen in der öffentlich-privaten Zusammenarbeit UP KRITIS und hat für KRITIS-Betreiber u.a. auch vom BSI eignungsgeprüfte branchenspezifische Sicherheitsstandards nach BSI-Gesetzt erarbeitet und veröffentlicht.

Bundesverband der IT-Anwender e.V. *Wirtschaftlicher Akteur*

Der Bundesverband der IT-Anwender e.V. tritt als Interessenvertreter für IT-Entscheiderinnen und -Entscheider verschiedener Unternehmen auf. Ziel des Netzwerks ist der Austausch zu Themen der Digitalisierung und die Interessenvertretung der Anwender sowohl gegenüber der Politik als auch der Anbieter. Verschiedene Special Interest Groups beschäftigen sich mit Themen der IT-Sicherheit. Im Rahmen eines Cyber Security Competence Centers tauschen sich Unternehmen zu Best Practices in der Cybersicherheit aus.

Bundesverband Deutsche Startups e.V. *Wirtschaftlicher Akteur*

Der Bundesverband Deutsche Startups e.V. repräsentiert die Interessen der Startups in Deutschland und dient als Netzwerk für Gründer, Startups und Unterstützer. Der Verband betreibt eine "Cyber Security Plattform" mit dem Ziel, Startups sowie etablierte Unternehmen der Cybersicherheitsbranche miteinander zu vernetzen, um so den Austausch über aktuelle Herausforderungen, Erfahrungen und Fachkenntnisse zu fördern. Die Mitglieder der Plattform arbeiten dazu an der Erstellung themenspezifischer Inhalte, gemeinsamer Projekte und organisieren darüber hinaus Veranstaltungen und Webinare.

Bundesverband deutscher Banken e.V. (Bankenverband) *Wirtschaftlicher Akteur*

Der Bankenverband vertritt als Stimme der privaten Finanzwirtschaft die Interessen des privaten Kreditgewerbes und vermittelt zwischen den Interessen der privaten Banken, Politik, Verwaltung, Verbraucherinnen und Verbraucher und Wirtschaft. Er ist in dieser Funktion auch Multiplikator für den Bankensektor in Fragen der Cybersicherheit. Für seine Mitglieder wirkt er vor allem bei der Entwicklung und Adaption von Cybersicherheitsstandards im Bankwesen konzeptionell mit.

Bundesverband für den Schutz Kritischer Infrastrukturen e.V. (BSKI) *Wirtschaftlicher Akteur*

Der BSKI ist eine Anlaufstelle für Betreiber Kritischer Infrastrukturen, um ganzheitliche Schutzkonzepte zu etablieren. Die Aufgabe des BSKI ist es, Sicherheitsrisiken für kritische Infrastrukturen und deren Zulieferer frühzeitig zu erkennen und durch gezielte Konzepte für „Prävention, Reaktion und Postvention“ zu reduzieren. Dabei werden hohe Schutzziele (technisch, organisatorisch, persönlich) für kritische Infrastrukturen verfolgt. Neben dem Initiieren von Forschungsprojekten wird der Dialog mit Wissenschaft und Politik forciert. Durch gezielte Schulungsprogramme, Publikationen und Veranstaltungen werden die Mitglieder für mögliche Risiken in ihren Infrastrukturen sensibilisiert. Durch die Zusammenarbeit mit Branchenexperten und zuständigen Behörden kann der BSKI kritische Infrastrukturen auch beratend unterstützen.

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom) *Wirtschaftlicher Akteur*

Der Bitkom, als Branchenverband der deutschen Informations- und Telekommunikationsbranche, beschäftigt sich mit der Förderung und Entwicklung von Märkten dieser Branche, auch im Themenbereich der Cybersicherheit. Der Bitkom dient als Akteur bei der Vernetzung von relevanten Anbietern sowie als Impulsgeber innerhalb der IuK-Branche und setzt sich für die Verbesserung wirtschaftlicher und auch politischer Rahmenbedingungen in Deutschland ein. Vorrangig engagiert sich der Bitkom für mittelständische und große Unternehmen im Internet- und Telekommunikationsbereich. Die Themen von Bitkom sind neben Cybersicherheit u.a. digitale Transformation, Modernisierung des Bildungswesens, Industrie 4.0 und Netzpolitik.

Bundesverband IT-Mittelstand e.V. (BITMi) *Wirtschaftlicher Akteur*

Der BITMi ist ein IT-Fachverband, der die Interessen mittelständischer IT-Unternehmen vertritt. Der BITMi fördert dabei die Vernetzung von Mitgliedern sowie den Zusammenschluss dieser. Die Förderung von Unternehmenswachstum und die Stärkung des Standorts Deutschland wird durch Netzwerkbildung u.a. durch eine Kooperation mit dem Bundeswirtschaftsministerium oder der Beteiligung an internationalen, nationalen und lokalen Projekten vorangetrieben. Der Verband ist zudem Mitglied im Digital-SME und vertritt seine Mitglieder damit auch auf europäischer Ebene. Themenschwerpunkte, die u.a. in Fachgruppen von Mitgliedern bearbeitet werden, sind bspw. IT-Sicherheit oder das Internet der Dinge.

Bundesverband IT-Sicherheit e.V. (TeleTrusT) *Gesamtgesellschaftlicher Akteur*

Der TeleTrusT verbindet als Kompetenzverbund nationale und internationale Mitglieder aus Wirtschaft, Staat und Wissenschaft sowie thematisch ähnliche Partnerorganisationen mit dem Ziel der Förderung der Sicherheit und Vertrauenswürdigkeit von Informations- und Kommunikationstechnik. Hierzu organisiert das Netzwerk Veranstaltungen, Arbeitsgruppen, Foren für Experten oder veröffentlicht Stellungnahmen zu aktuellen IT-Sicherheitsthemen zur Steigerung des Informationsaustauschs. Unter anderem wird mit dem Vertrauenssiegel "IT Security made in Germany" (ITSMIG) eine gemeinsame Außendarstellung der in der Arbeitsgruppe aktiven Unternehmen angestrebt. Das Netzwerk umfasst über 340 Mitgliedunternehmen (Stand Dezember 2019) sowie -institutionen aus unterschiedlichen Bereichen.

Bundesverband mittelständische Wirtschaft, Unternehmerverband Deutschlands e.V. (BVMW) *Wirtschaftlicher Akteur*

Der BVMW ist die Interessenvertretung des deutschen Mittelstands und ist mit einem Arbeitskreis IT-Sicherheit im Bereich Cybersicherheit aktiv. Der Arbeitskreis IT-Sicherheit verfolgt das Ziel, das Bewusstsein für IT-Sicherheit im Mittelstand zu stärken. Außerdem setzt er sich für eine steuerliche Bevorteilung von Investitionen in IT-Sicherheit und die Verhinderung einer Überregulierung durch Behörden zu IT-Sicherheitsstandards ein. Der Arbeitskreis besteht aus mehreren Experten und veröffentlicht regelmäßig Stellungnahmen und Ratgeber.

Deutsche Gesellschaft für Qualität e.V. (DGQ) *Wirtschaftlicher Akteur*

Die DGQ ist ein Qualitätsmanagement-Netzwerk Deutschlands. Einer der Themenblöcke, mit denen sich dieses Netzwerk auseinandersetzt, ist Cybersicherheit im Kontext der Feststellung von Qualität und des Managements dieser. Durch Fachbeiträge der einzelnen Fachgruppen leistet die Gesellschaft einen wichtigen Informationsbeitrag.

Deutsche Krankenhausgesellschaft e.V. (DKG) *Wirtschaftlicher Akteur*

Die DKG vertritt als Bundesverband 28 Mitgliedverbände von Krankenhausträgern und steht für deren Interessen, auch im Rahmen der Cybersicherheit, ein. Die DKG bezieht für ihre Mitglieder vor allem im Bereich der Absicherung von Krankenhaussystemen gegen Cyberangriffe für ihre Mitgliedverbände und deren Mitglieder Stellung.

Deutscher Industrie- und Handelskammertag e.V. (DIHK) *Wirtschaftlicher Akteur*

Der DIHK übernimmt als Dachorganisation im Auftrag und in Abstimmung mit den Industrie- und Handelskammern (IHKs) die Interessenvertretung der gewerblichen deutschen Wirtschaft gegenüber den Entscheidern der Bundespolitik und den europäischen Institutionen. Die IHKs unterstützen die Unternehmen vor-Ort, während Regelungen im politischen Rahmen durch den DIHK übernommen werden. Cybersicherheit gehört zu den Themen, in denen der DIHK die gewerbliche Wirtschaft vertritt. Der DIHK ist im Bereich der Daten- und Informationssicherheit aktiv und veröffentlicht Positionspapiere und Praxisleitfäden, die konkrete Anregungen und Tipps zur Datensicherheit enthalten. Darüber hinaus ist der DIHK zusammen mit den IHKs und DsiN an der Workshop-Reihe "IT-Sicherheit @ Mittelstand" beteiligt, die Möglichkeiten zur Vermeidung von Cyberattacken vermitteln soll. Außerdem ist der DIHK in der Allianz für Cyber-Sicherheit (ACS) im Fachbeirat tätig.

eco – Verband der Internetwirtschaft e.V. *Wirtschaftlicher Akteur*

Der Verband der Internetwirtschaft ist die Interessenvertretung von Unternehmen, deren Absatzmarkt überwiegend das Internet ist bzw. die sich aktiv an der Internetwirtschaft betätigen. Verbandszweck ist die Förderung neuer Technologien im Rahmen des Branchenschwerpunktes sowie seine Mitglieder gegenüber nationaler und internationaler Politik und Gremienarbeit zu vertreten, um somit die Rahmenbedingungen der Internetwirtschaft aktiv mitzugestalten. Auch im Rahmen der Cybersicherheit ist der Verband aktiv. So beschäftigt er sich bspw. in einer dedizierten Kompetenzgruppe "Sicherheit" mit Themen der Sicherheit von IT-Infrastrukturen der Internetwirtschaft. Die Arbeitsgruppe veröffentlicht hierzu bspw. Positionspapiere, beantwortet zentrale Fragen zur IT-Sicherheit oder organisiert Veranstaltungen.

Fachverband Informationstechnologie in Sozialwirtschaft und Sozialverwaltung e.V. (FINSOZ) *Wirtschaftlicher Akteur*

FINSOZ ist ein Verband aus dem Bereich der Sozialwirtschaft und -verwaltung, welcher die Interessen der Branche und deren IT-Anbieter im Bereich der aktiven Nutzung digitaler Technologien gegenüber Politik, Kostenträgern und Akteuren angrenzender Bereiche vertritt. Zudem bietet er seinen Mitgliedern eine branchenweite Plattform zum Erwerb von Qualifikationen und zur Vernetzung an. FINSOZ bietet eigene Seminare und Foren sowie die Zusammenarbeit in Arbeitskreisen an. Außerdem erstellt FINSOZ Positionspapiere. Im Bereich der Cybersicherheit ist FINSOZ, neben der themenbezogenen Interessenvertretung, aktiv in der Vernetzung und der Schaffung verbandsspezifischer Qualifikationsangebote tätig.

Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV) *Wirtschaftlicher Akteur*

Der GDV ist der Dachverband der privaten Versicherungsunternehmen in Deutschland, welcher zum einen als Dienstleister seiner Mitglieder fungiert, bspw. bei der Entwicklung von Musterbedingungen für verschiedene Versicherungsspaten, aber auch die Interessen der deutschen Versicherungswirtschaft gegenüber Gesellschaft und Politik vertritt. Cybersicherheit spielt für den GDV eine besondere Rolle. Der GDV verfolgt mit der Initiative CyberSicher das Ziel, KMU für IT-Sicherheit zu sensibilisieren aber auch die Rahmenbedingungen für einen Versicherungsschutz im Falle von Cyberangriffen zu gestalten. Auch setzt der GDV sich für Cybersicherheit und Standards in der Versicherungsbranche ein.

Gesellschaft für Informatik e.V. (GI) *Wirtschaftlicher Akteur*

Mit verschiedenen Fachbereichen, Regional- und Fachgruppen ist die GI Plattform und Sprachrohr für alle Disziplinen in der Informatik. Die GI vertritt auch im Bereich der Cybersicherheit die Positionen ihrer Mitglieder und befasst sich aktiv im Fachbereich Sicherheit mit dieser Thematik, welcher mehr als zehn Fachgruppen umfasst, die sich mit dem Thema Cyber- und IT-Sicherheit auseinandersetzen. Durch die Einbindung fachfremder Themen und Gruppen sollen sowohl gesellschaftliche als auch wissenschaftliche Bedürfnisse des Querschnittthemas Sicherheit erfüllt werden können. Neben der Forschung kommt daher der Vernetzung der Wissenschaft, Wirtschaft und Gesellschaft sowie der Zusammenarbeit mit anderen Hochschulen und Forschungseinrichtungen eine hohe Bedeutung zu.

Handelsverband Deutschland e.V. (HDE) *Wirtschaftlicher Akteur*

Der HDE stellt das Sprachrohr der Einzelhandelsbranche gegenüber der Politik auf Bundes- und EU-Ebene, gegenüber anderen Wirtschaftsbereichen, den Medien und der Öffentlichkeit dar. Zu den Schwerpunktthemen des HDE gehört die Sensibilisierung des Mittelstandes für das Thema IT-Sicherheit. Der HDE greift im Sinne seiner Mitglieder für die Gesellschaft relevante Themen (Datenschutz im Handel, sichere Lieferketten und sicherer Zahlungsverkehr) auf und kooperiert bei Cyberthemen mit dem BSI.

ISACA Germany Chapter e.V. *Wirtschaftlicher Akteur*

Das Germany Chapter von ISACA ist ein deutscher Berufsverband von IT-Revisoren, IT-Sicherheitsmanagern und IT-Governance-Experten. Der Verein leistet durch den Austausch und die Förderung von Fachwissen sowie durch die Schaffung von Standards einen Beitrag zur Cybersicherheit in Deutschland.

Microsoft Business User Forum e.V. *Gesamtgesellschaftlicher Akteur*

Das Microsoft Business User Forum e.V. ist eine Anwendergemeinschaft von Firmen, Organisationen und Einrichtungen der öffentlichen Verwaltung. Die Gemeinschaft ist im Dialog mit dem Hersteller Microsoft, um diesen für die Anforderungen großer Firmen zu sensibilisieren und durch den direkten Kontakt Optimierungen der Produkte zu erreichen. Kern der Anwendergemeinschaft sind die Arbeitsgruppen. Die Arbeitsgruppe "IT-Security-Management" formuliert aus den konkreten Erfahrungen von Großunternehmen heraus Sicherheitsanforderungen an Microsoft und treibt die Entwicklung von Sicherheitsfunktionen, die im deutschen Markt und Rechtsraum von besonderer Bedeutung sind, mit an. Die Arbeitsgruppe leistet einen Beitrag zur Cybersicherheit, da sie darauf achtet, dass die Anforderungen entsprechender Sicherheitsstandards von Microsoft-Produkten erfüllt werden. Die Arbeitsgruppe fungiert ebenfalls als Netzwerk, über das Frühwarnungen zu Sicherheitslücken und Hilfestellungen bei der Behebung von Sicherheitslücken frühzeitig kommuniziert werden.

Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V. (NAMUR) *Wirtschaftlicher Akteur*

Die NAMUR ist ein internationaler Verband zur Interessenvertretung von Anwenderunternehmen der Prozessindustrie im Bereich der Automationstechnik. Die NAMUR pflegt die Zusammenarbeit mit internationalen und nationalen Betreiberverbänden und ist aktiv in bereichsspezifischen Normungsgremien. Die NAMUR setzt sich im Arbeitskreis Automation Security für die Harmonisierung von Standards und Normen der Cybersicherheit in der Prozessautomatisierung ein und erarbeitet hierbei Leitfäden, Prüflinien und andere Hilfsmittel. Außerdem unterstützt der Arbeitskreis Automation Security andere Gremien und fördert den Erfahrungsaustausch zwischen Akteuren.

Verband der Elektrotechnik Elektronik Informationstechnik e.V. (VDE) *Wirtschaftlicher Akteur*

Der VDE ist ein technisch-wissenschaftlicher Verband, welcher Wissenschaft, Standardisierung, Prüfung, Zertifizierung und Anwendungsberatung im technologischen Kontext als Verbandszweck vereint. Neben Themen wie Energy, Mobility oder Smart Cities beschäftigt sich der VDE auch intensiv mit Cybersicherheit. Dazu zählen neben dem Kompetenzzentrum "Digitale Sicherheit" für Informations- und Unternehmenssicherheit auch Tätigkeiten in der Prüfung und Zertifizierung, die Durchführung von Forschungsprojekten, Normung und Standardisierung im Bereich der Cybersicherheit sowie eine IT-Sicherheitsplattform für industrielle KMU. Auch betreibt der VDE eine Übersichtsplattform zu sicherheitsrelevanten Normen und Gesetzen und Informationen zu juristischen Rahmenbedingungen der Cybersecurity.

Verbraucherzentrale Bundesverband e.V. (vzbv) *Gesamtgesellschaftlicher Akteur*

Der vzbv engagiert sich für eine gerechte und nachhaltige Gesellschafts- und Wirtschaftsordnung, die die Bedürfnisse des Menschen in den Mittelpunkt rückt. Im Bereich der Cybersicherheit setzt sich der Verband insbesondere für Themen wie Schutz der Privatsphäre und das Recht auf diskriminierungsfreien und chancengleichen Zugang zu Netzen und Inhalten ein. Hierzu formuliert der Verband Forderungen und tritt als Interessenvertretung für die Verbraucher auf.

Verein Deutscher Ingenieure e.V. (VDI) *Akteur aus Wissenschaft und Wirtschaft*

Der VDI ist als technisch-wissenschaftlicher Verein die deutsche Interessenvertretung der in ihm organisierten Ingenieurinnen und Ingenieure sowie Naturwissenschaftlerinnen und -wissenschaftler. Im Bereich Cybersecurity betätigt der VDI sich mit der Veröffentlichung von Handlungsempfehlungen und Richtlinien oder der Organisation von Veranstaltungen. Zusätzlich werden Webinare, Beratungsdienstleistungen und Weiterbildungen angeboten. Der VDI bezieht Position gegenüber Politik und Gesellschaft, auch in Fragestellungen der Cybersicherheit.

Verband der Automobilindustrie e.V. (VDA) *Wirtschaftlicher Akteur*

Der VDA ist der gemeinsame Branchenverband der deutschen Automobilhersteller und Automobilzulieferer. Der VDA vertritt die Interessen der deutschen Automobilindustrie gegenüber Gesellschaft und Politik, engagiert sich aber auch für Technologieförderung in der Branche. Der VDA ist auch im Bereich der Cybersicherheit aktiv und betreibt einen Arbeitskreis, welcher auf Informations- und Cybersicherheit spezialisiert ist. Im Fokus steht der Erfahrungsaustausch der Mitglieder. Darüber hinaus wird sich mit anderen Themen des Bereichs wie bspw. Konsolidierung, Vereinheitlichung und Erhöhung der Cybersicherheit im Supply Chain Bereich der Automobilbranche oder in der Cybersicherheit im Kontext des autonomen Fahrens beschäftigt.

Verband der TÜV e.V. (VdTÜV) *Wirtschaftlicher Akteur*

Der VdTÜV ist die Interessenvertretung der Technischen Überwachungs-Vereine (TÜV) in Deutschland. Der Verband der TÜV repräsentiert die TÜV-Unternehmen und weitere Unternehmen, die als unabhängige Organisationen Prüfdienstleistungen erbringen. Der Verband erarbeitet Stellungnahmen zu EU-Richtlinien, Gesetzen, Verordnungen, Technischen Regeln (z. B. VdTÜV-Merkblätter) und Normen. Er berät Parlamente, Ministerien sowie öffentliche und private Organisationen auf nationaler und internationaler Ebene. Durch den von ihm organisierten Erfahrungsaustausch ist der VdTÜV ein wichtiger Ansprechpartner in allen Fragen der Technischen Sicherheit. Der VdTÜV engagiert sich für die Wahrung des hohen Sicherheitsniveaus, die Sicherheit neuer Technologien sowie die Sicherheit globaler Prozessketten durch Weiterentwicklung der Qualitäts- und Sicherheitsstandards. Die "Digitale Transformation" mit den Themengebieten Cybersicherheit, Datenschutz, Digitale Agenda und Industrie 4.0 gehört zu den Schwerpunktthemen des VdTÜV, für die er sich mit Positionen und Stellungnahmen gegenüber Wirtschaft und Politik stark macht.

Verband für unbemannte Luftfahrt e.V. (UAV DACH) *Zivilgesellschaftlicher Akteur*

Der Verband für unbemannte Luftfahrt e.V. liefert einen Beitrag zu Cybersicherheitsthemen, indem er Innovationen für die unbemannte Luftfahrt in Zusammenarbeit mit Forschungseinrichtungen und Herstellern fördert. Die Fachgruppe Informationssicherheit des Verbands arbeitet an Technologien, um die Schutzziele der Drohnendaten sicherzustellen. Die Fachgruppe Zertifizierung und Standard in der Luftfahrt arbeitet an der Erstellung von Normen und Standards für Systeme der unbemannten Luftfahrt. Der Verband ist eine anerkannte Stelle beim Luftfahrt-Bundesamt zur Erstellung von Gutachten und der Erteilung von Betriebserlaubnissen und Zulassungen unbemannter Luftfahrzeuge.

Verband kommunaler Unternehmen e.V. (VKU) *Akteur aus Wirtschaft und Staat*

Im VKU organisieren sich kommunale Unternehmen, um gegenüber der Landes- und Bundespolitik die eigenen Interessen zu vertreten. Die kommunalen Unternehmen dieses Interessenverbandes entstammen den Bereichen der Energie- und Wasserversorgung, Abwasserentsorgung, Abfallwirtschaft und Stadtreinigung sowie der Telekommunikation. Aufgrund der Systemrelevanz vieler Mitgliedsunternehmen ist Cybersicherheit für den VKU ein Kernthema, der zudem regelmäßig Veranstaltungen organisiert und den breiten Austausch innerhalb, aber auch außerhalb des Verbandes, fördert.

Zentralverband des Deutschen Handwerks e.V. (ZDH) *Wirtschaftlicher Akteur*

Der ZDH agiert als Interessenvertretung für die Handwerksbetriebe in Deutschland. Dabei ist der Verband auch im Bereich der Digitalen Sicherheit aktiv. Unter anderem wurde in Kooperation mit dem BSI ein IT-Grundschutz-Profil entwickelt, welches den Handwerksunternehmen als Routenplaner im Bereich Cybersicherheit dienen und als praktische Arbeitshilfe die Informationssicherheit der Betriebe erhöhen soll. Außerdem veröffentlicht der ZDH konkrete Handlungsempfehlungen und Leitfäden, bspw. zum Thema Datenschutz. Darüber hinaus ist der ZDH im Beirat der ACS aktiv.

Zentralverband Elektrotechnik- und Elektronikindustrie e.V. (ZVEI) *Wirtschaftlicher Akteur*

Der ZVEI ist ein Industrieverband, der die Interessen der Elektroindustrie national und international vertritt. Die Themenfelder sind insbesondere wirtschafts-, technologie- und umweltpolitische Belange der Mitglieder. Der Bereich Cybersicherheit gilt beim ZVEI als Querschnittsthema mit Fokus auf Anwender, Industrial Security sowie unternehmensübergreifende Infrastrukturen. Alle ZVEI-Leitmärkte (Industrie 4.0, Energie, Gebäude, Mobilität, Gesundheit) haben vor diesem Hintergrund Initiativen zur Cybersicherheit etabliert.

Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e.V. (ZKI) *Wissenschaftlicher Akteur*

Der ZKI ist die Vereinigung der IT-Servicezentren der Hochschulen, Universitäten und Forschungseinrichtungen in Deutschland. Vereinszweck ist die Förderung der Informationsverarbeitung in Lehre und Forschung in Hochschulen und überwiegend öffentlich geförderten Einrichtungen der Großforschung und der Forschungsförderung. Ein Leitthema des ZKI ist die Cybersicherheit, hierfür existiert ein eigener Arbeitskreis, welcher Konzeptpapiere, Stellungnahmen und Pressemitteilungen mit Bezug auf sicherheitsrelevante Ereignisse veröffentlicht. Auch hat das ZKI in Kooperation mit dem BSI das IT-Grundschutzprofil für Hochschulen erarbeitet.

8 Steckbriefe der Cyberakteure und -initiativen

Hinweise zur Vollständigkeit

Die vorliegenden Datenblätter basieren vorrangig auf öffentlichen Informationen der Online-Präsenzen der betreffenden Akteure und Initiativen. Ergänzt wurden diese um Informationen aus weiteren öffentlich zugänglichen Datenbanken. Zudem wurden Informationen aus den Stakeholder- und Multiplikatorengesprächen sowie aus dem direkten Austausch mit den relevanten Akteuren und Initiativen berücksichtigt. Auch bestand die Möglichkeit, potentiell kompendiumsrelevante Organisationen mithilfe eines Online-Formulars über die Webseite des NPCS zu melden, um somit auch relevante Akteure und Initiativen ins Kompendium aufnehmen zu können, die durch die definierten Suchmuster und anhand der zur Verfügung stehenden Informationsquellen nicht gefunden werden konnten. Trotz tiefergreifender Analysen und Recherchen sowie sorgfältiger Informationsaufnahme und -verarbeitung besteht die Möglichkeit, dass relevante Initiativen oder Akteure nicht im Kompendium aufgeführt sind, weshalb diesbezüglich kein Anspruch auf Vollständigkeit bestehen kann.

Das Kompendium Cybersicherheit Deutschland soll lediglich einen Überblick der prägnantesten Informationen zu den Akteuren und Initiativen mit Bezug zur Cyber- und Informationssicherheit, respektive zu deren Beitrag zur deutschen Cybersicherheitslandschaft geben. Daher stellen die dargebrachten Informationen nur einen Auszug eines teilweise sehr umfangreichen Portfolios dar.

Einzelne Akteure und Initiativen haben einer Veröffentlichung an dieser Stelle widersprochen.

Hinweise zur Aktualität

Die Recherche erfolgte im Zeitraum 1. März 2019 bis 31. Dezember 2019, Meldungen per Online-Formular wurden bis zum 28. Februar 2020 berücksichtigt. Da die Erfassung einem strukturierten Verarbeitungsprozess folgt und den systematischen Auswertungen ein einheitlicher Datenbezugspunkt zugrunde zu legen ist, konnten nachträgliche Ergänzungen bzw. Aktualisierungen der Daten der betrachteten Akteure und Initiativen keine Berücksichtigung finden.

Die Online-Fassung soll in einem noch zu definierenden Folgeprojekt fortgeschrieben werden.

8.1 Zivilgesellschaftliche Initiativen und Akteure

AG KRITIS

Beitrag zur Cybersicherheit

Die AG KRITIS ist eine unabhängige Arbeitsgruppe zur Erhöhung der Versorgungssicherheit der Bevölkerung. Mitglieder sind Einzelpersonen, die sich in verschiedenen Funktionen und Bereichen mit Kritischen Infrastrukturen gemäß BSI-Gesetz i. V. m. BSI-Kritisverordnung beschäftigen. Das Ziel ist, gemeinsam mit Politik, Wirtschaft, Wissenschaft und Zivilgesellschaft, eine nachhaltige Verbesserung der IT- und OT-Sicherheit und Resilienz von Kritischen Infrastrukturen zu erreichen. Die Arbeitsgruppe veröffentlicht Artikel, Stellungnahmen und politische Forderungen und stellt regelmäßig Referenten auf Konferenzen und Kongressen. Darüber hinaus wurde ein Konzept zur Steigerung der Bewältigungskapazitäten in Cyber-Großschadenslagen entwickelt, dessen Kernpunkt die Gründung eines „Cyber-Hilfswerks“ ist.

Kontakt:

Saarbrückener Str. 115

53117 Bonn

ag.kritis.info

Zivilgesellschaftliche Initiative

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Die AG KRITIS fördert die Vernetzung der beteiligten Akteure im Bereich Kritischer Infrastrukturen, z.B. durch die Ausrichtung interdisziplinärer Workshops.

Bildung und Awareness

#Awareness in der Politik #Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft

Ziel der Arbeitsgruppe ist, gemeinsam mit Politik, Wirtschaft und Gesellschaft, eine nachhaltige Ver-besserung der IT- und OT-Sicherheit und Resilienz von Kritischen Infrastrukturen zu erreichen.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger
- Bürgerinitiative
- NGO
- Hacker

Die AG KRITIS richtet sich im Bereich der Zivilgesellschaft nicht nur an Bürger, sondern auch an andere Bürgerinitiativen mit überlappenden Interessen, NGOs und Mitglieder politischer Parteien sowie ethisch handelnde Hacker.

Wissenschaft

Wirtschaft

Die AG KRITIS richtet sich nicht nur an aktuelle Betreiber kritischer Infrastruktur, sondern auch solche, die durch eine hypothetische Senkung der Schwellenwerte in der KritisV in Zukunft zu Betreibern kritischer Infrastrukturen werden könnten.

Staat

Die AG KRITIS wendet sich an alle Beteiligten aus Politik, Wirtschaft, Wissenschaft und Zivilgesellschaft.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Literatur
- Blog
- Öffentlichkeitsarbeit
- Studie
- Sonstiges Informationsangebot

Die Arbeitsgruppe veröffentlicht Artikel, Stellungnahmen und politische Forderungen und stellt regelmäßig Referenten auf Konferenzen und Kongressen.

Antispam e.V.

Beitrag zur Cybersicherheit

Kontakt:

An der Marlach 21

67146 Deidesheim

antispam-ev.de

Zivilgesellschaftliche Initiative

Antispam e.V. setzt sich als gemeinnütziger Verein für den Schutz der Zivilgesellschaft vor Spam und zu Fragen des Verbraucherschutzes ein. Interessierte Nutzer können sich in einem Forum über aktuelle Spams informieren, Tipps erhalten oder selbst anderen Nutzern Hilfestellungen geben. Neben dem Forum bietet Antispam e.V. eine Newsübersicht, die aktuelle Informationen zum Thema Spam enthält und bei Interesse als RSS-Feed abonniert werden kann. Darüber hinaus steht ein Wiki zur Verfügung, in dem wichtige Fragen und zugehörige Antworten zu den Themen Spam und damit verbundenen Betrugsszenarien gebündelt werden. Bspw. liefert der Verein Aufklärung und Hinweise zum Umgang mit verdächtigen E-Mails und SMS, zu Abo-Fallen, betrügerischen Online-Shops oder zu versehentlich oder unwissend abgeschlossene Fernabsatzverträge.

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Antispam e.V. vernetzt interessierte Nutzer, die auf der Suche nach Hilfe und Informationen zum Thema Spam sind mit anderen Nutzern, die ihre Hilfe anbieten.

Bildung und Awareness

#Awareness in der Zivilgesellschaft

Alle Aktivitäten von Antispam e.V. dienen in erster Linie der Information und dem Schutz vor Spam und Betrugsszenarien. In der Kategorie „Computersicherheit“ bspw. finden sich praktische Tipps für Privatanwender zur Absicherung eigener Geräte.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger

Die Aktivitäten des Antispam e.V. richten sich an alle Bürger mit dem Ziel, diese vor Spam und Betrug zu schützen. Interessierte Personen können sich engagieren und am Informationsangebot mitwirken.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

Auf der Webseite wird ein Linkencoder angeboten, der zur Verschlüsselung von E-Mail-Adressen genutzt werden kann.

Information

- Informationsaufbereitung

Das Angebot des Antispam e.V. umfasst ein Wiki, ein Forum sowie eine Newsseite, die sich thematisch mit Spam und damit verbundenen Betrugsszenarien beschäftigen.

Cyber Security Challenge Germany (CSCG)

Beitrag zur Cybersicherheit

Die CSCG ist ein jährlich stattfindender Capture the Flag (kurz CTF) Wettbewerb, bei welchem sich Teilnehmende kompetitiv an herausfordernden Aufgaben aus den Bereichen Kryptografie, Stenografie, Exploitation, Web-Sicherheit und Reverse Engineering messen. An dem offiziellen Wettbewerb der CSCG können alle Personen zwischen 14 und 25 Jahren teilnehmen, grundsätzlich ist auch ein inoffizieller Wettbewerb für alle Interessierten zugänglich. Aus den besten 20 Teilnehmenden der Online-Qualifikation können sich anschließend im deutschen Finale, einem vor Ort Wettbewerb, 10 Personen für die European Cyber Security Challenge (ECSC) qualifizieren. Im Rahmen der ECSC treten (Stand 2020) 22 europäische Teilnehmerländer gegeneinander an. Eine Weltmeisterschaft befindet sich in Planung.

Ansprechpartner:

Nachwuchsförderung IT-Sicherheit e.V.

Wilhelm-Raabe-Str. 16

44791 Bochum

cscg.de

Zivilgesellschaftliche Initiative

Die CSCG wurde maßgeblich durch den TeleTrusT e.V., das Institut für Internet-Sicherheit if(is) und Heise Events gegründet. Bis Ende 2016 wurde das Projekt außerdem von der Initiative IT-Sicherheit in der Wirtschaft des Bundesministeriums für Wirtschaft und Energie gefördert. Seit 2020 obliegt die Organisation der CSCG dem gemeinnützen Verein Nachwuchsförderung IT-Sicherheit.

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Der Wettbewerb wurde ins Leben gerufen, um junge Talente aus dem Bereich der IT-Sicherheit zu identifizieren, zu fördern und mit interessierten Unternehmen aus der Wirtschaft im Rahmen von Recruiting-Messen zu vernetzen. Ein Hauptziel ist demnach, dem Fachkräftemangel im Umfeld der IT-Sicherheit entgegen zu wirken.

Bildung und Awareness

#Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft #Schulisches Bildungsangebot #Sonstiges Bildungsangebot

Die CSCG soll junge interessierte Menschen an das Themenfeld der IT-Sicherheit heranführen, weiterhin sollen bereits Erfahrenere durch spannende Aufgaben herausgefordert werden. Mit dem Aushängeschild CSCG soll gezielt auf den Bedarf für die Förderung von jungen IT-Sicherheitstalenten und insgesamt auf das Thema IT-Sicherheit aufmerksam gemacht werden.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger
- Kinder und Heranwachsende
- Hacker

An der CSCG können alle Personen mit einer deutschen Staatsbürgerschaft, die zwischen 14 und 25 Jahren alt sind, teilnehmen.

Wirtschaft

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Sonstige Dienstleistung

Im Rahmen der CSCG wird eine Recruiting-Messe organisiert, auf der sich Unternehmen jungen interessierten Menschen mit einem Interesse an dem Berufsfeld der IT-Sicherheit präsentieren können.

Cyber-Cops des Immanuel-Kant-Gymnasium Bad Oeynhausen

Beitrag zur Cybersicherheit

Das Immanuel-Kant-Gymnasium in Bad Oeynhausen bietet mit der Initiative Cyber-Cops Schülerinnen und Schülern die Möglichkeit, sich mit der Thematik Internet-Sicherheit im Kontext von Cybermobbing und sozialen Netzwerken auseinanderzusetzen. Hierzu werden Schülerinnen und Schüler speziell zu sog. „Cyber-Cops“ ausgebildet. An diese können sich andere Schülerinnen und Schüler mit Fragen und Problemen wenden.

Kontakt:

Grüner Weg 28

32547 Bad Oeynhausen

ikg-bo.de

Zivilgesellschaftliche Initiative

Thematische Schwerpunkte (Auszug)

Bildung und Awareness

#Schulung #Awareness in der Zivilgesellschaft
#Schulisches Bildungsangebot

Die Initiative schafft Awareness für die Relevanz der Thematik bei Schülerinnen und Schülern des Immanuel-Kant-Gymnasiums und ihren Lehrkräften.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger
- Kinder und Heranwachsende

Zielgruppe für das Informations- und Schulungsangebot der Initiative sind Schülerinnen und Schüler des Immanuel-Kant-Gymnasiums.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Sonstiges Informationsangebot

Das Angebot der Initiative umfasst Hilfestellungen der als „Cyber-Cops“ ausgebildeten Schüler und Schülerinnen zu Themen aus dem Bereich Internet-Sicherheit für Mitschülerinnen und Mitschüler sowie Lehrkräfte.

Deutschland sicher im Netz e.V. (DsiN)

Beitrag zur Cybersicherheit

Kontakt:

Albrechtstr. 10c

10117 Berlin

sicher-im-netz.de

Zivilgesellschaftlicher Akteur

DsiN ist ein gemeinnütziges Bündnis, das Verbraucherinnen und Verbraucher und kleinere Unternehmen im sicheren und souveränen Umgang mit der digitalen Welt unterstützt. Dafür bietet DsiN in Zusammenarbeit mit seinen Mitgliedern und Partnern konkrete Hilfestellungen sowie Mitmach- und Lernangebote für Menschen im privaten und beruflichen Umfeld an. Es existieren Initiativen des Vereins zu Themen wie bspw. IT-Sicherheit im Mittelstand und für Berufsschülerinnen und Berufsschüler. Vereinszwecke sind die Förderung der Bildung und Erziehung, die Verbraucherberatung, die Kriminalprävention sowie der Dialog mit der Wissenschaft und Forschung mit dem Ziel, Sicherheit und des Vertrauens in Informationstechnik und digitale Netze zu fördern. Des Weiteren initiiert DsiN Wettbewerbe und Mitmach-Angebote für Verbraucherinnen und Verbraucher sowie Unternehmen, die dazu anregen, sich mit dem Thema IT-Sicherheit zu beschäftigen. Schirmherr des Vereins ist seit 2007 der jeweilige Bundesinnenminister.

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

DsiN bietet über seine Mitglieder und Partner (darunter namhafte deutsche Firmen und behördliche Einrichtungen) ein leistungsfähiges Netzwerk. Die Initiative Deutschland Dialog für digitale Aufklärung zielt auf den direkten Dialog von Wirtschaft, Zivilgesellschaft und Bundesregierung zur Befähigung der Menschen, die Möglichkeiten der Digitalisierung zu nutzen, ab.

Bildung und Awareness

#Schulung #Awareness in der Zivilgesellschaft

DsiN richtet sich mit Vorträgen, Workshops, Medienmaterial, Fachtagungen, Ratgebern, Tools etc. an seine Zielgruppen.

Konzeption und Vorgehensweisen

#Authentifizierung #Endgerätesicherheit #Datenschutz

Die sichere Vergabe von Passwörtern und das Bewusstsein im Umgang mit der digitalen Identität gehört zu den Kernthemen des DsiN. Die Zielgruppe Wirtschaft wird mit dem Themengebieten "Sicherheit am Arbeitsplatz" angesprochen.

Betriebsbezogene Sicherheitsaspekte

#Cloudsicherheit

DsiN berät Unternehmen bei der Digitalisierung der Betriebsabläufe.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger

Als gemeinnütziges Bündnis unterstützt DsiN Verbraucherinnen und Verbraucher im sicheren und souveränen Umgang mit der digitalen Welt.

Wissenschaft

- Forschungseinrichtung

DsiN versteht sich als Partner für die Wissenschaft im Bereich Sicherheit in der Informationstechnik.

Wirtschaft

Als gemeinnütziges Bündnis unterstützt DsiN KMU im sicheren und souveränen Umgang mit der digitalen Welt.

Staat

DsiN versteht sich als Partner für die Politik. In diesem Zusammenhang ist der Verein bei der Umsetzung von Initiativen der Bundesregierung im Bereich der Sicherheit der Informationstechnik unterstützend tätig, insb. bei der Umsetzung des Nationalen Plans zum Schutz der Informationsinfrastrukturen (NPSI) im Bereich der Zielgruppen Bürgerinnen und Bürger sowie KMU.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Ausbildung und Schulung
- Sonstige Dienstleistung

DsiN bietet in Zusammenarbeit mit seinen Mitgliedern und Partnern Lernangebote und Hilfestellung zum Themenbereich IT-Sicherheit für Menschen im privaten und beruflichen Umfeld an. Unter der Schirmherrschaft des BMWi ist die Initiative zusammen mit der DIHK außerdem Träger der Workshopreihe "IT-Sicherheit@Mittelstand", die sich auf die Weiterbildung von KMU im Bereich IT-Sicherheit fokussiert.

Information

- Informationsaufbereitung
- Lernprogramm
- Newsletter
- Öffentlichkeitsarbeit
- Sonstiges Informationsangebot

DsiN unterstützt Verbraucher und Unternehmen mit aktuellen Informationen zu IT-Sicherheitsthemen und bietet Newsletter an. Über Kampagnen und Öffentlichkeitsarbeit ist DsiN aktiv und berichtet jährlich über den Sicherheitsindex Deutschland.

Produkt

- Sonstige Produkte

Das Bündnis DsiN ist im Zusammenhang mit digitaler Sicherheit für verschiedene Verbraucher-Tools bekannt: z.B. DsiN Sicherheitsbarometer-App, DsiN Passwortkarte, IT-Fitnesscheck.

Die Cybermights

Beitrag zur Cybersicherheit

"Die Cybermights" ist ein interaktives Spiel, das Kinder und Jugendliche spielerisch zum Thema Cybermobbing und Gefahren der digitalen Welt sensibilisieren soll. Das Spiel wird von zahlreichen Partnern unterstützt und lässt sich kostenlos im Browser spielen oder downloaden. Ziel ist die spielerische Vermittlung von Themen wie Datenschutz und sicherem Umgang mit Social Media.

Ansprechpartner:

mmc - Agentur für interaktive Medien GmbH

Isartalstr. 44a

80469 München

die-cybermights.de

Zivilgesellschaftliche Initiative

Thematische Schwerpunkte (Auszug)

Bildung und Awareness

#Awareness in der Zivilgesellschaft

Das Spiel “Die Cybermights“ zielt auf eine unterhaltsame Vermittlung von Medienkompetenz bei Kindern und Jugendlichen ab. Auf spielerische Weise sollen diese mit Themen wie Datenschutz und sicherer Nutzung von sozialen Netzwerken vertraut gemacht werden. Konkret werden die Nutzer und Nutzerinnen im Spiel zu Spam, Cybermobbing, Viren und Trojanern, Passwörtern, Pseudonymen, Datenschutz sowie Urheberrechten geschult. Darüber hinaus stehen auf der Webseite auch weitere, textuelle Informationen zu den einzelnen thematischen Schwerpunkten zur Verfügung.

Zielgruppe

Zivilgesellschaft

- Kinder und Heranwachsende

Das Spiel „Die Cybermights“ ist für Kinder ab 10 Jahren und Jugendliche konzipiert.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung

Neben der spielerischen Vermittlung der Cybersicherheitsthemen stehen die Informationen auch in textueller Form gebündelt auf der Webseite zur Verfügung.

Produkt

- Software
- Software/SaaS

"Die Cybermights" lässt sich sowohl im Browser spielen als auch kostenlos downloaden. Ziel des Spiels ist das Aufspüren eines Trickbetrügers, der durch das Ausspionieren des Handys einer Person deren private Daten erlangen konnte und diese nun gegen sie verwendet.

Digitale Gesellschaft e.V.

Beitrag zur Cybersicherheit

Der gemeinnützige Verein Digitale Gesellschaft e.V. wirkt im Themenbereich der Cybersicherheit bei den Themen Datenschutz, Urheberrecht, Vorratsdaten und Netzneutralität mit. Er setzt sich für Grundrechte und Verbraucherschutz im digitalen Raum ein und betreibt zu diesem Zweck ein Informationsportal für Verbraucherinnen und Verbraucher. Zum Erhalt und zur Fortentwicklung einer offenen digitalen Gesellschaft engagiert sich der Verein gegen den Rückbau von Freiheitsrechten im Netz, gegen alle Formen von Überwachung und für die Realisierung digitaler Potentiale bei Wissenszugang, Transparenz, Partizipation und kreativer Entfaltung.

Kontakt:

Groninger Str. 7

13347 Berlin

digitalegesellschaft.de
deinedatendeinerechte.de
dein-netz.org

Zivilgesellschaftlicher Akteur

Thematische Schwerpunkte (Auszug)

Bildung und Awareness

#Awareness in der Politik #Awareness in der Zivilgesellschaft #Schulisches Bildungsangebot

Der Verein trägt seine Positionen zu Cyberthemen an die Politik heran und ist mit politischen Gremien im Austausch. Über Projekte und Informationsportale klärt er Verbraucher über ihre Rechte im Netz auf und spricht explizit junge Menschen in schulischen und außerschulischen Veranstaltungen an, um diesen einen sicheren Umgang mit dem Internet zu ermöglichen.

Konzeption und Vorgehensweisen

#Datenschutz

Der Verein setzt sich für den Bereich des Datenschutzes ein.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger

Der Verein wendet sich mit seinen Angeboten an Bürgerinnen und Bürger, Verbraucherinnen und Verbraucher.

Staat

Der Verein vertritt die Interessen seiner Mitglieder gegenüber der Politik.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Blog
- Newsletter
- Öffentlichkeitsarbeit
- Sonstiges Informationsangebot

Der Verein ist mit Informationen und einem Blog zu Netzthemen präsent und veröffentlicht seine Stellungnahmen zu politischen Themen und Gesetzgebungen online. Auf seinem Informationsportal stellt er auch Musterschreiben zu Datenschutzthemen bereit. Außerdem wird ein Newsletter angeboten.

Produkt

- Sonstige Produkte

Der Verein betreibt ein Informationsportal, um spielerisch, mit Informationen oder Videos insb. über Datenschutzthemen aufzuklären.

Digitale Helden gGmbH

Beitrag zur Cybersicherheit

Die Digitale Helden gGmbH bildet Schülerinnen und Schüler sowie Lehrkräfte aus, die dann wiederum jüngere Schülerinnen und Schüler zu Themen wie persönliche Daten und Cybermobbing beraten können. Das Angebot umfasst bspw. ein gemeinnütziges Mentorenprogramm für Schulen, bei dem Grundkenntnisse zu Internetsicherheit, Datenschutz und Cybermobbing vermittelt werden. Darüber hinaus werden auch kostenlose Webinare für Eltern sowie Pädagoginnen und Pädagogen angeboten. Die Digitale Helden gGmbH verbindet Personen mit unterschiedlichen beruflichen Hintergründen aus Kommunikation, Technik und Pädagogik. Sie wird von verschiedenen Partnern aus Wirtschaft, Zivilgesellschaft und der öffentlichen Hand gefördert.

Kontakt:

Arnsburger Str. 58d

60385 Frankfurt am Main

digitale-helden.de

Zivilgesellschaftliche Initiative

Thematische Schwerpunkte (Auszug)

Bildung und Awareness

#Schulung #Awareness in der Zivilgesellschaft #Sonstiges Bildungsangebot

Die Digitale Helden gGmbH verfolgt das Ziel, Schulen und Familien bei der bewussten und kompetenten digitalen Kommunikation zu unterstützen und dadurch insbesondere zur Prävention von Cybermobbing beizutragen. Dazu bietet die Initiative verschiedene Weiterbildungsprogramme an, in denen die Inhalte auf geeignete Weise vermittelt werden.

Zielgruppe

Zivilgesellschaft

- Kinder und Heranwachsende
- Familien

Die Angebote von Digitale Helden gGmbH richten sich an Schülerinnen und Schüler, Eltern sowie Pädagoginnen und Pädagogen.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Lernprogramm
- Blog
- Newsletter

Die Digitale Helden gGmbH bietet verschiedene Webinare für Eltern sowie Pädagoginnen und Pädagogen an, in denen sich diese zu aktuellen Themen wie bspw. kindgerechten Apps informieren können. Darüber hinaus wird ein Mentorenprogramm angeboten, in dem Schülerinnen und Schüler der 8. bis 9. Klasse zu Mentoren im Bereich der "digitalen Welt" ausbildet werden, die dann wiederum als Ansprechpartner zu Themen wie Cybermobbing und Datenschutz für jüngere Schülerinnen und Schüler bereitstehen.
Außerdem werden auf der Webseite Beiträge zu aktuellen Themen aus dem Bereich Cybermobbing oder Datenschutz in Form eines Blogs veröffentlicht. Zusätzlich steht ein Newsletter zur Verfügung, der sich mit Tipps zur bewussten Internetnutzung an Familien richtet.

Hoax-Info Service

Beitrag zur Cybersicherheit

Der Hoax-Info Service ist eine Webseite, die eine Übersichtsliste als Nachschlagewerk zu aktuellen Hoaxes (durch E-Mail verbreitete Falschmeldungen), Kettenbriefen, Computerviren und weitern Sicherheitsinformationen bereitstellt und pflegt. Empfänger von Hoaxes können diese weiterleiten und zur Aktualität der Übersichtsliste, die sog. Hoax-Liste, beitragen. Neben der Hoax-Liste gibt es Informationsmaterial zu Sicherheitslücken und Sicherheitspatches, etwa von Browsern, Betriebssystemen sowie Programmiersprachen, aber auch zu Antivirus-Programmen und weiteren Informationen rund um die Sicherheit im Internet.

Kontakt:

Haselerstr. 17g

14050 Berlin

hoaxinfo.de

Zivilgesellschaftliche Initiative

Thematische Schwerpunkte (Auszug)

Bildung und Awareness

#Awareness in der Zivilgesellschaft

Das Informationsmaterial des Hoax-Info Service dient der Aufklärung der Internetnutzer bezüglich Hoaxes, Kettenbriefen und anderer schädlicher E-Mail-Inhalte und -Anhänge.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger

Zielgruppe des Hoax-Info Service sind alle, die sich über Hoaxes u. ä. informieren möchten oder davon betroffen sind.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung

Der Hoax-Info Service betreibt die Informationssammlung und -aufbereitung zur Aufklärung rund um die Themen Hoaxes, Kettenbriefe, Computerviren, Browsern, Betriebssystemen etc.

Horst Görtz Stiftung

Beitrag zur Cybersicherheit

Die Horst Görtz Stiftung setzt sich als Stiftung bürgerlichen Rechts vorrangig für die gemeinnützige Förderung der Forschung und Lehre im Bereich der Informationssicherheit ein. Die Stiftung unterstützt bspw. das Horst Görtz Institut für IT-Sicherheit und das Institut für Sicherheit im E-Business an der Ruhr-Universität Bochum, vergibt Stipendien an Studierende der IT-Sicherheit und finanziert Forschungsprojekte auf diesem Gebiet. Zudem verleiht sie den Deutschen IT-Sicherheitspreis für herausragende nationale Innovationen.

Kontakt:

Tannenwaldallee 31

61348 Bad Homburg v.d.H.

horst-goertz.de
hg-stiftung.de

Zivilgesellschaftlicher Akteur

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Die Stiftung unterstützt die Vernetzung innerhalb der deutschen Wissenschaftsgemeinschaft auf dem Gebiet der Cybersicherheit, bspw. durch Stiftungsprofessuren, Preisverleihungen und aktive Mitgliedschaften in Wissenschaftsnetzwerken wie dem CAST e.V.

Bildung und Awareness

#Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft #Berufliches Bildungsangebot

Die Stiftung hat diverse Förderprojekte aufgelegt u.a. zur Entwicklung von Lernprogrammen und Zusatzqualifikationen zum Thema Informationssicherheitsbewusstsein für den Berufseinstieg an der TU Wildau.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger
- Akademikerinnen und Akademiker

Die Stiftung fördert gezielt Studierende mit Stipendien.

Wissenschaft

- Information und Kommunikation

Die Stiftung verleiht den deutschen IT-Sicherheitspreis zur Förderung des Innovationspotentials der deutschen IT-Sicherheitswirtschaft.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Sonstige Dienstleistung

Das Angebot der Horst Görtz Stiftung besteht aus der Förderung des Innovationspotentials der Wissenschaft und Wirtschaft im Bereich der IT-Sicherheit in Deutschland.

JUUUPORT e.V.

Beitrag zur Cybersicherheit

Der JUUUPORT e.V. setzt sich für einen respektvollen Umgang im Internet ein. Dazu bietet der Verein eine Online-Beratung von jungen Menschen für junge Menschen an. Sogenannte Scouts bieten ehrenamtlich ihre Hilfe an und beraten bspw. zu Cybermobbing oder Datendiebstahl. Als Scouts können sich Jugendliche im Alter von 14 bis 19 Jahren anmelden, die anschließend von Expertinnen und Experten aus den Bereichen Recht, Internet und Online-Beratung auf ihre Beratungstätigkeit vorbereitet werden. Darüber hinaus werden auf der Webseite aktuell relevante Artikel rund um die Themen Sicherheit in der digitalen Welt und bewusste Mediennutzung veröffentlicht und gängige Fragen in einem FAQ zusammengestellt.

Kontakt:

Seelhorststr. 18

30175 Hannover

juuuport.de

Zivilgesellschaftliche Initiative

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Der JUUUPORT e.V. bietet jungen Menschen, die Opfer von Datendiebstahl, Datenmissbrauch oder Cybermobbing wurden oder Fragen zu diesen Themen haben, eine Plattform und konkrete Hilfemaßnahmen in Form von Beratungen an. Das Beratungsprinzip ist dabei eine Hilfe von jungen Menschen, den sog. Scouts, für andere junge Menschen, um so der Zielgruppe geeignet gerecht zu werden.

Bildung und Awareness

#Awareness in der Zivilgesellschaft #Schulisches Bildungsangebot

Neben der Beratung klärt der JUUUPORT e.V. im eigenen Onlinemagazin über aktuelle Themen des sicheren Umgangs mit digitalen Medien und dem Internet auf und schafft somit Awareness in der Zielgruppe der Heranwachsenden und Jugendlichen. Auch bietet er kostenloses Informationsmaterial und Broschüren u.a. für die Nutzung in Schulen an.

Konzeption und Vorgehensweisen

#Datenschutz

Die ehrenamtlichen Scouts beraten Hilfesuchende, welche Opfer von Datendiebstahl bzw. -missbrauch wurden und geben Hinweise zur Schadensminimierung und Absicherung eigener Daten zur Verhinderung künftiger Vorfälle. Zudem beraten die sog. Scouts des JUUUPORT e.V. auch in Fragen des Datenschutzes.

Zielgruppe

Zivilgesellschaft

- Kinder und Heranwachsende

Zielgruppe des JUUUPORT e.V. sind alle Jugendlichen, die Fragen zum Thema Cybermobbing haben oder nach Hilfe suchen.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Beratung

JUUUPORT e.V. bietet individuelle Online-Beratungen an. Dieses Beratungsangebot kann sowohl über die Webseite als auch über gängige Messengerdienste in Anspruch genommen werden.

Information

- Informationsaufbereitung

Das Angebot des JUUUPORT e.V. umfasst sowohl aufbereitete Informationen in Form von Artikeln auf der Webseite oder eine Sammlung gängiger Fragen und deren Beantwortung. Außerdem werden Online-Seminare zu Themen wie Privatsphäre oder Cybermobbing für Schulklassen, Jugendclubs oder Vereine angeboten, bei denen die Teilnehmer interaktiv Fragen stellen oder diskutieren können.

Kuketz IT-Security

Beitrag zur Cybersicherheit

Kontakt:

Ludwig-Erhard-Allee 10

76131 Karlsruhe

kuketz-blog.de

Zivilgesellschaftliche Initiative

Kuketz IT-Security ist eine unabhängige Informationsplattform rund um die Themen IT-Sicherheit, Datenschutz und Datenschutzrecht, die zum Ziel hat, diese Themen jedem Interessierten verständlich zugänglich zu machen. Neben der Veröffentlichung aktueller Beiträge steht vor allem die praxisnahe Anwendbarkeit der vermittelten Informationen im Fokus. Betreiber von Kuketz IT-Security ist eine Privatperson, die sich auch beruflich in ihrer Tätigkeit im Penetrationtesting mit Themen der IT-Sicherheit auseinandersetzt. Kuketz IT-Security bietet einen Blog und ein Forum an, in dem sich die Nutzer zu verschiedenen Themen der IT-Sicherheit untereinander austauschen können. Die Community von Kuketz IT-Security arbeitet zudem an eigenen nützlichen und kostenfreien Tools und Diensten, wie bspw. einer eigenen Instanz einer Open Source Software für sichere Videokonferenzen.

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

In einem Forum können sich Nutzer des Blogs untereinander austauschen und gegenseitig Hilfe zu Themen wie Sicherheit und Datenschutz, Betriebssystemen oder Software leisten.

Bildung und Awareness

 # Awareness in der Zivilgesellschaft

Die regelmäßig erscheinenden Artikel des Blogs thematisieren aktuelle Themen und Fragestellungen rund um die IT-Sicherheit. In einer „Empfehlungsecke“, welche stetig erweitert und aktualisiert wird, werden Hilfestellungen zum sicheren Umgang mit dem Internet und IuK bereitgestellt. Dabei werden die Leser und Anwender informiert und sensibilisiert.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger

Der Blog richtet sich an alle interessierten Nutzer, die sich kritisch mit den Themen IT-Sicherheit und Datenschutz auseinandersetzen möchten.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Blog

Auf dem Blog werden regelmäßig Beiträge zu aktuellen Themen der IT-Sicherheit veröffentlicht. Neben Beiträgen zu aktuellen Entwicklungen werden auch konkrete Hilfestellungen und Empfehlungen angeboten. Darüber hinaus werden Analysen veröffentlicht, die bspw. das Datensendeverhalten von Gesundheits-Apps untersuchen.

Produkt

- Software

Zusätzlich zum Blog werden verschiedene Dienste angeboten, wie bspw. eine quelloffene Software zur sicheren Videokommunikation, die besonderen Fokus auf die Privatsphäre der Nutzer legt.

MalwareMustDie

Beitrag zur Cybersicherheit

Die Initiative MalwareMustDie wird durch eine Gruppe von Aktivistinnen und Aktivisten bzw. Hackern betrieben Sie widmet sich der Bekämpfung von Schadsoftware insb. durch die Beschreibung von Angriffsmustern zur Awareness-Schaffung und die Analyse von Malware-Code.

Kontakt:

Erreichbar auf Twitter unter

@MalwareMustDie

malwaremustdie.org

Zivilgesellschaftliche Initiative

Thematische Schwerpunkte (Auszug)

Bildung und Awareness

#Awareness in der Zivilgesellschaft

Die Initiative hat sich die Sensibilisierung der Gesellschaft zum Thema Schadsoftware als Ziel gesetzt.

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen MalwareMustDie analysiert Proben von Schadsoftware, um diesbezügliche Berichte zu veröffentlichen und Angriffsmuster zu beschreiben.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger
- Hacker

Wirtschaft

Informationsartikel und Veröffentlichungen der Initiative sind insb. für andere (White-Hat-)Hacker interessant, zielen aber auch auf Bürger, Behörden und Wirtschaftsakteure.

Staat

- Behörde/Verwaltung

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Blog
- Sonstiges Informationsangebot

MalwareMustDie veröffentlich neben Analysen zu Schadsoftware auch kleinere Tools und Code-Auszüge zur Verwendung durch Interessierte. Über ihren Blog und Social-Media-Auftritt veröffentlicht die Initiative außerdem Stellungnahmen und Beiträge zu aktuellen Themen bezüglich Schadsoftware.

Mobilsicher

Beitrag zur Cybersicherheit

Mobilsicher.de ist ein Informationsportal für einen sicheren Umgang mit dem Handy und wird vom iRights e.V. in Kooperation mit dem Institut für Technik und Journalismus (ITUJ)

e.V. betrieben. Hierzu bietet das Portal Informationen zu den Themen Datenschutz, Privatsphäre und Sicherheit bei Mobilgeräten in Form von Erklärungen und Tipps. Darüber hinaus werden Einstellungen erklärt und Apps hinsichtlich ihrer Sicherheit getestet. Das Projekt wird vom BMJV gefördert.

Ansprechpartner:

iRights e.V.

Linienstraße 13

10178 Berlin

mobilsicher.de

Zivilgesellschaftliche Initiative

Thematische Schwerpunkte (Auszug)

Bildung und Awareness

#Awareness in der Zivilgesellschaft

Das Informationsangebot der Initiative richtet sich an alle Smartphone-Nutzer und umfasst sämtliche Themen rund um Datenschutz, Sicherheit und Privatsphäre.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger
- Kinder und Heranwachsende
- Familien
- Seniorinnen und Senioren

Das Infoportal der Initiative richtet sich an alle Nutzerinnen und Nutzer von Smartphones, explizit auch an Anfängerinnen und Anfänger.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Journalismus

Die Informationen der Initiative werden in Form von journalistischen Beiträgen, Ratgebern und Videos aufbereitet.

SCHAU HIN! Was Dein Kind mit Medien macht.

Beitrag zur Cybersicherheit

SCHAU HIN! ist eine Initiative des BMFS, der beiden öffentlich-rechtlichen Sender Das Erste und ZDF sowie der AOK – Die Gesundheitskasse. Sie unterstützt Eltern und Erziehende dabei, ihre Kinder im sicheren Umgang mit Medien zu fördern („SCHAU HIN! Was Dein Kind mit Medien macht."). Dazu werden auf der Webseite konkrete Tipps, Empfehlungen und News veröffentlicht. Das Informationsangebot ist thematisch gegliedert und bietet in jeder Rubrik eine Kategorie "Sicherheit und Risiken", die Informationen wie bspw. Sicherheitseinstellungen oder Empfehlungen für Eltern enthalten. In jeder Rubrik wird auf relevante Studien verwiesen, die die Handlungsempfehlungen wissenschaftlich untermauern.

Ansprechpartner:

Projektbüro SCHAU HIN!

c/o denkwerk b_projekte für bildung und prävention gGmbH

Chausseestraße 13

10115 Berlin

schau-hin.info

Zivilgesellschaftliche Initiative

Thematische Schwerpunkte (Auszug)

Bildung und Awareness

#Awareness in der Zivilgesellschaft

SCHAU HIN! unterstützt mit einem gezielten Informationsangebot Eltern im Umgang mit der Mediennutzung ihrer Kinder. Das Informationsangebot ist auf der Webseite verfügbar und enthält viele Informationen zur Sicherheit der Internetnutzung bei Smartphones, Spielen, sozialen Netzwerken und weiteren Themen.

Konzeption und Vorgehensweisen

#Endgerätesicherheit #Datenschutz

SCHAU HIN! unterstützt mit Anleitungen die sichere Einrichtung von Smartphones, Tablets, Computern sowie Konsolen für Kinder und Jugendliche und gibt Tipps zu Berechtigungen von Apps und Jugendschutzeinstellungen. Außerdem gibt es Hinweise zur sicheren Internetnutzung, bspw. auch durch Nutzung von Altersgrenzen- und Jugendschutzeinstellungen sowie den Schutz privater Daten.

Zielgruppe

Zivilgesellschaft

- Familien

Das Angebot der Initiative „SCHAU HIN!" richtet sich in erster Linie an Eltern und Erziehende.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Newsletter
- Öffentlichkeitsarbeit
- Podcast

Das Angebot von "SCHAU HIN!" besteht aus thematisch breit gefächerten Themenbereichen der digitalen Medien, die immer auch hinsichtlich ihrer Sicherheit und bestehender Risiken betrachtet werden. Die Informationen stehen in Form von Artikeln auf der Webseite zur Verfügung. Bei individuellen Fragen können sich Eltern zudem an sogenannte Mediencoaches wenden, die weitere Tipps geben. Außerdem ist ein Medienquiz verfügbar, mit dem Kinder und Eltern ihre Kenntnisse testen können. Das Informationsangebot kann zusätzlich über verschiedene Newsletter abonniert werden. In einer Mediathek werden des Weiteren Podcast-Folgen und Videos angeboten. "SCHAU HIN!" informiert über die sichere Mediennutzung von Kindern auch durch Experteninterviews in Print- und Onlinemedien sowie durch informative Beiträge auf diversen Social-Media-Plattformen.

Selbstdatenschutz

Beitrag zur Cybersicherheit

Selbstdatenschutz.de ist eine von einer Privatperson betriebene Webseite, die Erklärungen, Hilfestellungen und konkrete Anleitungen zu den Themen Datenschutz, digitaler Selbstschutz, Vermeidung von Datenmissbrauch und Absicherung eigener Daten durch Verschlüsselung bereitstellt.

Kontakt:

Warschauerstr. 66

10243 Berlin

selbstdatenschutz.info

Zivilgesellschaftlicher Akteur

Thematische Schwerpunkte (Auszug)

Bildung und Awareness

#Awareness in der Zivilgesellschaft

Die Internetseite sensibilisiert mit ihren Themen für einen sicheren Umgang mit den eigenen Daten und liefert zu Ratgeber und Anleitungen.

Konzeption und Vorgehensweisen

#Authentifizierung #Endgerätesicherheit #Datenschutz

Mit ihren Beiträgen sensibilisiert die Seite die Adressaten im Thema IT-Sicherheit insbesondere aus dem Bereich der Verschlüsselung.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger

Innerhalb der Zielgruppe richten sich die Inhalte an alle Interessierten.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Blog

Der Blog veröffentlicht Beiträge, Ratgeber und Tutorials zur Internetsicherheit. Hierbei liegt ein Fokus auf Verschlüsselungsthemen.

SICHERES NETZ HILFT e.V.

Beitrag zur Cybersicherheit

Der SICHERES NETZ HILFT e.V. verfolgt das Ziel, Medienkompetenz und Internetsicherheit zu fördern. Hierzu bildet der Verein sogenannte Mediencoaches aus und veranstaltet Vorträge, Seminare, Workshops oder Aktionstage an Schulen zur Aufklärung über Chancen und Risiken des Internets. SICHERES NETZ HILFT e.V. setzt sich aus Einzelpersonen mit thematisch verschiedenen beruflichen Hintergründen zusammen. Das Angebot richtet sich an eine breite Zielgruppe, wird jedoch zielgruppenspezifisch zugeschnitten.

Kontakt:

Herzbergweg 6

65760 Eschborn

sicheres-netz-hilft.de

Zivilgesellschaftliche Initiative

Thematische Schwerpunkte (Auszug)

Bildung und Awareness

#Schulung #Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft

Der SICHERES NETZ HILFT e.V. verfolgt in erster Linie das Ziel der Aufklärung zur sicheren Medien- und Internetnutzung. Die Inhalte werden dabei auf verschiedene Arten bspw. in Form von Workshops oder Vorträgen vermittelt.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger
- Kinder und Heranwachsende
- Seniorinnen und Senioren

Wissenschaft

Die Informationsangebote zielen auf eine breite gesamtgesellschaftliche Zielgruppe ab. Dabei bietet der SICHERES NETZ HILFT e.V. Aktionstage für Schulen und Seniorinnen und Senioren, aber auch für Unternehmen an.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Ausbildung und Schulung

Der SICHERES NETZ HILFT e.V. bildet zertifizierte Mediencoaches aus, die sowohl zu aktuellen Medieninhalten als auch zu den damit verbundenen Gefahren geschult werden.

Information

- Informationsaufbereitung
- Lernprogramm

Das Angebot des SICHERES NETZ HILFT e.V. umfasst Vorträge, Workshops, Seminare und Aktionstage rund um das Thema Mediennutzung und Internetsicherheit. Auf der Webseite sind darüber hinaus Tipps und Informationen zu digitalen Medien verfügbar, bspw. werden Ratschläge zur Sicherheit von Smartphones oder Empfehlungen zur sicheren Internetnutzung für Kinder veröffentlicht.

Verein Bürgernetz e.V.

Beitrag zur Cybersicherheit

Der Verein Bürgernetz e.V. unterstützt Initiativen, Schulen sowie Bürgergruppen aus Münster und überregional aus dem Münsterland im sicheren Umgang mit dem Internet und bietet organisatorische und technische Unterstützung an. Der Verein Bürgernetz fördert den kompetenten und kritischen Umgang mit den neuen Medien.

Kontakt:

Verspoel 7/8

48143 Münster

buergernetz-muenster.de

Zivilgesellschaftliche Initiative

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Der Verein bietet eine Plattform für Schulen, Initiativen und Verbände zum Themenbereich Internet bzw. Internetnutzung und einen Rahmen für den gegenseitigen Austausch hierzu.

Bildung und Awareness

#Schulung #Awareness in der Zivilgesellschaft

Der Verein bietet Schulungen und Vorträge zu den Themen Internet bzw. Internetnutzung und mobile Endgeräte an.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger
- Bürgerinitiative

Wissenschaft

- Bildungseinrichtung

Schulen gehören zu den Zielgruppen des Vereins.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Ausbildung und Schulung
- Beratung

Der Verein bietet Schulungen, Vorträge und Sprechstunden an.

Information

- Informationsaufbereitung
- Öffentlichkeitsarbeit

Der Verein stellt Informationen über Internetthemen zur Verfügung und betreibt Öffentlichkeitsarbeit vor Ort in Münster.

Produkt

- Clouddienste/PaaS

Der Verein stellt Vereinen, Initiativen, Schulen und Bürgerinnen und Bürgergruppen seine Server-Infrastruktur zur Verfügung.

Virus Help Munich (VHM)

Beitrag zur Cybersicherheit

Die Initiative VHM ist ein privater Zusammenschluss von Antivirus-Forschern, die Informationen und Hilfe für Betroffene von Attacken mit Computerviren bereitstellen und den Informationsaustausch der Mitglieder untereinander fördern. Außerdem werden neue Computerviren analysiert, um aktuelle Informationen zu diesen veröffentlichen zu können, Virenschutzsysteme beurteilt und Hilfestellungen zu damit verbundenen Aspekten angeboten.

Kontaktaufnahme über die Webseite:

Klewitzstr. 7

39112 Magdeburg

virushelpmunich.de

Zivilgesellschaftliche Initiative

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Durch eine Mitgliedschaft können sich Interessierte an der Arbeit des VHM beteiligen und sich mit den anderen Mitgliedern austauschen. Das Informations- und Hilfsangebot steht aber auch Nichtmitgliedern zur Verfügung.

Bildung und Awareness

#Detektion von sicherheitsrelevanten Ereignissen
#Behandlung von Sicherheitsvorfällen & IT-Forensik

Von VHM werden neue Viren analysiert und Informationen hierzu veröffentlicht. Für den Schadensfall werden Informationen zum weiteren Vorgehen zur Verfügung gestellt. Für verschiedene Viren wird spezifische Software zur Entfernung angeboten.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger

Zielgruppen von VHM sind Betroffene von Computerviren und Personen, die sich über Computerviren und deren Abwehr informieren wollen.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung

VHM veröffentlicht verschiedene Informationen rund um das Thema Computerviren und deren Abwehr bzw. Maßnahmen nach Schadensfällen.

Produkt

- Software

Von VHM wird eigenentwickelte Antivirus-Software zur Verfügung gestellt.

8.2 Wissenschaftliche Initiativen und Akteure

Arbeitsgruppe "Multimedia and Security"

Beitrag zur Cybersicherheit

Die Arbeitsgruppe "Multimedia and Security" der Otto-von-Guericke Universität in Magdeburg beschäftigt sich mit verschiedenen Themenfeldern der Cybersicherheit. Dies umfasst bspw. Digitale Wasserzeichen, Medien-, Netzwerk- und Computer-Forensik sowie den Entwurf von Mediensicherheitsprotokollen. Aus mehreren Forschungsprojekten heraus veröffentlicht die Arbeitsgruppe auch wissenschaftliche Publikationen. Darüber hinaus bietet die Arbeitsgruppe verschiedene Angebote für Schülerinnen und Schüler zur Weiterbildung und Bewusstseinsschaffung im Bereich Cybersicherheit.

Ansprechpartner:

Otto-von-Guericke-Universität Magdeburg

Universitätsplatz 2

39106 Magdeburg

omen.cs.uni-magdeburg.de

Wissenschaftlicher Akteur

Thematische Schwerpunkte (Auszug)

Bildung und Awareness

#Awareness in der Zivilgesellschaft
#Universitäres Bildungsangebot

Unter dem Motto "Security-by-Design" bietet die Arbeitsgruppe einen sog. Datensicherheits-Kompass an, welcher von den Nutzern selbst zusammengestellt wird und somit für ein besseres Verständnis in Bezug auf verschiedene IT-Sicherheitsthemen sorgt. Weiterhin wird unter dem Namen "KOMPASS - Digitalisierung aber sicher! Entdecke Souveränität und Nachhaltigkeit!" ein Schülerwettbewerb veranstaltet.

Konzeption und Vorgehensweisen

#Kryptographie #Datenschutz

Die Forschungsgruppe "Watermarking and Steganography Group" forscht in dem Gebiet der automatischen Detektion von Copyright-Verletzungen und Manipulationen sowie der Stenografie.

Detektion und Reaktion

#Behandlung von Sicherheitsvorfällen & IT-Forensik

Die Forschungsgruppe "Protocol Group" der Arbeitsgruppe befasst sich unter anderem mit der Erstellung von Richtlinien für forensische Investigationen.

Netze und Kommunikation

#Netzkomponenten

In der Forschungsgruppe "Security Evaluation Group" der Arbeitsgruppe wird die Evaluation und Analyse von Netzen und Betriebssystemen erforscht.

Zielgruppe

Zivilgesellschaft

- Kinder und Heranwachsende
- Akademikerinnen und Akademiker

Die Forschungsergebnisse der Arbeitsgruppe richten sich insbesondere an Akademikerinnen und Akademiker aus dem jeweiligen Fachgebiet. Die Bildungs- und Awarenessangebote richten sich vorrangig an Schülerinnen und Schüler.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Wissenschaftliche Veröffentlichung

Die Arbeitsgruppe veröffentlicht wissenschaftliche Publikationen sowie weitere Informationsmaterialien, wie einen Kompass für digitale Selbstverteidigung, mit welchem Wissen für die Ausgestaltung von Schul-IKT und Medienbildung vermittelt wird.

Cybersicherheitsforschung am Deutschen Forschungszentrum für Künstliche Intelligenz GmbH (DFKI)

Beitrag zur Cybersicherheit

Kontakt:

Trippstadter Str. 122

67663 Kaiserslautern

dfki.de

Wissenschaftlicher Akteur

Das DFKI ist eine Forschungseinrichtung zu innovativen Softwaretechnologien auf der Basis von Methoden der Künstlichen Intelligenz. Einer der Forschungsschwerpunkte des DFKI bildet die IT-Sicherheit. Das Tätigkeitsfeld umfasst sowohl anwendungsorientierte Grundlagenforschung und Prototypenentwicklung als auch patentfähige Lösungen im Bereich der Informationstechnologie. Darüber hinaus ist das DFKI Partner des ZF-Technologiezentrums für KI und Cybersecurity. Zusätzlich betreibt das DFKI mit dem CERTLAB ein Labor für Zertifizierung und Digitale Souveränität, welches KI-Systeme unter anderem hinsichtlich ihrer Sicherheit untersucht. Das Kompetenzzentrum Sichere Systeme am DFKI setzt sich mit dem Spannungsfeld zwischen innovativer Softwareentwicklung, IT-Sicherheit und öffentliche Sicherheit auseinander.

Thematische Schwerpunkte (Auszug)

Konzeption und Vorgehensweisen

 # Kryptographie #Quanten-Kryptographie & Post-Quanten-Kryptographie #Datenschutz

Im Rahmen eines langfristigen Projektes zur Verschlüsselung medizinischer Daten entwickelt das DFKI bspw. eine effektive Post-Quanten-Kryprographie. Auch wird das Thema Datenschutz behandelt.

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen #Cloudsicherheit

Das DFKI forscht an der Entwicklung sicherer Cloud-Lösungen, bspw. zur intelligenten Nutzung erneuerbarer Energien in Smart Energy Micro Grids.

Infrastrukturelle Sicherheitsaspekte

#physische IT-Sicherheit

Das Kernthema eines der Forschungsprojekte des DFKI ist bspw. physikalische Sicherheit durch dynamische Hardware-Rekonfiguration.

Netze und Kommunikation

#Netzarchitektur und -design

Das DFKI forscht zu sicheren Netzen und Kommunikation, z.B. im Bereich neuer Netzwerkarchitektur für das industrielle Internet oder skalierbarer Sicherheitsarchitekturen für Geschäftsprozesse von Häfen.

Vernetzung von Systemen, IoT

#Künstliche Intelligenz

Kernthema des DFKI ist die Künstliche Intelligenz. Im Rahmen diverser Projekte wird auch an im Themenfeld vernetze Systeme, wie etwa Industrie 4.0, Gebäudeautomation oder in der modernen Landwirtschaft geforscht.

Zielgruppe

Wissenschaft

Wirtschaft

- Aerospace / Luft- und Raumfahrt
- Automobilbranche / Automotive
- Baugewerbe
- Energieversorgung
- Handel
- Information und Kommunikation
- Land- und Forstwirtschaft
- Maritimes Gewerbe

Die verschiedenen Projekte des DFKI dienen zum einen der Forschung, sprechen je nach Projektausrichtung und -beteiligung aber auch wirtschaftliche Akteure an.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Entwicklung

Das DFKI betreibt anwendungsorientierte Grundlagenforschung und entwickelt Prototypen und einsatzfähige Softwarelösungen.

Information

- Wissenschaftliche Veröffentlichung

Das DFKI publiziert Ergebnisse aus ihrer Forschungstätigkeit.

Produkt

- Software

Das Ergebnis von Projekten des DFKI können Softwareprototypen oder patentfähige Lösungen sein.

CYSEC - Profilbereich für Cybersicherheit an der TU Darmstadt

Beitrag zur Cybersicherheit

Kontakt:

Prankratiusstr. 2

64289 Darmstadt

cysec.tu-darmstadt.de

Wissenschaftlicher Akteur

Im Profilbereich Cybersicherheit (CYSEC) arbeiten Wissenschaftlerinnen und Wissenschaftler der TU Darmstadt an zentralen Themen der Cybersicherheit und des Privatheitsschutzes. CYSEC ist einer von sechs Profilbereichen der TU Darmstadt. Ziel der Profilbereiche ist es, Grundlagen zu erforschen, Lösungen für gesellschaftliche Herausforderungen zu schaffen, Kompetenzen über die einzelnen Fachbereiche hinweg zu bündeln und Forschungsnetzwerke mit Partnern aller Gesellschaftsgruppen zu bilden. Innerhalb der TU Darmstadt stellt CYSEC eine Plattform für den interdisziplinären Austausch und die Förderung des akademischen Nachwuchses dar. An CYSEC sind derzeit insgesamt 33 Fachgebiete aus acht Fachbereichen der TU Darmstadt beteiligt: Informatik, Physik, Elektrotechnik und Informationstechnik, Gesellschafts- und Geschichtswissenschaften, Biologie, Humanwissenschaften, Maschinenbau, Rechts- und Wirtschaftswissenschaften. In Verbund- und Einzelprojekten betreibt CYSEC Grundlagen- und anwendungsorientierte Forschung. Die TU Darmstadt ist Mitwirkende am Nationalen Forschungszentrum für angewandte Cybersicherheit ATHENE. In diesem Zusammenhang tragen eine Reihe von Wissenschaftlerinnen und Wissenschaftler, die dem Profilbereich CYSEC zugeordnet sind, mit ihrer Forschung zu ATHENE bei.

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Die TU Darmstadt trägt über CYSEC mit ihren Kernkompetenzen in Forschung und Lehre zur Stärkung des Standortes Darmstadt bei. Der Profilbereich Cybersicherheit arbeitet mit den unterschiedlichen Netzwerk- und Medienpartnern in der Region z.B. im Rahmen von Bürgerinnen und Bürgerdialogen und Podcast-Formaten zusammen.

Bildung und Awareness

#Awareness in der Politik #Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft #Schulisches Bildungsangebot #Berufliches Bildungsangebot #Universitäres Bildungsangebot

CYSEC fördert die gesamtgesellschaftliche Sensibilisierung für Cybersicherheit durch Events wie Feriencamps oder Aktionen zum „Girls' Day“. Außerdem ist CYSEC in das Lehrangebot der TU Darmstadt eingebunden.

Konzeption und Vorgehensweisen

#Kryptographie #Quanten-Kryptographie & Post-Quanten-Kryptographie #Blockchain #Authentifizierung #Informationssicherheitsmanagement #Endgerätesicherheit #Identitätsmanagement #Berechtigungsmanagement #Datenschutz

Ein Kernbereich der Forschung von CYSEC ist Kryptographie. Der Schwerpunkt "Privatheit und Vertrauen" forscht zu Herausforderungen im Bereich Privatsphäre.

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen #Cloudsicherheit

Die Forschung von CYSEC im Bereich der Cloud Security fokussiert die Durchsetzung hoher Vertraulichkeitsstandards und Integrität von ausgelagerten Daten und Berechnungen. Außerdem untersucht CYSEC neuartige virtuelle Systemarchitekturen und Programmierungsmodelle, um die Sicherheit von Cloud-Umgebungen weiter zu verbessern. Weitere Schwerpunkte sind Anomalie- und Angriffsdetektion in Netzen und IT-Systemen sowie biometriebasierte Authentifikationsverfahren.

Detektion und Reaktion

#Behandlung von Sicherheitsvorfällen & IT-Forensik

Neben dem Schwerpunkt "Sichere Softwaresysteme" thematisiert CYSEC auch das Forschungsgebiet "Nachweisbare Sicherheit", in welchem die Verifikation der Sicherheit von IT-Systemen untersucht wird. CYSEC liefert Methoden und Werkzeuge für eine Verifikation der Sicherheit von IT-Systemen. Außerdem befasst sich die Forschung von CYSEC auch mit den Schritten vor und nach der Verifikation, d.h. wie man Sicherheitsaspekte so erfasst, dass sie für die Verifikation geeignet sind, und

auch wie die Prüfungsergebnisse an verschiedene Stakeholder kommuniziert werden können.

Infrastrukturelle Sicherheitsaspekte

#Betriebs- und Steuerungstechnik #Intelligente Messsysteme #physische IT-Sicherheit

Weitere Schwerpunkte sind Sicherheit in Sensorik und cyberphysiaklischen Systemen.

Netze und Kommunikation

#Netzarchitektur und -design #Netzkomponenten

Ein weiterer Forschungsschwerpunkt von CYSEC liegt in der Sicherheit des Internets und Kritischer Infrastrukturen.

Vernetzung von Systemen, IoT

#Smart Home #Autonomes Fahren #Fahrassistenzsysteme #Künstliche Intelligenz

Die Forschung in CYSEC beschäftigt sich auch mit der Anwendung von IT-Sicherheit innerhalb des IoT.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger
- Kinder und Heranwachsende
- Akademikerinnen und Akademiker
- Medien

Mit universitären Lehrangeboten, medialen Beiträgen, Vorträgen und Ferienbetreuungsangebote schafft CYSEC Awareness in der Zivilgesellschaft.

Wissenschaft

- Forschungseinrichtung

Als Forschungsbereich adressiert CYSEC andere Partner aus der Wissenschaft.

Wirtschaft

- Aerospace / Luft- und Raumfahrt
- Automobilbranche / Automotive
- Energieversorgung
- Gesundheits- und Sozialwesen
- Information und Kommunikation
- Beratung
- Verkehr / Infrastruktur
- Kritische Infrastruktur

CYSEC kooperiert mit verschiedenen Unternehmen diverser Branchen und Sparten.

Staat

- Bund
- Land
- Behörde/Verwaltung
- Ministerium

CYSEC arbeitet eng mit verschiedenen Bundes- und Landesbehörden, wie u.a. dem BSI oder dem Hessen CyberCompetenceCenter (Hessen3C) zusammen und unterstützt Messestände und Konferenzen der hessischen Ministerien.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Ausbildung und Schulung
- Beratung
- Konzept
- Prüfung/Audits/Zertifizierung/Standardisierung

Information

- Informationsaufbereitung
- Literatur
- Lernprogramm
- Newsletter
- Öffentlichkeitsarbeit
- Wissenschaftliche Veröffentlichung
- Studie

Aus der Forschung gehen verschiedene wissenschaftliche Veröffentlichungen und Informationen hervor. Im Bereich Lehre werden Lehrveranstaltungen und der Masterstudiengang "IT-Sicherheit" angeboten.

Distributed Artificial Intelligence Laboratory (DAI-Labor)

Beitrag zur Cybersicherheit

Die Technische Universität Berlin unterhält in ihrem Distributed Artificial Intelligence Laboratory (DAI-Labor) das Competence Center Security (CC Security), ein Forschungszentrum, sowie das Anwendungszentrum Cybersecurity. Während das CC Security sich mit Forschungsfragen rund um „intelligente“ Cybersicherheit in Verbindung mit Telekommunikations- und Informationsnetzwerken befasst, liegt der Schwerpunkt des Anwendungszentrums Cybersecurity auf Anwendungsforschung und Entwicklung von intelligenten Lösungen zum Schutz Kritischer Infrastrukturen.

Ansprechpartner:

Sekr. TEL 14

Ernst-Reuter-Platz 7

10587 Berlin

dai-labor.de

Wissenschaftlicher Akteur

Thematische Schwerpunkte (Auszug)

Bildung und Awareness

#Universitäres Bildungsangebot

Vom CC Security werden Lehrveranstaltungen an der TU Berlin angeboten. Themen in diesen Veranstaltungen sind der Einsatz von künstlicher Intelligenz im Bereich Cybersicherheit und Sicherheitsaspekte in der Softwareentwicklung.

Konzeption und Vorgehensweisen

#Informationssicherheitsmanagement #Endgerätesicherheit

Im Vordergrund stehen u.a. KI-basierte Lösungen für den Schutz Kritischer Infrastrukturen, die auf Sicherheit, Robustheit und Erhalt der Verfügbarkeit abzielen. Schwerpunkte hierbei sind IT-Risikomanagement, Erkennung von Angriffen und Schwachstellen, Vorhersage von Bedrohungen und automatisierte Reaktionen. Darüber hinaus geht es auch um Themen der mobilen Sicherheit, insbesondere im Hinblick auf Privatsphäre und Stärkung der Datensouveränität.

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen #Monitoring

Schwerpunktmäßig beschäftigt sich das DAI-Labor mit Systemen zur kontinuierlichen Sicherheitsüberprüfung von IT-Systemen, der Erkennung möglicher Bedrohungen und Angriffen und der Reaktion auf erkannte Sicherheitsprobleme.

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen #Behandlung von Sicherheitsvorfällen & IT-Forensik

Ein weiterer Forschungsschwerpunkt ist bspw. intelligente Anomalieerkennung. Ein besonderes Interesse liegt dabei auf der Evaluation von KI-basierten Sicherheitslösungen und der Erzeugung synthetischer Daten zur Evaluation.

Infrastrukturelle Sicherheitsaspekte

#SPS & ICS #physische IT-Sicherheit

Die Sicherheit in intelligenten (Strom-)Netzen (Smart Grids) und anderen cyber-physischen Systemen sind Schwerpunktthemen des Anwendungszentrums Cybersicherheit.

Netze und Kommunikation

#Netzarchitektur und -design #Netzkomponenten #Netzmanagement #Funknetze

Forschungsfragen rund um Netzwerk- und Sicherheitssimulation zählen zu den Schwerpunkten des DAI-Labors. Ein Open Source Projekt des CC Security ist ein selbst entwickeltes Werkzeug zur Netzwerksimulation.

Vernetzung von Systemen, IoT

#Smart Home #Autonomes Fahren #Künstliche Intelligenz

Das DAI-Labor beschäftigt sich seit längerem mit Smart Homes und betreibt eine Teststrecke für autonomes Fahren in Berlin. Die Lösungen des CC Security kommen auch in Projekten zu diesen Themen zum Einsatz.

Zielgruppe

Wissenschaft

- Forschungseinrichtung

Das DAI-Labor verfolgt den Living Lab-Ansatz einer offenen Umgebung für Experimente, in der Forscher, Industrie und Öffentlichkeit gemeinsam kreative Ideen verwirklichen können.

Wirtschaft

- Energieversorgung
- Information und Kommunikation
- Verkehr / Infrastruktur
- Wasserver- und -entsorgung
- Kritische Infrastruktur

Ein Fokus wird vor allem auf Kritische Infrastrukturen gelegt.Das CC Security entwickelt Lösungen zur Evaluation der Bedrohungslage in behördlichen Netzwerken.

Staat

- Behörde/Verwaltung

Das CC Security entwickelt Lösungen zur Evaluation der Bedrohungslage in behördlichen Netzwerken.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Ausbildung und Schulung
- Beratung
- Entwicklung
- Konzept

In den Kompetenz- und Anwendungszentren erforscht und entwickelt das DAI-Labor Lösungen zu verschiedenen Cybersicherheitsthemen.

Information

- Informationsaufbereitung
- Wissenschaftliche Veröffentlichung
- Studie

Das DAI-Labor veröffentlicht im Rahmen seiner Forschung insb. Studien und Publikationen.

Produkt

- Software

Ergebnisse aus Forschungsprojekten stehen Interessenten aus der Wirtschaft und der Verwaltung für gemeinsame Evaluations-/Forschungsprojekte zur Verfügung.

Exzellenzcluster CASA: Cybersicherheit im Zeitalter großskaliger Angreifer

Beitrag zur Cybersicherheit

Der Exzellenzcluster CASA ist am Horst-Görtz-Institut für IT-Sicherheit der Ruhr-Universität Bochum angesiedelt. Hier forschen Wissenschaftler aus der Computersicherheit, der Kryptographie, der Elektrotechnik, Mathematik und Psychologie zur nachhaltigen Sicherheit vor großskaligen Angreifern. Das Forschungsprojekt wird zunächst für sieben Jahre mit rund 30 Millionen Euro von der Deutschen Forschungsgemeinschaft gefördert. Die Grundlagen-Forschung verfolgt einen interdisziplinären Ansatz, der nicht nur technische Fragen adressiert, sondern sich auch der Interaktion zwischen menschlichem Verhalten und IT-Sicherheit widmet. Thematisch gliedert sich CASA in die Schwerpunkte "Kryptographie der Zukunft", "Eingebettete Sicherheit", "Sichere Systeme" sowie "Benutzerfreundlichkeit". Mittels eines Transferlabors sollen Forschungsergebnisse praktische Anwendung in der realen Welt finden.

Ansprechpartner:

Exzellenzcluster CASA / Horst Görtz Institut für IT-Sicherheit

Universitätsstr. 150

44780 Bochum

casa.rub.de

Wissenschaftlicher Akteur

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Der Transfer wissenschaftlicher Ergebnisse in die Praxis ist ein zentraler Bestandteil des Exzellenzclusters. CASA profitiert hier vom großen Kooperationsnetzwerk des schon lange bestehenden Horst Görtz Instituts für IT-Sicherheit, das aus mehr als 50 Partnern auf der ganzen Welt besteht – von Behörden über spezialisierte Unternehmen bis hin zu Global Playern.

Bildung und Awareness

#Awareness in der Politik #Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft #Sonstiges Bildungsangebot

Mit einer breiten Öffentlichkeitsarbeit aus lokalen Events, Online-Lesungen, Zeitungsreportagen oder Whitepapers vermittelt CASA die Relevanz der IT-Sicherheits-Forschung verschiedenen Zielgruppen. Distinguished Lectures bspw. stehen allen Interessierten offen. Mit Gastlesungen für die lokale Öffentlichkeit schärft CASA zudem auch das Bewusstsein von Laien gegenüber Themen der IT-Sicherheit.

Konzeption und Vorgehensweisen

#Kryptographie #Quanten-Kryptographie & Post-Quanten-Kryptographie #Authentifizierung #Endgerätesicherheit #Datenschutz #IT-Sicherheitsstandards

Der Forschungsschwerpunkt "Kryptographie der Zukunft" beschäftigt sich mit Themen wie der Kryptographie zum Schutz der Privatsphäre und von Betriebsgeheimnissen sowie neuen Ansätzen zu quanten-resistenter Verschlüsselung, die im Standardisierungsprozess um Post-Quanten-Kryptographie des National Institute of Standards and Technology (NIST) Anwendung finden.

Im Bereich der „Eingebetteten Sicherheit“ wird untersucht, wie Schwachstellen auf Hardware-Ebene eliminiert werden können. Dazu werden nicht nur physikalische Backdoors und Plattform-Trojaner im Prozess des Hardware Reverse Engineering analysiert, sondern auch psychologische Studien zum besseren Verständnis der Arbeitsweise von Hackern erstellt.

Der Schwerpunkt des Forschungsbereichs "Sichere Systeme" widmet sich der Analyse von Schwachstellen auf der Software-Ebene und adressiert eine Entwicklung intelligenter Sicherheitssysteme. Hier werden unter anderem auch Methoden des Maschinellen Lernens genutzt, um Angriffstaktiken zu erforschen und neue Verteidigungsmechanismen zu entwerfen.

Dem Faktor Mensch in der IT-Sicherheit widmet sich der Forschungsschwerpunkt „Benutzerfreundlichkeit“. Dabei wird analysiert, wie menschliches Verhalten und technische Voraussetzungen so zusammenwirken, dass die Nutzbarkeit von Sicherheits- und Datenschutzmechanismen verbessert wird.

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen

In Kooperation mit investigativen Journalisten decken CASA-Wissenschaftler regelmäßig Sicherheitslücken und Datenschutz-Schwachstellen in realen Anwendungsgebieten auf.

Infrastrukturelle Sicherheitsaspekte

#physische IT-Sicherheit

Im Schwerpunkt "Eingebettete Sicherheit" wird insbesondere die Interaktion von Sicherheitssystemen mit der physikalischen Umgebung erforscht.

Netze und Kommunikation

#Funknetze

Im Forschungsschwerpunkt "Sichere Systeme" beschäftigen sich Forscher mit Schwachstellen in Mobilfunknetzen (LTE und 5G). Dabei stehen sie im Austausch mit Telekommunikationsunternehmen, die ihre Produkte mit Hilfe der Forschungsergebnisse verbessern können.

Vernetzung von Systemen, IoT

#Smart Home #Autonomes Fahren #Künstliche Intelligenz

CASA-Forscher haben unter anderem Schwachstellen in Sprachassistenten aufgedeckt und neue mathematische Verfahren zur automatisierten Detektion von computergenerierten Bildern (Deep Fakes) entwickelt. Außerdem analysieren sie neue Verfahren zur Absicherung von Hardware und Software, die auch im Bereich des Autonomen Fahrens genutzt werden.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger
- Kinder und Heranwachsende
- Akademikerinnen und Akademiker
- Angestellte
- Familien
- Seniorinnen und Senioren
- Medien
- NGO
- priv. Stiftung
- Hacker
- Partei

Wissenschaft

- Forschungseinrichtung

Wirtschaft

- Aerospace / Luft- und Raumfahrt
- Automobilbranche / Automotive
- Energieversorgung
- Freiberufliche wissenschaftliche technische Dienstleistungen
- Information und Kommunikation
- Beratung
- Verkehr / Infrastruktur
- Kritische Infrastruktur

Ziele des Projektes sind der Ausbau der Grundlagenforschung auf dem Gebiet der Cybersicherheit und die Integration der Ergebnisse in die Praxis.

Staat

- Bund
- Land
- Ausschuss/Gremium
- Behörde/Verwaltung
- Einrichtung
- Ministerium
- öfftl. Stiftung

Ziel des Exzellenzclusters CASA ist es, nachhaltige IT-Sicherheit gegen großskalige Angreifer zu entwickeln. Dazu gehören vor allem national-staatliche Angreifer, die eine reale Bedrohung für die nationale Sicherheit bedeuten können.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Journalismus
- Investigativer Journalismus
- Newsletter
- Öffentlichkeitsarbeit
- Wissenschaftliche Veröffentlichung
- Studie

Die Ergebnisse der Forschungsarbeit des CASA werden in Form von Publikationen veröffentlicht. Durch die Zusammenarbeit mit investigativen Journalisten wird das Thema IT-Sicherheit außerdem von CASA in die Öffentlichkeit gebracht. Durch strukturelle Öffentlichkeitsarbeit werden Forschungsergebnisse in verschiedenen Formen (Events, Social Media, Pressemitteilungen) an die breite Öffentlichkeit sowie an ein wissenschaftlich interessiertes Fachpublikum kommuniziert.

Fach- und Arbeitsgruppen der IT-Sicherheit an der Hochschule Darmstadt (h_da)

Beitrag zur Cybersicherheit

An der Hochschule Darmstadt (h_da) forschen interdisziplinär vier Arbeitsgruppen im Bereich der IT-Sicherheit. Schwerpunktthemen sind dabei Biometrie und Internetsicherheit, User-Centered Security, mobile und sichere Telekommunikationsdienste und sichere Ende-zu-Ende Kommunikationsplattformen. Die Fachgruppe IT-Sicherheit koordiniert zentralisiert die Forschung, Lehre und Weiterbildung an der h_da.

Kontakt:

Haardtring 100

64295 Darmstadt

h-da.de/forschung/-forschungsthemen/it-sicherheit/

Wissenschaftlicher Akteur

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Die h_da wirkt in ATHENE (Nationales Forschungszentrum für angewandte Cybersicherheit) mit. Sie arbeitet dort in diversen Projekten eng mit der TU Darmstadt, dem Fraunhofer SIT und Fraunhofer IGD sowie dem CAST e.V.

Bildung und Awareness

#Universitäres Bildungsangebot #Sonstiges Bildungsangebot

Die h_da bietet den kooperativen Studiengang IT-Sicherheit sowie diverse Weiterbildungsangebote an.

Konzeption und Vorgehensweisen

#Kryptographie #Authentifizierung #Identitätsmanagement #Berechtigungsmanagement

Forschungsthemen der Arbeitsgruppen der h_da umfassen Personenerkennung mittels Fingerabdrucks bzw. Sprache sowie mobile Telekommunikationsdienste zur gegenseitigen Authentifizierung und Identifizierung von Gesprächsteilnehmern.

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen

Die Entwicklung und Implementierung von Software und IT-Systeme unter Anwendung der Methoden der Mensch-Maschine-Interaktion sind Themen der Arbeitsgruppe User-Centered Security der h_da.

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen #Behandlung von Sicherheitsvorfällen & IT-Forensik

Die Arbeitsgruppe da/sec der h_da forscht zu Themen der Angriffserkennung und -reaktion in Netzwerken sowie der digitalen Forensik.

Zielgruppe

Wissenschaft

- Bildungseinrichtung
- Forschungseinrichtung

Zielgruppe der h_da sind Wissenschaft und Lehre.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Ausbildung und Schulung
- Entwicklung
- Sonstige Dienstleistung

Neben wissenschaftlicher Forschung und Entwicklung werden an der h_da der Kooperative Studiengang IT-Sicherheit (KITS) sowie weitere Module und Weiterbildungen zur IT-Sicherheit angeboten.

Information

- Wissenschaftliche Veröffentlichung
- Studie
- Sonstiges Informationsangebot

Im Rahmen der Forschungsarbeit mehrerer Arbeitsgruppen werden von der h_da insb. wissenschaftliche Publikationen und Studien veröffentlicht.

Forschungsinstitut Cyber Defence und Smart Data (CODE)

Beitrag zur Cybersicherheit

Ansprechpartner:

Universität der Bundeswehr München

Werner-Heisenberg-Weg 39

85579 Neubiberg

unibw.de/code

Wissenschaftlicher Akteur

Das Forschungsinstitut (FI) (CODE) wurde mit der Satzung vom Februar 2017 als zentrale wissenschaftliche Einrichtung der Universität der Bundeswehr München (UniBw M) errichtet. CODE ist die ressorteigene, universitäre Forschungseinrichtung der Bundeswehr und des Bundes. Das FI CODE betreibt Grundlagen-, Ressort- sowie anwendungsorientierte und Auftragsforschung in verschiedenen Bereichen der Cybersecurity. Das FI CODE verfolgt das Ziel, Innovationskompetenzen aus Forschung und Industrie zu bündeln sowie die Interaktion, sowohl mit Behörden als auch der Industrie, zu stärken. Im Einzelnen sind dies Auftragsforschung und wissenschaftliche Dienstleistungen im Themenfeld Cybersicherheit, Anstoßen von Produktentwicklungen aus Forschungsvorhaben sowie die Unterstützung von Start-ups. Des Weiteren die Aus-, Fort- und Weiterbildung von Offizieren, zivilen Studierenden, Doktoranden, PostDocs, Mitarbeiterinnen und Mitarbeitern der Bundeswehr und anderen Behörden des Bundes mit dem Schwerpunkt Cybersicherheit sowie politische, strategische und wissenschaftliche Beratung der CODE Stakeholder. Zudem der Aufbau des europäischen CODE-Ökosystems (Cybercluster). Die Forschungsthemen gliedern sich thematisch in die drei Forschungscluster Cyber Defence, Smart Data (inkl.KI und ML) und Quantentechnologien.

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

CODE verfolgt das Ziel, durch eine enge Verknüpfung der akademischen Community, dem Bedarfsträger BMVg, Sicherheitsbehörden und der Industrie, bestehende Innovationskompetenzen auszuschöpfen und internationale Cybersicherheitsforschung zu betreiben. Durch eine enge und einzigartige Vernetzung der genannten Stakeholder treibt CODE strategische Initiativen zur Cybersicherheit der Gesellschaft auf nationaler und internationaler Ebene voran und ist zentraler Ansprechpartner für die technologische Weiterentwicklung.

Bildung und Awareness

#Universitäres Bildungsangebot #Schulung #Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft #Awareness in der Politik #Sonstiges Bildungsangebot

An der Universität der Bundeswehr München werden mit Unterstützung des FI CODE Bachelor- und Masterstudiengänge mit Bezug zu Cyber- und IT-Sicherheit angeboten. Das FI CODE veranstaltet zudem Workshops, Konferenzen und Veranstaltungen zu diversen Themen aus dem Gebiet der Cybersicherheit.

Konzeption und Vorgehensweisen

#Endgerätesicherheit #Datenschutz

Die Forschungsarbeit des FI CODE ist in die drei Forschungscluster Cyber Defence, Smart Data und Quantentechnologienunterteilt. Geforscht wird u.a. in den Bereichen der Netzsicherheit, sicheren Softwareentwicklung, Data Science und Härtung von IT-Systemen.

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen #Monitoring #Kryptographie #Quanten-/Post-Quanten-Kryptographie #Authentifizierung #ISMS #Endgerätesicherheit #Identitäts- und Berechtigungsmanagement #Compliance Management #Datenschutz

In den Forschungsfeldern „Cyber-Sicherheit“ und „Smart Data“ von CODE wird vor allem Auftrags- und Ressortforschung durchgeführt. Bedrohungsanalyse in der Luft- und Raumfahrt ist eines dieser Themen.

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen #Behandlung von Sicherheitsvorfällen & IT-Forensik

Angriffsdetektion ist einer der Forschungsschwerpunkte von CODE, welcher sowohl in zivilem als auch im militärischen Kontext erforscht wird.

Infrastrukturelle Sicherheitsaspekte

Die universitäre Forschung von CODE im Bereich Kritischer Infrastrukturen deckt vor allem und Cyberabwehr zur Aufrechterhaltung von Systemen ab.

Zielgruppe

Zivilgesellschaft

Wissenschaft

Wirtschaft

Staat

Ziel von CODE ist neben der Forschung auch die stärkere Verknüpfung von Wissenschaft, Wirtschaft und Behörden im Bereich der Cybersicherheit.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Wissenschaftliche Veröffentlichung
- Studie

CODE betreibt sowohl Grundlagenforschung als auch anwendungsorientierte Forschung. Das Institut forscht aber auch für Ressorts und auf Auftrag. Zusätzlich bietet CODE verschiedene Studienangebote im Bereich Cybersicherheit an. Darüber hinaus führt CODE eine jährliche Konferenz durch, bei der sich Experten aus Wissenschaft, Wirtschaft und Politik austauschen können.

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC

Beitrag zur Cybersicherheit

Kontakt:

Lichtenbergstr. 11

85748 Garching

aisec.fraunhofer.de

Wissenschaftlicher Akteur

Der Fokus des Fraunhofer AISEC liegt in der Unterstützung von Unternehmen bei der Absicherung ihrer Systeme, Infrastrukturen, Produkte und Angebote. Im Spannungsfeld zwischen wirtschaftlichen Erfordernissen, Benutzerfreundlichkeit und Sicherheitsanforderungen entwickeln die Mitarbeitenden Sicherheits-Technologien zur Erhöhung der Verlässlichkeit, Vertrauenswürdigkeit und Manipulationssicherheit von IT-basierten Systemen und Produkten. Das Kompetenzfeld des Fraunhofer AISEC erstreckt sich von der integrierten Sicherheit eingebetteter Systeme und Hardware-Komponenten über Betriebssysteme, Applikationen und Cloud-basierte Services bis hin zu Lösungen zur sicheren Software- und System-Entwicklung und zur Nutzung Maschineller Lerntechniken für die Cybersicherheit sowie der Sicherheit von Industrieanlagen und Automotive-Systemen. Mit dem AISEC-Cybersicherheitszentrum werden zusätzlich hochmoderne Laborumgebungen für die Forschungs- und Entwicklungsarbeit im Bereich Cybersicherheit zur Verfügung gestellt.

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Das Fraunhofer AIESEC ist mit zahlreichen Partnern der öffentlichen Hand oder aus der Wirtschaft verbunden und vernetzt sich zudem intensiv über seine Mitwirkung in einschlägigen IT-Organisationen. Strategische Partnerschaften mit global agierenden Industrieunternehmen sowie mit internationalen Universitäten, insbesondere der TU München, garantieren wissenschaftliche Exzellenz der Forschungsarbeit sowie deren marktgerechte Umsetzung.

Bildung und Awareness

#Schulung #Awareness in der Politik #Awareness in der Wirtschaft #Berufliches Bildungsangebot #Universitäres Bildungsangebot

Im Rahmen des Lernlabors Cybersicherheit bietet das Fraunhofer AISEC Schulungen mit dem Schwerpunkt Embedded Systems, Mobile Security, IoT und weiteren Themen an. Der Fokus der Schulungen liegt auf der praktischen Anwendungsorientierung von IT-Security-Techniken, die durch ein modulares, berufsbegleitendes und bedarfsorientiertes Weiterbildungskonzept vermittelt werden. Über die Anbindungen an die TU München, die FU Berlin sowie die OTH Amberg-Weiden bieten Mitarbeitende des Fraunhofer AISEC diverse universitäre Bildungsangebote an.

Konzeption und Vorgehensweisen

#Kryptographie #Quanten-Kryptographie & Post-Quanten-Kryptographie #Blockchain #Authentifizierung #Endgerätesicherheit #Identitätsmanagement #Berechtigungsmanagement #Datenschutz

Das Fraunhofer AISEC forscht an modernen Verschlüsselungstechniken, um Systeme und Daten abzusichern. Schwerpunkte bilden unter anderem ABE-Verfahren, Post-Quantum-Kryptographie, aber auch datenschutzbewahrende Verfahren wie Searchable Encryption. Das Fraunhofer AISEC entwickelt moderne, dezentrale Identitätsmanagementlösungen, die es Nutzern ermöglicht, digitale Identitäten und Attribute sicher und selbstbestimmt zu verwalten und anderen Parteien zur Verfügung zu stellen. Zudem entwickelt das Fraunhofer AISEC Lösungen für eine sichere Nutzung mobiler Endgeräte im Unternehmensumfeld, ohne die private Nutzung zu beschränken.

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen #Cloudsicherheit

Das Fraunhofer AISEC betreibt ein Cloud-Security-Labor, in dem Lösungen, Werkzeuge und Umgebungen zur Verfügung stehen, um alle Komponenten eines Cloud-Ökosystems zu analysieren und die Sicherheit von Cloud-basierten Diensten kontinuierlich zu überprüfen und zu erhöhen. Darüber hinaus umfasst das Angebot des Cloud-Labors Interoperabilitätstests und die Vergleichsanalyse von Sicherheitsfunktionen. Das Fraunhofer AISEC betreibt ein Cloud-Security-Labor, in dem Lösungen, Werkzeuge und Umgebungen zur Verfügung stehen, um alle Komponenten eines Cloud-Ökosystems

zu analysieren und die Sicherheit von Cloud-basierten Diensten kontinuierlich zu überprüfen und zu erhöhen. Darüber hinaus umfasst das Angebot des Cloud-Labors Interoperabilitätstests und die Vergleichsanalyse von Sicherheitsfunktionen.

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen

Das Fraunhofer AISEC erforscht mittels KI-basierter Verfahren kognitive Sicherheitslösungen, um automatisiert und mit hoher Treffergenauigkeit sicherheitsrelevante Ereignisse und Abweichungen vom erwarteten Normalverhalten zu detektieren.

Infrastrukturelle Sicherheitsaspekte

#SPS & ICS #physische IT-Sicherheit

Das Fraunhofer AISEC entwickelt technologische Schutzmaßnahmen und Methoden, um elektronische Geräte und Unternehmenswerte zu schützen. Ein Schwerpunkt liegt dabei auf der Entwicklung von Hardware- und Software-basierten Schutzmaßnahmen, um Systeme und Produkte vor Manipulationen oder Imitation zu schützen. Ein weiterer Fokus liegt auf der Abwehr von Angreifern, die physischen Zugriff auf ihr Angriffsziel besitzen, bspw. durch die Absicherung und Integration von Microcontrollern und Secure Elements.

Netze und Kommunikation

#Netzarchitektur und -design #Funknetze

Das Fraunhofer AISEC erforscht neueste Netzwerkarchitektur und erprobt diese im operativen Betrieb. Darüber hinaus betreibt das Fraunhofer AISEC Labore mit eigenen 3G/4G Basisstationen und führt darin Sicherheitsuntersuchungen durch. Im Bereich IoT erforscht das Fraunhofer AISEC skalierende und datenschutzbewahrende Lösungen für drahtlose Sensornetze.

Vernetzung von Systemen, IoT

#Smart Home #Autonomes Fahren #Künstliche Intelligenz

Das Fraunhofer AISEC betreibt ein eigenes Automotive-Security-Labor, das Sicherheitsuntersuchungen an kompletten Fahrzeugen ermöglicht. Während simulierten Fahrten können Sensordaten wie Laser, Radar oder Bildverarbeitungsdaten erfasst und analysiert werden.

In mehreren Laborumgebungen im Bereich Industrial Security ist es möglich, Security-Analysen in den Bereichen vernetzte Produktion, IoT oder Gebäudeautomation durchzuführen. Im Labor für kognitive Sicherheit entwickelt das Fraunhofer AISEC Lösungen zur Erkennung von Anomalien in vernetzten Systemen.

Zielgruppe

Wissenschaft

- Bildungseinrichtung
- Forschungseinrichtung

Das Fraunhofer AISEC adressiert mit seinen Leistungen wissenschaftliche Einrichtungen und kooperiert in Projekten mit Hochschulen und anderen Forschungseinrichtungen.

Wirtschaft

- Aerospace / Luft- und Raumfahrt
- Automobilbranche / Automotive
- Energieversorgung
- Gesundheits- und Sozialwesen
- Information und Kommunikation
- Verkehr / Infrastruktur
- Kritische Infrastruktur

Das Fraunhofer AISEC unterstützt Firmen aller Branchen und Dienstleistungssektoren und stellt seine Leistungen Wirtschaftsunternehmen branchenübergreifend zur Verfügung. Zu den Kunden des Fraunhofer AISEC zählen Hersteller, Zulieferer und Anwender unter anderem aus den Bereichen der Chipkartensysteme, Telekommunikation, dem Automobilbau und deren Zulieferindustrie, Logistik und Luftfahrt, Maschinenbau und Automatisierungstechnik, dem Gesundheitswesen, der Software-Industrie sowie dem öffentlichen Sektor und dem E-Government.

Staat

- Bund
- Land
- Behörde/Verwaltung

Das Fraunhofer AISEC entwickelt direkt einsetzbare Lösungen im Auftrag der öffentlichen Hand, erstellt Sicherheitskonzepte auf dem neuesten Stand der Technik und berät bei der Einführung von Informationssicherheitskonzepten in der öffentlichen Verwaltung.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Beratung
- Entwicklung
- Konzept
- Prüfung/Audits/Zertifizierung/Standardisierung

Das Fraunhofer AISEC unterstützt Unternehmen darin, ihre Infrastrukturen, Produktionsanlagen, Geschäftsprozesse und Vertriebsnetze sicher und verlässlich zu betreiben. Dafür berät das Fraunhofer AISEC Firmen bei der Implementierung von IT-Sicherheitsmaßnahmen in Hardware- und Softwarelösungen, erstellt Sicherheitskonzepte und entwickelt kundenindividuelle Sicherheitslösungen. Ebenso führt das Institut im Auftrag von Unternehmen Sicherheitsanalysen und Risk-Assessments durch, um Schwachstellen aufzudecken und entsprechende Schutzmaßnahmen zu entwickeln.

Information

- Informationsaufbereitung
- Literatur
- Newsletter
- Öffentlichkeitsarbeit
- Wissenschaftliche Veröffentlichung

Das Fraunhofer AISEC forscht an unterschiedlichen Disziplinen der Cybersicherheit und veröffentlicht diese Ergebnisse auf Konferenzen und in wissenschaftlichen Publikationen. Begleitet werden diese Veröffentlichungen durch zusätzliches Informationsmaterial und Maßnahmen der Presse- und Öffentlichkeitsarbeit.

Produkt

- Clouddienste/PaaS
- Software

Das Fraunhofer AISEC bietet mit dem Clouditor eine Lösung zur kontinuierlichen Überprüfung der Sicherheit von Cloudplattformen. Weitere Open-Source-basierte Produkte sind u.a. Software-Plattformen, die vertrauenswürdige Ausführungsumgebungen sowohl für mobile Endgeräte, Gateways und auch Server bereitstellen oder auch Sicherheitsanalysewerkzeuge zur automatisierten Schwachstellenanalyse

Fraunhofer-Institut für Sichere Informationstechnologie SIT

Beitrag zur Cybersicherheit

Das Fraunhofer SIT forscht mit über 200 Wissenschaftlerinnen und Wissenschaftlern an zentralen Sicherheitsherausforderungen für Zivilgesellschaft, Wirtschaft und Staat und betreibt praxisorientierte Forschung und Innovationsentwicklung. Das Fraunhofer SIT unterstützt seine Partner bei der Konzeption neuer IT-Systeme, dem Schutz von IT-Infrastrukturen sowie der Entwicklung neuer Produkte und Dienstleistungen. Gleichzeitig unterstützt das Fraunhofer SIT andere Organisationen in IT-Sicherheitsfragen und engagiert sich in der nationalen und internationalen Standardisierung. Das Fraunhofer SIT wirkt mit am Nationalen Forschungszentrums für angewandte Cybersicherheit ATHENE in Darmstadt.

Kontakt:

Rheinstr. 75

64295 Darmstadt

sit.fraunhofer.de

Wissenschaftlicher Akteur

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Das Fraunhofer SIT ist mit zahlreichen Partnern aus Wissenschaft, Wirtschaft und Staat verbunden und vernetzt sich zudem über seine Mitwirkung in nationalen und internationalen Interessensgruppen zu Cybersicherheit und Privatsphärenschutz. In eigenen Veranstaltungen und Formaten adressiert das Fraunhofer SIT die jeweilige Zielgruppe, wie bspw. in den "Eberbacher Gesprächen", wo ein gezielter Gedankenaustausch in Sachen IT-Sicherheit zwischen Industrie und Forschung vorangetrieben wird. In Forschungsprojekten kooperiert das Fraunhofer SIT weltweit mit anderen Forschungsinstitutionen im Bereich Cybersicherheit.

Bildung und Awareness

#Schulung #Awareness in der Politik #Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft #Berufliches Bildungsangebot

Das Fraunhofer SIT kooperiert in der beruflichen Weiterbildung mit dem TeleTrusT und bietet das TeleTrusT Information Security Professional (T.I.S.P.) Seminar an. Ein breites Themenspektrum zeigt sich im Lernlabor Cybersicherheit (LLCS), in dem das Fraunhofer SIT mit verschiedenen praktisch angelegten Schulungsschwerpunkten aus den Bereichen IT-Forensik, Embedded Systems und Automotive Security vertreten ist. Das Fraunhofer SIT betreibt zudem eine Cyber Range zur Simulation realistischer Sicherheitsszenarien.

Konzeption und Vorgehensweisen

#Kryptographie #Quanten-Kryptographie & Post-Quanten-Kryptographie #Blockchain #Authentifizierung #Informationssicherheitsmanagement #Endgerätesicherheit #Identitätsmanagement #Berechtigungsmanagement #Datenschutz #IT-Sicherheitsstandards

Das Fraunhofer SIT arbeitet an Techniken und Methoden um IT-basierte Systeme zu spezifizieren, zu analysieren, zu verifizieren und zu validieren. Es entwickelt bspw. Scanner zur Identifikation von Schwachstellen in Software, quantencomputerresistenten Verschlüsselungsverfahren oder Werkzeuge zur Durchführung von Bedrohungs- und Risikoanalysen sowie zur Konzeption von Sicherheitskonzepten.

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen #Cloudsicherheit #Monitoring

Das Fraunhofer SIT forscht an Methoden und Werkzeugen zur Erkennung von und Reaktion auf Cyberangriffe, an der Wiederherstellung eines sicheren Zustands in komplexen Systemen nach Angriffen. Zudem entwickelt es Sicherheitsarchitekturen und Prozesse zur Angriffsvermeidung und Schadensreduktion. Das Fraunhofer SIT erstellt und implementiert Sicherheitskonzepte zur Einbindung von Cloud-Angeboten, bewertet Sicherheitsmechanismen von Cloud-Anbietern sowie Service-Level-Agreements und hilft bei der Einhaltung rechtlicher Vorgaben. Zusätzlich führt das Fraunhofer SIT Machbarkeitsstudien über die Auslagerung von Daten und Diensten in die Cloud durch.

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen #Behandlung von Sicherheitsvorfällen & IT-Forensik

Zur Unterstützung der IT-Administrationsaufgaben in Organisationen bietet das Fraunhofer SIT Trainingsangebote auf seiner Cyber Range an. Im Feld der IT-Forensik werden Tools zur forensischen Analyse untersucht und weiterentwickelt. Auch wird an den Themen Textforensik, Datenträgerforensik und Bildforensik geforscht.

Infrastrukturelle Sicherheitsaspekte

#physische IT-Sicherheit

Das Fraunhofer SIT entwickelt Technologien, die die dynamische M2M-Kommunikation im Rahmen von Industrie 4.0 effizient und sicher unterstützen, wie bspw. hardwarebasierte Sicherheit, Protokolle, Security Management und Monitoring.

Netze und Kommunikation

#Netzarchitektur und -design #Netzkomponenten

Das Fraunhofer SIT beschäftigt sich in seiner Forschung sehr intensiv mit Internetsicherheit. Die Forscherinnen und Forscher des Fraunhofer SIT untersuchen Sicherheitslücken in Standards und im Design oder der Implementierung der verwendeten Systeme und Dienste für ein breites Spektrum von Angriffen, darunter bspw. Denial of Service-Angriffen (DoS) oder Advanced Persistent Threats.

Vernetzung von Systemen, IoT

#Autonomes Fahren #Fahrassistenzsysteme #Künstliche Intelligenz

Das Fraunhofer SIT beschäftigt sich mit den Sicherheits- und Datenschutzaspekten von Cyber-Physical Systems (CPS). Ein weiterer Bereich der Forschung des Fraunhofer SIT behandelt zudem Sicherheitsfragen in modernen Automobilen, insbesondere im Rahmen des autonomen Fahrens und in Smart Cities.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger
- Kinder und Heranwachsende
- Akademikerinnen und Akademiker
- Angestellte
- Medien

Das Fraunhofer SIT informiert Bürgerinnen und Bürgerinnen und Bürgerinnen und Bürgern über aktuelle Erkenntnisse und Forschungsthemen. Hierfür nutzen die Forscherinnen und Forscher verschiedene mediale Formate wie Web Talks, Diskussionsforen, soziale Netzwerke, Podcasts und auch an Bürgerinnen und Bürgerinnen und Bürgerinnen und Bürger gerichtete Präsenzveranstaltungen zu Themen der Cybersicherheit und des Privatsphärenschutzes.

Wissenschaft

- Bildungseinrichtung
- Forschungseinrichtung

Das Fraunhofer SIT steht in engen Austausch zu diversen anderen wissenschaftlichen Einrichtungen und organisiert bspw. auch Fachkonferenzen. Auch beteiligt sich das Fraunhofer SIT im Rahmen der Hochschullehre.

Wirtschaft

- Automobilbranche / Automotive
- Energieversorgung
- Finanzdienstleistung
- Handel
- Information und Kommunikation
- Sonstiges verarbeitendes Gewerbe
- Verkehr / Infrastruktur
- Kritische Infrastruktur

Die Forschung und Entwicklung des Fraunhofer SIT ist darauf angelegt, gewonnene Expertisen und Ergebnisse in die Wirtschaft zu transferieren. Neben dem Wissenstransfer richtet sich das Fraunhofer SIT mit verschiedenen Trainings- und Weiterbildungsangeboten an die Zielgruppe Wirtschaft.

Staat

- Bund
- Land
- Behörde/Verwaltung
- Einrichtung
- Ministerium
- öfftl. Stiftung

Das Fraunhofer SIT ist mit zahlreichen Partnern der öffentlichen Hand verbunden und steht im ständigen Austausch mit Ministerien auf Bund- und Länderebene. Das Fraunhofer SIT hat bspw. bei der Sicherheitsanalyse der Corona-Warn-App mitgewirkt.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Beratung
- Entwicklung
- Konzept
- Prüfung/Audits/Zertifizierung/Standardisierung

Das Fraunhofer SIT unterstützt Unternehmen bei der Entwicklung von IT-Sicherheitsmaßnahmen, erstellt Konzepte und entwickelt kundenindividuelle Sicherheitslösungen. Ebenso führt das Fraunhofer SIT im Auftrag Audits durch. Das Spektrum reicht von Anforderungs- und Bedrohungsanalysen, Sicherheitsanalysen von Software, Diensten, Hardware, Netzen, Primitiven oder Protokollen bis hin zur Erkennung von Schwachstellen, Detektion von Angriffen, forensische Analysen und Analysen von Daten zur Erkennung von Fakes bzw. Deepfakes.

Information

- Informationsaufbereitung
- Journalismus
- Newsletter
- Öffentlichkeitsarbeit
- Wissenschaftliche Veröffentlichung
- Studie

Das Fraunhofer SIT stellt über seine Forschungsergebnisse Informationsmaterial, Studien, Fachartikel und Whitepaper kostenfrei zur Verfügung, viele davon auch online. Regelmäßig werden Medienvertreter durch Pressemitteilungen und Veranstaltungen über Entwicklungen und Ergebnisse des Instituts informiert. Das Fraunhofer SIT bietet einen Informationsdienst, mit dem es registrierten Nutzerinnen und Nutzer individuell und themenspezifisch informiert.

Produkt

- Software

Die im Fraunhofer SIT entstehenden Lösungen und Werkzeuge werden von Technologieherstellern, Dienstanbietern, Betreibern von Infrastrukturen oder Anwendern zur Verbesserung der Sicherheit in der eigenen Produkte implementiert. Mit der Volksverschlüsselung und Key2B hat das Fraunhofer SIT Tools für eine sichere Ende-zu-Ende Verschlüsselung von E-Mails entwickelt. Für Bürgerinnen und Bürgerinnen und Bürgerinnen und Bürger ist die Volksverschlüsselung kostenfrei nutzbar. Key2B ist das Pendant für den kommerziellen Einsatz in Unternehmen.

FZI Forschungszentrum Informatik

Beitrag zur Cybersicherheit

Das FZI ist eine gemeinnützige Einrichtung für Anwendungsforschung und Technologietransfer im Bereich der Informatik. Sie wird gefördert durch das Land Baden-Württemberg und betreibt das Kompetenzzentrum IT-Sicherheit (KIS) als zentrale Anlaufstelle für angewandte IT-Sicherheit mit Forschungsbezug zum Mittelstand auf Landesebene. Ein spezifischer Themenschwerpunkt des KIS ist die IT-Sicherheit im Bereich von IoT. Das FZI ist an den Projekten Cyberwehr Baden-Württemberg (Cyberwehr BW, siehe hierzu den Steckbrief), CyberProtect und FLUIT: Sicherheit für vernetztes Flugverkehrsmanagement beteiligt.

Kontakt:

Haid-und-Neu-Str. 10-14

76131 Karlsruhe

fzi.de

Wissenschaftlicher Akteur

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Das FZI vernetzt mit besonderem Augenmerk auf Baden-Württemberg die Anwendungsforschung im Bereich der IT-Sicherheit mit der Wirtschaft. Es ist Innovationspartner des Karlsruher Instituts für Technologie (KIT) sowie Mitglied der Innovationsallianzen innBW und TechnologieRegion Karlsruhe. Außerdem ist das FZI Partner im DIZ | Digitalen Innovationszentrum sowie im Spitzencluster Elektromobilität Süd-West.

Bildung und Awareness

#Schulung #Awareness in der Wirtschaft

In Fragen der IT-Sicherheit werden Unternehmen mittels Sensibilisierungs- und Schulungsmaßnahmen durch das FZI unterstützt.

Konzeption und Vorgehensweisen

#Compliance Management #Datenschutz

Das FZI verbindet am KIS die Querschnittsthemen juristischer Forschung und der Informatik um technisch geprägte Fragestellungen und würdigt sie aus rechtlicher Sicht, wie bspw. Datenschutz, IT-Sicherheitsrecht und IT-Strafrecht.

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen

Das KIS bietet u.a. Bedrohungs- und Sicherheitsanalysen sowie die Entwicklung von Modellierungs- und Analysewerkzeugen an.

Netze und Kommunikation

#Netzarchitektur und -design #Netzkomponenten #Netzmanagement

Das FZI beschäftigt sich insb. mit der Netzwerksicherheit bezogen auf IoT-Systeme.

Vernetzung von Systemen, IoT

#Smart Home

Das FZI befasst sich mit der Konzeption sicherer IoT-Systeme, darunter auch mit Fragen der Hardware-Sicherheit, sicherer Betriebssysteme und Anwendungen sowie deren Entwicklung innerhalb eines Cyber-physischen Systems.

Zielgruppe

Wissenschaft

- Forschungseinrichtung

Wirtschaft

Das Angebot und der Fokus des FZI richtet sich zielgruppenspezifisch vor allem branchenübergreifend an den Mittelstand in Baden-Württemberg, aber auch an Behörden und die Wissenschaft.

Staat

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Beratung
- Entwicklung
- Konzept
- Sonstige Dienstleistung

Angebote des FZI sind bspw. Bedrohungsanalysen, Austausch zu Best Practices und Methoden der IT-Sicherheit, Technologiebewertungen, IT-Sicherheitstests und Forschung an innovativen und anwendbaren Sicherheitslösungen.

Information

- Wissenschaftliche Veröffentlichung
- Studie
- Sonstiges Informationsangebot
-

Im Rahmen seiner Forschungsarbeit veröffentlicht das FZI wissenschaftliche Publikationen und Fachartikel sowie Open Source-Quellcode.

Hasso-Plattner-Institut für Digital Engineering gGmbH (HPI)

Beitrag zur Cybersicherheit

Kontakt:

Prof.-Dr.-Helmert-Str. 2-3

14482 Potsdam

hpi.de

Wissenschaftlicher Akteur

Das Hasso-Plattner-Institut (HPI) in Potsdam forscht im Bereich Digital Engineering und bietet ein breites Studienangebot. Mit den Bachelor- und Master-Studiengängen „IT-Systems Engineering“, "Cybersecurity", "Digital Health" und "Data Engineering" bietet die Digital-Engineering-Fakultät der Universität Potsdam ein besonders praxisnahes ingenieurwissenschaftliches Informatik-Studium an. Die HPI School of Design Thinking ist Europas erste Innovationsschule für Studierende nach dem Vorbild der Stanforder d.school. Schwerpunkt der HPI-Lehre und -Forschung sind die Grundlagen und Anwendungen großer, hoch komplexer und vernetzter IT-Systeme. Hinzu kommen das Entwickeln und Erforschen nutzerorientierter Innovationen für alle Lebensbereiche. Cybersicherheit ist die Grundlage für gut funktionierende IT-Systeme, daher widmet das HPI dem Thema einen besonderen Stellenwert, der sich über die Ausrichtung der jährlich stattfindenden "Potsdamer Konferenz für Nationale CyberSicherheit" sowie in führenden IT-Sicherheitsforschungen rund um Themen wie APT-Abwehr, sichere Identitäten und Kryptographie drehen. Darüber hinaus betreibt das HPI den "Identity Leak Checker" und die "Vulnerability Database" mit deren Hilfe Privatpersonen und Unternehmen ihre digitalen Identitäten und IT-Systeme kostenfrei schützen können.

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Das HPI betreibt Forschung zusammen mit Partnern aus Wissenschaft und Wirtschaft. Neben den Forschungspartnerschaften hält das HPI strategische Partnerschaften mit Akteuren aus Wirtschaft und Wissenschaft und ist in Netzwerken und Verbänden aktiv. Das HPI ist zudem Veranstalter von einschlägigen Veranstaltungen zum Thema Cybersicherheit, die der Information und Vernetzung dienen, bspw. das HPI Cybersecurity Symposium, die Potsdamer Konferenz für nationale CyberSicherheit sowie weitere Konferenzen (Industrie 4.0 Konferenz).

Bildung und Awareness

#Schulung #Awareness in der Politik #Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft #Schulisches Bildungsangebot #Berufliches Bildungsangebot #Universitäres Bildungsangebot #Sonstiges Bildungsangebot

Das HPI ist eine universitäre Ausbildungsstätte mit hoher Praxisnähe durch internationale Kontakte in die Forschung, Wirtschaft und Industrie. Neben Studierenden und Partnern spricht das HPI mit einem offenen, interaktiven Online-Bildungsangebot (Open Campus) die Gesamtgesellschaft (Schülerinnen und Schüler sowie und Berufstätige) an, um Wissen aus der Informationstechnologie und Informatik zu verbreiten. Über die erste selbstentwickelte europäische MOOC-Plattform www.openhpi.de bietet das HPI kostenfreie Online-Kurse für Personen jeden Alters und Wissensstands zu unterschiedlichen Themen der IT-Sicherheit an ("Sicherheit im Internet", "Blockchain", "Sichere E-Mail", Sicherheit in Social Media", etc.).

Konzeption und Vorgehensweisen

#Kryptographie #Blockchain #Authentifizierung #Informationssicherheitsmanagement #Identitätsmanagement #Berechtigungsmanagement #Compliance Management #Datenschutz

Das HPI forscht zu diversen Themen der Cybersicherheit, unter anderem zu kryptografischen Verfahren, zu Themen des Datenschutzes und Digitalisierung, Informationssicherheitssysteme inkl. Messbarkeit von Sicherheit und Einhaltung von Sicherheitsprozessen. Besonderer Forschungsschwerpunkt liegt auf der Abwehr von "Advanced Persistent Threat"-Attacken, sicheren Identitäten (Passwortalternativen, Blockchain) und Cloudsecurity.

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen #Cloudsicherheit #Monitoring

Das IT-Security-Team des HPI erforscht Abwehrtechniken für "Denial of Sleep"-Angriffe und stellt bspw. Anwendungen wie den Identity Leak Checker zur Verfügung, um den Schutz von Identitäten zu überprüfen. Um den IT-Sicherheitsstatus zu analysieren, ist es notwendig, große Datenmengen in Echtzeit zu verarbeiten. Besonderer Forschungsschwerpunkt liegt auf der Abwehr und Überwachung großer Unternehmensdatenbanken, sicheren Identitäten (Passwortalternativen, Blockchain) und Cloudsecurity.

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen

Im Forschungsschwerpunkt "Abwehr von Advanced Persistent Threat - Attacken" kommen neuste Big Data Analytics und KI-Verfahren zum Einsatz.

Infrastrukturelle Sicherheitsaspekte

#SPS & ICS #physische IT-Sicherheit

Das Institut erforscht die theoretischen und konzeptionellen Grundlagen, die für automatisierte Produktion notwendig sind und trägt dazu bei, dass Programme und Systemarchitekturen für das komplexe Zusammenspiel von Internetprotokollen entwickelt werden. Insbesondere werden Multi-Cloud und Cloud-RAID-Technologien für den sicheren Einsatz der Zukunftstechnologie erforscht und erprobt.

Vernetzung von Systemen, IoT

#Smart Home #Autonomes Fahren #Fahrassistenzsysteme #Künstliche Intelligenz

Über verschiedene Fachgebiete werden alle Facetten des Themenbereiches IoT erforscht, um diese innovativen Technologien effizient und unangreifbar zu machen.

Zielgruppe

Zivilgesellschaft

Das HPI richtet sich mit seinem universitären Bildungsangebot an alle Interessierten. Mit dem Open Campus wird jedoch auch gesamtgesellschaftlich ein offenes Bildungsangebot zur Verfügung gestellt. Die am HPI entwickelte sichere openHPI-Plattform wird anderen global agierenden Firmen und internationalen Organisationen als Basis für eigene Bildungsangebote bereitgestellt. Über die HPI Schul-Cloud erforscht und entwickelt das HPI performante, sichere Cloudinfrastrukturen, die im deutschen Bildungssektor zum Einsatz kommen.

Wissenschaft

Das HPI hat einen hohen wissenschaftlichen Anspruch und lädt externe Wissenschaftler ausdrücklich dazu ein, die Ressourcen des HPI für ihre Forschungen zu nutzen. Wie z. B. über die global verteilten HPI Research Schools am Technion in Haifa/Israel, der Nanjing University/China, der University of Cape Town/Südafrika, der University of California in Irvine/USA und den Außenstellen am Mt. Sinai Hospital in NYC/USA. Darüber hinaus koordiniert das HPI die "Global Design Thinking Alliance" mit HPI zertifizierten Schools of Design Thinking auf allen Kontinenten, in deren Workshops neue Sicherheitsparadigmen für die digitale Welt erforscht werden.

Wirtschaft

Das HPI forciert Partnerschaften und eine enge Kooperation mit Wirtschaftsunternehmen, um dem hohen Anspruch an Praxisnähe der Ausbildung gerecht zu werden. Das Institut hat des Weiteren einen speziellen Fokus auf das Gesundheitssystem.

Staat

Über seine Potsdamer Konferenz für Nationale CyberSicherheit bietet das HPI für öffentliche Institutionen eine Gesprächsplattform zum Thema IT-Sicherheit, bei der Vertreter öffentlicher Behörden miteinander und mit Wirtschaft und Wissenschaft ins Gespräch kommen. Weiterhin schult das HPI in regelmäßigen Abständen Mitarbeiter öffentlicher Behörden und berät Bund, Länder und Kommunen in allen Fragen der IT-Sicherheit und digitaler Transformation.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Ausbildung und Schulung
- Entwicklung
- Konzept

Am HPI ist das Mittelstandskompetenzzentrum 4.0 für Brandenburg angesiedelt. In Workshops und Trainings zu verschiedenen Themen der Digitalisierung des Mittelstands werden KMU informiert, beraten und im Entwicklungsprozess der Digitalisierung ihrer Produkte begleitet. Wichter Kern der Trainings und Beratung liegt in Fragen der IT-Sicherheit. Digitale KMU können nur von Digitalisierung profitieren, wenn Ihre Lösungen IT-sicher sind. Über die HPI Academy werden eine Reihe von Workshops und Beratungen für große Firmen und Behörden angeboten, um die Partner bei Fragen der digitalen Transformation und IT-Sicherheit zu begleiten.

Information

- Informationsaufbereitung
- Lernprogramm
- Blog
- Newsletter
- Öffentlichkeitsarbeit
- Podcast
- Wissenschaftliche Veröffentlichung
- Studie
- Sonstiges Informationsangebot

Das HPI bietet nicht nur den Studierenden, sondern auch einer breiteren Öffentlichkeit diverse Informationsmöglichkeiten an. Besonders hervorzuheben ist die Open Campus-Plattform des HPI, auf der Online-Kurse und Beiträge, wie Vorlesungen und Studien, zur Verfügung gestellt werden. Außerdem wird auf der Webseite eine Datenbank für IT-Angriffsanalysen angeboten, durch deren Hilfe gezielt Software-Sicherheitslücken gesucht werden können. Weiterhin werden im HPI Podcast "Neuland" regelmäßig aktuelle Themen aus der IT-Forschung thematisiert und über die Kolumne "Meinels Web-Tutorial" in Spektrum der Wissenschaft klärt der Institutsdirektor des HPI die breite Öffentlichkeit über die Funktionsweise des Internets und Webs sowie ihrer Sicherheitsaspekte auf.

Produkt

- Clouddienste/PaaS

Das HPI bietet die HPI Schul-Cloud, die MOOC-Plattform openHPI sowie weitere Instanzen der HPI-Lernplattform für interessierte Behörden, Unternehmen und wissenschaftliche Institutionen als PaaS/On-Premise Produkte an. Darüber hinaus können Landesbehörden den Identity-Leak-Checker-Client erwerben, mit der sämtliche Landesdomains dahingehend überwacht werden können, ob Identitätsdaten von Landesmitarbeitern von öffentlichen Leaks betroffen sind

Helmholtz-Zentrum für Informationssicherheit gGmbH (CISPA)

Beitrag zur Cybersicherheit

Kontakt:

Stuhlsatzenhaus 5

66123 Saarbrücken

cispa.de

Wissenschaftlicher Akteur

Die Forschung des CISPA umfasst verschiedene Aspekte von IT-Sicherheit und Datenschutz: Design, Analyse und Verifikation von Protokollen und Systemen, Mechanismen zum Schutz der Endnutzer-Privatsphäre, Forschung zu neuen Angriffsvektoren, Universallösungen für Software- und Netzwerksicherheit. Das CISPA wird als wesentlicher Akteur eingestuft, da es Forschung und Transfer mit einem gesamtgesellschaftlichen Diskurs kombiniert. Das CISPA behandelt die drängenden, großen Herausforderungen der Forschung in den Bereichen Cybersicherheit und Datenschutz, mit denen die Gesellschaft im Zeitalter der Digitalisierung konfrontiert wird. Das CISPA arbeitet in den Forschungsbereichen Cybersicherheit und Datenschutz international mit anderen Einrichtungen zusammen, sowohl in der Grundlagen- als auch der anwendungsorientierten Forschung.

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Das CISPA ist in der Großregion Saarbrücken mit anderen Forschungseinrichtungen lokal vernetzt, ebenso grenzüberschreitend mit französischen und luxemburgischen Einrichtungen. Eine Vernetzung findet ebenfalls über die Helmholtz-Gemeinschaft sowie über internationale Forschungstätigkeit statt, wie bspw. Stanford in den USA. Das CISPA-Stanford Center for Cybersecurity ist ein gemeinsames Zentrum für Cybersicherheitsforschung des CISPA und der Stanford University, welches das hohe Potenzial einer für beide Seiten vorteilhaften Zusammenarbeit zwischen CISPA und Stanford auf dem Gebiet der Cybersicherheit erkennt und dem Wunsch der Wissenschaftler auf beiden Seiten nach gemeinsamer Forschung folgt.

Bildung und Awareness

#Universitäres Bildungsangebot

Das CISPA hat 2014 den Bachelorstudiengang der Cybersicherheit an der Universität des Saarlandes ins Leben gerufen.

Konzeption und Vorgehensweisen

#Endgerätesicherheit #Datenschutz

Das CISPA forscht an sicheren und mobilen autonomen Systemen bzgl. Datenschutz und Softwaresicherheit. Es liefert einen Beitrag zur Entwicklung von Methoden und Werkzeugen, um Sicherheit für Systeme und Software zu garantieren.

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen #Monitoring

Das CISPA beschäftigt sich mit Methoden und Werkzeugen für Systemmonitoring, -analyse und Programmreparaturen, um Lösungen zum Schutz vor Angriffen möglich zu machen.

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen
#Behandlung von Sicherheitsvorfällen & IT-Forensik

Am CISPA wird die Entwicklung von Erkennungs- und Verteidigungsmechanismen zur Vermeidung von Cyberangriffen und Cyberangriffsschäden vorangetrieben.

Vernetzung von Systemen, IoT

#Künstliche Intelligenz

Das CISPA betreibt anwendungsorientierte Forschung zu Techniken des Maschinenlernens in sicherheitsrelevanten Bereichen, insbesondere als Beitrag zum neuen Gebiet des "Adversial Machine Learning", um manipulierte Daten als Input für autonome Systeme nachzuweisen.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger

Eine Mission des CISPA ist der Dialog mit Bürgerinnen und Bürgern und die Wissensvermittlung über Cyberthemen, insb. Datenschutzthemen.

Wissenschaft

- Bildungseinrichtung
- Forschungseinrichtung

Die Vernetzung mit anderen Akteuren innerhalb der Helmholtz-Gemeinschaft und im Rahmen von Kooperationen und Partnerschaften mit Bildungs- und Forschungseinrichtungen dient dem Wissenstransfer.

Wirtschaft

- Automobilbranche / Automotive
- Information und Kommunikation

Das CISPA spricht mit seinen Forschungsbeiträgen im Schwerpunkt Unternehmen der Automobilbranche sowie der Informations- und Kommunikationsbranche an.

Staat

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Ausbildung und Schulung

Das CISPA stellt eine universitäre Forschungs- und Bildungseinrichtung dar.

Information

- Informationsaufbereitung
- Newsletter
- Wissenschaftliche Veröffentlichung
- Studie

Das CISPA stellt Forschungsergebnisse und aktuelle Informationen im Themenbereich Cybersicherheit in Form von Newslettern, Veröffentlichungen und Studien online zur Verfügung.

Horst Görtz Institut für IT-Sicherheit (HGI)

Beitrag zur Cybersicherheit

Das HGI wurde mit dem Ziel der Begegnung der europaweiten Defizite in der Forschung zur IT-Sicherheit im Jahr 2002 gegründet. Heute forschen rund 200 Wissenschaftler in den verschiedenen Forschungsfeldern "Kryptographie der Zukunft", "Sichere Systeme", "Eingebettete Sicherheit", "Sicherheit und Usability" und "Interdisziplinäre Aspekte der IT-Sicherheit". Neben Spitzenforschung auf dem Gebiet der IT-Sicherheit bietet das HGI Studiengänge zur IT-Sicherheit an. Darüber hinaus wird der Transfer der Forschungsergebnisse in die Praxis im Rahmen verschiedener Kooperationen gefördert.

Kontakt:

Universitätsstr. 150

44780 Bochum

hgi.rub.de

Wissenschaftlicher Akteur

Thematische Schwerpunkte (Auszug)

Bildung und Awareness

#Universitäres Bildungsangebot

Das Lehrangebot des Instituts umfasst vier Studiengänge zur IT-Sicherheit.

Konzeption und Vorgehensweisen

#Kryptographie #Quanten-Kryptographie & Post-Quanten-Kryptographie

Die Forschung des HGI erstreckt sich über die verschiedenen Themenfelder. Der Interdisziplinarität der IT-Sicherheit wird durch die Zusammenarbeit in der Forschung mit Disziplinen wie bspw. Jura oder Psychologie begegnet.

Zielgruppe

Wissenschaft

- Bildungseinrichtung
- Forschungseinrichtung

Das HGI ist auf die Weiterentwicklung der Forschung sowie die Lehre und Ausbildung im Bereich IT-Sicherheit ausgerichtet.

Wirtschaft

Zum Transfer der Forschungsergebnisse in die praktische Anwendung kooperiert das HGI mit verschiedenen Partnern.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Ausbildung und Schulung

Information

- Informationsaufbereitung
- Wissenschaftliche Veröffentlichung
- Studie

Die Forschungsergebnisse des HGI werden im Rahmen von Publikationen veröffentlicht oder in Praxiskooperationen angewendet.

Institut für Datenwissenschaften am Deutschen Zentrum für Luft- und Raumfahrt e.V. (DLR)

Beitrag zur Cybersicherheit

Das DLR ist ein Forschungszentrum der Bundesrepublik Deutschland. Die Forschung des Instituts für Datenwissenschaften am DLR konzentriert sich auf die Bereiche Datenmanagement, IT-Sicherheit und sichere Softwaretechnik. Diese Forschungstätigkeiten ergänzen etablierte Forschungsgebiete an anderen DLR-Instituten. Das Institut unterhält eine Abteilung für IT-Sicherheit, die Tools analysiert und entwickelt, um die Sicherheit in einer vernetzten Welt zu gewährleisten. Im Vordergrund steht die Sicherheit von Soft- und Hardware sowie Remote-Verbindungen zu Rechenzentren und Cloud-Diensten.

Kontakt:

Mälzerstraße 3

07745 Jena

dlr.de

Wissenschaftlicher Akteur

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Das Institut für Datenwissenschaften arbeitet in enger Kooperation mit der Bundesverwaltung, anderen Forschungseinrichtungen und Industriepartnern zusammen.

Konzeption und Vorgehensweisen

#Endgerätesicherheit

Die Arbeitsgruppe Sichere Softwaretechnik des Instituts für Datenwissenschaft befasst sich mit intelligenten und datengetriebenen Methoden zur Analyse von Softwareentwicklungsprozessen und der Sicherheit der daraus entstandenen Produkte. Schwerpunkte sind etwa die statistische Modellierung und Validierung von Softwaresicherheit. Eine wichtige Rolle spielt dabei auch die Nutzung von maschinellem Lernen und Künstlicher Intelligenz, bspw. zur Vorhersage und Reparatur von Sicherheitslücken oder bei der sicheren Entwicklung von Systemen für maschinelles Lernen und Künstliche Intelligenz.

Betriebsbezogene Sicherheitsaspekte

#Cloudsicherheit #Monitoring

Das Institut für Datenwissenschaften forscht in den Bereichen Datenmanagement und Datenanalyseverfahren und entwickelt Tools, um die Sicherheit von Cloud-Diensten zu gewährleisten.

Netze und Kommunikation

#Netzmanagement

Das Institut für Datenwissenschaften beschäftigt sich mit der Analyse und Entwicklung von Tools, um die Sicherheit in einer stark vernetzten Welt zu fördern.

Zielgruppe

Wissenschaft

- Forschungseinrichtung

Das Institut für Datenwissenschaften adressiert mit seinen Leistungen wissenschaftliche Einrichtungen.

Wirtschaft

Das Institut für Datenwissenschaften adressiert mit seinen Leistungen branchenübergreifend Wirtschaftsunternehmen für angewandte Forschung.

Staat

Das Institut für Datenwissenschaften arbeitet über die eigene Forschung hinaus im Auftrag der Bundesregierung an relevanten Themen.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Entwicklung

Das Institut für Datenwissenschaften entwickelt Lösungen für Sicherheitsthemen von Unternehmen und öffentlichen Einrichtungen.

Information

- Wissenschaftliche Veröffentlichung
- Studie

Das Institut für Datenwissenschaften stellt Veröffentlichungen zu seiner Forschungstätigkeit in einer Publikationsdatenbank online zur Verfügung.

Institut für Informatik 4 der Rheinischen Friedrich-Wilhelms-Universität Bonn

Beitrag zur Cybersicherheit

Die Abteilung 4 „Security and Networked Systems“ des Instituts für Informatik der Rheinischen Friedrich-Wilhelms Universität Bonn forscht und lehrt in sieben Arbeitsgruppen, bspw. „IT-Sicherheit“ oder „Usable Security and Privacy“, zu verschiedenen Themengebieten der IT-Sicherheit. Im Rahmen des Lehrangebots für Studiengänge im Bereich Cyber Security ist die Abteilung 4 maßgeblich beteiligt.

Kontakt:

Institut für Informatik 4

Endenicher Allee 19A

53115 Bonn

net.cs.uni-bonn.de

Wissenschaftlicher Akteur

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Die universitären Wissenschaftler der Abteilung 4 sind an verschiedenen Kooperationen und Projekten beteiligt. In diesem Rahmen wird auch eine strategische Partnerschaft mit dem Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) gepflegt.

Bildung und Awareness

#Universitäres Bildungsangebot

Von Abteilung 4 gehen für die Bachelor- und Masterstudiengänge Cyber Security verschiedene Lehrveranstaltungen im Bereich der IT-Sicherheit aus.

Konzeption und Vorgehensweisen

#Kryptographie #Datenschutz

Der Bereich der angewandten Kryptographie bildet einen Schwerpunkt der Forschung und Lehre, ebenso wie Privacy und Datenschutz.

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen #Monitoring

Das kooperative Sicherheitsmonitoring zählt ebenfalls zum Arbeitsbereich der Arbeitsgruppe IT Security.

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen

Die der Abteilung 4 untergliederten Arbeitsgruppen forschen an Themen der Sicherheit und Effizienz im Internet, bspw. Intrusion Detection, Honeypots oder der Analyse von Malware.

Netze und Kommunikation

#Netzarchitektur und -design #Netzmanagement

Einer der Schwerpunkte der Abteilung 4 bildet die Forschung an Netzwerken und Vernetzung, bspw. an infrastrukturunabhängige, drahtlose Multi-Hop-Netze in taktischen Szenarien sowie deren Sicherheit in Krisensituationen.

Vernetzung von Systemen, IoT

#Smart Home

Ein Themenkomplex der Forschung und Lehre der Abteilung 4 ist die Sicherheit in der Gebäudeautomation.

Zielgruppe

Wissenschaft

- Bildungseinrichtung
- Forschungseinrichtung

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Ausbildung und Schulung

Verschiedene Lehrangebote im Bereich der IT-Sicherheit, insbesondere im Studiengang Cyber Security.

Information

- Wissenschaftliche Veröffentlichung
- Studie

Aus der Forschungsarbeit resultieren wissenschaftliche Publikationen.

Institut für Internet-Sicherheit – if(is)

Beitrag zur Cybersicherheit

Das if(is) der Westfälischen Hochschule forscht zu verschiedenen Themen im Bereich IoT und Cybersicherheit. Aus einigen ehemaligen Projekten und Forschungsthemen sind bereits Ausgründungen entstanden und das Institut ist mit Unternehmen zur Durchführung von Forschungsprojekten vernetzt.

Kontakt:

Neidenburger Str. 43

45897 Gelsenkirchen

internet-sicherheit.de

Wissenschaftlicher Akteur

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Das if(is) führt Forschungsprojekte mit verschiedenen nationalen und internationalen Universitäten sowie Unternehmen durch und koordiniert über diverse Initiativen Kontakte und Wissensvermittlung rund um IT-Sicherheit.

Bildung und Awareness

#Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft #Universitäres Bildungsangebot

Das if(is) bietet neben dem Masterstudiengang "Internet-Sicherheit" auch Workshops, Videokurse und Informationsmaterial zu den Themengebieten Awareness, Cybersicherheit und Digitalisierung an. Zu einzelnen Fachthemen werden auch Informationen für Unternehmen und interessierte Bürgerinnen und Bürger veröffentlicht.

Konzeption und Vorgehensweisen

#Kryptographie #Blockchain #Authentifizierung #Endgerätesicherheit #Identitätsmanagement #Berechtigungsmanagement #Datenschutz

Die Forschungsprojekte und -bereiche des if(is) decken verschiedene Themen ab, u.a. Blockchain-Technologie, Künstliche Intelligenz und Cybersicherheit, Identifikations-, Authentifikations- und Signatur-Systeme, technischer Datenschutz, IoT-Security, Smart Car Security, Smart Home Security, Mobile Security, Trusted Computing und sicheres/vertrauenswürdiges Cloud Computing.

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen #Cloudsicherheit #Monitoring

Neben der Entwicklung von Internet-Frühwarn- und Lagebildsystemen und der Absicherung von Banktransaktionen beschäftigt sich das if(is) auch mit dem Thema Cloudsicherheit. Im Forschungsbereich "Internetkennzahlen" wird die Komplexität von Kritischen Infrastrukturen analysiert, um dadurch Entwicklungen auf diesem Sektor abschätzen zu können.

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen #Behandlung von Sicherheitsvorfällen & IT-Forensik

Im Bereich "Internet-Frühwarnsysteme" des if(is) sind bspw. Projekte zur frühzeitigen Erkennung von Virenwellen im Internet verankert. Weitere Themen in diesem Bereich sind: Threat Intelligence, Malware and Botnet Detection, Software Reverse Engineering, Malware Analysis und IoT Forensics.

Netze und Kommunikation

#Netzarchitektur und -design #Netzkomponenten

Über das if(is) laufen verschiedene Forschungsvorhaben wie bspw. Trusted Network Access Control oder die Einführung von Trusted Computing Technologien auf Netzwerkebene (TCN).

Vernetzung von Systemen, IoT

#Smart Home #Fahrassistenzsysteme #Künstliche Intelligenz

Ein weiterer Forschungsschwerpunkt des if(is) liegt auf den Themen Secure eMobility sowie Smart Car, Smart Grid und Smart Traffic. In vielen Bereichen wird mithilfe Künstlicher Intelligenz aus den vorhandenen Daten Wissen generiert, um die Wirkung der Cybersicherheitsmaßnahmen sowie das Erkennen von Angriffen zu verbessern.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger
- Akademikerinnen und Akademiker

Die Ergebnisse aus ausgewählten Forschungsbereichen und -projekten des if(is) stehen allen Gesellschaftsteilnehmern zur Verfügung, richten sich aber durch ihren starken Fachbezug häufig an Akademikerinnen und Akademiker. Leitfäden zur Sicherheit im Internet oder von Mobilgeräten sollen allen Bürgerinnen und Bürgern die Möglichkeit geben, eine gewisse Grundsicherheit für ihre digitalen Aktivitäten zu erreichen.

Wissenschaft

- Bildungseinrichtung
- Forschungseinrichtung

Die Forschungsergebnisse des if(is) werden im wissenschaftlichen Rahmen veröffentlicht.

Wirtschaft

- Kritische Infrastruktur

Neben den Wirtschaftspartnern unterschiedlicher Branchen bei der Durchführung von Forschungsprojekten richten sich die Ergebnisse und Empfehlungen des if(is) zu seinen Fachthemen auch allgemein an Unternehmen.

Staat

- Bund
- Behörde/Verwaltung
- Ministerium

Viele Angebote des if(is), wie bspw. der "Marktplatz IT-Sicherheit" können auch ausdrücklich von öffentlichen Verwaltungen genutzt werden. Das if(is) setzt Studien für das BSI und Bundes- und Landesministerien um.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Ausbildung und Schulung
- Beratung
- Entwicklung
- Konzept

Neben dem Masterstudiengang "Internet-Sicherheit" und einzelnen Lehrveranstaltungen an der Hochschule werden durch das if(is) auch Unternehmen und Organisationen zu Themen der Cybersicherheit beraten und Drittmittelprojekte umgesetzt.

Information

- Informationsaufbereitung
- Literatur
- Wissenschaftliche Veröffentlichung
- Studie

Das if(is) veröffentlicht neben Studien und Büchern auch Pressematerialien und Informationsvideos zu fachspezifischen Themen.

Kompetenzzentrum für angewandte Sicherheitstechnologie (KASTEL)

Beitrag zur Cybersicherheit

KASTEL wurde 2011 vom BMBF initiiert und am Karlsruhe Institut of Technology (KIT) eingerichtet. Durch den Zusammenschluss verschiedener Kompetenzfelder sollen hier umfassende Ansätze für die Gesamtsicherheit in ausgewählten Anwendungsbereichen geschaffen werden.

Ansprechpartner:

Geb. 50.34/Raum 270

Am Fasanengarten 5

Geb. 50.34

76131 Karlsruhe

kastel.kit.edu

Wissenschaftlicher Akteur

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Zur Förderung von Gründungsvorhaben Studierender im Bereich der IT-Sicherheit bietet KASTEL mit dem sog. "StartUpSecure" einen Gründungsinkubator an. In diesem werden die Gründer entlang ihres Gründungsprozesses durch verschiedene Angebote unterstützt und vernetzt.

Bildung und Awareness

#Schulung #Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft #Universitäres Bildungsangebot

KASTEL bietet ein Qualifikationskonzept an, in dessen Rahmen das notwendige Wissen zum Entwurf und zur Realisierung von Sicherheitslösungen vermittelt und bescheinigt wird. Das Angebot richtet sich sowohl an Studierende als auch Doktoranden und soll zur Heranbildung von Fachpersonal verhelfen. Darüber hinaus organisiert KASTEL auch Veranstaltungen, die neben Akademikerinnen und Akademikern und Schülern auch interessierte Bürgerinnen und Bürger adressieren.

Konzeption und Vorgehensweisen

#Kryptographie #Quanten-Kryptographie & Post-Quanten-Kryptographie #Blockchain #Authentifizierung #Informationssicherheitsmanagement #Endgerätesicherheit #Identitätsmanagement #Berechtigungsmanagement #Compliance Management #Datenschutz

Im Forschungsgebiet Datenschutz entwickelt KASTEL Konzepte zu verschiedenen Bereichen der Thematik. Zu diesen gehören unter anderem die Beweisbarkeit von Sicherheitslösungen, die sichere Verarbeitung von Daten, die dazugehörigen rechtlichen Aspekte sowie die Entwicklung von Werkzeugen und Methoden zur kontinuierlichen und systematischen Anpassung an aktuelle Sicherheitsbedarfe.

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen #Cloudsicherheit

Im betrieblichen Bereich forscht KASTEL zur Absicherung von Produktionsanlagen und Cloudlösungen

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen

KASTEL forscht an Verfahren zur automatischen Erkennung von Angriffen (Network Intrusion Detection).

Infrastrukturelle Sicherheitsaspekte

#Betriebs- und Steuerungstechnik #SPS & ICS #Intelligente Messsysteme #physische IT-Sicherheit

Im Kontext von Industrie 4.0 forscht KASTEL an Möglichkeiten zur Absicherung von kritischen Infrastrukturen wie bspw. Produktionsanlagen und Stromnetzen.

Netze und Kommunikation

#Netzarchitektur und -design #Netzkomponenten #Netzmanagement #Funknetze

Sichere Kommunikationsnetze sind ein Forschungsschwerpunkt in KASTEL.

Vernetzung von Systemen, IoT

#Smart Home #Autonomes Fahren #Künstliche Intelligenz

Viele der Forschungsfelder und -gebiete des Kompetenzzentrums beziehen sich auf die Anwendung in sog. Smart Environments oder in der Mobilität, also Systemen mit einer Vielzahl von Sensoren und Aktoren, welche miteinander vernetzt sind.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger
- Akademikerinnen und Akademiker

Die Forschungs- und Lehrangebote des Zentrums richten sich vorranging an Akademikerinnen und Akademiker aus verschiedenen Fachgebieten. Zielgruppe von angebotenen Veranstaltungen sind darüber hinaus auch interessierte Bürgerinnen und Bürger. Das "KASTEL StartUpSecure"-Programm richtet sich an alle interessierten Gründer.

Wissenschaft

- Bildungseinrichtung
- Forschungseinrichtung

Die Forschungsergebnisse und -projekte richten sich auch an andere, kooperierende Projektpartner und nationale Forschungsinstitute.

Wirtschaft

- Energieversorgung
- Information und Kommunikation
- Verkehr / Infrastruktur
- Kritische Infrastruktur

Staat

- Bund
- Land
- Behörde/Verwaltung
- Ministerium

KASTEL veröffentlicht anlassbezogen Stellungnahmen und Positionspapiere zu aktuellen Themen.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Beratung
- Sonstige Dienstleistung

Im Rahmen des Gründungsinkubators "KASTEL StartUpSecure" des Kompetenzzentrums werden die Gründer in einem mehrstufigen Prozess in ihren Vorhaben unterstützt, bspw. durch die Vermittlung von Mentoren und Kontakten sowie die Weiterentwicklung und Begleitung von Ideen.

Information

- Informationsaufbereitung
- Wissenschaftliche Veröffentlichung
- Studie

Neben wissenschaftlichen Veröffentlichungen publiziert KASTEL themenspezifische Studien und Positionspapiere.

Lernlabor Cybersicherheit (LLCS)

Beitrag zur Cybersicherheit

Ansprechpartner:

Fraunhofer Academy

Hansastr. 27c

80686 München

cybersicherheit.fraunhofer.de

Wissenschaftlicher Akteur

Die Fraunhofer Academy bietet im LLCS transferorientierte Weiterbildungsangebote für Fach- und Führungskräfte aus Industrie und Verwaltung an. Das LLCS dient der Simulation realer Bedrohungsszenarien zur Entwicklung geeigneter Lösungskonzepte. Das modulare Angebot erstreckt sich über verschiedene Schwerpunkte wie industrielle Produktion und Kritische Infrastrukturen, Hochsicherheit und Emergency Response, Internetsicherheit, IT-Forensik, Qualität softwarebasierter Produkte oder Embedded Systems, mobile Sicherheit und IoT. Neben einer thematischen Gliederung werden auch branchenspezifische Seminare angeboten. Hierfür arbeiten Wissenschaftler ausgewählter Hochschulen und Fraunhofer-Instituten an mehreren Standorten in Deutschland zusammen, um die relevanten Domänen und Branchen der IT-Sicherheit umfassend abzudecken. So kann aktuelles IT-Sicherheitswissen des LLCS in offenen Seminaren, inhouse Weiterbildungen von Unternehmen und bei ausgewählten Bildungspartnern erworben werden.

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Ziel des LLCS ist die Qualifizierung von IT-Security Fachkräften und Spezialisten in aktuellen Anwendungsfeldern der IT-Sicherheit. Dazu erfolgen u.a. der Aufbau hochwertiger IT-Security- Labore für den Einsatz in Forschung und Weiterbildung, die Etablierung eines Transfernetzwerkes IT-Sicherheit durch Einbindung von Industrie und Wissenschaft in Fachbeiräten, die Schaffung zusätzlicher Trainings- und Lehrkompetenzen durch Train-the-Trainer-Formate und didaktische Qualifizierung sowie eine Stärkung der Forschung an Fachhochschulen im Bereich der IT-Sicherheit.

Bildung und Awareness

#Schulung #Awareness in der Politik #Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft #Berufliches Bildungsangebot #Universitäres Bildungsangebot

Das LLCS der Fraunhofer Academy bietet für Fachkräfte, Entscheider und Anwender berufsbegleitende Weiterbildung. In kompakten, transferorientierten Lernformaten werden Erkenntnisse aus anwendungsorientierter Forschung und Industrieprojekten bedarfsgerecht und praxisnah aufbereitet. Die aufgebauten Labore eignen sich auch hervorragend, um - neben der Qualifizierung von Mitarbeitenden aus Unternehmen und Behörden - das Angebot für Studierende im Umfeld der IT-Sicherheit attraktiver und praxisnäher zu gestalten. Die beteiligten Hochschulen erweitern durch die Kooperation ihr Angebot an Studierende im Rahmen von Praktika, Bachelor- und Masterarbeiten. Die Hochschulen erhalten zudem eine attraktive Forschungsinfrastruktur, die die Hochschulen bei der Profilbildung als forschungsstarke Einrichtung unterstützt. Das Lernlabor Cybersicherheit versteht es als Auftrag, auch in der breiten Öffentlichkeit für die Bedeutung von IT-Sicherheitskompetenz zu werben. Die Sensibilisierung für Bedrohungsszenarien und das Aufzeigen geeigneter Präventionsstrategien ist Gegenstand zahlreicher Kommunikationsmaßnahmen (z.B. Beteiligung an der MS Wissenschaft), die auch eine interessierte Öffentlichkeit jenseits der IT-Fachabteilungen erreicht.

Konzeption und Vorgehensweisen

#Kryptographie #Quanten-Kryptographie & Post-Quanten-Kryptographie #Blockchain #Authentifizierung #Informationssicherheitsmanagement #Endgerätesicherheit #Identitätsmanagement #Berechtigungsmanagement #Datenschutz #IT-Sicherheitsstandards

Es werden Seminare zu Cybersicherheit im Kontext folgender thematischer Schwerpunkte angeboten: "Entwicklung und Testung sicherer Software", "Produktzertifizierung", "Mobile Application Security", "IT-Sicherheitstechnologien" (z.B. Blockchain), "Datenschutz", "Embedded Systems", sowie "Identität und Identitätsnachweis".

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen #Monitoring

Das Seminarangebot umfasst Kurse zu den Oberthemen Netzwerksicherheit, Industrie 4.0 und Energie- und Wasserversorgung.

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen #Behandlung von Sicherheitsvorfällen & IT-Forensik

Das Seminarangebot umfasst auch Kurse zu den Oberthemen "IT-Forensik" sowie "Schadsoftware- und Firmwareanalyse".

Infrastrukturelle Sicherheitsaspekte

#Betriebs- und Steuerungstechnik #SPS & ICS #Intelligente Messsysteme #RZ-Infrastruktur #physische IT-Sicherheit

Das Seminarangebot ist vor allem auf die Branchen industrielle Produktion sowie Energie- und Wasserversorgung ausgerichtet.

Netze und Kommunikation

#Funknetze

Auch im Themenbereich Netzwerksicherheit werden unterschiedliche Seminare angeboten.

Vernetzung von Systemen, IoT

Unter den Schwerpunkten "Industrielle Produktion" und "IoT-Sicherheit" werden z.B. Kurse zur Cybersicherheit im Kontext von Industrie 4.0 angeboten.

Zielgruppe

Wirtschaft

Das LLCS richtet sich an Fach- und Führungskräfte aus Wirtschaft und öffentlicher Verwaltung sowie Ermittlungsbehörden.

Staat

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Ausbildung und Schulung
- Beratung
- Entwicklung
- Konzept

Neben den Weiterbildungen bieten die beteiligten Fraunhofer-Institute und Fachhochschulen Dienstleistungen innerhalb von Forschung und Entwicklung an.

Information

- Informationsaufbereitung
- Journalismus
- Blog
- Newsletter
- Öffentlichkeitsarbeit
- Wissenschaftliche Veröffentlichung

Mit seinem breiten Modulangebot stellt das LLCS eine Weiterbildungsmöglichkeit im Bereich Cybersicherheit dar.

Max-Planck-Institut für Cybersicherheit und Schutz der Privatsphäre (CSP)

Beitrag zur Cybersicherheit

Das CSP in Bochum wurde 2019 gegründet und forscht zu den technischen Grundlagen und der Interdisziplinarität von Cybersicherheit und Datenschutz. Neben der Grundlagenforschung zur Cybersicherheit soll auch die Lehre ausgebaut werden. Im Rahmen der Forschung werden außerdem ökonomische, juristische und soziale Aspekte der Entwicklungen betrachtet. Mit einem jährlichen Budget von 20 Millionen Euro soll das Institut fünf Jahre nach seiner Gründung zwölf Forschungsgruppen und 200 Mitarbeiter umfassen.

Kontakt:

Universitätsstr. 60

44789 Bochum

mpi-sp.org

Wissenschaftlicher Akteur

Thematische Schwerpunkte (Auszug)

Bildung und Awareness

#Universitäres Bildungsangebot

Neben der Forschung betreibt das CSP auch Lehre im Bereich Cybersicherheit und Schutz der Privatsphäre.

Konzeption und Vorgehensweisen

Das CSP betreibt Grundlagenforschung im breiten Themenbereich IT- und Cybersicherheit sowie Datenschutz.

Zielgruppe

Wissenschaft

- Bildungseinrichtung
- Forschungseinrichtung

Ziel des CSP ist die Weiterentwicklung der Grundlagenforschung in der Cybersicherheit sowie die Ausbildung von Nachwuchskräften mittels gezielter Lehre.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Wissenschaftliche Veröffentlichung
- Studie

Neben der Lehre werden die Ergebnisse der Forschungsarbeit des CSP in Form von Publikationen festgehalten.

Nationales Forschungszentrum für angewandte Cybersicherheit (ATHENE)

Beitrag zur Cybersicherheit

Kontakt:

Rheinstr. 75

64295 Darmstadt

athene-center.de

Wissenschaftlicher Akteur

ATHENE (ehemals CRISP) ist ein Forschungszentrum für angewandte Cybersicherheit und Privatsphärenschutz. ATHENE ist eine Forschungseinrichtung der Fraunhofer-Gesellschaft unter Mitwirkung der Darmstädter Fraunhofer-Institute SIT und IGD sowie der TU Darmstadt und der Hochschule Darmstadt. Das Zentrum wird gefördert vom BMBF und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) und hat seinen Standort in der Wissenschaftsstadt Darmstadt. ATHENE forscht und entwickelt im Rahmen von staatlich geförderten Projekten oder im Rahmen von Forschungsaufträgen der Wirtschaft bzw. staatlicher Organe. In ATHENE arbeiten mehr als 500 Wissenschaftlerinnen und Wissenschaftler an relevanten Fragestellungen der Cybersicherheit und des Privatsphärenschutzes. ATHENE deckt mit seinen Forschungs- und Entwicklungsarbeiten ein breites Spektrum von Themen ab, die für verschiedene Technologien und Anwendungsbereiche relevant sind.

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

ATHENE ist mit den verschiedenen Organisationen aus Zivilgesellschaft, Wissenschaft, Wirtschaft und Staat, national wie international vernetzt. ATHENE wirkt im Rahmen der Vernetzung u.a. an weltweit genutzten Standards mit. Weitere Multiplikationseffekte mit der Wirtschaft erreicht ATHENE durch Vernetzung einschlägigen Branchenverbänden der Wirtschaft. Durch seinen Gründungsinkubator ATHENE StartupSecure, durch den Digital Hub Cybersecurity und durch den German-Israeli Partnership Accelerator (GIPA) ist ATHENE Anlaufstation für Gründer und Gründungsinteressierte im Bereich Cybersicherheit und Privatsphärenschutz.

Bildung und Awareness

#Schulung #Awareness in der Politik #Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft #Berufliches Bildungsangebot #Universitäres Bildungsangebot #Sonstiges Bildungsangebot

Im Bereich der Lehre werden Studierende an den mitwirkenden Hochschulen sowohl in Grundlagenvorlesungen als auch in vertiefenden Spezialvorlesungen Kenntnisse der Cybersicherheit und des Privatsphärenschutzes vermittelt. Die Lehrveranstaltungen werden im Rahmen von Bachelor und Master-Studiengängen angeboten. Zusätzlich werden berufsbegleitende Weiterbildungen angeboten. ATHENE betreibt eine Cyber Range, welche die Möglichkeit bietet, Reaktion und Behandlung von Cyberangriffen zu simulierten sowie in realen Szenarien und Umgebungen zu trainieren. ATHENE organisiert Vorträge und Veranstaltungen für alle Gesellschaftsgruppen, wie bspw. Coding4Kids und eigene Beiträge zum vom BMBF und Bundesministerium für Familie, Seniorinnen und Senioren, Frauen und Jugend (BMFSFJ) geförderten Girls Day.

Konzeption und Vorgehensweisen

#Kryptographie #Quanten-Kryptographie & Post-Quanten-Kryptographie #Blockchain #Authentifizierung #Informationssicherheitsmanagement #Endgerätesicherheit #Identitätsmanagement #Berechtigungsmanagement #Datenschutz #IT-Sicherheitsstandards

ATHENE beschäftigt sich in Forschung und Entwicklung mit einem breiten Spektrum von Fragestellungen der Cybersicherheit und des Privatsphärenschutzes. In diesem Zusammenhang beschäftigt sich ATHENE beispielsweise mit Sicherheit von Software und der Schwachstellenerkennung, Kryptographie, der Biometrie, der Sicherheit des Internets, der Sicherheit bei der Vernetzung von Geräten sowie der Sicherheit im Bereich der Mobilität.

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen #Cloudsicherheit #Monitoring

Für Unternehmen oder auch Organisationen der öffentlichen Hand betreibt ATHENE über das Internet zugängliche Dienste, mittels derer diese die Sicherheit der von ihnen genutzten Netzwerkkomponenten bzw. der sicheren Konfiguration von Netzwerkkomponenten

überprüfen können. ATHENE verfügt außerdem über Kompetenzen im Aufbau und im Betrieb von Security Operation Centers. Das Spektrum der für die Absicherung des Betriebs behandelten Angriffe umfasst bspw. den Schutz vor Distributed Denial of Service-Angriffen (DDoS), die Erkennung von Malware und APT. Zur Absicherung des Betriebs stehen auch Werkzeuge zur Verfügung, die von ATHENE im Rahmen von Forschungs- und Entwicklungsprojekten entwickelt wurden, z.B. zur Visualisierung von sicherheitsrelevanten Ereignissen.

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen #Behandlung von Sicherheitsvorfällen & IT-Forensik

ATHENE unterstützt Organisationen der Wirtschaft und der öffentlichen Hand bei der Erkennung von Cyberangriffen und der Reaktion auf Cyberangriffe, zudem bei der Wiederherstellung eines sicheren Zustands und beim planmäßigen Hochfahren von Infrastrukturkomponenten. Auch forscht und unterstützt ATHENE bei der Entwicklung von Sicherheitsarchitekturen und Prozessen, mit denen solche Angriffe zukünftig vermieden und Schäden reduziert werden können.

Infrastrukturelle Sicherheitsaspekte

#Betriebs- und Steuerungstechnik #SPS & ICS #Intelligente Messsysteme #physische IT-Sicherheit

ATHENE forscht u.a. im Bereich der Sicherheit Kritischer Infrastrukturen, cyberphysikalischen Systemen, Netzwerksicherheit und Domain Validation.

Netze und Kommunikation

#Netzarchitektur und -design #Netzkomponenten #Netzmanagement #Funknetze

ATHENE beschäftigt sich in einem Schwerpunkt mit der Verbesserung der Sicherheit von Kommunikationsnetzen. ATHENE untersucht hierbei die Sicherheit grundlegender Protokolle des Internets wie DNS, BGP oder NTP. Neben der Sicherheit dieser Protokolle forscht ATHENE auch an der Umsetzung dieser Protokolle in Netzwerkkomponenten wie z.B. Routern und zieht hierbei auch mögliche Fehlkonfigurationen von Netzwerkkomponenten und die Implikationen für Sicherheitseigenschaften in Betracht. Im Bereich der Kommunikationssicherheit beschäftigt sich ATHENE auch mit Sicherheitsfragestellungen für Technologien unterhalb der Netzwerkschicht, wie etwa moderne Drahtlostechnologien.

Vernetzung von Systemen, IoT

#Smart Home #Autonomes Fahren #Fahrassistenzsysteme #Künstliche Intelligenz

ATHENE beschäftigt sich mit Sicherheitsfragestellungen im Zusammenhang mit IoT in verschiedenen Anwendungsdomänen und kooperiert hierzu mit Vertretern dieser Anwendungsdomänen. Weitere Forschungsbereiche sind die Sicherheit in Smart Citys, wie z.B. in autonomen Straßenbahnen, die Anwendung von KI in der Cybersicherheit, die Sicherheit des autonomen und vernetzten Fahrens oder die Sicherheit hochvernetzter Produktionsanlagen.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger
- Kinder und Heranwachsende
- Akademikerinnen und Akademiker
- Angestellte
- Medien
- Hacker

Viele von ATHENE veröffentlichte Informationen und Angebote richten sich auch an die Zivilgesellschaft, so bspw. die Volksverschlüsselung zur vertraulichen Kommunikation.

Wissenschaft

- Bildungseinrichtung
- Forschungseinrichtung

ATHENE steht in engem Austausch mit anderen Akteuren und Initiativen der Wissenschaft und ist aktiv in der Ausbildung von Fachkräften.

Wirtschaft

- Aerospace / Luft- und Raumfahrt
- Automobilbranche / Automotive
- Energieversorgung
- Finanzdienstleistung
- Gesundheits- und Sozialwesen
- Information und Kommunikation
- Sonstiges verarbeitendes Gewerbe
- Verkehr / Infrastruktur
- Kritische Infrastruktur

Die Forschung und Entwicklung in ATHENE ist darauf ausgelegt, gewonnene Expertisen und Ergebnisse in die Wirtschaft zu transferieren. Die wirtschaftliche Zielgruppe von ATHENE beinhaltet ein breites Spektrum an Branchen und Unternehmen.

Staat

- Bund
- Land
- Gebietskörperschaft
- Ausschuss/Gremium
- Behörde/Verwaltung
- Ministerium

ATHENE unterstützt staatliche Einrichtungen durch Forschungs- und Entwicklungsarbeit und das Einbringen von Fachexpertisen, bspw. im Rahmen der Schwachstellenanalyse der Corona-Warn-App.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Ausbildung und Schulung
- Beratung
- Entwicklung
- Konzept
- Prüfung/Audits/Zertifizierung/Standardisierung

ATHENE bietet Dienstleistungen in den drei Bereichen Entwicklung, Analysen und Tests sowie Sicherheitsdienste an. Entwicklung umfasst den Entwurf von Sicherheitsarchitekturen, Konzepten, Verfahren, Protokolle, Methoden, Werkzeugen, Prozessen und Softwareimplementierungen. Im Bereich Analysen und Tests werden Anforderungs- und Bedrohungsanalysen, Sicherheitsanalysen von Software, Diensten, Hardware, Netzen oder Protokollen usw. angefertigt. ATHENE bietet auch Sicherheitsdienste, wie bspw. die Ausstellung von Public-Key-Zertifikaten für überprüfte Identitäten von Bürgerinnen und Bürgerinnen und Bürgerinnen und Bürgern an. Zudem fertigt ATHENE Vergleiche, Benchmarks etc. an und ist in der Ausbildung aktiv.

Information

- Informationsaufbereitung
- Literatur
- Lernprogramm
- Newsletter
- Öffentlichkeitsarbeit
- Wissenschaftliche Veröffentlichung
- Studie

ATHENE bereitet seine Ergebnisse zielgruppengerecht auf und stellt dieses den entsprechenden Adressaten zur Verfügung. Neue Erkenntnisse und Ergebnisse werden im Rahmen von wissenschaftlichen Veröffentlichungen zur Verfügung gestellt. Neben diesen führt ATHENE auch Studien durch. Abhängig von der Kritikalität der Ergebnisse stellt ATHENE neue Erkenntnisse entweder der Allgemeinheit oder zunächst nur einem begrenzten Adressatenkreis, wie bspw. Softwarehersteller, in deren Software Schwachstellen gefunden wurden, zur Verfügung.

Produkt

- Hardware
- Software

Die in ATHENE entstehenden Produkte als Ergebnisse aus Forschung und Entwicklung haben für die Verwertung am Markt zumeist einen Prototypenstatus. Für die von ATHENE entwickelten Lösungen werden Lizenzen vergeben, um diese zu marktreifen Produkten weiterzuentwickeln oder in Produkte oder Geschäftsmodelle zu integrieren.

netlab - CyberSecurity-Verbund Sachsen-Anhalt

Beitrag zur Cybersicherheit

Kontakt:

Friedrichstr. 57-59

38855 Wernigerode

netlab.hs-harz.de, cslsa.de

Wissenschaftliche Initiative

Das Forschungsprojekt „CyberSecurity Verbund Sachsen-Anhalt“ ist ein Gemeinschaftsprojekt der Hochschule Harz, der Martin-Luther-Universität Halle-Wittenberg (MLU) und der Otto-von-Guericke-Universität Magdeburg (OVGU). Als Teil der Digitalen Agenda des Landes Sachsen-Anhalts wird es vom Land und aus Mitteln des Europäischen Fonds für regionale Entwicklung (EFRE) finanziert. Der CyberSecurity-Verbund Sachsen-Anhalt wird als F&E-Projekt am netlab der Hochschule Harz durchgeführt und wissenschaftlich koordiniert durch die drei Verbundpartner. Das netlab-Team am Fachbereich Automatisierung und Informatik der Hochschule Harz beschäftigt sich mit verschiedenen Themenfeldern der Cybersicherheit. Diese umfassen z.B. Sicherheitsanalysen, -konzeptionen und -entwürfe oder Security by Design für Wirtschaft, Verwaltung und Hochschulen bzw. das Bildungswesen auf Basis von Sicherheitskomponenten und -standards wie PKI, eIDAS und Sicherheitsprotokollen. Am netlab werden Forschungsprojekte im Bereich Cybersicherheit, E-Government und Digitalisierung durchgeführt und wissenschaftliche Publikationen veröffentlicht. Netlab wird gefördert von der EU, dem Bund und dem Land Sachsen-Anhalt.

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Innerhalb des CyberSecurity-Verbund Sachsen-Anhalt findet weitreichende Vernetzung, auch über den Kreis der Verbundpartner hinweg, statt.

Bildung und Awareness

#Schulung #Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft #Universitäres Bildungsangebot

Konzeption und Vorgehensweisen

#Kryptographie #Authentifizierung #Informationssicherheitsmanagement #Identitätsmanagement #Berechtigungsmanagement #Datenschutz

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen #IT-Administration

Im Rahmen der Projekte TREATS und StudIES+ wurden eIDAS-basierte Anwendungen und Servicekonten für Hochschulen und das Bildungswesen, bspw. für Zeugnis- und Praktikumswesen, mit Transfermöglichkeiten in weitere Bereiche entwickelt und in Kooperation mit den Projektpartnern sowie externen Partner wie der Stiftung für Hochschulzulassung erprobt. Dabei wird der Anschluss an das europäische EMREX-Netzwerk und Einbringungen in Umsetzungsvorhaben nach dem OZG berücksichtigt.

Netze und Kommunikation

#Netzarchitektur und -design #Netzkomponenten #Netzmanagement

Vernetzung von Systemen, IoT

Am netlab werden Sicherheitsanalysen von Netzen, Betriebssystemen und Anwendungen und deren Härtung u.a. durch Einsatz von Sicherheitskomponenten und Sicherheitsmanagement erforscht, u.a. die Übertragung von eIDAS-Infrastrukturen und -Anwendungen in IT-Verbünde und Netzwerkmanagement, z.B. für Anwendungen im Bereich Industrie 4.0.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger
- Kinder und Heranwachsende
- Akademikerinnen und Akademiker
- Angestellte
- Seniorinnen und Senioren

Die Forschungsergebnisse am netlab richten sich insbesondere an Akademikerinnen und Akademiker und Angestellte.

Wissenschaft

- Bildungseinrichtung
- Forschungseinrichtung

F&E-Projekte und -Ergebnisse werden in Lehre und weitere Forschungen eingebracht.

Wirtschaft

- Finanzdienstleistung
- Freiberufliche wissenschaftliche technische Dienstleistungen
- Gesundheits- und Sozialwesen
- Grundstücks- und Wohnungswesen
- Handel
- Information und Kommunikation
- Beratung
- Rechtsanwälte
- Sonstige wirtschaftliche Dienstleistungen
- Sonstiges verarbeitendes Gewerbe
- Verkehr / Infrastruktur
- Kritische Infrastruktur

F&E-Projekte und -Ergebnisse insbesondere fließen in Beratungen, Kooperationen und weitere F&E-Projekte der Wirtschaft ein.

Staat

- Bund
- Land
- Gebietskörperschaft
- Behörde/Verwaltung
- Einrichtung
- Ministerium
- öfftl. Stiftung

Entwicklungen und Ergebnisse werden in Projekte, Vorhaben und Diskussionen mit Zuständigen des Bundes und dem Land Sachsen-Anhalt, inkl. deren Behörden, Verwaltungen und Einrichtungen, eingebracht.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Ausbildung und Schulung
- Beratung
- Entwicklung
- Konzept

Information

- Informationsaufbereitung
- Öffentlichkeitsarbeit
- Wissenschaftliche Veröffentlichung
- Sonstiges Informationsangebot

Die Arbeitsgruppe veröffentlicht wissenschaftliche Publikationen sowie weitere Informationsmaterialien.

Produkt

- Clouddienste/PaaS
- Software
- Software/SaaS
- Vernetzte Produkte (IoT)

F&E-Projekte und -Ergebnisse insbesondere zur Cybersicherheit werden in Beratungen, Kooperationen, Konzeptionen, Entwicklungen, Demonstrationen bzw. Erprobungen und weitere F&E-Projekte eingebracht.

Open Competence Center for Cyber Security (open-c3s)

Beitrag zur Cybersicherheit

Das open-c3s ist ein Verbund aus neun in der IT-Sicherheit tätigen Hochschulen zur Entwicklung digital gestützter wissenschaftlicher Aus- und Weiterbildungsprogramme. Ziel ist die Aus- und Weiterbildung von Fachkräften im Bereich der IT-Sicherheit.

Aktueller Verbundsprecher:

Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)

Department Informatik

Martensstr. 3

91058 Erlangen

open-c3s.de

Wissenschaftliche Initiative

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Mehrere Hochschulen aus verschiedenen Bundesländern entwickeln im Verbund von open-c3s gemeinsam die angebotenen Aus- und Weiterbildungsprogramme.

Bildung und Awareness

#Universitäres Bildungsangebot

Aus open-c3s sind bislang fünf Aus- und Weiterbildungsprogramme hervorgegangen, die an unterschiedlichen Hochschulen angeboten werden.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger
- Akademikerinnen und Akademiker

Das Angebot von open-c3s umfasst sowohl Bachelor- als auch Masterstudiengänge, einen Einführungsstudiengang und ein Zertifikatprogramm. Es ist an interessierte Bürgerinnen und Bürger und Akademikerinnen und Akademiker gerichtet.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Ausbildung und Schulung

Die im Verbund von open-c3s entwickelten fünf Weiterbildungsprogramme im Bereich Cybersicherheit sind: Studium Initiale, Bachelorstudiengang Informatik/IT-Sicherheit, Zertifikatsprogramm für gezielte wissenschaftliche Weiterbildung im Cybersicherheitsbereich, Masterstudiengang IT-Governance, Risk and Compliance Management und Masterstudiengang Digitale Forensik.

Passau Institute of Digital Security (PIDS)

Beitrag zur Cybersicherheit

Das PIDS der Universität Passau zielt auf die Interdisziplinarität zwischen Informatik, Recht und Wirtschaft ab. Fokus des Instituts bildet die Forschung im Kontext von IT-Sicherheit und Recht, die in verschiedenen Projekten bspw. rechtliche Fragen von digitalen Identitäten, Datenschutzrecht, Websicherheit oder Cloudsicherheit thematisiert. Darüber hinaus besteht ein auf IT-Sicherheit und Sicherheitsrecht ausgerichtetes Lehrangebot.

Kontakt:

Innstr. 41

94032 Passau

pids.uni-passau.de

Wissenschaftlicher Akteur

Thematische Schwerpunkte (Auszug)

Bildung und Awareness

#Universitäres Bildungsangebot

Neben der Forschung betreibt das PIDS auch Lehre im Bereich IT-Sicherheit und Sicherheitsrecht.

Konzeption und Vorgehensweisen

#Datenschutz

Das PIDS forscht im Rahmen von Sicherheitsrecht insbesondere an Themen des Datenschutzes.

Netze und Kommunikation

#Netzarchitektur und -design #Funknetze

Das PIDS forscht in den Arbeitsgruppen Internet Law and Policy, Computer Networking and Energy Systems, Security and Reliability in Cloud Environments, IT-Security und Computer Engineering zu relevanten Themen der Cybersicherheit.

Zielgruppe

Zivilgesellschaft

- Bildungseinrichtung
- Forschungseinrichtung

Ziel des Instituts ist insbesondere die interdisziplinäre Forschung und Lehre.

Wissenschaft

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Wissenschaftliche Veröffentlichung
- Studie

Die Ergebnisse der Forschungsarbeit des PIDS kommen in der Lehre, in verschiedenen Projekten sowie in Publikationen zum Ausdruck.

"Serious Games "- Forschung an der Technischen Hochschule Wildau

Beitrag zur Cybersicherheit

An der TH Wildau wird im Fachbereich Wirtschaft, Informatik, Recht in mehreren Projekten im Bereich der Awareness in der Cybersicherheit geforscht. Die Awareness-Konzepte, die auf Schüler und Berufseinsteiger ausgerichtet sind, werden durch die Horst Görtz Stiftung gefördert. Außerdem wird erforscht und vom BMBF gefördert, wie eine Karriere im Bereich der Cybersicherheit für Frauen attraktiver gemacht werden kann. Das Leitthema der Projekte ist Lernen durch „Serious Games“ und wird ab 2020 auf KMU und Mitarbeitende ausgedehnt.

Kontakt:

Fachbereich Wirtschaft, Informatik, Recht

Hochschulring 1

15745 Wildau

th-wildau.de

secaware4school.wildau.biz

security.wildau.biz

secaware4job.th-wildau.de

Wissenschaftlicher Akteur

Thematische Schwerpunkte (Auszug)

Bildung und Awareness

#Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft #Schulisches Bildungsangebot

Im Projekt SecAware4school werden Schüler der Klassen 6 bis 11 in erlebnisorientierten Lernszenarien für IT-Sicherheitsthemen sensibilisiert. Außerdem wurde im Projekt SecAware4job eine Zusatzqualifikation im Bereich der IT-Sicherheits-Awareness für Berufseinsteiger entwickelt. Das Projekt Gendersensible Studien- und Berufsorientierung für den Beruf Security Spezialistin, kurz Security, beschäftigt sich mit Attraktivitätssteigerung der Cybersicherheitsbranche speziell für weibliche Fachkräfte.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger
- Kinder und Heranwachsende

Die bisherigen Forschungsprojekte zielen speziell auf Schüler und Berufseinsteiger ab. Zukünftig werden KMU im Mittelpunkt stehen.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Wissenschaftliche Veröffentlichung
- Studie
- Sonstiges Informationsangebot

Informationen zu den Projekten werden auf den jeweiligen Webseiten veröffentlicht. Die Resultate der Begleitforschung werden zudem publiziert.

Produkt

- Sonstige Produkte

Im Rahmen diverser Projekte werden Serious Games entwickelt, um erlebnisorientiert Inhalte zu vermitteln. Diese Spiele werden bspw. Schulen zur Verfügung gestellt.

Stiftung Neue Verantwortung e.V. (SNV)

Beitrag zur Cybersicherheit

Kontakt:

Berliner Freiheit 2

10785 Berlin

stiftung-nv.de

Wissenschaftlicher Akteur

Die SNV ist eine als Verein organisierte gemeinnützige Denkfabrik, die sich mit den politischen und gesellschaftlichen Fragen des technologischen Wandels auseinandersetzt. Um die inhaltliche Unabhängigkeit zu gewährleisten und der Arbeit zugleich einen stabilen institutionellen Rahmen zu geben, hat sich die SNV für eine Mischfinanzierung durch möglichst viele unterschiedliche Geldgeber entschieden. Alle Analysen, Handlungsempfehlungen oder sonstigen Papiere werden deshalb auch auf der Website der SNV veröffentlicht und stehen immer der Öffentlichkeit zur Verfügung. Bei der SNV beschäftigen sich Experten aus verschiedenen Arbeitsgebieten in diversen Themen, sowohl an IT-Sicherheitsthemen (u.a. IoT, 5G), als auch an nationaler und internationaler Cybersicherheitspolitik (u.a. VEP, Staatliches Hacken, Schutz der Wahlen), sowie am Grundrechte-Schutz (u.a. Kontrolle der Nachrichtendienste. Ziel der SNV ist die Entwicklung konkreter Vorschläge für die Politik zur Gestaltung des gesamtgesellschaftlichen technologischen Wandels. Auch vertritt die SNV die Position der Zivilgesellschaft in Sachen Digitalisierungspolitik. Die SNV veröffentlicht Artikel und Studien, veranstaltet aber auch Konferenzen, Workshops oder Vorträge.

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Die SNV vernetzt Akteure der Cybersicherheit und bündelt dadurch Wissen von Forschungsorganisationen, Unternehmen, zivilgesellschaftlichen Gruppen, Behörden und engagierten Bürgerinnen und Bürgern. Im Bereich IT-Sicherheitspolitik betrachten die Experten bspw. IT-Lieferketten, Strategien von Cyber-Kriminellen oder europäische Normengebung umfassend und interdisziplinär. Dafür beziehen sie in ihrer Recherche die Perspektive von Datenschützen, Wirtschaftsvertretern, Behördenmitarbeitern und weiteren beteiligten Akteuren ein.

Bildung und Awareness

#Awareness in der Politik #Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft

Die SNV trägt mit ihrer Arbeit zu aktuellen politischen und gesellschaftlichen Fragen der Digitalisierung und neuer Technologien zu einer breiten Sensibilisierung für IT-Sicherheitsthemen bei. Bspw. werden im Arbeitsgebiet „IT-Sicherheit im Internet der Dinge“ Aspekte der IT-Sicherheit im Kontext der immer weiterwachsenden Vernetzung thematisiert. Im Arbeitsgebiet „Internationale Cyber-Sicherheitspolitik“ werden Fragestellungen der internationalen IT-Sicherheitspolitik insb. aus gesellschaftlichem Blickwinkel diskutiert und Empfehlungen für die Politik abgeleitet. Zudem werden Fragestellungen zu digitalen Grundrechten und Überwachung im Kontext der Demokratie betrachtet.

Zielgruppe

Zivilgesellschaft

Wissenschaft

Wirtschaft

Staat

Die SNV befasst sich mit politischen und gesellschaftlichen Fragen der Digitalisierung und neuer Technologien und adressiert somit perspektivisch eine breite Zielgruppe. Dazu soll die Expertise und das praktische Wissen von externen

Forschungsorganisationen, Unternehmen, Behörden und der Gesellschaft genutzt werden. Zusätzlich fertigt die SNV Lösungsskizzen anhand aktueller Problemanalysen an.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Newsletter
- Wissenschaftliche Veröffentlichung

Das Angebot der SNV umfasst Publikationen und verschiedene Veranstaltungen wie Workshops, Vorträge, Konferenzen oder Diskussionen. Außerdem wird ein Newsletter angeboten, der die Leser über die aktuellsten Aktivitäten der SNV informiert.

Weizenbaum-Institut für vernetzte Gesellschaft

Beitrag zur Cybersicherheit

Kontakt:

Hardenbergstr. 32

10623 Berlin

weizenbaum-institut.de

Wissenschaftlicher Akteur

Das Weizenbaum Institut für vernetzte Gesellschaft untersucht aus interdisziplinärer Perspektive den Wandel durch die Digitalisierung. Eine Forschungsgruppe setzt sich speziell mit dem Thema "Digitalisierung und vernetzte Sicherheit" auseinander. Durch Publikationen und Veranstaltungen werden Akteure vernetzt und der Wissenstransfer gefördert. Das Weizenbaum-Institut ist ein Verbundprojekt, bestehend aus der Freien Universität Berlin, der Humboldt-Universität zu Berlin, der TU Berlin, der Universität der Künste Berlin, der Universität Potsdam und dem Fraunhofer-Institut für Offene Kommunikationssysteme (FOKUS). Koordinator des Verbundes ist das Wissenschaftszentrum Berlin für Sozialforschung. Das Weizenbaum-Institut wird vom BMBF gefördert.

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Durch die Organisation von Veranstaltungen und den angestrebten Wissenstransfer vernetzt das Institut verschiedene Akteure aus Politik, Wirtschaft, Wissenschaft und Gesellschaft.

Bildung und Awareness

#Endgerätesicherheit #Datenschutz #IT-Sicherheitsstandards

Eine Forschungsgruppe des Weizenbaum-Institutes widmet sich der Untersuchung von Sicherheitskonzepten und Sicherheitslösungen im Hinblick auf deren Auswirkungen auf Privatsphäre und zivilgesellschaftliches Leben. Erforscht werden u.a. die Anwendbarkeit und Resilienz von Technologien sowie Denk- und Handlungsmuster der Nutzer im Kontext soziologischer Aspekte der Sicherheit bzw. gefühlter Sicherheit von IT-Systemen. Das Weizenbaum-Institut untersucht zudem Sicherheits- und Datenschutzaspekte behördlicher App-Technologien zur Bevölkerungswarnung.

Vernetzung von Systemen, IoT

#Künstliche Intelligenz

Im Fokus der Forschung des Weizenbaum-Instituts stehen auch die Entwicklung von Sicherheitslösungen für IoT-Systeme sowie die Kritikalität KI-basierter Systeme.

Zielgruppe

Zivilgesellschaft

Wissenschaft

Wirtschaft

Staat

Die Ergebnisse der Forschungsgruppen richten sich, abhängig vom Forschungsgegenstand, an Adressaten in der Politik, Wirtschaft, Wissenschaft und Gesellschaft.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Literatur
- Wissenschaftliche Veröffentlichung
- Studie

Zur Bewältigung des digitalen Wandels bemüht sich das Institut um einen Wissenstransfer zwischen Politik, Wirtschaft, Wissenschaft und Gesellschaft. Hierzu werden insb. Forschungsergebnisse publiziert und Veranstaltungen organisiert.

8.3 Wirtschaftliche Initiativen und Akteure

IT Security made in Germany (ITSMIG)

Beitrag zur Cybersicherheit

Kontakt:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Chausseestr. 17

10115 Berlin

teletrust.de/itsmig

Wirtschaftliche Initiative

Das markenrechtlich geschützte TeleTrusT-Vertrauenszeichen ITSMIG darf von Unternehmen zeitlich befristet getragen werden, die den Unternehmenshauptsitz in Deutschland haben, vertrauenswürdige IT-Sicherheitslösungen ohne versteckte Zugänge anbieten, in Deutschland IT-Sicherheitsforschung und -entwicklung betreiben sowie die gesetzlichen Anforderungen an den Datenschutz einhalten. Zur Beantragung des Vertrauenszeichens muss eine Konformitätseigenerklärung unterzeichnet werden. ITSMIG befasst sich mit der Schaffung und Weiterentwicklung des gleichnamigen Vertrauenszeichens deutscher IT-Sicherheits-unternehmen. Der TeleTrusT ist Träger der zusammen mit dem BMWi und dem BMI durch die IT-Sicherheitswirtschaft etablierten Initiative. Ziel der als eingetragene Marke agierenden Initiative ist die gemeinsame Außendarstellung der in ihr organisierten deutschen IT-Sicherheitswirtschaft sowie die Förderung von Zusammenarbeit und Darstellung deutscher IT-Sicherheitskompetenz in relevanten Exportmärkten.

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

ITSMIG fungiert als Interessenvertretung, übernimmt vernetzende Aktivitäten für Marktteilnehmer der IT-Sicherheitswirtschaft und sorgt für einen Informationsaustausch zwischen Fach- und Führungskräften der Branche.

Konzeption und Vorgehensweisen

#Datenschutz #IT-Sicherheitsstandards

Das Vertrauenszeichen ITSMIG soll Nutzern und Geschäftspartnern symbolisieren, dass der Anbieter der IT-Sicherheitslösung vertrauenswürdig ist und höchsten qualitativen Standards entspricht.

Zielgruppe

Wissenschaft

Wirtschaft

Dem Netzwerk können sich Unternehmen sowie Forschungs- und Entwicklungseinrichtungen aus dem Bereich IT-Sicherheit anschließen. Auch Verbraucher profitieren von der Vergabe des Vertrauenszeichens.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Öffentlichkeitsarbeit

Die Initiative repräsentiert seine Mitglieder und fördert und organisiert den Informationsaustausch der Mitglieder mit verschiedenen Zielgruppen.

it's.BB - IT-Sicherheitsnetzwerk Berlin-Brandenburg

Beitrag zur Cybersicherheit

Das it's.BB sieht seine Aufgabe darin, Ansprechpartner für IT-Sicherheitsfragen in der Hauptstadtregion zu sein und themenspezifisch Kontakt mit dort ansässigen Unternehmen herzustellen. Zur Erfüllung dieser Aufgabe haben sich 2018 zehn Gründungsmitglieder aus der Cybersicherheits- und IT-Branche, regionale IT-Dienstleister, Softwarehersteller, Berater und Zertifizierer zusammengeschlossen.

Ansprechpartner:

c/o NKMG mbH

Poßweg 45

14163 Berlin

itsbb.net

Wirtschaftliche Initiative

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

it's.BB fungiert als Vermittler bei regionalen Projekten und Kooperationen, setzt sich aber auch für verbesserte Fachkräftegewinnung durch Kooperationen mit Hochschulen ein. it's.BB begleitet zudem Forschungs- und Förderprogramme. Die Vernetzung mit Unternehmen aus dem KRITIS-Bereich steht ebenfalls im Fokus.

Bildung und Awareness

#Schulung #Awareness in der Politik #Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft

it's.BB veranstaltet regelmäßig Awareness Veranstaltungen für Wirtschaftsunternehmen, Politik, öffentliche Verwaltungen und interessierte Bürgerinnen und Bürger.

Konzeption und Vorgehensweisen

#Kryptographie #Blockchain #Authentifizierung #Informationssicherheitsmanagement #Endgerätesicherheit #Identitätsmanagement #Berechtigungsmanagement #Compliance Management #Datenschutz #IT-Sicherheitsstandards

it's.BB arbeitet an der Entwicklung eines praxisnahen Sicherheitschecks für KMU, spricht Empfehlungen für vorhandene IT-Sicherheitsstandards aus und bietet hierfür Anwendungsbeispiele.

Zielgruppe

Wissenschaft

- Bildungseinrichtung
- Forschungseinrichtung

Der it's.BB kooperiert eng mit den regionalen Bildungs- und Forschungseinrichtungen.

Wirtschaft

- Aerospace / Luft- und Raumfahrt
- Automobilbranche / Automotive
- Energieversorgung
- Gesundheits- und Sozialwesen
- Information und Kommunikation
- Rechtsanwälte
- Verkehr / Infrastruktur
- Wasserver- und -entsorgung
- Abfallentsorgung
- Kritische Infrastruktur

Das Angebot von it's.BB richtet sich an Unternehmen in der Hauptstadtregion Berlin-Brandenburg sowie an Hochschulen, die an Kooperationen interessiert sind.

Staat

- Bund
- Land
- Gebietskörperschaft
- Behörde/Verwaltung
- Ministerium
- öfftl. Stiftung
-

Der it's.BB kooperiert eng mit öffentlichen Stellen.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung

Durch it's.BB werden unter anderem Praxishilfen und Checklisten sowie Empfehlungen und Anwendungsbeispiele vorhandener Standards für die Mitglieder erarbeitet.

Karlsruher IT-Sicherheitsinitiative (KA-IT-SI)

Beitrag zur Cybersicherheit

Die KA-IT-SI ist ein Zusammenschluss verschiedener Unternehmen aus der Region Karlsruhe und Umgebung. Das Netzwerk hat zum Ziel, mittelständische Unternehmen im Hinblick auf IT-Sicherheitsthemen zu sensibilisieren, erforderliches Wissen zu vermitteln und den Austausch von Erfahrungen unter IT-Sicherheitsverantwortlichen zu fördern. Dazu werden eine Vielzahl themenbezogener Fachveranstaltungen angeboten. Die Initiative wird unter anderem durch das Fraunhofer IOSB, das KIT, die IHK und die Stadt Karlsruhe unterstützt.

Ansprechpartner:

Secorvo Security Consulting GmbH

Ettlinger Str. 12-14

76137 Karlsruhe

ka-it-si.de

Wirtschaftliche Initiative

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Die angebotenen Fachveranstaltungen fördern den Erfahrungs- und Wissensaustausch von IT-Sicherheitsverantwortlichen.

Bildung und Awareness

#Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft #Schulisches Bildungsangebot

Durch die Angebote der Initiative sollen insbesondere mittelständische Unternehmen für die Bedeutung der IT-Sicherheit sensibilisiert werden sowie aktuelle Sicherheitsbedrohungen und Wege zum professionellen Umgang mit IT-Sicherheit aufgezeigt werden. Dazu findet unter anderem jährlich der "Tag der IT-Sicherheit" statt. Weiterhin bietet die Initiative verschiedene Formate (z.B. "Krypto im Advent", "Kryptobox", "Anti-Prism-Party") sowie ein besuchbares Kryptologikum zur Sensibilisierung und Aufklärung der Gesellschaft im Bereich Datenschutz und Kryptographie.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger
- Kinder und Heranwachsende

Die verschiedenen Kryptographie-Formate richten sich insbesondere an Heranwachsende aber auch an Bürgerinnen und Bürger, die sich mit der Thematik vertraut machen wollen.

Wirtschaft

Die Angebote der Initiative zielen insbesondere auf den Mittelstand der Region Karlsruhe ab. Der "Tag der IT-Sicherheit" richtet sich konkret an Geschäftsführer, IT-Leiter und Sicherheits- und Datenschutzbeauftragte von Unternehmen der Region Karlsruhe.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Sonstiges Informationsangebot

Das Angebot der Initiative besteht vorrangig aus verschiedenen Fachveranstaltungen zum Thema IT-Sicherheit. Darüber hinaus werden verschiedene Projekte im Bereich Kryptographie, z.B. ein besuchbares Kryptologikum oder der Wettbewerb "Krypto im Advent" durchgeführt.

Koordinierungsstelle IT-Sicherheit des DIN e.V. (KITS)

Beitrag zur Cybersicherheit

Die KITS ist Teil des DIN e.V. und agiert als Vermittler zwischen unterschiedlichen Regelsetzern für IT-Sicherheit. Dazu koordiniert die Stelle die Aktivitäten der unterschiedlichen Akteure, die an der Entwicklung von branchenspezifischen Normen und Standards im Bereich IT-Sicherheit beteiligt sind. Sie setzen sich außerdem für den gegenseitigen Austausch von Informationen im Bereich Cybersicherheit ein. So sollen branchenspezifische Normungsaktivitäten koordiniert, Insellösungen vermieden und eine übergreifende, vernetzte Sicherheit geschaffen werden. In Zuge dessen erstellt KITS auch die Normungs-Roadmap IT-Sicherheit.

Kontakt:

Saatwinkler Damm 42/43

13627 Berlin

din.de

Wirtschaftlicher Akteur

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Die KITS-Konferenz hat zum Ziel, durch das Zusammenbringen von Fachexperten aus Wissenschaft, Wirtschaft, Politik und Gesellschaft ein politisches Forum zum Dialog und zur Schaffung eines koordinierten Umgangs mit Sicherheitsproblemen zu schaffen.

Bildung und Awareness

#Awareness in der Politik #Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft

Durch öffentlich zugängliche Veranstaltungen, Workshops und Konferenzen soll das Bewusstsein für die Relevanz der IT-Sicherheit geschaffen werden.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger

Wissenschaft

Staat

Wirtschaft

Die Aktivitäten der KITS richten sich insbesondere an die DIN-Normenausschüsse, Verbände, Fachexperten, Behörden sowie an Unternehmen. Das bereitgestellte Informationsmaterial sowie die Veranstaltungen richten sich darüber hinaus auch an die Öffentlichkeit.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Beratung

Die Normenausschüsse werden von der KITS bei der Entwicklung von Normen, die für die IT-Sicherheit von Relevanz sind, beraten.

Information

- Informationsaufbereitung
- Sonstiges Informationsangebot

Durch die Erstellung der deutschen Normungs-Roadmap IT-Sicherheit wird die aktuelle Situation sowie zukünftige Entwicklungen in verschiedenen Schwerpunktgebieten der IT-Sicherheit dargestellt. Weiterhin übernimmt die KITS die Pflege eines Verzeichnisses aller IT- und informationssicherheitsrelevanten Normungsvorhaben, veröffentlicht themenbezogenes Informationsmaterial und präsentiert die Ergebnisse im Rahmen unterschiedlicher Formate wie z.B. Messen und bei Unternehmen.

Nachwuchsförderung IT-Sicherheit e.V.

Beitrag zur Cybersicherheit

Der Verein Nachwuchsförderung IT-Sicherheit hat im Jahr 2020 die Organisation der CSCG (siehe hierzu den Steckbrief der CSCG) übernommen. Hierbei handelt es sich um einen jährlich stattfindenden CTF-Wettbewerb, bei welchem sich Teilnehmende kompetitiv an herausfordernden Aufgaben aus den Bereichen Kryptografie, Stenografie, Exploitation, Web-Sicherheit und Reverse Engineering messen. Darüber hinaus unterstützt der Verein lokale Netzwerke zur Fortbildung im Bereich der IT-Sicherheit und zur Teilnahme an CTF-Wettbewerben. Mit der Organisation von Recruiting-Messen sollen insbesondere heranwachsende Talente im Bereich IT-Sicherheit mit Unternehmen vernetzt werden.

Kontakt:

Wilhelm-Raabe-Str. 16

44791 Bochum

nfits.de

Wirtschaftliche Initiative

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Ziel des Vereins ist in erster Linie, junge Menschen für den Bereich IT-Sicherheit zu begeistern. Dazu gehört unter anderem die Durchführung der CSCG. Weiter soll die Vernetzung junger Talente und Interessierter vorangebracht werden. Auch dem Thema Chancengleichheit hat sich der Verein angenommen, so soll auch der Anteil von jungen Frauen im Bereich der IT-Sicherheit gezielt gefördert werden.

Bildung und Awareness

#Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft #Sonstiges Bildungsangebot

Grundsätzlich soll das wichtige Thema IT-Sicherheit in der Gesellschaft und der Wirtschaft weiter vorangebracht werden, immer jedoch vor dem Hintergrund, dass die Förderung von jungen Nachwuchskräften von großer Bedeutung ist.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger
- Kinder und Heranwachsende
- Hacker

Der Verein ist offen für Unterstützende hinsichtlich des Themenbereiches Nachwuchsförderung in der IT-Sicherheit und besteht aus Personen aus der Wirtschaft und dem universitärem Umfeld mit Bezug zu dem Thema IT-Sicherheit. Auf durch den Verein organisierten Recruiting-Messen können Kontakte zu zukünftigen Arbeitgebern aufgebaut werden.

Staat

Wissenschaft

- Bildungseinrichtung
- Forschungseinrichtung

Es werden Kooperationen mit Bildungs- und Forschungseinrichtungen angestrebt, zum einen mit dem Ziel in einer engen Zusammenarbeit auf den Bedarf an Nachwuchsförderung hinzuweisen und zum anderen um herangehenden Nachwuchskräften auch die Chancen einer Karriere im Bereich der Wissenschaft näher zu bringen.

Staat

Unternehmen können den Verein im Rahmen einer Fördermitgliedschaft unterstützen und so die gemeinnützigen Ziele der Förderung der Jugendhilfe sowie die Förderung der Volks- und Berufsbildung einschließlich der Studierendenhilfe begünstigen.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

Der Verein Nachwuchsförderung IT-Sicherheit organisiert Recruiting-Messen, auf denen sich interessierte Unternehmen einem breiten Publikum an potenziellen heranwachsenden IT-Sicherheitsfachkräften präsentieren können.

Information

- Lernprogramm
- Sonstiges Informationsangebot

Der Verein zur Nachwuchsförderung IT-Sicherheit nimmt unter anderem auch die Aufgabe der Öffentlichkeitsarbeit und des Informationsangebotes wahr, insbesondere, um über Aktivitäten rund um das Themengebiet IT-Sicherheit zu informieren. Hierzu gehört die Veröffentlichung von Informationen bezüglich der Cyber Security Challenge Germany, der European Cyber Security Challenge sowie allgemeiner Aktivitäten des Vereins.

Nationale Initiative für Informations- und Internet-Sicherheit e.V. (NIFIS)

Beitrag zur Cybersicherheit

Die NIFIS hat sich zum Ziel gesetzt, Unternehmen im Kampf gegen die wachsenden Gefahren im Internet technisch, organisatorisch und rechtlich zu stärken. Es sollen die Vertraulichkeit, Verfügbarkeit und Integrität von Daten in digitalen Netzen gefördert und gewährleistet sowie Konzepte zum Schutz vor Angriffen aus dem Datennetz entwickelt, in pragmatische Lösungen umgesetzt und anschließend der Industrie zur Verfügung gestellt werden. In erster Linie richtet sich die Initiative an Wirtschaftsunternehmen, prinzipiell können sich jedoch alle an IT-Sicherheit interessierten Personen anschließen. Darüber hinaus sind auch Akteure der Wissenschaft sowie der Politik im Verein vertreten.

Ansprechpartner:

BMI

Berkersheimer Bahnstr. 5

60435 Frankfurt am Main

nifis.de

Wirtschaftliche Initiative

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Die Mitglieder von NIFIS werden durch die interdisziplinäre Arbeitsweise miteinander vernetzt und zur aktiven Kommunikation angeregt. NIFIS will insbesondere Anwender mit Anbietern vernetzen.

Bildung und Awareness

#Awareness in der Wirtschaft #Sonstiges Bildungsangebot

Die NIFIS führt Veranstaltungen zum Thema Informationssicherheit durch, die neben den Mitgliedern auch von Gästen besucht werden können.

Konzeption und Vorgehensweisen

#Informationssicherheitsmanagement #Compliance Management #Datenschutz

NIFIS bietet seinen Mitgliedern eine automatisierte und verschlüsselte Online-Datensicherung an.

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen

Mitglieder von NIFIS erhalten aktuelle und individuelle Warnhinweise zu sicherheitsrelevanten Bedrohungen per E-Mail.

Zielgruppe

Wirtschaft

- Automobilbranche / Automotive
- Energieversorgung
- Finanzdienstleistung
- Freiberufliche wissenschaftliche technische Dienstleistungen
- Handel
- Information und Kommunikation
- Beratung
- Rechtsanwälte
- Sonstige wirtschaftliche Dienstleistungen
- Sonstiges verarbeitendes Gewerbe
- Verkehr / Infrastruktur
- Abfallentsorgung

Die von NIFIS erarbeiteten Resultate richten sich an die Wirtschaft.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Beratung
- Sonstige Dienstleistung

Neben der Bereitstellung von Handlungsempfehlungen bietet NIFIS seinen Mitgliedern unentgeltlich eine Online-Datensicherung sowie eine Daten- und Hardwareversicherung an.

Information

- Informationsaufbereitung
- Öffentlichkeitsarbeit
- Studie

NIFIS informiert auf seiner Webseite über sicherheitsbezogene Nachrichten und Warnhinweise. Darüber hinaus werden Fachbeiträge, Studien und Stellungnahmen publiziert.

networker NRW e.V.

Beitrag zur Cybersicherheit

Kontakt:

Karolingerstr. 96

45141 Essen

networker-nrw.de

Wirtschaftliche Akteur

Der networker NRW e.V. ist ein Netzwerk persönlicher Kontakte im Bereich der Unternehmens-IT in Nordrhein-Westfalen. Der Arbeitskreis Informationssicherheit des Vereins treibt das Thema Cybersicherheit inhaltlich und sorgt für eine themenbezogene Zusammenarbeit der Mitgliedsunternehmen. Außerdem organisiert der networker NRW e.V. Veranstaltungen und Roadshows, bei denen verschiedene Sprecher zu aktuellen Themen wie Cybercrime und IT-Trends der Sicherheit referieren. Der networker NRW e.V. steht im Austausch mit verschiedenen Ministerien und Branchenverbänden und ist Partner des Bayerischen IT-Sicherheitsclusters (siehe den diesbezüglichen Steckbrief) für ISIS12, einem Modell mit konkreten Maßnahmen zur Einführung eines ISMS für KMU und Kommunen in 12 Schritten. ISIS12 basiert auf den IT-Grundschutz-Katalogen und dem Standard ISO/IEC 27001. Zudem engagiert sich der networker NRW e.V. in der ACS als Multiplikator.

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Der networker NRW e.V. bündelt die Kompetenzen der beteiligten Akteure und unterhält Kontakte zu Wirtschaft und Staat. Sein Arbeitskreis Informationssicherheit arbeitet mit öffentlichen Stellen und Zertifizierungsstellen zusammen, um Mitgliedsunternehmen bei der Umsetzung von Maßnahmen und Auditierungen der Cybersicherheit zu unterstützen.

Bildung und Awareness

#Awareness in der Wirtschaft

Mit dem umfangreichen Austausch, der themenspezifischen Vernetzung sowie den Veranstaltungsangeboten sensibilisiert der networker NRW e.V. seine Mitgliedsunternehmen für Cybersicherheitsthemen.

Zielgruppe

Wirtschaft

Das Netzwerk richtet sich an interessierte Unternehmen aus Nordrhein-Westfalen.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung

Der networker NRW e.V. informiert seine Mitglieder im Rahmen diverser Veranstaltungen und durch aktive Netzwerkpflege.

ReDi School of Digital Integration gGmbH

Beitrag zur Cybersicherheit

Kontakt:

Zinnowitzerstr. 8

10115 Berlin

redi-school.org

Wirtschaftlicher Akteur

Zweck der ReDI School of Digital Integration, einer Non-Profit-Organisation, ist die Förderung und Berufsbildung von Asylsuchenden, Geflüchteten und Menschen ohne Zugang zum Bildungssystem sowie die Förderung des bürgerschaftlichen Engagements zugunsten der Vorgenannten. Die Unterstützungsleistungen dienen der wirtschaftlichen und sozialen Integration von Geflüchteten in Deutschland, insbesondere durch die Bereitstellung von Kursen und Weiterbildung zur Erlangung von Programmier- und arbeitsmarktnahen IT-Kenntnissen. Die ReDI School vermittelt außerdem Kontakte zu potentiellen Arbeitgebern und Mentorenschaften und hilft beim Aufbau eines beruflichen Netzwerks. Insbesondere werden Schulungen angeboten, in deren Rahmen Wissen für IT-affine Menschen zu sicherheitsrelevanten Themen mithilfe von Software-Tools diverser Hersteller vermittelt wird, bspw. zu Bot Frameworks, künstlicher Intelligenz oder Identitätsmanagement.

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Die ReDI School of Digital Integration arbeitet mit Wirtschaftsunternehmen zusammen, welche Online-Schulungen zu ihren Systemen anbieten.

Bildung und Awareness

#Schulisches Bildungsangebot

Die ReDI School of Digital Integration bietet Weiterbildungsmaßnahmen zu sicherheitsrelevanten Digitalisierungsthemen und Programmiersprachen an, wie bspw. die Absicherung von Daten in Azure-Cloud und SQL-Servern gegen unbefugte Zugriffe. Neben einzelnen Kursen bietet die ReDI School of Digital Integration auch komplette Karriere-Vorbereitungskurse an. In „Computer Networking“ werden außerdem die Grundzüge der Netzwerksicherheit behandelt.

Zielgruppe

Zivilgesellschaft

Das Angebot der ReDI School of Digital Integration richtet sich an Asylsuchende, Geflüchtete und Menschen ohne Zugang zum Bildungssystem.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Ausbildung und Schulung

Die ReDI School of Digital Integration bietet Bildungsangebote zu digitalen Themen und vermittelt berufliche Kontakte, um Menschen in Deutschland zu integrieren.

Sicherheit macht Schule

Beitrag zur Cybersicherheit

Die Initiative "Sicherheit macht Schule" ist ein von Microsoft Deutschland getragenes Angebot, welches sich an Schulen richtet. Hierbei werden kostenfrei Unterrichtsmaterialien zu verschiedenen Themen der Internetsicherheit veröffentlicht. Damit fördert die Initiative die Awareness bei Kindern und Jugendlichen im Schulalter im Umgang mit dem Internet.

Ansprechpartner:

Microsoft Deutschland GmbH

Konrad-Zuse-Str. 1

85716 Unterschleißheim

sicherheit-macht-schule.de

Wirtschaftliche Initiative

Thematische Schwerpunkte (Auszug)

Bildung und Awareness

#Awareness in der Zivilgesellschaft #Schulisches Bildungsangebot

Die Initiative bietet Lehrmaterialien zum Thema Sicherheit im Internet an

Zielgruppe

Zivilgesellschaft

- Kinder und Heranwachsende

Staat

Wissenschaft

- Bildungseinrichtung

Die Initiative adressiert mit ihrem Angebot Schulen, deren Lehrpersonen sowie Kinder und Jugendliche im Schulalter.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Lernprogramm
- Sonstiges Informationsangebot

Im Rahmen der Initiative werden u.a. Unterrichtsmaterialien, Lehrvideos, das Ergebnis von Umfragen und ein Kinder- und Jugendmagazin veröffentlicht.

Teachtoday

Beitrag zur Cybersicherheit

Teachtoday ist eine Initiative der Deutschen Telekom, welche die kompetente Mediennutzung und den sicheren Umgang mit digitalen Medien fördert. Die Initiative wurde 2008 unter der Schirmherrschaft der EU-Kommission gegründet, seit 2014 führt die Deutsche Telekom die Initiative in Eigenverantwortung. Auf dem siebensprachigen Portal von Teachtoday werden praxis- und alltagsnahe Informationen und Tipps, eine Toolbox mit Projektideen, Trainings, Lernsnacks und das SCROLLER-Kindermedienmagazin zu Themen der kompetenten Mediennutzung wie Sicherheit und Datenschutz angeboten. Aktionen vor Ort für Kinder, Eltern und pädagogische Fachkräfte ergänzen das Angebot der Initiative.

Kontakt:

Deutsche Telekom AG

Friedrich-Ebert-Allee 140

53113 Bonn

teachtoday.de

Wirtschaftliche Initiative

Thematische Schwerpunkte (Auszug)

Bildung und Awareness

#Awareness in der Zivilgesellschaft

Die von Teachtoday angebotenen Informationen und Materialien fördern einen sicheren und kompetenten Umgang mit Medien. Dazu werden bspw. konkrete Trainings, Projektideen, das Kindermedienmagazin SCROLLER und Ratgeber für Eltern und Pädagogen, aber auch gezielt Inhalte für Kinder angeboten.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger
- Kinder und Heranwachsende
- Familien
- Seniorinnen und Senioren

Das Angebot von Teachtoday richtet sich an Kinder, Jugendliche, Eltern und Großeltern sowie pädagogische Fachkräfte.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Lernprogramm
- Blog
- Newsletter
- Sonstiges Informationsangebot

Das Informationsangebot von Teachtoday umfasst Themenwellen zu aktuellen Themen der sicheren und kompetenten Mediennutzung sowie einen Blog, eine Toolbox aber auch Aktionen vor Ort wie Workshops. Zudem wird das Kindermedienmagazin SCROLLER angeboten, unter anderem zu den Themen persönliche Daten und Datensicherheit, welches als Print-, aber auch als Onlineausgabe verfügbar ist.

8.4 Staatliche Initiativen und Akteure

Agentur für Innovation in der Cybersicherheit (Cyberagentur)

Beitrag zur Cybersicherheit

Die Cyberagentur ist ein Auftrag aus dem aktuellen Koalitionsvertrag und wird gemeinsam von BMI und BMVg verantwortet. Das Ziel der Cyberagentur ist es, die Finanzierung und Förderung von ambitionierten Forschungsvorhaben mit hohem Innovationspotenzial auf dem Gebiet der Cybersicherheit und diesbezüglicher Schlüsseltechnologien für die Bedarfsdeckung des Staates im Bereich der Inneren und Äußeren Sicherheit zu initiieren. Die Bundesregierung will mit der Cyberagentur Deutschland zu mehr eigener Technologie-Souveränität in der Cybersicherheit verhelfen. Die Cyberagentur wird zukünftig der Identifikation von Innovationen sowie der konkreten Auftragserteilung für die Entwicklung von Lösungen im Bereich Cybersicherheit dienen. Konkret wird die Cyberagentur als Kapitalgeber für Innovationen in der Cybersicherheit fungieren. Die Cyberagentur wird voraussichtlich noch im 1. Halbjahr 2020 gegründet.

Ansprechpartner:

BMI

Alt-Moabit 140

10557 Berlin

BMVg

Stauffenbergstr. 18

10785 Berlin

Staatliche Initiative

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Durch die aktive Förderung von Innovationen im Bereich Cybersicherheit soll mittel- bis langfristig der Schutz von Bürgerinnen und Bürgern, Verwaltung und Wirtschaft sichergestellt und die nationale Souveränität in der Cybersicherheit unterstützt werden. Zudem ist die Schließung von Lücken in der Forschungsarbeit zur Cybersicherheit geplant.

Konzeption und Vorgehensweisen

#Quanten-Kryptographie & Post-Quanten-Kryptographie

Grundsätzlich sollen Forschungsvorhaben gefördert werden, die potenziell einen strategischen Vorteil für die gesamtstaatliche Sicherheitsvorsorge bieten können. Thematisch sollen diese aus den Bereichen Quantentechnologie in der Cybersicherheit, KI in der Cybersicherheit, Alternative Rechnerarchitekturen, Interaction Sens-Act-Control sowie Resiliente IT-Systeme hervorgehen.

Zielgruppe

Zivilgesellschaft

Wissenschaft

Staat

Die finanzielle Förderung von Forschungsvorhaben soll in erster Linie die Innovationslandschaft Deutschlands bereichern und mittel- bis langfristig die gesamtstaatliche Sicherheitsvorsorge im Cyberraum sicherstellen.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

Die Cyberagentur identifiziert Forschungsprojekte mit hohem Innovationspotential für die Bedarfsdeckung des Staates im Bereich der Cybersicherheit. Nach Abschluss eines Projekts oder Programms verwaltet die Agentur die Ergebnisse und stellt sie der Bundesregierung zur Verfügung.

BSI für Bürger

Beitrag zur Cybersicherheit

BSI für Bürger ist ein Informationsangebot des BSI, welches sich an Privatanwender richtet. Auf der Webseite stehen kostenfreie Tipps und Empfehlungen zum sicheren Umgang mit dem Internet, zu aktuellen Sicherheitsrisiken und -hinweisen sowie als Erklärvideos zur Verfügung. Zusätzlich werden ein Podcast sowie eine Hotline angeboten. Zusammen mit dem BMI plant das BSI eine bundesweite Informations- und Sensibilisierungskampagne zur IT-Sicherheit durchzuführen.

Ansprechpartner:

BSI

Godesberger Allee 185-189

53175 Bonn

bsi-fuer-buerger.de

Staatliche Initiative

Thematische Schwerpunkte (Auszug)

Bildung und Awareness

#Awareness in der Zivilgesellschaft

Das gesamte Angebot der Initiative ist auf die Aufklärung der Bürgerinnen und Bürger zum sicheren Umgang mit dem Internet ausgerichtet. Das Informationsangebot, das auf der Webseite verfügbar ist, erstreckt sich über verschiedene Kategorien und Themengebiete. Es wird über Risiken wie bspw. Identitätsdiebstahl, Cybermobbing oder Schadprogramme informiert. Darüber hinaus stehen aber auch Empfehlungen und konkrete Hilfestellungen, z.B. zur Schadensbeseitigung, zur Verfügung.

Im Rahmen der bundesweiten Informationskampagne zur IT-Sicherheit wurde eine repräsentative Umfrage zum Thema Internetsicherheit durchgeführt, deren Ergebnisse der weiteren inhaltlichen Gestaltung der Informationskampagne dienen. Durch die Umfrage wurde ermittelt, welche Gefahren die Internetnutzer als relevant wahrnehmen.

Im Rahmen der bundesweiten Informationskampagne zur IT-Sicherheit wurde eine repräsentative Umfrage zum Thema Internetsicherheit durchgeführt, deren Ergebnisse der weiteren inhaltlichen Gestaltung der Informationskampagne dienen. Durch die Umfrage wurde ermittelt, welche Gefahren die Internetnutzer als relevant wahrnehmen.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger

Das Angebot der Initiative steht allen interessierten Bürgerinnen und Bürgern offen.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Newsletter
- Podcast

Neben Tipps und Empfehlungen auf der Webseite werden von der Initiative auch Newsletter, Erklärvideos, ein Podcast, Broschüren und eine Hotline für Verständnisfragen angeboten. Thematisch deckt das Angebot dabei zahlreiche Themen der IT-Sicherheit ab.

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Beitrag zur Cybersicherheit

Das BSI stellt als Behörde eine unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit in der Informationsgesellschaft für Staat, Wirtschaft und Gesellschaft dar. Das BSI untersucht und bewertet bestehende Sicherheitsrisiken und bietet seinen Kunden Dienstleistungen in den Kernbereichen Information, Beratung, Entwicklung und Zertifizierung an. Die Arbeit der Behörde wird von dem Ziel geleitet, das Niveau der Informationssicherheit in Behörden und Unternehmen stetig zu erhöhen. Das BSI setzt sich dafür ein, dass die Sicherheit der Informationsgesellschaft gewahrt bleibt. Dafür werden vom BSI Handlungsbedarfe identifiziert und Lösungsvorschläge erarbeitet.

Kontakt:

Godesberger Allee 185-189

53175 Bonn

bsi.bund.de

Staatlicher Akteur

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Das BSI pflegt ein Verbindungswesen in Deutschland, indem regional verteilt feste Ansprechpartner vor-Ort zur Verfügung stehen, um eine schnelle und direkte Kontaktaufnahme mit dem BSI ermöglichen. Die Ansprechpartner geben einen Überblick über Angebote und Expertise des BSI und vermitteln bei Bedarf Beratung und Unterstützung.

Über verschiedene Veranstaltungen und Netzwerke (IT-Grundschutz-Tag, BSI-Symposium, Deutscher IT-Sicherheitskongress, ACS etc.) ist das BSI gesamtgesellschaftlich im Kontakt und Austausch.

Im BSI sind andere staatliche Organe, wie das IT-Lagezentrum, das IT-Krisenreaktionszentrum und das Cyber-Abwehrzentrum integriert.

Mit der 2012 gegründeten ACS verfolgt das BSI das Ziel, die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen zu stärken und bietet damit eine Plattform zur Kooperation zwischen Wirtschaft, Behörden, Forschung und Wissenschaft sowie anderen Institutionen.

Bildung und Awareness

#Schulung #Awareness in der Politik #Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft #Berufliches Bildungsangebot

Das BSI erhöht durch verschiedene Maßnahmen die Awareness für IT-Sicherheit in Politik, Wirtschaft, Wissenschaft und Zivilgesellschaft. Dafür stellt das BSI Hilfsmittel, z.B. in Form von Beratung, Informationen, dem Grundschutz-Kompendium oder technischen Richtlinien zur Verfügung.

Das BSI stellt Schulungsanbietern ein Curriculum zur Durchführung der IT-Grundschutz-Basisschulung und der IT-Grundschutz-Aufbauschulung zur Verfügung, um eine einheitliche und hohe Qualität in der Weiterbildung zum IT-Grundschutz sicherzustellen. Prüfungen zum IT-Grundschutz-Berater werden nur durch das BSI abgenommen. Schulungsanbieter müssen ggü. dem BSI eine Selbsterklärung abgeben und ihre Qualifikation für Schulungen nachweisen. Mit dem jährlich stattfindenden Deutschen IT-Sicherheits-kongress wendet sich das BSI an Experten aus Unternehmen und der Wissenschaft, um IT-Sicherheitsthemen zu diskutieren. Mit dem BSI-Symposium wendet sich das BSI an Partner aus Politik, Wirtschaft, Verwaltung und Gesellschaft, um sich zu Themen der Cyber- und IT-Sicherheit auszutauschen und Multiplikatoren zu gewinnen. Die Veranstaltungsreihe "BSI im Dialog" richtet sich an Anwender und Hersteller und fördert den direkten Austausch.

Konzeption und Vorgehensweisen

#Kryptographie #Quanten-Kryptographie & Post-Quanten-Kryptographie #Blockchain #Authentifizierung #Informationssicherheitsmanagement #Endgerätesicherheit #Identitätsmanagement #Berechtigungsmanagement #Compliance Management #Datenschutz #IT-Sicherheitsstandards

Das BSI gibt zu verschiedenen Themen aus dem Bereich Cybersicherheit Hilfestellungen, z.B. durch die Veröffentlichung von Leitfäden und praxisorientierten Hintergrundinformationen zu Vorgehensweisen, mit denen die Sicherheit in Institutionen geprüft und erhöht werden kann.

Das BSI ist bei der kontinuierlichen Bewertung und Fortentwicklung kryptografischer Verfahren tätig und formuliert regelmäßig Empfehlungen und Standards. Dabei stehen nicht nur kryptografische Verfahren im

Fokus, sondern auch deren praktische Umsetzung und Implementierung. Das BSI bereitet ebenfalls die Zukunftstechnologie Post-Quanten-Kryptographie vor und wird in den nächsten Jahren die Aktivitäten mitgestalten und begleiten.

Neben der Zertifizierung von IT-Produkten und IT-Systemen im Hinblick auf deren Sicherheitsfunktionalitäten bietet das BSI eine sogenannte Zertifizierung nach Technischen Richtlinien (TR) an, die vom BSI entwickelt und publiziert werden. Die Konformität eines IT-Produktes oder -Systems zu einer Technischen Richtlinie kann durch das BSI mit einem Zertifikat bestätigt werden.

Der vom BSI entwickelte und veröffentlichte IT-Grundschutz-Katalog ist eine bewährte Methodik, um das Niveau der Informationssicherheit in Behörden und Unternehmen jeder Größenordnung zu erhöhen. Die Angebote des IT-Grundschutzes gelten in Verwaltung und Wirtschaft als Maßstab, wenn es um die Absicherung von Informationen und den Aufbau eines Managementsystems für Informationssicherheit (ISMS) geht. Sie enthalten Empfehlungen zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen zu unterschiedlichen Aspekten der Informationssicherheit. Anwender aus Behörden und Unternehmen sowie Hersteller oder Dienstleister können mit den BSI-Standards ihre Geschäftsprozesse und Daten sicherer gestalten. Um die Umsetzung der BSI-Empfehlungen zu fördern, bietet das BSI entsprechende Schulungen und Veranstaltungen zu Cyber- und IT-Sicherheitsthemen an.

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen

Mit der 2012 gegründeten ACS verfolgt das BSI das Ziel, die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen zu stärken. Die ACS und ihre Partner stellen ein stetig wachsendes Repertoire an Informationen zur Cyber-Sicherheitslage sowie Handlungsempfehlungen zur Verfügung.

Detektion und Reaktion

#Behandlung von Sicherheitsvorfällen & IT-Forensik

Das BSI betreibt das CERT-Bund (Computer Emergency Response Team für Bundesbehörden), das die zentrale Anlaufstelle für präventive und reaktive Maßnahmen bei sicherheitsrelevanten Vorfällen in Computer-Systemen ist.

Mit dem Bürger-CERT stellt das BSI zudem umfangreiche Informationen zu aktuellen Attacken und Sicherheitslücken für Privatpersonen zur Verfügung.

Der vom BSI veröffentlichte Leitfaden IT-Forensik richtet sich an Betreiber von IT-Systemen, Administratoren und Sicherheitsverantwortliche. Er beschreibt für diese Zielgruppen IT-Forensik als eine methodisch vorgenommene Datenanalyse auf Datenträgern und Computernetzen zur Aufklärung von IT-Vorfällen.

Infrastrukturelle Sicherheitsaspekte

#Betriebs- und Steuerungstechnik #SPS & ICS #physische IT-Sicherheit

Das BSI hat nach BSI-Gesetz/KritisV weitreichende Rechte und Pflichten zum Schutz Kritischer Infrastrukturen. Darüber hinaus engagiert sich das BSI in allen Bereichen der IT-Sicherheit von Industrieanlagen, zu denen auch Kritische Infrastrukturen zählen.

Mit dem ICS Security Kompendium veröffentlicht das BSI ein Grundlagenwerk für die IT-Sicherheit in industriellen Steuerungsanlagen. Es werden allgemeinen Grundlagen der Automation erläutert, sowie auf Besonderheiten und Standards in diesem Bereich aufmerksam gemacht. Das Kompendium enthält eine Sammlung von Maßnahmen und einer Vorgehensweise, um die Umsetzung zu prüfen.

Netze und Kommunikation

#Netzarchitektur und -design #Netzkomponenten #Netzmanagement #Funknetze

Mit den BSI-Standards zur Internet-Sicherheit (ISi-Reihe) werden Behörden und Unternehmen umfassende Informationen zur Verfügung gestellt, damit diese ihre Internet-Aktivitäten möglichst eigenständig sicher neu aufbauen, erweitern oder anpassen können. Die ISi-Reihe behandelt die Themen Netzdesign, Netzkomponenten, Dienste und Anwendungen den Datenzugriff und -transport über das Netz. Zudem ist das BSI gemäß § 109 TKG gemeinsam mit der Bundesnetzagentur und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit für die Sicherheitsanforderungen für den Betrieb von Telekommunikations- und Datenverarbeitungssystemen zuständig. Der hierfür erstellte Sicherheitskatalog wird nach öffentlicher Konsultation veröffentlicht.

Zielgruppe

Zivilgesellschaft

- Bürger

Das BSI stellt mit seinem Angebot "BSI für Bürger" der Gesellschaft ausführliche Informationen zu aktuellen Cyber-Risiken, Handlungsempfehlungen, Checklisten und Tipps zur Verfügung.

Wissenschaft

- Bildungseinrichtung
- Forschungseinrichtung

Die Wissenschaft wird bspw. mit dem Dialog zur Schaffung eines sicheren Rechtsrahmen für IT-Sicherheitsforschung, einer Sicherheitskonferenz oder der Forschungskoordinierung adressiert.

Wirtschaft

- Bildungseinrichtung
- Forschungseinrichtung

Die Wissenschaft wird bspw. mit dem Dialog zur Schaffung eines sicheren Rechtsrahmen für IT-Sicherheitsforschung, einer Sicherheitskonferenz oder der Forschungskoordinierung adressiert.

Staat

- Bund
- Land

Das BSI unterstützt Behörden von Bund und Ländern in Fragen der IT-Sicherheit.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Beratung
- Prüfung/Audits/Zertifizierung/Standardisierung
- Sonstige Dienstleistung

Unternehmen und Behörden, die ihre erfolgreichen Aktivitäten zur Erhöhung der Informationssicherheit nachweisen möchten, bietet das BSI Möglichkeiten der Testierung bzw. Zertifizierung an.
Das BSI als die nationale Cyber-Sicherheitsbehörde erarbeitet Mindeststandards für die Sicherheit der Informationstechnik des Bundes auf der Grundlage des § 8 Abs. 1 BSIG. Als gesetzliche Vorgabe definieren diese Mindeststandards ein konkretes Mindestniveau für die Informationssicherheit.
Die Sicherheitsberatung ist die zentrale Anlaufstelle des BSI für alle Anfragen zur Beratung und Unterstützung bei Fragen zur Informationssicherheit und zum materiellen sowie IT-Geheimschutz. Die Dienstleistungen der Sicherheitsberatung richten sich primär an Dienststellen der öffentlichen Verwaltung.

Information

- Informationsaufbereitung
- Newsletter
- Studie
- Sonstiges Informationsangebot

Das BSI bietet mit seinen publizierten BSI-Standards Methoden und Vorgehensweisen zu verschiedenen Themen aus dem Bereich der Informationssicherheit. Darin werden allgemeine Anforderungen definiert und Methoden und Vorgehensweisen an die Hand gegeben, um eine Absicherung der IT in Einrichtungen und Unternehmen zu realisieren. Mit dem IT-Grundschutz-Kompendium stellt das BSI ein Arbeitswerkzeug zur Verfügung, in dem Gefährdungen, Sicherheitsanforderungen und Umsetzungsmethoden ausführlich erläutert werden. Des Weiteren bietet das BSI Studien, Lageberichte und technische Richtlinien an, um über IT-Sicherheit zu informieren und Umsetzungshilfen zu geben.
Speziell für Privatpersonen bietet das BSI über das Angebot "BSI für Bürger" umfangreiche Informationen zu allen aktuellen Cyber-Risiken sowie Handlungsempfehlungen und Tipps an, ebenfalls in Form des Bürger-CERT-Newsletters.

Regulierung

- Beratung
- Prüfung/Audits/Zertifizierung/Standardisierung
- Sonstige Dienstleistung

Das BSI ist als Verwaltungs- und Regulierungsbehörde für den Bereich IT-Sicherheit zuständig.
Für den Schutz Kritischer Infrastrukturen bestehen hierzu weitreichende Zuständigkeiten und Pflichten im Zusammenhang mit dem BSI-Gesetz und der BSI-KritisV. Bspw. ist das BSI die zentrale Meldestelle in Angelegenheiten der IT-Sicherheit für Betreiber Kritischer Infrastrukturen sowie Digitaler Dienste nach der EU-NIS Richtlinie.

Deutsche Akkreditierungsstelle GmbH (DAkkS)

Beitrag zur Cybersicherheit

Die DAkkS vereint im Sektorkomitee Informationstechnik / Informationssicherheit (SK IT-IS) seine Aktivitäten im Bereich der IT-Sicherheit. Insbesondere der Unterausschuss Cyber- und Informationssicherheit akkreditiert bspw. Zertifizierungs- und Inspektionsstellen aus dem Bereich der Cybersicherheit. Durch internationale Abkommen werden durch die DAkkS akkreditierte Bewertungsleistungen sogenannter Konformitätsbewertungsstellen auch in vielen weiteren Ländern anerkannt.

Kontakt:

Spittelmarkt 10

10117 Berlin

dakks.de

Staatlicher Akteur

Thematische Schwerpunkte (Auszug)

Konzeption und Vorgehensweisen

#IT-Sicherheitsstandards

Durch ihre Position als nationale Akkreditierungsstelle akkreditiert die DAkkS gemäß internationaler Normen und bewertet Konformitätsbewertungsstellen wie Laboratorien, Zertifizierungs- und Inspektionsstellen, Anbieter von Eignungsprüfungen und Referenzmaterialhersteller. Eine Konformitätsbewertungsstelle kann durch das DAkkS akkreditiert werden, sofern diese die jeweilig entsprechenden internationalen Normen erfüllt.

Zielgruppe

Zivilgesellschaft

Wissenschaft

Wirtschaft

Staat

Das DAkkS akkreditiert Konformitätsbewertungsstellen, wodurch diese wiederum ihre Glaubwürdigkeit gegenüber relevanten Zielgruppen signalisieren können.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Prüfung/Audits/Zertifizierung/Standardisierung

Durch die besondere Dynamik im Bereich der Cyberbedrohungen bestehen besondere Anforderungen an eine ausreichende und angemessene Cybersicherheit. Mittels Akkreditierungen von Bewertungsstellen kann die DAkkS international anerkannte Standards auszeichnen und somit Vertrauen schaffen.

digital@bw

Beitrag zur Cybersicherheit

Mit der Digitalisierungsstrategie digital@bw hat die Landesregierung Baden-Württemberg ihre Vision einer der digitalen Zukunft für das Land vorgelegt. Cybersicherheit ist ein zentrales Querschnittsthema der Strategie. Datensicherheit, Datenschutz und Verbraucherschutz im digitalen Zeitalter stehen in diesem Bereich im Fokus. Die Strategie bündelt verschiedene Projekte, die den Cyberraum für Wirtschaft, Wissenschaft, Verwaltung und Bürgerinnen und Bürgerinnen und Bürgerinnen und Bürger Baden-Württembergs sicherer machen. So bspw. die Einrichtung der Cyberwehr BW (siehe hierzu den Steckbrief) oder die Cybersicherheitsagentur Baden-Württemberg.

Ansprechpartner:

Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg,

Referat 72 – Digitalisierungsstrategie und Cybersicherheit

Willy-Brandt-Str. 41

70173 Stuttgart

digital-bw.de

Staatliche Initiative

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Durch ressortübergreifende Zusammenarbeit und Kooperation mit Partnern aus Wirtschaft und Forschung schaffen die Akteure im Rahmen mehrerer Projekte neue Netzwerke und verstärken die Vernetzung im Land.

Bildung und Awareness

#Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft #Awareness in der Politik

Durch eine Informationskampagne, die auch das Thema Cybersicherheit beinhaltet, über eine zentrale Informationsplattform sowie durch projektbezogene Informationsmaßnahmen schaffen die Akteure größeres Bewusstsein für das Thema in allen Gesellschaftsbereichen.

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen

Die Cyberwehr BW (siehe hierzu den Steckbrief) unterstützt KMU im Falle eines IT-Sicherheitsvorfalls.

Vernetzung von Systemen, IoT

#Künstliche Intelligenz #Smart Home #Autonomes Fahren #Fahrassistenzsysteme

Das Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg hat im Rahmen der Digitalisierungsstrategie digital@bw unter anderem ein Forschungsprojekt im Bereich IT-Sicherheit und Autonomes Fahren in Auftrag gegeben. Ziel des Projektes ist die Befähigung der Sicherheitsbehörden, die von einer Automotive IT ausgehenden Risiken, in ihrer Aufgabe zur Gewährleistung der öffentlichen Sicherheit zu beherrschen. Ein Schwerpunkt stellt dabei die Analyse und Identifikation neuer Bedrohungen durch das vernetzte und autonome Fahren dar.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger
- Angestellte

Mit verschiedenen Informationsmitteln verankern die Akteure das Thema Cybersicherheit allgemein stärker im Bewusstsein der Bürgerinnen und Bürgerinnen und Bürgerinnen und Bürger und vermitteln grundlegendes Wissen.

Wissenschaft

- Forschungseinrichtung

Die Cybersicherheitsagentur Baden-Württemberg vernetzt künftig alle Akteure der Cybersicherheit. Zu ihren Aufgaben wird außerdem gehören, Wissenschaft, Bürgerinnen und Bürgerinnen und Bürgerinnen und Bürger, Wirtschaft und Verwaltung zum Thema Cybersicherheit zu sensibilisieren und mit Beratung konkrete Hilfeleistung zu bieten.

Wirtschaft

Auch der Schutz der Unternehmen im Land Baden-Württemberg im Fokus von digital@bw. Die Cyberwehr BW ist Teil der künftigen Cybersicherheitsarchitektur des Landes Baden-Württemberg. Das Ministerium für Inneres, Digitalisierung und Migration fördert das erfolgreiche Projekt auch in der jetzt anlaufenden zweiten Förderphase.

Staat

- Land
- Behörde / Verwaltung
- Einrichtung
- Ministerium

Die Cybersicherheitsagentur Baden-Württemberg vernetzt künftig alle Akteure der Cybersicherheit. Zu ihren Aufgaben wird außerdem gehören, Bürgerinnen und Bürgerinnen und Bürgerinnen und Bürger, Wirtschaft, Wissenschaft und Verwaltung zum Thema Cybersicherheit zu sensibilisieren und mit Beratung konkrete Hilfeleistung zu bieten. Die Cybersicherheitsagentur Baden-Württemberg agiert über die Grenzen des Landes hinaus als zentraler Ansprechpartner für Akteure der Cybersicherheit im Bund, in der EU sowie international. Ziel der optimierten Cybersicherheitsarchitektur ist der Schutz der IT des Landes durch die strategische Steuerung und Überwachung landesweiter Sicherheitsmaßnahmen.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Beratung

Durch Beratungsprojekte wie bspw. die Cyberwehr BW oder das IT Security LAB (ein Programm zur Innovations- und Gründerförderung) bekommen Bürgerinnen und Bürgerinnen und Bürgerinnen und Bürgern sowie Unternehmen des Landes gezielt Unterstützung, außerdem werden Start-Ups im Bereich Cybersicherheit gefördert.

Information

- Informationsaufbereitung
- Öffentlichkeitsarbeit

Im Rahmen verschiedener Projekte stellen die Akteure Informationen sowohl für die Öffentlichkeit allgemein als auch für spezifische Zielgruppen bereit. Die Jahresfachveranstaltung "CyberSicherheitsForum" findet im Jahr 2021 bereits zum dritten Mal statt und bildet eine internationale Plattform für Expertinnen und Experten im Bereich Cybersicherheit. In einem Plenum und verschiedenen Fachforen identifizieren die ca. 500 Gäste aktuelle Trends und erarbeiten Lösungen auf drängende Fragen zum Thema Cybersicherheit.

European Cyber Security Month (ECSM)

Beitrag zur Cybersicherheit

Der ECSM ist eine jährliche Sensibilisierungskampagne der EU, die jeweils im Oktober in ganz Europa stattfindet. Federführend für den ECSM ist die europäische Cybersicherheitsagentur ENISA. Die deutsche Koordinierungsstelle ist das BSI. Ziel ist es, das Bewusstsein für Cybersicherheitsbedrohungen zu schärfen und die Bedeutung der Cybersicherheit bei Bürgerinnen und Bürgern und Organisationen hervorzuheben. Im Rahmen des ECSM werden bspw. Social-Media-Aktionen, Beratungsbusse, Workshops, Vorträge, Leitfäden oder Mitmachaktionen angeboten. Außerdem können eigene Aktionen im Rahmen des ECSM angeboten werden.

Ansprechpartner:

BSI

Godesberger Allee 185-189

53175 Bonn

cybersecuritymonth.eu
bsi.bund.de/ecsm

Staatliche Initiative

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Die öffentlichkeitswirksame Behandlung des Themas Cybersicherheit dient auch der Vernetzung aller Teilnehmer und Interessengruppen. Bei allen Social-Media-Aktionen wird das Hashtag #ecsm zur Verlinkung genutzt.

Bildung und Awareness

#Awareness in der Politik #Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft

Hauptthema des ECSM ist die Stärkung des Bewusstseins zum sicheren Umgang mit IT in allen Gesellschaftsgruppen. Hierfür finden während des Aktionsmonats europaweit verschiedenste Veranstaltungen statt und es werden zahlreiche Informationen, Hilfestellungen und Praxisbeispiele in diversen Formaten angeboten.

Zielgruppe

Zivilgesellschaft

Wissenschaft

Wirtschaft

Staat

Die Aktionen des ECSM richten sich gesamtgesellschaftlich an alle Interessierten.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Journalismus
- Öffentlichkeitsarbeit
- Sonstiges Informationsangebot

Das Angebot von Informationen zur Sensibilisierung für das Thema Cybersicherheit während des ECSM ist sehr breit gefächert. Es reicht von Mitmachaktionen über Pressearbeit und Erklärvideos bis hin zu öffentlichen Vorträgen und Informationstouren auf Marktplätzen. Sämtliche Aktionen werden auf der Webseite des ECSM veröffentlicht.

Förderprogramm für Innovative Hafentechnologien (IHATEC)

Beitrag zur Cybersicherheit

IHATEC ist ein Förderprogramm des BMVI zur Stärkung der Innovationskraft der Hafenwirtschaft und hat u.a. zum Ziel, die digitalen Infrastrukturen und die IT-Sicherheit deutscher Häfen zu verbessern. Mithilfe der Fördermittel werden auch verschiedene Projekte zur IT-Sicherheit finanziert, welche sich mit der Erkennung und Verhinderung von Cyberattacken befassen.

Projektträger:

TÜV Rheinland Consulting GmbH

Am Grauen Stein

51105 Köln

innovativehafentechnologien.de

Staatliche Initiative

Thematische Schwerpunkte (Auszug)

Konzeption und Vorgehensweisen

#Endgerätesicherheit #IT-Sicherheitsstandards

Die durch IHATEC geförderten Projekte dienen der Erforschung und Entwicklung von innovativen Konzepten und Anwendungen sowie Erarbeitung von Standards im Bereich der Cybersicherheit für Häfen, Transportketten und die gesamte maritime Branche.

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen #Monitoring

Einzelne Projekte von IHATEC beschäftigen sich mit dem Thema der Verhinderung von Cyberattacken auf deutsche Häfen. So auch das Forschungsprojekt SecPro-Port, welches mit dem Ansatz skalierbarer Sicherheitsarchitekturen auf Basis einer Prozess- und Bedrohungsanalyse arbeitet, damit die Produktivität des Gesamtsystems auch bei Angriffen gewahrt bleibt. Die Forschungsergebnisse sollen die Basis eines künftigen Informationssicherheitsstandards für Häfen bilden.

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen

Das durch IHATEC geförderte Forschungsprojekt AUTOSEC widmet sich der Erhöhung der Sicherheit im digitalisierten Container-Terminalprozess sowie der Entwicklung von Schutzmaßnahmen zur Erkennung und Verhinderung von Cyberangriffen auf Häfen und Logistikketten. Hierzu wird ein Methoden- und Werkzeugset entwickelt, welches bei Konzeption, Einführung und Betrieb sicherer Automatisierungsvorhaben skalierbar unterstützt. Eine Evaluierung von Prototypen findet in Wilhelmshaven und Magdeburg statt. Mit der Erkennung und Abwehr von Cyberattacken auf die Hafenwirtschaft befasst sich ebenfalls das Projekt HITS-Moni, welches zur Verknüpfung verschiedener, an hafenspezifische Schwachstellen angepasste IT-Tools forscht.

Infrastrukturelle Sicherheitsaspekte

#RZ-Infrastruktur

Die Verbesserung der digitalen Infrastruktur im Rahmen des Projektes SecurePort soll zum einen die IT-Sicherheit im Hafenbetrieb und der dazugehörigen Logistikketten verbessern, zum anderen aber auch allgemein den Digitalisierungsgrad in diesem Umfeld erhöhen.

Zielgruppe

Wissenschaft

- Forschungseinrichtung

Die Ausschreibungen von IHATEC richten sich an Forschungs- und Wissenseinrichtungen und außeruniversitäre Forschungseinrichtungen.

Wirtschaft

- Information und Kommunikation
- Maritimes Gewerbe
- Beratung
- Verkehr / Infrastruktur

Die Förderrichtlinie IHATEC richtet sich vorrangig an Unternehmen der Hafenwirtschaft in Verbindung mit industriellen Entwicklungspartnern.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Beratung
- Entwicklung
- Konzept

IHATEC dient der Unterstützung von Forschungs- und Entwicklungsprojekten, die zur Entwicklung oder Anpassung innovativer Technologien in den deutschen See- und Binnenhäfen beitragen. Hierbei spielt die Digitalisierung und damit auch die Cybersecurity, gerade vor dem Hintergrund kritischer Infrastrukturen, einen wesentlichen Beitrag. Im Rahmen des Programms werden daher auch verschiedene Projekte im Bereich IT-Sicherheit umgesetzt.

Forschungsrahmenprogramm „Selbstbestimmt und sicher in der digitalen Welt“

Beitrag zur Cybersicherheit

Das Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt“ bündelt ressortübergreifend die Aktivitäten zur Cybersicherheitsforschung und fördert diese an Hochschulen und Forschungseinrichtungen sowie in Unternehmen mit dem Ziel der Entwicklung innovativer Sicherheitstechnologien für Wirtschaft und Zivilgesellschaft sowie der Etablierung der Bundesrepublik Deutschland als Leitanbieter für IT-Sicherheitslösungen. Im Rahmen des Forschungsrahmenprogrammes wurden die Forschungsschwerpunkte vor allem auf die Nutzung von Schlüsseltechnologien wie Künstliche Intelligenz und Quantencomputer, sichere und vertrauenswürdige IKT-Systeme, IT-Sicherheit in spezifischen Anwendungsfeldern wie Medizin, vernetzten Produktionsanlagen oder Kritischen Infrastrukturen, Datenschutz und sichere Hardware gelegt. Mit der Koordination des Forschungsrahmenprogramms ist das BMBF betraut.

Ansprechpartner:

BMBF

Referat Kommunikationssicherheit; IT-Sicherheit

53170 Bonn

forschung-it-sicherheit-kommunikationssysteme.de

Staatliche Initiative

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Im Rahmen des Forschungsprogrammes werden ATHENE in Darmstadt, CISPA in Saarbrücken sowie KASTEL in Karlsruhe als Kompetenzzentren der IT-Sicherheitsforschung gefördert, welche als Knotenpunkte für wissenschaftliche Vernetzung agieren. Darüber hinaus werden bspw. auch Projekte der internationalen Zusammenarbeit gefördert, um die internationale Vernetzung und den wissenschaftlichen Austausch voranzutreiben.

Konzeption und Vorgehensweisen

#Quanten-Kryptographie & Post-Quanten-Kryptographie #Endgerätesicherheit #Identitätsmanagement #Berechtigungsmanagement #Datenschutz

Gefördert werden Projekte zur Erforschung von Quantenkryptographie, Quantennetzwerken und Quantenkommunikation, wie bspw. die Initiative QuNET zum Aufbau eines hochsicheren Quantennetzwerk zur Kommunikation zwischen Bundesbehörden. Das Forschungsrahmenprogramm deckt eine Vielzahl an Technologien wie bspw. Blockchain in der IT-Sicherheit neben Themen wie Endgerätesicherheit und Datenschutz ab.

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen

Die vom Forschungsrahmenprogramm geförderten Forschungsprojekte befassen sich auch mit Bedrohungen und Angriffen im und aus dem Cyberspace sowie dem Schutz und der Abwehr derselben.

Netze und Kommunikation

#Netzarchitektur und -design #Netzkomponenten

Sichere vernetze Datenzentren über Landesgrenzen hinweg ist einer der Schwerpunkte der Förderung durch das Forschungsrahmenprogramm. Hierbei arbeiten Partner aus Deutschland, Frankreich, Finnland und Schweden im Projekt SENDATE mit dem Ziel zusammen, eine sichere Netzinfrastruktur zu schaffen, die zukünftige Anforderungen an Kapazität, Latenz und Energieeffizienz erfüllt.

Vernetzung von Systemen, IoT

Zur Verbesserung der IT-Sicherheit von vernetzen Produktionsanlagen existieren diverse geförderte Forschungsprojekte. Eines davon ist das Nationale Referenzprojekt zur IT-Sicherheit in der Industrie 4.0, kurz IUNO. Hierin forschen 14 deutsche Industrieunternehmen gemeinsam mit sieben Universitäten und Forschungseinrichtungen mit dem Ziel der Reduktion von Angriffspunkten. Dazu werden konkrete Anwendungsschwerpunkte beleuchtet, Demonstratoren entwickelt und Methoden erforscht, welche sichere Daten, Dienste und Prozesse bei übergreifender Vernetzung von Industrieanlagen gewährleisten.

Zielgruppe

Wissenschaft

- Forschungseinrichtung

Wirtschaft

Adressaten des Forschungsrahmenprogrammes sind primär Universitäten und Forschungseinrichtungen, aber auch Forschungskooperationen aus Wissenschaft und Wirtschaft.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Sonstige Dienstleistung

Das Forschungsrahmenprogramm finanziert Forschungs- und Entwicklungsprojekte innerhalb der Domäne der Cybersicherheit.

Internet-ABC e.V.

Beitrag zur Cybersicherheit

Kontakt:

Internet-ABC e.V.

c/o Landesanstalt für Medien NRW

Zollhof 2

40221 Düsseldorf

internet-abc.de

Staatliche Initiative

Der gemeinnützige Verein Internet-ABC e.V. bietet mit dem Onlineangebot www.internet-abc.de Hilfestellung und Informationen zum sicheren Umgang mit dem Netz. Das Angebot richtet sich an Kinder im Alter von 5 bis 12 Jahren, aber auch an Eltern und Lehrkräfte. Im Kinderbereich lernen die Kinder Schritt für Schritt die Grundlagen für einen sicheren Umgang mit dem Internet. Herzstück des Internet-ABC sind die interaktiven Lernmodule für die Kinder der Klassen 3-6. Auf verständliche, kindgerechte Weise werden hier Themen wie Cybermobbing, Datenschutz oder Computerviren erklärt. Daneben bietet der Kinderbereich noch weitere Möglichkeiten, das Internet zu erkunden. So können sie sich an Foren beteiligen, eine eigene Umfrage erstellen oder in Angeboten wie dem Baukasten kreativ werden. Alle Angebote werden dabei von einer Redaktion betreut. Eltern und Lehrkräfte erhalten auf eigenen Seiten Tipps und Hilfestellungen, wie sie Kinder dieser Altersgruppe einen kompetenten Umgang mit dem Internet vermitteln können. Das Internet-ABC unterstützt Eltern bei ihren alltäglichen Fragen rund um die Mediennutzung ihrer Kinder und bietet Lehrkräften umfangreiche Unterrichtsmaterialien zum Einsatz in der Grundschule, aber auch für die Klassen 5+6 an. Seit 2019 haben Lehrkräfte auch die Möglichkeit, erstmals auch mit noch leseunkundigen Kindern der Klassen 1+2 anhand eines "Mitmach-Hefts" einen ersten Zugang zu den Themen Medien und Internet zu schaffen. Das Internet-ABC wird von den deutschen Landesmedienanstalten betrieben, die sich in dem gleichnamigen Verein zusammengeschlossen haben. Das Lernangebot ist sicher, werbefrei und nicht kommerziell. Sämtliche Inhalte sowie die analogen Begleit- bzw. Unterrichtsmaterialien können kostenlos genutzt bzw. bezogen werden. Seit April 2020 wird zudem auf das Setzen von Cookies verzichtet.

Thematische Schwerpunkte (Auszug)

Bildung und Awareness

#Awareness in der Zivilgesellschaft #Schulisches Bildungsangebot #Sonstiges Bildungsangebot

Der Internet-ABC e.V. bietet Kindern einen altersgerechten Zugang zu allen Themen rund um das Internet. Auf diese Weise werden auch Themen wie bspw. Cybermobbing oder Datenschutz behandelt, sodass Kinder bereits frühzeitig ein Bewusstsein dafür entwickeln. Die Inhalte werden auf eine spielerische Weise vermittelt, um der Zielgruppe gerecht zu werden. Darüber hinaus werden auch Informationen für Eltern und Lehrkräfte bereitgestellt, die diesen im Umgang mit den Kindern zum Thema Internet helfen sollen.

Zielgruppe

Zivilgesellschaft

- Kinder und Heranwachsende
- Familien

Das Angebot des Internet-ABC ist auf Kinder im Alter von 5 bis 12 Jahren sowie Eltern und Lehrkräfte ausgerichtet.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Lernprogramm
- Newsletter

Das Informationsangebot des Internet-ABC e.V. besteht aus Lernmodulen zu verschiedenen Themen des Internets, darunter Cybermobbing, Datenschutz und Computerviren, umfasst aber auch Beiträge zu anderen aktuellen medien- bzw. internetrelevanten Themen. Zusätzlich werden für die Zielgruppen Eltern und Lehrkräfte Erklärungen, Tipps und Empfehlungen sowie themenspezifische Artikel bereitgestellt.

IT-Sicherheit in der Wirtschaft

Beitrag zur Cybersicherheit

Mit der Initiative "IT-Sicherheit in der Wirtschaft" unterstützt das BMWi Unternehmen darin, die eigene IT-Sicherheit zu verbessern. Insbesondere KMU) sollen für das Thema sensibilisiert und durch konkrete Hilfsangebote (z. B. durch Webseitenchecks, Handlungsleitfäden, Schulungs- und Lehrmaterialien) unterstützt werden. Des Weiteren wurde im Rahmen der Initiative die Transferstelle IT-Sicherheit im Mittelstand (TISiM – siehe hierzu den Steckbrief) eingerichtet, deren Hauptaufgaben der Wissens- und Technologietransfer sowie die Adressierung von zielgruppengerechten Angeboten und Öffentlichkeitsmaßnahmen ist. Weiterhin fördert die Initiative Einzel- und Verbundprojekte, die aktiv zur Sensibilisierung und Unterstützung von KMU und Handwerk beim Thema IT-Sicherheit beitragen und Unterstützungsleistungen zum sicheren Einsatz digitalisierter Prozesse und Geschäftsmodelle zielgruppengerecht und praxisnah aufbereiten.

Ansprechpartner:

BMWi

Scharnhornstr. 34-37

10115 Berlin

it-sicherheit-in-der-wirtschaft.de

Staatliche Initiative

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

An der Initiative sind Experten aus Wirtschaft, Wissenschaft und Verwaltung beteiligt, die im Rahmen der Initiative beraten und Unterstützung leisten.

Bildung und Awareness

#Awareness in der Wirtschaft

Die Initiative bietet Awareness-Kampagnen für KMU der Wirtschaft an.

Konzeption und Vorgehensweisen

#Informationssicherheitsmanagement #Endgerätesicherheit #Datenschutz

Das Aufzeigen von technischen Möglichkeiten und Prozessen, um dem Datenschutz Rechnung zu tragen, gehört zu den Themenfeldern der Initiative. Sie widmet sich auch dem Thema, wie Unternehmen mobiles Arbeiten sicher gestalten können. Tools und Informationen der Initiative unterstützen KMU, ein IT-Sicherheitsmanagement aufzubauen.

Betriebsbezogene Sicherheitsaspekte

#Cloudsicherheit

Die Initiative klärt über eine sichere Cloudnutzung und die Wahl seriöser Cloud-Anbieter auf.

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen
#Behandlung von Sicherheitsvorfällen & IT-Forensik

Die Initiative bietet Online-Tools an, um den Webauftritt des Unternehmens auf Schadprogramme prüfen zu lassen, und gibt Anleitungen, wie Malware entfernt werden kann (sog. Webseiten-Check).

Zielgruppe

Wirtschaft

Die Initiative spricht hauptsächlich KMU branchenübergreifend an.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Newsletter
- Sonstiges Informationsangebot

Die Initiative stellt Unternehmen Ratgeber und Tools zum Themenbereich IT-Sicherheit zur Verfügung. Der Transfer von herstellerneutralen Initiativen und konkrete Hilfsangeboten sowie passgenauen Aktionsplänen erfolgt über die TISiM (www.tisim.de) bzw. über regionale Anlaufstellen, sog. Schaufenster, bei IHKn und Multiplikatoren.

EU-Initiative klicksafe - Awareness Centre Germany

Beitrag zur Cybersicherheit

Die von der EU geförderte Initiative klicksafe verfolgt das Ziel, Internetnutzern die kompetente und kritische Nutzung von Internet und Neuen Medien zu vermitteln und ein Bewusstsein für die Chancen und Gefahren dieser Angebote zu verschaffen. Die EU-Initiative klicksafe ist das nationale Awareness Centre für Deutschland, und koordiniert das nationale Safer Internet Centre zu dem die Hotlines (Internetbeschwerdestellen) von jugendschutz.net, eco und FSM sowie die Helpline NgK-NummergegenKummer gehören. Safer Internet Centre gibt es in 27 europäischen Ländern. Sie sind organisiert in den Netzwerken INSAFE und INHOPE. Gemeinsam setzen sie die Better Internet for Kids Strategie der Europäischen Union in den Nationalstaaten um.

Ansprechpartner:

Medienanstalt Rheinland-Pfalz,
Team Medienkompetenz

Turmstr. 10

67059 Ludwigshafen am Rhein

klicksafe.de

Staatliche Initiative

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Die Vernetzung unterschiedlicher Institutionen und Akteure aus den Bereichen Internet, Medienkompetenz und -bildung sowie Jugendschutz ist ein Schwerpunkt der Arbeit von klicksafe. So werden aktuelle Themen zur Internetsicherheit diskutiert, Handlungsbedarfe festgestellt oder gemeinsame Forderungen und Maßstäbe formuliert. Kooperationspartner aus Politik, Wirtschaft, Gesellschaft und dem Bildungsbereich arbeiten in der Initiative klicksafe zusammen.

Bildung und Awareness

#Awareness in der Zivilgesellschaft

Klicksafe ist eine Sensibilisierungskampagne zur Förderung der Medienkompetenz im Umgang mit dem Internet und neuen Medien im Auftrag der Europäischen Kommission. Im Fokus steht das Ziel, die Zivilgesellschaft über Cyberthemen aufzuklären.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger
- Kinder und Heranwachsende
- Familien
- NGO

Durch das Projekt sollen Kinder, Jugendliche und Eltern angesprochen werden.

Wissenschaft

- Bildungseinrichtung

Durch das Projekt sollen Lehrkräfte sowie Pädagoginnen und Pädagogen angesprochen werden.

Wirtschaft

Staat

Durch das Projekt sollen auch Unternehmen und Betreiber von Internetseiten und Social Media angesprochen werden. Außerdem findet eine Zusammenarbeit mit Länder- und Bundesministerien sowie Kooperationen mit Institutionen des Kinder- und Jugendschutzes und Institutionen der Medienbildung statt

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Ausbildung und Schulung
- Beratung
- Konzept
- Sonstige Dienstleistung

Klicksafe bietet Konzepte und Schulungen, um Kompetenzen im Umgang mit dem Internet zu erlangen. Dazu entwickelt klicksafe vielfältige digitale und Printmedien, um die Zielgruppen umfassend zu informieren. Außerdem übernimmt klicksafe die Koordination des Safer Internet Day - SID Deutschland.

Information

- Informationsaufbereitung
- Lernprogramm
- Newsletter
- Öffentlichkeitsarbeit
- Studie
- Sonstiges Informationsangebot

Klicksafe stellt für Schüler und Jugendliche, Eltern und Pädagogen themenbezogene und zielgruppenspezifische Materialien zur Verfügung, um Medienerziehung und -bildung zu leisten.

Kommunales IT-Sicherheitsbündnis Niedersachsen (Kitsin)

Beitrag zur Cybersicherheit

Die Initiative Kitsin ist ein Bündnis aus 50 Kommunen Niedersachsens, die über eine gemeinsame Plattform Wissen zu IT-Sicherheitsthemen teilen und gemeinsam Handlungsempfehlungen für ihren Wirkungsbereich erarbeiten.

Ansprechpartner:

Geschäftsstelle des Kitsin

Derzeit: Stadt Delmenhorst, IT-Service

Email: ges-chaeftsstelle@kitsin.de

Lange Str. 1a

27749 Delmenhorst

kitsin.de

Staatliche Initiative

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Die Initiative Kitsin dient der Vernetzung von Kommunen in Niedersachsen zu IT-Sicherheitsthemen. Kitsin arbeitet eng mit dem Niedersachsen-CERT (N-CERT), dem Computer-Emergency-Response-Team der niedersächsischen Landes- und Kommunalverwaltung zusammen.

Bildung und Awareness

#Awareness in der Politik #Berufliches Bildungsangebot

Kitsin baut für seine Mitglieder eine Wissensplattform auf, um Wissen gemeinsam zu erarbeiten, zu teilen und um Erfahrungen sowie Best Practices untereinander auszutauschen.

Zielgruppe

Staat

Das Bündnis Kitsin richtet sich an niedersächsische Kommunalverwaltungen.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

Das Bündnis bündelt das Notfallmanagement der teilnehmenden niedersächsischen Kommunen bei IT-Sicherheitsvorfällen. Es bietet allen Mitgliedern Unterstützung bei Sicherheitsvorfällen. Diese Unterstützung erfolgt auf freiwilliger Basis.

Information

- Sonstiges Informationsangebot

Das Bündnis tauscht sich im Mitgliederkreis zu IT-Sicherheitsthemen aus, berichtet über Erfahrungen und leitet daraus gemeinsame Handlungsempfehlungen ab. Neben der telefonischen und schriftlichen Kommunikation findet ein persönlicher Erfahrungsaustausch in Form von Jahrestagungen zu IT-Sicherheitsthemen statt.

Mittelstand-Digital

Beitrag zur Cybersicherheit

Mit dem Förderschwerpunkt "Mittelstand-Digital" unterstützt das BMWi den Mittelstand beim Einsatz von modernen Informations- und Kommunikationstechnologien, der Digitalisierung und Vernetzung sowie der Anwendung von Industrie 4.0. Dabei werden auch die Aspekte der IT-Sicherheit behandelt.

Ansprechpartner:

BMWi

Scharnhornstr. 34-37

10115 Berlin

mittelstand-digital.de

Staatliche Initiative

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Die Initiative initiiert und betreibt Mittelstand 4.0-Kompetenzzentren, die Unternehmer auf dem Weg der Digitalisierung informieren und konkret unterstützen. Über die Kompetenzzentren werden Unternehmen miteinander in Kontakt gebracht sowie Vernetzung und Austausch gefördert.

Bildung und Awareness

#Awareness in der Wirtschaft

Die Initiative stellt eine Plattform für KMU dar, um sich über Themen der IT-Sicherheit und Digitalisierung zu informieren.

Zielgruppe

Wirtschaft

Die Initiative dient branchenübergreifend KMU zur Information und Unterstützung.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Newsletter
- Sonstiges Informationsangebot

Die Initiative dient dem Austausch und der Information von Unternehmen über Themen der IT-Sicherheit und Digitalisierung.

Nationaler Pakt Cybersicherheit (NPCS)

Beitrag zur Cybersicherheit

Der NPCS ist ein Projekt unter Federführung des Bundesministeriums des Innern, für Bau und Heimat. Ziel des Nationalen Pakts Cybersicherheit ist es, die Gesellschaftsgruppen Staat, Wirtschaft, Wissenschaft und Zivilgesellschaft in gemeinsamer Verantwortung für die Sicherheit im Cyberraum zusammenzubringen, die Vernetzung bestehender Initiativen und Akteure in Deutschland zu fördern, herausragende Akteure der Cybersicherheitslandschaft in Deutschland zu identifizieren und die vertrauensvolle Zusammenarbeit der unterschiedlichen Akteure im Bereich der Cybersicherheit zu intensivieren. Der NPCS stellt hierbei einen Beitrag Deutschlands zum „Paris Call for Trust and Security in Cyberspace“ dar. Die öffentlichkeitswirksame Außenkommunikation für den NPCS nimmt eine Quadriga aus hochrangigen Vertretern der jeweiligen Gesellschaftsgruppen war .

Ansprechpartner:

BMI

Alt-Moabit 140

10557 Berlin

nationaler-pakt-cybersicherheit.de

Staatliche Initiative

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Im NPCS werden die zahlreichen bereits bestehenden Initiativen und Akteure, die einen Beitrag zur Erhöhung der Cybersicherheit in Deutschland leisten, identifiziert und ihre Vernetzung unterstützt. Hierzu werden auch besonders herausragende Beiträge ermittelt und Aspekte identifiziert, die in einer Umsetzungsphase des Nationalen Pakts Cybersicherheit für eine weitere Stärkung der Cybersicherheit in Deutschland in den jeweiligen Gesellschaftsgruppen zukünftig verstärkt angegangen werden können.

Bildung und Awareness

#Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft

Im Rahmen von unterschiedlichen Veranstaltungs- und Kommunikationsformaten trägt der NPCS zur Steigerung der Awareness für das Thema Cybersicherheit in den Gesellschaftsgruppen Staat, Wirtschaft, Wissenschaft und Zivilgesellschaft bei.

Zielgruppe

Zivilgesellschaft

Wissenschaft

Wirtschaft

Staat

Als gesamtgesellschaftliche Initiative richtet sich der NPCS gleichermaßen an Staat, Wirtschaft, Wissenschaft und Zivilgesellschaft.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Vernetzung

Bereits bestehende und neue Initiativen im Bereich der Cybersicherheit werden in der Vernetzung untereinander unterstützt. *

Information

Der NPCS bietet durch die Veröffentlichung des Online-Kompendiums einen strukturierten Überblick über die Cybersicherheitslandschaft in Deutschland. Hierbei werden sowohl bereits bestehende Stärken identifiziert und herausgehoben als auch Aspekte ermittelt, die für eine weitere Stärkung der Cybersicherheit in Deutschland verstärkt angegangen werden können.

RAG Cyber des VdRBw

Beitrag zur Cybersicherheit

Kontakt:

Zeppelinstr. 7A

53177 Bonn

reservistenverband.de/cyber/

Staatliche Initiative

Der Verband der Reservisten der Deutschen Bundeswehr e.V. (VdRBw) betreibt eine Reservistenarbeitsgemeinschaft (RAG) Cyber, die beim Aufbau einer Cyber-Reserve unterstützen soll. Ziel dieser Cyber-Reserve der Bundeswehr ist die Bündelung von Cyber- und IT-Kompetenzen zur personellen Unterstützung der Cyber-Community der Bundeswehr. Neben der Einbindung von Reservisten wird auch aktiv nach zivilen Experten und Freiwilligen gesucht, die bspw. Cyberangriffe für Übungszwecke simulieren, um so die nationale Sicherheit auch im Cyberraum sicherzustellen. Das Konzept der Cyber-Reserve soll ziviles IT-Fachwissen der Bundeswehr zugänglich machen. Die Cyber-Reserve steht daher aktiven Soldaten und Reservisten aber auch allen geeigneten Personen aus dem Cyberumfeld, die bisher keine Berührungspunkte mit der Bundeswehr hatten, offen.

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Ziel der Cyber-Reserve der Bundeswehr ist die Bündelung der Kompetenzen im Bereich Cybersicherheit, um so die Cybersicherheit Deutschlands zu unterstützen. Die Cyber-Reserve bildet sich aus Spezialisten aller Gesellschaftsgruppen, weshalb durch diesen Ansatz eine breit angelegte fachliche Vernetzung stattfinden kann. Der Wissenstransfer und der Aufbau von übergreifenden Fähigkeiten findet in gemeinsamen Übungen von Cyber-Spezialisten aus Behörden, Gesellschaft und Wirtschaft zur Cyber-Verteidigung statt. Um dem Stellenwert dieses Themas gerecht zu werden, hat der Verband sich im Jahr 2017 entschlossen, eigens einen Beauftragten Cyber des Präsidiums innerhalb der Verbandsarbeit zu institutionalisieren, welcher eine übergreifende Reservisten-Arbeitsgemeinschaft leitet.

Bildung und Awareness

#Schulung #Awareness in der Politik #Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft #Sonstiges Bildungsangebot

Der originäre Auftrag des Verbandes der Reservisten der Deutschen Bundeswehr e.V. sieht neben dessen Mittler- und Multiplikatorfunktion in der Gesellschaft auch explizit die Ausbildung und Inübunghaltung von Reservisten der Bundeswehr vor. Dies gilt neben den allgemein militärischen Themen auch für die Dimension Cyber- und Informationsraum. So unterstützen heute bereits Reservisten die aktive Truppe bei Ausbildungsthemen und bilden sich darüber hinaus in regionalen Arbeitsgemeinschaften gegenseitig fort. Im Zuge von sicherheitspolitischen Veranstaltungen wird versucht, Awareness innerhalb der Gesellschaft für dieses sicherheitsrelevante Thema zu schaffen und zu vertiefen. Der Kontakt zur Wirtschaft wird seitens des Verbandes gepflegt, weil sich aus diesem zusätzliche Reservisten generieren lassen. Dass deren Weiterbildung innerhalb der Bundeswehr auch für den zivilen Arbeitgeber einen Gewinn für das Unternehmen darstellt, gilt es in das Bewusstsein der Unternehmer zu rufen.

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen #Monitoring #IT-Administration

Die Cyber-Reserve soll die Schlagkraft und Abwehrfähigkeit der deutschen Streitkräfte im Cyber- und Informationsraum sowie die Fähigkeit der Bundeswehr, hybriden Bedrohungen im Rahmen der Landes- und Bündnisverteidigung zu begegnen, verbessern.

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen

Die Cyber-Reserve unterstützt die Bundeswehr in der Reaktion auf identifizierte Cyberangriffe, aber auch bei der Abwehr von Hass- und Propagandakampagnen im Cyberspace.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger

Den Begriff der Cyber-Reserve weiter auslegend (vgl. hierzu auch das Konzept der Cyber-Community der Bw) adressiert die RAG Cyber des VdRBw alle Interessierten zu diesem Thema und somit nicht nur beorderte und unbeorderte Reservisten. Die Bundeswehr geht hier einen neuen Weg im Rahmen ihres Anteils an der gesamtgesellschaftlichen Sicherheitsvorsorge, die auch alle Bürgerinnen und Bürger angeht.

Wissenschaft

Mit Forschungseinrichtungen, wie bspw. das FI CODE an der Universität der Bundeswehr in München, kooperiert die RAG Cyber des VdRBw.

Wirtschaft

Der Verband der Reservisten der Deutschen Bundeswehr e.V. richtet sein Angebot grundsätzlich an alle Arbeitgeber und Arbeitnehmer, die Reservisten beschäftigen oder aber potenziell geeignete Interessierte hierfür freistellen könnten.

Staat

- Bund

In der Cyber-Reserve können sich neben ehemaligen Berufssoldaten und Zeitsoldaten aus dem IT-Bereich auch Seiteneinsteiger aktiv engagieren. Spezialisten aus verschiedensten Bereichen, auch Führungskräfte einschlägiger Unternehmen oder Professoren sollen ihre Kompetenzen einbringen. Darüber hinaus werden auch Freiwillige gesucht, die sich im Rahmen eines ehrenamtlichen oder bürgerschaftlichen Engagements beteiligen.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Ausbildung und Schulung
- Beratung
- Konzept
- Prüfung/Audits/Zertifizierung/Standardisierung

Die Spezialisten der Cyber-Reserve sollen die Aufgabenwahrnehmung der gesamtstaatlichen Sicherheitsvorsorge unterstützen und sich bspw. in Projektarbeiten, Beratungsleistungen oder Vorträgen einbringen. Dies geschieht vornehmlich in Form von Beorderungen.

Information

- Öffentlichkeitsarbeit

Bekanntestes Printmedium des Verbandes ist die Zeitschrift loyal, in welcher immer wieder auch Fachbeiträge zu Cyber abgedruckt werden. Darüber hinaus existiert eine eigene Seite/Rubrik zum Thema Cyber auf der Webseite sowie den Social-Media-Kanälen des Verbandes. Zusätzlich werden Inhalte über unterschiedlichste Medien der Bundeswehr veröffentlicht. Außerdem wird die Plattform community.bundeswehr mit Cyber-Themen und Arbeitskreisen dort bedient.

Runder Tisch zur IT-Sicherheit für Verbraucher

Beitrag zur Cybersicherheit

Das BMJV und das BMI führen eine gemeinsame Dialogreihe in Form eines Runden Tischs zum Thema IT-Sicherheit für Verbraucher durch. Die Dialogveranstaltungen finden gemeinsam mit Vertreterinnen und Vertretern aus der Zivilgesellschaft, der Wissenschaft und der Wirtschaft statt. Ziel des gemeinsamen Austauschs ist das Aufzeigen von Potenzialen und Verbesserungsmöglichkeiten sowohl hinsichtlich technischer Schutzmaßnahmen als auch zur Verbrauchersensibilisierung.

Ansprechpartner:

BMI

Alt-Moabit 140

10557 Berlin

BMJV

Mohrenstr. 37

10117 Berlin

Staatliche Initiative

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Der Dialog des Runden Tischs zur IT-Sicherheit für Verbraucher dient dem Austausch der Ministerien (BMJV, BMI) mit der Zivilgesellschaft und der Wirtschaft und soll Verbesserungsmöglichkeiten für bestehende Maßnahmen im Bereich der IT-Sicherheit identifizieren. Zusätzlich sollen Anwendungshindernisse durch IT-Sicherheitsaspekte für Verbraucherinnen und Verbraucher reduziert werden.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger

Wissenschaft

Wirtschaft

Die Dialogreihe des Runden Tischs zur IT-Sicherheit für Verbraucher verfolgt die im Koalitionsvertrag verankerte Aufgabe, Bürgerinnen und Bürger und Kleinunternehmen zur Gefahrenabwehr im Bereich der Cybersicherheit geeignet zu sensibilisieren. Im Rahmen der Veranstaltung kommen Vertreter der Zivilgesellschaft, der Wissenschaft, der Wirtschaft sowie des BMI und des BMJV zusammen und diskutieren zu aktuellen Themen der Cybersicherheit wie bspw. die durch das BSI vorgestellten Mindestanforderungen zur IT-Sicherheit vernetzter Geräte, das Konzept eines IT-Sicherheitskennzeichen für internetfähige Verbraucherprodukte oder die Planung einer nationalen Informationskampagne zur IT-Sicherheit von BMI und BSI.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

Der Runde Tisch zur IT-Sicherheit für Verbraucher dient in erster Linie dem Austausch verschiedener Akteure aus Staat, Wirtschaft, Wissenschaft und Zivilgesellschaft, womit die Sicherheit der Bürgerinnen und Bürger im Netz verbessert werden soll. Im Rahmen der Dialogreihe sollen geeignete Schutz- und Sensibilisierungsangebote für die Verbraucherinnen und Verbraucher entwickelt werden.

StartUpSecure

Beitrag zur Cybersicherheit

StartUpSecure ist eine Initiative des BMBF zur Förderung von Startups in der IT-Sicherheit und Teil der Gründerinitiative "Mehr Chancen für Gründungen". Die Initiative dient der Einrichtung von Gründungsinkubatoren, die als Beratungszentren für Forscher mit Gründungsideen an verschiedenen Standorten vertreten sind. Außerdem werden Unternehmensgründungen im Bereich der IT-Sicherheit in verschiedenen Phasen unterstützt. Sowohl die Phase der Entwicklung als auch die konkrete Markteinführung von Produkten oder Dienstleistungen werden in zwei Abschnitten gefördert. Mit der Initiative will das BMBF den Wissenstransfer von der Forschung in die Wirtschaft unterstützen. Im Rahmen der Initiative wurden Gründungsinkubatoren bei ATHENE in Darmstadt, am CISPA in Saarbrücken, dem KASTEL in Karlsruhe sowie an der Ruhr-Universität Bochum eingerichtet.

Ansprechpartner:

BMBF

Heinemannstr. 2

53175 Bonn

forschung-it-sicherheit-kommunikationssysteme.de/foerderung/startup-secure

Staatliche Initiative

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Die Gründungsinkubatoren der Initiative unterstützen Gründer auch beim Aufbau von Unternehmenskontakten und professionellen Netzwerken.

Zielgruppe

Wissenschaft

Wirtschaft

StartUpSecure richtet sich an Gründer, die auf Basis innovativer Ideen aus der Forschung Unternehmen gründen möchten.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Beratung

Im Rahmen der Initiative werden Gründungsinkubatoren eingerichtet, die als Beratungszentren für Gründungsideen fungieren. Außerdem werden Gründungen im Bereich der IT-Sicherheit bei der Darstellung der technischen Umsetzbarkeit, der Erarbeitung eines Businessplans oder der Markteinführung unterstützt.

Surfen mit SIN(N) - Sicherheit im Netz

Beitrag zur Cybersicherheit

Das Netzwerk „Surfen mit SIN(N) –Sicherheit im Netz“ setzt sich aus verschiedenen in der Stadt Bielefeld ansässigen Akteuren zusammen und hat zum Ziel, über Potenziale und insb. Risiken der Internetnutzung aufzuklären. Dazu werden verschiedene Schülerprojekte initiiert, Elternabende veranstaltet sowie Weiterbildungsmöglichkeiten für Lehrkräfte angeboten.

Ansprechpartner:

Sozial- und Kriminalpräventiver Rat der Stadt Bielefeld

33602 Bielefeld

surfen-mit-sinn.de

Staatliche Initiative

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

“Surfen mit SIN(N) – Sicherheit im Netz“ dient der Verbreitung von Fachkenntnissen zum Themenbereich der Risiken der Internetnutzung.

Bildung und Awareness

#Schulung #Awareness in der Zivilgesellschaft #Schulisches Bildungsangebot

Im Rahmen von „Surfen mit SIN(N) – Sicherheit im Netz“ werden Schüler, Eltern und Lehrer zur risikoarmen Nutzung von Online-Medien geschult. Die verschiedenen Veranstaltungen können bspw. zu Themen wie Persönlichkeitsrechten, Smartphones, Datenschutz, Cybermobbing oder Computerviren sein.

Zielgruppe

Zivilgesellschaft

- Kinder und Heranwachsende

Das Angebot von „Surfen mit SIN(N) – Sicherheit im Netz“ richtet sich an Schüler, Eltern und Lehrkräfte in der Stadt Bielefeld. Die Workshops für Schüler sind für die Jahrgangsstufen 3 bis 10 konzipiert.

Wissenschaft

- Bildungseinrichtung

Das Netzwerk „Surfen mit SIN(N) – Sicherheit im Netz“ bietet Veranstaltungen für Bielefelder Schulen an.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Lernprogramm

Zum Angebot von „Surfen mit SIN(N) – Sicherheit im Netz“ zählen Fachtage und Lehrertage sowie Elternabende und Schülerprojekte in der Stadt Bielefeld.

UP KRITIS

Beitrag zur Cybersicherheit

Im UP KRITIS, einer öffentlich-privaten Kooperation, arbeiten KRITIS-Betreiber, deren Verbände sowie die zuständigen staatlichen Stellen zusammen. Der UP KRITIS hat das Ziel, die Versorgung mit kritischen Infrastrukturdienstleistungen in Deutschland aufrechtzuerhalten. Da Kritische Infrastrukturen immer mehr auf IKT angewiesen sind, ist deren Sicherheit ein zentraler Aufgabenschwerpunkt des UP KRITIS. Ergebnisse der Arbeiten des UP KRITIS werden betroffenen Unternehmen und teilweise auch der Öffentlichkeit zur Verfügung gestellt. Diese Informationen betreffen u.a. politische Strategien, Sicherheitsgesetze und Regelungen, den Stand der Technik, Lageinformationen sowie Informationen zu Organisationen mit Aufgaben zum Schutz Kritischer Infrastrukturen.

Ansprechpartner:

Geschäftsstelle UP KRITIS

BSI

Referat WG 11

Godesberger Allee 185-189

53175 Bonn

upkritis.de

Staatliche Initiative

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Die am UP KRITIS beteiligten Organisationen arbeiten auf Basis gegenseitigen Ver-trauens zusammen. Sie tauschen sich untereinander aus und lernen voneinander im Hinblick auf den Schutz von KRITIS. Themen, die im UP KRITIS diskutiert und vorangetrieben werden, beinhalten unter anderem: Förderung der Robustheit von IKT-Komponenten in kritischen Prozessen, Austausch über aktuelle Vorkommnisse, gemeinsame Einschätzung und Bewertung der Cyber-Sicherheitslage, Erarbeitung gemeinsamer Dokumente und Positionen, Auf- und Ausbau von Krisenmanagementstrukturen, koordinierte Krisenreaktion und -bewältigung sowie die Durchführung von Notfall- und Krisenübungen.

Bildung und Awareness

#Awareness in der Politik #Awareness in der Wirtschaft

Der UP KRITIS informiert auf der Website upkritis.de über den Schutz Kritischer Infrastrukturen und veröffentlicht Informationsmaterial.

Konzeption und Vorgehensweisen

#Authentifizierung #Informationssicherheitsmanagement #Endgerätesicherheit #Identitätsmanagement #Berechtigungsmanagement #Compliance Management #Datenschutz #IT-Sicherheitsstandards

Arbeitskreise des UP KRITIS setzen sich mit den Themen auf technischer und strategischer Ebene auseinander und erarbeiten Dokumente zu spezifischen Themen.

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen #Cloudsicherheit #Monitoring #IT-Administration

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen #Behandlung von Sicherheitsvorfällen & IT-Forensik

Ein 2020 gegründeter Themenarbeitskreis wird die Thematik Detektion aus Sicht der KRITIS-Betreiber und des BSI abgrenzen und erarbeiten. Die teilnehmenden Organisationen tauschen sich regelmäßig zu Vorfällen aus.

Infrastrukturelle Sicherheitsaspekte

#Betriebs- und Steuerungstechnik #SPS & ICS #Intelligente Messsysteme #RZ-Infrastruktur #physische IT-Sicherheit

Netze und Kommunikation

#Netzarchitektur und -design #Netzkomponenten #Netzmanagement #Funknetze

Zielgruppe

Wirtschaft

- Kritische Infrastruktur

Im UP KRITIS kooperieren Unternehmen, die Betreiber Kritischer Infrastrukturen sind, deren Fachverbände und die zuständigen Behörden. Die KRITIS-Betreiber aus der Wirtschaft gehören zu den 8 Sektoren der Kritischen Infrastrukturen: Energie, Gesundheit, Informationstechnik und Telekommunikation, Transport und Verkehr, Medien und Kultur, Wasser, Finanz- und Versicherungswesen sowie Ernährung.

Staat

- Bund
- Land
- Behörde/Verwaltung
- Ministerium

Der UP KRITIS hat vom BMI ein Mandat erhalten. Mit dieser politischen Stimme kann er insbesondere an Regulierungsvorhaben und sonstigen Sachverhalten beteiligt und angehört werden und die Belange von Betreibern Kritischer Infrastrukturen vertreten.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Studie
- Sonstiges Informationsangebot

Über upkritis.de werden Informationen zu Gesetzen, Strategien, Leitfäden und Studien zur Verfügung gestellt. Es werden zudem sektorübergreifende und sektorspezifische Publikationen veröffentlicht.

8.5 Gesamtgesellschaftliche Initiativen und Akteure

Arbeitsgruppe „Sicherheit Vernetzter Systeme“ - Plattform Industrie 4.0

Beitrag zur Cybersicherheit

Die Plattform Industrie 4.0 beschäftigt sich mit allgemeinen Fragestellungen rund um das Thema Industrie 4.0 und wird vom Bundeswirtschaftsminister sowie von der Bundesforschungsministerin gemeinsam mit hochrangigen Vertretern aus Wirtschaft, Wissenschaft und Verbänden geleitet. Ein großes Handlungsfeld ist hierbei der Bereich der Sicherheit, der durch die Arbeitsgruppe „Sicherheit vernetzter Systeme“ bearbeitet wird. Durch den gemeinsamen Dialog wird Cybersicherheit auf der Plattform Industrie 4.0 weiterentwickelt.

Geschäftsstelle:

Plattform Industrie 4.0

BMWi

Scharnhorststr. 34-37

10115 Berlin

plattform-i40.de

Gesamtgesellschaftliche Initiative

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Durch die Arbeitsgruppe „Sicherheit vernetzter Systeme“ kommen Entscheidungsträger aus Wirtschaft und Politik auf globaler Ebene zusammen.

Bildung und Awareness

#Awareness in der Politik
#Awareness in der Wirtschaft

Die Ergebnisse der Arbeitsgruppe werden in Form von Handlungsempfehlungen mit Politik und Wirtschaft geteilt. Durch Veranstaltungen mit Entscheidungsträgern aus Wirtschaft und Politik wird Awareness für die Thematik geschaffen.

Konzeption und Vorgehensweisen

#Authentifizierung #Identitätsmanagement #Berechtigungsmanagement #Datenschutz

Die Initiative entwickelt zu verschiedenen Themen wie z.B. der Identifikation, der Authentifizierung und dem Datenschutz Lösungsansetze und konkrete Anwendungsbeispiele für eine sichere vernetzte Industrie.

Infrastrukturelle Sicherheitsaspekte

#physische IT-Sicherheit

Die Initiative beschäftigt sich mit den Sicherheitsaspekten der Vernetzung von Hardwarekomponenten im Rahmen von Industrie 4.0.

Netze und Kommunikation

Ein Kernthema der Initiative ist die sichere Kommunikation im Rahmen von Industrie 4.0.

Zielgruppe

Staat

Wirtschaft

Das Angebot der Initiative richtet sich übergreifend an alle politischen und wirtschaftlichen Akteure der Plattform.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Wissenschaftliche Veröffentlichung
- Studie

Berichte und Positionspapiere der Initiative zu aktuellen Fragestellungen werden von den teilnehmenden Akteuren über die Plattform veröffentlicht.

Competence Center for Applied Security Technology e.V. (CAST)

Beitrag zur Cybersicherheit

Das CAST sieht sich als Plattform, Kompetenznetzwerk und Ansprechpartner für IT-Sicherheits-Fragen. In ihm organisieren sich Akteure aus allen Gesellschaftsbereichen. Sein Ziel ist es, in einem breiten Bereich der Wirtschaft und des öffentlichen Sektors die Bedeutung der IT-Sicherheit zu fördern. Hierzu bietet das CAST Veranstaltungen, Workshops, Informationsaufbereitung und Beratung zu IT-Sicherheitstechnologien an. Zu aktuellen Themen sind im CAST Arbeitskreise eingerichtet. Auch stiftet das CAST einen Förderpreis IT-Sicherheit sowie einen Promotionspreis IT-Sicherheit.

Kontakt:

Rheinstr. 75

64295 Darmstadt

cast-forum.de

Gesamtgesellschaftliche Initiative

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Das CAST ist ein Forum zur Vernetzung von Wissenschaft, Wirtschaft, Zivilgesellschaft und Staat. Es unterhält überdies Partnerschaften zu weiteren Organisationen und Institutionen des Fachbereiches IT-Sicherheit wie bspw. dem Nationalen Forschungszentrum für angewandte Cybersicherheit (ATHENE).

Bildung und Awareness

#Schulung #Awareness in der Politik #Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft #Berufliches Bildungsangebot #Universitäres Bildungsangebot #Sonstiges Bildungsangebot

Das CAST bietet Workshops zur Aus- und Weiterbildung sowie Veranstaltungen zur Sensibilisierung für alle Gesellschaftsbereiche an.

Konzeption und Vorgehensweisen

#Kryptographie #Quanten-Kryptographie & Post-Quanten-Kryptographie #Blockchain #Authentifizierung #Informationssicherheitsmanagement #Endgerätesicherheit #Identitätsmanagement #Berechtigungsmanagement #Compliance Management #Datenschutz #IT-Sicherheitsstandards

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen #Cloudsicherheit #Monitoring #IT-Administration

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen #Behandlung von Sicherheitsvorfällen & IT-Forensik

Vernetzung von Systemen, IoT

#Smart Home #Autonomes Fahren #Fahrassistenzsysteme #Künstliche Intelligenz

Zielgruppe

Wirtschaft

Das CAST richtet sein Angebot mehrheitlich an Unternehmen, die öffentliche Verwaltung sowie die Forschung/Wissenschaft in allgemeinen Formaten ohne spezifischen Zielgruppenfokus.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Ausbildung und Schulung
- Beratung
- Sonstige Dienstleistung

Das CAST bietet Veranstaltungen, Aus- und Weiterbildungen im Rahmen von Workshops, Konferenzen, Tutorials und Förderpreise zu verschiedenen Themen im Bereich IT-Sicherheit an. Außerdem werden Anwender bei der Nutzung passender IT-Sicherheitslösungen beraten.

Information

- Informationsaufbereitung
- Newsletter
- Öffentlichkeitsarbeit
- Sonstiges Informationsangebot

Das CAST organisiert Arbeitskreise zum Erfahrungsaustausch und zur Entwicklung von Lösungskonzepten, Whitepaper und Vorträge. Für die Mitglieder wird ein Newsletter veröffentlicht.

CrypTool-Portal

Beitrag zur Cybersicherheit

CrypTool ist ein nicht-kommerzielles Open-Source-Projekt und bietet kostenlose E-Learning-Software zu den Themen Kryptographie und Kryptoanalyse an. Das Projekt, an dem zahlreiche Universitäten und Forschungsinstitute mitwirken, wird hauptsächlich durch ehrenamtliche Mitarbeit getragen. Außerdem wurde ein Buch zum Lernen, Experimentieren und Anwenden bezogen auf kryptographischen Verfahren verfasst.

Ansprechpartner:

CrypTool-Projekt,

Universität Siegen

Kohlbettstr. 15

57072 Siegen

cryptool.org

Gesamtgesellschaftliche Initiative

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Hochschulen aus verschiedenen Ländern, Forschungsinstitute und Unternehmen arbeiten in der Entwicklung von CrypTool zusammen.

Bildung und Awareness

#Schulung #Awareness in der Zivilgesellschaft #Sonstiges Bildungsangebot

Die Software CrypTool, initial entwickelt für Awareness Trainings einer Bank, bietet als Open-Source Lösung allen Bürgerinnen und Bürgern eine Schulungsmöglichkeit zur Kryptographie.

Konzeption und Vorgehensweisen

#Kryptographie #Quanten-Kryptographie & Post-Quanten-Kryptographie

Der Schwerpunkt des Angebotes von CrypTool liegt konzeptionell auf Kryptographie und Kryptoanalyse.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger

Die frei zugängliche Software CrypTool soll jedem die Möglichkeit bieten, sich mit der Thematik der Kryptographie auseinanderzusetzen und persönlich fortzubilden.

Wissenschaft

Unternehmen können das Angebot von CrypTool zur Fortbildung der eigenen Mitarbeiter nutzen.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Literatur

Zum Projektangebot gehört auch ein kostenloses Buch zum Thema Kryptologie und Kryptokurse für Schüler und Lehrer. Sowohl die Software- als auch Informationsangebote stehen dabei auf deutscher und zusätzlich auf englischer Sprache zur Verfügung.

Produkt

- Software

CrypTool ist eine frei zugängliche E-Learning-Software zu Kryptographie und Kryptoanalyse. Die Software läuft unter Windows, Linux und macOS und im Browser auch auf Smartphones.

Cyber Security Cluster Bonn e.V.

Beitrag zur Cybersicherheit

Kontakt:

Godesberger Allee 139

53175 Bonn

cyber-security-cluster.eu

Gesamtgesellschaftliche Initiative

Das Cyber Security Cluster Bonn ist eine als eingetragener Verein aktive Initiative aller Cybersecurity-Einrichtungen der Region Bonn / Rhein-Sieg aus Wissenschaft, Wirtschaft sowie Behörden und öffentlichen Institutionen. Regional angesiedelte Akteure wie bspw. das Fraunhofer Institut FKIE, die Universität Bonn und die Hochschule Bonn-Rhein-Sieg sowie das BSI und das KdoCIR sollen die Kompetenzen der verschiedenen Bereiche zur Cybersicherheit bündeln und dadurch einen Cyber-Security-Standort in der Region begründen. Gemeinsam mit in Bonn ansässigen Cyber Security Akteuren aus der Wirtschaft wie Deutsche Telekom Security GmbH und mittelständischen Firmen wie CONET GmbH, axxessio GmbH und anykey GmbH will das Cyber Security Cluster Bonn im orchestrierten Zusammenspiel von Politik, Wissenschaft und Wirtschaft zur aktiven Immunisierung der Gesellschaft gegen Cyber-Attacken beitragen.

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Das Cyber Security Cluster Bonn veranstaltet zum Zweck der Vernetzung, Wissensvermittlung und Awareness jährlich das Cyber Securoty Tech Summit Europe. Akteure verschiedener Bereiche werden durch die Cluster-Arbeit verknüpft und geben ihr Wissen in Form von Aus- und Weiterbildungen weiter. Startups der Branche werden gezielt mittels Coachings gefördert. Das Cluster hat ein Konzept für die Transferleistung des Cyber Security Wissens zur gezielten Anwendung im Mittelstand für NRW entwickelt.

Bildung und Awareness

#Schulung #Awareness in der Politik #Awareness in der Wirtschaft #Berufliches Bildungsangebot #Universitäres Bildungsangebot

Durch die Initiative werden verschiedene Schulungen und Studiengänge angeboten. Das Expertengremium berät die Bundesregierung im Bereich Cybersecurity.

Konzeption und Vorgehensweisen

#Kryptographie #Authentifizierung #Informationssicherheitsmanagement #Endgerätesicherheit #Identitätsmanagement #Berechtigungsmanagement #Datenschutz #IT-Sicherheitsstandards

Ausgehend von den Kompetenzen und Tätigkeitsschwerpunkten der Mitglieder des Clusters liegen die Schwerpunkte der Arbeit des Clusters in den o.g. Kategorien.

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen #Behandlung von Sicherheitsvorfällen & IT-Forensik

Am Standort Bonn befinden sich mehrere wichtigen Cyber Security Betriebszentren des BSI und KdoCIR. Zusätzlich befindet sich in Bonn das Cyber Defense und Security Operation Center der Telekom Security. Erkenntnisse dieser Arbeit fließen aktiv in die Clusterarbeit ein.

Netze und Kommunikation

#Netzarchitektur und -design #Netzmanagement

BSI, das KdoCIR und die Telekom Security betreiben aktives Netzdesign und Netzmanagement unter dem Aspekt Cyber Sicherheit für Ihre Zuständigkeitsbereiche und teilen wichtige Erkenntnisse in der Clusterarbeit des Cyber Security Clusters Bonn.

Zielgruppe

Zivilgesellschaft

Staat

Neben einer stärkeren Vernetzung, auch unter staatlichen Akteuren, hat das Cyber Security Cluster Bonn die Beratung der Politik zum Ziel. Dazu hat das Cyber Security Cluster Bonn den Weisenrat für Cyber-Sicherheit ins Leben gerufen, der einmal jährlich seinen Bericht mit Empfehlungen an die Politik und Wirtschaft veröffentlicht.

Wissenschaft

In verschiedenen Kooperationen werden Forschungsprojekte der Initiative zur Cybersicherheit initiiert und Konferenzen veranstaltet.

Wirtschaft

Der praxisnahe Wissenstransfer innerhalb des Netzwerkes unterstützt den Know-How-Aufbau in allen tangierten Wirtschaftsbereichen - speziell auch in Richtung Mittelstand.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Ausbildung und Schulung
- Beratung
- Konzept

Die Initiative bietet Beratungsleistungen an, veranstaltet Konferenzen und Vorträge und fördert zudem Neugründungen durch Coachings.

Information

- Informationsaufbereitung
- Öffentlichkeitsarbeit
- Wissenschaftliche Veröffentlichung
- Studie
- Sonstiges Informationsangebot

In Zusammenarbeit zwischen Wissenschaft, Wirtschaft und Staat werden durch die Initiative konkrete Forschungsprojekte initiiert und Forschungsergebnisse in die Praxis transferiert.

Cyberwehr Baden-Württemberg

Beitrag zur Cybersicherheit

Die Cyberwehr Baden-Württemberg (Cyberwehr BW) ist eine Erstkontakt- und Beratungsstelle zur Cybersicherheit sowie Koordinierungsstelle gegen Hackerangriffe für kleine und mittlere Unternehmen in Baden-Württemberg. Sie dient als Vernetzungsplattform zwischen baden-württembergischen Sicherheitsbehörden, Wirtschaft und Wissenschaft. Die Cyberwehr BW ist ein Projekt von FZI Forschungszentrum Informatik, Secorvo Security Consulting GmbH, DIZ | Digitales Innovationszentrum GmbH sowie Cyberforum e.V.

Als Teil der Digitalisierungsstrategie digital@bw des Landes Baden-Württemberg wird die Cyberwehr BW vom Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg gefördert. Seit August 2020 ist die Hotline der Cyberwehr für alle KMU aus Baden-Württemberg erreichbar.

Ansprechpartner:

FZI Forschungszentrum Informatik

Haid-und-Neu-Str. 18

76131 Karlsruhe

cyberwehr-bw.de

Gesamtgesellschaftlicher Akteur

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Als gemeinsame Initiative aus Wissenschaft, Wirtschaft und Staat dient die Cyberwehr BW der regionalen Vernetzung dieser Gesellschaftsbereiche in Baden-Württemberg.

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen
#Behandlung von Sicherheitsvorfällen & IT-Forensik

Cyberwehr BW unterstützt bei der Angriffsabwehr und Schadensbegrenzung reaktiv, d.h. nach einem eingetretenen Vorfall.

Zielgruppe

Wirtschaft

Aktuell befindet sich Cyberwehr BW in einer Prototypphase. Das Einsatzgebiet der Vor-Ort-Einsätze ist auf KMU in der Pilotregion, d.h. den Stadt- und Landkreisen Karlsruhe, Rastatt und Baden-Baden beschränkt, jedoch nicht auf eine bestimmte Branche begrenzt. Der landesweite Ausbau des Angebotes ist geplant.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Beratung

Cyberwehr BW ist Kontakt- und Beratungsstelle bei Hackerangriffen und bietet eine initiale Vorfalldiagnose über eine kostenlose Hotline an. Bei Bedarf werden darüber hinaus Experten vermittelt, die für weitergehende Sofort-Hilfe-Maßnahmen zur Verfügung stehen.

Information

- Informationsaufbereitung

Cyberwehr BW liefert auf der Webseite Informationen zu Sofort-Hilfe-Maßnahmen für Opfer von Cyber-Angriffen.

Denkwerkstatt Sichere Informationsgesellschaft

Beitrag zur Cybersicherheit

Das Projekt „Denkwerkstatt Sichere Informationsgesellschaft - Institutionalisierung des gesellschaftlichen Dialogs“ wurde als Nachfolgeprojekt von "Digitale Gesellschaft: smart & sicher" (SuSi) auf Initiative des BSI initiiert. Mit der Durchführung der Dialogveranstaltungen wurde das nexus Institut in Kooperation mit dem Digitale Gesellschaft e.V. beauftragt. Ziel des Projektes ist eine gesamtgesellschaftliche Vernetzung und Einbindung von Akteuren zum Thema Cybersicherheit über alle Zielgruppen hinweg. Im Rahmen des Projekts findet in regelmäßigen Abständen das Dialogformat "Denkwerkstatt Sichere Informationsgesellschaft" statt. Dazu werden Workshops, Arbeitsgruppen und Veranstaltungen zu unterschiedlichen Themenbereichen angeboten, die eine gesamtgesellschaftliche Gestaltung und Lösungsfindung in Fragen der Cybersicherheit unterstützen.

Ansprechpartner:

nexus Institut für Kooperationsmanagement und interdisziplinäre Forschung GmbH

Willdenowstr. 38

12203 Berlin

denkwerkstatt-cybersicherheit.de

Gesamtgesellschaftliche Initiative

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Das Projekt bindet im Rahmen der angebotenen Veranstaltungen diverse Akteure über alle Zielgruppen hinweg ein und vernetzt Vertreter unterschiedlichster Bereiche zum Thema Cybersicherheit.

Zielgruppe

Zivilgesellschaft

Wissenschaft

Staat

Wirtschaft

Ziel des Projekts ist es, einen gesamtgesellschaftlichen Austausch zur Gestaltung der Cybersicherheit in Deutschland über alle Zielgruppen hinweg zu erreichen.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Öffentlichkeitsarbeit

Im Rahmen des Projekts werden themenspezifische Workshops, Arbeitsgruppen und Veranstaltungen angeboten.

Transferstelle IT-Sicherheit im Mittelstand (TISiM)

Beitrag zur Cybersicherheit

Kontakt:

Albrechtstr. 10c

10117 Berlin

tisim.de

Gesamtgesellschaftlicher Akteur

Die TISiM ist ein Verbundprojekt von Deutschland sicher im Netz (DSiN, vgl. eigener Steckbrief) als Konsortialführer, DIHK, Fraunhofer FOKUS (vgl. eigener Steckbrief), Fraunhofer IAO und der Hochschule Mannheim. Die Transferstelle wird gefördert durch das BMWi im Rahmen der Initiative IT-Sicherheit in der Wirtschaft (vgl. eigener Steckbrief). Die Transferstelle IT-Sicherheit im Mittelstand unterstützt KMU, Handwerksbetriebe, Freiberufler und Selbstständige bei der Umsetzung von IT-Sicherheit, indem sie Angebote zur IT-Sicherheit bündelt, praxisnah aufbereitet und passgenau vermittelt. Hierzu werden im weiteren Projektverlauf sogenannte „Schaufenster“ durch Industrie- und Handelskammern regional vor Ort betrieben. Auch ein mobiler Transferstellenbus ist geplant für eine verbesserte regionale Abdeckung. Bundesweit werden die Angebote der Transferstelle digital über die Virtuelle Transferstelle bereitgestellt.

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

An der Initiative sind Experten aus Wirtschaft, Wissenschaft, und Zivilgesellschaft beteiligt. Das Unterstützungsangebot für KMU ist regional über die Schaufenster, sowie bundesweit und digital über die Virtuelle Transferstelle erreichbar. Die Transferstelle bietet hierzu auch eine Vernetzung zu bestehenden regionalen Netzwerken an.

Bildung und Awareness

#Schulung #Awareness in der Politik #Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft

Die Initiative bietet verschiedenes Informationsmaterial sowie eigene Workshops zur Awareness-Steigerung und Umsetzung von IT-Sicherheitsmaßnahmen für KMU an.

Konzeption und Vorgehensweisen

#Informationssicherheitsmanagement #Endgerätesicherheit #Datenschutz

Die Transferstelle bietet interessierten KMU für deren spezifische Bedarfe Informationen zu existierenden Angeboten oder Initiativen im Bereich der IT-Sicherheit dar. Hierzu wird nach einer individuellen Bedarfsabfrage ein passgenaues Paket von Initiativen und Angeboten übermittelt. Als regionale Ansprechpartner stehen bundesweit ca. 80 Stellen unter anderem bei Industrie- und Handelskammern direkt vor Ort zur Verfügung.

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen #Cloudsicherheit #Monitoring #IT-Administration

Die Transferstelle vermittelt nötiges Basiswissen und verweist auf Angebote, die bei betriebsbezogenen Sicherheitsaspekten weiterhelfen, beraten und unterstützen können.

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen #Behandlung von Sicherheitsvorfällen & IT-Forensik

Es werden unterschiedliche Angebote für Unternehmen aufgezeigt, die bei der Erkennung von Sicherheitsrisiken und Ereignissen sowie bei deren Behandlung unterstützen können.

Zielgruppe

Wirtschaft

- Baugewerbe
- Finanzdienstleistung
- Freiberufliche wissenschaftliche technische Dienstleistungen
- Gastgewerbe
- Gesundheits- und Sozialwesen
- Handel
- Land- und Forstwirtschaft
- Rechtsanwälte
- Sonstige wirtschaftliche Dienstleistungen

Die Initiative spricht deutschlandweit KMU, Handwerksbetriebe, Freiberufler und Selbstständige branchenübergreifend an.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Beratung

Anfragende KMU, Handwerksbetriebe, Freiberufler und Selbstständige erhalten von der Transferstelle einen passgenauen Aktionsplan, der bestehende Angebot und Initiativen aufzeigt. Diese Unterstützung kann digital, vor Ort und über den mobilen Transferstellenbus abgerufen werden.

Information

- Informationsaufbereitung
- Journalismus
- Blog
- Newsletter
- Öffentlichkeitsarbeit
- Studie
- Sonstiges Informationsangebot

Die Transferstelle bietet anfragenden KMU, Handwerksbetrieben, Freiberuflern und Selbstständigen eine Vielzahl von stetig wachsenden Informationsmaterialien an.

8.6 Initiativen aus Wirtschaft und Staat

Allianz für Cyber-Sicherheit (ACS)

Beitrag zur Cybersicherheit

Die ACS wurde vom BSI in Zusammenarbeit mit dem Bitkom als Netzwerk aus IT-Herstellern, IT-Beratungs- und Dienstleistungsunternehmen sowie Anwenderunternehmen aller Branchen und Größen gegründet. Ziel der ACS ist die Stärkung der Cyber-Resilienz des Wirtschaftsstandortes Deutschland. Den mehr als 3.800 Unternehmen und Institutionen, welche Stand 2019 Teil dieser Initiative sind, stehen neben dem Austausch von Erfahrung und Expertise kostenlose Partner-Angebote zur Verbesserung der eigenen IT-Sicherheit zur Verfügung.

Ansprechpartner:

BSI

Godesberger Allee 185-189

53175 Bonn

allianz-fuer-cybersicherheit.de

Initiative aus Wirtschaft und Staat

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Rund 200 Partner und Multiplikatoren engagieren sich im Rahmen der ACS für einen breitbandigen Wissenstransfer und gemäß ihrem Motto "Netzwerke schützen Netzwerke". Für den Austausch wurden spezifische Formate wie Erfahrungs- und Expertenkreise kreiert. Die ACS unterstützt Dach- und Fachverbände bei der Konzeption von Profilen zur branchenspezifischen Umsetzung des IT-Grundschutzes.

Bildung und Awareness

#Schulung #Awareness in der Politik #Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft

Zur Stärkung des IT-Sicherheitsbewusstseins bietet die ACS aufbereitete Informationen in ihrem Informationspool an. Das "Übungszentrum Netzverteidigung" ist ein Schulungsformat für Mitglieder, in welchem die Ausnutzung und Schließung verschiedenster Sicherheitslücken theoretisch wie praktisch behandelt wird.

Zielgruppe

Wirtschaft

Der Großteil der Arbeit der ACS richtet sich ohne Branchenfokus an wirtschaftliche Akteure, wobei es explizite Angebote für KMU gibt. Viele bereitgestellte Informationen bieten jedoch auch für Behörden und wissenschaftliche Institutionen einen Mehrwert.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Ausbildung und Schulung
- Beratung
- Konzept

Innerhalb der ACS werden den Mitgliedern im Rahmen von Partner-Angeboten Schulungen, Workshops, Fachartikel sowie weitere Dienstleistungen wie Penetrationstests, Analysen und Erstberatungen angeboten.

Information

- Informationsaufbereitung
- Newsletter
- Öffentlichkeitsarbeit
- Studie
- Sonstiges Informationsangebot

Der Informationspool beinhaltet kostenlose Informationen zu aktuellen Cyber-Bedrohungslagen, allgemeinen Cyber-Risiken und geeigneten Maßnahmen zur Steigerung der Resilienz; aber auch Roadmaps zur individuellen und branchenbezogenen Umsetzung des IT-Grundschutzes (bspw. im Handwerk oder für KMU). Mitglieder mit Geheimschutzbetreuung oder Betreiber von kritischen Infrastrukturen erhalten in einem gesonderten Informationsbereich zusätzlich vertrauliche Informationen und Services wie bspw. Warnmeldungen.

Allianz Industrie 4.0 Baden-Württemberg

Beitrag zur Cybersicherheit

Die Allianz Industrie 4.0 Baden-Württemberg ist ein Netzwerk zur Bündelung der Kompetenzen im Bereich Produktionstechnik sowie Informations- und Kommunikationstechnik, um den Mittelstand im Prozess zur Industrie 4.0 u.a. mit dem Ziel der Datensicherheit zu unterstützen. Die Allianz Industrie 4.0 ist ein vom Wirtschaftsministerium Baden-Württemberg initiiertes und gefördertes Netzwerk, das beim VDMA e.V. Baden-Württemberg angesiedelt ist. Unter anderem beteiligt sich die Allianz Industrie 4.0 regelmäßig aktiv an verschiedenen Veranstaltungen zur Cybersicherheit wie z. B. dem "CyberSicherheitsForum" oder dem "Cybersecurity-Kongress Ostwürttemberg".

Ansprechpartner:

Koordinierungsstelle der Allianz Industrie 4.0 Baden-Württemberg beim VDMA e.V.

Baden-Württemberg

Kronenstr. 3

70173 Stuttgart

i40-bw.de

Initiative aus Wirtschaft und Staat

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

In den Gremien der Allianz Industrie 4.0 werden Themen wie Cybersicherheit bearbeitet und Handlungsweisen entwickelt, die im Netzwerk und den Partnern zur Verfügung gestellt werden. Zusätzlich beteiligt sich die Allianz Industrie 4.0 an verschiedenen Veranstaltungen zur Cybersicherheit.

Bildung und Awareness

#Awareness in der Wirtschaft

Neben Veranstaltungen werden in Kooperation mit weiteren Akteuren auch Seminare, Workshops und Sprechtage rund um Cybersecurity im Zusammenhang mit Produktionsanlagen angeboten.

Zielgruppe

Wirtschaft

- Aerospace / Luft- und Raumfahrt
- Automobilbranche / Automotive
- Gesundheits- und Sozialwesen
- Information und Kommunikation
- Sonstiges verarbeitendes Gewerbe

Die Angebote der Allianz Industrie 4.0 richten sich vorwiegend an Unternehmen, insbesondere KMU, aus der Industrie in Baden-Württemberg (Schwerpunkt Automotive und Maschinenbau sowie verarbeitendes Gewerbe), die sich im Transformationsprozess zur Industrie 4.0 befinden.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Beratung

Die Allianz Industrie 4.0 bietet Beratungsdienstleistungen rund um das Thema Cybersicherheit im Rahmen des Industrie 4.0 Scoutings an.

Information

- Informationsaufbereitung
- Newsletter
- Öffentlichkeitsarbeit
- Studie

Regelmäßig finden Veranstaltungen der Allianz Industrie 4.0 statt, oft gemeinsam mit Kooperationspartnern. Auf der Website stellt sie Veranstaltungen der Partner, Förderprogramme und Neuigkeiten zum Thema bereit. Ein Informationsportal zum Thema Cybersecurity ist derzeit im Aufbau.

CERT-Verbund

Beitrag zur Cybersicherheit

Der Computer Emergency Response Team (CERT)-Verbund ist ein Zusammenschluss von rund 45 Sicherheits- und Computer-Notfallteams aus Staat und Wirtschaft, die sich dem Schutz nationaler Netze der Informationstechnik verschrieben haben. Dadurch wird das Ziel verfolgt, gemeinsam und schnell auf Angriffe auf die Cybersicherheit reagieren zu können. Die Initiative wurde vom DFN-CERT zusammen mit dem CERT-Bund, Siemens-CERT, S-CERT und Telekom-CERT gegründet und steht prinzipiell allen deutschen CERTs offen.

Kontakt per Mail:

cv-lk@lists.cert-verbund.de

cert-verbund.de

Initiative aus Wirtschaft und Staat

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Der CERT-Verbund stellt eine Übersicht für die verschiedenen Akteure der Initiative bereit. Er ermöglicht einen regelmäßigen Austausch von Erfahrungen sowie themenspezifischen Informationen und Inhalten. Insbesondere im Bereich der IT-Vorfallsbearbeitung wird die IT-Sicherheit der Zielgruppen durch eine übergreifende Zusammenarbeit verbessert.

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen

Die beteiligten CERTs tauschen IT-sicherheitsrelevante Informationen untereinander aus.

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen
#Behandlung von Sicherheitsvorfällen & IT-Forensik

Die im Zusammenschluss des CERT-Verbunds kooperierenden Akteure verfolgen das Ziel, den Schutz nationaler Netze der Informationstechnik sicherzustellen und im Falle sicherheitsrelevanter Ereignisse gemeinsam und schnell reagieren zu können.

Zielgruppe

Wissenschaft

Universitäts-CERTs

Wirtschaft

Von der Arbeit des CERT-Verbunds profitieren insbesondere dessen Mitglieder, bestehende und entstehende CERT-Teams sowie die deutschsprachige Öffentlichkeit.

Staat

- Bund
- Land
- Behörde/Verwaltung

CERTs der Verwaltung als optionale Ergänzung zu den Verwaltungs-CERT-Verbünden.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Sonstiges Informationsangebot

Der CERT-Verbund bietet seinen Mitgliedern einen breit angelegten Informationsaustausch über eingesetzte Technik und Methoden sowie aktuelle Sicherheitsvorfälle. In Arbeitsgruppen werden zudem neue Ideen aufgegriffen, diskutiert und weiterentwickelt.

German Competence Centre against Cyber Crime e.V. (G4C)

Beitrag zur Cybersicherheit

Das G4C ist ein gemeinnütziger Verein, der seine Mitglieder über Themen der Cyberkriminalität informiert und deren fachlichen Austausch gewährleistet. Die Mitglieder sind v. a. wirtschaftliche Akteure, aber auch staatliche Akteure wie das Bundeskriminalamt (BKA) oder das Bundesamt für Sicherheit in der Informationstechnik (BSI) sind als Kooperationspartner vertreten. Ziele des G4C sind die Analyse von Cyberkriminalität und die Erarbeitung präventiver Maßnahmen, die Schaffung einer Austauschplattform sowie die Durchführung von Forschungsprojekten und Kampagnen.

Kontakt:

Borsigstr. 36

65205 Wiesbaden

g4c-ev.de

Initiative aus Wirtschaft und Staat

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

G4C versteht sich als Netzwerk gegen Cyberkriminalität. Hierzu werden Informationen und Erkenntnisse bspw. zu auftretenden Angriffsmustern untereinander ausgetauscht.

Bildung und Awareness

#Awareness in der Wirtschaft #Berufliches Bildungsangebot

G4C führt seit Gründung 2013 regelmäßig Workshops und Informationsveranstaltungen durch. Im Bereich Schulungs- und Fortbildungsinitiativen erfolgt eine Neupositionierung gemeinsam mit den entsprechenden Kooperationspartner und Mitgliedern.

Konzeption und Vorgehensweisen

#Authentifizierung #Informationssicherheitsmanagement #Compliance Management

G4C unterstützt im Rahmen des Backup-Checks die Bereiche Sicherheitsüberprüfungen von potentiellen Zulieferern und Bestandsdienstleistern sowie Sicherheitsüberprüfung im Bereich von kritischen Geschäftsprozessen.

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen
#Behandlung von Sicherheitsvorfällen & IT-Forensik

Um betroffene Unternehmen und deren Kunden zu schützen, setzt G4C sich in einer Kooperation mit dem BKA und dem BSI aktiv gegen Cyberkriminelle ein, die gehackte oder gestohlene Daten weiterleiten.

Infrastrukturelle Sicherheitsaspekte

#physische IT-Sicherheit

Zielgruppe

Wissenschaft

- Bildungseinrichtung

G4C betreibt mit zwei Bildungseinrichtungen eine enge Kooperation zur Aus- und Fortbildung der Mitarbeiter der Mitgliedsunternehmen zum Schutz gegen illegale Angriffe.

Wirtschaft

- Energieversorgung
- Finanzdienstleistung
- Gesundheits- und Sozialwesen
- Beratung
- Kritische Infrastruktur

Die Mitglieder von G4C setzen sich vorrangig aus den Branchen Banken, Versicherungen, Energieversorgung, Health-Care und Logistik zusammen.

Staat

- Bund
- Land
- Behörde/Verwaltung
- Einrichtung
- Ministerium

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Ausbildung und Schulung
- Beratung
- Konzept

Information

- Informationen, Austausch, Seminare und Veranstaltungen
- Hilfe zur Selbsthilfe
- Themen- und nutzerorientierte Arbeitsgruppen (geschlossen und offen)

Initiative Wirtschaftsschutz

Beitrag zur Cybersicherheit

Die durch das BMI koordinierte Dachinitiative zur Umsetzung der Nationalen Strategie für Wirtschaftsschutz analysiert gemeinsam mit Experten von Sicherheitsbehörden (BfV, BKA, BND und BSI), sowie Spitzenwirtschafts- und Sicherheitsverbänden (BDI, DIHK, ASW Bundesverband und BDSW) die Risikolage und entwickelt tragfähige Handlungskonzepte und Checklisten zu den Themenfeldern

- Ganzheitlicher Wirtschaftsschutz
- Cyber-, hybride und physische Sicherheitsrisiken
- Eigenschutzmaßnahmen von Unternehmen und Forschungseinrichtungen
- Unterstützungsmaßnahmen von Politik und Behörden zum Schutz deutscher Unternehmenswerte.

Ansprechpartner:

Initiative Wirtschaftsschutz c/o

BMI

Alt-Moabit 140

10557 Berlin

wirtschaftsschutz.info

Initiative aus Wirtschaft und Staat

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Mit den gebündelten Kompetenzen von Sicherheitsbehörden (BfV, BKA, BND und BSI), Spitzen-wirtschafts- und Sicherheitsverbänden (BDI, DIHK, ASW Bundesverband, BDSW) sowie Forschungseinrichtungen werden zunächst drängende Risiken analysiert, anschließend in tragfähige Handlungskonzepte umgesetzt und Interessierten auf der Internetplattform der Initiative zur Verfügung gestellt. Ferner existieren Kooperationsangebote zur themen- und/oder anlassbezogenen Vernetzung von staatlichen, unternehmerischen und wissenschaftlichen Akteuren.

Bildung und Awareness

#Awareness in der Wirtschaft

Durch die kostenfreie Bereitstellung von Informationen und Handlungsempfehlungen zu Sicherheitsfragen rund um den Wirtschaft- und Wissenschaftsschutz schafft die Initiative Awareness für die aktuellen Sicherheitsrisiken und leistet „Hilfe zur Selbsthilfe“.

Zielgruppe

Wirtschaft

Das Angebot richtet sich allgemein an die Wirtschaft, insb. jedoch an kleine und mittlere Unternehmen sowie Forschungseinrichtungen.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Studie
- Sonstiges Informationsangebot

Das Informationsportal der Initiative bietet bspw. Cyberbriefe, Lagebilder, Leitfäden, Faltblätter, Broschüren, Studien und Medienauswertungen. Auch veranstaltet die Initiative u.a. Wirtschaftsschutzkonferenzen.

IT-Sicherheitsinitiative Saarland

Beitrag zur Cybersicherheit

Die IT-Sicherheitsinitiative Saarland ist ein Netzwerk zur Förderung der im Saarland ansässigen Unternehmen und Behörden im Bereich der IT-Sicherheit , welches regelmäßig Fachtagungen und Workshops anbietet. Die Initiative soll auch als Marketing-Instrument für die anbietenden Unternehmen genutzt werden und sie mit potenziellen Anwendern in Verbindung bringen. Weiterhin werden interdisziplinäre Arbeitsgruppen gebildet sowie Vorträge und Weiterbildungsmaßnahmen unter Einbindung von Politik und Wissenschaft angeboten. Verantwortlich für die IT-Sicherheitsinitiative Saarland ist der saar.is – saarland.innovation & standort e.V.

Ansprechpartner:

saar.is – saarland.inno-vation & standort e.V.

Franz-Josef-Röder-Str. 9

66119 Saarbrücken

it-sicherheit.saarland

Initiative aus Wirtschaft und Staat

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Die Initiative ist in erster Linie eine Plattform zur Vernetzung von Anbietern und Anwendern im Bereich IT-Sicherheit.

Bildung und Awareness

#Schulung #Awareness in der Wirtschaft

Das Angebot umfasst Weiterbildungsmaßnahmen, die Arbeit in Fachgruppen und Vorträge.

Zielgruppe

Wissenschaft

Das Angebot der Initiative richtet sich auch an Wissenschaftler und Studierende der saarländischen Hochschulen.

Wirtschaft

- Information und Kommunikation

Die Initiative unterstützt Startups und Anbieter, aber auch anwendende Unternehmen im Bereich der IT-Sicherheit.

Staat

- Behörde/Verwaltung

Zur Zielgruppe der Initiative zählen u.a. Interessierte aus Behörden und Politik.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Lernprogramm

Von der Initiative werden interdisziplinäre Arbeitsgruppen gebildet sowie Weiterbildungsmöglichkeiten, Vorträge und Workshops angeboten.

Kompetenzzentrum Digitales Handwerk

Beitrag zur Cybersicherheit

Das Kompetenzzentrum Digitales Handwerk ist Teil der Förderinitiative „Mittelstand 4.0 – Digitale Produktions- und Arbeitsprozesse“, die im Rahmen des Förderschwerpunkts „Mittelstand-Digital – Strategien zur digitalen Transformation der Unternehmensprozesse“ vom BMWi gefördert wird. Zum Thema Cybersicherheit werden den Handwerksbetrieben kostenlose Informationsmaterialien und Veranstaltungen angeboten.

Ansprechpartner:

Zentralverband des Deutschen Handwerks e.V.

Mohrenstr. 20/21

10117 Berlin

handwerkdigital.de

Initiative aus Wirtschaft und Staat

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Das Kompetenzzentrum führt regelmäßig Cybersicherheitstage, Workshops und Webinare für Unternehmen, Handwerkskammern und Verbände durch, um die Cybersicherheit im Handwerk sukzessive zu erhöhen.

Bildung und Awareness

#Awareness in der Wirtschaft

Ein vom Kompetenzzentrum angebotener „Routenplaner - Cybersicherheit für Handwerksbetriebe“ soll KMU mit dem Thema Cybersicherheit vertraut machen.

Konzeption und Vorgehensweisen

#Informationssicherheitsmanagement #Endgerätesicherheit

Das Kompetenznetzwerk erstellt spezifische Arbeitshilfen zu den IT-Grundschutz-Bausteinen für Handwerksbetriebe.

Zielgruppe

Wirtschaft

Zielgruppe des Kompetenzzentrums sind Handwerksbetriebe und KMU.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung

Das Angebot des Kompetenznetzwerks umfasst Informationsmaterialien wie den Routenplaner Cybersicherheit für Handwerksbetriebe, um diesen Unterstützung bei der Umsetzung der Informationssicherheit zu bieten.

OPTIMOS 2.0

Beitrag zur Cybersicherheit

OPTIMOS 2.0 ist ein vom BMWi gefördertes Forschungsprojekt, in dessen Rahmen eine App zur elektronischen Identifikation mithilfe des Personalausweises entwickelt wird. Mittels der sogenannten elektronischen ID (eID) sollen eID-Dienstanbieter zukünftig Services auf hohem Sicherheitsniveau anbieten können. Das Projekt wird von einem Konsortium, bestehend aus verschiedenen Akteuren aus Wirtschaft und Wissenschaft, darunter u.a. die Freie Universität Berlin und die TU Dresden, unter der Leitung der Bundesdruckerei GmbH durchgeführt.

Ansprechpartner:

Bundesdruckerei GmbH

Kommandantenstr. 18

10969 Berlin

bundesdruckerei.de/de/Unternehmen/Innovation/Optimos

Initiative aus Wirtschaft und Staat

Thematische Schwerpunkte (Auszug)

Konzeption und Vorgehensweisen

#Authentifizierung #Identitätsmanagement #Berechtigungsmanagement

Im Rahmen des Projekts OPTIMOS 2.0 werden Technologien und die Infrastruktur zur sicheren Online-Authentifizierung mittels mobilen Geräten entwickelt. Diese sollen in Form eines "offenen Ökosystems" entwickelt werden, sodass Schnittstellen zu Sicherheitselementen relevanter Mobilgerätanbieter und Mobilfunknetzbetreiber geschaffen werden. Serviceanbieter können anschließend eID-Dienste auf dieser Basis anbieten und Nutzer sind in der Lage, die Daten ihres Personalausweises sicher in der entwickelten App zu hinterlegen.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger

Wirtschaft

Durch das im Rahmen des Forschungsprojekt OPTIMOS 2.0 entwickelte Ökosystem profitieren sowohl Serviceanbieter als auch Nutzer, die auf ein einheitliches Ökosystem zur elektronischen Authentifizierung auf einem hohen Sicherheitsniveau zurückgreifen können. Zusätzlich sollen Marktzugangshemmnisse für KMU und Markteinsteiger reduziert werden, da diese auf die technischen und organisatorischen Bestandteile des Projekts zurückgreifen können.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Produkt

- Software/SaaS

Das Ergebnis des Projekts OPTIMOS 2.0 ist eine eID-App, mit der sich Nutzer vertrauenswürdig ausweisen können.

Sicherheitsforum Baden-Württemberg

Beitrag zur Cybersicherheit

Das Sicherheitsforum Baden-Württemberg ist eine Sicherheitspartnerschaft zwischen staatlichen und wirtschaftlichen Akteuren und hat den Schutz von Firmenwissen zum Ziel. IT-Sicherheitsgefährdungen für Unternehmen aus Baden-Württemberg wurden in einer Studie erhoben und Handlungsempfehlungen insbesondere für kleine und mittlere Unternehmen erarbeitet. Neben der Teilnahme an Messen und Veröffentlichung von Informationsmaterial bietet die Initiative auch Beratung an.

Kontakt:

Willy-Brandt-Str. 41

70173 Stuttgart

sicherheitsforum-bw.de

Initiative aus Wirtschaft und Staat

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Das Sicherheitsforum vernetzt staatliche und wirtschaftliche Akteure aus Baden-Württemberg.

Bildung und Awareness

#Awareness in der Wirtschaft

Durch die Arbeit des Sicherheitsforums werden dessen Mitglieder für den Bereich der IT-Sicherheit sensibilisiert.

Konzeption und Vorgehensweisen

#Datenschutz

Hauptziel des Sicherheitsforums ist es, wichtige Unternehmensdaten vor Wirtschaftsspionage und Konkurrenzausspähung zu schützen.

Zielgruppe

Wirtschaft

Zielgruppe des Sicherheitsforums ist die baden-württembergische Wirtschaft.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Beratung

Das Sicherheitsforum bietet Beratung zu Sicherheitsfragen an.

Information

- Informationsaufbereitung
- Öffentlichkeitsarbeit
- Studie
- Sonstiges Informationsangebot

Das Sicherheitsforum führt Studien durch, ist auf Messen vertreten und veröffentlicht Informationen.

Sicherheitskooperation Cybercrime

Beitrag zur Cybersicherheit

Die Sicherheitskooperation Cybercrime besteht zwischen den Landeskriminalämtern Baden-Württemberg, Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz und Sachsen sowie dem Bitkom e.V. Durch den Austausch von Wissen und Kompetenzen zwischen der Polizei und der Digitalwirtschaft verfolgt die Kooperation das Ziel der Prävention und Bekämpfung von Cyberkriminalität.

Kontakt per Mail:

siko@bitkom.org

Albrechtstr. 10

10117 Berlin

sicherheitskooperation-cybercrime.de

Initiative aus Wirtschaft und Staat

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Im Rahmen der Kooperation werden die Kompetenzen der Digitalwirtschaft mit denen der teilnehmenden Landeskriminalämter miteinander vernetzt. Die beteiligten Landeskriminalämter haben einen Single Point of Contact eingerichtet, an welchen sich Behörden und Unternehmen bei Bedarf wenden können.

Bildung und Awareness

#Awareness in der Politik #Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft

Die Sicherheitskooperation Cybercrime bietet zur Förderung von Awareness hinsichtlich Cybercrime verschiedene Veranstaltungen an, hierzu gehört insbesondere eine jährlich stattfindende Jahrestagung, die rotierend durch die beteiligten Landeskriminalämter ausgerichtet wird und die sich mit aktuellen Themen im Kontext der Computerkriminalität befasst.

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen

Die Sicherheitskooperation Cybercrime warnt auf ihrer Webseite vor aktuellen Cyberangriffen und liefert hierfür detaillierte Informationen zu Detektionsregeln und technischen Indikatoren. Auch unterstützt der Bitkom e.V. im Rahmen der Sicherheitskooperation Cybercrime die Landeskriminalämter bei der Erstellung von Cybercrime-Lagebildern.

Zielgruppe

Zivilgesellschaft

- Bürgerinnen und Bürger
- Angestellte

Wirtschaft

Landeskriminalämter sowie Mitgliedsunternehmen des Bitkom e.V. können sich an der Kooperation beteiligen und von dessen Angebot profitieren.

Staat

- Behörde/Verwaltung

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Beratung

Im Vordergrund steht der Wissens- und Kompetenzaustausch in der Kooperation zwischen der Polizei und der Digitalwirtschaft.

Information

- Informationsaufbereitung
- Öffentlichkeitsarbeit
- Studie
- Sonstiges Informationsangebot

Die Sicherheitskooperation Cybercrime erarbeitet Informationsangebote zur Schaffung von Awareness zu Cybercrime und für die Präventionsarbeit. Außerdem beteiligt sie sich an Studien, bspw. zum Wirtschaftsschutz in der digitalen Welt. Vertreter der Sicherheitskooperation sind zudem auf Fachmessen mit Ständen und Vorträgen präsent.

8.7 Initiativen aus Wissenschaft und Wirtschaft

IT-Sicherheitscluster e.V.

Beitrag zur Cybersicherheit

Der IT-Sicherheitscluster e.V. verfolgt Themen aus dem Bereich Cybersicherheit, die aktuell im öffentlichen Fokus stehen, insb. IT-Security und Functional Safety, und den Kompetenzen und Interessen der Mitglieder entsprechen. Die Initiative hat es sich zur Aufgabe gemacht, die Wettbewerbsfähigkeit und die Marktchancen ihrer Mitgliedsunternehmen zu erhöhen. In ihr arbeiten Unternehmen, die IT-Sicherheitstechnologien nutzen, sowie Unternehmen der IT-Wirtschaft, Hochschulen, Forschungs- und Weiterbildungseinrichtungen und Juristen zusammen.

Kontakt:

Franz-Mayer-Str. 1

93053 Regensburg

it-sicherheitscluster.de

Initiative aus Wirtschaft und Wissenschaft

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Ein wesentliches Ziel der Initiative ist es, als Plattform zu fungieren und aktiv Kooperationen zu initiieren und zu unterstützen. Ihre Veranstaltungen dienen als Ausgangspunkt für Kooperationen. Das Clustermanagement stellt auf Anfrage auch gezielt Kontakte zwischen potentiellen Partnern her.

Bildung und Awareness

#Schulung #Berufliches Bildungsangebot

Die Initiative bietet Fortbildungen zu Sicherheitsthemen sowie Zertifikatslehrgänge (IT-Sicherheits-beauftragter / Informationssicherheitsanalyse / ISMS) an. Über öffentliche Veranstaltungen und Workshops informiert die Initiative Unternehmen und Privatanwender über Sicherheitsrisiken sowie technische und organisatorische Lösungen.

Konzeption und Vorgehensweisen

#Informationssicherheitsmanagement #Datenschutz

Die Initiative schult und unterstützt bei den Themen Datenschutz-Managementsystemen und ISMS. Sie hat u.a. eine Eigenentwicklung eines Datenschutzmanagementsystems erarbeitet.

Betriebsbezogene Sicherheitsaspekte

#Cloudsicherheit

Mit spezialisierten Foren arbeitet die Initiative an den Themenbereichen Cloud Computing und Cloudsicherheit.

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen

Infrastrukturelle Sicherheitsaspekte

#SPS & ICS

In speziellen Foren beschäftigt sich der Sicherheitscluster mit dem Themenbereich Sicherheit der industriellen IT.

Zielgruppe

Wissenschaft

- Bildungseinrichtung
- Forschungseinrichtung

Die Initiative unterstützt Projekte im Bereich Forschung und Entwicklung, Bildung und Wissenschaft.

Wirtschaft

Die Initiative spricht Unternehmen branchenübergreifend an.

Staat

- Behörde/Verwaltung

Die Leistungen der Initiative richten sich insb. an die kommunalen Verwaltungen.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Sonstige Dienstleistung

Die Initiative organisiert Workshops, Kongresse und Messen und fördert gegenseitiges Kennenlernen und Vernetzung.

Produkt

- Software

Die Initiative bietet als Eigenentwicklung ein Datenschutzmanagementsystem zum Schutz der personenbezogenen Daten in Unternehmen an, womit alle dokumentierten und implementierten Regelungen, Prozesse und Maßnahmen datenschutzkonform gesteuert und kontrolliert werden können.

Cyber Security Center - Kompetenzzentrum für Informationssicherheit

Beitrag zur Cybersicherheit

Das Cyber Security Center als Kompetenzzentrum dient zur Information über die Aktivitäten und Forschungsprojekte der Hochschule Albstadt-Sigmaringen im Bereich der Cybersicherheit und Digitalen Forensik. Das Cyber Security Center leistet wissenschaftliche Arbeit und nimmt Aufträge bspw. für Auftragsforschung, Vorträge oder Workshops an. Es betreibt auch einen Fachblog, auf welchem Studenten ihre Ausarbeitungen veröffentlichen können und der dem Transfer von Fachwissen zur Cybersicherheit in die Wirtschaft und Zivilgesellschaft dient.

Ansprechpartner:

Hochschule Albstadt-Sigmaringen

Anton-Günther-Str. 51

72488 Sigmaringen

cyber-security-center.de

Initiative aus Wirtschaft und Wissenschaft

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Das Forschungsprojekt SENTER (Strengthening European Network Centres of Excellence in Cybercrime) ist ein EU-Projekt des Cyber Security Center mit dem Ziel der Schaffung einer Anlaufstelle sowie eines Netzwerkes nationaler Cybercrime Kompetenzzentren auf europäischer Ebene.

Bildung und Awareness

#Schulung #Awareness in der Politik #Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft #Universitäres Bildungsangebot

Der Fachblog des Cyber Security Center dient der Information und Wissensvermittlung zur Förderung von Awareness. Im Projekt Open C³S (Open Competence Center für Cyber Security) entwickeln bspw. neun deutsche Hochschulen und Universitäten einen berufsbegleitenden Online-Studiengang auf dem Gebiet der Cybersicherheit.

Konzeption und Vorgehensweisen

#Kryptographie #Quanten-Kryptographie & Post-Quanten-Kryptographie #Blockchain #Authentifizierung #Informationssicherheitsmanagement #Endgerätesicherheit #Identitätsmanagement #Berechtigungsmanagement #Compliance Management #Datenschutz #IT-Sicherheitsstandards

Die Hochschule Albstadt-Sigmaringen forscht im gesamten Bereich der Cybersicherheit. Dabei spielt die Anwendungsorientierung eine große und entscheidende Rolle und wird durch die enge Vernetzung mit bekannten Cybersicherheitsfirmen sowie Behörden auf Landes-, Bundes- und Europäischer Ebene realisiert.

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen #Cloudsicherheit #Monitoring

Mit Projekten im Bereich Honey-Nets werden neue Möglichkeiten ML / AI basierter Anomalie- und Angriffserkennung erforscht und erprobt.

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen #Behandlung von Sicherheitsvorfällen & IT-Forensik

Digitale Forensik auf wissenschaftlicher Basis ist ein Kernbereich der Forschung und Ausbildung der Fakultät Informatik. Der berufsbegleitende Masterstudiengang Digitale Forensik feiert 2020 sein 10-jähriges Bestehen. In Kooperation mit der Universität des Saarlandes und der Friedrich-Alexander-Universität Erlangen-Nürnberg wird der Studiengang erfolgreich umgesetzt. Dabei spielt die Forschungsorientierung des Studiengangs eine herausragende Rolle und führt zu international anerkannten Forschungsleistungen (z.B. mehrfache Europäische Polizeipreise).

Infrastrukturelle Sicherheitsaspekte

#Betriebs- und Steuerungstechnik #SPS & ICS #physische IT-Sicherheit

Cybersicherheitsforschung ist besonders im KRITIS-Bereich wichtig. Hier forscht die Hochschule in Kooperation mit lokalen und überregionalen Energieversorgern. Der Bereich Physische- und Embedded/Hardwaresecurity wird aktuell mit einer weiteren dezidierten Professur gestärkt.

Netze und Kommunikation

#Netzarchitektur und -design

Vernetzung von Systemen, IoT

#Smart Home #Autonomes Fahren #Fahrassistenzsysteme #Künstliche Intelligenz

Das Forschungsprojekt SEKT behandelt den Aspekt der IT-Sicherheit von elektronischen Kommunikationssystemen in smarten textilen Produkten zur Entwicklung praxisrelevanter Sicherheitskonzepte. IT-Sicherheit im IoT Bereich wird in Kooperation mit der Fakultät Engineering erforscht, insbesondere spielen auf Informatikseite auch Themen wie XAI, also sichere, erklärbare KI eine große Rolle.

Zielgruppe

Zivilgesellschaft

Der Bereich der wissenschaftlichen Aus- und Weiterbildung wird in einem umfangreichen Portfolio von niederschwelligen Angeboten in Schulen, offenen Vorträgen für Bürgerinnen und Bürger, Kooperationen mit Medien, über ein akademisches Zertifikatsprogramm zur beruflichen Weiterbildung bis hin zu Events für ethisches Hacking intensiv betrieben.

Wissenschaft

Das Cyber Security Center adressiert mit seiner wissenschaftlichen Arbeit Studenten bzw. es bietet eine Plattform zur Veröffentlichung von Abschlussarbeiten. Darüber hinaus sind die Forschungsergebnisse des Cyber Security Center für andere Forschungseinrichtungen von Interesse, bspw. im Rahmen von gemeinsamen Projekten und wissenschaftlichen Netzwerken.

Wirtschaft

Die Auftragsforschung ist zielgruppenneutral und umfasst nahezu all Wirtschaftsbereiche, was in der Natur der Cybersicherheit als Querschnittsdisziplin begründet ist.

Staat

Der Forschungsbereich Cybersicherheit kooperiert sehr eng mit Sicherheits- und Strafverfolgungsbehörden auf Landes-, Bundes- und Europäischer Ebene. Die Hochschule und Mitglieder des Cyber Security Centers sind u.a. Framework Partner von CEPOL, Gründungsmitglied von ECTEG.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Ausbildung und Schulung
- Beratung
- Entwicklung
- Konzept
- Sonstige Dienstleistung

Das Cyber Security Center ist in die Lehre an der Hochschule Albstadt-Sigmaringen eingebettet. Zu seinen Dienstleistungen gehört auch Auftragsforschung für die Wirtschaft.

Information

- Informationsaufbereitung
- Journalismus
- Blog
- Öffentlichkeitsarbeit
- Wissenschaftliche Veröffentlichung
- Studie

Das Cyber Security Center stellt in einem Fachblog aktuelles Wissen im Bereich der Cybersicherheit bereit. Im Rahmen verschiedener Forschungsprojekte werden wissenschaftliche Veröffentlichungen publiziert und die Vernetzung auf nationaler und europäischer Ebene betrieben.

Cyber Security Rumble e.V.

Beitrag zur Cybersicherheit

Der Cyber Security Rumble ist eine Initiative der NVISO GmbH in Kooperation mit der Hochschule Bonn-Rhein-Sieg, der Universität Bonn und dem SANS Institut. In einem Cybersicherheits-Wettbewerb können Studierende und Experten in Teams gegeneinander antreten. Nach einer Qualifizierungsrunde werden die besten Teams zu einem Event vor Ort eingeladen, um im Finale gegeneinander anzutreten. Der Wettbewerb wurde zunächst 2015 in Belgien initiiert. Aufgrund der steigenden Nachfrage wurde 2019 eine ähnliche Initiative in Deutschland gestartet, die mit dem Cyber Security Rumble 2020 in seine zweite Auflage geht.

Kontakt:

Am Hopfengarten 22

60489 Frankfurt am Main

cybersecurityrumble.de

Initiative aus Wirtschaft und Wissenschaft

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Durch den Wettbewerb können die Teilnehmer der Initiative mit verschiedenen Unternehmen, Hochschulen und Institutionen (wie bspw. dem Bundesamt für Sicherheit in der Informationstechnik) in Kontakt treten.

Konzeption und Vorgehensweisen

Für Zwecke des Wettbewerbs werden von der Initiative verschiedenartige Aufgaben zu den relevanten Themen der Cybersicherheit entwickelt. Verschiedene studentische Teams treten nach dem Prinzip von „Capture The Flag“ gegeneinander an und müssen Aufgaben aus dem Cybersicherheitsumfeld mit unterschiedlichem Schwierigkeitsgrad lösen.

Zielgruppe

Zivilgesellschaft

Zielgruppe des Wettbewerbs der Initiative sind Studierende.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

Durch den fachlichen Wettbewerb in der Spielsituation offenbaren die Teilnehmenden ihre Kenntnisse zu den aufgerufenen Themenfeldern der Cybersicherheit. Auf dieser Grundlage entstehen Opportunitäten zum Aufbau von Karriere- und Fachnetzwerken. Für die Partner des Cyber Security Rumble aus Wissenschaft, Wirtschaft und Verwaltung eröffnet sich die Möglichkeit zur Gewinnung von künftigem Fachpersonal und Wissenschaftsnachwuchs.

eurobits e.V. – Europäisches Kompetenzzentrum für IT-Sicherheit Bochum

Beitrag zur Cybersicherheit

eurobits e.V. vereint seit 1999 Forschungsinstitute sowie Unternehmen aus den Bereichen IT- und Informationssicherheit und ist Ansprechpartner für Anfragen zu aktuellen IT-Sicherheitsthemen mit technologischem, wirtschaftlichen und wissenschaftlichem Bezug. Zudem bietet eurobits e.V. ein weit gefächertes Angebot an wissenschaftlichen Studiengängen und zertifizierten Weiterbildungsangeboten. Die Aktivitäten von eurobits zielen auf die Lückenschließung zwischen wissenschaftlicher technologischer Innovation hin zu anwendbaren Produkten ab. Die zunehmend wichtige Balance zwischen Technik und Mensch spiegelt sich in den Mitgliedsunternehmen von eurobits wider.

Kontakt:

Lise-Meitner-Allee 4

44801 Bochum

eurobits.de

Initiative aus Wirtschaft und Wissenschaft

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Die Initiative verbindet Akteure aus Wissenschaft, Wirtschaft und Behörden aus der Region Ruhr. Security-Forscher und Anbieter von Cyber-Sicherheitslösungen treffen Anwender aus allen Unternehmensbereichen und erarbeiten adäquate Lösungsansätze für aktuelle Bedrohungen. Darüber hinaus werden Kontakte zu anderen europäischen Regionen und Organisationen aufgebaut, um die entwickelten Lösungen auch in anderen Regionen Europas zu vermarkten.

Bildung und Awareness

#Schulung #Awareness in der Politik #Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft #Berufliches Bildungsangebot #Universitäres Bildungsangebot #Sonstiges Bildungsangebot

Mitglieder des Netzwerks bieten verschiedene Studien- und Weiterbildungsmöglichkeiten zur IT-Sicherheit und Informationssicherheit an. Mehrere Mitglieder haben eigene Angebote zu Awarenessschulungen und viele bilden aus.

Konzeption und Vorgehensweisen

#Kryptographie #Quanten-Kryptographie & Post-Quanten-Kryptographie #Authentifizierung #Informationssicherheitsmanagement #Datenschutz #IT-Sicherheitsstandards

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen #Cloudsicherheit

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen #Behandlung von Sicherheitsvorfällen & IT-Forensik

Infrastrukturelle Sicherheitsaspekte

#Betriebs- und Steuerungstechnik #SPS & ICS #Intelligente Messsysteme #RZ-Infrastruktur #physische IT-Sicherheit

Netze und Kommunikation

#Netzarchitektur und -design #Netzkomponenten #Funknetze

Vernetzung von Systemen, IoT

#Smart Home #Autonomes Fahren #Fahrassistenzsysteme #Künstliche Intelligenz

Zielgruppe

Wirtschaft

Ziel der Initiative ist der Technologietransfer im Bereich der IT-Sicherheit und Informationssicherheit zwischen Wissenschaft und Wirtschaft.

Staat

eurobits e.V. und seine Mitglieder sind in vielfältiger Weise mit staatlichen Organisationen vernetzt.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Ausbildung und Schulung
- Beratung
- Konzept
- Prüfung/Audits/Zertifizierung/Standardisierung
- Sonstige Dienstleistung

Es wird eine Preisverleihung für besonders gute Abschlussarbeiten im Bereich IT-Sicherheit durchgeführt. Außerdem beteiligt sich eurobits an verschiedenen Veranstaltungen und Messen. Mitglieder des Netzwerkes bieten Studien- und Weiterbildungsmaßnahmen zur IT-Sicherheit und Informationssicherheit an.

Information

- Informationsaufbereitung
- Lernprogramm
- Öffentlichkeitsarbeit
- Wissenschaftliche Veröffentlichung
- Studie

Sowohl eurobits selbst als auch seine Mitgliedsunternehmen bieten vielfältige Informationsmaterialien und Ausbildungsprogramme im Bereich IT-Sicherheit.

Freies Institut für IT-Sicherheit e.V. (IFIT)

Beitrag zur Cybersicherheit

Das IFIT ist ein Netzwerk aus Anwendern, Anbietern und wissenschaftlichen Einrichtungen des Themenbereichs IT-Sicherheit in der Region Nord-West-Deutschland. Das Ziel ist der Austausch über aktuelle Themen der Cybersicherheit zur Steigerung des Sicherheitsniveaus. Hierzu werden Veranstaltungen organisiert, Forschungs- und Entwicklungsprojekte unterstützt sowie die Zusammenarbeit der Mitglieder in Fachgruppen u.a. zu Industrial Security oder Datenschutz ermöglicht. Weiterhin zählt die Vermittlung von Experten, Ansprechpartnern und Beratungsdienstleistern zum Angebotsspektrum.

Kontakt:

Karl-Grunert-Str. 68

28277 Bremen

ifitev.de

Initiative aus Wirtschaft und Wissenschaft

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Innerhalb des Kompetenznetzwerkes des IFIT haben die Mitglieder die Möglichkeit sich zu Themen der IT-Sicherheit zu vernetzen und auszutauschen, aber auch mit neuen Akteuren in Kontakt zu treten. Bspw. auf ausgerichteten Konferenzen mit Netzwerkcharakter, wie den Bremer Security Foren oder den Security Days. Das IFIT ist zudem Multiplikator der ACS und der Gesellschaft für Datenschutz und Datensicherheit (GDD).

Bildung und Awareness

#Schulung #Awareness in der Wirtschaft

Vom IFIT werden vorwiegend Veranstaltungen, Konferenzen und Foren zu aktuellen Fachthemen organisiert. Die Sensibilisierung für einen sicheren Umgang mit Informations- und Kommunikationstechnik, bspw. durch Informationen über vorbeugende Maßnahmen, Gefahrenabwehr oder zur Minimierung der Auswirkung entstandener Schäden stehen hierbei im Fokus.

Zielgruppe

Zivilgesellschaft

- Akademikerinnen und Akademiker
- Angestellte

Neben Veröffentlichungen sind Angebote wie das IFIT-Sicherheitstelefon für Unternehmen und Institutionen nutzbar.

Wirtschaft

Die Angebote des IFIT richten sich an Unternehmen aus allen Branchen.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Ausbildung und Schulung
- Beratung

IFIT organisiert Weiterbildungen in Form von Seminaren, Trainings oder Konferenzen. Zusätzlich werden Beratungsdienstleistungen und Sicherheitschecks vermittelt, die von den Mitgliedsunternehmen durchgeführt werden.

Information

- Informationsaufbereitung
- Newsletter

Für Mitglieder stehen Newsletter und Sicherheitsinformationen zur Verfügung, außerdem besteht die Möglichkeit der Teilnahme und Zusammenarbeit mit anderen Mitgliedern in Fachgruppen.

nrw.uniTS

Beitrag zur Cybersicherheit

Das Netzwerk nrw.uniTS dient der Kooperationsförderung aller Akteure im Bereich der IT-Sicherheit in Nordrhein-Westfalen. Die Initiative hat das Ziel, Unternehmen gegen Sicherheitsrisiken vorzubereiten, Wissenschaft und Wirtschaft zu verbinden und aktuelle Trends der IT-Sicherheit zu begleiten. Das Projekt wird vom HGI der Universität Bochum getragen.

Ansprechpartner:

Horst Görtz Institut für IT-Sicherheit der Ruhr-Universität Bochum

Universitätsstr. 150

44801 Bochum

nrw-units.de

Initiative aus Wirtschaft und Wissenschaft

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

nrw.uniTS verknüpft Kontakte und Wissen von Einzelunternehmen und wissenschaftlichen Akteuren in Nordrhein-Westfalen.

Konzeption und Vorgehensweisen

Derzeit existieren thematisch verschiedene Arbeitsgruppen von nrw.uniTS, in denen Workshops durchgeführt und Whitepaper entwickelt werden. Die Arbeitsgruppe "Industrie 4.0" bietet Unternehmen Informationen und Hilfe zu IT-Sicherheits- und Datenschutzaspekten im Kontext der Industrial IT Security. Die Kompetenzgruppe "Managementsysteme" hingegen unterstützt Unternehmensleitungen bei der Erkennung, Bewertung und Bewältigung von IT-Risiken. Eine Fachgruppe "e-health" verfolgt das Ziel, für IT-Sicherheit im Gesundheitswesen zu sensibilisieren und konkrete Handlungsempfehlungen auszusprechen. Die Arbeitsgruppe "Websicherheit" stellt wiederum praktische Informationen zum Schutz von Web-Server-Infrastrukturen und Web-Clients zur Verfügung. Auch zu rechtlicher Beratung im Themenfeld IT-Recht sowie zum Themenbereich Datenschutz stehen zwei thematische Arbeitsgruppen den Unternehmen zur Unterstützung zur Verfügung.

Zielgruppe

Wirtschaft

Das Angebot von nrw.uniTS richtet sich branchenunabhängig an Unternehmen sowie an wissenschaftliche Einrichtungen.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Information

- Informationsaufbereitung
- Wissenschaftliche Veröffentlichung
- Studie

nrw.uniTS stellt Informationen zu Sicherheitsrisiken, Schutzmaßnahmen, aktuellen Trends und Zukunftsperspektiven im Bereich IT-Sicherheit bereit und bietet darüber hinaus Fachvorträge, Workshops und Netzwerkmöglichkeiten an. Die Inhalte sind dabei abhängig von der bereitstellenden Arbeitsgruppe und decken ein breites Spektrum zur IT-Sicherheit ab.

Sichere Webseiten und Content Management Systeme (SIWECOS)

Beitrag zur Cybersicherheit

SIWECOS ist eine Initiative zur Unterstützung von KMU zu IT-Sicherheitsthemen. Konkret sollen Sicherheitslücken auf deren Webseiten erkannt und behoben werden. Bspw. werden mithilfe einer Anwendung die Serversysteme der Unternehmen nach Sicherheitslücken durchsucht. Eine zweite Anwendung informiert das Unternehmen im Anschluss über identifizierte Sicherheitslücken, was dazu führt, dass das Unternehmen so frühzeitig Cyberangriffe unterbinden kann. Hierdurch soll auch das IT-Sicherheitsbewusstsein bei KMU gesteigert werden. SIWECOS ist ein Projekt des eco - Verband der Internetwirtschaft e.V. und wurde durch das BMWi im Rahmen der Initiative "IT-Sicherheit in der Wirtschaft" gefördert. Darüber hinaus sind mehrere wissenschaftliche und wirtschaftliche Kooperationspartner am Projekt beteiligt, darunter auch die Ruhr-Universität Bochum.

Ansprechpartner:

eco - Verband der Internetwirtschaft e.V.

Lichtstr. 43h

50825 Köln

siwecos.de

Initiative aus Wirtschaft und Wissenschaft

Thematische Schwerpunkte (Auszug)

Bildung und Awareness

#Awareness in der Wirtschaft

SIWECOS verfolgt das Ziel, das Bewusstsein für die Relevanz von IT-Sicherheit für KMU zu verstärken und gibt ihnen ein Werkzeug an die Hand um Sicherheitslücken auf ihren Webseiten zu erkennen und zu beheben.

Detektion und Reaktion

#Detektion von sicherheitsrelevanten Ereignissen
#Behandlung von Sicherheitsvorfällen & IT-Forensik

Mithilfe von konkreten Maßnahmen werden Unternehmen bei diversen Themen im Bereich Cybersicherheit unterstützt. Hierzu bietet SIWECOS den Unternehmen bspw. Sicherheitsscans deren Webseiten an oder spricht individuelle Handlungsempfehlungen zu Sicherheitsbedenken aus.

Zielgruppe

Wirtschaft

SIWECOS sensibilisiert KMU hinsichtlich der Relevanz von IT-Sicherheit und bietet hierzu konkrete Unterstützung an. Dadurch soll nachhaltig die Sicherheit beim Betrieb von Webseiten erhöht werden. Außerdem sollen die Unternehmen dazu befähigt werden, auf Augenhöhe mit IT-Dienstleistern zu kommunizieren.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

Das Angebot von SIWECOS umfasst verschiedene Sicherheitsscans von Webseiten und Content Management Systemen (CMS), sowie einen detaillierten Report, welcher identifizierte Sicherheitslücken bewertet und aufzeigt. Hier werden sowohl die Einstellungen des Webservers als auch Patchstände von CMS und von diesen verwendeten Plug-Ins überprüft und durch ein Scoring bewertet. Ein Service für Webhoster kommuniziert aktiv akute Sicherheitslücken und bietet Filtermöglichkeiten an, um Cyberangriffe bereits zu stoppen, bevor sie den Kunden erreichen.

Information

Zusätzlich zu allgemeinen Informationen zum Betrieb von Webseiten werden in einem Wiki verschiedene Informationen zur Webseitensicherheit, Umsetzung verschiedener Einstellungen mit Beispielen, nähere Details zu den Tools sowie Erläuterungen der verwendeten Begrifflichkeiten bereitgestellt. Bei Fragen zu einzelnen Sicherheitslücken oder zum Projekt im Allgemeinen bietet SIWECOS Hilfestellung per Mail an.

Verband Sichere Digitale Identität e.V. (VSDI)

Beitrag zur Cybersicherheit

Der VSDI ist das bundesweite Netzwerk für Unternehmen, Hochschulen und Forschungseinrichtungen, dass die Transformation von analogen zu digitalen Identitäten vorantreibt. Die Mitglieder arbeiten diesbezüglich an der Entwicklung eines ganzheitlichen Konzepts sowie den dafür notwendigen Lösungen und Produkten. Der Verband vermittelt die gebündelte Expertise seiner Mitglieder und tritt durch seine Initiativen dafür ein, sichere, nutzerfreundliche und datenschutzkonforme digitale Identitäten zu ermöglichen.

Kontakt:

Kommandantenstr. 18

10969 Berlin

vsdi.de

Initiative aus Wirtschaft und Wissenschaft

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Verband Sichere Digitale Identität steht als zentrale Anlaufstelle zum Thema sicherer, digitaler Identitäten zur Verfügung. Ziel der Initiative ist die Förderung des Austausch sowie die Vermittlung und Vernetzung der Mitglieder. Das Netzwerk setzt sich aus Unternehmen, Hochschulen und Forschungseinrichtungen zusammen und möchte die Expertise des Netzwerks gegenüber der Politik, Verwaltung und Wirtschaft repräsentieren und zur Schaffung von sicheren digitalen Identitäten beitragen.

Bildung und Awareness

#Awareness in der Politik #Awareness in der Zivilgesellschaft #Awareness in der Wirtschaft

Die Aktivitäten der Initiative sollen die Bedeutung sicherer digitaler Kommunikation unterstreichen und die Politik auffordern, nötige Rahmenbedingungen für digitale Identitäten zu schaffen. Dabei soll die Expertise der Wirtschaft genutzt werden und die Weiterentwicklung sicherer digitaler Identitäten staatlich gefördert werden.

Konzeption und Vorgehensweisen

#Kryptographie #Blockchain #Authentifizierung #Informationssicherheitsmanagement #Endgerätesicherheit #Identitätsmanagement #Berechtigungsmanagement #Datenschutz #IT-Sicherheitsstandards

Verband Sichere Digitale Identität e.V. setzt sich mit seinen Aktivitäten für die Entwicklung von sicheren digitalen Identitäten als Grundlage für eine sichere Vernetzung ein.

Betriebsbezogene Sicherheitsaspekte

#Schutz vor Angriffen #Cloudsicherheit

Infrastrukturelle Sicherheitsaspekte

#physische IT-Sicherheit

Vernetzung von Systemen, IoT

#Künstliche Intelligenz

Zielgruppe

Wirtschaft

Die Forderungen und Ziele des Vereins zielen auf die Schaffung sicherer digitaler Identitäten ab, wovon jeder Internetnutzer, die Wirtschaft aber auch die Politik profitieren können.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Beratung

Verband Sichere Digitale Identität berät die Bundespolitik zum Thema sichere Identitäten in der digitalen Transformation.

Information

- Informationsaufbereitung
- Lernprogramm
- Öffentlichkeitsarbeit

Auf der Webseite werden grundlegende Informationen rund um das Thema sicherer Identitäten zur Verfügung gestellt. Weiterhin werden im Rahmen eines Online-Spiels Tipps zu Maßnahmen und Verhaltensregeln zur Verbesserung der IT-Sicherheit vermittelt. Außerdem bündelt der Verband auf der Webseite sämtliche Veranstaltungen seiner Mitglieder und Partnerorganisationen sowie generelle Veranstaltungen zu Themen der Sicheren digitalen Identität in Form eines Terminkalenders. Zusätzlich präsentiert der Verband Sichere Digitale Identität sich regelmäßig auf verschiedenen Veranstaltungen.

8.8 Initiativen aus Wissenschaft und Staat

Digital Hub Cybersecurity

Beitrag zur Cybersicherheit

Der Digital Hub Cybersecurity ist Teil der Digital Hub Initiative der Bundesregierung, die Deutschland digital stärken und als Standort etablieren soll. Träger des Digital Hub Cybersecurity sind das Fraunhofer SIT, die TU Darmstadt, die IHK Darmstadt und die Stadt Darmstadt. Der Digital Hub Cybersicherheit unterstützt und berät Start-ups der Cybersicherheitsbranche durch Coachings und bringt diese mit mittelständische Unternehmen sowie Konzerne zusammen. Der Digital Hub Cybersecurity vernetzt wirtschaftliche und wissenschaftliche Akteure und erzielt somit auch eine Sensibilisierung im Bereich der Cybersicherheit.

Kontakt:

Rheinstr. 75

64295 Darmstadt

digitalhub-cyber-security.com

Initiative aus Wissenschaft und Staat

Thematische Schwerpunkte (Auszug)

Vernetzungs- und Multiplikatorfunktion

#Vernetzung & Multiplikator

Der Digital Hub Cybersecurity nutzt sein breitgefächertes Netzwerk um Gründer, Wissenschaft und etablierte Unternehmen zusammen zu bringen.

Bildung und Awareness

#Awareness in der Wirtschaft

Neben vernetzenden Aktivitäten dient der Digital Hub Cybersecurity auch der Schaffung von Awareness bei Investoren, Stakeholdern oder Influencern.

Zielgruppe

Wirtschaft

Das Angebot des Digital Hub Cybersecurity richtet sich an Start-ups im Bereich IT-Sicherheit, aber auch an etablierte Unternehmen, die sich der IT-Sicherheit im Kontext der Digitalisierung annehmen möchten.

Der Akteur liefert einen Beitrag durch folgendes Angebot

Dienstleistung

- Beratung

Der Digital Hub Cybersecurity unterstützt Start-ups der IT-Sicherheitsbranche bei der Kommerzialisierung, Skalierung und Internationalisierung. Außerdem werden Coachings angeboten.

Information

- Informationsaufbereitung

Der Digital Hub Cybersecurity organisiert regelmäßig Veranstaltungen zu relevanten Themen der Cybersicherheit und zur Netzwerkbildung.

9 Anhang

Auflistung betrachteter Organisationen

"Accenture ICS Cybersecurity" Accenture Dienstleistungen GmbH

"Bundesarbeitsgruppe Cybersicherheit" Wirtschaftsrat der CDU e.V.

"Cybermentor" Universität Regensburg

"Fachausschuss Cybersicherheit" Bundesverband der Deutschen Luft- und Raumfahrtindustrie e.V.

"IT-Sicherheit @ Mittelstand" Deutschland sicher im Netz e.V.

"Komm mach MINT – Nationaler Pakt für Frauen in MINT-Berufen" Kompetenzzentrum Technik-Diversity-Chancengleichheit e.V.

"Koordinierungsstelle KITS" DIN e.V.

"Mint Zukunft Schaffen" c/o Factory Works GmbH

"PITS" ProPress Verlagsgesellschaft m.b.H.

"Programm Exzellenzzentren an Berufsschulen" Bayerisches Staatsministerium für Unterricht und Kultus

"Projektgruppe Digitale Agenda Referat 16" Ministerium für Wirtschaft, Wissenschaft und Digitalisierung

des Landes Sachsen-Anhalt

"Serious Games" - Forschung an der Hochschule Wildau

"Sicherheitsforum Baden-Württemberg" Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg

"Sicherheitspartnerschaft NRW" Ministerium des Innern des Landes Nordrhein-Westfalen

"Wilhelm Büchner Hochschule" Hochschule für Berufstätige Darmstadt GmbH

.DEB UG (haftungsbeschränkt)

@bc® - Arendt Business Consulting

[Mer] Curius

12 Tower GmbH

1600 Cyber International GmbH

1984not Security GmbH

21unity GmbH

23plus1 Entwicklungs und Service UG

34digital GmbH

3GRC GmbH

8com GmbH & Co. KG

8S IT-Sicherheit e.K.

8Soft GmbH

9elements Agency GmbH

A.Hock MSR- und Electronic Service GmbH

a.s.k. Datenschutz

a.s.k. Datenschutz e.K.

A'PARI Consulting GmbH i.L.

a1 Digital Deutschland GmbH

Aachener Verlagsgesellschaft mbH

Aagon GmbH

AB Datenschutz UG (haftungsbeschränkt)

abat AG

ABB Deutschland

abl social federation GmbH

ACACIA Integration GmbH

Accellence Technologies GmbH

accessec GmbH

ACENT AG

achelos GmbH

Achtwerk GmbH & Co. KG

acmeo GmbH

ACP Holding Deutschland GmbH

Acronis Germany GmbH

Actisis GmbH

activeMind AG Management- und Technologieberatung

Ada Pellert

Ada-Lovelace-Projekt

Adaptron GmbH Solution Technology

Adazims UG (haftungsbeschränkt)

ADDIX Internet Services GmbH

adfidetia GmbH

Adiccon GmbH

admeritia GmbH

AdRem GmbH

ADVA Optical Networking SE

Advanced UniByte GmbH

advanto Software GmbH

Advidera GmbH & Co. KG

ADVISORI FTC GmbH

ADVOCARD Rechtsschutzversicherung AG

AEBERHARD Consulting GmbH

AERAsec Network Services and Security GmbH

AG KRITIS

Agentur für Innovation in der Cybersicherheit (Cyberagentur)

aggeris GmbH -it-sicherheitsberatung

AIA AG

Aidentity Data Protection UG (haftungsbeschränkt) c/o Eva Oertwig

AIG Europe S.A

AimBusiness GmbH

Airbus SE

AirITSystems GmbH

AIRNET Information Security Services GmbH

AIT Goehner GmbH

AIV Architekten- und Ingenieur-Versicherungsdienst GmbH & Co KG

AK GmbH, Beratungsgesellschaft Ader u. Kiupel GmbH

Akamai Technologies GmbH

Aktionsbund Digitale Sicherheit

aktiv gGmbH

aktiv-online.de

AL Datenschutz e.K

AL Project Security GmbH

Albert-Ludwigs-Universität Freiburg

albfinanz GmbH

Aletheia DS GmbH

Alexander Paharukov

Alexander von Humboldt Institut für Internet und Gesellschaft gGmbH

Alfahosting GmbH

Allar Networks & Consulting GmbH

Allgeier CORE Group GmbH

Allianz Deutschland AG

Allianz für Cyber-Sicherheit (ACS)

Allianz Industrie 4.0

ALLYSCA Assistance GmbH

Alpha-Soft Computer Security GmbH

Alphasozial UG (haftungsbeschränkt)

AlphaWin Hard- und Software GmbH

Alsterspree Verlag GmbH

Alter Solutions Deutschland GmbH

Althammer & Kill GmbH & Co. KG

AmiSysCon GmbH

AMS-develop e.K. Inhaber Eric Pannek

anapur AG

Andermann & Partner GmbH

Andreas Durnio Datenschutz & IT-Beratung

Andreas Hämmerle IT-Dienstleistungen

Andreas Hessel

Andreas Kunz EDV-Dienstleistungen

Andreas Mroß IT-Service und Beratung

Andreas Schleicher

Andreas Spindler -IT-Service-

Anglepoint Group (Germany) GmbH

Anmatho AG

Antago GmbH

Antares Computer Verlag GmbH

antares Informations-Systeme GmbH

AnTeCoS GmbH

Antispam e.V.

anykey GmbH

AOK-Bundesverband GbR

ap Verlag GmbH

apia systemhaus GmbH

apparet IT GmbH & Co. KG

Applied Security GmbH

APRO.GmbH Computer und Dienstleistung

aramido GmbH

Arbeitsgemeinschaf lebenslanges Lernen

Arbeitsgruppe "Multimedia and Security"

Arbeitsgruppe „Sicherheit Vernetzter Systeme“ - Plattform Industrie 4.0

Arbeitskreis "IT-Security" Digital Agentur Niedersachsen

Arbeitskreis Informationssicherheit der deutschen Forschungseinrichtungen (AKIF)

Argus Cyber Security Ltd. (Argus)

Arnd Noack Beratung IT-Mentoring

Arnold van Zyl

ARP GmbH

Arrow ECS GmbH

ARS NOVA Software GmbH

ARTADA GmbH

ARTEC IT Solutions AG

AsBo SpezialMakler GmbH

Ascora GmbH

ASIGEST Deutschland Versicherungsmakler GmbH

ASOFTNET

Assekuranz-Vermittlungs-Aktiengesellschaft Versicherungsmakler

Astica Consult GmbH

ASW Bundesverband

Allianz für Sicherheit in der Wirtschaft e.V.

ASW West - Allianz für Sicherheit in der Wirtschaft West e.V. (ASW West e.V.)

atarax GmbH & Co. KG

Atos Information Technology GmbH

atsec information security GmbH (atsec)

audius AG

AuraSec GmbH

ausecus GmbH

Auswärtiges Amt

AUTHADA GmbH

Autonubil System GmbH

Avast Deutschland GmbH (Avast)

AVG Deutschland GmbH (AVG)

AVi GmbH Service für Unternehmen

Avira Operations GmbH & Co. KG (Avira)

AV-TEST GmbH

AWARE7 GmbH

AXA Konzern Aktiengesellschaft

Axel Springer SE

AXSOS AG

ayway media GmbH

B&C BüroCommunikation

B³ | Informationstechnologie

B4Bmedia.net AG

Badger Systems GmbH

BankenService.Berlin GmbH

BANKINGCLUB GmbH

Bank-Verlag GmbH

baramundi software AG

Baris Sariyildiz "IT Ärzte Computerspezialisten"

Barmenia Allgemeine Versicherungs-AG

BARMER

Baru Systems

BASECAMO - Debattenraum und Public-Affairs-Blog von Telefónica Deutschland

Batix Software GmbH

BavariaDirekt eine Marke der OVAG - Ostdeutsche Versicherung Aktiengesellschaft

Bayer. Staatsministerium des Innern, für Sport und Integration

IT-Sicherheitscluster e.V.

Bayerisches Landesamt für Verfassungsschutz (BayLfV)

Bayerisches Staatsministerium der Finanzen und für Heimat

Bayerisches Staatsministerium des Innern, für Sport und Integration

bbg Betriebsberatungs GmbH

BBIT-Solutions UG (haftungsbeschränkt)

BB-ONE.net Ltd

bc digital GmbH

BCC Unternehmensberatung GmbH

BCS Bartels Computer Systeme GmbH

BDO Cyber Security GmbH

BDO Legal Rechtsanwaltsgesellschaft mbH

BDT-Media UG (haftungsbeschränkt)

Bechtle AG

becon GmbH

Benjamin Ehlers e.K

Benjamin-Franklin-Schule

BEO GmbH

berasec GmbH

Bergische Universität Wuppertal

BerIsDa GmbH

BerlinOnline Stadtportal GmbH & Co. KG

Bernd Abelmann

Bernd Christian Wege "Info Tech by DCS"

Bernd Frenz

Bernd Lothar Stange Computer Sofort Hilfe

BERNHARD Assekuranzmakler GmbH & Co. KG

Bernhard Brands

Berufsbildungswerk der Deutschen Versicherungswirtschaft (BWV) e.V.

Berufskolleg Wirtschaft und Verwaltung mit Wirtschaftsgymnasium

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Besim Karadeniz

be-solutions GmbH

best-practice innovations GmbH

Beta Systems IAM Software AG

Bettina Schramm

Beuth Hochschule für Technik Berlin

BF IT-Consulting GbR

BFK edv-consulting GmbH

Bildungswerk der Erzdiözese Köln e.V

Bindt Systems GmbH

binsec GmbH

biogoo.org

bit2.me GmbH

Bitdefender GmbH

Biteno GmbH

bitfire GmbH

bitformer GmbH

bitinspect GmbH

BITMARCK Holding GmbH

BITS Bernhardt IT Solutions GmbH

Bits For Future GmbH

BITsic GmbH

Bitstore IT-Consulting GmbH

BlackBerry Deutschland GmbH

Blackfort Technology Unternehmergesellschaft (haftungsbeschränkt)

Blinde Kuh e.V

Blitznote e.K.

Blockchain Bundesverband e.V.

Blockchain Competence Center Mittweida der Hochschule Mittweida

blu Gruppe AG

BNT GmbH

BÖCKER ZIEMEN GmbH & Co. KG

Bohnen IT GmbH

BonSure GmbH

Booz Allen Hamilton Inc. (BAH)

BorgWarner IT Services Europe GmbH

Borns Schüler Grund GbR

Boston Consulting Group GmbH

bpi solutions gmbh & co. kg

Brain Medien Dienste

Brainloop Aktiengesellschaft

BRANDCODE GmbH

Brandenburgische Technische Universität

Brandmauer IT GmbH

BREDEX GmbH

Breuer Cyber- und Datensicherheit

bridge4IT® e.K.

Bromund & Alef Gesellschaft für Informationstechnologie mbH

BSI für Bürger

BSI Group Deutschland GmbH

BSK Consulting GmbH

BSP-SECURITY

BSS BuCET Shared Services AG (BSS)

BTC Business Technology Consulting AG

BTS Bahntechnik Sachsen e.V.

Bugan IT Consulting UG (haftungsbeschränkt)

BULPROS

Bundesagentur für Arbeit (BA)

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Bundesdruckerei GmbH

Bundesfachverband der IT-Sachverständigen und Gutachter e.V

Bundeskriminalamt

Bundesmininsterium für Bildung und Forschung

Bundesministerin der Justiz und für Verbraucherschutz

Bundesministerium für Bildung und Forschung

Bundesnachrichtendienst (BND)

Bundesnotarkammer K.d.ö.R.

Bundesprüfstelle für jugendgefährdende Medien (BPjM)

Bundesregierung

Bundesverband der Deutschen Industrie e.V. (BDI)

BUNDESVERBAND DER DEUTSCHEN LUFT- UND RAUMFAHRTINDUSTRIE E.V. (BDLI), MESSE BERLIN GMBH

Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie (BDSV) e.V.

Bundesverband der IT-Anwender e.V.

Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. (vzbv)

Bundesverband Deutsche Startups e.V.

Bundesverband deutscher Banken e.V. (Bankenverband)

Bundesverband Deutscher Innovations-, Technologie- und Gründerzentren e.V. (BVIZ)

Bundesverband Frauenberatungsstellen und Frauennotrufe Frauen gegen Gewalt e.V (bff).

Bundesverband für den Schutz Kritischer Infrastrukturen e.V.

Bundesverband Gewaltprävention "Selbstbewusst & Stark e.V."

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom)

Bundesverband IT-Mittelstand e.V. (BITMi)

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Bundesverfassungsgericht

Bundeszentrale für politische Bildung (bpb)

Bündnis gegen Cybermobbing e.V.

Bürotechnik Nord GmbH

BÜROTEX metadok GmbH

Burt Daten- und Sicherungssysteme GmbH

BÜSCHEL Consulting für Datenschutz und Informationssicherheit

Business Academy Ruhr GmbH

Business IT Nord GmbH

Business.today network GmbH

BVMW - Bundesverband mittelständische Wirtschaft,

Unternehmerverband Deutschlands e.V.

BWI GmbH

b-wise GmbH

ByteStudio Unternehmergesellschaft (haftungsbeschränkt)

C&H Gesellschaft für Informationstechnologie mbH

Cactus eSecurity GmbH

Caemmerer Lenz

CamData GmbH

CANCOM SE

CAPCAD SYSTEMS AG

Cari GmbH

Carl Hanser Verlagsleitungsges. mbH

Carl-Friedrich-Gauß-Gymnasium

CARMAO GmbH

CASA: Cybersicherheit im Zeitalter großskaliger Angreifer

Caschys Blog

Cavalry GmbH

CBO Cani Blue-Ocean UG (haftungsbeschränkt)

CBO-Dienstleistungen GmbH

CBT Training & Consulting GmbH (CBT)

CBXNET combox internet GmbH

CCC City Computer Contor GmbH

CCVOSSEL GmbH

cdt digital GmbH

CEMA AG Spezialisten für Informationstechnologie (CEMA)

centron GmbH

Ceramex Media GmbH

CertCenter AG

Certgate GmbH

CERTIVATION GmbH

CERTIX IT-Security GmbH

CERT-Verbund

CertVision GmbH

Chair of Mobile Business & Multilateral Security (M-Chair)

Chaos Computer Club e.V. (CCC)

Chaos macht Schule

Cherry GmbH

Chiffry GmbH

Chilian IT GmbH

CHIMERCIAL GmbH

CHIP Digital GmbH

Christian J. Heining

Christian Kendi Iron Software

Christian Rödl

Christian Schülke

Christian Stobitzer

Chubb European Group SE

C-IAM GmbH

CIMAP GmbH

CIO Solutions GmbH

CIPHRON GmbH

Cisco Systems GmbH

Clearswift Deutschland

clever + smart administration UG (haftungsbeschränkt)

Cloudsitter GmbH

CM Systemhaus GmbH

CMS IT-Consulting GmbH

CND Computer und Netzwerk Dienstleistungen GmbH (CND)

co.met GmbH

COC AG

CoCoNet Computer-Communication Networks GmbH

COCUS NEXT GmbH

COGITANDA Risk Prevention GmbH

Cognitec Systems GmbH

Collegium Auditores GmbH

ColocationIX GmbH

Comarch AG

COMback GmbH

ComCode GmbH

ComConsult GmbH

comdatis it-consulting GmbH & Co. KG

Comlike Inh. John Chatfield e.K.

Comma Soft AG

commercetools GmbH

Communications & Network Consulting AG

Companity GmbH & Co KG

Compass Security Deutschland GmbH

COMPENDIUM GmbH

Competence Center for Applied Security Technology e.V. (CAST)

complimant AG

comply25 GmbH

Computacenter AG & Co. oHG

Computer Manufaktur GmbH

concentrade GmbH

Concept Heidelberg GmbH

Concepture Gruppe GmbH

CONET Technologies Holding GmbH

Confident Data GmbH

ConnecT Informationstechnik GmbH

Connecting Media – Andreas Kunz

conpal GmbH

ConProTech UG (haftungsbeschränkt)

consecco business.security.management c.g.aust GbR

Consist Software Solutions GmbH

consult GmbH

consulting1x1 GmbH

CONTECHNET Deutschland GmbH

Context Information Security GmbH

Continental Teves AG & Co.oHG

Controlware GmbH Kommunikationssysteme

Corporate Trust Business Risk & Crisis Management GmbH

Correct Power Institute GmbH

co-si-ma UG (haftungsbeschränkt)

Cosmos Versi-che-rung Akti-en-ge-sell-schaft

CPP Creating Profitable Partnerships GmbH (CCP)

CPS.HUB NRW - Competence Center for Cyber Physical Systems

Crashtest Security GmbH

Crede Experto IT Solutions GmbH

Creditplus Bank AG

Crissy Field GmbH

CRONIQ Ingenieurgesellschaft mbH

CrowdStrike GmbH

CryptoMagic GmbH

CrypTool Portal

CryptoTec AG

CSB Computer und Netzwerk Systeme GmbH

CSM MeinSystemhaus GmbH & Co. KG

CSM MeinSystemhaus GmbH & Co. KG

CSO GmbH

CSOC - eine Allianz der dhpg IT-Services GmbH und der synalis GmbH & Co. KG

cts GmbH

CubeItNow GmbH

CUBENet AG

cv cryptovision GmbH

cyan AG

Cyber + Resistant

Cyber Akademie GmbH

Cyber Investigate Deutschland

Cyber Peace

Cyber Protect Partnership (CPP)

Cyber Risk Agency GmbH

Cyber Security Center - Kompetenzzentrum für Informationssicherheit

Cyber Security Challenge Germany (CSCG)

Cyber Security Cluster Bonn e.V.

Cyber Security Coach

Cyber Security Rumble e.V.

Cyber Security Sharing and Analytics e.V. (CSSA)

CyberArk Software (DACH) GmbH

CyberBurg GmbH

Cyber-Cops des Immanuel-Kant-Gymnasium Bad Oeynhausen

CYBERDYNE Informationstechnologie GmbH

Cyberfanders

CyberForum e.V

CyberForum e.V.

CYBERLEAKS

Cybermobbing Prävention e.V.

Cybermobbing-Hilfe e.V

Cyber-Reserve der Bundeswehr

CyberSecurity manufaktur GmbH

Cybersicherheitsforschung am Deutschen Forschungszentrum für Künstliche Intelligenz GmbH (DFKI)

Cyber-Sicherheitsrat Deutschland e.V.

Cybersicherheitsstandort Bochum

Cybersicherheitssymposium Nordwest-Brandenburg

Cybersicherheitstag Niedersachsen

Cyberus Technology GmbH

Cyberwehr BW

Cycle SEC GmbH

CyDIS Cyber Defense and Information Security GmbH (CyDIS)

Cyken UG (haftungsbeschränkt)

CyMotive Technologies Ltd.

Cynops GmbH

CYOSS GmbH

Cypax GmbH

CyProtect Aktiengesellschaft

CYQUEO GmbH

Cyren GmbH

CYSEC Cyber Security TU Darmstadt

D&W Kompetenz-Agentur GbR

D.S. Datenservice GmbH

DAASI International GmbH

dacoso data communication solutions GmbH

Dagmar Pätzold Buchführungsservice

DamS Datenschutz am See UG (haftungsbeschränkt)

Daniel Aßmann - Datenschutz & QM

Daniel Horn "IT Service Horn"

Daniel Kuhlmann "IT-Service"

Danny Endert - Softwareentwicklung -

DARZ GmbH

Das Unternehmerhandbuch

daspro GmbH

Data Business Services GmbH & Co KG

Data Center Consulting UG (haftungsbeschränkt)

Data Protection UG (haftungsbeschränkt)

Data Recall GmbH

DATA RUN

DATA Security GmbH

Data Shield GmbH c/o Grohmann-Velchev

data2net oHG

DataCat SEC GmbH c/o Kristoff Stützner

Datacenter Infrastructure Munich GmbH

DataCo GmbH

DATAGROUP SE

DATAKOM GmbH

DATAKONTEXT GmbH

DATANET Gesellschaft für Entwicklung und Vertrieb von Hard- und Software mbH

Datanetix GmbH

Dataport

Datasec Datenschutz GmbH

DataSecureIT GmbH

Datatree AG

Dat-Con GmbH

Datenbeschützerin Regina Stoiber GmbH

DATENCOACH.DE für fachgerechte Datenhaltung UG (haftungsbeschränkt)

datendrang AG

Datennetze & Rechnerkommunikation GmbH

Datenschutz Arnsberg GmbH

datenschutz cert GmbH

Datenschutz Pöllinger GmbH

Datenschutz Schmidt GmbH & Co. KG

Datenschutz Symbiose GmbH

datenschutz-concept GmbH

DATENSCHUTZ-METROPOL GmbH

datenschutzticker.de

Datensicherheit Nord UG (haftungsbeschränkt)

Datensicherheit.de

Datentechnik Ranglack

Datenwacht UG (haftungsbeschränkt)

Datenzentrum West GmbH & Co. KG

DATEV eG

DatSecure GmbH

DATUS AG

Davor Kolaric

Dawico Deutschland GmbH

DBSC Ruban GmbH

DDI - Deutsches Datenschutz Institut GmbH

de-bit Computer Service GmbH

Defendat GmbH

defensIT UG (haftungsbeschränkt)

Deichmann+Fuchs Verlag GmbH & Co. KG

DeinData UG (haftungsbeschränkt)

DEKRA e.V

DEKRA e.V.

DEKRA SE

Dell GmbH

Deloitte GmbH Wirtschaftsprüfungsgesellschaft

Demand Software Solutions GmbH

dence GmbH

Denkwerkstatt Sichere Informationsgesellschaft

Dennis Lenke "Lenke-Consulting"

der VÃ–B-Service GmbH

Dermalog Identification Systems GmbH

deron Consulting GmbH

deron services GmbH

DETACK GmbH

Detecon International GmbH

Detlef Brian Klanten IT-Dienstleistungen netDE-SIGN.de - Der IT-Partner

DeuDat GmbH

DEURAG Deutsche Rechtsschutz-Versicherung AG

Deutor Cyber Security Solutions GmbH

Deutronix UG (haftungsbeschränkt)

Deutsche Akademie der Technikwissenschaften e.V

Deutsche Akademie der Technikwissenschaften e.V. (acatech)

DEUTSCHE ÄRZTEBLAT

Deutsche Bank AG

Deutsche Cyber-Sicherheitsorganisation (DCSO) GmbH

Deutsche Fernsehlotterie gemeinnützige GmbH

Deutsche Geesetzliche Unfallversicherung e.V.

Deutsche Gesellschaft für Qualität e.V. (DGQ)

Deutsche Krankenhausgesellschaft e.V

Deutsche Telekom AG

Deutsche Versicherungsakademie GmbH (DVA)

Deutschen Gesellschaft für Wehrtechnik e.V

Deutscher Anwaltverein e.V

Deutscher Kinderschutzbund Kreisverband Erlangen e.V

Deutscher Landkreistag

Deutsches Institut für Compliance e.V

Deutsches Institut für IT-Sicherheit GmbH

Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)

Deutschland sicher im Netz e.V.

Deutschland sicher im Netz e.V. (DsiN)

Deutschlandradio

DeviceLock Europe GmbH

DF Vermögensberatung GmbH

DFN-CERT Services GmbH

dfv Conference Group GmbH

DGI Deutsche Gesellschaft für Informationssicherheit AG

DHC Business Solutions GmbH & Co. KG

dhpg IT-Service GmbH

Dialog-Medien und Emmaus-Reisen GmbH

Diana Nadeborn

Die Cybermights

Diehl Stiftung & Co. KG

Dieter Gusenbauer EDV-Beratung Soft Concept

DigiFors GmbH

digika - Digital Katalyst Technologie GmbH

Digital Academy

Digital Hub Cybersecurity

Digital Pioneer

digital@bw

Digitalcourage pEp UG (haftungsbeschränkt)

Digitale Gesellschaft e.V.

Digitale Helden gGmbH

Digitaler Hub Region Bonn AG

Digitalpolitik EU

Digitalstadt Darmstadt GmbH

DigiTrace GmbH

digitronic computersysteme GmbH

DIGITTRADE GmbH

DIHK | Deutscher Industrie- und Handelskammertag e.V.

diisi UG (haftungsbeschränkt)

Dimension Data Germany AG & Co. KG

Dipl. Kfm

Diplom-Informatiker (FH) Philipp Christopher Rothmann, M.Comp.Sc.

direkt gruppe GmbH

Dirk Größer

Unternehmensberatung

Dirk Hahn

Dirk Schulz IT-Consulting

DISOTECH GmbH

Distributed Artificial Intelligence Laboratory (DAI-Labor)

ditpro GmbH & Co. KG

DIZ | Digitales Innovationszentrum GmbH

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

dl-DATEN GmbH

DMKN GmbH

DMN Solutions GmbH

DNV GL SE

DocRAID(R) - professional data privacy protection

DocuSign Germany GmbH

DOK SYSTEME Ingenieurgesellschaft für Kommunikationstechnik mbH

Dolphi Untch IT-Beratung

DomainProfi GmbH

Dorsch Informationssicherheit UG (haftungsbeschränkt)

DOS Software-Systeme GmbH

DoWorks GmbH

DP Consultants UG (haftungsbeschränkt)

DPA Drewes Privacy Advice GmbH

dpi Solutions GmbH

DPRT Business Services GmbH

DQS BIT GmbH

DQS GmbH

Dr. Husmann + Partner GmbH

Dr. Leonard und Labusch Partnerschaftsgesellschaft Ingenieure

Dr. Pape & Co. Consulting GmbH

Dr. Radberg VBK GmbH

Dr. Thiele IT-Beratung

Dreamlab Technologies Deutschland GmbH c/o GÖRG Partnerschaft von ReA mbB

Dresden-Hosting KG

DriveLock SE

DS DATA SYSTEMS GmbH

DS EXTERN GmbH

DS Media GmbH

DS Mentoring GmbH IT-Projects & Consulting

DSB Münster GmbH

DSBE GmbH

dsb-protect GmbH

DSC GmbH

DSG UG (haftungsbeschränkt)

dsgvo NORD GmbH

DSN Holding GmbH

DSS-Connect GmbH

Duale Hochschule Baden-Württemberg

Dynalogy e.K.

e.Comsys GmbH

e.consult AG

E+S Rückversicherung AG

e2 Security GmbH

ebbinghaus digitale Datenverarbeitungs GmbH

EBERTLANG Distribution GmbH

EBP Deutschland GmbH

e-brix UG (haftungsbeschränkt) & Co. KG

eBusiness Lotse

echoway GmbH

eco – Association of the Internet Industry (eco - Verband der Internetwirtschaft e.V.)

eco – Verband der Internetwirtschaft e.V.

EDISON WESLEY KLEINFIELD GmbH

edv2go GmbH

EDV-Partner Ingenieurgesellschaft für Informationstechnologie mbH

EDV-Unternehmensberatung Floß GmbH

EFiS Aktiengesellschaft

EGC EUROGROUP CONSULTING AG

Ehrenfeld Media GmbH

Eibl-IT GmbH

Einstein-Gymnasium Potsdam

elanize KG

Elbe Digital

Elisabeth Hoffmann

Eliseu Macedo Gomes, Go In Tech EDV Dienstleistungen

ELKOM GmbH Elektro- & Kommunikationstechnik

Elmar Brunsch Datenschutz Beratung Computertechnik

ELOWARE GmbH

Elternrat der Max-Brauer Schule

emele IT-Consult GmbH

EMnify GmbH

EnBW Energie Baden-Württemberg AG

e-Networkers GmbH

Enge IT-Solutions GmbH

Engelmann Sales GmbH

engine-productions GmbH

ENTIRETEC AG

Enver Bastanoglu

Envistacom Germany GmbH

Enzyklopädie der Wirtschaftsinformatik, Universität Potsdam

EPERI GmbH

ERGO Direkt AG

Eric Kühn

Erik Gremeyer

Ernst & Young GmbH

esatus AG

esb EWIV

ESC Wirtschaftsprüfung GmbH

ESecurity-CERT GmbH

ESET Deutschland GmbH

ESG Elektroniksystem- und Logistik-GmbH (ESG)

esko-systems GmbH & Co. KG

eSourceONE GmbH

essendi it GmbH

ETES GmbH

Etienne Daniel Benjamin Müllers

euboia GmbH

EURACTIV Deutschland

eurobits e.V. – Europäisches Kompetenzzentrum für IT-Sicherheit Bochum

euromicron AG

euromicron Deutschland GmbH

Europäische Akademie für Informationsfreiheit und Datenschutz e.V. (EAID)

Europäisches Integrationszentrum Rostock e.V

European Cyber Security Month (ECSM)

European Institute for Computer Anti-Virus Research e.V. (EICAR)

EUROSEC GmbH

Evidian SA

EW Medien und Kongresse GmbH

exali AG- Das Versicherungsportal für Dienstleister und freie Berufe

exceet Secure Solutions GmbH

exone IT

Extrinsus GmbH

eye -keep Gesellschaft für Internet- und IT-Dienstleistungen mbH

eyeo GmbH

F5 Networks GmbH

Fach- und Arbeitsgruppen der IT-Sicherheit an der Hochschule Darmstadt (h_da)

Fachhochschule Wedel gGmbH

Fachin & Friedrich Systems and Services KG

Fachverband Informationstechnologie in Sozialwirtschaft und Sozialverwaltung e.V (FINSOZ)

Fachverband Sanitär Heizung Klima Nordrhein-Westfalen (SHK NRW)

fantomas Designgesellschaft mbH & Co. KG

Faronics Corporation

FaroVision GmbH

Fast Lane Institute for Knowledge Transfer GmbH

FAST-DETECT GmbH

Faulhaber Gesellschaft für Informationssicherheit mbH & Co. KG

FCH Gruppe AG

Fedic GmbH

Feil Rechtsanwaltsgesellschaft mbH

Felix Mühlberg

Fels Consulting UG (haftungsbeschränkt)

Feuersozietät Berlin Brandenburg Versicherung Aktiengesellschaft

FH Aachen

FH Münster

FID SOFTWARE GmbH

FIDES Treuhand GmbH & Co. KG

FinalCompliance UG (haftungsbeschränkt)

finally safe GmbH

FINANCE SECURITY GmbH

Finanz Colloquium Heidelberg GmbH (FCH)

FinTech Headquarter UG (haftungsbeschränkt)

Firewall Live

FIVE STAR BITS e.K

FlexSecure

Flughafen München GmbH

FLY Systemhaus GmbH

FM Insurance Europe S.A

for broker GmbH

Förderkreis der Westfälischen Hochschule in Gelsenkirchen e.V

Förderprogramm für Innovative Hafentechnologien (IHATEC)

FORENSIK.IT GmbH

format8 GmbH

Formblitz GmbH

Form-Solutions GmbH

forsacon GmbH

Forschungsinstitut Cyber Defence (CODE)

Forschungsrahmenprogramm „Selbstbestimmt und sicher in der digitalen Welt“

Forschungszentrum CODE der Universität der Bundeswehr München (UniBwM)

FORUM Gesellschaft für Informationssicherheit mbH (FORUM IS)

FORUM VERLAG HERKERT GMBH

FPZ Data Protection GmbH

fragFINN e.V.

Frama Deutschland GmbH

Frank Röhling IT-Service und Sicherheit

Frank W. Holliday

FRANKFURT BUSINESS MEDIA GmbH

Fraunhofer Institut für Graphische Datenverarbeitung (IGD)

Fraunhofer-Anwendungszentrum Industrial Automation (IOSB-INA)

Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (Fraunhofer AISEC)

Fraunhofer-Institut für Sichere Informationstechnologie (Fraunhofer SIT)

Fred Rösner IT-Beratung

Freie Demokratische Partei e.V

Freies Institut für IT-Sicherheit e.V. (IFIT)

Freistaat Sachsen

Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V.

Fresh Compliance GmbH

FRIEDA-Frauenzentrum e.V.

Friederike Scholz

Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)

Frommel Multimedia

FrontEnd IT GbR

F-Secure GmbH

FSP GmbH Consulting & IT-Services

FSZ GmbH

FUSKO GmbH

Future Solutions GmbH

FYNE Consulting GmbH

FZI Forschungszentrum Informatik

G DATA | Advanced Analytics GmbH

G DATA CyberDefense AG (G DATA)

G4C German Competence Centre against Cyber Crime e.V.

GAI NetConsult GmbH

GAIMS GmbH

GARDEZ CONSULTING

GBS Europa GmbH

GCM Go City Media GmbH

GDI Gesellschaft für Datenschutz und Informationssicherheit mbH

Gecko-IT Systemhaus UG (haftungsbeschränkt)

Gehrkens.IT GmbH

genoBIT GmbH

genua GmbH

German Capital Management AG

GES Systemhaus GmbH & Co. KG

Gesamtschule Immanuel Kant

Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV)

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

Gesellschaft für Datenschutz und Datensicherheit e.V.

Gesellschaft für Datensicherheit & Datenschutz mbH

Gesellschaft für Digitale Technologien mbH

Gesellschaft für Informatik e.V. (GI)

Gesellschaft für Video- und Datentechnik mbH

Gesellschaft für wissenschaftliche Datenverarbeitung mbH

get in GmbH

Getrud-Bäumer-Realschule Bielefeld

Getsec UG

Gewerkschaft Erziehung und Wissenschaft (GEW)

GFAD Systemhaus AG

GFC-NetCare & Telecom GmbH

GfI Gesellschaft für Informationssicherheit mbH

GHI Datenschutz UG (haftungsbeschränkt)

Giegerich & Partner GmbH

Giesecke+Devrient GmbH

Gilbert Köhler IT Management

GINDAT GmbH

GISA GmbH

GKC GmbH

GLENDE.CONSULTING GmbH & Co. KG

Global Player Initiative des Bundeskriminalamts

Global-Sec GmbH

Glück & Kanja Consulting AG

GNS Systems GmbH

Goethe-Schiller-Gymnasium

GoingPublic Media AG

Golem Media GmbH

GORISCON GmbH

Gothaer Versicherungsbank VVaG

GovConnect GmbH

Governikus GmbH & Co. KG

GRÃœNEwolke UG (haftungsbeschränkt)

Greenbone Networks GmbH

greeneagle certification GmbH

Gronau IT Cloud Computing GmbH

GRONEMEYER IT GmbH

Grothe IT-Service GmbH

grouptime GmbH

Gruidae Consulting UG (haftungsbeschränkt)

Grund- und Mittelschule Grossaitingen

GSD Software Design GmbH

GSI Helmholtzzentrum für Schwerionenforschung GmbH

gSolution IT-Services KG

GT ARC gemeinnützige GmbH

Günter Born

Günter Don Systembetreuung

Gymnasium des Main-Kinzig-Kreises in Maintal

Gymnasium Paulinum

Haase IT Solutions GmbH

HackCheck GmbH

Hacker Werkstatt

Hagen & Kruse GmbH & Co.KG

Hahn GmbH

Haikiki GmbH

Handelsblatt GmbH

Handelskammer Bremen - IHK für Bremen und Bremerhaven

Handelsverband Deutschland e.V. (HDE)

HANDS on TECHNOLOGY e.V.

Handwerkskammer Berlin

Handwerkskammer Frankfurt-Rhein-Main

Handwerkskammer Münster

Handwerkskammer Wiesbaden

Hannover IT e.V.

Hans-Hermann Dirksen

Hans-Litten-Schule

Oberstufenzentrum für Recht und Wirtschaft

Harald Oest

Harscheidt IT-Consult GmbH

Hartmut Ihne

Hartmut Löw

Hasso-Plattner-Institut für Digital Engineering gGmbH (HPI)

HAUB + PARTNER GmbH

Haufe-Lexware GmbH & Co. KG

Haus des Stiftens gGmbH

Haverkamp Beratungsgesellschaft UG (haftungsbeschränkt)

HBK Datenschutz Consulting UG (haftungsbeschränkt)

HCT Network Consulting GmbH

HDI Global SE

HDSM Hamburger Daten-Schutz Management e.K

HEALTH-CARE-COM GmbH

HEC GmbH

Heidrich Internet Service GmbH

Heiko Rittelmeier

Heinemann Verlag GmbH

Heinlein Support GmbH

Hein-Moeller-Schule

Oberstufenzentrum Energietechnik II

Heinz Bilda - C & S Computer-Service -

Heise Medien GmbH & Co. KG

heise Security

Helfert Informatik GmbH & Co. KG

Helmholtz-Zentrum für Informationssicherheit gGmbH (CISPA)

Helmich IT-Security GmbH

Helmut Lingen Verlag GmbH

help and hope Stiftung

Henke Informatik GmbH

Henrich Publikationen GmbH

HERALEX GmbH

Herold Unternehmensberatung GmbH

Herrmann Computer e.K

Hertie School gGmbH

Herting Oberbeck Datenschutz GmbH

Hessische Landesregierung

Hessische Ministerin für Digitale Strategie und Entwicklung

HGS Fahrzeugbau GmbH

HiAudit GmbH

HIMA Paul Hildebrandt GmbH

HiScout GmbH

Hiscox SA

HiSolutions AG

HK2 / RA Karsten U. Bartels, LL.M.

HK2 Comtection GmbH

HK2 Rechtsanwälte

HM-Consult IT-Management GmbH

Hoax-Info Service

Hochschule Aalen - Technik und Wirtschaft

Hochschule Albstadt-Sigmaringen

Hochschule Albstadt-Sigmaringen, Fakultät Informatik

Hochschule Bochum

Hochschule Bonn-Rhein-Sieg

Hochschule Darmstadt Institut für Kommunikation & Medien

Hochschule der Bayerischen Wirtschaft (HDBW) gemeinnützige GmbH

Hochschule für angewandte Wissenschaften Ansbach

Hochschule für Technik und Wirtschaft Berlin

Hochschule für Technik und Wirtschaft Dresden

Hochschule für Wirtschaft und Recht (HWR) Berlin

Hochschule Furtwangen

Hochschule Hannover

Hochschule Karlsruhe Technik und Wirtschaft

Hochschule Mannheim (Fachhochschule)

Hochschule Mittweida, University of Applied Sciences

Hochschule Niederrhein

Hochschule Offenburg

Hochschule Ravensburg-Weingarten University of Applied Science

Hochschule Stralsund

Hochschule Trier

Hochschule Wismar

Hochschule Worms

Hochschulrektorenkonferenz

Holzhofer Consulting GmbH

Holzmann Medien GmbH & Co. KG

homemade code GmbH

Hornetsecurity GmbH

Horst Görtz Institut für IT-Sicherheit (HGI)

Horst Görtz Stiftung

Host Europe GmbH

Hostway Deutschland GmbH

HOWDEN CANINENBERG GMBH

HRES Development GmbH

HS Onlinemarketing GmbH

Hüthig GmbH

HvS-Consulting AG

I -Tech GmbH & Co. KG

I.A.M. Consultant GmbH

ibi systems GmbH

IBM Deutschland GmbH

ICN GmbH + Co. KG

ICT Solutions GmbH

IDG Business Media GmbH

IDG Tech Media GmbH / PC-WELT

iesy GmbH & Co. KG

IHK Schleswig-Holstein

IHK-Akademie Ostwestfalen GmbH

IHR Servicemitarbeiter - IT & EDV Systemhaus GmbH

ikomm GmbH

ILS - Institut für Lernsysteme GmbH

im Stifterverband für die Deutsche Wissenschaft e.V

IM42 Information Management Consulting GmbH

iMobileSitter

Imprivata, Inc.

inblock.io - Tim Bansemer

INCAS GmbH

Increase Your Skills GmbH

indevis IT-Consulting and Solutions GmbH (indevis)

Indu-Sol GmbH

Industrial IT Security GmbH

Industrie- und Handelskammer (IHK) Koblenz

Industrie- und Handelskammer für München und Oberbayern

Industrie- und Handelskammer Mittleres Ruhrgebiet, Körperschaft des öffentlichen Rechts

Industrie- und Handelskammer Nord Westfalen

Industrie- und Handelskammer Nürnberg für Mittelfranken

Industrie- und Handelskammer Ostbrandenburg

Industrie- und Handelskammer Potsdam

Industrie- und Handelskammer Siegen

Industrie- und Handelskammer zu Berlin

Industrie- und Handelskammer zu Dortmund

Industrie- und Handelskammer zu Köln

Industrie- und Handelskammer zu Schwerin

Industrieanlagen- Betriebsgesellschaft mbH (IABG)

Infineon Technologies AG

Infodas Gesellschaft für Systementwicklung und Informationsverarbeitung GmbH (INFODAS)

INFODAS Gesellschaft für Systementwicklung und Informationsverarbeitung mbH

Infolabor UG (haftungsbeschränkt)

Info-Point-Security GmbH

INFORA GmbH

Information Flow IT-Beratungsgesellschaft mbH

Information Security GmbH

Informationssicherheit und Datenschutz mbH

Informationsstelle Militarisierung (IMI) e.V.

Informationsverarbeitung für Versicherungen GmbH

INFOSERVE GmbH

infoteam Software AG

Infotecs Internet Security Software GmbH

Infradata GmbH

ING Bank eine Niederlassung der ING-DiBa AG

Ingenieurbüro Dr. Plesnik GmbH

Ingo Falk

Ingo Rischke EDV-Dienstleistungen

Initiativbüro "Gutes Aufwachsen mit Medien" c/o Stiftung Digiale Chancen

Initiative Innovationskraft für Sicherheit in der Wirtschaft (IISW)

Initiative Kommunikation und Sicherheit digitaler Systeme

Initiative Wirtschaftsschutz

Inlab Networks GmbH

INNAVIS Dienstleistungsges. für Datenschutz & Compliance mbH & Co. KG

Innenministerium Baden-Württemberg

innogy SE

innos Systemhaus GmbH

innovaphone AG

Innovationszentrum Mobiles Internet, LMU: Lehrstuhl für Mobile und Verteilte Systeme

innoventis GmbH

inoplex AG

Insecas GmbH

Insentis GmbH

insidas Verwaltungs GmbH

inside intermedia GmbH

Institut für Datenrettung IT Forensik

Institut für Datenwissenschaften am Deutschen Zentrum für Luft- und Raumfahrt e.V. (DLR)

Institut für digitale Infrastruktur - its-labs UG

Institut für Informatik 4 der Rheinischen Friedrich-Wilhelms Universität Bonn

Institut für Informationssicherheit der Hochschule Niederrhein (Clavis)

Institut für Internet-Sicherheit – if(is)

In-stitut für or-ga-ni-sa-to-ri-sche In-for-ma-ti-ons-sys-teme - inois GmbH

InsurLab Germany e.V.

INSYS MICROELECTRONICS GmbH

Intebit GmbH

integer GmbH

Integrata Cegos GmbH

Intel Deutschland GmbH

intension GmbH

INTER Allgemeine Versicherung AG

intercombosch GmbH

InterConnect GmbH & Co. KG

Internet-ABC e.V.

internett gmbh

InterNetX GmbH

intersoft consulting services AG

Intevation GmbH

inTIME Berlin

IP Interactive Unternehmergesellschaft (haftungsbeschränkt)

Iqanta GmbH

Ira Vaupel

ireo GmbH & Co. KG

IRM4U e.K.

ISACA Germany Chapter e.V.

IS-Consulting UG (haftungsbeschränkt)

isdacom GmbH

isential GmbH

ISiCO Datenschutz GmbH

isits AG International School of IT Security

ISL - Institut für IT-Sicherheit und Sicherheitsrecht

ISL Internet Sicherheitslösungen GmbH

ISO27k GmbH

iSQI GmbH

IST planbar GmbH

IT & Management Solutions GmbH

IT Compliance Systeme GmbH

IT Consult GmbH Gesellschaft für innovative Informationstechnologien

IT GmbH

IT Klub Mainz & Rheinhessen e.V

it mit System e.K.

iT Schneider Informationstechnik

IT Secure GmbH

IT Security Blog

IT Security made in Germany (ITSMIG)

IT Security Manufacture GmbH

IT Systemhaus Fiebig GmbH

IT Verlag für Informationstechnik GmbH

IT Vision Technology GmbH

it's.BB - IT-Sicherheitsnetzwerk Berlin-Brandenburg

IT-Beauftragter der Bundesregierung

IT-Bildungsnetz e.V.

ITC GmbH

ITC Hänsel GmbH

IT-Dienstleistungen Th. Koch

ITeam EWIV

itelio GmbH

itemis AG

iternas GmbH

IT-FORMATION GmbH

IT-GRC Consulting GmbH

ITkollektiv GmbH

IT-Linx GmbH

IT-On.NET GmbH

iT-RETTUNG

ITs Integration GmbH

IT-SCAN GMBH

IT-SECURITY Conference

IT-Security@Work GmbH (ISW)

IT-Service Network

IT-Service und Beratung Ulf Dinkelmann GmbH

ITSG Informationstechnische Servicestelle der Gesetzlichen Krankenversicherung GmbH

ItSicher.net UG (haftungsbeschränkt)

IT-Sicherheit in der Wirtschaft

IT-Sicherheit@Mittelstand

IT-Sicherheitsinitiative Saarland

IT-Sicherheitsmanagement GmbH

IT-Sicherheitstag Sachsen

IT-Talents GmbH

ituso GmbH

itWatch GmbH

IT-xPerts.GmbH

IUGITAS GmbH

J & R GmbH

Jan Schöne Web & Design

Janotta Partner Security Consulting

Jantzon & Hocke KG

Jasmin Lieffering

JAWA Systemlösungen GmbH

Jens-Albert Brauer IT-Diensnstleistungen

JFF – Jugend Film Fernsehen e.V.

Joachim Hornegger

JOBA ITK-Systeme GmbH

Johann Wolfgang Goethe-Universität Frankfurt

Johannes Baumgärtel Systemadministrator macsupport & itsupport

Johner Institut GmbH

Johnson Controls Systems & Service GmbH

Jolocom GmbH

Jonas Wendler IT&D

Jörg Collmann EDV -Organisation - Anwendungsberatung Ltd & Co. KG

Jörg Richter "Hoplit First Class IT Consulting + Business IT"

Jörg Zimmermann

Jürgen Dierlamm

Justus-Liebig-Universität Gießen

JUUUPORT e.V.

K&K Networks GmbH

K&K Software AG

Käfer IT Systeme e.K.

KAIROS Partners on time consulting GmbH

Karlsruher Institut für Technologie

Karlsruher IT-Sicherheitsinitiative (KA-IT-SI)

Karpetorix Software GmbH

Kaschkat-Engineering Gesellschaft mit beschränkter Haftung

Kaspersky Labs GmbH

Kassel GmbH

Katholischen Landesarbeitsgemeinschaft Kinder- und Jugendschutz NRW e.V

Kathrin M. Möslein

KBV - Kassenärztliche Bundesvereinigung

keepbit SOLUTION GmbH

Kegler IT GmbH & Co. KG

Kein Zugang möglich

Keitgen GmbH

Kentix GmbH

Kernkonzept GmbH

keydata GmbH

KeyIdentity GmbH

Key-Systems GmbH

Kia Soul EV

KikuSema GmbH

kippdata informationstechnologie GmbH

Kircher Datenschutz

KISTERS AG

KIT Kompetenzzentrum Informationstechnologie GmbH

KIWI.KI GmbH

KIWOCOM OHG

Klaus Kohnen

Klein Computer Systemhaus GmbH

Klicksafe

KluCon UG (haftungsbeschränkt)

KLW GmbH

Kolja Heymann Netzwerktechnik

Kommunaler Betrieb für Informationstechnik "KommunalBIT" AöR

Kommunales IT-Sicherheitsbündnis Niedersachsen (Kitsin)

Kompetenzzentrum Digitales Handwerk

Kompetenzzentrum für angewandte Sicherheitstechnologie (KASTEL)

Konica Minolta Business Solutions Deutschland GmbH

Konrad-Adenauer-Stiftung e.V

Konzept 17 GmbH

KonzeptAcht GmbH

KOSMICON GmbH

KPMG AG Wirtschaftsprüfungsgesellschaft

KPMG Wirtschaftsprüfungsgesellschaft AG

kreITiv eine Marke der ENWITO GmbH

KRITIS Consult GmbH

KroCo UG (haftungsbeschränkt)

Ksi Consult Ltd. & Co. KG

Kubuni UG (haftungsbeschränkt)

Kuketz IT-Security

KVB - Kassenärztliche Vereinigung Bayerns, KdöR

L1 Datenschutz GmbH

Lagerfeuer UG (haftungsbeschränkt) & Co. Betriebs KG

LaMa 4.net GmbH

LANCOM Systems GmbH

Land Baden-Württemberg

Land Nordrhein-Westfalen: Staatskanzlei des Landes Nordrhein-Westfale

LAND-DATA GmbH

Landesamt für Sicherheit in der Informationstechnik (LSI)

Landesamt für Verfassungsschutz Baden-Württemberg

Landesanstalt für Kommunikation Baden-Württemberg

Landesanstalt für Medien NRW

Landesarbeitsstelle Bayern e.V

Landesbetrieb Information und Technik Nordrhein-Westfalen (IT.NRW)

Landesmedienzentrum Baden-Württemberg

Landesregierung Rheinland-Pfalz

Langner Communications GmbH

LargeNet GmbH

Lars Hoffmann

Lars Karpiak IT-Dienstleistungen

LastBreach UG (haftungsbeschränkt)

Law4school

legitimis GmbH

Leipziger Messe GmbH

LEITWERK AG

Lemlock GmbH

Leopold Netzwerke GmbH

Lernlabor Cybersicherheit

lexICT Unternehmergesellschaft (haftungsbeschränkt)

LH Computer Systeme GmbH

LH DATAconsult UG (haftungsbeschränkt)

Ligenta Service GmbH

limes datentechnik® gmbh

Link11 GmbH

Linogate Internet Technologies GmbH

Linus Neumann

Linuxhotel GmbH

List + Lohr GmbH

LivingData Gesellschaft für angewandte Informationstechnologien mbH

LKS ADVERTISING

LoeScap Technology GmbH

LOROP GmbH consulting training - it & service

luckycloud GmbH

Ludwig-Maximilians-Universität München

LuebbeNet GmbH

Lufthansa Industry Solutions GmbH & Co. KG (LHIND)

LVM Versicherung

LWsystems GmbH & Co. KG

M&H Holding GmbH

M2B e.V

mabunta GmbH

MacEinsteiger

magility GmbH

mail.de GmbH

maincubes one GmbH

MajorSecurity GmbH

Makro Factory GmbH & Co. KG

Maltego Technologies GmbH

MalwareMustDie

MAMEDO IT-Consulting GmbH

Manfred Rekowski

Manu Carus

Manuel Hahs EDV-Fachhandel

MARA Systems GmbH

MARBLE MADNESS GmbH

Marc Sellmer zweikreis.de

Marcel Déjosez IT-Dienstleistungen

Marco Kobek IT Security

Marco Kubick

Marco Villani Hard- und Software

Marcus Bächer IT Bächer

Mario Jocksch -IT & Sicherheit-

Mario Willems

Maritimes Cluster Norddeutschland e.V

Mark Semmler GmbH

Markus Bender Informatik

Markus J Neuhaus Unternehmensberatung Mediation

Markus Lehner IT-Systemhaus "TechSys Networks"

Martin Halter Computerhandel

Martin Probst

Martin Teichmann IT-Dienstleistungen

Martina Böhmer

Marx Data Security GmbH

MARX Software Security GmbH

März Internetwork Services AG

Maschinenfabrik Reinhausen GmbH

MaskTech GmbH

MATRIX IT development GmbH

Matthias Baumgartner IT-Sicherheit

Matthias Jasinski

Matthias Leimpek Unternehmensberatung

Max von Breitenstein® Data Protect GmbH

Maxpert GmbH

Max-Planck-Gesellschaft zur Förderung der Wissenschaften e.V.

Max-Planck-Institut für Cybersicherheit und Schutz der Privatsphäre (CSP)

Max-Steenbeck-Gymnasium

May-Britt Kallenrode

Mayer-Berger GmbH

MB Connect Line GmbH Fernwartungssysteme

MBmedien Publishing GmbH

McAfee Germany GmbH

Mecklenburg-Vorpommern GmbH

MeckSecure UG

Medialine EuroTrade AG

mediatec.net GmbH

MediDas GmbH & Co. KG

Medienhaus Aachen GmbH

MEDIENHAUS Verlag GmbH

MediSoft GmbH

Mein Computerkind

MENCO Consulting GmbH

Mentana-Claimsoft GmbH

Mesterheide Rockel Hirz Trowe AG Holding

Metaebene Personal Media

metafinanz Informationssysteme GmbH

mgm security partners GmbH

MHS Systemberatung GmbH

Michael Deller - Zukunftszentrum Bayern

Michael Schöpf "s-con Datenschutz & ITK"

Michael Stefan

Michael Thurm EDV-Beratung

Michael Weiß IT-Consulting

Michaela Weiß

Microbee Systemhaus GmbH

Micromata GmbH

Microsoft Business User Forum e.V.

Microsoft Corporation

Microsoft Deutschland GmbH

Midland IT GmbH

migosens GmbH

Mike Barteczko

Ministerium des Innern des Landes Nordrhein-Westfalen

Ministerium des Innern und für Sport des Landes Rheinland-Pfalz

Leitstelle Kriminalprävetion

Ministerium für Inneres, Digitalisierung und Migration, Referat 35, Öffentlichkeitsarbeit

Ministerium für Inneres, Digitalisierung

und Migration Baden-Württemberg

Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen, Referat Presse und Kommunikation

Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg

MINT-Award IT-Sicherheit

MINT-Initiativkreis Trier

Mirko Bender

Mirko Mönninghoff Werbegestaltung "Mouseattack"

Mirko Pelloth

Mittelstand 4.0-Kompetenzzentrum Planen und Bauen

Mittelstand-Digital

Mittler Report Verlag GmbH

MJBADC Database Consulting GmbH

MKL GmbH

MMS-Secure, Inhaber Jürgen Saamen e.K.

Mobilsicher

modal gmbh + co kg

moderne betriebssysteme ag

ModulaTeam GmbH

modzero GmbH

Monika Broich

MORGENSTERN consecom GmbH

motosoft GmbH

movetech IT-Solutions

mowaSYSTEMS GmbH

MPC Service GmbH

m-privacy GmbH

msecure GmbH

msg systems ag

msm net meissner GmbH

MTRIX GmbH

Multi-Media Berufsbildende Schulen (MMBbS)

Munich Institute for IT Service Management GmbH (mITSM)

MUT GbR

my-files GmbH

Myra Security GmbH

N3XT IT Systems UG (haftungsbeschränkt)

NABICON IT-Business Consulting GmbH

nacom-consult UG (haftungsbeschränkt)

nacura it-SERVICE GmbH & Co. KG

NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V.

Nationale Initiative für Informations- und Internet-Sicherheit e.V. (NIFIS)

Nationaler Pakt Cybersicherheit (NPCS)

Nationales Cyber-Abwehrzentrum (Cyber-AZ)

Nationales Forschungszentrum für angewandte Cybersicherheit (ATHENE)

Natuvion GmbH

NCC Group GmbH

NConsult IT-Systemhaus GmbH

NCP engineering GmbH

neam IT-Services GmbH

NEISS GmbH

Neomint Studios GmbH

NeoNect GmbH

NEOX NETWORKS GmbH

NESO Security Labs GmbH

Net at Work GmbH

Net Concepts Stüber UG (haftungsbeschränkt)

net4sec UG (haftungsbeschränkt)

netconsult TechNet GmbH

netfiles GmbH

NETFOX AG

netgo GmbH

NetKom IT-Solutions GmbH

NETLINE Computer & Netzwerksysteme GmbH

NetMediaEurope

NetMediaEurope Deutschland GmbH

NetPlans GmbH

NetUSE AG

Network Box Deutschland GmbH

Network Partners IT Services und Consulting GmbH

networker NRW e.V.

networker NRW e.V.

Networkers AG

netz98 GmbH

netzhaus AG

netzorange IT-Dienstleistungen GmbH & Co. KG

Netzpiloten AG

netzpolitik.org e.V.

NETZWERK Software GmbH

Neuland@Homeland GmbH

Neumann IT-Security GmbH

Neun Zeichen GmbH

Neupart GmbH

new direction Cyber Security GmbH

neXenio GmbH

NEXIS GmbH

Nextron Systems GmbH

NH IT-Services GmbH

Nico Wiegand Consulting

nicos advice GmbH

nicos AG

Niedersächsisches Ministerium für Inneres und Sport

Nikolaus Stapels Consulting

Nils Wagemann

Nimbus Technologieberatung GmbH

NKMG mbH

NobleProg Limited

Nordrhein-Westfalen e.V

Norics GmbH

noris network AG

Notos Xperts GmbH

NovaStor GmbH

nowinta Investmentservice GmbH

now-i-trust GmbH

nrw.uniTS

NTT Security GmbH

NürnbergMesse GmbH

NVISO GmbH

OAK - Online Akademie GmbH & Co. KG

Oberstufenzentrum Informations- und Medizintechnik

OctoGate IT Security Systems GmbH

Octothorpe GmbH

OEVERMANN Networks GmbH

Öffentliche Versicherung Braunschweig

OFFICE KOMPLETT, Computer Service GmbH

OfficeCom GmbH

Oliver Kuhlemann

Oliver S. Hartmann

Omnis Consulting GmbH

OnCall-SEC UG (haftungsbeschränkt)

oncampus GmbH

onix - Dienstleistungs- und Handels-GmbH

On-Lab GmbH

Onlinezugangsgesetz zur Digitalisierung von Verwaltungsdienstleistungen

onsite.one UG (haftungsbeschränkt)

Open Competence Center for Cyber Security

Open Text Software GmbH

OpenAdvice IT Services GmbH

openpgp-schulungen

operational services GmbH & Co. KG

OPTIMA Business Information Technology GmbH

OPTIMOS 2.0

ORA IT-Systeme GmbH

Organisation Reiger+Boos Informationssysteme GmbH

ÖSA Versicherungen

OTARIS Interactive Services GmbH

Outpost24 GmbH

ÖVB Versicherungen

OVH GmbH

P4DT - Partners for Digital Transformation GmbH

PA Consulting Services Limited

Packetwerk GmbH

PALTRON GmbH

Panaccess Systems GmbH

PARIT GmbH

Parks Informatik GmbH

Partnerschaftsgesellschaft mbB

PASS IT-Consulting Dipl.-Inf. G. Rienecker GmbH & Co. KG

Passau Institute of Digital Security

Patrona Versicherungsmakler GmbH

Paul-Gerhardt-Gymnasium

PC-COLLEGE Training GmbH

PCF Service-Netz e.K

PC-Mentor GmbH

PCrisk Cyber Security Portal

PCS Keitel GmbH

PEASEC - Wissenschaft und Technik für Frieden und Sicherheit

percepticon

Perseus Technologies GmbH

Peter Lachenmair

Peter Suhling

PF IT Consult GmbH

philipp design GmbH

Philipp-Christopher Rothmann Beratender Wirtschaftsinformatiker

Philotech Systementwicklung und Software GmbH

PHOENIX CONTACT Cyber Security GmbH

Phoenix Contact GmbH & Co. KG

Phoenix Software GmbH

PI Informatik GmbH

Pilz GmbH & Co. KG

PINthing Unternehmergesellschaft (haftungsbeschränkt)

PiraCon GmbH

PixelBiotech GmbH

plan42 GmbH

Platinion GmbH

PlexCon GmbH

PlusServer GmbH

Polizei Nordrhein-Westfalen

POLYAS GmbH

Postanschrift ZEIT ONLINE GmbH

PPI AG

pragmatic technology consulting GmbH

praxiskom GmbH

PREKLA Datenschutz GmbH

PRESECURE Consulting GmbH

PRESENSE Technologies GmbH

PricewaterhouseCoopers GmbH

Primezert GmbH

Primo-Levi-Gymnasium

Prinz Service GmbH

priomni AG Aktiengesellschaft

PRIVACY Central GmbH

Privacy Handbuch

Private-ptm-Akademie – Gesellschaft für Informatik-Training und Kommunikationstechnologie mbH –

pro.DAT GmbH

Proact Deutschland GmbH

procilon IT-Solutions GmbH

Prodevion GmbH

Prodigialis GmbH

Prof. Dr.-Ing. Norbert Gronau

Lehrstuhl für Wirtschaftsinformatik, insbesondere Prozesse und Systeme

Universität Potsdam

professionals GmbH

profortis GmbH

proISMS GmbH

ProIT Service GmbH

Project Networks GmbH

Projekt 29 GmbH & Co. KG

projektmagazin

Berleb Media GmbH

proofdata e.K

proper-it GmbH

ProPress Verlagsgesellschaft m.b.H

Pro-Press Verlagsgesellschaft mbH

PROSECURITY PUBLISHING GMBH & CO. KG

Proservia GmbH & Co. KG

protectONE

Protiviti Deutschland GmbH

PROVINZIAL

Provinzial Rheinland Lebensversicherung AG

Proyet Consulting GmbH

PSW GROUP GmbH & Co. KG

PwC Cyber Security Services GmbH (PwC)

Q_PERIOR AG

QBE Europe SA/NV

QGroup GmbH

QiTEC GmbH

QKomm GmbH

QSC AG

qSkills GmbH & Co. KG

qualitatis IT Service Tilo Feldmann

Quandel Staudt Design GmbH

Quorum Control GmbH c/o Topping Bowers

QuoScient GmbH

R+V Allgemeine Versicherung AG

Radware GmbH – Main Office

Ralf Dieper config.IT EDV-Systeme & Dienstleistungen

Ralf Martin Meyer

Ralf Schmitz

RAM GmbH

Ratgeber Internetkriminalität

RatioProtect

Rau Systemberatung GmbH

RCKT Management GmbH

RDS CONSULTING GmbH

RebeIT GmbH

recensus UG (haftungsbeschränkt)

rechennetz it consulting GmbH

Rechtsanwälte Stückmann

REDDOXX GmbH

ReDi School of Digital Integration gGmbH

reduceo GmbH

Reflex Verlag GmbH

rehm Datenschutz GmbH

Reich & Kornack GmbH

Remynd Systems GmbH

René Fiehl IT-Management-Beratung "controlnet"

Rene Puttkammer - Beratung IT -

René Vorwergk EDV-Beratung

Reply AG

Resilien[i]T GmbH

retarus GmbH

RETAX KG

Reusch Rechtsanwaltsgesellschaft mbH

RGP DataCare UG (haftungsbeschränkt)

RHAPSODY Consulting GmbH

Rhebo GmbH

Rheindigital GmbH

Rheinmetall AG

RIPS Technologies GmbH

Riske IT GmbH

RiskNET GmbH

RO-BUST ACADEMY GmbH

Rohbot IT-Service UG (haftungsbeschränkt)

Rohde & Schwarz

Rohde & Schwarz Cybersecurity GmbH

Roland Gruppe

Roland Hermes "nosurf - IT-Systemhaus"

Rolf Schneider GmbH

Ronny Temler Dienstleistungen im Bereich Wirtschaftsinformatik

rootfabrik UG (haftungsbeschränkt)

Rottal-EDV Löw & Neulinger GmbH & Co. KG

Röttinger Unternehmensgruppe GmbH

Roux Verwaltungs GmbH

RSM GmbH

RT Data & IT Consulting GmbH

RÜHLCONSULTING GmbH

Ruhloff & Dauner GmbH

Ruhr-Universität Bochum

Runder Tisch zur IT-Sicherheit für Verbraucher

Rupert Paintmayer IT-Netzwerkservice "IP SECURE"

RWT Crowe IT Consulting GmbH

RWTH Aachen

S & P Unternehmerforum GmbH

S&L Netzwerktechnik GmbH

S.I.T. Secure Internet Traffic GmbH & Co. KG

Saarbrücker Versicherungsmakler SVM e.K

saaris - saarland.innovation&standort e.V

SAFE+ Algorithmics GmbH

Safe4Net GmbH

SAFECURITY e.K.

Samsung Electronics Co., Ltd

SAP Deutschland SE & Co. KG

SaphirIT GmbH

Sapiensis GmbH

Sartoris GmbH & Co. KG

save IT first GmbH

sayTEC AG

SBD Automotive Germany GmbH

Scalamat UG (haftungsbeschränkt)

Scanfabrik KG

Schadow-Gymnasium

SCHAU HIN!

scheible.it

Schleupen AG

Schlupfwinkel e.V

Schlüterschen Verlagsgesellschaft mbH & Co.KG

Schmalenberg GmbH

Schmid Datensicherheit GmbH

schmiddesign GmbH & Co. KG

Schneider Electric GmbH

scholze IT - Gesellschaft für Informationstechnologie mbH

Schönes und Seltenes IT Services Fabian Böhme e. K.

Schönhofer Sales and Engineering GmbH

School of Governance, Risk & Compliance (School GRC)

Institut für Kriminalistik | School of Criminal Investigation Forensic Science (School CIFoS)

School of Governance, Risk & Compliance (School GRC), Institut für Kriminalistik | School of Criminal Investigation Forensic Science (School CIFoS)

Schott-IT GmbH

schuba & höfken

SCHUFA Holding AG

Schule am Sandsteinweg

Schulung & Netzwerk UG (haftungsbeschränkt)

SCHUTZWERK GmbH

Schwarz Computer GmbH

Schwerhoff Consultants GmbH

SCIAS GmbH

S-COP GmbH

scoyo GmbH

SCURE Consulting GmbH

SD&C Solutions Development & Consulting GmbH (SD&C)

Sebastian Baier Avantage Corporate Communications

SEC Consult Deutschland Unternehmensberatung GmbH

sec³ Beratung GmbH & Co. KG

Secardeo GmbH

Seceidos GmbH & Co. KG

SECIANUS GmbH & Co. KG

secobit GmbH

SecoDat GmbH

Secodis GmbH

Secomba GmbH

Seconos IT & Data Services GmbH

secopan gmbh

Secorvo Security Consulting GmbH

SECOSYS-IT GmbH

secova GmbH & Co. KG

sector red GmbH

secucloud GmbH

Secuda Solutions GmbH

SECUDOS GmbH

SECUINFRA GmbH

SECULONIA GmbH

secunet Security Networks AG

SecuPedia - Die Plattform für Sicherheits-Informationen

Securai GmbH

SecurCon GmbH & Co. KG

Secure IT GmbH

Secure Mail UG (haftungsbeschränkt)

Secure Mobile Networking Lab (SEEMOO)

SecureLAN GmbH IT-Service und Consulting

secure-networker Ralf Rebholz e.K.

Securepoint GmbH

SECUREWARE GmbH

securime

SECURiON Rheinland-Pfalz GmbH

Security Research & Consulting GmbH

Secusmart GmbH

secuvera GmbH

SECVRE GmbH

secXtreme GmbH

SEDECO UG (haftungsbeschränkt)

Seeger GmbH & Co. KG

SEFIROT GmbH

Selbstdatenschutz

SEMASU GmbH

Semigator GmbH

SEMPACON Verwaltungs GmbH

Sengi GmbH

sense-IT GmbH

sepago GmbH

SEPPmail – Deutschland GmbH

SEQUDATA Unternehmensberatungsges. für Datensicherh. & Datenschutz mbH & Co.KG

SerNet Service Network GmbH

SERPENTEQ GmbH

Set Fire to Digial Media GmbH

Setmics Softwareentwicklung GmbH

SEVEN PRINCIPLES AG

Shared IT Professional GmbH & Co. KG

SHD System-Haus-Dresden GmbH

SHORT CUTS GmbH design & kommunikation

Shyann Networks GmbH

sic()sec GmbH

Sichere Identität Berlin-Brandenburg e.V.

Sichere Industrie

Sichere Webseiten und Content Management Systeme (SIWECOS)

SICHERES NETZ HILFT e.V.

Sicherheit macht Schule

Sicherheit.info

Sicherheitsforum Baden-Württemberg

Sicherheitskooperation Cybercrime

Sicher-Stark-Stiftung e.V.

sicotec Gesellschaft für System- und Modultechnik c/o Hans-Georg Wolf

Siegfried Finke

Siegfried Huhn IT-Dienstleistungen "NET IT-Service"

Siegfried Lambertz

Siemens Aktiengesellschaft

SIEVERS-SNC Computer & Software GmbH & Co. KG

SIGNAL IDUNA Allgemeine Versicherung AG

SIGNAL IDUNA Bauspar AG

SIGNET Gesellschaft für innovative Bildung mbH

Signicat GmbH

SIMEDIA Akademie GmbH

Simon Herzog Beratung "Team Quasi"

simply communicate GmbH

SIN – Studio im Netz e.V.

Sitz der Aktiengesellschaft

SIUS Consulting

SIUS Consulting®

Skyfillers GmbH

Skyhaus GmbH

Skymatic GmbH

SKYTALE | Online Akademie für IT-Sicherheit

SLA Digital Services OHG

SlimSec IT GmbH

Smartbox Computer e. K.

Smartify IT Solutions GmbH

SMC InformationsTechnologien Aktiengesellschaft

SMT BERATUNG UND VERWALTUNG GmbH

so.a.p. 4 solutions and products gmbh

Social Engineering Academy (SEA) GmbH

SoCura GmbH

SoftBCom Berlin GmbH

SoftGuide GmbH & Co. KG

SoftKom e.K

Softline AG

softScheck GmbH

Software Symbiose GmbH

Sogeti Deutschland GmbH

SoHaNet Technology GmbH

solitus GmbH

Sonntag & Partner Partnerschaftsgesellschaft mbH

Sophos Technology GmbH

Sopra Steria SE

Sorin Mustaca IT Security Consulting UG (haftungsbeschränkt)

SoSafe GmbH

SOURCEPARK GmbH

SPB - Safe Passage Berlin UG (haftungsbeschränkt)

Spektrum der Wissenschaft Verlagsgesellschaft mbH

SPGO Research Mannheim GmbH

Springer Fachmedien Wiesbaden GmbH

Springer Medizin Verlag GmbH

Spycutter GmbH

Squidmedia Systemhaus e.K

SRH Fernhochschule - The Mobile University

SRH Hochschule Berlin (Fachhochschule)

ssystems GmbH

Staatliche Berufsschule I Bayreuth

Staatsanwaltschaft Köln

Staatsinstitut für Frühpädagogik

Staatskanzlei des Landes Mecklenburg-Vorpommern, Landesmarketing MV

Staatsministerium Baden-Württemberg

stacktrace GmbH

Starke + Reichert GmbH & Co. KG

StartUpSecure

Staufenberg Consulting

Steen Harbach AG

Stefan Mikl - Spirit -

Stefan Pöhner – PHP Programmierer / Internetanwendungen / Webdesign

Stefan Reppien EDV GmbH

Stefan Stumm

Stefan. Baldwein.

Stephan Gitter GITTER Elektronik

steracon GmbH

Stiegler Legal

Stiftung Münchner Sicherheitskonferenz (gemeinnützige) GmbH

Stiftung Neue Verantwortung e.V. (SNV)

Stiftung Warentest

Stiftung Wissenschaft und Politik (SWP), Deutsches Institut für Internationale Politik und Sicherheit

stoll professional software GmbH

STOP Cybermobbing

Ströer Digital Publishing GmbH

Ströer Media Brands GmbH

Studiengang Security Management Technische Hochschule Brandenburg

Studienkreis GmbH

Studio GAUS GmbH

Stumpf Consulting GmbH

Styletronix.NET UG

Süd IT AG

Süddeutsche Zeitung GmbH

SÜDVERS Vorsorge GmbH

SuiGenerisData GmbH

Sunlight Security GmbH

Suppan Consulting GmbH

Surfen mit SIN(N) - Sicherheit im Netz

Susanne Borghoff

suxeedo GmbH

SVDSB UG (haftungsbeschränkt)

Sven Jürgens

Sven Thöne -IT-Dienstleistungen-

SWING Gesellschaft für EDV-Systemlösungen mbH

SWS Computersysteme AG

Symantec (Deutschland) GmbH

synalis GmbH & Co. KG

Synargos GmbH

SYNAXON AG

synetics GmbH

syracom consulting AG

syret GmbH

Syskron GmbH

SySS GmbH

Systancia Deutschland

Systemhaus Erdmann GmbH & Co. KG

Systemhaus GmbH

Systemhauser Bissinger GmbH

Systempartner Computervertriebs GmbH

t2informatik GmbH

TA Triumph-Adler GmbH

Tachyon Systems UG (haftungsbeschränkt)

Tajon PC-Sicherheit und Beratung GmbH

Tandberg Data GmbH

TÃœV SÃœD AG

TDSSG GmbH

TDT AG

Teachtoday

TEAL Technology Consulting GmbH

TeamDrive Systems GmbH

TeamSec GmbH

tec2date GmbH

TechniData TCC Products GmbH

Technische Hochschule Ingolstadt

Technische Universität Berlin

Technische Universität Darmstadt

Technische Universität Dort-mund

Technologie- und Managementberatung mbH

Tectia Germany - German Branch of Tectia Operations Ltd.

TeDo Verlag GmbH

Telefónica Germany GmbH & Co. OHG

Telekom Deutschland GmbH

Telekommunikation und neue Medien e.V

Telematik im Gesundheitswesen

telexiom AG

tellcom concept GmbH

Tenzir GmbH

Teralogic GmbH

Terrabit GmbH

TESIS SYSware Software Entwicklung GmbH

TfK-Technik für Kinder e.V.

Thales Management & Services Deutschland GmbH

thanh.IT Systemhaus Thanh Nguyen e.K.

THD - Technische Hochschule Deggendorf

The ADEX GmbH

THE BEAST GMBH

The Morpheus Tutorials

The unbelievable Machine Company GmbH

Thiesen Hardware- und Software-Design GmbH

Thinking Objects GmbH

Thinksurance GmbH

Thomas Bruno Mogge IT- und Kommunikationsberatung Mogge.Solutions

Thomas Huber

Thomas Krieger

Thomas Kuhn Hard- und Software

Thomas Michael Michalski IT-Dienstleistungen

Thomas W. Frick

Thomas Werning

Thomas Wilhelm IT-Dienstleistungen

Thosa-IT GmbH

Thüringer Ministerium für Inneres und Kommunales, Landespräventionsrat

Timo Jaudzim IT-Systemberatung

Tina Groll

TITAN IT & Security Solutions e.K.

Tobias Schrödel

Toedt, Dr. Selk & Coll. GmbH

Tom Albert Pfirsig

tops.net GmbH & Co. KG

Torsten Böttcher

Trägerverein der Freien Evangelischen Schule Hannover e.V

Trans4mation IT GmbH

TransFair GmbH

Transferstelle IT-Sicherheit im Mittelstand

TransMIT GmbH

transparent-beraten.de Maklerservice UG (haftungsbeschränkt)

TREND MICRO Deutschland GmbH

TRESSELT.DE Das Infoportal für Lehrer, Lehramtsantwärter und Schulleiter

TRIBUTUS Compliance Solutions GmbH

T-Systems International GmbH

T-Systems Multimedia Solutions GmbH

TTS Trusted Technologies and Solutions GmbH

TÜV Informationstechnik GmbH

TÜV Media GmbH

TÜV NORD AG

TÜV Rheinland AG

TÜV Technische Überwachung Hessen GmbH

TÜV Thüringen e.V

TUXGUARD GmbH

TWAIL UG (haftungsbeschränkt)

TWINSOFT biometrics GmbH & Co. KG

UIMC Dr. Vossbein GmbH & Co KG (UIMC)

UL International TTC GmbH (UL International)

Ulrich Klapp

UN1st-GmbH

Uniscon universal identity control GmbH

Unisys Deutschland GmbH

UNITED NEWS NETWORK GmbH 2002 - 2020

UNITY AG

Universität Bielefeld

Universität des Saarlandes

Universität Duisburg-Essen

Universität Heidelberg

Universität Konstanz

Universität Paderborn

Universität Siegen

Universität Stuttgart

Universität Trier

Universität zu Lübeck

UP KRITIS

Uptime Informations-Technologie GmbH

Urania Berlin e.V

usd AG

Utimaco IS GmbH

valvisio consulting GmbH

Varonis Systems (Deutschland) GmbH

VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V.

VDI

Verein Deutscher Ingeniure e.V.

VDI Verlag GmbH

VDI Wissensforum GmbH

VDI Württembergischer Ingenieurverein e.V

VDMA e.V

VdS Schadenverhütung GmbH

VdS Schadenverhütung GmbH (VdS)

VegaSystems GmbH & Co. KG

Verband der Automobilindustrie e.V. (VDA)

Verband der TÜV e.V.

Verband für Sicherheit in der Wirtschaft Berlin-Brandenburg e.V.

Verband für unbemannte Luftfahrt e.V. (UAV DACH)

Verband kommunaler Unternehmen e.V. (VKU)

Verbraucherzentrale Nordrhein-Westfalen e.V

Verbraucherzentrale NRW e.V

VERE e.V. (Verband zur Rücknahme und Verwertung von Elektro- und Elektronik-Altgeräten e.V.)

Verein Bürgerinnen und Bürgernetz e.V.

Verein für Sicherheitspartnerschaft in Schöneiche bei Berlin e.V.

Verein mathematisch-naturwissenschaftlicher Excellence-Center an Schulen e.V. (Verein MINT-EC)

Vereinigung der Aufsichtsräte in Deutschland e.V. (VARD)

Vereinigung für die Sicherheit der Wirtschaft e.V. (VSV)

Verifone GmbH

Verimi GmbH

Verizon Deutschland GmbH

VERLAG C.H.BECK oHG

Verlag Dr. Otto Schmidt KG

Verlag Werben & Verkaufen GmbH

Verlagsanstalt Handwerk GmbH

Verlagsgesellschaft Madsack GmbH & Co. KG

versicherungs- und finanzkontor friedrichs gmbh

Versicherungsbote Verlag UG

Versicherungsbüro Michael F. Stefer

Versicherungsforen Leipzig GmbH

Versicherungsmakler Rosanowske GmbH % Co. KG

Vertriebssoftware24 GmbH i.G.

VFR Verlag für Rechtsjournalismus GmbH

VGH Versicherungen

VHV Allgemeine Versicherung AG

viadee Unternehmensberatung AG

VICCON GmbH

VINCI Energies Deutschland ICT GmbH

VINDLER GmbH

VINTIN GmbH

Virtual Solution AG

Virus Help Munich

vis Gesellschaft für innovative Informationstechnologien mbH

VISTEC Internet Service GmbH

viventu solutions GmbH

VKU Service GmbH

Vogel Communications Group GmbH & Co. KG

Vogel Communications Group GmbH & Co.KG

Vogel IT-Medien GmbH

Volker Blees Rechtsanwalt u. Fachanwalt für Informationstechnologierecht

Volkmar Krannich

Volkshochschule Taufkirchen e.V

VORAX-IT GmbH

VTRUST GmbH

W&B GmbH

WAGO Kontakttechnik GmbH (nach Schweizer Recht) & Co. KG

WakeUp Media GbR

Waltraud Falkenberg e.Kfr.

wandrey GmbH

Warth & Klein Grant Thornton AG Wirtschaftsprüfungsgesellschaft (WKGT)

Was-Ist-Malware

waveit GmbH

WEBMARKETIERE GmbH

Wege aus der Einsamkeit e.V.

Wegweiser Media & Conferences GmbH

Wegweiser Media & Conferences GmbH Berlin

Weizenbaum-Institut für vernetzte Gesellschaft

WEKA BUSINESS MEDIEN GmbH

WEKA FACHMEDIEN GmbH

Welotec GmbH

Werbeagentur GmbH

Werbung-Web-Design GmbH

Werner Fromm EDV-Beratungs GmbH

Werth IT GmbH

Wessing & Partner Rechtsanwälte mbB

Westdeutscher Rundfunk Köln

Westermo Data Communications GmbH

Westfälische Hochschule (Fachhochschule)

Westfälische Provinzial Versicherung Aktiengesellschaft

Westküste UG (haftungsbeschränkt)

WGM Consulting GmbH

WGS IT GmbH

White Rabbit Security GmbH

wibocon Unternehmensberatung GmbH

Widas Concepts GmbH

Widas ID GmbH

Wiley-VCH Verlag GmbH & Co. KGaA

Willis Towers Watson GmbH

Wimmer IT GmbH & Co. KG

Wirtschaft digital Baden-Württemberg

WIRTSCHAFTScampus

Dr. Peemöller GmbH

Wirtschaftsförderung Land Brandenburg GmbH (WFBB)

Wissenschaftlicher Beirat des Cyber Security Body of Knowledge (CyBOK)

WIT GmbH

witdacon GmbH & Co. KG

Wittmann IT-Dienstleistungen

WMC Wüpper Management Consulting GmbH

WOLF Protection GmbH

Wolf Schwarm IT GmbH

Wolfgang Goethe-Universität Frankfurt

Wolfgang Krämer Computer Systeme

Wolters Kluwer Deutschland GmbH

Women in Cybersecurity Awards

Working ICT GmbH

WS IT-SYSTEME GmbH

WTI-Frankfurt-digital GmbH

Würth IT GmbH

Württembergische Gemeinde-Versicherung a.G

WWS-InterCom GmbH

www.cyber-security.online

www.internetwache.org

www.kostnix-web.de

www.schulprobleme.info

XignSys GmbH

x-ion Gesellschaft mit beschränkter Haftung

xiv-consult GmbH

x-tention Informationstechnologie GmbH

XXV Versicherungsmakler GmbH & Co. KG

yeebase media GmbH

Z_Punkt GmbH, The Foresight Company

ZAEVERS GmbH

za-networks GmbH

Zentrale für Unterrichtsmedien im Internet e.V

Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)

Zentralverband des Deutschen Handwerks e.V. (ZDH)

Zentralverband Elektrotechnik- und Elektronikindustrie e.V. (ZVEI)

Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e.V. (ZKI)

Zentrum Bayern Familie und Soziales, Bayerisches Landesjugendamt

Zentrum Digitalisierung.Bayern (ZD.B)

Zentrum für Schulqualität und Lehrerbildung

Zertificon Solutions GmbH

Zscaler Germany GmbH

Zukunftsforum Öffentliche Sicherheit e.V.

Zukunftsinstitut GmbH

Zürich Beteiligungs-Aktiengesellschaft (Deutschland)

Zweigniederlassung der Springer-Verlag GmbH

Impressum

Herausgeber

Bundesministerium des Innern, für Bau und Heimat (BMI)

Bezugsquelle

Bundesministerium des Innern, für Bau und Heimat

Alt-Moabit 140

10557 Berlin

Stand

November 2020

Druck

MKL Druck GmbH & Co.KG, 48346 Ostbevern

Gestaltung

PwC GmbH WPG

Grafiken

BMI

Artikelnummer

BMI20013

www.bmi.bund.de