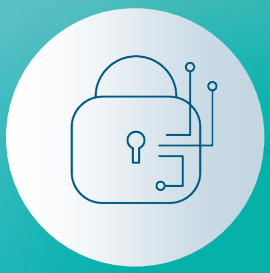
Fraunhofer

Wettbewerbsfaktor

Cybersicherheit



Aktueller Stand

Die digitale Transformation der Wirtschaft bietet große Wettbewerbspotenziale für den Wirtschafts- und Forschungsstandort Deutschland. Aber aus den digitalen Möglichkeiten erwachsen auch Risiken und Bedrohungen. Cyberkriminalität ist bereits heute allgegenwärtig, wenn beispielsweise Daten entwendet werden oder Hacken als Instrument in Kriegen genutzt wird.

Der jährlich durch Cyberkriminalität verursachte Schaden für die deutsche Wirtschaft steigt kontinuierlich; derzeit beträgt er rund 180 Mrd. €.[1] Das Bundesamt für Sicherheit in der Informationstechnik (BSI) attestiert, dass die Bedrohung im Cyberraum aktuell so hoch wie nie zuvor ist.[2] Oftmals fehlt es Unternehmen an Fachkräften, Know-how und Ressourcen, um Cyberangriffe effizient abwehren zu können. Auch in Zukunft wird die Cybergefährdung weiter ansteigen. Zudem ist Deutschland stark abhängig von ausländischen Hard- und Softwaremonopolisten.

Trotz zahlreicher Initiativen auf nationaler und EU-Ebene gibt es in Deutschland bei der Cybersicherheit noch großen Nachholbedarf. Im IMD[3] Digital Competitiveness Ranking belegt Deutschland beim Thema Cybersicherheit nur einen Platz im Mittelfeld. Es besteht die Gefahr, dass Deutschland international weiter abgehängt wird. Insbesondere die starke organisatorische und gesetzgeberische Fragmentierung erschwert es den Akteuren, schnell zu handeln.

Die angewandte Cybersicherheits- und Cyberresilienzforschung leistet im Wettlauf zwischen Angriff und Verteidigung entscheidende und frühzeitige Beiträge zu Prävention, Abwehr und Aufklärung. Sie ist fundamentaler Baustein aller Digitalisierungsstrategien und trägt dazu bei, das Sicherheitsniveau Deutschlands deutlich zu erhöhen, um Menschen, Unternehmen, kritische Infrastrukturen (KRITIS)[4] und den Staat gegenüber Angriffen nachhaltig resilient zu machen. Deutschland verfügt im Bereich Cyberresilienz über eine exzellente Forschungslandschaft mit international renommierten Einrichtungen, Instituten und Forschungsclustern. Angesichts des Ausmaßes, in dem die Bedrohungen im Cyberraum zunehmen, ist es jedoch erforderlich, noch stärker in die Forschung, Entwicklung und Umsetzung von Maßnahmen zur Cyberabwehr und Cyberresilienz sowie in die Schaffung geeigneter Rahmenbedingungen zu investieren.

[1] https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/DE/2024/2024-08-28-studie-bitkom.html

[2] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.html?nn=129410

[3] https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-competitiveness-ranking/rankings/wcr-rankings/#_tab_Rank

[4] »Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.« https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/kritis_node.html

Unsere forschungspolitischen Empfehlungen

Unsere Empfehlungen im Fokus

- Um den Cybersicherheitsstandort Deutschland souverän zu gestalten, bedarf es der **strukturellen Stärkung von Testlaboren und Zertifizierungsstellen** (samt niedrigschwelligem Zugang für KMU und Start-ups) sowie einer verstärkten **Förderung** bei der Forschung und Entwicklung von **Security-Testing-Werkzeugen** »made in Europe«.
- Cybersecurity-Aktivitäten sind kostspielig und rechnen sich erst im Falle eines Angriffs. Daher ist ein **langfristig geförderter Kompetenzaufbau erforderlich**. Dazu zählt beispielsweise die gezielte **finanzielle Förderung** von **KMU und Start-ups** im Bereich Cybersecurity-Know-how, z. B. durch Sonderabschreibungen sowie die **Einrichtung eines Cybersecurity-Pakts.**
- Um Cyberregulierung in Deutschland ganzheitlicher betrachten und so gezielter steuern zu können, bedarf es der **Weiterentwicklung der Cybersicherheitsstrategie** (u. a. unter Einbeziehung des EU-Kontexts), **des KRITIS-Dachgesetzes** und **des Digitalchecks.**
- Forschungsstrukturen im Bereich Cybersicherheit müssen auf die **Bedarfe der Wirtschaft** ausgerichtet werden. Deshalb gilt es, **regionale Forschungszentren** mit thematischen Schwerpunkten im Bereich Cybersicherheit zu **stärken** sowie **Frühwarnsysteme** noch umfassender in den Fokus der **Forschungsförderung** zu nehmen.
- Um die **Cybergovernance-Struktur** bündeln und damit effizienter aufstellen zu können, braucht Deutschland ein gestärktes und **unabhängiges BSI**, eine **Reform des Nationalen Cyber-Sicherheitsrats (NCSR)**, die **Weiterentwicklung des Nationalen Cyber-Abwehrzentrums** sowie die Schaffung einer/eines **Bundesbeauftragten für Cybersecurity**.
- Dem Staat kommt die Rolle zu, als »First Mover« zu agieren und **Zero-Trust-Strategien** in seinen eigenen IT-Infrastrukturen verpflichtend einzuführen, um den Schutz sensibler Daten deutlich zu verbessern. Die Einführung von Backdoors sollte in diesem Kontext verboten werden.
- Um »**Ethical Hacking**« zu **legalisieren** und damit die Cybersicherheitsforschung zu stärken, gilt es, rechtliche Klarheit durch die **Anpassung des Strafrechts zu schaffen.**

Im Fokus: Den Cybersicherheitsstandort Deutschland zukunftsfest und souverän gestalten

Cybersecurity-Know-how ist ein zentraler Standortfaktor, der über die digitale Zukunftsfähigkeit und Souveränität einer Region und eines Landes mitbestimmt. Der Auf- und Ausbau von Testlaboren und Zertifizierungsstellen spielt dabei eine Schlüsselrolle. Solche Einrichtungen ermöglichen es, Produkte und Infrastruktur bis auf die Hardwareebene zu analysieren und zu zertifizieren, wodurch einheitliche Sicherheitsstandards etabliert werden können. Prüflabore benötigen hochautomatisierte, leistungsfähige und vertrauenswürdige »Security Testing Tools« für Software und Hardware, die idealerweise bereits entwicklungsbegleitend bei den Produktherstellern zum Einsatz kommen. Die internationale Kooperation mit europäischen Partnern sowie führenden Nationen im Bereich der Cybersicherheit (wie Israel und den USA) ist dabei von besonderer Bedeutung. Es muss jedoch stetig hinterfragt werden, inwieweit wir Cybersecurity-Lösungen außerhalb der EU allgemein vertrauen können: Echte digitale Souveränität erlangen wir nur mit Lösungen »made in Europe«.

Leistungsfähige Prüflabore und -werkzeuge sind unabdingbar, setzen allerdings erst spät in der Entwicklung an. Denn sie analysieren bzw. zertifizieren erst das fertige Produkt. Um eine umfassende Cyberresilienz zu erreichen, ist es notwendig, Produkte gemäß dem Paradigma »Security by Design« zu entwickeln. Dies beginnt bei vertrauenswürdigen Chipdesigns und erstreckt sich über die gesamte Lieferkette bis hin zu sicheren Updateprozessen im Betrieb.

Aufgrund der immer komplexeren Handelsbeziehungen erfolgen Cyberangriffe zunehmend nicht mehr nur direkt, sondern auch über Lieferketten. Das bedeutet, dass anstelle eines bestimmten Unternehmens die Angriffe bei Lieferanten und Drittanbietern durchgeführt werden. Besonders mit Blick auf KRITIS-Einrichtungen rücken dort Komponententeile in den Fokus, die nicht in Deutschland oder Europa hergestellt werden und so Einfallstore für Cyberangriffe darstellen können. Deshalb sind Technologien erforderlich, die durchgehend sichere Lieferketten gewährleisten. Open-Source-Hardware wie etwa RISC-V spielt hierbei eine zentrale Rolle, da sie die erforderliche Transparenz und Flexibilität bietet, um unabhängige Technologien entwickeln zu können. Tools zur Bewertung und Verifikation von Hardware sind ebenfalls unverzichtbar, um die Sicherheit einer Vielzahl von Geräten zu gewährleisten. Um hier entsprechende Impulse setzen zu können, ist die finanzielle Unterstützung von Open-Source-Projekten erforderlich.

Um den Cybersicherheitsstandort Deutschland zukunftsfest und souverän zu gestalten, empfiehlt die Fraunhofer-Gesellschaft die Umsetzung der folgenden Maßnahmen:

Security-Testing-Technologien und Prüflabore »made in Europe«

- **Forschung und Entwicklung von Security-Testing-Werkzeugen**: Im Interesse der digitalen Souveränität gilt es, europäische Werkzeuge zur Überprüfung von IT-Systemen auf Cybersecurity-Schwachstellen zu entwickeln. Die Erforschung und Entwicklung produktreifer, leistungsfähiger und vertrauenswürdiger Werkzeuge muss langfristig finanziell gefördert werden.
- **Praxisnahe Standards und Gütesiegel**: Es sollten verbindliche und praxisorientierte Standards und Gütesiegel entwickelt werden, um ein hinreichendes Sicherheitsniveau für Produkte und Systeme zu gewährleisten.
- **Aufbau von Testlaboren und Zertifizierungsstellen**: Um die Sicherheit von Produkten und Systemen kontinuierlich zu überprüfen und zu steigern, sind Testlabore und Zertifizierungsstellen notwendig. Das schließt die Etablierung eines Zertifizierungsschemas für die bestehenden Testlabore und Zertifizierungsstellen ein. Von Anfang an mitzudenken ist ein **niedrigschwelliger Zugang für KMU**, damit diese die Anforderungen aus dem Cyber Resilience Act (**CRA**) und der **NIS2-Verordnung** einfacher umsetzen können.

Supply-Chain-Sicherheit

- Die Bundesregierung muss sich für eine **Anpassung der Richtlinien für staatliche Vergabeverfahren** einsetzen. Nur so können bei sicherheitskritischen Produkten Anbieter innovativer Lösungen aus der EU bevorzugt werden, was die Abhängigkeit von Know-how aus z. B. totalitären Regimen reduziert.

Systematischer Kompetenzaufbau

- Es ist erforderlich, mit den Bundesländern (analog zum Digitalpakt) einen **Cybersecurity-Pakt** zu schließen, um dringend benötigte Fähigkeiten im Bereich der Computer- und Cybersecurity-Fertigkeiten in das Bildungswesen zu tragen.
- Cybersecurity-Aktivitäten sind für Unternehmen kostspielig und rechnen sich erst im Falle eines Angriffs. Aufgrund der hohen Bedeutung von Cybersecurity-Know-how bedarf es einer gezielten **Förderung von KMU und Start-ups** durch **Sonderabschreibungen für Cybersecurity-Forschung** und den **Abschluss langfristiger Lieferverträge/Beauftragungen**.

Im Fokus: Ganzheitliches Lagebild zur Cybersicherheit etablieren

In Deutschland ist die Anzahl der relevanten Cybersicherheitsakteure infolge der Cybersicherheitsstrategie (2011) kontinuierlich gestiegen. Auf Bundesebene gibt es mittlerweile über 80 Akteure[5], die für Teilbereiche der Cybersicherheit zuständig sind. Dieses fragmentierte System führt oft dazu, dass zu viele Gesetze, Meldesysteme, Sicherheitsanforderungen und Empfehlungen nebeneinander bestehen, aber nicht miteinander kompatibel sind. Damit Cybersicherheitsgesetze zielgerichteter wirken, Meldeverfahren bürokratiearm eingehalten werden können und Kompetenzverteilungen nicht zum Kompetenzwirrwarr werden, bedarf es einer ganzheitlichen Betrachtung der Cyberregulierung in Deutschland. Diese muss mit der Schaffung einer effizienter aufgestellten Governancestruktur einhergehen, die u. a. auf Aufgabenbündelung setzt.

Ein wichtiger Schritt bei der ganzheitlichen Betrachtung von Cyberregulierung wurde bereits mit dem KRITIS-Dachgesetz unternommen. Zentral hierfür ist aus unserer Sicht eine zielführende und föderal-übergreifende Weiterentwicklung der Cybersicherheitsstrategie. Je früher ein Cyberangriff erkannt wird, desto eher können Maßnahmen ergriffen werden. Deshalb muss die Mandatierung einer bestehenden Behörde für ein nationales Frühwarnsystem Teil der Cybersicherheitsstrategie sein.

Zur Gewährleistung der notwendigen Schlagkraft der Cybersicherheitsarchitektur in Deutschland sind klarere und gebündelte Strukturen sowie ein ganzheitliches Lagebild zur Cybersicherheit erforderlich. Dafür schlagen wir folgende Maßnahmen vor:

Ganzheitliche Betrachtung der Cyberregulierung

- **Abwehr von physischen und Cyberangriffen**: Mit dem **KRITIS-Dachgesetz** (KRITIS-DachG) wurde ein wichtiger Schritt dahingehend unternommen, beide Dimensionen gemeinsam in einem Gesetz zu adressieren. Nun gilt es, dieses Vorhaben weiterzuentwickeln und es mit einem echten »**Allgefahrenansatz**« auf ein stabiles **Fundament** zu stellen. Neben der Bündelung der Zuständigkeiten für die einzelnen Angriffsarten ist zudem eine integrierende **Strategie erforderlich**, welche die fragmentierten **Förderlinien zusammenführt** und eine **Brücke zum Zivil- und Katastrophenschutz** schlägt.
- Überarbeitung des Digitalchecks: Um Vorhaben digitaltauglich zu gestalten, ist ein um **das Prinzip der Cyberresilienz erweiterter Digitalcheck** für Regelungsvorhaben erforderlich.
- **Weiterentwicklung der Cybersicherheitsstrategie**
  - In Deutschland sind die Cyberkompetenzen auf unterschiedliche Ministerien verteilt. Die derzeitige Cybersicherheitsstrategie muss nach den **Vorbildern USA und Israel** weiterentwickelt werden. Eine ambitionierte, übergreifende Strategie darf nicht wie derzeit an den föderalen und Ressortgrenzen enden – sie muss auch den **EU-Kontext einbeziehen**.
  - Darüber hinaus bedarf es einer **jährlichen Evaluation** samt **konkreterer, zeitlich, quantitativ und qualitativ messbarer Teilziele** zur effektiven Steuerung. Die Ziele müssen hinsichtlich ihrer **kurz- und langfristigen Wirkung differenziert** werden. Die Einführung von **Backdoors**, die Dritten Zugriff ermöglichen könnten, sollte **verboten** werden, um die Integrität der Sicherheitsmaßnahmen nicht zu untergraben.

Schaffung von Frühwarnsystemen

- Bisherige, rein auf »Opfersysteme und -netze« fokussierte Cyberabwehrsysteme funktionieren reaktiv. Um **präventiv handeln zu können**, ist es deshalb wichtig, Strukturen zu etablieren, die **aktive, täterzentrierte Informationsbeschaffung betreiben und damit Täterwerkzeuge, -methoden und -infrastrukturen ermitteln und erforschen**. Hierzu ist die Mandatierung und auskömmliche Finanzierung einer Behörde für aktive, täterzentrierte Informationsbeschaffung erforderlich.

Stärkung von Forschungsstrukturen für Cybersicherheit

- Mit der Strategie zur Errichtung und zum Ausbau von Forschungszentren für Cybersicherheit wurde ein wichtiger Schritt unternommen, um die Cybersicherheitsforschung in Deutschland voranzubringen. Nun gilt es, die

[5] https://www.interface-eu.org/publications/deutschlands-staatliche-cybersicherheitsarchitektur

regionalen Forschungszentren mit thematischen Schwerpunkten im Bereich Cybersicherheit zu stärken.

- Die künftige **Forschungsförderung für Cybersicherheit** muss sich stärker an praxisnahen Projekten ausrichten. Vorbild hierfür könnte die aktuelle Förderung von **Cybersicherheit in der 5G-/6G-Digitalisierung** sein. Erforderlich sind weitere ähnliche Forschungsinfrastrukturen für die angewandte Forschung, welche sich an realistischen, großen und komplexen Systemen orientieren.

Schaffung einer effizienten Governancestruktur:

- **BSI**: Mit dem BSI verfügt die Bundesregierung über eine wichtige Einrichtung auf Bundesebene, die als zentrale Anlaufstelle in der Cybersicherheitsarchitektur fungieren kann. Damit das BSI dieser Rolle gerecht werden kann, muss es **strukturell gestärkt** werden. Das bedeutet, dass das BSI **unabhängiger werden** muss, indem es aus dem Einflussbereich der Bundesministerien genommen wird.
- **NCSR**: Neben einer BSI-Neuordnung sollte auch der **NCSR reformiert** werden. Damit der Rat seine Aufgaben künftig besser erfüllen kann, bedarf es u. a. einer **Erweiterung um die Bereiche Wissenschaft/ angewandte Forschung und Zivilgesellschaft**.
- **Nationales Cyber-Abwehrzentrum**: Zur Stärkung der Abwehr von Cyberangriffen ist es sinnvoll, das Cyber-Abwehrzentrum zu einer **operativen Cyberabwehr** umzufunktionieren. Dafür wäre es u. a. notwendig, das Cyber-Abwehrzentrum mit einem **eigenen, auskömmlichen Budget** auszustatten.
- **Bundesbeauftragte/r für Cybersecurity/Informationssicherheit**: Ähnlich der Stelle der/des Bundesdatenschutzbeauftragten sollte eine Stelle für Cybersecurity/Informationssicherheit geschaffen werden, welche befugt ist, das Thema Cybersecurity interministeriell zu koordinieren.

Im Fokus: Moderne Cybersicherheitsinfrastrukturen

Moderne Cybersicherheitsinfrastrukturen erfordern sichere und vertrauenswürdige Hardware und Software als Grundlage für zuverlässige digitale Produkte und Infrastrukturen. Vertrauenswürdige Hardware und Software basieren auf dem Prinzip »Security by Design«, bei dem Sicherheitsaspekte schon in der Entwicklungsphase berücksichtigt und Produkte regelmäßig auf Schwachstellen geprüft werden.

Zero-Trust-Konzepte bilden eine zentrale Säule moderner Sicherheitsstrategien, da sie davon ausgehen, dass kein Netzwerk oder Gerät per se vertrauenswürdig ist. Stattdessen wird jeder Zugriff streng überwacht und authentifiziert, unabhängig von seinem Ursprung. Diese Strategie ist besonders relevant für Behörden und andere öffentliche Einrichtungen, die mit sensiblen Daten umgehen und/oder besonderen operativen Sicherheitsanforderungen unterliegen, etwa Behörden und Organisationen mit Sicherheitsaufgaben (BOS) oder KRITIS.

Die Aufdeckung und Analyse von Schwachstellen in Hard- und Software ist ein zentraler Bestandteil der Cybersicherheitsforschung. Forschende stehen jedoch häufig vor rechtlichen Unsicherheiten, wenn es darum geht, wie sie ihre Erkenntnisse weitergeben oder veröffentlichen dürfen. Insbesondere im Strafrecht bestehen Risiken, wenn Sicherheitslücken an die Öffentlichkeit gelangen oder betroffenen Unternehmen gemeldet werden. Um die Zusammenarbeit zwischen Forschung, Industrie und Behörden zu fördern, ist eine Anpassung des Strafrechts erforderlich.

Einsatz von Open-Source-Vertrauensankern

- Besonders in sicherheitskritischen Bereichen sollten Open-Source-Lösungen entwickelt und verwendet werden, um die Transparenz und Überprüfbarkeit der Systeme zu gewährleisten. Dies erfordert auch die **finanzielle Förderung von Open-Source-Projekten und -Audits.**

Verpflichtende Implementierung von Zero-Trust-Konzepten in Behörden

- Behörden sollten Zero-Trust-Strategien verpflichtend einführen, um den Schutz sensibler Daten deutlich zu verbessern.
- Der **Staat** sollte dabei u. a. über innovative öffentliche Beschaffung (IÖB)[6] eine **Vorreiterrolle** einnehmen und als »First Mover« agieren, indem er **moderne Sicherheitskonzepte frühzeitig in der öffentlichen Verwaltung umsetzt**. Gleichzeitig ist es entscheidend, die **End-to-End-Verschlüsselung konsequent zu stärken**, um sicherzustellen, dass Daten bei der Übertragung optimal geschützt sind. Auch hier sollte im Sinne der Sicherheitsintegrität die Einführung von **Backdoors verboten** werden.

Reform des Strafrechts zur Unterstützung der Cybersicherheitsforschung

- Eine **Anpassung des Strafrechts** ist erforderlich, um rechtliche Klarheit zu schaffen und die Cybersicherheitsforschung zu fördern, insbesondere im Bereich der Analyse von Sicherheitslücken. Das Bundesministerium der Justiz (BMJ) hat hierzu in dieser Legislaturperiode einen ersten, wichtigen Referentenentwurf vorgelegt.[7] Durch die vorgezogenen Neuwahlen 2025 ist es umso wichtiger, dass die neue **Bundesregierung das Projekt wieder aufgreift und die dringend benötigte Reform durchführt.**

[6] Kompetenzzentrum innovative Beschaffung: für die innovative öffentliche Beschaffung

[7] www.bmj.de/SharedDocs/Gesetzgebungsverfahren/DE/2024_Computer-StrafR.html?nn=13870

Schnittstellen

● **Hauptbezug**
○ **Nebenbezug**

	Innovative Gesundheitsforschung	Circular Economy	Zukunftsfähige Wasserversorgung	Energiesystem der Zukunft	Leistungsfähige und nachhaltige Mobilitätswirtschaft	Digitaler Industriestandort	Cybersicherheit	Quantentechnologien	Verteidigungsforschung in der Zeitenwende	Luft- und Raumfahrt	ZukunftsMissionBau. Sicher.nachhaltig.bezahlbar.
Innovative Gesundheitsforschung	●					○					
Circular Economy		●	○	○	○	○				○	○
Zukunftsfähige Wasserversorgung		○	●			○					
Energiesystem der Zukunft		○		●	○	○				○	○
Leistungsfähige und nachhaltige Mobilitätswirtschaft		○		○	●	○				○	
Digitaler Industriestandort	○	○	○	○	○	●	○	○	○		○
Cybersicherheit						○	●	○			
Quantentechnologien						○	○	●			
Verteidigungsforschung in der Zeitenwende						○			●	○	
Luft- und Raumfahrt		○		○	○				○	●	
ZukunftsMissionBau. Sicher.nachhaltig.bezahlbar.		○		○		○					●

Über die Fraunhofer-Gesellschaft

Die Fraunhofer-Gesellschaft mit Sitz in Deutschland ist eine der führenden Organisationen für anwendungsorientierte Forschung. Im Innovationsprozess spielt sie eine zentrale Rolle – mit Forschungsschwerpunkten in zukunftsrelevanten Schlüsseltechnologien und dem Transfer von Forschungsergebnissen in die Industrie zur Stärkung unseres Wirtschaftsstandorts und zum Wohle unserer Gesellschaft.

Die 1949 gegründete Organisation betreibt in Deutschland derzeit 76 Institute und Forschungseinrichtungen. Die gegenwärtig knapp 32 000 Mitarbeitenden, überwiegend mit natur- oder ingenieurwissenschaftlicher Ausbildung, erarbeiten das jährliche Finanzvolumen von 3,4 Mrd. €. Davon fallen 3,0 Mrd. € auf den Bereich Vertragsforschung.

Kontakt

Herausgeber
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V.
Im Auftrag des Vorstands
Hansastraße 27 c, 80686 München
https://www.fraunhofer.de

Ansprechperson
Pierre Prasuhn
Zentrale der Fraunhofer-Gesellschaft, Abteilung Wissenschaftspolitik
Telefon: +49 30 688 3759-1607
E-Mail: pierre.prasuhn@zv.fraunhofer.de

Verzeichnis der Mitwirkenden

Christian Banse, Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC

Dr. Matthias Becker, Fraunhofer-Institut für Entwurfstechnik Mechatronik IEM

Prof. Dr. Eric Bodden, Fraunhofer-Institut für Entwurfstechnik Mechatronik IEM

Dr. Stefan Dziwok, Fraunhofer-Institut für Entwurfstechnik Mechatronik IEM

Dr.-Ing. Matthias Hiller, Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC

Dr. Michael Kreutzer, Fraunhofer-Institut für Sichere Informationstechnologie SIT

Dr. Dietmar Laß, Fraunhofer-Verbund IUK-Technologie

Dr. Richard Johannes Luyken, Zentrale der Fraunhofer-Gesellschaft

Dr. Matthias Meyer, Fraunhofer-Institut für Entwurfstechnik Mechatronik IEM

Alexander Nouak, Fraunhofer-Verbund IUK-Technologie

Dr. Johannes Nowak, Zentrale der Fraunhofer-Gesellschaft

Prof. Dr. Elmar Padilla, Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE

Prof. Dr. Alexander Pflaum, Fraunhofer-Institut für Integrierte Schaltungen IIS

Dr. Ulrich Pordesch, Zentrale der Fraunhofer-Gesellschaft

Pierre Prasuhn, Zentrale der Fraunhofer-Gesellschaft

Tina Stefanova, Zentrale der Fraunhofer-Gesellschaft

Maximilian Steiert, Zentrale der Fraunhofer-Gesellschaft