Fraunhofer

FRAUNHOFER-VERBÜNDE IUK-TECHNOLOGIE, VERTEIDIGUNGS- UND SICHERHEITSFORSCHUNG

STRATEGIE- UND POSITIONSPAPIER CYBER-SICHERHEIT 2020:

HERAUSFORDERUNGEN FÜR DIE IT-SICHERHEITSFORSCHUNG

Strategie- und Positionspapier Cyber-Sicherheit 2020

Strategie- und Positionspapier Cyber-Sicherheit 2020:

Herausforderungen für die IT-Sicherheitsforschung

Herausgeber

Prof. Dr.-Ing. Reimund Neugebauer
Präsident der Fraunhofer-Gesellschaft

Prof. Dr. Matthias Jarke
Vorsitzender Fraunhofer-Verbund IuK-Technologie

Prof. Dr. rer. nat. Klaus Thoma
Vorsitzender Fraunhofer-Verbund Verteidigungs- und Sicherheitsforschung VVS

Redaktion

Prof. Dr.-Ing. Jürgen Beyerer
Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB

Prof. Dr. Claudia Eckert
Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC

Prof. Dr. Peter Martini
Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE

Prof. Dr. Michael Waidner
Fraunhofer-Institut für Sichere Informationstechnologie SIT

INHALT

Mit Beiträgen der Fraunhofer-Institute

- Angewandte und Integrierte Sicherheit AISEC
- Digitale Medientechnologie IDMT
- Eingebettete Systeme und Kommunikationstechnik ESK
- Experimentelles Software Engineering IESE
- Intelligente Analyse- und Informationssysteme IAIS
- Kommunikation, Informationsverarbeitung und Ergonomie FKIE
- Nachrichtentechnik, Heinrich-Hertz-Institut HHI
- Offene Kommunikationssysteme FOKUS
- Optronik, Systemtechnik und Bildauswertung IOSB
- Sichere Informationstechnologie SIT

1 ZUSAMMENFASSUNG

Informations- und Kommunikationstechnologien (IKT) sind wesentliche Innovationstreiber für die deutsche Wirtschaft, von der Finanzbranche bis zum Maschinenbau, von der Energiewirtschaft bis zum Gesundheitssystem: »Digitale Gesellschaft«, »Industrie 4.0« und »Internet der Dinge« charakterisieren als Schlagworte eine Entwicklung, bei der die gesamte deutsche Wirtschaft von IKT durchdrungen wird und bei der die Wirtschaft konsequent die Innovationspotentiale nutzt. Dabei wird ein ebenso hoher wie dringender Bedarf an schnell wirksamer angewandter Forschung zu IT-Sicherheit und Schutz der Privatsphäre offensichtlich.

Für die Deutsche Forschung und Wirtschaft eröffnet sich die Chance, mit »Cyber Security Made in Germany« einen wesentlichen und nachhaltigen Beitrag zum Erfolg des Standorts Deutschland zu leisten. Dies umfasst sowohl die Sicherheit der Wirtschaft, des Staates und der einzelnen Bürger, als auch die Vermarktung von neuartiger Sicherheitstechnologie auf dem Weltmarkt. Die deutsche Wirtschaft wird im globalen Wettbewerb den hohen Erwartungen dadurch gerecht, dass sie über herausragende Fähigkeiten im Bereich der Systemintegration verfügt: Preisgünstige Komponenten des Weltmarkts werden mit hochwertigen Eigenentwicklungen zu einzigartigen Gesamtsystemen mit gutem Preis- Leistungsverhältnis verknüpft. Profitiert werden kann hierbei vom hervorragenden Ruf des Gütesiegels »Made in Germany«, das weltweit hohes Ansehen genießt.

»Cyber Security Made in Germany« hat das Potential, analog zu einem weiteren Erfolgsfaktor für den Standort Deutschland zu werden, wenn es gelingt, schlüssige Gesamtsysteme mit hoher Wirtschaftlichkeit, angemessen hohes Sicherheitsniveau und Schutz der Privatsphäre zu realisieren. Ein fokussiertes und koordiniertes Forschungsprogramm zur IT-Sicherheit ist eine wesentliche Voraussetzung, um die hohe technische Kompetenz des Wirtschaftsstandortes Deutschland zu erhalten und auszubauen sowie wertbeständige Lösungen zu entwickeln.

Dieses Positionspapier der Fraunhofer-Gesellschaft gibt Empfehlungen zur Ausrichtung und Schwerpunktbildung eines solchen Forschungsprogramms. Die Fraunhofer-Gesellschaft mit ihren 18 IKT-orientierten Instituten ist bestens aufgestellt, um die IT-Sicherheit zum Nutzen für Staat, Bürger und die Wirtschaft maßgeblich zu verbessern.

2 BEDEUTUNG DER IT-SICHERHEIT

Informations- und Kommunikationstechnologie (IKT) durchdringt alle unsere Lebens- und Arbeitsbereiche. IKT ist der Innovationsmotor nahezu aller Branchen, etwa Automobilindustrie, Maschinenbau, Automatisierungsindustrie, Banken und Versicherungen und natürlich die IKT-Branche selbst. IKT ist eingebettet in die zunehmend »smarter« werdenden Produkte. IKT steuert und überwacht die gesamten Herstellungsprozesse und ist das zentrale Rückgrat von Systemen der Vertriebslogistik und der erforderlichen Wartungsprozesse (z. B. Fernwartung).

Neben unbestreitbaren Vorteilen bringt diese zunehmende IKT-Durchdringung auch ganz erhebliche Risiken und Probleme mit sich. Die Enthüllungen von Edward Snowden zu den Spionageaktivitäten internationaler Geheimdienste haben dies sehr plakativ vor Augen geführt.[1] Die kritischen Branchen bzw. die KRITIS-Sektoren[2] und auch deren Kunden sind in zunehmendem Maße von einer funktionierenden, verlässlichen und resilienten IKT abhängig. Es ist deshalb für den Standort Deutschland existentiell, in kritischen Bereichen möglichst vertrauenswürdige und sichere IKT zu realisieren, wo möglich die zunehmende Abhängigkeit von vertrauenswürdiger und sicherer IKT in Schlüsselbereichen der Wirtschaft und Gesellschaft systematisch zu *reduzieren* und zugleich die vorhandene Technologie- und Systemführerschaft in kritischen Schlüsselindustrien *auszubauen*.

2.1 Kulturwandel durch Systemforschung

Die Stärken der deutschen Industrie liegen in der Entwicklung von High-Tech-Produkten für den Weltmarkt. Hierdurch entstehen Wertschöpfungen und hochqualifizierte Arbeitsplätze im Land. Diese Stärken gilt es zu bewahren und weiter auszubauen. Um dies zu erreichen, ist ein Wandel hin zu einer neuen Sicherheitskultur in den deutschen Schlüsselbranchen erforderlich. Ein solcher Wandel erfordert die Abkehr von der heute vorherrschenden Vorgehensweise, Sicherheit erst in einem sehr späten Stadium einer Entwicklung zu bedenken. Vielmehr muss Sicherheit im Sinne von »Security by Design« als integraler Bestandteil aller Phasen und Entwicklungsstufen im Lebenszyklus von Produkten, Systemen, Infrastrukturen und Dienstleistungen betrachtet werden. Dies schließt auch die Menschen und deren Ausbildung mit ein. Der Lebenszyklus umfasst die vertrauenswürdige, gesicherte Produktion smarter, verlässlicher Produkte ebenso wie deren sicheren Einsatz sowie die Etablierung sicherer Dienste und Prozesse für deren verlässlichen Betrieb. Deutschland genießt mit seiner langen Historie als Land der Ingenieure international einen hervorragenden Ruf und ist auch wegen seines eigenen hohen Anspruchs an den Privatsphärenschutz bestens geeignet, als Vorreiter für einen solchen Wandel zu agieren und damit die eigene Wirtschaft zukunftssicher aufzustellen.

[1] Dossier zur NSA-Überwachung auf SPIEGEL Online; *http://www.spiegel.de/thema/nsa_ueberwachung*

[2] *http://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/sektoren_node.html*

Ein solcher Wandel erfordert forschungspolitische Rahmen und Unterstützungen, damit neue Methoden, Technologien und systemische Ansätze konzipiert, in einem breit angelegten realen Umfeld erprobt und für den Transfer in die Praxis vorbereitet werden können. Entsprechende förderpolitische Maßnahmen sollten auf Bundesebene ressortübergreifend gebündelt werden, um sichere Lösungen für Schlüsselbranchen zu entwickeln. Dazu gehören Methoden und Verfahren zur Absicherung von existierenden Technologien ebenso wie der Ausbau von Technologieführerschaft in zentralen Bereichen der IT-Sicherheitstechnologie und die Entwicklung von Methoden, Werkzeugen und Infrastrukturen zur sicheren Integration von Lösungen.

Das Thema »Industrie 4.0«, also die vierte industrielle Revolution, ist ein zentrales Zukunftsthema für den Industriestandort Deutschland.[3] Industrie 4.0 birgt das Potenzial einer umfassenden Erneuerung der deutschen Wirtschaft. Es bestehen die Chance und die Notwendigkeit, bei den Entwicklungen im Rahmen von Industrie 4.0 die IT-Sicherheit von Anfang an mitzudenken und zu integrieren. Nur so lassen sich sichere smarte Produkte, eine vertrauenswürdige Produktion, der vertrauenswürdige Einsatz und sichere Betrieb erreichen.

Benötigt werden anwendungsnahe Lösungen, die schnell zur Marktreife geführt werden können. Da auch bei Industrie 4.0 die IKT der zentrale Innovationstreiber sein wird, müssen IKT Forschungseinrichtungen und Unternehmen eingebunden werden. Jedoch ist eine starke interdisziplinäre Zusammenarbeit mit dem Maschinenbau, der Mechatronik und der Mikroelektronik zwingend erforderlich, um den geforderten systemischen Ansatz zu entwickeln.

2.2 Rolle der Fraunhofer-Gesellschaft

Die Fraunhofer-Gesellschaft ist exzellent aufgestellt, um die Herausforderungen im engen Verbund mit der Industrie zu erkennen, zu meistern und eine führende Rolle in der Ausgestaltung des Themas IT-Sicherheitsforschung in Deutschland und Europa einzunehmen.

Fraunhofer ist die größte Forschungsorganisation für anwendungsorientierte Forschung in Europa. Mehr als 22 000 Menschen forschen in den Themenfeldern Energie, Gesundheit, Kommunikation, Mobilität, Umwelt und Sicherheit. Das Thema der Cybersicherheit wird von den FhG Instituten sehr breit und disziplinenübergreifend abgedeckt. Eine führende Rolle hierbei nehmen neben den Instituten des Verbunds für Informations- und Kommunikationstechnik und des Verbunds Verteidigungs- und Sicherheitsforschung auch Institute der Mikroelektronik und der Mikrosystemtechnik ein. Die Fraunhofer-Gesellschaft verfügt über eine international einzigartige Bündelung an Know-how, um beispielsweise innovative Sicherheitstechnologien in Hardware zu fertigen oder neue Materialien für eine erhöhte IT-Sicherheit zu entwickeln. Maßnahmen zur Erhöhung der physischen und logischen IT-Sicherheit wachsen zunehmend zusammen. Hierbei müssen auch stets die Benutzbarkeit und die menschlichen Faktoren berücksichtigt werden.

[3] Deutschlands Zukunft als Produktionsstandort sichern; Forschungsunion, Berlin 2013; *http://www.forschungsunion.de/pdf/industrie_4_0_abschlussbericht.pdf*

3 ANGEWANDTE FORSCHUNG ZUR IT-SICHERHEIT

Innerhalb der IKT ist die IT-Sicherheit ein Querschnittsgebiet.[4] Jede neue Anwendung der IKT erzeugt neue Risiken und damit neue Herausforderungen für die IT-Sicherheit und für den Schutz der Privatsphäre. Die Weiterentwicklung der Informations- und Kommunikationstechnologie selbst erzeugt neue Angriffsmöglichkeiten und stellt bekannte Sicherheitstechnologien und -verfahren in Frage.

3.1 Herausforderungen durch zunehmende Digitalisierung

Wie in der verarbeitenden Industrie, so ist auch in der gesamten Wirtschaft ein klarer Trend zu beobachten. Dieser wird mit vielen unterschiedlichen Namen beschrieben, beispielsweise ›Ubiqitious Computing‹ oder ›Internet der Dinge‹. Gemeinsam ist ihnen allen jedoch, dass Computer allgegenwärtig werden und somit die Grenze zwischen digitaler und physikalischer Welt und damit auch ein bisher verlässlicher Schutzwall schwindet. Wo noch vor wenigen Jahren kritische Infrastrukturen autonom gearbeitet haben, wurden heute bereits erste Angriffe aus der digitalen Welt auf Pumpsysteme bekannt. Dies erhöht nicht nur die potentiellen Auswirkungen von erfolgreichen Angriffen sondern macht auch ein prinzipielles Umdenken beim Umgang mit diesen Gefahren notwendig.

Große Herausforderungen für die IT-Sicherheit ergeben sich somit aus der sich ändernden Anwendungslandschaft. Zudem hat sich auch die Angriffslandschaft in den letzten Jahren dramatisch verändert. Cyberkriminalität und Cyber-Spionage haben sich professionalisiert. Angriffe richten sich zunehmend gezielt auf bestimmte Organisationen oder einzelne Personen und entziehen sich den üblichen Schutzmechanismen wie Firewalls, Anti-Viren-Programmen und Intrusion Detection Systemen. Die finanziellen Möglichkeiten der Angreifer wachsen mit dem Anstieg des Schadenspotenzials. Die Frühwarn- und Verteidigungsstrategien von Unternehmen, Verwaltung und privaten Nutzern sind dieser Situation nicht gewachsen. Neue Ansätze werden benötigt.

Zunehmend kritisch für die IT-Sicherheit wird die Haltung vieler Beteiligter, IT-Sicherheit als sekundäres Ziel zu betrachten. Produkte mit eingebetteten IKT-Elementen, wie Steuerungssensoren beispielsweise in der Medizintechnik, oder reine IKT Produkte wie Software-Programme, werden vor der Auslieferung nicht ausreichend auf Sicherheitsprobleme getestet und müssen aufwendig im Betrieb nachgerüstet werden. Manchmal ist dies gar nicht mehr möglich und es werden sehr teure Rückrufaktionen für die angreifbaren Produkte erforderlich. Standardkonfigurationen sind oft unsicher und werden im Betrieb nie geändert. Werden Systeme integriert, so prallen oft inkompatible Sicherheitsvorgaben aufeinander und die Gesamtsicherheit sinkt. Diesen Trends entgegen wirkt das Prinzip von »Security by Design«, nach dem IT-Sicherheit von Anfang an und über den kompletten Lebenszyklus eines Produkts bzw. einer Dienstleistung hinweg berücksichtigt werden muss. Hierzu gehören insbesondere neue Ansätze in der Software- und Hardwareentwicklung, wie sicherheitsfokussierte Entwicklungsprozesse, modell-getriebene

[4] Claudia Eckert, IT – Sicherheit – Konzepte, Verfahren, Protokolle; R. Oldenbourg Verlag, 2013

Sicherheit, automatisiertes Sicherheitstesten, sicherheitsfreundlichere Programmiersprachen und Verfahren zur Absicherung der Software Supply-Chains, aber auch neue Ansätze im Systemmanagement.[5]

Die Entwicklung sicherer IKT in Deutschland ist ein wichtiges Ziel, wird jedoch nur einen kleinen Teil des Problems abdecken können: Ein großer Teil der benötigten IKT muss auf dem Weltmarkt eingekauft werden. Um auch hier Sicherheit gewährleisten zu können, müssen Mindeststandards entwickelt werden und technische Methoden, wie die Einhaltung dieser Mindeststandards überprüft oder sogar nachgewiesen werden kann.

Die maximale theoretisch erreichbare Sicherheit wird in IT-Systemen selten erreicht, da die Benutzbarkeit vieler Sicherheitsmechanismen zu aufwendig oder fehleranfällig ist und nicht auf den Menschen als Anwender zugeschnitten wurde. Forschung und Entwicklung in den Bereichen der IT-Sicherheit und der digitalen Privatsphäre muss stets unter Berücksichtigung der menschlichen Aspekte und der Benutzbarkeit unternommen werden, um die praxisrelevante Einsetzbarkeit der entwickelnden Lösungen zu sichern. Hierbei müssen mit Fokusgruppen, Interviews, Labor-, Online- und Feldstudien Anforderungen erhoben, Entwürfe kontrolliert und Technologiedemonstratoren validiert werden. Nur so kann gewährleistet werden, dass die maximal praktisch erreichbare Sicherheit umgesetzt werden kann.

Hochwertige und effiziente Ausbildung sowie lebenslanges Lernen werden zu einem entscheidenden Erfolgsfaktor, sowohl für jeden einzelnen als auch für Deutschland insgesamt. Dieses beinhaltet auch das Erlernen des sicheren und verantwortungsvollen Umfangs mit IKT.

Am Beispiel des Zukunftsthemas Industrie 4.0 wird nachfolgend verdeutlicht, dass Systemforschungsansätze benötigt werden, um die komplexen Herausforderungen der Sicherheit in der digitalen Wirtschaft und der digitalen Gesellschaft zu meistern.

3.2 Sicherheits-Systemforschung am Beispiel Industrie 4.0

Das Zukunftsthema Industrie 4.0, das der vierten industriellen Revolution, verdeutlicht exemplarisch sowohl die wirtschaftlichen Chancen der deutschen Sicherheitsforschung als auch die besonderen Forschungsherausforderungen, die nur durch einen Systemforschungsansatz gemeistert werden können. In Industrie 4.0 verschwinden die Grenzen zwischen den vormals getrennten IKT-Bereichen der Wirtschaft. Produktions-IT, Vertriebslogistik, Zulieferindustrie und Business-IT werden vernetzt, und damit werden IT-Systeme mit ganz unterschiedlichen Sicherheitsanforderungen und Angriffsflächen verbunden. Angreifern eröffnen sich damit neue Möglichkeiten, in Systeme einzudringen und Schäden, auch in der physischen Welt zu verursachen. Viren, die man von Desktop-PCs kennt, finden sich auf einmal in Produktionsanlagen wieder. Maschinen werden zur Fernwartung freigegeben, ohne diese Zugänge ausreichend abzusichern.

[5] Michael Waidner, Michael Backes, Jörn Müller-Quade (Hrsg.): Entwicklung sicherer Software durch Security by Design; SIT Technical Report, Fraunhofer Verlag, München 2013; *https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Trendbericht_Security_by_Design.pdf*

Maschinen und Produkte werden in Industrie 4.0 zu intelligenten, vernetzten cyberphysikalischen Systemen. Viele dieser Systeme müssen strikten Einschränkungen hinsichtlich Größe, Energieverbrauch und Kosten genügen. Entsprechendes gilt für ihre Sicherheit: Verschlüsselungsdienste, Betriebssysteme und Anwendungen wurden bislang ohne diese Einschränkungen entwickelt und müssen deshalb neu überdacht werden. Je umfangreicher und dynamischer die Vernetzung wird, desto wichtiger wird, dass sich Systeme, bzw. auch einzelne Komponenten bis hin zu einzelnen Produkten untereinander, sicher identifizieren, als unverändert erkennen und sicher miteinander kommunizieren können. Sichere und überprüfbare Identitäten von Maschinen, der Schutz vor gefälschten und nachgemachten Produkten und die sichere Maschine-zu-Maschine Kommunikation sind neue und wichtige Herausforderungen für die angewandte IT-Sicherheitsforschung. Aber auch die Mensch-Maschine Interaktion wirft im Industrie 4.0 Umfeld neue Probleme für die IT-Sicherheit auf. Die steigende Komplexität der Netzwerke und Systeme, zusammen mit den eingeschränkten Interaktionsmöglichkeiten, erfordern neue Konzepte für benutzbare IT-Sicherheit. Insbesondere, da in diesem Umfeld Benutzer mit wenig bis keiner IT-Expertise mit den Systemen sicher arbeiten müssen.

Entlang der gesamten Wertschöpfungskette bzw. in den entstehenden neuen Wertschöpfungsnetzen werden in Industrie 4.0 bestehende Produktions- und Geschäftsfunktionen aufgebrochen und auf unterschiedliche, oft voneinander wirtschaftlich unabhängige Parteien verteilt. Das Internet ist das zentrale Kommunikationsmedium, Cloud-Computing das zentrale Paradigma zur Erbringung kostengünstiger, standardisierter IT-basierter Dienste. Damit dies gelingt, werden sichere und vertrauenswürdige Identitäten auch für Dienste und Menschen benötigt. Dienste müssen sicher, dynamisch und über Organisationsgrenzen hinweg integrierbar sein. Die Kommunikation muss zuverlässig und sicher erfolgen, und die Systeme müssen über lange Zeiträume resilient und verlässlich arbeiten trotz zunehmender Cyber-Angriffe. Die verarbeitenden Daten und Informationen sind das ›Öl‹ der Industriegesellschaft. Starke Maßnahmen zum Schutz vor gezielter Wirtschaftspionage sind für das Überleben der Deutschen Hightech-Industrie, insbesondere des Mittelstandes im Maschinen- und Anlagenbau, unerlässlich. Daten in der Cloud müssen gegen unerlaubten Zugriff geschützt sein. Wer Daten in der Cloud verarbeiten lässt, muss darauf vertrauen können, dass die Verarbeitung korrekt und sicher erfolgt. Kurzfristig fehlt es an Prüfkriterien und -methoden. Mittelfristig fehlen effiziente und nutzerfreundliche Verschlüsselungstechniken, die die Sicherheit der Verarbeitung in der Cloud erzwingen.

Alle Elemente in Industrie 4.0 – Menschen, Maschinen, Produktionsanlagen, Geschäftsfunktionen, Produkte und Dienste – erzeugen ständig Daten. Die Optimierung von Ressourcen und der Wertschöpfungskette insgesamt profitiert davon, wenn diese Daten in Realzeit zusammengeführt und effizient analysiert werden können. Dieses sogenannte ›Big Data-Paradigma‹ birgt offenkundige und größtenteils ungelöste Probleme für den Informationsschutz von Unternehmensdaten und den Schutz der Privatsphäre von Bürgern. Zugleich birgt »Big Data« aber auch die Chance, unbekannte Angriffe schneller erkennen und abwehren zu können. Die Erhebung qualitativ hochwertiger, nicht manipulierter Daten aus unterschiedlichen Datenquellen und deren menschengerechte Auswertung in Echtzeit sind die Voraussetzung für eine verbesserte Lagebilderstellung und eine effektive Reaktion im Problem- oder Notfall. Auch dies erfordert umfangreiche neue Forschung.

Die Arbeitnehmer in Industrie 4.0 sind mobil, organisieren sich global und handeln oft selbstständig. Arbeitszeiten und -orte sind flexibel. Dementsprechend muss die IKT für die Arbeitnehmer mobil, vielseitig und sehr einfach verwendbar sein. Auch hinter diesen Anforderungen verbergen sich Herausforderungen für die Forschung: von der Kommunikationssicherheit in mobilen Netzen über sichere Betriebskonzepte wie der sicheren und verlässlichen Integration mobiler Endgeräte in mobile Geschäftsprozesse, wie der Produktion, der Wartung oder auch dem Vertrieb und der Logistik, bis hin zum fundamentalen Problem der Benutzbarkeit von IKT und dem Abwehren von Innentäter- und Social Engineering-Angriffen.

Die Kapitel 5 und 6 des Positionspapiers geben einen ausführlicheren Überblick über die hier nur skizzierten aktuellen Forschungsfragen und erläutern konkrete technologische Ansätze, um die damit adressierten Forschungsprobleme zu lösen.

4 FORSCHUNGSAGENDA »CYBER-SICHERHEIT 2020«

Die Fraunhofer-Gesellschaft schlägt ein Sieben-Punkteprogramm für eine nationale Forschungsagenda »Cyber-Sicherheit 2020« vor:[6]

1. **Digitale Souveränität – Deutschland muss in Kernbereichen der IT-Sicherheit unabhängig werden**
   Das Forschungsprogramm muss die Entwicklung flexibler, durch Dritte überprüfbarer IT-Sicherheitslösungen als Vertrauensbausteine IKT-basierter Infrastrukturen unterstützen. Ziel soll sein, die technologische Unabhängigkeit Deutschlands in Schlüsselbereichen der IKT, wie Unternehmenssoftware und eingebettete Systeme, und im Kontext branchenübergreifender Zukunftsprojekte[7] , wie Industrie 4.0 und Internet-basierte Dienste für die Wirtschaft zu gewährleisten.

2. **Anwendungslabore zur Cyber-Sicherheit – Sicherheitsforschung muss sich im praktischen Einsatz bewähren**
   Das Forschungsprogramm muss mit einer groß angelegten Offensive zur Sicherheitsforschung im Kontext eines Zukunftsprojekts, z. B. Industrie 4.0, ein interdisziplinäres Systemforschungsprojekt starten. Durch den Aufbau und Betrieb industrienaher Anwendungslabore müssen Möglichkeiten und Wirksamkeit der neuen Systemlösungen gegen Cyberkriminalität und Wirtschaftsspionage empirisch untersucht und demonstriert werden.

3. **Security by design – Sicherheit muss von Anfang an mitgedacht werden**
   Das Forschungsprogramm muss die Entwicklung von Methoden, Prozessen und Werkzeugen unterstützen, so dass die Sicherheit über den gesamten Lebenszyklus von Produkten, Lösungen und Diensten – also im Sinne von »Security by Design« – gewährleistet werden kann. Dies muss auch die Integration und überprüfbare Erhöhung der Sicherheit von Bestandssystemen unterstützen.

4. **Überprüfbarkeit durch Dritte – Sicherheit muss vertrauenswürdig werden**
   Das Forschungsprogramm muss die Erarbeitung neuer Ansätze unterstützen, die es ermöglichen, Komponenten, Produkte, Lösungen und Dienste über deren gesamten Lebenszyklus in Bezug auf deren Sicherheit zu prüfen und die erreichte Sicherheit nachweisbar zu machen.

5. **Privacy by Design – Verantwortung für den Privatsphärenschutz und die Vertraulichkeit persönlicher Daten**
   Das Forschungsprogramm muss gleichermaßen den Schutz von Wirtschaft, Staat und Bürgern vor Cyberkriminalität und Spionage unterstützen. Insbesondere muss der besondere Wert von persönlichen Daten berücksichtigt und deren Schutz verbessert werden. Daten, darunter ganz besonders persönliche Daten wie Kundenprofile, stellen einen erheblichen Wert für die Wirtschaft dar. Diese gilt es durch geeignete Mittel entsprechend dem Prinzip von »Privacy by Design« vor unerlaubtem Zugriff und Missbrauch zu schützen. Zum Schutz der Privatsphäre müssen Technologien und Infrastrukturen entwickelt, getestet

[6] Diese Punkte sind in Übereinstimmung mit den von den drei BMBF-Kompetenzzentren CISPA, EC SPRIDE und KASTEL am Runden Tisch zur IT-Sicherheit formulierten Empfehlungen: *http://www.cased.de/files/130917_RT-IT-Sicherheit_Forschung.pdf*

[7] Zukunftsprojekte; BMBF, Berlin 2012; *http://www.bmbf.de/de/19912.php*

und unterstützt werden, die auch angesichts Dienstanbieter außerhalb des deutschen und europäischen Rechtsraums effektiven und nachweisbaren Schutz bieten.

6. **Lagebilder für Entscheider – Wissen über die eigene (Un)Sicherheit**
   Das Forschungsprogramm muss die effiziente und aktuelle Erstellung von Lagebildern unterstützen, basierend auf der Zusammenführung und sicheren Analyse von Informationen zu Verwundbarkeiten und Sicherheitsvorfällen. Dies ermöglicht Entscheidungsträgern eine fundierte Einschätzung der Sicherheitslage und ist die Voraussetzung für ein verantwortungsbewusstes, nachhaltiges Handeln.

7. **Menschengerechte IT-Sicherheit – Technik darf den Menschen nicht überfordern**
   Das Forschungsprogramm muss die zu entwickelnden Sicherheitsmechanismen und Prozesse menschengerecht gestalten. Denn nur wenn die Mechanismen und Prozesse eine gute Benutzbarkeit aufweisen, können und werden sie fehlerfrei eingesetzt werden. Mit den entsprechenden Methoden der benutzbaren Sicherheit und Privatsphäre müssen Entwickler, Administratoren, Sicherheitsexperten sowie nicht-technische Anwender in die Lage versetzt werden, sicherheitsrelevante Aufgaben zu erfüllen. Hierbei müssen sowohl individuelle wie auch gesellschaftliche Aspekte berücksichtigt werden.

5 CHANCE UND NOTWENDIGKEIT DER DEUTSCHEN CYBER-SECURITY-FORSCHUNG

Die vorausgehenden Kapitel haben die Bedeutung der IT-Sicherheit für den Wirtschafts- und Innovationsstandort Deutschland motiviert und die wichtigsten Handlungsfelder aufgezeigt. In diesem Kapitel werden die Chancen und auch die Notwendigkeit einer Verstärkung der Deutschen Cyber-Sicherheitsforschung noch einmal ausführlicher erläutert. Im abschließenden Kapitel werden dann konkrete Vorschläge für Forschungs- und Entwicklungsaktivitäten dargestellt.

5.1 IT-Sicherheits-Forschungslandschaft

Herausragende Forschung zu Fragestellungen der IT-Sicherheit ist heute in Deutschland an Hochschulen und außeruniversitären Forschungseinrichtungen selbstverständlich. Gleichzeitig entwickeln auf der Anwenderseite Unternehmen unterschiedlichster Branchen unabhängig voneinander Sicherheitslösungen, um dem Bedarf ihrer Kunden zu begegnen. Dabei ist bis heute eine Lücke spürbar, die sich darin zeigt, dass Grundlagen-Know-how, das durch Fördervorhaben erarbeitetet wurde, und dringend notwendige praxisorientierte Ansätze nicht zur Deckung gebracht werden.

In der Förderung der IT-Sicherheitsforschung gibt es Schwerpunkte zu aktuellen und wichtigen Themen wie Sicherheit in unsicheren Umgebungen, Schutz von Internet-Infrastrukturen, eingebaute Sicherheit und Herausforderungen zum Schutz von IT-Systemen und zur Identifikation von Schwachstellen. Seit 2011 werden drei Kompetenzzentren der Grundlagenforschung zu IT-Sicherheit gefördert, um vorhandene starke Kompetenzen an Hochschulen und hochschulnahen Einrichtungen regional zu bündeln.

Zu diesen Schwerpunkten wurden unterschiedlichste Projekte gestartet, die einerseits Akzente bei der Beantwortung spezifischer Forschungsfragen setzen und andererseits notwendige Grundlagen für weitere Arbeiten legen. Einzelne Themenschwerpunkte blieben bislang offen. Trotz der intensiven Bearbeitung ausgewählter Themenschwerpunkte in geförderten Projekten ist vielfach nicht von einer abschließenden Behandlung der Themen auszugehen. Eine konsequente Übertragung in die Praxis findet nicht im notwendigen Maße statt. Dadurch besteht zu verschiedenen Schwerpunkten über die genannten aktuellen Förderprogramme hinaus auch künftig weiterer Forschungs- und vor allem Umsetzungsbedarf.

Auch durch eine fortlaufende und immer schnellere und versiertere Weiterentwicklung und Anpassung der Angreifer ist kontinuierlicher praxisnaher Forschungsbedarf gegeben.

Neue Anwendungsfelder für IT-Sicherheitsforschung entstehen kontinuierlich, z. B. bei der Energieversorgung, in den Bereichen von Mobilität und Piraterieschutz, um nur einige Themen zu nennen, die in der jüngeren Vergangenheit in den Fokus des öffentlichen Interesses gerückt sind. In vielen dieser neuen Anwendungsgebiete werden Fragen zur IT-Sicherheit bisher nur unzureichend angesprochen. Aber auch bei etablierten Themen wie Automatisierung, ›mobile Systeme‹ und Cloud Computing fehlen anwendungsnahe Lösungen.

5.2 Stärkung der anwendungsorientierten Forschung

In der aktuellen Forschungslandschaft wird ein IT-Sicherheits-Förderprogramm benötigt, das die Brücke von den Erkenntnissen und Methoden der Grundlagenforschung zur Anwendung schlägt. Sicherheit von IT-Systemen darf keine optionale Eigenschaft sein. Bereits beim Entwurf von Anwendungen, die IT-Systeme enthalten, müssen nichtfunktionale Eigenschaften wie IT-Sicherheit berücksichtigt werden. Gleichzeitig dürfen Sicherheitsanforderungen den Nutzen und die Wirtschaftlichkeit von Lösungen nicht in Frage stellen. Dasselbe gilt sowohl für den Betrieb sicherer Systeme wie auch für das Erschließen neuer Anwendungsfelder. Anwendungsorientierte Forschung ist hier in der Lage, technologische Notwendigkeiten der IT-Sicherheit und praxisorientierte Anforderungen der Unternehmen wie der Bürger in Einklang zu bringen.

Umsetzung der Grundlagen in marktfähige Lösungen

Angriffstechniken entwickeln sich in einem immer schnelleren Tempo weiter. Ihnen begegnende Sicherheitslösungen hinken in der Regel deutlich hinterher. Zudem entwickelt sich die Informations- und Kommunikationstechnik selbst in einem hohen Tempo weiter, sodass das wirtschaftliche Interesse fehlt, die Sicherheitslücken von schnell veraltenden Produkten zu schließen. Darüber hinaus wird IT-Sicherheit bei der Entwicklung und Vermarktung neuer Produkte regelmäßig als Hindernis für die schnelle Besetzung von Marktsegmenten betrachtet.

Dem kann nur durch anwendungsorientierte Forschung zum sicheren Entwurf und vor allem zum sicheren Betrieb von IT-Lösungen sowie durch neuartige Ansätze zur Erkennung und Verhinderung von Sicherheitsvorfällen begegnet werden. Erkenntnisse aus den Grundlagen müssen in systematischer Weise auf unterschiedlichste Anwendungsfelder übertragen werden. So können auch neu entstehende Anwendungsgebiete direkt von praxisnahen und erprobten Lösungsansätzen profitieren. Auf diese Weise stellt IT-Sicherheit nicht mehr ein Hindernis dar, sondern wird im internationalen Vergleich ein wirtschaftlicher Mehrwert für deutsche Unternehmen.

Schutz der Wirtschaft und der Bürger

Kaum ein IT-System ist nicht mit anderen Systemen vernetzt, kaum ein Bereich unseres Lebens ist noch ohne Unterstützung durch IT-Systeme vorstellbar. Die Tendenz ist steigend und mittlerweile gibt es viele neue Anwendungsfelder, die ohne vernetzte IT-Systeme nicht realisierbar wären.

Eine derartige Durchdringung bedeutet auch eine spürbare Abhängigkeit von Informations- und Kommunikationstechnik. Spürbar besonders dann, wenn IT-Systeme ihren Dienst versagen. Wird dieses Versagen bewusst und gezielt herbeigeführt, entstehen negative Folgen, von Umsatzausfällen über Störungen der öffentlichen Sicherheit bis hin zur Gefährdung von Menschenleben.

Kritische Infrastrukturen, die Versorgung der Bevölkerung und das Funktionieren des wirtschaftlichen Systems voneinander abhängiger Unternehmen müssen über sichere und zuverlässige IT-Systeme vor Manipulation geschützt werden.

Kosten senken

Unzureichender Schutz der IT-Infrastruktur von Unternehmen bedeutet ein immenses Risiko von IT-Angriffen. Neben unmittelbaren Umsatzausfällen und kaum zu beziffernden Reputationsschäden ist der Aufwand, um festzustellen, ob und welche IT-Systeme manipuliert wurden, kaum zu kalkulieren. Nur eine absolute Minderheit der Unternehmen verfügt über ein erprobtes Notfallmanagement. Gesetzliche Vorgaben gelten nur für wenige Branchen und doch kommt es auch hier wiederholt zu Sicherheitsvorfällen.

Unternehmen benötigen Lösungen zum Informationssicherheitsmanagement und zur Abschätzung von IT-Risiken. Zwar existieren viele Modelle – ein an der Praxis und den aktuellen technischen Möglichkeiten ausgerichtetes IT-Sicherheitsmanagement jedoch fehlt. Die anwendungsorientierte Forschung ist gefordert, diese Defizite schnellstmöglich zu beheben.

Wettbewerbsfähigkeit international ausbauen

Die deutsche Grundlagenforschung zu IT-Sicherheit und Sicherheitslösungen aus Deutschland genießen international hohes Ansehen. Bei einigen Themenfeldern wie IT-Sicherheit für Automatisierung und Energieversorgung oder Datenschutz hat Deutschland eine Vorreiterrolle. Andere Nationen wie die USA, Japan, Großbritannien, Frankreich und Italien haben jedoch ihre Märkte bereits gut entwickelt, und in Russland, China, Indien und Brasilien stellt IT-Sicherheit einen bedeutenden Wachstumsmarkt dar.[8] Es ist daher abzusehen, dass der globale Markt für IT-Sicherheit künftig noch stärker umkämpft sein wird als heute.

Die konsequente Förderung der deutschen anwendungsorientierten Forschung schafft die erforderlichen Voraussetzungen, um auf diesem global bedeutsamen Markt die deutsche Spitzenposition zu halten und zudem auf bisher weitgehend nicht erschlossene Themenfelder auszuweiten.

[8] Global IT Security Risks, Kaspersky Lab, 17. Juni 2011.

6 FORSCHUNGS- UND ENTWICKLUNGSBEDARF

Um die in Kapitel 4 skizzierten sieben Punkte *der Forschungsagenda Cyber-Sicherheit 2020* erfolgreich umzusetzen, sind in den kommenden Jahren weitere intensive Forschungs- und Entwicklungsanstrengungen erforderlich. Die Ausführungen in den Kapitel 2, 3 und 4 haben verdeutlicht, dass eine stärkere anwendungsorientierte, systemische Forschung dringend erforderlich ist. Sie haben zudem gezeigt, dass Deutschland mit seinen anwendungsorientierten Forschungsinstituten und deren enger Anbindung an die Wirtschaft sehr gut aufgestellt ist, um vertrauenswürdige Systemlösungen zu entwickeln und zusammen mit den industriellen Partnern zu marktfähigen Produkten zu veredeln. Um die technologische Souveränität des Innovationstandortes Deutschland nachhaltig zu gewährleisten und die Forschungsagenda umzusetzen, wird empfohlen, die nachfolgend detailliert beschriebenen Forschungsthemen mit hoher Priorität zu fördern. Die Themen sind in alphabetischer Reihenfolge aufgeführt.

- Cloud-Sicherheit
- Cyber-Physical Systems
- Datenschutz und Privacy Management
- Energieerzeugung und Energieversorgung
- Frühwarnsysteme
- Industrielle Produktion und Automatisierung
- IT-Forensik
- IT-Sicherheit für Mobilität
- Mediensicherheit
- Netzsicherheit
- Piraterieschutz
- Physically Embedded Cyber Security
- Secure Engineering
- Secure Mobile Systems
- Sicherheit gegen Seitenkanal- und Fehlerangriffe

- Sicherheitsmanagement
- Vertrauenswürdige Systeme
- Zusammenspiel Safety und Security

6.1 Cloud-Sicherheit

Cloud Computing ist die nächste Revolution im Umgang mit IT-Ressourcen. Das Auslagern von Hard- und Software »in die Cloud« ist ein großer Schritt hin zu einem neuen IT-Paradigma. Heute nutzen die meisten Firmen PC-Arbeitsplätze, die mit zentralen Servern im eigenen Hause verbunden sind. Das erfordert die Beschaffung von Servern, die Installation von Server-Software und schließlich auch die Pflege und Aktualisierung von Hard- und Software. Hinzu kommen Aufwendungen für Sicherheitsprogramme, Backup-Konzepte und vieles mehr. Hard- und Software kosten in der Anschaffung einmalig, in der Aktualisierung und Instandhaltung aber fortlaufend Geld. Hierfür ist eigenes Personal notwendig, das sich ausschließlich um die IT-Infrastruktur kümmert und das so für das Kerngeschäft des Unternehmens nicht zur Verfügung steht. All diese Kosten können durch Cloud Computing in einem erheblichen Umfang reduziert werden. Gerade kleine und mittelständische Unternehmen können sich dadurch wesentlich stärker auf ihr Kerngeschäft konzentrieren.

Viele potentielle Anwender des Cloud Computings sehen die Chancen, zögern aber dennoch, sich auf die neue Technologie einzulassen. Das Auslagern in die Cloud führt inhärent auch zu einem Verlust an Kontrolle. Wird man in der Cloud noch alle gesetzlichen Anforderungen, insbesondere in Bezug auf den Datenschutz, einhalten? Sind die Daten dort auch vor unbefugtem Zugriff geschützt? Sind sie von den Daten anderer Cloud-Kunden hinreichend stark getrennt? Kann man dem fremden Administrator überhaupt trauen? Bindet man das eigene Unternehmen durch den Umzug in die Cloud für lange Zeit an einen Anbieter?

Das sind, wie Studien[9] ergeben, die häufigsten Bedenken, die eine Nutzung der Cloud verhindern. Hinzu kommen Sorgen um die Verfügbarkeit der Daten in der Cloud, und auch die Tatsache, dass der Cloud-Kunde in der Regel kein Audit des Cloud-Providers durchführen kann: Der Kunde weiß nicht einmal, in welchem Teil der Welt seine Daten liegen. Diese Bedenken und Umstände führen zur Ablehnung der Technologie.

Forschungsaufgaben im Umfeld sicheren Cloud Computings umfassen:

- Modellierung von Regeln zur Einhaltung gesetzlicher Vorgaben (Compliance)
- Metriken zur Modellierung und vertrauenswürdigen Überwachung von Sicherheitsvorgaben

[9] Driving Profitable Growth Through Cloud Computing, IBM Study, 2008

- Identitätsmanagement in föderierten Cloud-Umgebungen
- Entwicklung cloudzentrierter Bedrohungsmodelle
- Mechanismen zur sicheren Virtualisierung
- Technologien, die Datenschutz und Privacy gewährleisten
- Vertrauens- und Policy-Management
- Sichere Synchronisation stationärer und mobiler Geräte über Cloud-Infrastrukturen
- Modelle und Verfahren zur Nutzung der Cloud für hochsensible Daten
- Sichere Videoanalysesysteme zur Auswertung von Live-Videoströmen im Rahmen des Cloud Computing
- Erkennung und Bekämpfung von Schadsoftware in der Cloud
- Entwicklung von Kontrollmechanismen zur Auditierung von Cloud-Dienstanbietern
- Integration von Technologien zur systematischen Datennutzungskontrolle in Cloud-Infrastrukturen

6.2 Cyber-Physical Systems

Cyber-Physical Systems (CPS) sind eingebettete Systeme. Sie verfügen über Sensoren oder Aktoren, werten eigenständig Daten aus und speichern diese. CPS sind über Netzwerke miteinander verbunden und kommunizieren über Mensch-Maschine-Schnittstellen.

Eingesetzt werden CPS für Überwachungs-, Steuerungs- und Regelfunktionen, oder sie übernehmen Funktionen der Daten- und Signalverarbeitung. Traditionell findet man eingebettete Systeme in den Bereichen Luft- und Raumfahrt, Automobilindustrie, chemische Industrie, Energie, Gesundheitswesen, Produktion und Automatisierung, Transport und Logistik und Endverbraucherlösungen wie Unterhaltungselektronik.

Die zunehmende Leistungsfähigkeit und Vernetzung von CPS erfordern neue Ansätze und Technologien für nicht-funktionale Anforderungen wie Schutz und Sicherheit. Teilweise ergeben sich diese Anforderungen erst aus der Vernetzung und müssen in vielen Anwendungsgebieten erstmals berücksichtigt werden.

Neben klassischen Fragestellungen zu Verlässlichkeit, Betriebssicherheit und Verschlüsselung der Kommunikation gibt es eine Reihe spezifischer Rahmenbedingungen. So verfügen CPS weiterhin über eine gegenüber Arbeitsplatzrechnern stark eingeschränkte Rechenleistung.

Zudem sind in vielen Fällen Größe und Gewicht der eingebetteten Systeme zu beachten. Durch die Umsetzung in Hardware sind Möglichkeiten zur Konfiguration und für Updates zur Laufzeit bereits durch den Entwurf vorgegeben.

Im Sinne einer breiten Akzeptanz von CPS sind Anforderungen an den Schutz der Privatsphäre und den Datenschutz in allen Phasen des System-Lebenszyklus' zu berücksichtigen. Entscheidend sind Eingriffsmöglichkeiten durch den Anwender und die Transparenz der Datenverarbeitung. Dabei muss insbesondere der Interdependenz von technischen, wirtschaftlichen und sozialen Prozessen Rechnung getragen werden.

Forschungsfragen im Themenfeld Cyber-Physical Systems umfassen:

- Sicherheitsfragen vernetzter intelligenter und interaktiver Technik
- Auswirkungen auf das Sicherheitsniveau und insbesondere Abhängigkeiten von spezifischen Randbedingungen wie Energiebedarf, Rechenleistung und Datenübertragung
- Forschung und Entwicklung von spezialisierten kryptographischen Verfahren und Sicherheitstechnologien
- Kombinierte Sicherheitsmechanismen in Software und Hardware: u. a. integrierte Betriebs- und Datensicherheit, zuverlässige und skalierbare Hardware und dedizierte Hardware zum Schutz gegen Manipulation und Sabotage
- Verfügbarkeit: Betriebsmodi für Notfälle, in die Cyber-Physical Systems umschalten können, wenn sie angegriffen werden
- Architekturen und Best-Practice-Ansätze zur Implementierung von Sicherheitsfunktionalitäten auf Embedded Systems
- Sicherheitsfunktionalitäten für Systeme mit geringer Systemleistung
- Redundante, diversitäre Kommunikation mit Cyber-Physical Systems
- Reputation (Vertrauenswürdigkeit) vernetzter eingebetteter Systeme insbesondere zur Ad-hoc-Vernetzung und bei Veränderungen zur Laufzeit; Sicherstellen der funktionalen Anforderungen bei Reputationsverlust
- Qualitätssicherung: standardisierte Testverfahren für definierte Sicherheitsstufen
- Verteilte intelligente Sensorik
- Verfahren zur Überprüfung der Korrektheit von Daten aus verteilten Sensoren
- Verfahren zur energieeffizienten Authentifikation in Sensornetzwerken

- Methoden zur Bestimmung des Vertrauens in Sensoren und ihre Daten bei On-demand-Integration
- Untersuchung der Echtzeitfähigkeit existierender Technologien der Datennutzungskontrolle für eingebettete Systeme
- Verfahren zur systematischen Analyse der Wechselwirkung von IT Sicherheit und Betriebssicherheit

6.3 Datenschutz und Privacy Management

Der illegale Handel mit persönlichen Daten, wie etwa E-Mail-Adressen und Adressdaten, ist ein florierendes Geschäft, über das fast jede Woche in den Medien berichtet wird. In vielen Fällen handelt es sich um Daten, die unrechtmäßig aus häufig unzureichend geschützten Systemen beschafft wurden. Die Anzahl der Datenpannen hat in der letzten Zeit beträchtlich zugenommen. Selbst große Unternehmen, darunter weltweit agierende Banken und Telekommunikationsunternehmen, waren davon betroffen. Für sie sind der Imageschaden und der damit verbundene wirtschaftliche Schaden erheblich. Darüber hinaus besteht die Gefahr rechtlicher Auseinandersetzungen wegen Verletzung von Compliance-Anforderungen oder aufgrund von Schadenersatzforderungen Betroffener.

Sowohl soziale Netzwerke als auch E-Commerce-Anbieter speichern eine Unmenge schützenswerter personenbezogener Daten. Neue Ansätze zum bargeldlosen Zahlungsverkehr mit Smartphones sowie WLAN-Ortung zu Marketingzwecken und Videoüberwachung machen den Datenschutz auch in der Offline-Welt zu einem prägenden Thema. Die Herausforderung besteht darin, die Chancen neuer Technologien zu nutzen, ohne einen unverhältnismäßig hohen Eingriff in die Persönlichkeitsrechte des Einzelnen oder die Gefahr eines Identitäts- und Datendiebstahls befürchten zu müssen.

Identitäts- und Zugriffsmanagement (IAM) ist zwar als Begriff etabliert, doch zeigen die erwähnten Vorfälle, dass die Realisierung mangelhaft und die alleinige Fokussierung auf diesen Baustein des Datenschutzes nicht ausreichend ist. Eine Schwäche vieler Umsetzungen besteht darin, dass Identitätsmanagement nicht als integraler Teil eines organisationsweiten Datenschutz-Compliance-Frameworks konzipiert wurde. Die Beherrschung der komplexen Systeme ist durch isolierte Datenschutzbemühungen nicht mehr zu erreichen, sondern erfordert ein strukturübergreifendes Privacy Management. Moderne Systeme müssen daher von Beginn an nicht nur funktionale Anforderungen berücksichtigen, sondern sie müssen gleichermaßen Anforderungen an den Datenschutz Rechnung tragen, um bei Nutzern eine breite Akzeptanz erzielen zu können (Privacy by Design). Privacy Impact Assessments (PIA) helfen dabei, neue Prozesse datenschutzkonform zu entwickeln sowie bestehende Prozesse im Hinblick auf Datenschutzrisiken zu bewerten.

Einen zusätzlichen Impuls erhält die Forschung nach innovativen Datenschutzkonzepten durch die Novellierung des Datenschutzes auf europäischer Ebene. Die Umsetzung findet über zwei

europäische Rechtsinstrumente statt: Einerseits durch eine EU-Datenschutzverordnung zur ganzheitlichen Neufassung des Datenschutzes, andererseits durch eine Richtlinie zur Ausformung der spezialrechtlichen Datenschutzregelungen für den Bereich der polizeilichen und justiziellen Zusammenarbeit. Dabei sind insbesondere das Recht auf Vergessen, Datenexport sowie erweiterte Auskunftsrechte in den Fokus geraten.

Insgesamt machen das wachsende öffentliche Bewusstsein und die gestiegene Gefährdungslage durch die Allgegenwärtigkeit personenbezogener Daten den Datenschutz zu einem zentralen Thema von Forschung und Gesellschaft.

Forschungsfragen im Umfeld des Datenschutzes und der Privatsphäre umfassen:

- Entwicklung einheitlicher Standards, Prozesse und Methoden, um IT-Sicherheitsanforderungen im Software-Entwicklungsprozess frühzeitig zu berücksichtigen
- Einbettung unterschiedlichster Transparenzmaßnahmen (Auskunft, Benachrichtigung, Hinweis) in ein ganzheitliches Framework für Betroffenenrechte
- Identitätsmanagement für eine Vielzahl von realen, pseudonymen und anonymen Identitäten
- Metriken für die Messung von Datenschutzanforderungen, sowie Maßnahmen zur fortwährenden Verifikation ihrer Einhaltung
- Einsatzspezifische Frameworks zur einfachen Durchführung von PIAs
- Mechanismen zur Erhöhung der Transparenz und Auditierbarkeit
- Entwicklung datenschutzfreundlicher Technologien, die sowohl Unternehmen als auch Kunden einen Mehrwert bieten
- Methoden zur Erkennung und Verfolgung von Datenschutzverletzungen in Echtzeit
- Verfahren zum automatischen Abgleich von Datenschutzanforderungen und Geschäftsmodellen über Unternehmensgrenzen hinweg
- Datenschutzkonforme Datenmigration: Methoden und technische Unterstützung für kohärentes Datenschutzmanagement zwischen verschiedenen Anbietern
- Definition und Durchsetzung digitaler Rechte und Beschränkungen (Zugriff, Auswertung, Weitergabe) über Anbietergrenzen hinweg
- Verfahren zur Kontrolle der eigenen Daten im Internet hinsichtlich Zugriff und Verteilung

- Verhinderung des zunehmenden Kontrollverlusts in offenen sozialen Umgebungen mit vernetzt und ganz oder teilweise autonom interagierenden Systemen und Akteuren
- Nutzerbezogene Lösungen für den Einsatz von (Pseudo-)Identitäten
- Erstellung, Management und Durchsetzung von Datenschutzrichtlinien
- Konzepte zur Datensparsamkeit
- Entwicklung von Verfahren zur Datenerhebung und -verarbeitung unter Berücksichtigung der Privatsphäre
- Nachweisbar sichere Verfahren zur Speicherung und Verarbeitung sensibler Daten in Drittanbieter-IT-Infrastrukturen (Cloud Computing)
- Ganzheitliche Ansätze zur Erkennung und Verhinderung des Abflusses von sensiblen Daten, »Data Leakage Prevention«
- Transparenz, Erstellung, Management und Durchsetzung von technischen Datenschutzrichtlinien, die von einem durchschnittlichen Nutzer bzw. Betroffenen verstanden werden
- Reputation: Veränderung des Vertrauens zu Webseiten und Netzkomponenten über die Zeit
- Sicherheit (innere Sicherheit, Organisationssicherheit) versus Privatsphäre
- Garantierte Vertraulichkeit bei Meldungen von Cyber-Security-Vorfällen seitens betroffener Unternehmen an staatliche Stellen
- Filter-Komponenten für klassifizierte Medienströme, um Zugriff ausschließlich auf diejenigen eingestuften Informationen zu erlauben, die zur nachgewiesenen Ermächtigung des Empfängers passen – insbesondere bei Medienströmen (Audio/Video)
- Datenschutz in Überwachungsmaßnahmen bei gleichzeitiger Steigerung der Effizienz
- Kontextbasierte Personenerkennung mit Verhaltensmustern zur Identifikation
- Homomorphe Verschlüsselung für Bildverarbeitungsalgorithmen zum Schutz sensibler Daten direkt nach der Aufnahme unabhängig von der folgenden Bildauswertung
- Verfahren zur Endnutzer-tauglichen Spezifikation von Sicherheitspolicies
- Verfahren zur Etablierung von Datennutzungskontrolle für unternehmensübergreifende Kommunikation

6.4 Energieerzeugung und Energieversorgung

Das Energienetz ist eine hochkritische Infrastruktur. Wirtschaft und Gesellschaft sind abhängig von einer stabilen und bedarfsoptimierten Versorgung mit Energie. Die Entwicklung eines intelligenten Stromnetzes (»smart grid«) erfordert nicht nur, neue Möglichkeiten der Energieversorgung zu untersuchen, sondern zwingendermaßen auch neue Gefahren zu betrachten.

Die Vernetzung und Steuerung von Stromerzeugern, Stromspeichern und Stromnetzen bis hin zum Endkunden bedeutet eine deutliche Erhöhung von Kommunikationsschnittstellen. Dabei stammen Lösungen, Dienstleistungen und Zugriffe von sehr unterschiedlichen Akteuren. In einem derart heterogenen Szenario implementieren nicht alle Anbieter Standards auf Weisen, die zueinander kompatibel sind, und nicht alle Lösungen arbeiten sicher und zuverlässig.

Dadurch entsteht eine Vielzahl bisher unbekannter Risiken für Netzverfügbarkeit, Systemsicherheit und Datenschutz. Für die Komponente Smart Meter hat das BSI mit dem Schutzprofil für Smart Meter einen Schritt in die richtige Richtung getan.[10] Für alle anderen Systeme und Prozesse im Smart Grid fehlen solche Vorgaben bisher.

Beispielhafte Sicherheitsrisiken im Smart Grid sind:

- Sabotage des Energienetzes (Synchronisation der Power Management Units) zur fehlerhaften Netzbetriebsführung bis hin zum Kontrollverlust
- Sabotage von Energieerzeugungsanlagen, z. B. durch Vorgabe manipulierter Sollwerte bis hin zu Kommunikationsausfall und Kontrollverlust über die Anlage
- Angriffe auf Infrastrukturkomponenten wie SCADA-Systeme analog zum Stuxnet-Wurm 2010
- Missbrauch und Manipulation von Messwerten (Smart Meter) für Verhaltensanalysen oder zum wirtschaftlichen Vorteil oder Schaden des Endkunden

Ein intelligentes Stromnetz bedingt neue Geschäftsprozesse, u. a. zur erhöhten Integration erneuerbarer Energien und zur Ausbildung regionaler Energiemärkte. Dazu gehören auch Prozesse zu Bilanzierung, Regelleistung, Messwerterfassung und -übermittlung, Energieangebot und -nachfrage und zur Energieabrechnung.

Diese Geschäftsprozesse sowie die beteiligten Hard- und Softwaresysteme gilt es gegen Manipulation und ungewollten Informationsabfluss zu schützen, um weitreichende wirtschaftliche Schäden zu verhindern und eine stabile Energieversorgung zu gewährleisten.

[10] Bundesamt für Sicherheit in der Informationstechnik, Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen, v1.2 final release, BSI-CC-PP-0073, 18.03.2013

Insgesamt besteht folgender Forschungsbedarf:

- Architekturen zur Realisierung des Smart Grid/Smart Market z. B. im Hinblick auf dezentrale Energieerzeugung
- Sicherheit durch verteilte Energienetzsimulationen auf Embedded Systems
- Möglicher Missbrauch von Daten
- Verfügbarkeit der Daten abhängig von Vertragsbeziehungen
- Prozesse zur Bereitstellung und Verteilung der Daten (Notwendigkeit und Art der Verschlüsselung der Daten)
- Zugriffskonzepte (Authentifizierung der Marktakteure)
- Schutz der Endnutzerdaten (Privacy): Modelle für die Datenhaltung, Nutzerschnittstellen, Schlüsselverwaltung
- Messwerte und Smart-Meter-Daten als zusätzliche Sensoren (Verhinderung der Rückkopplung und Schlussfolgerung auf individuelle Daten und individuelles Verhalten)
- Verhindern von Angriffen auf die Versorgungsinfrastruktur und Erkennen von spezifischen Angriffsmustern
- Schutz spezifischer und neuartiger Geschäftsprozesse
- Analyse der Sicherung von Smart-Grid-Funktionen durch Dezentralisierung von Energieleitsystem-Intelligenz
- Messwerte bzw. Energiedaten zur Führungsunterstützung im Sicherheitsfall (Verbrauchs- und Erzeugungsprognosen)
- Auswirkung und Verhinderung des Missbrauchs von Energiedaten (wirtschaftliche Bevorteilung, Eingriff in die Netzbetriebsführung)
- Sicherstellung von Smart-Grid-Funktionen durch redundante, unabhängige Informationshaltungskonzepte
- Datenhaltung: erforderliche Daten und flexible Zugriffsrollen
- Schutzentwicklung für öffentliche Gebäude mit hoher wirtschaftlicher, politischer und gesellschaftlicher Brisanz:
- Steuerung des Energiehaushalts, Energiemanagement im Haus

- Zugriff auf Verbraucheranwendungen (Beleuchtung, Wärme, Klimaanlage) im Rahmen des Demand Site Management

- Konzepte für sichere autarke Notstromversorgung gegenüber Cyberangriffen

6.5 Frühwarnsysteme

Die Informations- und Kommunikationstechnologie ist heutzutage aus dem privaten und beruflichen Alltag nicht mehr wegzudenken. Auch wird Informations- und Kommunikationstechnologie zunehmend in neuen Bereichen wie der industriellen Produktion oder auch in kritischen Infrastrukturen eingesetzt – beispielsweise in der Energie- und Wasserversorgung. Die moderne Gesellschaft ist somit abhängig von funktionierenden Informations- und Kommunikationsinfrastrukturen, welche jedoch immer mehr durch Schadsoftware bedroht sind. So berichtet McAfee[11], dass allein im ersten Quartal 2012 über 7 Mio. neue, bislang unbekannte Schadsoftware-Varianten identifiziert wurden. Durch diese schnelle Entwicklung von Schadsoftware wird es immer schwieriger, Betreiber von Informations- und Kommunikationssystemen rechtzeitig über neue Bedrohungen zu informieren und somit zu schützen.

Ein Ansatz mit diesem Problem umzugehen ist der Einsatz von IT-Frühwarnsystemen, um so früh wie möglich auf erkannte oder sich abzeichnende IT-Sicherheits-relevante Vorfälle reagieren zu können und damit einhergehende Auswirkungen abzuwenden oder zu minimieren. Sobald ein Vorfall erkannt wird, werden andere Systeme über das Frühwarnsystem informiert. Wichtig ist hierbei, dass die Daten zur Frühwarnung korrekt und rechtzeitig bei den Empfängern ankommen. Um den oft benötigten Gesamtüberblick zu ermöglichen, werden immer häufiger kooperative Ansätze untersucht, die eine übergreifende kooperative Auswertung verschiedener Teilsichten ermöglicht.

Die Bedeutung des Themas IT-Frühwarnung wird auch in den Aktivitäten des Bundesamts für Sicherheit in der Informationstechnik und dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) deutlich, die im Rahmen der Cyber-Sicherheits-Strategie eine Allianz für Cyber-Sicherheit[12] initiiert haben, bei der IT-Frühwarnung eine zentrale Rolle einnimmt.

Im Handlungsfeld der Frühwarnung sind noch viele offene Fragen zu lösen und folgende Forschungsaufgaben haben große Relevanz:

- Erforschung neuer Konzepte für IT-Frühwarnsysteme in neuen Anwendungsgebieten (z. B. zum Schutz kritischer Infrastrukturen)

[11] *http://www.mcafee.com/de/resources/reports/rp-quarterly-threat-q1-2012.pdf.*

[12] *https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2012/Allianz-fuer-Cyber-Sicherheit_07032012.html.*

- Weiterentwicklung sensorbasierter und quellenbasierter Datengewinnung
- Entwicklung von Verfahren zur automatisierten Analyse von Frühwarninformationen, die eine Bedrohungslage bestimmen und automatisiert Handlungsbedarf und Reaktionsmöglichkeiten ableiten lassen
- Weiterentwicklung kollaborativer Ansätze zur Verbesserung der Frühwarnung
- Frühwarnung für gezielte Angriffe
- Verfahren zur Erkennung von APTs (Advanced Persistent Threats)
- Verfahren, Prozesse und Werkzeuge zur effizienten Analyse von APTs
- Verfahren zur Erstellung eines Gesamtlagebildes bezüglich Schadsoftware, krimineller Gruppen und daraus resultierender aktueller Bedrohungen
- Automatische Verfahren zur Massen-Analyse von Schadsoftware und Ableitung von Erkennungskriterien
- Kooperative, z. B. reputationsbasierte Erkennung von Bedrohungen wie Schadsoftware oder bösartigen Webseiten
- Botnetze
  - Erkennung von Botnetzen
  - Verfahren zur Vermessung und Beurteilung von Botnetzen
  - Verfahren zur Überwachung von Botnetzen
  - Verfahren zur Unterstützung der Übernahme und Abschaltung von Botnetzen
  - Desinfektion von Systemen, die mit Schadsoftware infiziert sind
  - Verfahren zur Schadensminimierung (z. B. Blockierung von Finanztransaktionen) und Ermittlung der Täter
- Automatische Verfahren und Techniken, die Massenausbreitungen von Schadsoftware eindämmen
- Techniken und Verfahren, die Auswirkungen von Verfügbarkeitsangriffen mindern
- Heuristische und adaptive Risikoerkennung

6.6 Industrielle Produktion und Automatisierung

In der industriellen Automatisierungstechnik ist der Einsatz standardisierter IT-Techniken zu Kommunikationszwecken nicht mehr wegzudenken. Es wird ein Grad der Vernetzung möglich, der Überwachung, Steuerung und Konfiguration von Produktionsanlagen von beliebigen Standorten aus erlaubt.

Dieser Einzug der durchgängigen Kommunikation mit standardisierten offenen Protokollen und Techniken in Produktionsanlagen bringt neben vielen Vorteilen neue Gefahren durch unberechtigte Zugriffe Dritter oder Fehlbedienungen mit sich. Für TCP/IP-Netzwerke sind diverse Angriffsmöglichkeiten bekannt und entsprechende Hackertools sind im Internet frei verfügbar. Nicht zuletzt zeigen seit 2010 der Wurm »Stuxnet« und die Suchmaschine »Shodan« für Schwachstellen in öffentlich zugänglichen Prozesssteuerungssystemen[13] , in welche Richtung sich die Gefahrenlage entwickeln wird.

In einigen Bereichen sind die bekannten Techniken aus der Netzwerksicherheit für die speziellen Anforderungen wie Echtzeitverarbeitung in der industriellen Automatisierungstechnik nicht ausreichend oder für die speziellen Industrial Ethernet-Protokolle nicht oder nur mit aufwendigen Modifikationen einsetzbar.

Wesentliche Unterschiede zur Büro-IT stellen die potentiellen Auswirkungen und Gefahren von Angriffen auf Produktionssysteme dar, wie gravierende Personen- und Sachschäden, Umweltkatastrophen sowie wirtschaftliche Schäden durch verdeckte Manipulationen.

Industrielle Automatisierungstechnik ist ein Eckpfeiler für eine funktionierende Volkswirtschaft einer Industrienation und IT-Sicherheit stellt entsprechend eine Basisfunktion für die Integration von IT-Technik in Produktionsanlagen dar.

Forschungsfragen für sichere Produktions- und Automatisierungssysteme sind:

- Sichere und zuverlässige Protokolle industrieller Kommunikation (z. B. Audio-Video-Bridging-basierende Echtzeit-Ethernet-Protokolle)
- Sichere und zuverlässige Zeitsynchronisationsprotokolle in der Prozesstechnik
- Garantierte Sicherheitsniveaus bei automatisch rekonfigurierbarer Automatisierungstechnik (wandlungsfähige Automatisierungsanlagen)
- Verfahren und Algorithmen zur sicheren Erkennung von Eingriffen auf die Leitebene in der industriellen Produktion (z. B. chemische Produktionsanlagen)

[13] Bundesamt für Sicherheit in der Informationstechnik, Quartals-Lagebericht 4/2010

- Verfahren und Algorithmen zur Detektion von Eingriffen in die Feldbusebene von Produktionsanlagen
- Sichere Erkennung von unsachgemäßen und die Sicherheit beeinträchtigenden Stelleingriffen in der Leitebene von Produktionsanlagen durch das Bedienpersonal
- Erkennung, Analyse und Bekämpfung von Schadsoftware für SCADA-Systeme
- Sichere Verfügbarkeit von industrieller Kommunikation zur Minimierung von Produktionsausfällen im Schadensfall

6.7 IT-Forensik

Viele Kriminelle nutzen heute Computer und Internet für ihre Zwecke. Das Spektrum krimineller Handlungen ist breit: es reicht von Wirtschaftsspionage über IT-Angriffe und Identitätsmanipulation bis hin zu Kinderpornographie. Die Hälfte aller deutschen Konzerne ist von IT-basierter Wirtschaftsspionage betroffen, wobei ein jährlicher Schaden von mehr als 4 Milliarden Euro angenommen wird.[14] Wiederholte IT-Angriffe auf Datenbanken mit Kreditkartennummern gehen mittlerweile so weit, dass sie deutliche Auswirkungen auf die Börsennotierungen von Kreditkartenunternehmen haben.[15] Die massenhafte Verfügbarkeit von Speicherplatz und immer höhere Bandbreiten bis zu den Endgeräten stellen Ermittler vor ein großes Ressourcenproblem.[16] Die Möglichkeit zur wirksamen und zeitnahen informationstechnischen Aufklärung von Delikten ist sehr wichtig: sie verhilft Opfern zu ihrem Recht, schreckt Täter ab und wirkt somit in indirekter Weise präventiv.

In der Regel hinterlassen Täter digitale Spuren. Sie zu erkennen, sicherzustellen und auszuwerten ist Aufgabe der IT-Forensik. Die aktuellen technischen Entwicklungen stellen Ermittler dabei immer häufiger vor große Herausforderungen: So hat etwa die Masse der statischen und dynamischen Daten derart stark zugenommen, dass sich die Informationen nur mit Hilfe von Spezialwerkzeugen bearbeiten und auswerten lassen. Ein weiteres Problem besteht in der allgemeinen technologischen Weiterentwicklung von Hardware, Systemen und Applikationen. Werkzeuge müssen stetig weiterentwickelt werden, um mit der rasanten technischen Entwicklung Schritt zu halten, z. B. durch die Weiterentwicklung von mobilen Systemen oder der Cloud-Technologie. Außerdem nutzen Täter die Computertechnik selbst immer effektiver, um ihre Spuren zu verwischen und die Beweissicherung zu erschweren. Eine Herausforderung ergibt sich durch den möglichen oder gezielten Einsatz von Anti-Forensik. Dabei versuchen Täter durch den Einsatz von Techniken, die Anwendung von IT-forensischen Vorgehensweisen

[14] Spiegel Online: Studie zur Industriespionage – Jeder zweite deutsche Konzern wird ausgespäht. April 2012.

[15] manager magazin: Sicherheitslücke – Hacker knacken US-Kreditkarten. März 2012.

[16] B.-D. Meier, A. Hüneke: Herstellung und Verbreitung von Kinderpornographie über das Internet. Forschungsbericht, Uni Hannover, 2011.

und Werkzeugen zu umgehen. Ein Beispiel ist die trickreiche Umgehung der von den Ermittlern eingesetzten Methoden zur automatisierten Erkennung kinderpornographischer Inhalte.

Es sind IT-forensische Werkzeuge gefragt, die sowohl hinreichend effektiv als auch effizient arbeiten. Bei diesen Werkzeugen muss unterschieden werden zwischen Werkzeugen zur Untersuchung statisch vorliegender Daten und Werkzeugen für die Live-Forensik, welche in Echtzeit in den Netzen eine Vorqualifizierung bei dynamischen Daten vornehmen. Beide Arten von Werkzeugen werden für eine zielgerichtete und erfolgreiche Ermittlungsarbeit benötigt.

Im Handlungsfeld der IT-Forensik sind folgende Forschungsaufgaben zu leisten:

- Entwicklung von Verfahren, die eine robuste und effiziente automatisierte Erkennung von verbotenen Inhalten für verschiedene Medientypen (Bilder, Videos) ermöglichen
- Entwicklung von Verfahren zur Erkennung von verbotenen Inhalten aus Dateifragmenten nach dem Löschen von Dateien
- Neue Verfahren für die robuste und schnelle Erkennung von ähnlichen Dateien
- Neue Verfahren und Werkzeuge zur Identifikation und zur Beweissicherung für Betrugsdelikte
- Verfahren zur forensischen Untersuchung und Vorqualifizierung in Echtzeit in laufenden Systemen (Live Forensics)
- Entwicklung leistungsfähiger Dekodierer für proprietäre Protokolle
- Entwicklung von statistischen Verfahren zur Erkennung von Wirtschaftskriminalität im Rahmen von Insider-Angriffen
- Mobile Forensics für moderne Betriebssysteme von Smartphones
- Entwicklung von Verfahren zur Analyse der Leistungsfähigkeit IT-forensischer Werkzeuge
- Verbesserung von bestehenden IT-forensischen Werkzeugen
- Abstraktion zur Reduktion der existierenden Komplexität bei Logging und Data Mining
- Data Mining auf Logging-Daten als Basis von IDS-, IPS- und forensischer Verfahren, beweissichere Protokollierung
- Schnelle Klassifikation von großen Datenmengen (Big Data)
- Schnelle, automatische Suche nach Bild- und Videoinhalten in großen Datenbanken (Objektsuche, Image Retrieval), insbesondere im Internet

- Effiziente massiv-parallele Verfahren zur Analyse verschlüsselter Inhalte
- Natural Language Processing in der Computer-Forensik als Assistenzsystem für Ermittlungsbehörden
- Internationale Standardisierung im Bereich der Weiterverwendung von Rohdaten für Ermittlungen, insbesondere für Cloud-basierte Dienste

6.8 IT-Sicherheit für Mobilität

Heutige Fahrzeugsysteme sind bereits mit einer Vielzahl von IT-Komponenten ausgestattet, die miteinander vernetzt sind. In naher Zukunft wird sich der Anteil an elektronischen Systemen in Fahrzeugen weiter erhöhen und es werden immer mehr Fahrzeugfunktionen in Software realisiert sein. Dies ist kostengünstig, aber viele Funktionen werden auch erst durch IT realisierbar. Doch die Einführung von IT in die Fahrzeugwelt bringt nicht nur Vorteile mit sich, sondern offenbart auch neue Herausforderungen für die Fahrzeughersteller, Zulieferer und Diensteanbieter.

Die Vernetzung von Fahrzeugen mit dem Internet oder auch die anvisierte Einführung von Fahrzeug-zu-Infrastruktur-Kommunikation und Fahrzeug-zu-Fahrzeug-Kommunikation (Car-to-X) wird fundamentale Änderungen mit sich bringen. Die bisher in sich geschlossenen Fahrzeugnetze werden zur Außenwelt immer mehr geöffnet und somit werden Fahrzeuge auch von außen angreifbar – im schlimmsten Fall sogar bequem aus dem Internet dank vorgefertigter Angriffstools. Werden aber Fahrzeughersteller, Zulieferer und Diensteanbieter in die Lage versetzt, diese Probleme zu lösen, stehen ihnen neue Möglichkeiten und Märkte für innovative Produkte offen.

Es sind somit allumfassende IT-Sicherheitslösungen gefragt, die nicht nur die Kommunikation mit der Umwelt, sondern auch innerhalb des Fahrzeugs, sowie die Dienste in der Infrastruktur beziehungsweise im Backend absichern. Solche Sicherheitslösungen müssen von Beginn an betrachtet werden (Security by Design) und auch bereits in der Entwicklungsphase die Zeit nach der Produktion berücksichtigen (Security during Operation). Das heißt, die IT-Sicherheitskonzepte sind für den gesamten Produktlebenszyklus eines Fahrzeugs und der angebotenen Dienste nötig (Security Management). Erst dadurch werden viele innovative Produkte möglich, die Marktpotential haben und die hierzu erforderliche Nutzerakzeptanz erreichen.

Im Handlungsfeld der Automotive Security sind daher folgende Forschungsaufgaben besonders relevant:

- Entwicklung von IT-Sicherheitslösungen zum Schutz des Fahrzeugs selbst (In-Vehicle Security, Embedded Security) unter Berücksichtigung sämtlicher involvierter Technologien
- Untersuchung des Zusammenhangs zwischen Safety und Security (Safety by Security) (vgl. Abschnitt »Zusammenspiel Safety und Security« 6.15)

- Untersuchung von möglichen Migrationsstrategien zur sicheren Einführung des Internet-Protokolls (IP) in Fahrzeugen zur weiteren Kostenreduktion und zur Realisierung neuer Fahrzeugfunktionen
- Entwicklung tragfähiger Lösungsansätze zur Aktualisierung von IT-Sicherheitsmechanismen über den gesamten Produktlebenszyklus
- Entwicklung von Intrusion-Detection-Systemen (IDS) für Fahrzeuge
- Entwicklung von automatisierten Validierungswerkzeugen von IT-Sicherheitsarchitekturen
- Untersuchung von eMobility-spezifischen IT-Sicherheitsansätzen
- Entwicklung von ganzheitlichen IT-Sicherheitslösungen für Intelligent Transport Systems (ICT)
- Entwicklung von Lösungen zum Komponentenschutz und zur Erkennung von gefälschten Komponenten (vgl. Abschnitt »Piraterieschutz« 6.11)

6.9 Mediensicherheit

Digitale Medien sind heute ein fester Bestandteil der Informationsgesellschaft. Sie sind digitales Gut, wenn es um den Verkauf von Filmen, Musik, Hörbüchern und E-Books geht. Sie sind aber auch Informationsträger, wenn sie in Onlinenachrichten zum Unterlegen von Meldungen dienen, oder wenn die Nachrichten selbst zum digitalen Medienstrom werden. Gleichzeitig sind digitale Medien heute leicht zu manipulieren, so dass oft wenig Vertrauen in digitale Bilder gesetzt wird.

Der Schutz digitaler Medien hat daher zwei wichtige Aspekte: Urheberrecht und Manipulationsschutz. Im Umfeld des Urheberrechts gilt es, Schutzkonzepte anzubieten, die von Rechteinhabern und Kunden gleichermaßen akzeptiert werden. Hier setzen sich digitale Wasserzeichen immer mehr durch, erfordern aber auch eine kontinuierliche Weiterentwicklung, um neuen Medientypen und Verbreitungsformen zu genügen.

Aus technischer Sicht eng verwandt mit dem Schutz von Urheberrechten ist die Verfolgung der Weitergabe geheimer Dokumente. Zwar werden bereits seit langer Zeit vertrauliche Mitteilungen individualisiert, um Informanten aufzudecken, eine Automatisierung durch digitale Wasserzeichen kann diese Prozesse aber stark vereinfachen. Denkbar ist hier beispielsweise ein Einsatz bei Patentierungsvorgängen und ähnlichen Dokumenten, um Wirtschaftsspionage zu erschweren oder aufzudecken.

Der Manipulationsschutz hat zum Ziel, digitale Manipulationen an Medien aufzudecken. Dazu müssen Werkzeuge erstellt werden, die beispielweise der Redaktion eines Online-Magazins

eine schnelle Prüfung auf verdächtige Spuren verbreiteter Manipulationswerkzeuge erlauben. Nur so ist es möglich, zum einen mit der Geschwindigkeit der Informationsverbreitung über das Internet Schritt zu halten, gleichzeitig aber auch vertrauenswürdig zu bleiben. Entsprechende Werkzeuge sind heute in der Forschung bekannt, haben aber noch nicht Produktreife erreicht. Deren praxisgerechte Weiterentwicklung wird eine Aufgabe sein, der sich die Informationsgesellschaft in der Zukunft stellen muss.

Die folgenden Forschungsaufgaben sind zu bewältigen:

- Transfer von Wasserzeichenverfahren in Lösungen zur Verfolgung von Geheimnisverrat
- Entwicklung von neuen Wasserzeichenverfahren für elektronische Dokumente auf Basis der geschriebenen Sprache
- Effiziente Methoden zum Auffinden von mit Wasserzeichen markierten Medien
- Transfer bekannter Methoden zur Manipulationserkennung digitaler Medien in Endbenutzerwerkzeuge
- Weiterentwicklung der Manipulationserkennung digitaler Medien (Audio, Video, Einzelbild)
- Weiterentwicklung für Verfahren zur effizienten Erzeugung von Transaktionswasserzeichen
- Erarbeiten von Kodierungsmethoden, die gegen eine große Zahl von zusammenarbeitenden Angreifern Resistenz bieten
- Erstellen von Endbenutzerwerkzeugen zur Erkennung von medienerzeugenden Geräten (Geräteballistik)
- Entwicklung von Markierungsmethoden für kleine oder einfach aufgebaute Bildtypen wie Logos oder Galeriebilder
- Absicherung von Daten z. B. durch neuartige DRM-Technologien in Ergänzung zur Absicherung von Endgeräten
- Digitales Urheberrecht und Nutzungskontrolle:
  - Verfolgung von Verbreitungswegen von digitalen Daten (Video-, Bildmaterial, Texten, Software, Nachrichten)
  - Neue Protokolle zum Digital Rights Management zum Schutz von geistigem Eigentum (Intellectual Property)

- Verfahren für digitale Wasserzeichen und Steganographie
- Automatische Erkennung markierter Komponenten

- Privacy-by-Design-Konzepte für den sicheren Austausch von Videos und Bildern im Internet
- Verfahren zum Schutz und zur automatischen Erkennung von Manipulationen an Bildern und Videos (z. B. Watermarking, Zertifizierung)

6.10 Netzsicherheit

Der überwiegende Teil der IT-Systeme ist mit anderen Systemen vernetzt, kaum ein Bereich unseres Lebens ist noch ohne Unterstützung durch IT-Systeme vorstellbar. Diese Entwicklung wird sich fortsetzen, zumal es heute viele neue Anwendungsfelder gibt, die ohne vernetzte IT-Systeme nicht realisierbar oder nicht wirtschaftlich wären.

Mit dem Grad der Vernetzung steigt der Grad der Abhängigkeit der Wirtschaft und des öffentlichen Lebens von einer funktionierenden Kommunikationsinfrastruktur. Neben technischem Versagen geht dabei die größte Gefahr von bewusst herbeigeführten Manipulationen aus.

Das Rückgrat für den Datenverkehr und alle verteilten Anwendungen und Geschäftsprozesse bildet das Kommunikationsnetzwerk. Angriffe auf das Netzwerk selbst stellen eine der größten Bedrohungen dar, weil sich mit verhältnismäßig geringem Aufwand eine sogar kaskadierende Wirkung von Ausfällen und Manipulationen erreichen lässt.

Gleichzeitig kann das Netzwerk bei spezifischen Angriffen wertvolle Unterstützung zur Erkennung von Angriffen auf Anwendungen und Unternehmen und bei der globalen Lagedarstellung liefern. Bei verteilten und verdeckten Angriffen bildet die Kommunikationsinfrastruktur die einzige Basis, eine umfassende Auswertung der Vorgänge zu erstellen.

Typische Gefahren für Anwendungen und Nutzer, die vom Netzwerk ausgehen, sind: Verbreitung von Schadsoftware (Viren, Trojanische Pferde), Eindringen in (Unternehmens-)Netze, Informationsbeschaffung (u. a. für Industriespionage und Social Engineering), Abfangen und Manipulation von Daten, Auslesen sensibler Daten (z. B. Datenbanken mit Kundendaten, Passwörter), Überlastung oder Sabotage von Infrastrukturkomponenten (Denial-of-Service-Angriffe).

Für diese sich stets weiterentwickelnden Gefahren und Angriffsszenarien gibt es heute keine oder nicht ausgereifte Schutz- oder Gegenmaßnahmen. Angreifer können mit vergleichsweise geringem Aufwand hohe Schäden für die Wirtschaft erzielen und eine Gefahr für Menschenleben auslösen.

Die Absicherung der Kommunikationsinfrastruktur bedeutet ein dauerhaftes Engagement in der Weiterentwicklung von Sicherheitsmaßnahmen und -lösungen, wie z. B.:

- Schutz von Internet-Infrastrukturtechnologien
- Schutz der Konnektivität und Verfügbarkeit von Kommunikationsdiensten
- Methoden zur formalen Beschreibung physikalischer und logischer Komponenten und deren dynamischer Beziehungen
- Überwachung und Monitoring physikalischer und logischer Komponenten und deren dynamischer Beziehungen
- Systematische Erfassung (Protokollierung), Beobachtung und Überwachung von Netzwerk- und Infrastrukturkomponenten
- Simulative Untersuchung und Analyse der Abhängigkeit vernetzter kritischer Infrastruktur
- Kooperatives Monitoring zur Erkennung von BGP-Internet-Routing-Manipulationen und -Anomalien und zur Erkennung von DNS-Manipulationen und -Anomalien
- Erkennen und Verhindern von Manipulationen bei Ultra-low-latency Networks (Financial Trading)
- Absicherung der Kommunikation in dynamischen Gruppen
- Entscheidungsunterstützung zur Erkennung und Klassifizierung von Angriffen und Sicherheitslücken, z. B. basierend auf Verfahren des maschinellen Lernens
- Methoden zur Gewährleistung grundlegender Vertrauensbeziehungen von Kommunikationspartnern

6.11 Piraterieschutz

Durch die unlautere Nachahmung von Produkten, Komponenten und Design entstehen große wirtschaftliche Schäden, die immer neue Rekordwerte erreichen. Die Geschädigten sind in erster Linie die Unternehmen, deren Produkte illegal nachgeahmt und vervielfältigt werden. Nachgeahmte Ware wird dann zu wettbewerbs- und marktverzerrenden Konditionen angeboten. Die negativen Auswirkungen reichen über den Verlust von Marktanteilen und Imageschäden bis hin zu Arbeitsplatzabbau. In unmittelbarer Folge wird damit auch die Volkswirtschaft belastet. Allein den jährlichen Verlust im deutschen Maschinen- und Anlagenbau schätzte der Verband Deutscher Maschinen- und Anlagenbau (VDMA) in einer 2012 veröffentlichten Studie[17] auf 7,9 Milliarden Euro. Von den VDMA-Mitgliedsunternehmen sind 67 % von Produktpiraterie betrof-

[17] VDMA Studie Produktpiraterie 2012

fen, Tendenz steigend. Am häufigsten werden Komponenten und ganze Maschinen kopiert. Aber auch Konsumenten sind von negativen Auswirkungen betroffen; falls beispielsweise einem Käufer anstatt eines vermeintlichen Markenprodukts eine minderwertige Fälschung verkauft wurde, deren Sicherheit und Zuverlässigkeit in Frage steht.

Insbesondere das Know-how im Maschinenbau und der Elektrotechnik ist stark bedroht. So werden sowohl einzelne Bauteile als auch ganze Systeme und Anlagen von mechanischen Baugruppen oder Elektroniksystemen gefälscht. Durch moderne Verfahren zum Reverse Engineering und Rapid Prototyping stehen ausgefeilte Methoden und Werkzeuge für die Systemanalyse, Manipulationen und den Produktnachbau zur Verfügung. Die Möglichkeiten zum Schutz von Produkten vor Piraterie sind ebenso vielfältig wie die betroffenen Produkte. Originalware kann mit speziellen Kennzeichnungen und Markierungen versehen sein. Damit wird jedoch der Nachbau und ein Know-how-Verlust nicht verhindert, sondern lediglich eine Unterscheidung zwischen Original und Fälschung ermöglicht. Um der Piraterie entgegenzuwirken, sind Schutzmaßnahmen zu ergreifen, die auf die Sicherung des eigenen Kern-Know-hows zielen. Beim Schutz von Cyber-Physischen Systemen können effektive und effiziente Maßnahmen im technologischen Bereich liegen. Durch geeignete Maßnahmen kann dem Reverse Engineering oder der unerwünschten Manipulation an der Elektronik oder Software entgegengewirkt werden.

Es sind Methoden und Werkzeuge zum Vorbeugen der Produktpiraterie gefragt, die den gesamten Produktentwicklungs- und -lebenszyklus berücksichtigen. Bereits in der Konzeptions- und Entwurfsphase eines Produkts sind Schutzziele und entsprechende Maßnahmen aufeinander abzustimmen. Das wird in der Regel Auswirkungen auf die Produktion, den Vertrieb und den Service haben.

Im Handlungsfeld der Produktpiraterie sind folgende Forschungsaufgaben zu leisten:

- Entwicklung von Verfahren zum Schutz des Know-hows in Cyber-Physischen Komponenten
- Unterstützung bei der Herstellung von geschützten Basiskomponenten
- Entwicklung von Verfahren zur effizienten Integration der sicheren Basiskomponenten in Produktionsumgebungen
- Unterstützung bei der Etablierung von Industriestandards für geschützte Komponenten und sichere Kommunikation (Feldbus)
- Standardisierung von Prüfmöglichkeiten, um Originalware von Nachahmungen zu unterscheiden
- Untersuchung der Safety- und IT-Security-Implikationen
- Entwicklung von Verfahren zur Verhinderung von Manipulationen an Hardware und Software

- Entwicklung von Verfahren zur Entdeckung von Manipulationen an Hardware und Software

6.12 Physically Embedded Cyber Security

Physically Embedded Cyber Security (PECS) bezeichnet die ganzheitliche Betrachtung von physikalischer und informationeller Sicherheit. PECS geht davon aus, dass in der heutigen Zeit in vielen komplexen Systemen Sicherheit weder allein in physikalischer noch allein in informationeller Hinsicht erreicht werden kann. Vielmehr zeichnen sich sicherheitskritische Systeme stets dadurch aus, dass vernetzte informationsverarbeitende Systeme in physikalisch zu schützenden Umgebungen eingebettet sind (System-of-Systems-Ansatz).

PECS bedeutet dabei beispielsweise Sicherheit vor unerlaubtem Zugriff. So können etwa kritische Infrastrukturen ganzheitlich geschützt werden, indem der physikalische Zugang zu entsprechenden Bereichen beobachtet wird und gleichzeitig die informationsverarbeitenden Systeme in ihrem Ablauf beobachtet werden.

Allgemein wird eine Korrelation zwischen Ereignissen beider »Welten«, der physikalischen Welt und der informationellen Welt, hergestellt. Ereignisse, welche in einer Welt festgestellt werden, können in der anderen Welt bestätigt oder verworfen werden. Auch die gezielte Suche nach Ereignissen (aktuell oder forensisch) in der jeweils anderen Welt beim Auftreten eines physikalischen oder informationellen Ereignisses ist denkbar.

PECS meint jedoch auch die Sicherheit vor Unfällen und unsachgemäßer Bedienung von Systemen (Safety). So kann beispielsweise die Sicherheit einer industriellen Produktionsanlage dadurch erhöht werden, dass die eingesetzten Maschinen als physikalische Komponenten in informationelle Sicherheitssysteme eingebettet sind. Dadurch können etwa bestimmte Verfahrwege einer Maschine ausgeschlossen werden können.

PECS beinhaltet naturgemäß die Bereiche der physikalischen Sicherheit und der informationellen Sicherheit. PECS ergänzt diese Bereiche um die Fragestellung der ganzheitlichen Betrachtung beider Welten: So müssen Modellierungen des Zusammenspiels der beiden Welten gefunden werden, welche die Erkennung von kompatiblen bzw. sich widersprechenden Ereignissen aus beiden Bereichen erlauben. Dies beinhaltet auch die Modellierung und Erkennung von kombinierten physikalischen und informationellen Angriffsmustern auf physikalisch eingebettete informationsverarbeitende Systeme.

Forschungsaufgaben im Themenfeld PECS umfassen:

- Informationelle Sicherheit:
    - Modellierung von informationellen Abläufen (z. B. Anmeldevorgang, Datenzugriffsmuster, Zugriffszeiten etc.) und Ableitung sicherheitsrelevanter Ereignisse

- Sicherheit an der Schnittstelle zwischen physikalischer und informationeller Welt:
  - Ganzheitliche Modellierung von Ereignissen und Abläufen in physikalischer und informationeller Hinsicht
  - Klassifikation von Anomalien
  - Ableitung des sicherheitsrelevanten Zusammentreffens physikalischer und informationeller Ereignisse (Datenfusion)
  - Maschinelle Herleitung nicht klassifizierter Anomalien
- Zielgerichtete Analyse der jeweils anderen Welt beim Auftreten eines physikalischen bzw. informationellen Ereignisses
- Automatische Korrelation klassifizierter Ereignisse in der einen Welt mit klassifizierten Ereignissen der anderen Welt
- Automatische Korrelation klassifizierter Ereignisse in der einen Welt mit nicht klassifizierten oder unspezifischen Ereignissen der anderen Welt

6.13 Secure Engineering

IT-Produkte wie z. B. Anwendungssoftware haben zu oft erhebliche Sicherheitslücken. Diese Lücken stellen für Anwender und Hersteller große Risiken dar. Um die Sicherheitseigenschaften von IT-Produkten zu verbessern, müssen Hersteller für die Entwicklung und Pflege der Produkte sogenannte Security Lifecycles etablieren, die sich über den gesamten Lebenszyklus der Produkte erstrecken. Bei der Produktentwicklung müssen Fragestellungen der IT-Sicherheit bereits in der Designphase, also vom ersten Entwicklungsschritt an, mitberücksichtigt werden. Dadurch können Hersteller die Sicherheit ihrer Produkte verbessern und immense Kosten für eine späte Beseitigung von Sicherheitslücken reduzieren.

Die Einführung von Prozessen und Methoden zur systematischen Verbesserung der IT-Sicherheit von IT-Produkten ist für viele Unternehmen eine Entscheidung von strategischer Bedeutung. Effektive und effiziente Maßnahmen zur Verbesserung der IT-Sicherheit sind notwendig, um die Wettbewerbsfähigkeit von Herstellern mittel- bis langfristig zu sichern. Die überwiegende Anzahl von Herstellern ist bisher nicht in der Lage, entsprechende Maßnahmen für einen auf die eigenen Produktionserfordernisse angepassten Security Lifecycle umzusetzen. Hierzu fehlt den Unternehmen bisher das erforderliche Know-how. Darüber hinaus gibt es jedoch viele offene Fragen im Bereich der anwendungsorientierten Forschung, die noch zu beantworten sind, damit Unternehmen ihren Security Lifecycle verbessern können.

Für die Designphase von Produkten sind handhabbare ingenieurmäßige Methoden nötig, mittels derer die Sicherheitsanforderungen von Anfang an adäquat erfasst und berücksichtigt

werden können. Dies umfasst z. B. Aspekte des Requirement Engineerings und des Threat Modellings. Für grundlegende Entscheidungen hinsichtlich der Sicherheitsarchitektur sind Best Practices erforderlich. Darüber hinaus sind geeignete Testmethoden für die verschiedenen Phasen der Produktentwicklung notwendig. Handlungsbedarf besteht hier sowohl hinsichtlich Methodik als auch hinsichtlich geeigneter Testwerkzeuge, insbesondere für spezielle Technologie- und Anwendungsbereiche.

Damit die Ansätze für den sicheren Entwurf praxistauglich sind, müssen sie die praktischen Erfordernisse heutiger Produktionsprozesse berücksichtigen. Zum Beispiel muss der Security Lifecycle die typischen Supply Chains bei der heutigen verteilten Herstellung von Anwendungssoftware (z. B. Integration von Open Source Software, Third Party Code, Legacy Code) unterstützen.

Auch wenn die Ansätze des Secure Engineerings die Sicherheitseigenschaften von IT-Produkten verbessern, wird man dennoch auch hier systematische Vorgehensweisen benötigen, um mit Schwachstellen und stattgefundenen Angriffen auf IT-Produkte umzugehen (Response).

Forschungsbedarf besteht in den folgenden Bereichen:

- Entwicklung, Anpassung, Verbesserung von Engineering-Methoden zur Verbesserung des Sicherheitsniveaus von IT-Produkten
- Entwicklung von Methoden zur sicheren Integration von Komponenten
- Entwicklung prozessorientierter Sicherheitsmodelle, um die Modellierung der Interdependenzen technischer, sozialer und wirtschaftlicher Prozesse hinsichtlich ihrer Sicherheitsanforderungen zu ermöglichen
- Kompositionalitätseigenschaften für IT-Sicherheit in System-of-Systems-Architekturen
- Zertifizierung bei der Integration von Komponenten
- Ansätze für leichtgewichtige Zertifizierung von Software
- Übertragung und Tauglichkeitsanalyse von Methoden aus anderen Anwendungsfeldern (z. B. Safety-Technologien)
- Methoden des Requirements Engineering für spezielle Anwendungsbereiche
- Spezialisierung von Methoden des Threat Modellings für ausgewählte Technologie- und Anwendungsbereiche
- Sicherheitsarchitekturen für spezielle Anwendungs- und Technologiebereiche als Best Practices
- Statische Analysemethoden

- Dynamische Analysemethoden
- Sicherheitsarchitekturen für IT-Sicherheit (Security) und funktionale Sicherheit (Safety)
- Wirtschaftlichkeitsbetrachtungen von Methoden des Secure Engineering / Security Lifecycles
- Entscheidungsunterstützung in Secure Engineering Methoden
- Entwicklung von Testmethoden und Werkzeugen für Sicherheitstests in der Designphase
- Entwicklung von Testmethoden und Werkzeugen für Sicherheitstests in der Implementierungsphase
- Methoden für sicheres Design und sichere Implementierung bei Produktlinien
- Zusammenhang Usability und IT-Sicherheit für Secure Engineering

6.14 Secure Mobile Systems

Mobile Systeme wie Smartphones oder Tablet-PCs haben in der jüngsten Vergangenheit enorm an Bedeutung gewonnen. Mobilgeräte sind sehr leistungsfähig geworden und gehören wegen ihrer Praktikabilität und Vielseitigkeit sowohl zum beruflichen wie auch privaten Alltag sehr vieler Menschen. Außer zu Kommunikationszwecken werden mobile Systeme heute immer mehr für solche Anwendungen verwendet, die früher ausschließlich auf stationären PCs und Notebooks ausgeführt wurden. Durch die hohe Popularität von Mobilgeräten werden heute auch zunehmend vertrauliche und schützenswerte Daten auf diesen Geräten verarbeitet und gespeichert. Das führt dazu, dass Mobilgeräte zunehmend Ziele von Angriffen sind. Jedoch hat sich gezeigt, dass Sicherheitslösungen und Konzepte aus der Welt der nicht-mobilen Systeme nicht einfach auf mobile Systeme übertragen werden können.

Für viele Benutzer ist es heute wichtig, dass sie das gleiche Gerät sowohl zu privaten wie auch beruflichen Zwecken einsetzen können. Das führt in der Praxis dazu, dass sich Benutzer häufig beliebige Software auf das genutzte mobile System installieren, wodurch sich fast zwangsläufig Sicherheitskonflikte ergeben. Deshalb braucht man Sicherheitslösungen, mittels derer der Zugriff auf Ressourcen (z. B. Daten, Netzwerkverbindungen, Betriebssystemfunktionen) sinnvoll kontrolliert werden kann.

Die Anzahl integrierter Technologien und Funktionalitäten bei Mobilgeräten hat erheblich zugenommen. Dadurch sind mobile Systeme oft fehleranfälliger als stationäre Arbeitsplatzsysteme und eröffnen neue Schwachstellen. Gerade die gleichzeitige Verwendung von verschiedenen Funktechnologien bietet die Gefahr von ungewollten und unkontrollierten Netzwerkverbindungen. Dies bedeutet für die Unternehmensinfrastruktur besonders hohe Risiken. Angriffe, etwa mittels Code Injection, Return-Oriented Programming oder Schadsoftware haben gezeigt,

dass die Sicherheitsarchitekturen von modernen Smartphones keinen adäquaten Schutz gegen diese Bedrohungen bieten können. Dadurch ist es möglich, dass Mobilgeräte immer wieder kompromittiert werden.

Ohne besondere Schutzmaßnahmen sind Angriffe im mobilen Kontext schneller und einfacher durchzuführen und haben meist eine größere Tragweite als bei stationären Systemen. Der Einsatz mobiler Systeme erfordert ineinandergreifende Sicherheitsmaßnahmen, die einen angemessenen Schutz im gesamten Nutzungsszenario bieten. Mobile Systeme sind verstärkt Bedrohungen ausgesetzt, da sie meist in ungeschützten Umgebungen genutzt werden. Ihre Schnittstellen sind daher leicht zugänglich.

Forschungsfragestellungen in diesem Zusammenhang sind:

- Korrelation von Sicherheitsanforderungen, technologischen Lösungsansätzen, Kundenakzeptanz marktrelevanter Forschung und Entwicklung, sowie Leitlinien
- Sichere Mandantenfähigkeit (Repräsentation der Interessen verschiedener Stakeholder auf einem Endgerät)
- Offene Hardware-Sicherheitsplattformen und deren freie Nutzung durch Dritte, beispielsweise Smartcard
- Sichere Einbindung von Endgeräten in vertrauenswürdige Umgebungen (Trusted Virtual Domains)
- Sichere Bindung von Smart Devices untereinander und in die Cloud
- Private Social and Mobile Networks (Sicherheitsarchitekturen)
- Entwicklung von Lösungen zur kontextbasierten Anwendung von Sicherheitsmechanismen
- Sicherheitskonzepte für mobile Endgeräte zur Nutzung von Unternehmensressourcen, sichere Integration in IT-Infrastruktur von Unternehmen
- Dynamic Mobile Device Management: Kombination aus festem Regelwerk (Policy) und dynamischer Erkennung von sicherheitsrelevanten Veränderungen
- Konzepte und Überprüfung des sicheren Managements des Smartphone-Lebenszyklus
- Praktische Sicherheitstests für mobile Systeme
- Effiziente Sicherheitstests für Apps, auch hinsichtlich Policys

- Entwicklung von vertrauenswürdigen Plattformen

- Entwicklung von sicheren NFC-Anwendungen für mobile Systeme
- Entwicklung und Integration von Sicherheitshardware für Smartphones
- Next Generation Mobile Platforms and Applications
- Secure Multiparty Computation mit mobilen Geräten
- Cloud-basierte Schadsoftware-Erkennung zur ressourcenschonenden Analyse und Bekämpfung von Schadsoftware auf mobilen Systemen
- Verfahren zur Endnutzer-tauglichen Spezifikation von Sicherheitspolicies auf mobilen Endgeräten

6.15 Sicherheit gegen Seitenkanal- und Fehlerangriffe

Informationssicherheit wird in einer vernetzten Welt durch den Einsatz von kryptographischen Algorithmen und Protokollen gewährleistet. Lange stand die mathematische, kryptoanalytische Sicherheit von verwendeten kryptographischen Algorithmen im Vordergrund, weil das Angriffsmodell nur logische Schnittstellen und Kommunikationskanäle miteinbezog. Mit dem zunehmenden Technologiefortschritt sind nun Geräte, welche zur Informationssicherheit eingesetzt werden, verstärkt eingebettet und einem Angreifer physisch zugänglich. Beispiele hierfür sind sowohl Kreditkarten und Reisepässe als auch eingebettete Systeme, wie man sie in Automobilen für Zugangssysteme oder für eine zukünftig stärkere Vernetzung von Automobilen und Umwelt finden kann. In all diesen Anwendungen muss Information geschützt werden.

Nun muss man heutzutage davon ausgehen, dass ein potentieller Angreifer sich zumindest zeitweise physischen Zugang zu solchen Geräten verschaffen kann. Auf diese Art kann ein Angreifer zusätzliche Informationskanäle nutzen, wie zum Beispiel den Stromverbrauch oder die elektromagnetische Abstrahlung eines Gerätes während der kryptographischen Berechnung. Außerdem kann ein Angreifer ein Gerät gezielt manipulieren. Zum Beispiel kann er mit einem Laser während der Berechnung Fehler in einen geöffneten integrierten Schaltkreis einbringen. Diese Aspekte werden unter dem Begriff der physikalischen Implementierungssicherheit zusammengefasst und beinhalten die sogenannten Seitenkanal- und Fehlerangriffe.

In den vergangenen Jahren konzentrierte sich diese Bedrohung hauptsächlich auf die klassischen Anwendungen eingebetteter Informationssicherheit, nämlich auf Smartcards, und betraf Reisepässe, Personalausweise und Kreditkarten. Aktuell ist es aber notwendig, zum Beispiel auch in Automobilanwendungen Sicherheitsmaßnahmen gegen Seitenkanalangriffe zu integrieren.

Seit Beginn der Erforschung der physikalischen Implementierungssicherheit von kryptographischen Algorithmen in den 1990er Jahren sind bis heute mittlerweile schon mehr als 700[18] solcher Angriffe bekannt geworden. Für Sicherheit zu sorgen bedeutet einen ständigen Wettlauf gegen jährlich wachsende Bedrohungen. Geräte, die heute entwickelt werden, müssen

auf lange Dauer bekannten, aber auch neuen, zur Entwicklungszeit unbekannten Angriffen widerstehen. Daher ist es von großer Wichtigkeit, Schutzmaßnahmen zu entwickeln, welche langfristige Informationssicherheit von kryptographischen Implementierungen gewähren und damit neue Möglichkeiten der potentiellen Angreifer vorwegnehmen.

In diesem Handlungsfeld sind folgende Forschungsaufgaben von großer Relevanz:

- Erforschung des Einflusses auf Seitenkanalangriffe durch hochpräzise Messtechnik, z. B. hoch-auflösende Messung von elektromagnetischer Abstrahlung
- Erforschung der Implikationen einer mehrfachen Laser-Fehlerinjektion für integrierte Implementierungen
- Erforschung der Auswirkung von bisher nicht eingesetzten Methoden aus der Statistik und des maschinellen Lernens auf die Seitenkanalanalyse
- Erforschung von Gegenmaßnahmen zur Prävention gegen Klassen von Angriffen, so dass auch zukünftige Variationen von bestehenden Angriffen oder gänzlich neue Angriffe auf lange Dauer verhindert werden

6.16 Sicherheitsmanagement

Eigeninteresse, gesetzliche Anforderungen sowie branchenspezifische Vorgaben und Auflagen bedingen, dass die Informationstechnik in Unternehmen und Behörden oftmals sehr hohen und heterogenen Sicherheitsanforderungen und Nachweisverpflichtungen unterliegt. Um diesen Anforderungen zu genügen, ist eine umfassende Sicht auf die Informationssicherheit erforderlich, die nicht nur die technischen Komponenten im Blick hat, sondern den Schutz der Informationstechnik strikt an den Erfordernissen der Geschäftsprozesse der Unternehmung ausrichtet. Damit wird das Sicherheitsmanagement zu einem Handlungsfeld, das strategisch gesteuert werden muss.

Ein stringentes Controlling der Aktivitäten zur Informationssicherheit ist dabei unverzichtbar. Aus Managementsicht ist es wünschenswert, zu beliebigen Zeitpunkten eine schnelle und kompakte Information über den Zielerreichungsgrad und eventuelle Abweichungen zu erhalten. Dies leisten die aktuell genutzten Verfahren nicht. Insbesondere der auf Compliance basierende Ansatz, der auf die Implementierung einschlägiger Standards in diesem Bereich (wie IT-Grundschutz, ISO 27001) zielt, liefert noch zu wenig Handlungsempfehlungen, die für die Praxis nutzbar wären. Vor allem das Fehlen von hinreichend validen Kennzahlensystemen, mit denen die Informationssicherheit in einer Organisation überwacht werden kann und die belastbare Aussagen über den Status des Sicherheitsniveaus und den Zielerreichungsgrad liefern können, stellt ein Problem dar. Hier gilt es, die vorhandenen Ansätze zu belastbaren Metriken weiterzuentwickeln, die über die

[18] »700+ Attacks Published on Smart Cards: The Need for a Systematic Counter Strategy«, Matthias Wagner, COSADE 2012

Überwachung technischer Systeme hinausgehen, und diese in ein System von Kennzahlen zu integrieren, das eine ganzheitliche Sicht der Informationssicherheit reflektiert.

Das Thema Messbarkeit berührt auch die ökonomische Bewertung von Sicherheitsinvestitionen und die Ausgestaltung praktischer Sicherheitsprozesse. Es fehlen nach wie vor brauchbare Verfahren, mit denen sich komplexere Investitionen kalkulieren lassen. Dies ist insbesondere für mittelständische Unternehmen ein großes Hindernis, bei denen notwendige Investitionen unterbleiben, weil ihr ökonomischer Nutzen nicht transparent wird.

Besondere Herausforderungen für das Informationssicherheitsmanagement stellen sich bei IT-Anwendungsbereichen, in denen die IT-Risiken noch nicht umfassend erforscht sind. Dies sind aktuell Cloud-Umgebungen und Produktionsinfrastrukturen, insbesondere dort, wo IT-Systeme kritische Infrastrukturen kontrollieren und steuern. Hier fehlt es an Konzepten und Lösungen für ein integriertes Sicherheitsmanagement, das auf Risiken ausgerichtet ist und alle Komponenten der Leistungskette umfasst. Auch hier gibt es einen Bedarf an angemessenen Maßzahlen und Verfahren für ihre Implementierung.

Im Handlungsfeld Informationssicherheitsmanagement besteht folgender Forschungsbedarf:

- Messbarkeit der Effizienz von Sicherheitsmanagementsystemen
- Economics of Security, z. B. Methoden zur Abschätzung der Wirtschaftlichkeit verschiedener Ausgestaltungen von Security Lifecycles
- Entwicklung von Methoden zur Steuerung und Kontrolle von Sicherheitsanforderungen bei der organisationsübergreifenden Entwicklung von Software (Integration von 3rd Party Code)
- Entwicklung von Methoden zum Risikomanagement in neuen Anwendungs- und Technologiefeldern (z. B. Cloud, Produktion)
- Verfahren zur Messbarkeit und zum Vergleich von Impact und Risiken von Sicherheitsvorfällen
- Weiterentwicklung von integrierten Information Security Management Systemen
- Analyse des Einflusses von Compliance-Vorgaben auf IT-Sicherheit und Sicherheitsmanagement
- Untersuchung der Effektivität verschiedener Methoden zur Awareness-Bildung
- Entwicklung von Ansätzen zum organisationsübergreifenden Sicherheitsmanagement
- Sicherheits- und Vertrauenswürdigkeitsmaße zur Bewertung und Nachvollziehbarkeit von Sicherheit durch Nutzer

6.17 Vertrauenswürdige Systeme

Die Software moderner Rechensysteme wird immer komplexer. Damit steigt die Gefahr, dass die Software Sicherheitslücken aufweist, die durch einen Angreifer ausgenutzt werden können. Wie die Vergangenheit gezeigt hat, bieten konventionelle Technologien wie Virenscanner und Firewalls alleine keinen ausreichenden Schutz. Infolgedessen kann die Vertrauenswürdigkeit von Systemen im Allgemeinen nicht garantiert werden. Dies gilt nicht nur für klassische Desktop-Systeme, sondern auch für die immer leistungsfähiger werdenden eingebetteten Systeme, wie z. B. Smartphones, Heimrouter oder auch Smart-Meter-Systeme. Insbesondere für sicherheitsrelevante Anwendungen, wie z. B. Online-Banking, muss sichergestellt werden, dass das hierfür verwendete System vertrauenswürdig ist.

Um Vertrauenswürdigkeit in einem Rechensystem zu schaffen, können Virtualisierungsschichten und Vertrauensanker in Hardware z. B. durch sogenannte Hardware-Security-Module (HSM) eingesetzt werden. Virtualisierung, im Desktop- und Serverbereich auch durch die Prozessoren in Hardware unterstützt, schafft eine komplette Abschottung von Anwendungen, Prozessen oder sogar ganzen Betriebssystemen, die in einer Art Container »eingesperrt« werden. Falls nun ein Angreifer Schwachstellen ausnutzt, die in einem Container ausgeführt werden, kann dieser den Container nicht verlassen und das restliche System ist geschützt. So können insbesondere auch vertrauenswürdige Container festgelegt werden, in denen verifizierte und vertrauenswürdige Software, abgeschottet vom Rest des Systems, ausgeführt wird. In solchen Containern können dann besonders sicherheitskritische Anwendungen ausgeführt werden.

Virtualisierung alleine ist aber oftmals noch nicht ausreichend. So muss sichergestellt sein, dass das System zum Startzeitpunkt vertrauenswürdig war und kein Angreifer den Code der Virtualisierungssoftware ersetzt oder manipuliert hat. Hierzu sind Konzepte für einen sicheren Bootvorgang notwendig, welche üblicherweise spezielle Hardware-Sicherheits-Module (HSM) nutzen. Ein solches HSM bietet neben einem sicheren Speicher für kryptographische Schlüssel und einer sicheren Ausführungsumgebung für kryptographische Operationen meist noch weitere Funktionen zur Erkennung von Manipulationen an der Systemsoftware. Beispielsweise gibt es hier diverse Konzepte der Trusted Computing Group (TCG)[19] rund um das Trusted Platform Module (TPM).

Die derzeitigen Lösungen sind meist nicht generisch einsetzbar und spezielle Anwendungsfälle benötigen angepasste Lösungen. Somit sind in diesem Handlungsfeld folgende Forschungsaufgaben von großer Relevanz:

- Erforschung virtualisierungsbasierter Verfahren zur Konstruktion vertrauenswürdiger Systeme
- Verwendung von Hardware-Security-Modulen (HSM) zur Vertrauensbildung

[19] TCG Trusted Computing Group -- *http://www.trustedcomputinggroup.org.*

- Übertragung von TCG-Konzepten auf eingebettete Systeme wie z. B. Smartphones oder Smart-Meter-Systeme
- Erweiterung bisheriger TCG-Konzepte zur Abdeckung neuartiger Anwendungsfälle
- Realisierung kostengünstiger Sicherheitslösungen zur Vertrauensbildung unter Nutzung existierender Hardware-Erweiterungen (z. B. ARM TrustZone)

6.18 Zusammenspiel Safety und Security

Unsere Gesellschaft hängt in zunehmendem Maße von der Funktion technischer Systeme ab. Daher kommt der Verlässlichkeit der Systeme eine besonders hohe Bedeutung zu. Kein technisches System ist perfekt, d.h. es weist Schwachstellen auf. Treffen Bedrohungen auf Schwachstellen, so kann es zu einer Gefahr für Mensch, Maschine und Umfeld kommen. Um die Gefährdung auf einem akzeptablen Niveau zu halten, sind Maßnahmen zur Erhöhung der Sicherheit notwendig.

Die englische Sprache bietet gegenüber dem Deutschen mit »Safety« und »Security« eine Präzisierung des Begriffes »Sicherheit«. »Safety« bedeutet funktionale Sicherheit, technische Sicherheit und die Vermeidung von nicht akzeptablen Risiken für Menschen, Maschinen und ihre Umgebung. Diese funktionale Sicherheit umfasst den Schutz von Komponenten und Systemen und damit auch den Schutz von Menschen gegen Fehlfunktionen. »Security« dagegen steht für Informationssicherheit, IT-Sicherheit, den Schutz gegen unautorisierte Eingriffe in Komponenten und Systeme einer Maschine oder Anlage.

Die beiden Begriffe sind jedoch nicht unabhängig voneinander: Die funktionale Sicherheit schließt auch die Informationssicherheit mit ein, was bedeutet, dass ohne einen gewissen Grad an Informationssicherheit keine ausreichende funktionale Sicherheit erzielt werden kann.

Fragen der Informationssicherheit für technische Systeme haben stark an Bedeutung gewonnen, da sich durch die Verwendung von offenen Informations- und Kommunikationstechnologien (z. B. PC-Technik, Ethernet, Wireless etc.) eine zunehmende Kompatibilität zu marktgängiger Schadsoftware eingestellt hat. So ist seit 2010 eine Suchmaschine namens »Shodan« bekannt, die nach Prozesssteuerungssystemen sucht, die öffentlich zugänglich sind.[20] Ein prominentes Beispiel für Schadsoftware ist der Wurm »Stuxnet«, der 2010 auf der ganzen Welt Industrieanlagen befallen hat.

Interessanterweise werden funktionale Sicherheit (Safety) und Informationssicherheit (Security) derzeit in getrennten Fachwelten behandelt. Auch Anbieter von Produkten und Lösungen für Informationssicherheit und funktionale Sicherheit stellen Zusammenhänge zwischen diesen beiden Gebieten noch nicht her. Funktionale Sicherheit ist in allen vernetzten Systemen jedoch

[20] Bundesamt für Sicherheit in der Informationstechnik, Quartals-Lagebericht 4/2010

nicht ohne Informationssicherheit realisierbar. Gleichzeitig können aus beiden Ansätzen gegenläufige Anforderungen entstehen, beispielsweise für das Systemverhalten in Notfällen.

Zwischen Safety und Security gibt es vielfältige Querbeziehungen und Übereinstimmungen in Basistechniken. Bisher werden solche Abhängigkeiten weder beim Systementwurf noch beim Betrieb technischer Systeme systematisch berücksichtigt. Benötigt werden integrierende Systemarchitekturen sowie Konzepte und Modelle zur Umsetzung eines ganzheitlichen Sicherheitsbegriffs.

Forschungsaufgaben in diesem Zusammenhang sind:

- Gemeinsame Systemarchitekturen für funktionale Sicherheit (Safety) und Informationssicherheit (Security)
- Konzepte und Methoden zur Integration und Umsetzung des ganzheitlichen Sicherheitsbegriffs (Safety + Security)
- Berücksichtigung von Wechselwirkungen zwischen funktionalen und nicht-funktionalen Anforderungen zum Zeitpunkt des Entwurfs
- Übertragung und Tauglichkeitsanalyse von Sicherheitstechniken aus industriellen Anwendungsfeldern
- Schutz von Notrufsystemen gegen Missbrauch und Angriffe
- Simulationsmethoden zur Prüfung und zum Nachweis der Zuverlässigkeit von Notruf-, Frühwarn- und Katastrophenmanagementsystemen
- Generisches Protokoll-Monitoring auf der Basis anwendungsspezifischer Constraint-Modelle unter Beachtung von Semantik und Pragmatik, z. B. in Service Oriented Architectures
- Situationsbewusstsein (Situation Awareness) und Entscheidungsunterstützung
- Methoden und Werkzeuge zur Modellierung von sicherheitskritischen Systemumgebungen und bestehenden Abhängigkeiten
- Modell-basierte Analyse der Auswirkungen von Gegenmaßnahmen gegen erkannte Bedrohungen auf funktionale Sicherheit
- Modell-basierte Entscheidungsunterstützung zur Bewertung und Auswahl von Handlungsalternativen
- Security Metrics – Maße für Schutzzielerreichung
- Ergonomische Darstellung von Sicherheitslagebildern

IMPRESSUM

HERAUSGEBER

Prof. Dr.-Ing. Reimund Neugebauer
Präsident der Fraunhofer-Gesellschaft
Prof. Dr. Matthias Jarke
Vorsitzender Fraunhofer-Verbund IuK Technologie
Prof. Dr. rer. nat. Klaus Thoma
Vorsitzender Fraunhofer-Verbund Verteidigungs- und Sicherheitsforschung VVS

PRODUKTION

Frotscher Druck GmbH, Darmstadt

GESTALTUNG

Marion Mayer, riondesign

ANSCHRIFT DER REDAKTION

Fraunhofer-Verbund IUK-Technologie
Anna-Louisa-Karsch-Straße 2
10178 Berlin
thomas.bendig@iuk.fraunhofer.de

TITELBILD

iStock.com