Prof. Dr. Thorsten Holz _ Prof. Dr. (TU NN) Norbert Pohlmann
Prof. Dr. Eric Bodden _ Prof. Dr. Matthew Smith _ Dipl.-Wi.-Ing. Jörg Hoffmann

Human-Centered Systems Security

IT-Sicherheit von Menschen für Menschen

universitätbonn
fir an der RWTH Aachen
PADERBORN UNIVERSITY The University for the Information Society
if(is) internet-sicherheit.
hgi Horst Görtz Institut für IT-Sicherheit

Impressum

Prof. Dr. Thorsten Holz
thorsten.holz@rub.de
Horst Görtz Institut für IT-Sicherheit (HGI)
Universitätsstraße 156, 44780 Bochum
https://www.hgi.rub.de

Prof. Dr. (TU NN) Norbert Pohlmann
pohlmann@internet-sicherheit.de
Institut für Internet-Sicherheit – if(is)
Neidenburger Straße 43, 45897 Gelsenkirchen
https://www.internet-sicherheit.de

Prof. Dr. Eric Bodden
Heinz Nixdorf Institut / Universität Paderborn / Fraunhofer IEM
Zukunftsmeile 1, 33102 Paderborn
https://blogs.uni-paderborn.de/sse

Prof. Dr. Matthew Smith
Universität Bonn / Institut für Informatik 4 / Fraunhofer FKIE
Friedrich-Ebert-Allee 144, 53113 Bonn
https://net.cs.uni-bonn.de

Dipl.-Wi.-Ing. Jörg Hoffmann
joerg.hoffmann@fir.rwth-aachen.de
Forschungsinstitut für Rationalisierung (FIR) e. V. an der RWTH Aachen
Campus-Boulevard 55, 52074 Aachen
http://www.fir.rwth-aachen.de

Gesamtgestaltung | Layout:
c74 gestaltung & design, Dortmund
Cornelia Robrahn | www.c74.org

Webversion 1. Auflage 2016

Bildnachweise:
Titelcollage: C. Robrahn, shutterstock: ProStockStudio, Bruce Rolff, kurhan; iStock: alengo, Yakobchuk; S. 3 oben: li: Horst Görtz Institut für IT-Sicherheit (HGI), mitte: if(is) – Institut für Internet-Sicherheit, re: Frauke Döll, S. 3 unten: li: Barbara Frommann Uni Bonn, re: Jörg Hoffmann; S. 4: shutterstock: iconspro, Bruce Rolff, kurhan; iStock: alengo, Yakobchuk; S. 5,7,8,13: C. Robrahn; U4: C. Robrahn, shutterstock: iconspro, Bruce Rolff, kurhan; iStock: alengo, Yakobchuk;

Gefördert durch

Ministerium für Innovation, Wissenschaft und Forschung des Landes Nordrhein-Westfalen

nrw-uniTS
IT-SICHERHEIT NORDRHEIN-WESTFALEN

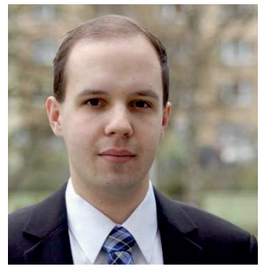
Die Autoren

Prof. Dr. Thorsten Holz
Horst Görtz Institut für
IT-Sicherheit (HGI)
Ruhr-Universität Bochum
thorsten.holz@rub.de

Prof. Dr. (TU NN) Norbert Pohlmann
if(is) – Institut für Internet-Sicherheit
Westfälische Hochschule,
Gelsenkirchen
pohlmann@internet-sicherheit.de

Prof. Dr. Eric Bodden
Professur für Praktische
Informatik (Softwaretechnik)
Universität Paderborn /
Direktor Fraunhofer IEM
eric.bodden@uni-paderborn.de

Prof. Dr. Matthew Smith
Leiter der Arbeitsgruppe
„Usable Security And Privacy“
Rheinische Friedrich-Wilhelms-
Universität Bonn / Mitglied des
Fraunhofer FKIE
smith@cs.uni-bonn.de



Dipl.-Wi.-Ing Jörg Hoffmann
Fachgruppenleiter
IT-Komplexitätsmanagement
FIR e. V. an der RWTH Aachen
joerg.hoffmann@fir.rwth-aachen.de

Das Strategiepapier wurde im Rahmen des vom Ministerium für Innovation, Wissenschaft und Forschung (MIWF) des Landes Nordrhein-Westfalen initiierten Round Table IT-Sicherheit angestoßen und umgesetzt. Die Erstellung dieses Dokuments wurde unterstützt von dem IT-Sicherheitsnetzwerk nrw.uniTS.

Informationen rund um dieses Dokument, über die Autoren und die neuste Version zum Download erhalten Sie unter: www.it-sicherheit-nrw.de
Stand: 12. Dezember 2016

Inhaltsverzeichnis

Motivation

Informationstechnische Systeme durchdringen alle Bereiche unseres täglichen Lebens. Während Smartphones, Tablets und Smart-TVs den Endanwender bereits erobert haben, stehen Technologien wie Smart Home, Smart Production und Smart Grid kurz davor, weitere wichtige Bereiche des privaten und geschäftlichen Lebens von Grund auf zu erneuern. Eine ernstzunehmende Herausforderung dabei ist die zunehmende Vernetzung der industriellen Produktion durch modernste Informations- und Kommunikationstechnik *(Industrie 4.0)*. Die Hoffnung der Wirtschaft ist groß: Die Technologien sollen neue Geschäftsmodelle und Wertschöpfungsketten erschließen sowie neue Dienstleistungsmodelle erlauben, die zuvor nicht möglich waren.

Eins der größten Hemmnisse dieser positiven Entwicklung ist jedoch der Mangel an IT-Sicherheit. Trotz jahrelanger intensiver Forschung und Entwicklung an sicheren IT-Systemen steigen die Anzahl der erfolgreichen Angriffe, und deren Ausmaß jährlich. Eine Studie des Digitalverbands Bitkom von April 2015 zeigt, dass mehr als die Hälfte (51 Prozent) aller deutschen Unternehmen in den vergangenen zwei Jahren Opfer von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden sind. Jährlich entsteht dadurch in Deutschland ein Schaden von rund 51 Milliarden Euro. In den kommenden Jahren wird der Schaden sogar auf rund 306 Milliarden Euro geschätzt. Durch die fortschreitende Digitalisierung bzw. durch technische Entwicklungen wird auch die Angreifbarkeit der verwendeten IT-Systeme in Folge dessen weiter steigen. Wie ist dies zu erklären und wie können wir diesen Bedrohungen entgegenwirken?

Die Autoren dieser Forschungsagenda haben den *Faktor Mensch* als eines der Grundprobleme in der IT ausgemacht. Existierende Forschungsvorhaben widmen sich beispielsweise verstärkt der sicheren Entwicklung von Hardware/ Softwaresystemen oder der Erforschung von Prinzipien für *Security by Design/Privacy by Design.* Weitestgehend unerforscht geblieben ist jedoch bisher die Frage wie Sicherheitsmechanismen auf allen Ebenen der Wertschöpfungskette so gestaltet werden können, dass sie für die betreffenden Personenkreise auch effektiv anwendbar sind. Für Forschung zum *Faktor Mensch* sehen wir eine besondere Stärke am Wissenschaftsstandort NRW. Die Problematik ist drängend, denn während die IT-Sicherheitsforschung der letzten Jahre vor allem neue technischen Lösungen hervorgebracht hat, sind es letztendlich *Menschen*, die diese Lösungen einsetzen und anwenden. Wie sich zeigt, sind die Menschen heutzutage auf allen Ebenen der Wertschöpfungskette mit den ihnen anvertrauten Sicherheitsmechanismen überfordert (siehe auch Abbildung 1):

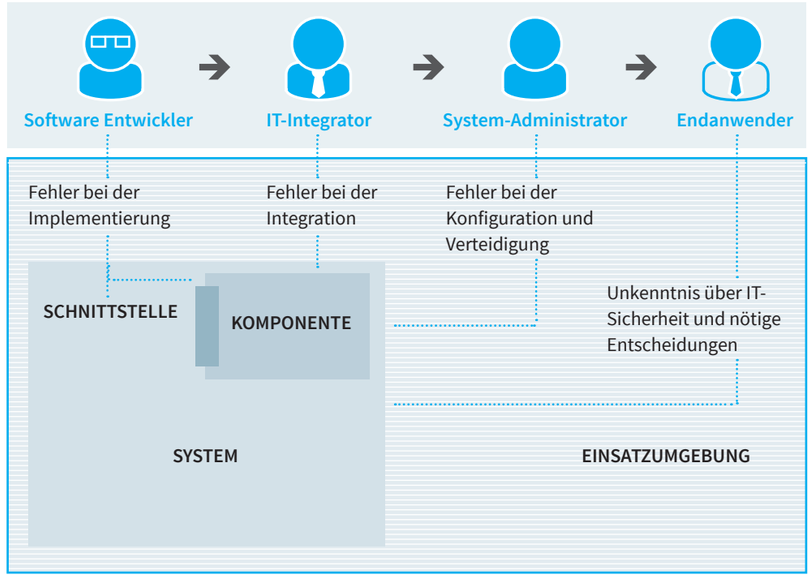


ABBILDUNG 1: ZUSAMMENSPIEL DER EINZELNEN PARTEIEN UND POTENTIELLE SICHERHEITSPROBLEME

- **Softwareentwickler** können keine wohlinformierten Sicherheitsaussagen über Komponenten Dritter treffen. Darüber hinaus sind sie häufig bei der Verwendung wichtiger Sicherheitsschnittstellen (z. B. Krypto-Bibliotheken) überfordert und machen Fehler. Ebenso sind sie aufgrund

mangelnder modularer Sicherheitskonzepte nicht in der Lage, flächendeckend sichere Software zu erstellen.

- **IT-Integratoren** haben oft starkes Wissen in ihrer eigenen Anwendungsdomäne (z. B. Fahrzeug- oder Maschinenbau, Gesundheitswesen oder der chemischen Industrie), jedoch mangelnde Expertise in IT-Sicherheit und der Integration entsprechender Mechanismen. Hinzu kommt, dass sich manche Sicherheitsprobleme erst durch die Anwendung einer Software in einer bestimmten Domäne ergeben. Eigentlich benötigt man also Methoden, die auch die Einhaltung domänenspezifischer Sicherheitsanforderungen gewährleisten.
- **Systemadministratoren** müssen Systeme sicher konfigurieren und zuverlässig Angriffe erkennen sowie diesen begegnen. Jedoch wissen sie oft zu wenig über Angriffs- und Verteidigungsstrategien. Dabei erweitert sich deren Aufgabengebiet vom klassischen IT-Betrieb hin zur Betreuung von komplexen IT-Systemen in Produktionsanlagen und Produkten.
- **Endanwender** nutzen IT-Systeme in allen möglichen Lebensbereichen, sowohl privat als auch beruflich. Sie haben in der Regel keinerlei Expertise im Bereich IT-Sicherheit, müssen aber trotzdem vor Identitätsdiebstahl, Datendiebstahl und -manipulation sowie ähnlichen Gefahren geschützt werden. Themen wie Sicherheitsupdates, Fehlermeldungen bezüglich potentieller Sicherheitsprobleme, Schadsoftware und ähnliche Aspekte stellen weitere Herausforderungen für den Endanwender dar. Darüber hinaus werden sie geplagt von Unmengen an Passwörtern, die nicht notiert und mehrfach verwendet werden sollen. Die Anforderungen, die heutige Sicherheitskonzepte an Endanwender stellen sind unrealistisch und werden daher in der Praxis meist nicht eingehalten. Im Unternehmen differenziert sich die Gruppe der Endanwender in Nutzer (z. B. Industriearbeiter, Handwerker oder Büroarbeiter) und Entscheider. Auch hier müssen die Nutzer entsprechend ihren spezifischen Anforderungen geschult und sensibilisiert werden. Manager stehen vor der großen Herausforderung, die richtigen Entscheidungen im Kontext der IT-Sicherheit für ihr Unternehmen zu treffen. Sie müssen Regeln festlegen, IT-Security-Projekte vorantreiben und Risiken minimieren.

Im Resultat scheint es nicht verwunderlich, dass aufgrund der o. g. Probleme der Faktor *Mensch* bei den vielen Angriffen der letzten Jahre als *schwächstes Glied in der Kette* am Entstehen der betreffenden Sicherheitslücken beteiligt war. Informationstechnologien werden von Menschen gestaltet und können nur so sicher sein wie die Sicherheitskonzepte der Menschen, die sie gestalten. Ziel der Forschung muss daher sein, Sicherheitskonzepte, Methoden und Technologien zu entwickeln, die auf allen Ebenen der Wertschöpfungskette den beteiligten Menschen nur solche Entscheidungen abverlangen, die sie auch qualifiziert treffen können. Die übergeordnete Fragestellung ist, wie die Nutzerakzeptanz von IT-Sicherheitsmechanismen erhöht werden kann. Die hier vorgestellte Forschungsagenda zeigt Forschungsbedarf in verschiedenen Bereichen auf, um so alle Nutzergruppen entsprechend ihrer spezifischen Herausforderungen zu berücksichtigen.

Bedarfsanalyse

Den o. g. Problemen kann nur dann effektiv begegnet werden, wenn die *Benutzbarkeit* auf allen Ebenen der IT-Sicherheit systematisch verbessert wird. Hierzu muss der Faktor *Mensch* in technischen Systemen besser verstanden und berücksichtigt werden. Die folgenden Beispiele illustrieren dabei einige der Herausforderungen:

- Das Entstehen von Softwarefehlern muss untersucht werden. Zusätzlich müssen Werkzeuge erforscht und entwickelt werden, die bei der Erstellung und Überprüfung von (sicherer) Software unterstützen. Insbesondere die automatische Überprüfung auf Sicherheitslücken ist ein schwieriges Problem. Entsprechende Tools zur automatisierten Erkennung von potentiellen Fehlern müssen in Hinblick auf Bedienbarkeit entwickelt und evaluiert werden.
- Fehler von IT-Integratoren müssen analysiert werden. Ferner ist die Entwicklung von Werkzeugen und Prozessen notwendig, die es ihnen ermöglichen, in ihrer jeweiligen Anwendungsdomäne sichere Software einzusetzen. Darüber hinaus muss erforscht werden, wie eine vertrauenswürdige Integration von Sicherheitslösungen in existierende Infrastrukturen erfolgen kann.
- Es muss geprüft werden, wie und warum Systemadministratoren in ihrem jeweiligen Anwendungskontext Fehler machen. Außerdem müssen mächtige und zugleich benutzbare Werkzeuge entwickelt werden, die eine sichere Konfiguration von Systemen ermöglichen und den Administrator bestmöglich unterstützen. Darüber hinaus muss erforscht werden, wie Software zur Angriffserkennung und -abwehr Ergebnisse und Lagebilder generieren können, die direkt und einfach zu nutzende Informationen liefern, mit denen Systemadministratoren präventive Maßnahmen ergreifen und damit Schäden begrenzen können.
- Endanwender benötigen einfach zu verwendende und gut erklärte IT-Lösungen, die auf ihre Bedürfnisse zugeschnitten sind. Ziel sind dabei Sicherheitslösungen, die für Nutzer möglichst transparent sind und dennoch im Bedarfsfall ein Eingreifen des Endanwenders ermöglichen. Dazu müssen sowohl für den privaten, als auch für den geschäftlichen Bereich passende Lösungen entwickelt werden, da die früher existierenden Grenzen zunehmend verschwimmen. Endanwender benötigen sichere IT-Lösungen und Wissen über deren Nutzung. Dieses gilt für Smartphones und soziale Netzwerke genauso wie für die Maschinen auf dem Shopfloor und für dienstliche Rechner und betriebliche Anwendungssysteme. Dem Management müssen Richtlinien, Quantifizierungshilfen und Best-Practices an die Hand gegeben werden, um gerade im Hinblick auf die zunehmende Digitalisierung die richtigen Entscheidungen für eine sichere Unternehmens-IT treffen zu können.

Abbildung 2 zeigt das Zusammenspiel der verschiedenen Akteure. Jede Handlung – wie z. B. das Erstellen oder Konfigurieren von Systemen – stellt eine Fehlerquelle dar. Jeder Akteur der Wertschöpfungskette erbt die Fehler der Vorgänger und kann selbst neue Fehler hinzufügen. Originär entstandene Fehler werden entlang der Wertschöpfungskette „weitergereicht“ und können im Nachhinein kaum korrigiert werden.

Daraus lässt sich ableiten, dass Akteure wie Entwickler und Kryptographen eine viel wichtigere Rolle für die IT-Sicherheit spielen als Endnutzer und somit deren Fehler viel größere Auswirkungen haben. Diese Gewichtung ist in der Abbildung mit einem hell/dunkel Verlauf gekennzeichnet. Der größte Forschungsbedarf liegt somit in der Entwicklung sicherer und benutzerfreundlicher Systeme.

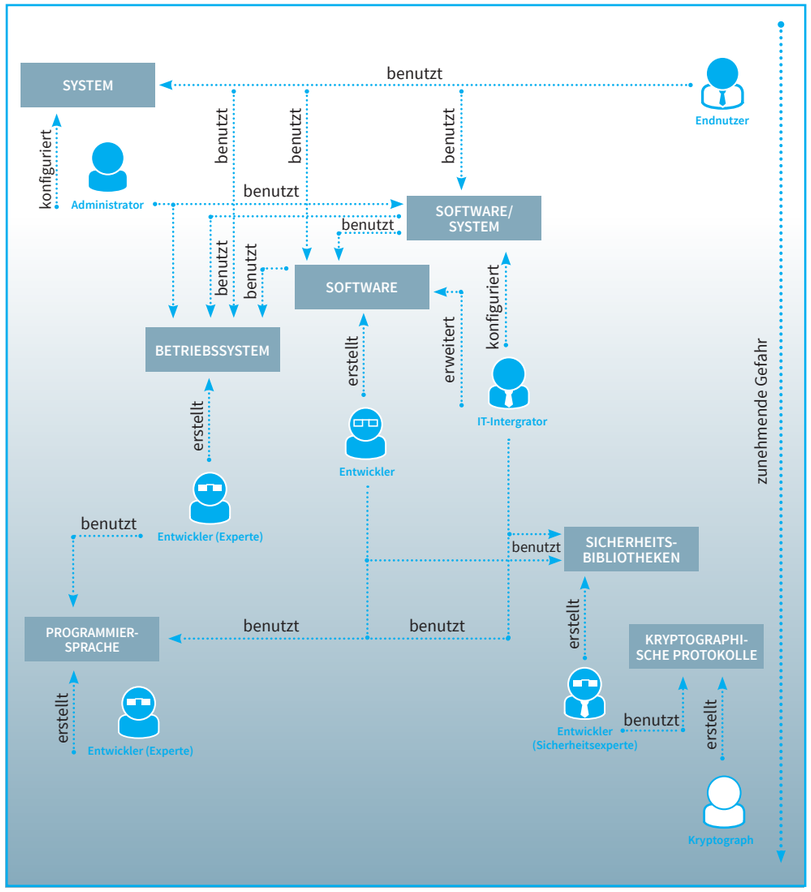
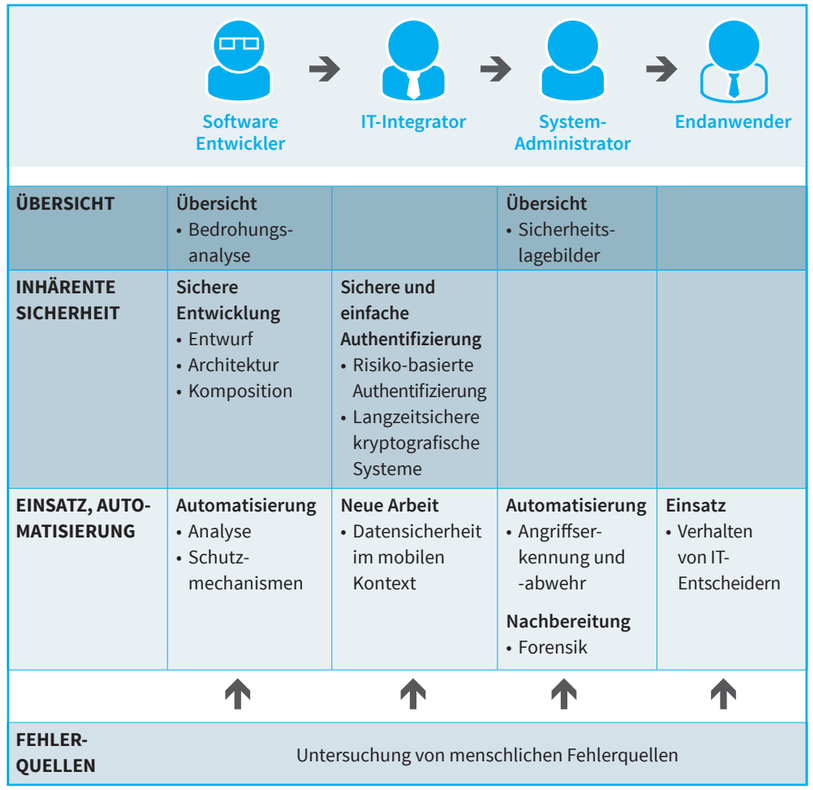


ABBILDUNG 2: ZUSAMMENSPIEL DER VERSCHIEDENEN AKTEURE UND DEREN BEZIEHUNGEN FORSCHUNGSBEDARF

FORSCHUNGSBEDARF

ABBILDUNG 3: ZUSAMMENFASSUNG FORSCHUNGSBEDARF ZU *HUMAN-CENTERED SYSTEMS SECURITY*



Basierend auf der Bedarfsanalyse ergibt sich ein Forschungsbedarf in den vier Bereichen Bedrohungsanalysen, Fehlerquellen in der Softwareentwicklung, sichere Entwurfsmethodologien und sichere Software- und System-Architekturen. Diese werde im Folgenden skizziert sowie eine Schätzung der zeitlichen Aufwände abgegeben und mögliche Fördergeber aufgezeigt. (vgl. auch Abbildung 3) Die skizzierten Forschungsfelder ergänzen die im Strategiepapier „IT-Sicherheit für NRW 4.0 – Gemeinsam ins digitale Zeitalter. Aber sicher“ dargelegten Herausforderungen für die Wissenschaft.

Den ersten Teil der Wertschöpfungskette bei IT-Systemen bilden die **Softwareentwickler.** Sie erschaffen neuartige Softwareprodukte, in der Regel unter Verwendung einer ganzen Reihe existierender Softwarekomponenten Dritter und müssen dabei sehr komplexe Problemstellungen lösen. Die wesentlichen Herausforderungen zur Unterstützung von Softwareentwicklern zielen darauf ab, eine ganze Reihe von Problemen systematisch zu lindern. Insbesondere die folgenden Herausforderungen sollen dabei betrachtet werden. Der *Faktor Mensch* soll in allen Punkten berücksichtigt werden. Hierzu werden Benutzerstudien durchgeführt, um die erforschten Methoden empirisch zu validieren:

- **Effektive, reproduzierbare Bedrohungsanalyse:**
  Der erste Schritt zur Erstellung eines sicheren IT-Systems liegt in der systematischen Erfassung der auf dieses System einwirkenden Bedrohungen: Effektiver Schutz ist nur möglich, wenn der Ursprung der Problematik erkannt ist. Hier gilt es Softwarearchitekten bei dieser wichtigen Aufgabe zu unterstützen, um das Übersehen und Fehleinschätzen von Bedrohungen zu vermeiden. Es sollen daher Methoden und Werkzeuge geschaffen werden, welche eine reproduzierbare Bedrohungsanalyse (idealerweise durch reguläre Softwareentwickler) erlauben. (~5 Jahre, EFRE)
- **Untersuchung von menschlichen Fehlerquellen bei der Softwareentwicklung:**
  Fehler von Entwicklern sind kritisch für die Sicherheit entlang der gesamten Wertschöpfungskette. Um Entwickler effektiv bei der Erstellung von sicherer Software zu unterstützen, muss auch die Ursache der Fehler erforscht werden – insbesondere hinsichtlich der menschlichen Einflussfaktoren. Hierzu müssen Benutzerstudien durchgeführt werden, um die mentalen Modelle und das Verhalten von Entwicklern zu studieren. (5 Jahre, MIWF/EFRE)
- **Sichere Entwurfsmethodologien:**
  Neben all den beteiligten Technologien ist die Softwareentwicklung vor allem ein von vielerlei unterschiedlichen Menschen getriebener Prozess. In einem solchen Prozess stehen dem Wunsch nach sicherer Software andere Faktoren wie eine kurze Time-to-Market, Konkurrenzdruck, die Änderung von Anforderungen und Technologien, usw. gegenüber. Das Ziel systematischer Entwurfsmethodologien ist es, all diesen Faktoren kontrolliert zu begegnen, um pareto-optimale Lösungen zu finden. Es soll erforscht werden, wie – trotz der oben genannten Einflussfaktoren – die Sicherheit von Softwaresystemen optimal gesteigert werden kann. (~5 Jahre, EFRE/MIWF)
- **Sichere Software- und System-Architekturen:**
  Während sich viele Schwachstellen auf der Ebene des Programmcodes finden, entstehen ebenso viele Schwachstellen bereits auf der Ebene von Softwarearchitekturen, durch ein fehlerhaftes Verständnis von Sicherheitskonzepten und Garantien, die diese für Teile der Architektur liefern. Es soll daher erforscht werden, wie aus den Ergebnissen einer bestehenden Bedrohungsanalyse Architekturen abgeleitet werden können, die diesen Bedrohungen auf nachweisbar sichere Weise Abwehrmechanismen entgegensetzen (unter der Annahme, dass sie Konzepte selbst sicher implementiert sind). Sicherheitsanforderungen sollen sich so über mehrere Ebenen nachverfolgen und verfeinern lassen. (5 Jahre, EFRE)
- **Sichere Komposition:**
  Es soll erforscht werden, wie sich Komponenten Dritter sicher in ein bestehendes Softwaresystem einbinden lassen. Hierzu sollen u.a. auch die nötigen und möglichen Interaktionsprotokolle zwischen der Gesamtsoftware und ihren Komponenten untersucht und wo möglich konstruktiv vereinfacht werden. Die Schaffung benutzbarer Schnittstellen und Protokolle für die Anwendung kryptografischer Verfahren scheint ein besonders wichtiger Anwendungsfall dieser Forschung zu sein (1-3 Jahre, MIWF).
- **Automatisierte Analyse von Softwarecodes und -modellen:**
  Um die Kosten für die Behebung von Sicherheitsschwachstellen möglichst gering zu halten, ist es essentiell diese möglichst früh in der Wertschöpfungskette zu entdecken. Als wichtiges Mittel sollen hierzu automatisierte Analysen von Softwareartefakten und -modellen erforscht werden, welche möglichst ohne manuelle Hilfe des Softwareentwicklers Softwareschwachstellen aufzeigen können. Ein besonderes Augenmerk muss hierbei auch der Präsentation der Analyseergebnisse gewidmet werden, denn schließlich müssen die Softwareentwickler diese Ergebnisse korrekt deuten und verstehen können. (1-5 Jahre, MIWF/EFRE)
- **Schutzmechanismen für Softwaresysteme:**
  Fehler sind menschlich – diese Weisheit gilt auch in der Softwareentwicklung. Hierdurch bedarf es besonderer Schutzmechanismen, die im Falle von menschlichen Fehlern greifen. Es soll erforscht werden, wie Softwaresysteme durch automatisierte Härtungstechnologien angriffssicherer gestaltet werden können, indem die Technologien beispielsweise die Ausnutzung der bestehenden Schwachstellen verhindern. (1-3 Jahre, EFRE/MIWF)

Darüber hinaus besteht ein großer Bedarf an Sicherheitsanforderungen im Bereich der **IT-Integratoren.** Wie oben bereits erläutert, verfügen sie oft über großes Wissen in ihrer Anwendungsdomäne, haben jedoch kaum Wissen im Bereich der IT-Sicherheit. Entsprechend müssen Methoden erforscht und entwickelt werden, die die Einhaltung auch domänenspezifischer Sicherheitsanforderungen gewährleisten können. Konkret besteht dabei vor allem Bedarf im Bereich des **sicheren und einfach zu nutzenden Identitätsmanagement,** da dieses eine Grundvoraussetzung für sichere Systeme darstellt. Außerdem besteht in diesem Bereich ein Bedarf an **nutzbaren und langzeitsicheren kryptographischen Verfahren,** weil Kryptographie einen Grundbaustein von sicheren Systemen bildet. Die folgenden Themenkomplexe sollen hierbei erforscht werden:

- **Untersuchung von menschlichen Fehlerquellen bei der IT-Integration:**
  Wie bereits zuvor skizziert, sind Fehler von IT-Integratoren kritisch für die integrierten Systeme. Um IT-Integratoren effektiv bei der Integration von Software zu unterstützen, müssen auch an dieser Stelle Gründe und Ursachen der Fehler, die durch den Menschen verursacht werden, aufgrund nicht existenter Forschung offenbart werden. Benutzerstudien sollen die mentalen Modelle und das Verhalten von IT-Integratoren studieren, um darauf aufbauend Problemquellen zu beseitigen und zur Entwicklung von adäquaten Unterstützungsmethoden beizutragen. (5 Jahre, MIWF/EFRE)
- **Risikobasierte Authentifizierungsmechanismen:**
  Die Benutzerauthentifizierung, also das Verifizieren der Identität einer Person, ist eine zentrale Komponente im Design vieler IT-Systeme. Passwort-basierte Verfahren oder allgemeiner wissensbasierte Verfahren sind weit verbreitet, haben aber mehrere Nachteile: Passwörter sind für den Benutzer nur schwer zu merken, sie besitzen häufig geringe Entropie und sind daher leicht zu

erraten, sie sind anfällig für Phishing-Angriffe, und das Verwenden eines Passwortes für mehrere Dienste führt zu einem „Kaskadeneffekt“, da ein Angriff gegen einen Dienst die Sicherheit mehrerer Dienste beeinträchtigen kann. Bei der *risikobasierten Authentifizierung* werden Anmeldeversuche anhand der verfügbaren Informationen in „unverdächtige“ und „verdächtige“ Aktivitäten eingeteilt. Verfügbare Informationen umfassen hierbei beispielsweise die verwendete IP-Adresse und darauf basierende Ortsbestimmung, Informationen zu benutzter Software und installierten Erweiterungen, Zeit und Frequenz der Anmeldeversuche, und mehr. Dieser Prozess verläuft für den Benutzer vollständig transparent. Diese Verfahren können zum einen dazu eingesetzt werden, passwortbasierte Authentifizierung zusätzlich zu stärken, zum anderen können sie aber auch als Basis für eine passwortlose Authentifizierung dienen, falls die Klassifizierung hinreichend präzise arbeitet. Eine wissenschaftliche Untersuchung soll zum einen die Zuverlässigkeit der Verfahren erhöhen, zum anderen aber auch eine größere Zahl von Unternehmen als bisher in die Lage versetzen, risikobasierte Authentifizierung zu verwenden und damit den Komfort und die Sicherheit ihrer Benutzer zu verbessern. (1-3 Jahre, EFRE/MIWF)

- **Sicherheitskonzepte für neue Arbeitswelten:**
  Die zunehmende Digitalisierung verändert die heutige Arbeitswelt. Durch die zunehmende Entgrenzung von Arbeit und Privatem sowie der erhöhten Mobilität von Arbeitnehmern erhöhen sich die Ansprüche an IT-Sicherheitskonzepte. Beispielsweise werden (private) mobile Endgeräte in unterschiedlichen Anwendungskontexten genutzt. Die dabei generierten, diverse Daten gilt es zu trennen und effektiv zu schützen. (1-5 Jahre, EFRE)
- **Effektive, funktionale, langzeitsichere kryptografische Systeme:**
  Die Sicherheit aller derzeit im Einsatz befindlichen klassischen Kryptographieverfahren beruhen auf der Schwierigkeit, diverse zahlentheoretische Probleme schnell auf modernen Computern lösen zu können. Quantencomputer beruhen auf quantenmechanischen Gesetzen und können die oben genannten Probleme sehr schnell lösen (d.h. mit Hilfe von Quantencomputern kann jegliche klassische Kryptographie gebrochen werden). Derzeit ist es unklar, ob und wann Quantencomputer hergestellt werden können. Führende internationale Forscher gehen jedoch davon aus, dass dieses in den nächsten 10-20 Jahren passiert. Für diesen Fall muss bereits jetzt begonnen werden effiziente, asymmetrische kryptografische Verfahren zu entwickeln, welche auch in der Lage sind von Quantencomputern aus gesteuerte Angriffe abzuwehren. Gitter-basierte Systeme haben sich in den letzten Jahren zwar als vielversprechend herausgestellt, allerdings fehlt es ihnen noch an Effizienz. Derzeitige Kandidaten sind noch einige Faktoren langsamer als klassische Verfahren. Zur Weiterentwicklung dieses Ansatzes wird in den nächsten Jahren umfangreiche mathematische Grundlagenforschung benötigt, welche die Theorie von Gitter-basierter Kryptographie vertieft. (1-10 Jahre, MIWF / DFG)

Aufgrund der Komplexität heutiger Systeme ist es bisher nicht möglich, komplett sichere Systeme zu entwickeln und deshalb besteht ein Bedarf im Bereich der **reaktiven Sicherheit,** um auf Sicherheitsvorfälle effizient und zeitnah reagieren zu können. Dabei müssen die drei ineinandergreifenden Themenkomplexe *Prävention, Erkennung* und *Reaktion* betrachtet werden, um ein ganzheitlich ausgerichtetes Angriffsmanagement umzusetzen. Auch in diesem Bereich spielt der *Faktor Mensch* eine wichtige Rolle. Insbesondere **Systemadministratoren** müssen in die Lage versetzt werden, Systeme sicher zu konfigurieren und zuverlässig Angriffe erkennen zu können. Darüber hinaus ist eine effiziente Strategie zur Abwehr von Angriffen nötig, um schnell auf Schutzzielverletzungen reagieren zu können. In der Praxis sind Administratoren jedoch meist unwissend über Angriffs- und Verteidigungsstrategien. Deshalb ist eine Unterstützung dieser Nutzergruppe durch weitere Forschungsanstrengungen nötig, um ein *nutzbares* Angriffsmanagement zu entwickeln. Konkreter Bedarf besteht dabei in den folgenden Themengebieten:

- **Untersuchung von menschlichen Fehlerquellen bei der IT-Administration:**
  Fehler von Administratoren sind kritisch für die Systeme selbst sowie alle Nutzer der Systeme. Um Administratoren effektiv bei der Administration von Software zu unterstützen, müssen auch an dieser Stelle die Ursache der Fehler eruiert und evaluiert werden. Basierend auf Benutzerstudien können Methoden zur Eliminierung der Fehlerquellen erforscht werden. (5 Jahre, MIWF/EFRE)
- **Automatisierte Angriffsprävention, -erkennung und -abwehr:**
  Es soll erforscht werden, in wie fern die Bereitstellung von Softwaretools zur Unterstützung von Systemadministratoren beitragen können. Dazu werden die drei Aspekte des Angriffsmanagements betrachtet: Zur Angriffsprävention soll eine automatisierte Lösung für eine sichere Konfiguration und Absicherung von Computersystemen entwickelt werden. Eine verlässliche, automatisierte und präzise Erkennung von Angriffen sowohl auf Netzwerk- als auch Endsystemebene ist nötig, um zeitnah Sicherheitsvorfälle aufdecken zu können. Ergänzend dazu ist auch eine automatisierte Reaktion auf Angriffe erstrebenswert, um bei einem Sicherheitsvorfall ad hoc reagieren zu können.
  In diesen drei Bereichen sollen Methoden entwickelt werden, die Systemadministratoren bei ihrer Arbeit durch automatisierte Prozesse unterstützen und so effiziente Reaktionen auf die steigende Anzahl an Vorfällen gewährleisten. (1-10 Jahre, EFRE/MIWF)
- **Verlässliche Generierung von IT-Sicherheitslagebildern:**
  Das IT-Sicherheitsniveau innerhalb von IT-Netzwerken (Firmennetzwerke, Behördennetzwerke, Internet, ...) hängt von vielen Faktoren ab und ist dementsprechend schwierig für Systemadministratoren zu beurteilen. Diese Nutzergruppe muss deshalb in die Lage versetzt werden, schnell und einfach einen Überblick zum aktuellen Systemzustand zu erhalten. Entsprechende menschengerechte Methoden und Tools zur verlässlichen Generierung von IT-Sicherheitslagebildern sollten erforscht und in der Praxis erprobt werden. Darüber hinaus wäre die Gründung eines Cyber-Lagezentrums in NRW zur Erstellung von Kommunikationslagebildern für öffentliche Einrichtungen in Kommunen, Ministerien und Firmen wünschenswert, soweit die sicherheitstechnische Bewertung eine Weitergabe der Information zulässt. Fragen nach dem Zustand der IT-Systeme in den angeschlossenen Infrastrukturen und dem Reaktionsbedarf könnten so beantwortet werden. Dies würde auch einen anonymen Vergleich untereinander ermöglichen und das gemeinsame IT-Sicherheitsniveau mittel- und langfristig erhöhen. (1-3 Jahre, EFRE)
- **Automatisierte Unterstützung für Incident Response/Recovery und forensische Analyse:**
  Um eine effiziente Reaktion auf Sicherheitsvorfälle zu ermöglichen ist die Entwicklung von menschengerechten Forensiktools zur Aufklärung nötig, um entsprechende Angriffe effektiver und schneller aufklären zu können. Dabei muss erforscht werden, wie juristisch nutzbare Informationen bestmöglich gesammelt und ausgewertet werden können. Fragen der Skalierbarkeit und des Datenschutzes müssen dabei berücksichtigt werden. Gezielte Forschung zur Entwicklung neuartiger und effektiver Konzepte für eine wirkungsvolle Reaktion auf Sicherheitsvorfälle, zum Beispiel durch automatisierte Umkonfiguration von Systemen oder Netzwerkeinstellungen, ist hierbei essentiell. (1-5 Jahre, EFRE)

Parallel zu den betrachteten Gruppen der Softwareentwickler, IT-Integratoren und Systemadministratoren ist auch die Gruppe der **Endanwender** zu beachten. Sie nutzen die entwickelten Systeme sowie IT-Sicherheitsmechanismen (in unterschiedlicher Intensität) und sind somit Konsumenten aller vorgenannten Gruppen. Aus einer Untersuchung des Verhaltens verschiedener Nutzergruppen lassen sich wiederum **Anforderungen an die Umsetzung von IT-Sicherheitsaspekten** im Bereich der Entwicklung, Implementierung und Administration ableiten, sowie Handlungsempfehlungen für Awareness-Maßnahmen definieren.

- **Nutzerstudien zu Fehlerquellen bei Endanwendern:**
  Endanwender sind die Nutzer der Komponenten, Software und Systemen. Bei dieser Nutzung machen sie Fehler, wie z. B. der sorglose Umgang mit Daten oder durch die Umgehung von implementierten Sicherheitsfunktionen, weil sie sich durch diese in ihrer Arbeit behindert sehen oder absichtlich Sabotageakte begehen. Eine Untersuchung dieser Fehler in den verschiedenen betrieblichen und privaten Anwendungsdomänen ist deshalb nötig, um Fehlerquellen zu identifizieren und durch die vorgenannten Maßnahmen Lösungen zu entwickeln. Dabei sollten alle relevanten Nutzergruppen (z. B. Industriearbeiter, Handwerker, Büroarbeiter und Entscheider) berücksichtigt werden. (5 Jahre, MIWF/EFRE)
- **Entscheidungsverhalten von Entscheidern über IT-Security:**
  Im industriellen Kontext wird die Entscheidung über Sicherheitsmaßnahmen nicht nur vom Endanwender selbst, sondern von der Organisations- und Entscheidungsstruktur im Unternehmen beeinflusst. Auch hier werden Fehler gemacht, die negative Auswirkung auf die IT-Sicherheit haben. Es muss daher untersucht werden, wer Entscheidungen trifft, warum sie getroffen und welche Kriterien in die Entscheidungsfindung einbezogen wurden. Eine Zusammenfassung dieser Fehlerquellen dient wiederum der Gesamtkonzeptionierung der oben vorgesehenen Maßnahmen und aggregiert die Ergebnisse für die Anwendung in der industriellen Praxis. (1-5 Jahre, MIWF/EFRE)

Bestehende Fördermaßnahmen

Die Bundesregierung hat im März 2015 das Forschungsrahmenprogramm für IT-Sicherheit unter dem Titel „Selbstbestimmt und sicher in der digitalen Welt“ veröffentlicht. Es bündelt erstmals ressortübergreifend die Aktivitäten zur IT-Sicherheitsforschung und fördert die Entwicklung sicherer, innovativer IT-Lösungen mit einem Fokus auf anwendungsorientierter (Grundlagen-)Forschung. Bis zum Jahr 2020 wird dieses Forschungsrahmenprogramm mit rund 180 Millionen Euro vom Bundesministerium für Bildung und Forschung (BMBF) gefördert. Dabei konzentriert sich das Programm auf vier große Forschungsschwerpunkte:

(1) Neue Hightech-Technologien für die IT-Sicherheit,
(2) sichere und vertrauenswürdige IKT-Systeme,
(3) Anwendungsfelder der IT-Sicherheit und
(4) Privatheit und Schutz der Daten.

Der *Faktor Mensch* wurde dabei nicht explizit berücksichtigt. Es bestehen aber natürlich Anknüpfungspunkte zu den in diesem Dokument skizzierten Forschungsherausforderungen.

Ergänzend zur Förderung des Bundes werden in anderen Bundesländern zahlreiche Schritte unternommen und Investitionen getätigt, um dem hohen Forschungsbedarf im Bereich IT-Sicherheit zu begegnen. Dort wurden verschiedene Initiativen gestartet; wie z. B. die von der hessischen Landesregierung ausgesprochenen „Bekenntnisse zu Security Valley“. So ist das in Darmstadt angesiedelte Kompetenzzentrum stark aufgestellt und bis Juni 2018 stehen dort 34 Millionen Euro für die Forschung zur Verfügung. Auch andere Bundesländer wie beispielsweise Bayern, Saarland, Berlin und Baden-Württemberg haben die Wichtigkeit der IT-Sicherheitsindustrie und IT-Sicherheitsforschung ebenfalls erkannt und investieren Millionenbeträge in die Forschung. In Baden-Württemberg soll beispielsweise „Karlsruhe bis 2020 zum führenden IT-Gründerstandort Deutschlands“ ausgebaut werden. Das Strategiepapier „IT-Sicherheit für NRW 4.0 – Gemeinsam ins digitale Zeitalter. Aber sicher“ liefert in Kapitel 4 einen Überblick zu laufenden Förderinitiativen in anderen Bundesländern. Diese Auswertung zu laufenden Förderinitiativen in anderen Bundesländern zeigt ganz deutlich, dass NRW geeignete Maßnahmen einleiten muss, um die vorhandenen Kompetenzen im Bereich IT-Sicherheit zu bündeln und auszubauen.

Auf der europäischen Ebene ist IT-Sicherheit im Rahmen von Horizon 2020 nicht mehr als eigenständiges Forschungsthema vertreten, das Thema wird im gesamten Programm nur randständig berücksichtigt. Im Kontext des Arbeitsprogramms zu „Sicheren Gesellschaften“ werden teilweise Themen der IT-Sicherheit betrachtet. Allerdings geht es vorrangig um die Umsetzung von Prototypen, Tests und Demonstratoren basierend auf existierenden Techniken. Der Forschungsanteil ist bei diesen Ausschreibungen oft marginal. Im Rahmen eines Public-Private-Partnerships zwischen der European Cyber Security Organisation (ECSO), die die Industrie, Anwender, Behörden, KMUs und Verbände im Bereich Cyber Security repräsentiert, und der EU wurde eine Zusammenarbeit im Bereich Cyber-Sicherheit vereinbart. Generelles Ziel dieser Partnerschaft ist es, die EU in der Erfüllung der Ziele von Horizon 2020, der European Cyber Security Strategy und der Digital Single Market Strategy zu unterstützen. Aspekte sind z. B. die Förderung von Marktentenwicklung, Jobs, Investitionen, Entwicklung, Piloten, vertrauenswürdige Lösungen, Dienste und Prozesse, Awareness, usw. im Bereich Cyber Security. Die EU unterstützt diese Aktivitäten im Zeitraum 2017 bis 2020 mit 450 Millionen Euro aus dem Horizon 2020 Programm.

Forschungsagenda für NRW

Im Folgenden skizzieren wir eine Forschungsagenda für das Bundesland NRW im Bereich IT-Sicherheit, welche die oben vorgestellten Aspekte zu *Human-Centered Systems Security* flankiert. Diese Forschungsagenda dient dem Ausbau der Förderung von Forschung zu sicheren und zuverlässigen IT-Systemen als prospektive Maßnahme. Dabei betrachten wir Zeithorizonte von 1-3 Jahren, etwa fünf Jahren und längerfristige Zeiträume von etwa zehn Jahren. Hierbei geben wir Empfehlungen ab, wie die identifizierten Forschungsthemen durch existierende Förderlinien (z. B. EFRE, DFG, BMBF, etc.) unterstützt werden können und identifizieren darüber hinaus Themen, die aufgrund ihrer Relevanz vom Land NRW selbst unterstützt werden sollten (vgl. Abbildung 4).

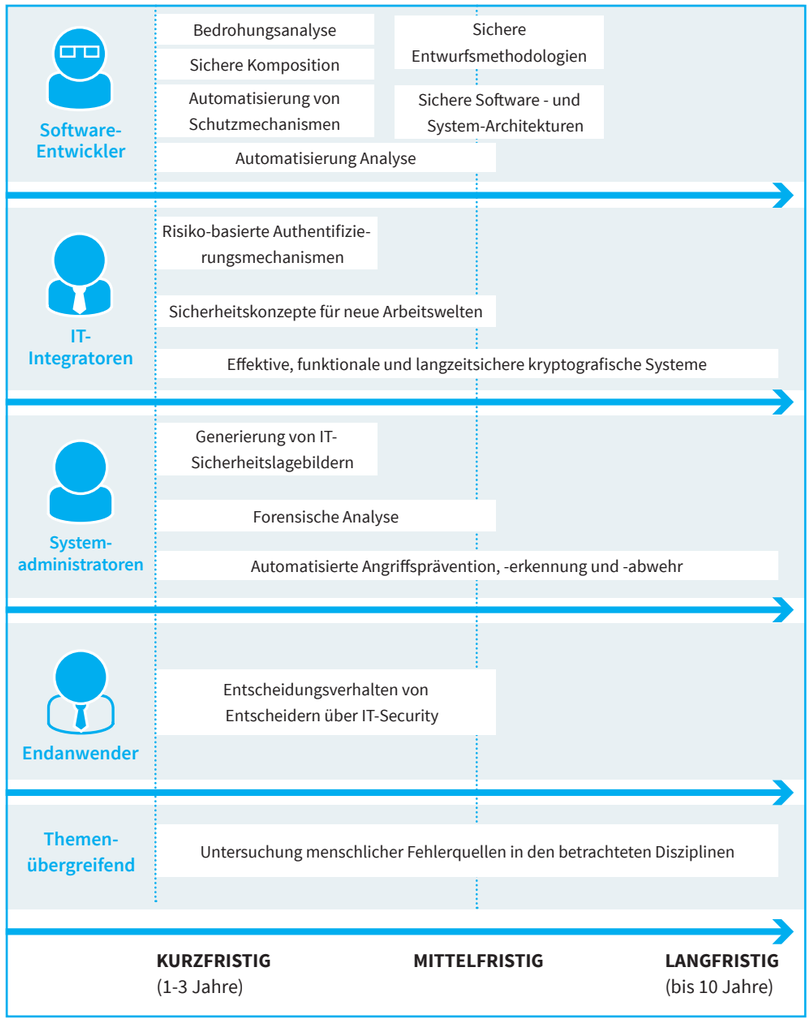


ABBILDUNG 4: FORSCHUNGSHERAUSFORDERUNGEN AUF KURZ-, MITTEL- UND LANGFRISTIGE SICHT

Kurzfristige Herausforderungen

Die vorangegangene Analyse verdeutlicht den generellen Bedarf an Untersuchungen zu menschlichen Fehlerquellen bei den verschiedenen Akteuren. Entsprechende Projekte sollten durchgeführt werden, um den Forschungsbedarf besser zu verstehen. Zur Unterstützung der Softwareentwickler sehen wir einen unmittelbaren Bedarf an der Erforschung

(1) sicherer Komposition von Softwareartefakten,
(2) Schutzmechanismen für Softwaresysteme, und
(3) der automatisierten Analyse von Softwarecodes und -modellen. Zur Unterstützung der IT-Integratoren liegt der Bedarf vor allem bei den
(4) Sicherheitskonzepten für neue Arbeitswelten, insbesondere im Kontext von mobilen Anwendungen. Administratoren sollten durch
(5) Methoden zur automatisierten Angriffsprävention, -erkennung und -abwehr sowie
(6) die verlässliche Generierung von IT-Sicherheitslagebildern unterstützt werden. Bei den Endanwendern besteht vor allem Bedarf an
(7) Nutzerstudien zu Fehlerquellen bei verschiedenen Nutzergruppen und
(8) Entscheidungsunterstützung für Manager in Unternehmen in NRW.

All diese Themen benötigen zum einen heute dringend praktikable Lösungen, zum anderen ist die Forschung aber bereits so weit gediehen, dass solche Lösungen in den kommenden Jahren zu erwarten sind.

Empfehlungen für initiale Modellprojekte
Um die o. g. Themen zeitnah umsetzen zu können, sollte das Land NRW mehrere Modellprojekte unterstützen. Diese Projekte haben zum einen das Ziel, die wichtigsten Akteure im Bundesland in Bezug auf die Forschungsagenda zu vernetzen und zu synchronisieren. Zum anderen sollen die Projekte offen und flexibel gehalten werden, um so zeitnah auf neue Forschungsbedarfe zu reagieren und die Beteiligung verschiedener Akteure zu gewährleisten. Konkret wären Modellprojekte zu den beiden Themengebieten *Automatisierte Softwareanalyse* sowie *Einfacher nutzbare Kryptografie* geeignet.

Automatisierte Softwareanalyse
Die Anzahl an kritischen Schwachstellen, die in Software gefunden wird, steigt jedes Jahr und eine punktuelle Bekämpfung dieses Problems scheint wenig aussichtsreich. Es ist zwingend nötig, Softwareentwickler dabei zu unterstützen, Schwachstellen zu finden und zu vermeiden. Es gibt bereits eine Vielzahl von technischen Ansätzen, die Software auf Sicherheitslücken untersuchen. Allerdings leiden diese unter schlechter Benutzbarkeit und vielen Fehlmeldungen, die ihre Nützlichkeit in der Praxis sehr einschränken. In diesem Projekt werden die Expertisen von verschiedenen Standorten in NRW kombiniert, um Techniken der automatischen Softwareanalyse, die auf den Menschen zugeschnitten sind, zu erforschen. Forscher an verschiedenen Standorten in NRW haben bereits Vorarbeiten in diesem Gebiet geleistet. Beispielsweise ist der *DREAM++ Decompiler* der erste auf den Menschen zugeschnittene Malware-Decompiler, also ein Analysetool für Schadsoftware. DREAM++ wurde auf der NDSS-Konferenz 2015 mit dem *Distinguished Paper Award* prämiert. Darüber hinaus wurden von Forschern aus NRW verschiedene Techniken zur Entdeckung von Softwareschwachstellen in PHP-Applikationen, Android-Apps oder Java-Applikationen entwickelt. Jedoch besteht noch viel Bedarf an automatisierten und benutzbaren Analysen von Softwareartefakten und -modellen.

Einfacher nutzbare Kryptografie
In den letzten Jahren veröffentlichte Sicherheitsschwachstellen wie BEAST, BREACH, CRIME, FREAK, Heartbleed und Logjam zeigen sehr deutlich, dass nicht nur (fachfremde) Endnutzer Probleme mit der Benutzbarkeit von Sicherheitstechnologien haben, sondern das Sicherheitsexperten und Entwickler ebenfalls Fehler machen. In den oben genannten Fällen haben Softwareentwickler bei der Umsetzung von sicherheitskritischen kryptographischen Protokollen Fehler begangen und damit gefährliche Schwachstellen in die Welt gesetzt. Der Bedarf an Unterstützung von Entwicklern und benutzbarer Kryptographie ist groß. Ein Verbundprojekt in diesem Bereich hätte das Potenzial mehrere wichtige Standorte für das Thema IT-Sicherheit miteinander zu vernetzen. In Bochum liegt ein Fokus der Forschung jeher auf der Kryptografie, aber auch an anderen Standorten gibt es Experten für kryptografische Systeme beispielsweise in Paderborn, wo dieser Fokus momentan weiter ausgebaut wird. Andere Forschungsgruppen aus NRW arbeiten an Methoden zur sicheren Softwareentwicklung mit Fokus auf der sicheren Nutzung kryptografischer Schnittstellen. In Bonn betreibt man Forschung zum *Faktor Mensch* und Usable Security. Die Zusammenführung der Expertise von verschiedenen Standorte würde es ermöglichen, die Benutzbarkeit kryptographischer Systeme zu erforschen und *benutzbare* Kryptographie zu entwickeln. Hierbei würden die Expertisen in den Bereichen Kryptographie, Software Entwicklung und Usable Security zu einer neuen regionalen Stärke im Bereich *Usable Cryptography* fusionieren.

Mittelfristige Herausforderungen

Die folgenden Themen sind nicht weniger wichtig, als die oben genannten Themen; auf Grund des aktuellen Stands der Wissenschaft bedarf es allerdings noch längerfristiger Forschung, um zu verwertbaren Ergebnissen zu führen. Hier steht zum einen die Erforschung einer systematischeren, reproduzierbareren Form der Bedrohungsanalyse im Vordergrund. Diese sollte vor allem mit Hilfe praktischer Anwendungsszenarien erforscht werden. Deshalb empfiehlt sich hier eine enge Kooperation mit der Wirtschaft speziell mit solchen Unternehmen, die in der Software- und/oder Systementwicklung tätig sind. Thematisch ähnlich gelagert ist der Bereich der systematischen Erforschung von menschlichen Fehlerquellen bei der Softwareentwicklung und - zur Vermeidung dieser - die Erforschung sicherer Entwurfsmethoden, sowie sicherer Software- und Systemarchitekturen. In diesem Bereich ist noch viel Grundlagenforschung vonnöten. Diese sollte jedoch in enger Abstimmung mit Partnerunternehmen erfolgen. Für die Erforschung von Sicherheitskonzepten für neue Arbeitswelten ist eine Kollaboration mit Unternehmen notwendig, die IT-Systeme benutzen bzw. diese in ihre Systeme integrieren. Mit Hilfe dieser Partner könnte dann auch die Erforschung von menschlichen Fehlerquellen bei der sicheren Integration bzw. Administration erforscht werden. Grundlagenforschung ist nötig, um effektive, funktionale, langfristig sichere kryptografische Systeme zu entwickeln. Die Erforschung der automatisierten Unterstützung für Incident Response/Recovery und forensische Analyse sollte gemeinsam mit Unternehmen der IT-Sicherheitsindustrie und mit Unternehmen, in denen IT-Systeme administriert und überwacht werden müssen, erfolgen. Hier sollte ein möglichst großer Teil der Zulieferkette abgedeckt werden.

Längerfristige Herausforderungen

Einige der identifizierten Themen erfordern langfristiger Forschung, da in großen Teilen noch die entsprechenden Grundlagen fehlen. Dies schließt beispielsweise die Themen

(1) effektive, reproduzierbare Bedrohungsanalyse,
(2) sichere Software- und System-Architekturen und
(3) automatisierte Angriffsprävention, -erkennung und -abwehr mit ein.

Diese Herausforderungen sollten bei der Umsetzung dieser Forschungsagenda berücksichtigt werden, um langfristige Bedrohungen ebenfalls abzudecken.