Deutscher Bundestag **Drucksache 18/4304**

18. Wahlperiode 12.03.2015

Unterrichtung

durch die Bundesregierung

Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit

Selbstbestimmt und sicher in der digitalen Welt 2015 - 2020

Inhaltsverzeichnis

Zugeleitet mit Schreiben des Bundesministeriums für Bildung und Forschung vom 11. März 2015.

1 Selbstbestimmt und sicher in der digitalen Welt

Informations- und Kommunikationstechnologien (IKT) durchdringen alle Bereiche unserer Gesellschaft. Ohne IKT gibt es keine modernen Krankenhäuser, keine zuverlässige Wasser- und Stromversorgung, kein zeitgemäßes Bankensystem, keinen wettbewerbsfähigen Automobil- oder Maschinenbau und erst recht keine Industrie 4.0. Der alltägliche Gebrauch von Smartphones, Tablets und vernetzten Fernsehern ist für die meisten Menschen eine Selbstverständlichkeit.

Umso wichtiger ist es, dass wir uns jederzeit auf sichere IKT verlassen können, die stabil funktioniert und IT-Angriffen standhält. Durch zunehmende Digitalisierung und Vernetzung sind heute lebenswichtige Infrastrukturen der Wirtschaft und des öffentlichen Lebens ver-letzbarer denn je. Allein die Deutsche Telekom registriert täglich bis zu einer Million Angriffe auf ihr Netz. Unternehmen und Staaten sind einer wachsenden Gefahr durch Cyberattacken ausgesetzt. Wenn beispielsweise nach einem Hacker-Angriff die Stromversorgung flächendeckend ausfällt, sind auch Verkehrsleitsysteme, Krankenhäuser, Logistikketten oder die Wasserversorgung massiv betroffen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beobachtet jeden Tag fünf gezielte Spionageangriffe auf die Bundesverwaltung. Rund 30.000 Zugriffsversuche aus dem Regierungsnetz auf Webseiten, die böswillig manipuliert wurden, werden jeden Monat verhindert. 2013 stieg die weltweite Zahl der Angriffe auf die IT-Sicherheit von Unternehmen im Vergleich zum Vorjahr um 48 Prozent auf 42,8 Millionen. Dies entspricht 117.330 Angriffen pro Tag. Allein die wirtschaftlichen Schäden werden für 2013 weltweit auf bis zu 575 Milliarden Dollar geschätzt.

Darüber hinaus sind die Bürgerinnen und Bürger auch in ihrem Privatleben betroffen. Beim Umgang mit ihren persönlichen Daten geraten sie immer wieder in einen Zwiespalt. Einerseits wollen und müssen sie Daten preisgeben, um Produkte und Dienste der Cyberwelt nutzen zu können. Dadurch entstehen aber andererseits immer umfassendere Profile, die miteinander vernetzt, gehandelt und ausgewertet werden können. Alleine Facebook hat über 1,3 Milliarden Nutzer. Sie teilen alle 20 Minuten rund eine Million Links und tauschen etwa drei Millionen Nachrichten aus. Facebook sammelt dabei geschätzt etwa 500 Terabyte (TB) Daten täglich. Zum Vergleich: Die gesamte US-Library of Congress umfasst lediglich 20 TB. Da kaum jemand weiß, wie seine Daten mit anderen Informationen verbunden werden, wer sie nutzt und was weiter mit ihnen passiert, sind die meisten Bürgerinnen und Bürger der Big-Data-Welt weitestgehend ausgeliefert und in ihrem informationellen Selbstbestimmungsrecht deutlich eingeschränkt.

Wir brauchen daher IT-Sicherheit. Weil aber neue Schutzmechanismen meist sofort neue Angriffsmethoden zur Folge haben, ist IT-Sicherheit in erster Linie als vorausschauender Prozess zu verstehen. Aufgabe der Forschung ist es, innovative Schutzmaßnahmen und belastbare Lösungen zu entwickeln, die auch in Zukunft noch funktionieren und mit denen sich der Teufelskreis zwischen Angriff und Reaktion durchbrechen lässt.

Die IT-Sicherheitsforschung hat dabei auch immer die Bedarfe der Bürgerinnen und Bürger, der Unternehmen und der öffentlichen Einrichtungen im Blick. Damit IT-Sicherheit für alle zur Selbstverständlichkeit wird, brauchen wir Lösungsansätze, bei denen die praktische Anwendung von Anfang an mitgedacht wird. Dies geht nur, wenn alle Beteiligten einen kontinuierlichen Dialog miteinander führen. Technologische Ansätze und Lösungen zu IT-Sicherheitsstandards sind ebenso gefordert wie ethische, juristische oder ökonomische Forschungsbeiträge.

IT-Sicherheit ist ein wichtiges Element der staatlichen Daseinsvorsorge. Dabei steht der Staat in einem ständigen Spannungsfeld – zwischen dem Anspruch der Bürgerinnen und Bürger auf Schutz ihrer Daten einerseits und den Sicherheitsbedürfnissen unserer Gesellschaft andererseits.

Das Vertrauen der Nutzerinnen und Nutzer in die IT-Infrastruktur setzt voraus, dass der Staat das Mögliche tut, um die IT-Sicherheit zu garantieren. Wirksame IT-Sicherheit bedeutet deshalb vor allem, dass die IT-Infrastruktur vor dem Zugriff unberechtigter Dritter geschützt wird. Recht und Gesetz gelten in der realen gleichermaßen wie in der virtuellen Welt. Das Netz ist kein rechtsfreier Raum, der vor der Strafverfolgung und den Sicherheitsbehörden schützt.

Die Bundesregierung greift die Herausforderungen der Sicherung von IT-Systemen und des Schutzes der Daten als zentrale Forschungsthemen auf. Mit dem Forschungsrahmenprogramm „Selbstbestimmt und sicher in der digitalen Welt“ investiert die Bundesregierung in die vorausschauende Gestaltung technischer Systeme und die Rahmenbedingungen ihrer Nutzung, um vor Cyber-Angriffen zu schützen und das Recht des Bürgers auf informationelle Selbstbestimmung zu wahren. Das Programm richtet sich an Hochschulen und Forschungseinrichtungen sowie an Unternehmen und Anwender und bündelt die Forschungsaktivitäten der Bundesregierung zur IT-Sicherheit. Das Forschungsrahmenprogramm setzt maßgebliche Ziele der „Hightech-Strategie 2020 für

Deutschland“ um, in der innovative Lösungen für die digitale Wirtschaft und Gesellschaft als prioritäre Zukunftsaufgabe verankert sind. Weil sich die Anforderungen der IT-Sicherheit sehr schnell ändern, ist das Forschungsrahmenprogramm als flexibler Rahmen konzipiert, der an veränderte Voraussetzungen und neue Herausforderungen angepasst werden kann.

Mit dem Forschungsrahmenprogramm greift die Bundesregierung auch wesentliche Querschnittsthemen der Digitalen Agenda 2014-2017 auf: „Ohne Vertrauen in die Sicherheit und Integrität der digitalen Welt wird es nicht gelingen, die wirtschaftlichen und gesellschaftlichen Potenziale des digitalen Wandels zu erschließen“.

Digitale Technologien zur IT-Sicherheit sind ein dynamisches Innovationsfeld mit einem enormen Wertschöpfungspotenzial. Mit dem Forschungsrahmenprogramm „Selbstbestimmt und sicher in der digitalen Welt“ eröffnet sich die Chance, Deutschland zu einem Leitanbieter für IT-Sicherheitslösungen zu machen. Die Voraussetzungen hierfür sind sehr gut. Deutsch-land ist international führend im Datenschutzrecht und kann mit seiner hervorragenden Forschungslandschaft deutliche Akzente setzen. Da die Datenflüsse, insbesondere im Internet, nicht an Landesgrenzen Halt machen, treibt die Bundesregierung auch den Entwicklungsprozess auf europäischer Ebene voran.

2 Ziele und Leitlinien

Die im Forschungsrahmenprogramm aufgezeigten Forschungsthemen orientieren sich an zehn Zielen und Leitlinien:

- **IT-Sicherheit ist Daseinsvorsorge**

  Der rasante technologische Fortschritt der Informations- und Kommunikationstechnologien sowie das sich wandelnde Nutzerverhalten führen zu ständig neuen Bedrohungslagen. IT-Sicherheit ist daher eine langfristig angelegte Aufgabe, um bereits heute Lösungen für die Herausforderungen von morgen bereit zu stellen.

- **IT-Sicherheit schafft Vertrauen**

  Vertrauen und Akzeptanz sind unabdingbare Voraussetzung für die Nutzung der vielfältigen Chancen, die die Digitalisierung von Gesellschaft und Wirtschaft bietet. Nachweisbar sichere, verlässliche und nutzerfreundliche IT-Produkte und Dienstleistungen müssen die Grundlage für dieses Vertrauen schaffen.

- **IT-Sicherheit schützt die Privatsphäre der Bürgerinnen und Bürger**

  Bürgerinnen und Bürger müssen in die Lage versetzt werden, ihr Recht auf digitale Selbstbestimmung wahrzunehmen und selbst zu entscheiden, welche Daten über sie erhoben und wie diese Daten genutzt werden dürfen. Bürgerinnen und Bürger haben in der digitalen Welt ein „Recht auf Vergessen“.

- **IT-Sicherheit stärkt den Standort Deutschland**

  Die Wertschöpfungsketten nahezu aller Wirtschaftsbereiche wie bei Industrie 4.0 verändern sich mit dem Fortschreiten der Digitalisierung. IT-Sicherheit schützt die in diesem Kontext entstehenden neuen Geschäftsmodelle und fördert somit das wirtschaftliche Wachstum. Parallel hierzu baut die IT-Sicherheitswirtschaft ihre internationale Position mit Hilfe innovativer Technologien und Verfahren aus.

- **IT-Sicherheit gewährleistet den Betrieb kritischer Infrastrukturen**

  Der Ausfall einer oder mehrerer kritischer Infrastrukturen hat gravierende Auswirkungen für das staatliche Gemeinwesen und die Bevölkerung in Deutschland. IT-Sicherheit soll den Schutz von kritischen Infrastrukturen erhöhen, um deren Verfügbarkeit sicherzustellen und Kettenreaktionen zu verhindern.

- **IT-Sicherheit orientiert sich an den Bedürfnissen der Nutzerinnen und Nutzer**

  IT-Sicherheitslösungen werden nur eingesetzt, wenn sie sich im täglichen Einsatz bewähren. IT-Sicherheitslösungen müssen das erforderliche Maß an Schutz und Datentransparenz gewährleisten und zugleich für den Anwender einfach nutzbar und leicht verständlich sein.

- **IT-Sicherheit ist messbar**

  Die Messbarkeit von IT-Sicherheit ermöglicht die Bewertung gesellschaftlicher und technischer IT-Sicherheitsrisiken sowie der entsprechenden Lösungsansätze. IT-Sicherheitsforschung entwickelt die hierfür notwendigen Parameter und Methoden.

- **IT-Sicherheit ist interdisziplinär**

  IT-Sicherheit erfordert vernetztes Denken und Handeln über Disziplingrenzen und Prozessketten hinweg – von der Forschung und Entwicklung bis hin zur Anwendung von IT-Sicherheitslösungen. Daher werden gesellschaftliche, rechtliche und wirtschaftliche Fragestellungen von Anfang an mit berücksichtigt.

- **IT-Sicherheit ist europäisch**

  Die europäischen Industriegesellschaften sind ohne leistungsfähige und sichere Informations- und Kommunikationssysteme kaum existenzfähig. Deutschland wird gemeinsam mit seinen europäischen Partnern eigene technologische Kernkompetenzen in der IT-Sicherheit ausbauen, um die Abhängigkeit von außereuropäischen Akteuren zu verringern.

- **IT-Sicherheit ist international**

  Die Herausforderungen der digitalen Welt können weder im nationalen noch im europäischen Alleingang gelöst werden. IT-Sicherheit erfordert internationale Lösungen, die die erforderlichen Rechtsgrundlagen und Standards liefern. Nur so können neue IT-Sicherheitslösungen auch weltweit Wirkung zeigen.

3 Forschungsschwerpunkte für die Zukunft

Basierend auf den genannten Herausforderungen und Zielen konzentriert sich das Forschungsrahmenprogramm auf vier große Forschungsschwerpunkte, in denen sowohl technische als auch wirtschaftliche und gesellschaftliche Aspekte der IT-Sicherheit zum Tragen kommen.

- **Hightech für die IT-Sicherheit**

  Im ersten Forschungsschwerpunkt stehen die technischen Voraussetzungen für eine zukunftsfähige und sichere IKT im Zentrum, wie zum Beispiel hardwarebasierte Sicherheitsmodule, Verfahren für effiziente Kryptografie und digitales Identitätsmanagement sowie Technologien zur Quantenkommunikation.

- **Sichere und vertrauenswürdige IKT-Systeme**

  Da IT-Sicherheit nicht nur einzelne Elemente betrifft, sondern in der Gesamtheit funktionieren muss, liegt der zweite Forschungsschwerpunkt auf sicheren und vertrauenswürdigen IKT-Systemen. Dazu gehören eine transparente und benutzerfreundliche Gestaltung der IT-Sicherheit, ein sicherer Schutz vor Internet-Angriffen auch in heterogenen Systemstrukturen sowie ein verstärkter Wissens- und Produktschutz.

- **IT-Sicherheit in Anwendungsfeldern**

  Die spezifischen Anforderungen von besonders komplexen und bedeutsamen Anwendungsfeldern wie vernetzte Produktionsanlagen, kritische Infrastrukturen, Medizin und Verkehr stehen im dritten Forschungsschwerpunkt im Fokus.

- **Privatheit und der Schutz von Daten**

  Die Privatheit und der Schutz der persönlichen Daten sind elementare Voraussetzungen für ein selbstbestimmtes Leben jedes Bürgers und jeder Bürgerin und bilden damit das Thema des vierten Forschungsfeldes. Hier werden unter anderem Aspekte der Netzkultur und die Herausforderungen von Big Data untersucht.

3.1 Hightech für die IT-Sicherheit

Um die Informations- und Kommunikationstechnologien für die Anforderungen der Zukunft fit zu machen, sind innovative und sichere Werkzeuge und Komponenten eine wesentliche Grundvoraussetzung.

3.1.1 Hardwarebasierte Sicherheitsanker

Sicherheitsanker sind technische Bausteine, die das Auslesen und Verändern besonders geschützter Bereiche verhindern. Das können z.B. spezielle Sicherheits-Chips sein. Solche Anker können zur Speicherung sensibler Daten wie kryptografischer Schlüssel oder Zertifikate dienen, sind aber auch als Ausgangspunkt für integre Prozesse geeignet, z.B. das Hochfahren eines Systems. Vertrauenswürdige Firmware bildet in Verbindung mit hardwarebasierten Sicherheitsankern die Basis für sicherheitskritische Plattformen und Anwendungen.

Nahezu täglich gibt es Berichte über neue Analyse- und Angriffstechnologien. Entsprechend gibt es auch immer mehr Angriffsmöglichkeiten auf Hardware-Bausteine. Aufgabe der Forschung ist die Entwicklung von Sicherheitsankern für sicherheitskritische Systeme und Anwendungen, die sowohl langfristig Angriffen widerstehen als auch effizient und kostengünstig in IT-Systeme integrierbar sind.

Forschungsthemen sind insbesondere:

- Manipulationsresistente hardwarebasierte oder hardwarenahe Bausteine, die in Verbindung mit nachprüfbar vertrauenswürdiger Firmware sowohl für eingebettete und mobile Systeme als auch für Serversysteme geeignet sind;
- herstellerübergreifende Aggregation unterschiedlicher Sicherheitsanker;
- Validierung der Sicherheit von Sicherheitsankern;
- Verhinderung und Erkennung von Hardware-Manipulationen.

3.1.2 Digitales Identitätsmanagement

Vertrauen im Internet entsteht dann, wenn Nutzer sich auf sichere, eindeutig zurechenbare Identitäten von Personen verlassen können. Auch bei Objekten, beispielsweise im Internet der Dinge, ist es wichtig, dass diese Identitäten nicht einfach umgangen, gefälscht oder gestohlen werden können. Die Folgen von Identitätsdiebstahl können gravierend sein – sie reichen von Cybermobbing über betrügerische Kauf- und Verkaufstransaktionen bis hin zur Wirtschaftsspionage. Mit der Verbreitung des Internet nimmt die Zahl der Fälle von Identitätsdiebstahl im Netz jedoch stetig zu. Im Jahr 2014 wurden im Rahmen der Analyse von Bot-Netzen rund 16 Millionen gestohlene digitale Identitäten entdeckt.

Erforderlich sind Vertrauensinfrastrukturen mit Identitäten, die von den Nutzerinnen und Nutzern selbstbestimmt und sicher verwaltet werden können und auch im „Internet der Dinge“ und im Umfeld von Industrie 4.0 zum Schutz beitragen.

Forschungsthemen sind insbesondere:

- Nutzerzentriertes Identitätsmanagement, das die einzelnen Anwender und deren Privatsphäre schützt;
- Weiterentwicklung des Identitätsmanagements von bestehenden Individuallösungen zu standardisierten, übergreifenden und breit einsetzbaren Lösungen;
- Kombination verschiedener Formen von digitalen Identitäten für mehr Sicherheit;
- effiziente Implementierung von digitalen Identitäten für Objekte, um so das Internet der Dinge sicher gestalten zu können.

3.1.3 Langfristig sichere und effiziente Kryptografie

Bezahlen im Web, das Verschicken von privaten Nachrichten, das Einloggen bei Facebook – sicher wird all dies nur mit vertrauenswürdigen kryptografischen Verfahren.

Die derzeit am weitesten verbreiteten kryptografischen Verfahren basieren auf komplexen Algorithmen, die von herkömmlichen Computern nicht in einer überschaubaren Zeit zu knacken sind.

Quantencomputer dagegen sind in der Lage, in überlagerten Zuständen zu rechnen und würden damit große Teile der heute verwendeten kryptografischen Verfahren unbrauchbar machen. Theoretische Ansätze für alternative Verfahren gibt es bereits. Von einem Praxiseinsatz sind Quantencomputer-resistente Algorithmen aber noch weit entfernt.

Benötigt werden für die Praxis geeignete kryptografische Verfahren, die heute sicher sind und auch sicher bleiben, wenn es leistungsfähige Quantencomputer gibt.

Viele Anwendungen erfordern kryptografische Sicherungen für einzelne, manchmal sehr kleine und kostengünstige Bauteile, z.B. Sensoren. Diese verfügen aber oft nur über geringe Speicher- und Rechenressourcen, so dass sich gegenwärtige kryptografische Verfahren nur sehr eingeschränkt implementieren lassen.

Forschungsthemen sind insbesondere:

- Quantencomputer-resistente Algorithmen, die nachweisbar sicher und effizient in derzeit gängige Anwendungen implementiert werden können;
- Verfahren, die eine Verarbeitung verschlüsselter Daten erlauben und nachweisbar sicher und effizient in Anwendungen implementiert werden können;
- praktikable Verfahren für sichere Kommunikation bei gegenseitigem Misstrauen;
- „leichtgewichtige“, aber dennoch beweisbar sichere kryptografische Verfahren, die insbesondere in Systemen mit begrenzten Ressourcen eingesetzt werden können.

3.1.4 Quantenkommunikation

Die Quantenkommunikation ermöglicht es, sensible Informationen wie zum Beispiel kryptografische Schlüssel oder die Zugangsdaten zu Bankkonten so zu übertragen, dass deren Vertraulichkeit gewahrt bleibt. Jedes Mithören des Informationsaustausches durch einen Angreifer kann vom Empfänger bemerkt werden.

Bislang sind Verbindungen auf Basis der Quantenkommunikation nur über Distanzen bis zu 150 km möglich. Will man jedoch Informationen über weitere Entfernungen übertragen, muss der unvermeidbaren Abschwächung des übermittelten Signals entgegengewirkt werden.

Ein klassischer Wiederholverstärker empfängt das Signal, verstärkt es und schickt es weiter. In der Quantenmechanik impliziert jedoch jede Messung eine Veränderung der Photonen. Dieses grundlegende Prinzip, das auch die Quantenkommunikation abhörsicher macht, verhindert somit eine Verstärkung des Signals im klassischen Sinne. „Verstärker" in der Quantenkommunikation, sogenannte Quanten-Repeater, arbeiten dagegen mit quantenmechanisch verschränkten Photonenpaaren.

Aufgabe der Forschung ist es, die Leistungsfähigkeit von Quanten-Repeatern zu erhöhen, um die Quantenkommunikation auch über weite Entfernungen zu ermöglichen.

Forschungsthemen sind insbesondere:

- Verbesserung der Leistungsfähigkeit von Quanten-Repeatern durch längere Speicherzeiten, höhere Effizienz und bessere Signalquellen;
- Weiterentwicklung von bereits in Labortests erfolgreichen Konzepten einzelner Technologien und deren Kombination bis hin zur Anwendungsreife;
- theoretische Grundlagen zur Informationsübertragung in Quanten-Netzwerken, insbesondere die Entwicklung optimaler Übertragungs- und Korrekturverfahren;
- Analyse von zielgerichteten Störungen und Seitenkanalangriffen gegen die neuen Technologien und die Entwicklung von wirksamen Gegenmaßnahmen gegen solche Angriffe.

3.1.5 Neue Sicherheitstechnologien

IT-Sicherheit ist ein fortlaufendes Wettrennen mit den Angreifern. Jede neue technologische Entwicklung sorgt für neue Angriffsmöglichkeiten. Wer auf einem heute sicheren Zustand verharrt, wird morgen für Cyber-Kriminelle ein leichtes Opfer. Denn auch Cyber-Kriminelle machen sich den Fortschritt zunutze und agieren heutzutage schneller und professioneller denn je. Die neuen Kommunikationswege werden dabei auch genutzt, sich der Strafverfolgung zu entziehen.

Um neue Angriffsszenarien gleich im Vorfeld auszuschalten und die Aufklärung von IT-Sicherheitsvorfällen zu erleichtern, werden im Bereich der neuen Sicherheitstechnologien diese Entwicklungen kurzfristig aufgegriffen und Projekte gefördert, die neue technologische Ansätze erforschen und entwickeln.

Ein erstes Thema für die neuen IT-Sicherheitstechnologien ist die Erforschung neuer datenschutzkonformer Methoden für die Erkennung und Aufklärung von IT-Sicherheitsvorfällen. Sie eröffnen Möglichkeiten, Anomalien und Auffälligkeiten im Zusammenhang mit IT-Systemen – auch in Echtzeit – datenschutzkonform zu erkennen und festzustellen, ob ein technisch oder rechtlich erheblicher Vorfall vorliegt. Nach Eintreten eines Vorfalls können mittels forensischer Methoden digitale Spuren erfasst, analysiert und ausgewertet werden. Schnelle und effiziente Entscheidungen können dazu beitragen, den Schaden gering zu halten. Weitere, derzeit noch nicht absehbare Forschungsthemen zu neuen Sicherheitstechnologien werden kurzfristig aufgegriffen.

3.2 Sichere und vertrauenswürdige IKT-Systeme

Das Vertrauen sowohl der Bürgerinnen und Bürger, Verbraucherinnen und Verbraucher als auch der Unternehmen in die Sicherheit der IKT ist angesichts von kriminellen Angriffen, Tracking und Profiling seitens IT-Unternehmen, Cyber- und digitaler Wirtschaftsspionage stark gesunken. Vier von fünf Internetnutzerinnen und -nutzern halten ihre Daten nicht mehr für sicher.

Wirksame Maßnahmen gegen Cyberkriminalität, Sabotage, Spionage und sonstige IT-Störfälle sowie der faire und vertrauensvolle Umgang mit Daten und Informationen können Vertrauen schaffen und sind daher Kernanliegen von sicherer und vertrauenswürdiger Informationsverarbeitung. Ein selbstbestimmter und eigenverantwortlicher Umgang der Nutzerinnen und Nutzer mit IKT-Systemen erfordert die Möglichkeit, die Entscheidungsfreiheit zur Produktauswahl, Konfiguration und Anwendung von IKT-Systemen und die vollständige Kontrolle über die IKT-Systeme zu besitzen.

Dabei geht es darum, nicht nur einzelne Komponenten oder Anwendungen sicher zu machen, sondern komplexe Systeme zu schützen. Sicherheit ist dabei im Sinne von „Security by Design" bereits bei der Entwicklung von IT-Systemen mitzudenken. Vertrauenswürdige, aber auch für Anwender praktikable Lösungen für den Schutz

der Privatsphäre, für die Absicherung mobiler Geräte und Geschäftsprozesse sowie für den Schutz vernetzter Produktions- und Automatisierungsanlagen sind ein elementarer Beitrag für den IKT-Standort Deutschland.

3.2.1 Transparenz und Benutzerfreundlichkeit

Bei der Entwicklung von IT-Sicherheitslösungen steht heute meistens die Abwehr von Angriffen im Vordergrund. Aspekte der Transparenz, Bedienbarkeit und Verständlichkeit finden nur wenig Beachtung. IT-Sicherheitslösungen, die zu kompliziert oder nicht transparent sind, werden jedoch oft gemieden, umgangen oder versehentlich fehlgenutzt.

Alle gängigen E-Mail-Clients und Messaging-Applikationen unterstützen zum Beispiel eine Ende-zu-Ende-Verschlüsselung – nur ist sie nicht Standard, sondern muss erst nachträglich eingeschaltet werden. Dass die meisten Anwender Standardeinstellungen nicht ändern, ist einer der Hauptgründe für die mangelnde Verbreitung einer sicheren E-Mail-Kommunikation.

Gefordert sind IT-Sicherheitslösungen, die das erforderliche Maß an IT-Sicherheit gewährleisten und dabei so transparent sind, dass die Nutzerinnen und Nutzer sie intuitiv und effizient bedienen können. Darüber hinaus müssen die Lösungen auch in dem Sinne transparent sein, dass sie durch Dritte, beispielsweise durch Zertifizierungsstellen, vollständig überprüft werden können.

Forschungsthemen sind insbesondere:

- Verständliche und intuitiv benutzbare Technologien (wie z. B. Suchmaschinen) unter Berücksichtigung von Transparenz, Risikoeinschätzung und Kontrolle für Nutzerinnen und Nutzer;
- Technologien, mit denen sich die Auswirkungen menschlichen Fehlverhaltens, von Ereignissen höherer Gewalt oder von zielgerichteten Angriffen minimieren lassen;
- Mechanismen für eine sichere und vertrauenswürdige Kontrolle von eigenen, persönlichen Daten, die im Internet gespeichert sind;
- benutzerfreundliche Kontroll- und Vertrauensinfrastrukturen als Grundlage für einen wirksamen Schutz der eigenen Daten, insbesondere hinsichtlich einer Ende-zu-Ende-Verschlüsselung.

3.2.2 Schutz vor Internet-Angriffen

Die offene Struktur und die Anonymität des Internets tragen dazu bei, dass die Zahl der Internet-Angriffe stetig zunimmt. Angriffswerkzeuge und -methoden sind einfach und kostengünstig verfügbar. Die Möglichkeiten, vertrauliche Informationen zu erlangen, Sabotageakte durchzuführen und mit kriminellen Handlungen Geld zu verdienen sind vielfältig. Schwachstellen, Schadsoftware sowie illegal erlangte Daten werden oftmals auf einem globalen Markt gehandelt („Malware-as-a-Service“).

Zielgerichtete Angriffe dringen unter anderem in Netzwerke ein, um individuelle Malware zu installieren, die lange Zeit unentdeckt bleiben kann. Der eigentliche Angriff findet oftmals erst Wochen oder Monate später statt.

Um hier gegensteuern zu können, werden Analysemethoden zur frühzeitigen Erkennung und zur Erstellung eines IT-Sicherheitslagebildes sowie Warnsysteme, Strategien und Methoden zur Abwehr und Verfolgung von Angriffen über das Internet benötigt.

Forschungsthemen sind insbesondere:

- Übergreifende Konzepte und Technologien, die weniger angreifbar und gegen Internet-Angriffe besser geschützt sind;
- effiziente Analysemethoden, mit denen anhand von Anomalien Angriffe in Echtzeit und mit hoher Zuverlässigkeit aufgespürt und analysiert sowie zu einem ganzheitlichen IT-Sicherheitslagebild aggregiert werden können;
- Modelle, Bewertungs- und Prognoseverfahren zur Ableitung von Präventionsmaßnahmen und Handlungsbedarfen;
- Vermeidung, frühzeitige Erkennung und Abwehr von zielgerichteten, mehrstufigen Angriffen und Schadsoftware auch in mobilen Geräten;

- Next Generation Intrusion Detection Systeme, die über die Erkennung von Anomalien im Netzwerkverkehr hinausgehen und frühzeitig neue Bedrohungen wie zum Beispiel Hardware-Trojaner und moderne Schadsoftware erkennen können.

3.2.3 Nachweisbare IT-Sicherheit

Bürgerinnen und Bürger, Unternehmen und öffentliche Verwaltung benötigen die Gewissheit, dass ihre Daten, ihr Wissen und ihre Produkte auch im digitalen Zeitalter geschützt sind. Vertrauen entsteht dann, wenn die Sicherheit von IKT-Systemen nachweisbar und somit für die Nutzerinnen und Nutzer transparent und messbar ist.

Konzeptionelle Mängel oder Implementierungsfehler in Hard- oder Software können zu schwerwiegenden IT-Sicherheitsvorfällen führen. Die Sicherheitslücke „Heartbleed“ in dem weit verbreiteten Sicherheitsprotokoll OpenSSL, die über zwei Jahre unentdeckt blieb, ist dafür das bisher gravierendste Beispiel. Ein kleiner Fehler traf hunderttausende Webseiten und potenziell hunderte Millionen Nutzerinnen und Nutzer.

Künftig sollen alle Beteiligten vom Entwickler über den Integrator bis zum Anwender in die Lage versetzt werden, IKT-Systeme hinsichtlich potenzieller Sicherheitslücken bewerten zu können. Aufgabe ist dabei, IT-Sicherheit als wesentlichen Qualitätsindikator bereits bei der Entwicklung und Herstellung von IT-Produkten durchgängig zu berücksichtigen. Von besonderem Interesse sind dabei Geschäftsmodelle für IT-Sicherheitslösungen auf der Basis offener Standards und freier Software.

Forschungsthemen sind insbesondere:

- Berücksichtigung der IT-Sicherheit und Privatheit in der Entwicklung und Herstellung von Hardware- und Software-Produkten, Systemen und Dienstleistungen („Security and Privacy by Design“);
- statische und dynamische Codeanalyse von Software, um höchstmögliche Fehlerfreiheit und Wirksamkeit zu gewährleisten;
- Qualitätsbewertung der IT-Sicherheit von Hard- und Software sowie der Analysewerkzeuge;
- Quantifizierung der Kostenvorteile sicherer IT-Produkte aus betriebswirtschaftlicher Sicht;
- effiziente Zertifizierung der Sicherheit von IT-Produkten (Hard- und Software) und Systemen unter Berücksichtigung immer kürzer werdender Produktzyklen und geringer Kostenbudgets.

3.2.4 IT-Sicherheit in heterogenen Systemstrukturen

Vom Internet der Dinge, der damit verbundenen autonomen Vernetzung bis hin zu service-orientierten Plattformen – IKT-Systeme setzen sich heutzutage aus einer Vielzahl von Komponenten über Länder- und Branchengrenzen hinweg zusammen. Mit dem Einsatz von Produkten unbekannter Herkunft steigt jedoch das Risiko von Sicherheitslücken oder auch versteckten Schadfunktionen, die sich zum Beispiel in der Steuerungssoftware oder im Mikrochip verbergen können. Dadurch können auch von IT-Produkten wie Druckern oder IP-Telefonen erhebliche Gefahren ausgehen.

Es ist sicherzustellen, dass auch in komplexen, heterogenen IKT-Systemen und in nicht-vertrauenswürdigen Umgebungen das erforderliche IT-Sicherheitsniveau langfristig und nachhaltig gewährleistet werden kann.

Forschungsthemen sind insbesondere:

- Modellierung und Bewertung der IT-Sicherheit von Hard- und Software, von (mobilen) Geräten und vom Gesamtsystem;
- Modelle, Architekturen und Mechanismen, welche das erforderliche IT-Sicherheitsniveau eines Gesamtsystems auch dann gewährleisten, wenn einzelne Komponenten nicht vertrauenswürdig sind (z. B. bei Anwendungen auf unsicheren Plattformen oder Betriebssystemen);
- Schutz besonders kritischer Kommunikationskanäle und Komponenten, z. B. in software-gesteuerten Strukturen wie Software-Definierten-Netzen (SDN) oder in neuen Mobilfunkprotokollen;
- physischer – und gleichzeitig praktikabler und kostengünstiger – Zugriffsschutz von IKT-Systemen und besonders zu schützenden Komponenten;
- nachweisbare Einhaltung des erforderlichen IT-Sicherheitsniveaus in Lieferketten, bei der Integration in bestehende Systeme und bei Austausch oder Update einzelner Produkte oder Komponenten.

3.2.5 Wissens- und Produktschutz

In Deutschland entsteht durch Know-how-Verlust und die unlautere Nachahmung von Produkten ein enormer wirtschaftlicher Schaden. Allein im Jahr 2013 lag der Verlust durch Produkt- und Markenpiraterie im deutschen Maschinen- und Anlagenbau bei 7,9 Milliarden Euro. Und die Tendenz ist steigend.

Auf Chips beispielsweise finden sich Programmcodes ebenso wie Software zur Steuerung von Prozessen – Informationen, die meist mit verhältnismäßig geringem Aufwand ausgelesen werden können. Vernetzte Systeme von der Telekommunikationsanlage, der Produktionsanlage bis zum Stromnetz können durch manipulierte Chips angreifbar werden. Letztendlich kann durch den Einsatz eines manipulierten oder minderwertigen Plagiats sowohl die IT-Sicherheit als auch die Zuverlässigkeit von Infrastrukturen, Netzen und Anwendungen gefährdet werden. Technisches Wissen und Produkte sollen daher jederzeit geschützt werden können. Andererseits dürfen Wissens- und Produktschutz nicht dazu führen, dass Eigentümern der selbstbestimmte Einsatz ihrer Produkte verwehrt wird.

Forschungsthemen sind insbesondere:

- Praktikable und nachweisbar wirksame Verfahren des Softwareschutzes;
- Verhinderung von Reverse Engineering von Hard- und Softwareprodukten;
- Kombination und Integration unterschiedlicher Verfahren und Maßnahmen für den Wissens- und Produktschutz, z. B. mit verschiedenen Wirkungsorten und –graden.

3.3 IT-Sicherheit in Anwendungsfeldern

Nahezu jedes dritte Unternehmen in Deutschland erlebte in den vergangenen zwei Jahren Angriffe auf seine IKT-Systeme. 58 Prozent der betroffenen Unternehmen geben an, dass die Angriffe „vor Ort“ erfolgten und zum Beispiel gezielt Daten gestohlen oder Schadprogramme per USB-Stick eingeschleust wurden. 30 Prozent der Unternehmen berichten, dass die Angriffe über das Internet erfolgt sind.

Sowohl bestehende als auch neue Geschäftsmodelle wie „Industrie 4.0“, „Smart Home“ oder „Smart Services“ – das Verschmelzen von Produkten und internetbasierten Diensten – sind nur erfolgreich, wenn sich sowohl Bürgerinnen und Bürger als auch Unternehmen auf den Schutz ihrer Daten und IT-Systeme verlassen können. IT-Sicherheit schafft Vertrauen, trägt so zur Akzeptanz von Innovationen bei und wird damit zum strategischen Erfolgsfaktor auch für deutsche Unternehmen.

Dabei haben jedoch einige Anwendungsfelder derart spezifische Anforderungen an die IT-Sicherheit, dass diese sich nicht mit Standardlösungen abdecken lassen. Im Folgenden sind besonders relevante Anwendungsfelder benannt, für die ein Bedarf an spezifischen, maßgeschneiderten Lösungen bereits heute klar zu erkennen ist. Weitere relevante Anwendungsfelder wie z.B. Smart-Home oder Smart-Services können ebenfalls berücksichtigt werden.

3.3.1 IT-Sicherheit für Industrie 4.0

Unter Industrie 4.0 wird eine durchgängige, umfassende und weltweite Vernetzung von Produkten und Prozessen in der industriellen Wertschöpfung verstanden. Maschinen, Anlagen und Produkte werden bei Industrie 4.0 intelligenter und „reden“ miteinander – vom ERP-System für die Auftragssteuerung über die SCADA-Rechner der Steuerungsebene bis zum Sensor auf der Feldebene. Damit überträgt sich die Bedrohung durch Cyber-Angriffe auf IT-Systeme auch auf industrielle Maschinen und Steuerungsanlagen.

Industrienetze sind ein attraktives Ziel nicht nur für Cyber-Kriminelle. Auch für einen konkurrierenden Maschinenbauer kann es lohnenswert sein, in das Netz eines deutschen Mitbewerbers einzudringen und dort zielgerichtet Malware zu platzieren. Ob die Fertigung gestört oder ein heimlicher Zugang zum Unternehmensnetz und damit zu sensiblen Geschäftsdaten hergestellt wird – für das geschädigte Unternehmen kann dies erhebliche finanzielle Verluste bedeuten. So entsteht der deutschen Wirtschaft durch Industriespionage jährlich ein Gesamtschaden von ca. 4,2 Milliarden Euro. Jedes dritte Unternehmen erlitt einen finanziellen Verlust aufgrund von Spionage. Über 50 % der materiellen Schäden traten dabei durch einen Ausfall, Diebstahl oder die Schädigung von IT- oder Telekommunikationsanlagen auf.

Der Schutz vor Wirtschaftskriminalität und Industriespionage braucht neue Lösungen für die IT-Sicherheit und deren durchgängige Integration in die vertikalen und horizontalen Wertschöpfungsketten. Im industriellen Umfeld ist jedoch die Heterogenität und Langlebigkeit von Maschinen und Anlagen eine große Herausforderung. Betriebszyklen verlaufen teilweise über Monate, Wartungsfenster stehen nur begrenzt zur Verfügung.

Sicherheitslösungen sollten, soweit möglich, standardisiert sein bzw. auf standardisierte Schnittstellen setzen, damit der Wettbewerb nicht behindert und kostengünstige Lösungen ermöglicht werden.

Forschungsthemen sind insbesondere:

- Nachhaltige IT-Sicherheit über den gesamten Lebenszyklus der industriellen Maschinen und Anlagen unter Berücksichtigung industrieller Spezifika wie zum Beispiel Echtzeit-anforderungen;
- Integration von IT-Sicherheitslösungen ohne Ausfallzeiten in bestehende Systeme und in neu vernetzte Produktionsumgebungen;
- modulare, für Produzenten, Integratoren und Anwender skalierbare und standardisierte IT-Sicherheitslösungen, insbesondere zur sicheren Kopplung von Prozesssteuerungs-systemen;
- Quantifizierung der IT-Sicherheit als Grundlage für Kosten-Nutzen-Abschätzungen von IT-Sicherheitsinvestitionen;
- rechtliche (z. B. Haftung, Datenschutz und Urheberrecht) und soziologische Fragen.

3.3.2 IT-Sicherheit in kritischen Infrastrukturen

Mit den neuen digitalen Technologien wächst die Zahl der Angriffspunkte. Kritische Infrastrukturen sind umso verwundbarer, je mehr sie von den digitalen Technologien abhängig sind. In Deutschland wurde vom Bundesministerium des Innern eine Einteilung der kritischen Infrastrukturen in neun Sektoren vorgenommen: Energie, Transport und Verkehr, Informationstechnik und Telekommunikation, Finanz- und Versicherungswesen, Gesundheit, Staat und Verwaltung, Wasser, Medien und Kultur sowie Ernährung. Die Abwehr von Gefahren erfordert gemeinsame Schutzkonzepte von Staat und Betreibern der Infrastrukturein-richtungen. In Deutschland befinden sich etwa vier Fünftel der kritischen Infrastrukturen in privatwirtschaftlicher Verantwortung.

Unter den Namen „Dragonfly“ zum Beispiel greifen Hacker in jüngster Zeit amerikanische und europäische Energieunternehmen an. Der Selbstversuch eines Stadtwerks in Deutschland hat gezeigt, dass ein beauftragter Hacker in nur 2 Tagen in das Steuerungsnetz des Stadtwerks eindringen konnte. In einer Metropole wie Berlin würde z.B. ein durch einen Cyber-Angriff verursachter einstündiger Stromausfall zur Mittagszeit voraussichtlich knapp 23 Millionen Euro kosten. Doch nicht nur die wirtschaftlichen Folgen können dramatisch sein. Wenn die Stromversorgung von Krankenhäusern durch Hackerangriffe auf Energiekonzerne lahmgelegt wird oder die Notstromversorgung von einer Malware abgeschaltet wird, sind auch Menschenleben in Gefahr. Länger andauernde Stromausfälle haben zudem massive Auswirkungen auf alle Lebensbereiche, wie z.B. die Wasserversorgung, den Abfallkreislauf, den Verkehr und die Lebensmittelversorgung. Gerade die Energiewende erfordert einen erhöhten Bedarf an Informationstechnologie. Die Stromversorgung wird immer innovativer, dezentraler und computergesteuerter – die Stromnetze werden folglich immer verwundbarer.

Aufgabe der Forschung ist es, gemeinsam mit den Betreibern kritischer Infrastrukturen Methoden und Werkzeuge für eine zuverlässige Absicherung der lebenswichtigen IT-Systeme zu entwickeln, so dass Versorgungsleistungen, die über kritische Infrastrukturen erbracht werden, jederzeit garantiert werden können.

Forschungsthemen sind insbesondere:

- Analyse und Bewertung von Angriffspotenzialen für kritische Infrastrukturen und ihre Auswirkungen hinsichtlich möglicher Domino- und Kaskadeneffekte;
- Konzeption umfassender Schutzkonzepte und hochwertiger sowie gleichzeitig kosteneffizienter IT-Infrastrukturen;
- frühzeitiges Erkennen von Störungen und Ausfällen in kritischen Infrastrukturen und Lösungen zu deren Beschränkung auf ein Mindestmaß;
- umgehende und autonome Wiederherstellung der Versorgungsleistung bei gleichzeitiger Gewährleistung der erforderlichen IT-Sicherheit;
- Erfassung und Bewertung von sicherheitsrelevanten Ereignissen zur langfristigen und kontinuierlichen Verbesserung des Schutzstandards, zur Erstellung eines IT-Sicherheitslagebildes und zur Unterstützung des Risikomanagements;
- praktikable und kostengünstige IT-Sicherheitslösungen für einen nachhaltigen und kontinuierlichen Schutz der kritischen Infrastrukturen und die Sicherstellung der Integrität über den gesamten Lebenszyklus.

3.3.3 Sichere IKT-Anwendungen in der Medizin

Computergestützte Chirurgie, Vernetzung der medizinischen Bildgebung und mobile Lösungen für das Echtzeit-Monitoring von Patienten – auch im Gesundheitsbereich wird IKT immer wichtiger.

In der Medizintechnik ist die Vernetzung von Geräten bereits fortgeschritten, doch handelt es sich größtenteils um herstellerspezifische Komplettlösungen. Wünschenswert wäre es, die Daten eines Patienten von jedem beliebigen Gerät eines jeden beliebigen Herstellers abrufen zu können – und zwar von der Einlieferung eines Patienten in eine Klinik bis zu seiner Entlassung und idealerweise bis zur weiteren ambulanten Behandlung. Bevor diese Vision Wirklichkeit werden kann, müssen medizinische Geräte aber zunächst hohe Zulassungsanforderungen erfüllen. Besonders schwer zu erbringen sind die Sicherheitsnachweise bei der Vernetzung von Geräten unterschiedlicher Hersteller.

Angesichts einer immer älter werdenden Gesellschaft gewinnt zudem die Frage nach der IKT-unterstützten medizinischen Versorgung in den eigenen vier Wänden an Bedeutung. Häusliche Betreuung kann durch Telemedizin und Smart Home-Technologien deutlich unterstützt, in manchen Fällen erst ermöglicht werden.

Garantiert werden soll die bestmögliche Versorgung der Patientinnen und Patienten – ob in der Klinik, im Wohnumfeld oder Pflegebereich. Die Herausforderung besteht darin, den Schutz der sensiblen Gesundheitsdaten auch bei fortschreitender Digitalisierung und herstellerunabhängiger Vernetzung der Gesundheitswirtschaft zu gewährleisten.

Forschungsthemen sind insbesondere:

- Sichere und dynamische Vernetzung von Medizingeräten in Planung, Diagnose und Therapie sowie in der klinischen IT-Umgebung;
- sichere Integration mobiler Geräte z.B. im Operationssaal oder in der klinischen IT-Umgebung;
- patientenorientierte, datenschutz- und rechtskonforme Lösungen für eine intelligente Vernetzung im Wohn- und Pflegebereich.

3.3.4 IT-Sicherheit in Verkehr und Logistik

Die Vernetzung im Auto ist heute immens: Je nach Fahrzeugklasse werden bis zu 50 vernetzte Komponenten über Mikroprozesse angesteuert. In einem modernen Auto arbeiten mehr als 100 Sensoren und bis zu 200 Prozessoren. Darüber hinaus vernetzen sich Fahrzeuge als kooperative Verkehrs- und Transportinfrastrukturen. Sie bilden Verbundsysteme über Fahrzeug-zu-Fahrzeug (Car2Car) und Fahrzeug-zu-Infrastruktur (Car2X) Kommunikation und erhöhen so Verkehrssicherheit und Transporteffizienz. Auch für den effizienten Einsatz von Flugzeug, Bus und Bahn sowie für Logistikunternehmen werden die neuen vernetzten Strukturen immer wichtiger.

Die neuen Technologien der so genannten Connected Cars bringen mobile Kommunikation in die Autos. Systeme dieser Art müssen vor gezielten IT-Angriffen, insbesondere auch wegen der weitreichenden Folgen für Fahrzeugführer und andere Verkehrsteilnehmer, genauso geschützt werden wie Server oder Heim-PC.

Zum Aufbaukooperativer Verkehrsinfrastrukturen müssen sich die beteiligten Partner auf die Informations- und Datensicherheit der anderen Partner verlassen können. Ein fehlendes Sicherheitskonzept wird die Akzeptanz für die Anwendungen beziehungsweise den Kauf kooperativer Systeme deutlich verringern. Andererseits dürfen Sicherheitslösungen den Wettbewerb nicht behindern, und sollten daher auf standardisierte Schnittstellen setzen.

Es ist erforderlich, Voraussetzungen für IT-Sicherheitslösungen zum Schutz des Fahrzeugs (In-Vehicle Security, Embedded Security), des Fahrzeugführers und anderer Verkehrsteilnehmer und zum autonomen Fahren zu schaffen. Auch die Kommunikationskanäle zwischen den Fahrzeugen bedürfen besonderen Schutzes.

Forschungsthemen sind insbesondere:

- Schutz der Fahrzeugkommunikation (Car2X), Fahrzeugsteuerung und der Fahrzeugdaten;
- Konzeption von ganzheitlichen, die Privatsphäre respektierenden IT-Sicherheitslösungen für intelligente Verkehrslenkung und -steuerung und ihre Integration in bestehende Infrastrukturen;
- Aktualisierung von IT-Sicherheitsmechanismen über den gesamten Produktlebenszyklus.

3.4 Privatheit und der Schutz von Daten

Internetnutzerinnen und -nutzer in Deutschland waren im Jahr 2013 durchschnittlich 169 Minuten täglich online, das ist über ein Viertel mehr als im Vorjahr.

Für Internetdienste und die Nutzung sozialer Netzwerke bezahlen immer mehr Menschen mit personenbezogenen Informationen. Dies wird durch die mobile Nutzung noch verstärkt. Was mit diesen Daten anschließend passiert, an wen sie weiterverkauft und wie sie genutzt werden, haben die Nutzer meist selbst nicht mehr in der Hand. Dabei entstehen neue Bedrohungen: Der online sichtbare Besuch einer Veranstaltung kann zur Einladung für Kriminelle werden, in eine dann leerstehende private Wohnung einzubrechen. Zahlreiche Aktivitäten werden zudem gespeichert, gesammelt und zu Profilen aggregiert – oft ohne dass die Nutzer dieses ahnen. Das betrifft alle Anwender mobiler Kommunikation, seien es Smartphones, Navigationsgeräte oder das Wearable, mit dem ein Freizeitsportler seine Vitaldaten erfasst und speichert.

3.4.1 Privatheit und selbstbestimmtes Leben in der digitalen Welt

Damit Bürgerinnen und Bürger ihr Recht auf Selbstbestimmung wahrnehmen und ihre Privatsphäre schützen können, sind zum einen die technischen Voraussetzungen zu schaffen. Zum anderen ist die individuelle Medienkompetenz der Nutzerinnen und Nutzer zu stärken und darauf zu achten, dass Geschäftsmodelle, die auf der Auswertung personenbezogener Daten basieren, eine Kontrolle durch die Nutzerinnen und Nutzer zulassen.

Herausforderung für die Forschung ist es, Technologien zum Schutz der Privatheit so einzurichten, dass sie auch von Laien effektiv und mit niedrigem Zusatzaufwand genutzt werden können. Digitale Dienstleistungen müssen so gestaltet sein, dass die Nutzerinnen und Nutzer die volle Souveränität und Kontrolle über ihre Daten behalten. Der technikgestützte Datenschutz („Privacy by design“) soll ausgebaut und verbessert werden.

Forschungsthemen sind insbesondere:

- Herausforderungen die sich aus der zunehmenden Vernetzung von Lebensbereichen (Smart Home, E-Mobilität u. a.) für den Schutz persönlicher Daten ergeben;
- Mechanismen und Möglichkeiten des Selbstdatenschutzes, die intuitiv zu nutzen und deren Schutzwirkungen umfassend, verständlich und nachvollziehbar sind, beispielsweise durch Anbringen eines Gütesiegels;
- Verfahren und Infrastrukturen für die vertrauliche und anonyme Kommunikation im Internet, die auch für Laien anwendbar sind;
- technische, organisatorische und rechtliche Grundlagen, die den Nutzerinnen und Nutzern eine zuverlässige Delegation von komplexen Datenschutzaufgaben an Dienstleister ermöglichen;
- neue Formen der Online-Kommunikation, die informationelle Selbstbestimmung und den Schutz der Privatheit ermöglichen.

3.4.2 Netzkultur – Leben und Wertewandel im Internet-Zeitalter

Das Internet hat sich in den vergangenen 20 Jahren zu einer universellen Plattform für die Kommunikation entwickelt. Die berufliche und private Kommunikation wird zunehmend in digitale Räume verlegt. Verbindliche Gemeinschaften werden durch offene Netzwerke ergänzt. Das alltägliche Leben wird durch die digitalen Angebote unterstützt und kulturell bereichert, aber auch beschleunigt.

Die globale und ständige Verfügbarkeit der digitalen Angebote fördert sozio-technologische Innovationen und trägt zur individuellen Selbstverwirklichung bei. Gleichzeitig entstehen neue Verhaltensweisen und Kulturtechniken. Die vielfältigen Auswirkungen des Internets auf unser Leben und den damit verbundenen Wertewandel – die Netzkultur – zu verstehen und wissenschaftlich zu fassen ist bisher nur ansatzweise gelungen.

Eine zentrale Aufgabe der Forschung besteht darin, die Entwicklungen der Netzkultur hinsichtlich ihrer gesellschaftlichen Implikationen zu bewerten. Dazu gehört auch die Unterstützung von Innovationen und gesellschaftlichen Entwicklungen durch geeignete Normen und Leitbilder. Für eine solche übergreifende Betrachtungsweise müssen Sozialwissenschaft, Rechtswissenschaft, Ethik und Technikwissenschaft zusammenarbeiten.

Forschungsthemen sind insbesondere:

- Untersuchung und interdisziplinäre Begleitung des Wertewandels im Internet-Zeitalter und den damit zusammenhängenden sozialen Praktiken;
- gesamtgesellschaftliche Beurteilung des Stellenwertes von Normen und Werten in der digitalen Welt;
- Untersuchung und Förderung des kulturellen Umfeldes für neue Geschäftsfelder wie Smart Services, welche aus dem Zusammenwachsen von digitaler und „realer" Welt entstehen und der Herausforderungen, die sich daraus für den Schutz der informationellen Selbstbestimmung ergeben;
- sichere und demokratische Gestaltung von Möglichkeiten der direkten politischen und gesellschaftlichen Beteiligung.

3.4.3 Privatheit und Big Data

Die Nutzung sozialer Medien wie Facebook und Twitter und die fortschreitende Vernetzung unterschiedlicher Systeme wie zum Beispiel von Kameras zur Verkehrssteuerung oder der Automobile einer Carsharing-Flotte, tragen zu einer erheblichen Anhäufung von Daten bei. Bei jeglicher Aktivität im Internet, ob bei der Nutzung von Online-Angeboten, dem Besuch von Such- oder Verkaufsportalen oder der Nutzung von webgestützten Sensorsystemen zur Kontrolle von Herzschlag oder Blutdruck bei Sportlern. Immer werden Datenspuren hinterlassen.

Der Markt für den Handel mit Daten wächst rasant. Der globale Umsatz mit Big-Data-Produkten und -Dienstleistungen stieg im Jahr 2014 auf rund 73,5 Milliarden Euro. Dies entspricht einem Zuwachs von 66 % im Vergleich zum Vorjahr.

Die Bekanntgabe einzelner persönlicher Details empfinden viele als harmlos – manchmal sogar als nützlich, wenn zum Beispiel Produkte und Dienstleistungen im Internet entsprechend individueller Präferenzen bedarfsorientiert angeboten werden. Allerdings ermöglichen

solche Informationen, Aussagen über Interessen, Lebensweisen und Gewohnheiten abzuleiten. Computerbasierte Technologien sind in der Lage, aus einer großen Menge von Daten die unzähligen oftmals winzig kleinen Datenspuren jeder einzelnen Person herauszufiltern und detaillierte Profile von Gruppen und Einzelpersonen zu erstellen.

Solche Profile können Menschen in „Schubladen" einsortieren, ohne dass dies für den Einzelnen noch nachvollziehbar oder zu korrigieren ist. Das kann schwerwiegende Folgen haben, wenn beispielsweise ein potenzieller Arbeitgeber einen Bewerber aufgrund privater Vorlieben ablehnt oder Versicherungen aufgrund bekannt gewordener Hinweise auf die persönliche Lebensführung nur unter verschärften Bedingungen abgeschlossen werden können.

Aufgabe der Forschung ist es, Konzepte zu schaffen, die die Grundrechte der Bürgerinnen und Bürger (Persönlichkeitsrecht, Privatsphäre, Schutz der informationellen Selbstbestimmung) auch bei Big Data-Anwendungen gewährleisten.

Forschungsthemen sind insbesondere:

- Gestaltung von Big Data-Diensten nach dem Prinzip der Datensparsamkeit, insbesondere dass Profilbildung und darauf basierende Geschäftsmodelle ohne die Erhebung individualisierter personenbezogener Daten auskommen;
- Anonymisierung und Pseudonymisierung bei Big Data-Diensten;
- Entwicklung neuer juristischer und technischer Konzepte für den Schutz sensibler Daten in Big Data-Analysen;
- Durchsetzung der Zweck- und Kontextbindung personenbezogener Daten in Big Data Analysen, technisch wie rechtlich;
- Definition von Metriken für Privatheit;
- Gestaltung von Data Mining Verfahren und -Anwendungen, die eine Profilbildung oder Benachteiligung für betroffene Nutzer ausschließen.

4 IT-Sicherheitsforschung gestalten

4.1 Nationale Kompetenzen ausbauen

Eine innovative IT-Sicherheitsforschung bietet die Chance, nicht nur Cyberbedrohungen abzuwehren, sondern auch sichere IT-Produkte und Dienstleistungen zu entwickeln und so Deutschland zu einem führenden Anbieter für IT-Sicherheitstechnologie zu machen und seine digitale Souveränität zu stärken.

Forschung fördern und vernetzen

Seit 2006 bündelt die Bundesregierung ressortübergreifend ihre Forschungs- und Innovationsaktivitäten in der Hightech-Strategie 2020, um Deutschlands Spitzenstellung in Schlüsseltechnologien auszubauen und die Umsetzung von Forschungsergebnissen in Produkte und Dienstleistungen zu beschleunigen.

Die Forschungsförderung zur IT-Sicherheit trägt dazu bei, einen im internationalen Maßstab hohen Leistungsstand der IT-Sicherheitsforschung zu erreichen und die zeitnahe Verwertung der Forschungsergebnisse zu sichern. Sie erfolgt vor allem im Rahmen von Verbund- oder Einzelprojekten in den genannten Förderschwerpunkten.

Verbundprojekte sind ein wesentliches Instrument der Projektförderung, in denen wissenschaftliche Einrichtungen und Unternehmen interdisziplinär zusammenarbeiten. Eine wichtige Rolle spielen in den Projekten vor allem die Anwender und Endnutzer, damit der Transfer in die Anwendung sichergestellt ist. Bei den Auswahlentscheidungen über einzelne Fördermaßnahmen werden neben der Qualität des Forschungsansatzes auch die Wirtschaftlichkeit und ein ausgewogenes Verhältnis zwischen Aufwand und Nutzen betrachtet.

Kompetenzen bündeln

Seit 2011 fördert das BMBF drei Kompetenzzentren für IT-Sicherheitsforschung, die neue Ansätze zur IT-Sicherheitsforschung entwickeln:

- CISPA – Center for IT-Security, Privacy and Accountability in Saarbrücken;
- EC-SPRIDE – European Center for Security and Privacy by Design in Darmstadt;
- KASTEL – Kompetenzzentrum für angewandte Sicherheitstechnologie in Karlsruhe.

Die Kompetenzzentren sind herausragende Standorte in der IT-Sicherheitsforschung in Deutschland. Die Bündelung von nationalen Forschungskompetenzen vermeidet kostenintensive Doppel- und Parallelstrukturen und ermöglicht, Forschungsinhalte geeignet zu konsolidieren.

Die Zentren sind als regionale Schwerpunkte angelegt, die vor Ort die Kompetenzen zu Fragen der IT-Sicherheitsforschung bündeln und interdisziplinär arbeiten. Sie greifen kontinuierlich aktuelle und neue Forschungsfragen auf und erarbeiten zeitnah und flexibel Einschätzungen, Handlungsempfehlungen und Lösungen zu aktuellen Herausforderungen. Alle drei Zentren decken ein großes Spektrum der IT-Sicherheitsforschung ab und bearbeiten ihren Profilen entsprechend vorzugsweise die Schwerpunkte Design, Integration und Analyse. In ihrer Bedeutung als nachhaltige wissenschaftliche Basis und zur Stärkung der Expertise deutscher Forschung und Industrie in Fragen der Cybersicherheit werden die Kompetenzzentren weiter gestärkt.

www.kompetenz-it-sicherheit.de

Das Forum „Privatheit und selbstbestimmtes Leben in der Digitalen Welt“ ist ein interdisziplinär zusammengesetzter Expertenkreis, der im Rahmen eines Projektes gesellschaftlich relevante Fragestellungen zum Schutz der Privatheit aus verschiedenen wissenschaftlichen Perspektiven analysiert und Vorschläge für ganzheitliche Lösungsansätze erarbeitet.

Das Forum identifiziert hierzu die relevanten Schnittstellen zwischen den Disziplinen und tritt in einen intensiven wissenschaftlichen und öffentlichen Diskurs, aus dem heraus neue Forschungsthemen entwickelt werden.

www.forum-privatheit.de

KMU fördern

Der Anteil der IT-Sicherheitswirtschaft beläuft sich in Deutschland auf knapp 10 % der gesamten IT-Branche. Gerade für kleine und mittlere Unternehmen ist IT-Sicherheit ein wichtiges Geschäftsfeld. Für mehr als die Hälfte der mittelständischen Unternehmen in Deutschland ist IT-Sicherheit der maßgebliche Technologietrend in der Informationstechnik.

Junge dynamische Unternehmen mit innovativen Ideen für neue IT-Sicherheitslösungen werden vom Bundesministerium für Bildung und Forschung darin unterstützt, international im rasant wachsenden und sich ständig verändernden Bereich der IT-Sicherheit flexibel zu agieren. Mittelständische IT-Unternehmen sind eher langfristig aufgestellt und spielen eine wichtige Rolle für den breiten Einsatz neuer IT-Sicherheitslösungen. Forschungsaktivitäten von kleinen und mittleren Unternehmen werden daher besonders gefördert.

Das Bundesministerium für Bildung und Forschung bietet seit 2007 mit der Förderinitiative KMU-innovativ zusätzlich zu den klassischen Förderprogrammen einen schnellen und leichten Zugang zu Technologieförderprogrammen.

www.kmu-innovativ.de

4.2 Europäische und internationale Zusammenarbeit stärken

Forschung und Innovation sichern auf dem globalen Markt die Wettbewerbsfähigkeit Deutschlands und Europas. Die aktuellen Herausforderungen können nicht im nationalen Alleingang gelöst werden. Im Rahmen dieses Programmes sollen durch bilaterale Maßnahmen und Beteiligung an Maßnahmen der EU-Kommission nationale Interessen gebündelt und gemeinsame Lösungen erforscht werden.

Horizont 2020

Das europäische Rahmenprogramm für Forschung und Innovation „Horizon 2020“ bündelt die bisher getrennten EU-Programme der Forschungs- und Innovationsförderung. Mit seinem interdisziplinären Ansatz nimmt es den gesamten Innovationszyklus in den Blick und fördert so die Zusammenarbeit und den Austausch von Ideen. Ziel der deutschen IT-Sicherheitsforschung ist es, in den drei thematischen Säulen international relevante Forschungsthemen zur IT-Sicherheit zu verankern:

- Exzellenz europäischer Wissenschaft: Sichern der Wettbewerbsfähigkeit der Europäischen Union durch herausragende Forschungsleistungen;
- industrielle Führungsrolle: Förderung industrieller Investitionen und Forschung insbesondere im Bereich der Schlüsseltechnologien;
- gesellschaftliche Herausforderung: Förderung von Forschung und Innovationen zur Lösung der großen gesellschaftlichen Herausforderungen entlang der gesamten Wertschöpfungskette von der Forschung bis zur Markteinführung.

Beispiele sind die Forschungsschwerpunkte Quantenkommunikation und Kryptografie, die sich in den Säulen „Exzellenz europäischer Wissenschaft“ bzw. „Industrielle Führungsrolle“ wiederfinden.

Maßnahmen zur Umsetzung des Forschungsrahmenprogramms führen hinsichtlich des EU-Haushaltes zu keinem zusätzlichen Mehraufwand. Die Maßnahmen müssen aus den vorhandenen Ansätzen des EU-Haushalts finanziert werden können, die Obergrenzen des Mehrjährigen Finanzrahmens 2014 – 2020 (MFR) der EU dürfen nicht überschritten werden.

www.horizon2020.de

Fit für Europa

Um die Beteiligung deutscher Akteure an Vorhaben der europäischen IT-Sicherheitsforschung und insbesondere am Rahmenprogramm für Forschung und Innovation „Horizont 2020“ zu stärken, werden national vorhandene Kompetenzen gebündelt und im Hinblick auf zukünftige Themen der europäischen IT-Sicherheitsforschung ausgebaut. Mit Fördermaßnahmen soll die europäische und interdisziplinäre Kooperation von Partnern aus Forschungseinrichtungen gemeinsam mit Wirtschaft und Endnutzern zu einem erfolgreichen europäischen Netzwerk mit deutscher Beteiligung ausgebaut werden.

EUREKA

EUREKA ist eine Initiative für anwendungsnahe Forschung in Europa und bietet Industrie und Wissenschaft einen Rahmen für bi- oder multinationale Kooperationsprojekte. Die Initiative trägt dazu bei, die in Europa vorhandenen fachlichen und finanziellen Ressourcen auch in der IT-Sicherheitsforschung effektiver zu nutzen und damit die Wettbewerbsfähigkeit Europas auf dem Weltmarkt zu stärken.

Das Projekt „Safe and Secure European Routing – SASER“ ist ein Beispiel für eine erfolgreiche Kooperation, in der Partner aus fünf europäischen Ländern gemeinsam wissenschaftliche und technologische Lösungen für

leistungsstarke Kommunikationsnetze mit hohen Sicherheitsstandards und nachhaltiger Kosten- und Energiestruktur entwickeln. Dieser erfolgreiche Ansatz soll fortgeführt werden, um auch in Zukunft über wettbewerbsfähige europäische Technologien zu verfügen.

4.3 Dialog ausbauen

Innovative IT-Sicherheitslösungen müssen den vielfältigen Anforderungen und Bedürfnissen staatlicher, wirtschaftlicher und privater Nutzerinnen und Nutzer entsprechen. Ein gesellschaftlicher Dialog, der von der Wissenschaft über die Wirtschaft bis zu den Bürgerinnen und Bürgern alle einbezieht, kann zu einem besseren Verständnis der Bedürfnisse der Beteiligten und zu adäquatem Handeln beitragen. Damit es gelingt, die IT-Sicherheitsforschung an den Bedürfnissen des Marktes auszurichten und wissenschaftliche Erkenntnisse schnell und effizient wirtschaftlich zu verwerten, ist eine enge Verzahnung von Wissenschaft und Wirtschaft erforderlich. Gleichzeitig soll eine transparente Darstellung der Forschungsergebnisse in der Öffentlichkeit gewährleistet werden.

In der IT-Sicherheitsforschung gewinnen rechtliche, ökonomische und soziale Fragestellungen immer mehr an Bedeutung. Umfassende und umsetzbare Lösungen für IT-Sicherheit können nur im Dialog der Disziplinen und im Rahmen breiter interdisziplinärer Zusammenarbeit erreicht werden.

Das Forschungsrahmenprogramm verfolgt zudem einen systemischen Ansatz, der die komplette Innovationskette von der Grundlagenforschung über die angewandte Forschung bis hin zur Wertschöpfung der Ergebnisse berücksichtigt. Sowohl bei der Identifizierung der Förderschwerpunkte und der Umsetzung der Vorhaben als auch bei der Verwertung der Forschungsergebnisse erfolgt ein kontinuierlicher Austausch zwischen den Hochschulen, der außeruniversitären Forschung und den Unternehmen. Die Forschungsergebnisse werden so schneller in Innovationen am Markt und in die Gesellschaft überführt und für Endanwenderinnen und Endanwender nutzbar gemacht.

Bei gesellschaftlich kontroversen Fragestellungen wie bei den Themen Privatheit und IT-Sicherheit kann eine sachliche und fachlich fundierte Diskussion mit den Bürgerinnen und Bürgern eine realistische Abschätzung der Chancen und Risiken für den Einzelnen und die Gesellschaft ermöglichen und den erreichbaren Konsens ausloten.

Die Dialoge sollen den Bürgerinnen und Bürgern

- Wissen und Orientierung in der Vielfalt von Information geben;
- eine Plattform bieten, über die Chancen und Herausforderungen von Privatheit und IT-Sicherheit zu diskutieren;
- ermöglichen, sich im offenen Austausch mit Expertinnen und Experten eine fundierte Meinung zu bilden.

Die Ergebnisse der Dialoge mit den Bürgerinnen und Bürgern werden in die Ausgestaltung der Forschungsfelder mit einbezogen.

4.4 Wissenschaftlichen Nachwuchs fördern

Um sichere IT-Produkte und Dienstleistungen in Deutschland auf höchstem technologischen Stand anbieten zu können, müssen vorhandene Innovationspotenziale konsequent genutzt werden. Deshalb steigt der Bedarf an qualifizierten wissenschaftlichen Nachwuchskräften im Bereich der IT-Sicherheit in Deutschland stetig.

Eine IT-Sicherheitsforschung, die den Herausforderungen des globalen Wettbewerbs in Wissenschaft und Wirtschaft gerecht werden will, misst der Förderung des wissenschaftlichen Nachwuchses hohe Priorität bei. Entsprechende Initiativen sollen im Rahmen des Programmes gestärkt werden. Dadurch werden auch Anreize für die Gründung junger, innovativer Unternehmen geschaffen.

Forschungsprojekte und Kompetenzzentren bieten Nachwuchsforscherinnen und -forschern die Möglichkeit, ihre Arbeit mit anerkannten Forscherinnen und Forschern zu diskutieren und Communities zwischen Nachwuchs und etablierten Forschern aufzubauen.

4.5 Rahmenbedingungen des Forschungsrahmenprogramms

IT-Sicherheit ist immer anwendungsbezogen. In allen Bereichen, die von der Informationstechnik berührt werden, muss auch die IT-Sicherheit von Anfang an mitgedacht werden. Die Verbindung von IT-Sicherheitstechnologie und Anwendungsfeldern kann dabei völlig neue Chancen und Geschäftsfelder eröffnen. Für die

IT-Sicherheit von Industrie 4.0 ist es zum Beispiel nicht ausreichend, herkömmliche etablierte IT-Sicherheitslösungen in die neue, vernetzte IT-Produktionswelt zu übertragen. Industrie 4.0 benötigt neue anspruchsvolle Ansätze für Architekturen und Prozesse. Dieses Forschungsrahmenprogramm trägt dazu bei, diese Chancen zu nutzen.

Die Maßnahmen dieses Forschungsrahmenprogramms stehen dabei nicht isoliert, sondern sind insbesondere mit folgenden Aktivitäten der Forschungspolitik verzahnt: dem Programm zur Forschung zur zivilen Sicherheit, der Gesundheitsforschung (insbesondere der individualisierten Medizin), neuen Themenfeldern wie „Innovationen für die Produktion, Dienstleistung und Arbeit von morgen“, „Informationsgesellschaft“ und „Elektroniksysteme“ sowie der Forschungsagenda zum demografischen Wandel.

Das Forschungsrahmenprogramm ist als offenes Programm angelegt. Daher ist geplant, innerhalb der Programmlaufzeit eine Prüfung vorzunehmen, ob die ursprünglichen Programmannahmen, die Akteursstruktur und der Forschungsfokus noch gelten oder das Programm inhaltlich zu aktualisieren oder zu ergänzen ist. Dabei wird auch eine ausgaben-seitige Haushaltsanalyse durchgeführt, die die finanzielle Umsetzbarkeit der Maßnahmen betrachtet.

Das Forschungsrahmenprogramm ist somit eine offene Plattform für Anwendungsthemen im Kontext IT-Sicherheit unter Einbindung aller relevanten Aktivitäten in den Anwendungs-feldern der Hightech-Strategie: digitale Wirtschaft und Gesellschaft, nachhaltiges Wirtschaften und Energie, gesundes Leben, intelligente Mobilität, zivile Sicherheit und innovative Arbeitswelt.

Für die Laufzeit von 2015 - 2020 plant allein das BMBF über 180 Mio. Euro für das Forschungsrahmenprogramm zur Förderung der IT-Sicherheit bereitzustellen. Die Maßnahmen stehen im Einklang mit dem Bundeshaushalt und dem Koalitionsvertrag.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333