CPS.HUB /NRW
Competence Center for
Cyber Physical Systems

DISKUSSION

CYBER PHYSICAL SECURITY IN NRW

/ August 2018

Chancen und Herausforderungen für Wissenschaft und Wirtschaft

INHALT

Cyber Physical Security in Nordrhein-Westfalen

Im Zuge der Digitalisierung von Produkten und Services gewinnt das Thema Sicherheit zunehmend an Bedeutung – insbesondere vor dem Hintergrund, dass immer mehr Gegenstände eingebettete IT-Systeme haben, die miteinander oder mit dem Internet vernetzt sind. Cyber Physical Systems stellen die technologische Basis der Kombination von IT mit der physikalischen Welt dar und spielen in zahlreichen Bereichen ein große Rolle – so zum Beispiel in den Zukunftsfeldern Industrie 4.0, Logistik 4.0, Smart Health, Smart Energy und Smart Circular Economy. Bisher abgeschottete Systeme wie z. B. Fahrzeuge werden durch die Vernetzung angreifbar. Es gilt deshalb, potenzielle Angriffspunkte in Hinsicht auf Software-, Systemsicherheit und Datenschutz zu analysieren, um Cyber Physical Security nicht zum Hemmnis, sondern zum Enabler für innovative Anwendungen zu machen.

Das vorliegende Papier ist für den IT-Sicherheits-Roundtable der Ministerien für Wirtschaft, Innovation, Digitalisierung und Energie sowie Wissenschaft und Kultur im Rahmen zweier Workshops mit ausgewählten Experten aus Wissenschaft und Wirtschaft und einem anschließenden Diskussions- und Konsolidierungsprozess entstanden.

Dank

Sebastian Barchnicki, Secunet Security Networks AG / Ralf Benzmüller, G-Data Software / Prof. Eric Bodden, Heinz-Nixdorf-Institut, Fraunhofer IEM / Dr. Roland Büschkes (Toyota Insurance Management) / Prof. Philipp Cimiano, Universität Bielefeld / Bernd Fuhlert, @yet GmbH / Prof. Barbara Hammer, Universität Bielefeld / Prof. Thorsten Holz, Horst-Görtz-Institut / Prof. Tibor Jager, Universität Paderborn / Martin Kowalski, nrw.uniTS / Hubert Martens, networker NRW / Dr. Matthias Meyer, Fraunhofer IEM / Prof. Norbert Pohlmann, Westfälische Hochschule Gelsenkirchen, if(is) / Prof. Matthew Smith, Rheinische-Friedrich-Wilhelms-Universität Bonn, Fraunhofer FKIE / Michael Sparenberg, Institut für Internet-Sicherheit if(is) / Kai Wittenburg, neam IT-Services GmbH

Kontakt:

CPS.HUB NRW

Institut SIKoM+ | Bergische Universität Wuppertal
Rainer-Gruenter-Straße 21
42119 Wuppertal

E-Mail: security@cps-hub-nrw.de
Telefon: +49 202 439-1026

Redaktion:

Bergische Universität Wuppertal
Monika Gatzke
Jacqueline Stork

August 2018

Gefördert durch:

EUROPÄISCHE UNION
Investition in unsere Zukunft
Europäischer Fonds
für regionale Entwicklung

EFRE.NRW
Investitionen in Wachstum
und Beschäftigung

Ministerium für Wirtschaft, Innovation,
Digitalisierung und Energie
des Landes Nordrhein-Westfalen

1. Cyber Physical Security in NRW

Die Digitalisierung und Vernetzung der Gesellschaft und der Wirtschaft schreitet rasant voran: Bis zum Jahr 2020 sollen rund 100 Milliarden Devices im Internet of Things miteinander vernetzt sein.[i] Das schafft für jeden einzelnen Annehmlichkeiten im Alltag und Vorteile für Unternehmen und die Wirtschaft, gleichzeitig steigt aber das Bedrohungspotenzial durch eine nicht ausreichende IT-Sicherheitsarchitektur.

Der volkswirtschaftliche Schaden ist enorm. Eine Bitkom-Studie ermittelte einen Schaden durch Spionage, Sabotage und Datendiebstahl von rund 55 Milliarden Euro pro Jahr für die deutsche Wirtschaft. Insbesondere Nordrhein-Westfalen ist hiervon als führender Industrie-Standort Deutschlands betroffen. Arbeit 4.0 und Industrie 4.0 können nur nachhaltig erfolgreich sein, wenn IT-Sicherheit dabei von Beginn an mitgedacht und als Standortvorteil verstanden wird. Zahlreiche Studien belegen aktuell, dass der Mangel an IT-Sicherheit ein Hemmnis für die digitale Transformation darstellt. So möchten 74 Prozent der Unternehmen die digitale Transformation nicht auf Kosten ihrer IT-Sicherheit vorantreiben, zudem befürchten 21 Prozent Umsatzeinbußen durch die Verzögerung der Digitalisierung aufgrund von IT-Sicherheitsbedenken – so die Ergebnisse einer Studie von Bitkom in Zusammenarbeit mit der Bundesdruckerei.[ii] Im Jahr 2017 gaben 7 von 10 Industrieunternehmen an, Opfer von Sabotage, Datendiebstahl oder Spionage in den vergangenen zwei Jahren geworden zu sein, jedes fünfte Unternehmen vermutet dies. Bei fast einem Drittel (23 Prozent) der betroffenen Unternehmen sind dabei sensible Daten abgeflossen.[iii]

Um die positiven Aspekte der Digitalisierung nutzen zu können, muss der IT-Sicherheitssektor weiter ausgebaut werden. Nordrhein-Westfalen verfügt dabei bereits über eine hervorragende Ausgangslage: Ca. 700 Forscher an knapp 20 Forschungseinrichtungen erzielen exzellente Forschungsergebnisse in allen Bereichen der IT-Sicherheit (u.a. Softwaresicherheit, IT-Sicherheit für embedded Systems und Kryptografie).[iv] Diese Forschung ist essentiell, um die Wettbewerbsfähigkeit des Standorts NRW langfristig zu sichern. IT-Sicherheit fungiert dabei als Enabler der digitalen Transformation.

Zum heutigen Zeitpunkt existieren bundesweit ca. 1.468 verschiedene Anbieter von IT-Sicherheitstechnologien, von denen etwa 415 in NRW ansässig sind.[v]

2. Einschätzung durch die Wissenschaft

Im Rahmen eines Workshops mit ausgewählten IT-Sicherheitsexperten aus der Forschung wurden zukunftsweisende Themen identifiziert. Dabei kristallisierten sich einerseits Themen mit einem langfristigen Zeithorizont heraus, deren Relevanz sich für die Wirtschaft erst in Zukunft manifestieren wird, deren Erforschung aber schon jetzt notwendig ist, um die Anschlussfähigkeit Nordrhein-Westfalens zu sichern. Andererseits zeigten sich aber auch Themenschwerpunkte, die einen mittelfristigen oder gar kurzfristigen Zeithorizont haben, bei denen also aktuell ein großer Innovationsbedarf besteht.

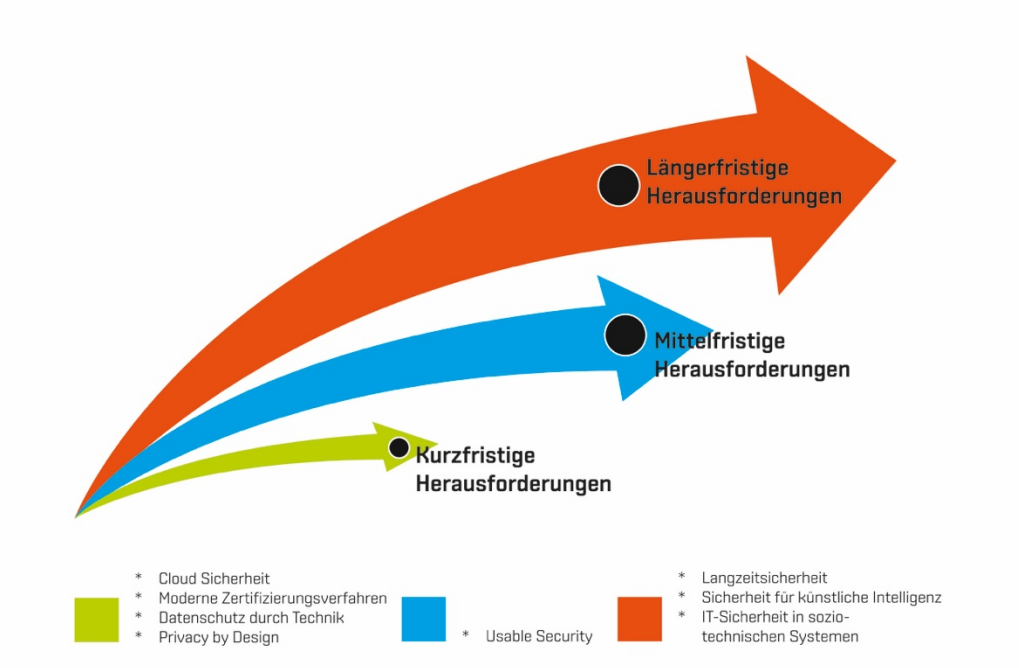

Abbildung 1: Einschätzung durch die Wissenschaft - Die Herausforderungen im zeitlichen Horizont. Eigene Darstellung

2.1. Längerfristige Herausforderungen

Folgende Ergebnisse spiegeln die Einschätzung der IT-Sicherheitsexperten aus der Forschung wider:

a) Langzeitsicherheit

Um Langzeitsicherheit zu gewährleisten, wird insbesondere Forschung in den Bereichen Privacy by Design, Modularisierung von Komponenten von eingebetteten Systemen und IT-Sicherheit bei Angriffe von Quantencomputern benötigt. Privacy by Design bedeutet, dass wichtige Sicherheits- und Privatsphärefragen bereits in der Entwicklung mitgedacht werden. Um beispielsweise Softwareentwickler dabei zu unterstützen, muss erforscht werden, wie Schwachstellen automatisiert und möglichst früh im Entwicklungsprozess sowie möglichst zuverlässig erkannt werden können.

Eingebettete Systeme setzen sich häufig aus standardisierten Hard- und Softwarekomponenten zusammen. Das bringt zwar Vorteile, wie etwa die einfache Integration in verschiedenen Anwendungskontexten, der Nachteil ist aber, dass die Komponenten durch ihre zahlreichen Schnittstellen anfällig für Manipulation und Angriffe sind. Es gilt, neue Systemarchitekturen zu entwickeln, die eine dynamische, graduelle Anpassung von Sicherheitskonzepten und -kontrollen ermöglichen. Hierbei stellt sich u.a. die Frage, wie Komponenten sinnvoll modularisiert werden können, damit aufwendige Sicherheitszertifizierungen nicht wie bislang nach jedem Sicherheitsupdate erneut erforderlich werden, und damit sich beispielsweise auch hardwarebasierte Verschlüsselungskomponenten über die Zeit kostengünstig tauschen lassen, um die Sicherheit des Gesamtsystems zu erhalten. Außerdem gilt es zu klären, wie Systemarchitekturen auch nicht-vertrauenswürdige oder unveränderbare Komponenten sicher integrieren können. Deshalb sollte darüber hinaus eine übergeordnete Metrik entwickelt werden, die eine Bewertung eines Systems inklusive deren Komponenten hinsichtlich IT-Sicherheitsmechanismen vornehmen kann.

Langzeitsicherheit kann nur ermöglicht werden, wenn auch die Sicherheit gegen Angriffe von Quantencomputern schon jetzt mit erforscht wird. Sollte der Durchbruch im Bereich der Quantencomputer gelingen, werden diese um Größenordnungen schneller als herkömmliche PCs und auch Großrechner sein. Quantencomputer wären dann in der Lage, verschiedene Arten von bisher existierenden Verschlüsselungssystemen zu brechen, die bislang als sicher gelten. Die Erforschung und Entwicklung von neuen, gegen Quantencomputer-Angriffe sichere, kryptographische Algorithmen muss bereits jetzt vorangetrieben werden, um auch künftig gegen neue Angriffsmethoden geschützt zu sein. Offene Forschungsfragen / -bereiche sind beispielsweise die Entwicklung neuer Verschlüsselungsmethoden, u. a. basierend auf Gittern oder Problemen wie *Learning with Errors* (LWE), die Entwicklung von Methoden, um kurz- und langfristige kryptographischen Schutz von Nachrichten zu gewährleisten (*Crypto Agility*) und die Erforschung und Vermeidung von Seitenkanal-Angriffen, die in der Lage sind, Kryptographie zu umgehen.

b) Sicherheit für künstliche Intelligenz

Die Fortschritte im Bereich der künstlichen Intelligenz stellt die IT-Sicherheitsforschung vor völlig neue Herausforderungen. Autonome Systeme (Fahrzeuge, Roboter, Softwaresysteme) haben ein (mehr oder weniger) ausgeprägtes Verständnis der eigenen Aufgaben und Fähigkeiten, weshalb sie Ursache und Wirkung der eigenen Aktionen beurteilen können und selbstständig Handlungsentscheidungen treffen können. Es besteht die Gefahr, dass ein nicht-intendiertes Außerkraftsetzen der IT-Sicherheit die Sicherheit der Nutzer und Produktionsabläufe gefährdet. Durch das hohe Maß an Eigenständigkeit und Flexibilität bieten autonome Systeme neue, bislang unbekannte und unerforschte Einfallstore von außen. Es gibt in diesem Bereich noch zahlreiche offene Fragen: Wie kann sichergestellt werden, dass autonome Systeme die Qualität der Daten richtig beurteilen? Wie können selbstlernende Systeme vor simulierten oder manipulierten Außeninformationen geschützt werden? Ziel ist es, Sicherheitsstufen von autonomen Systemen zu identifizieren und zu definieren. Hierzu gilt es u.a. zu erforschen, ob die

Unterteilung eines autonomen Systems in mehrere Subsysteme sinnvoll sein kann, so dass sich die Subsysteme dann in gewissem Maß gegenseitig kontrollieren. Hierfür braucht es revisionsfähige Systeme und austauschbare Softwarekomponenten für autonome Systeme.

Eine zweite Herausforderung ergibt sich durch den verstärkten Einsatz subsymbolischer Techniken wie etwa tiefer neuronaler Netze, die zum Beispiel in der Bild- und Sprachverarbeitung den Stand der Technik darstellen: diese agieren weitgehend als Black-Box Softwarekomponenten, so dass insbesondere in realen dynamischen Umgebungen keine zuverlässigen Sicherheitsgarantien gegeben werden können, und hier bei im Training nicht abgedeckten Bereichen zum Teil höchst überraschende Effekte eintreten können. Gleichzeitig sind die Verfahren aufgrund ihrer Performanz in vielen Bereichen unverzichtbar. Hier stellt sich die Herausforderung, neuartige Sicherheitskonzepte zu entwickeln, welche die zuverlässige Funktionalität dieser Verfahren auch in sich ändernden Umgebungen garantieren und ihre Limitationen explizit benennen können, etwa durch die Integration von Zusicherungen im Rahmen von Greybox-Modellen, die Substantiierung durch für den Menschen interpretierbare Erklärungskomponenten, oder die Integration neuartiger Technologien des Maschinellen Lernens im Kontext von Konzept-Drift.

c) IT-Sicherheit in sozio-technischen Systemen

Neben der technischen und physikalischen Komponente ist der Faktor Mensch auch in großen Systemen von herausragender Bedeutung. In sozio-technischen Systemen von Systemen (Cyber-Physical-Social-Systems) fehlt es bislang an Lösungen und ganzheitlichen Betrachtungen. An dieser Stelle ist interdisziplinäre Forschung notwendig, um die neu entstehenden Risiken in sozio-technischen Systemen zu identifizieren, zu analysieren und zu beseitigen. Beispielsweise muss ein tiefgründiges Verständnis entwickelt werden für die verschiedenen Rollen, die Menschen in einem solchen sozitechnischen System einnehmen: Menschen können IT-Sicherheit unterstützen, indem sie beispielsweise Vorfälle erkennen, melden oder mitigieren, sie können aber auch als Angreifer oder gar Innentäter der IT-Sicherheit entgegenwirken. Durch Social Engineering-Angriffe wiederum können eigentlich

positiv gesinnte Menschen arglistig durch einen Angreifer dazu gebracht werden, die IT-Sicherheit zu schwächen. Es bedarf qualitativer und quantitativer Methoden, um Sicherheit und Unsicherheit in solchen Szenarien messbar zu machen, und um fundierte, dynamische Risikomodelle zu entwickeln. Das Zusammenspiel des technischen Designs, rechtlicher Regulierung, ethischer Fragestellungen und die Interaktion zwischen Mensch und Wirtschaft gilt es künftig umfassend zu erforschen.

Eine besondere Herausforderung entsteht hier durch die Tatsache, dass ein Verständnis des Nutzerverhaltens relevant ist, um einerseits das zu erwartende Verhalten von Nutzern und damit verbundene potentielle Schwachstellen zuverlässig identifizieren zu können. Andererseits ist diese Einsicht nötig, um technische Softwaresysteme so zu entwerfen, dass sie mit der menschlichen Intuition kompatibel sind, um so Fehler aufgrund von beim Nutzer vorliegenden Fehlvorstellungen zu minimieren. Es besteht also die Herausforderung, verlässliche Konzepte und Designprinzipien kognitiver Interaktion für Cyber-Physical-Social-Systems zu entwerfen.

2.2. Mittelfristige Herausforderungen

Usable Security

Bislang ist der Faktor Mensch wesentlich an Sicherheitslücken in Systemen beteiligt. Abgesehen von fehlender Security-Awareness führen häufig Bedienfehler zu Systemausfällen. Auch entstehen Sicherheitslücken häufig durch Fehler bei der Softwareentwicklung oder bei der Konfiguration von Systemen durch Administratoren und Integratoren, die z. B. durch zu kompliziert zu benutzende Softwarebibliotheken für Sicherheitsfunktionen (Security Code) oder unübersichtliche Konfigurationsdialoge begünstigt werden. Deshalb gilt es zu erforschen, wie die Usability von IT-Sicherheit systemisch auf allen Ebenen verbessert werden kann. Und: Wie kann die Systemelastizität gegenüber Bedienfehlern erhöht werden?

2.3. Aktuelle Innovationsbedarfe

a) Cloud-Sicherheit:

Cloud-Lösungen kommen im Umfeld von Industrie 4.0 bereits häufig zum Einsatz, da sie erlauben, Daten zentral zu speichern und wiederum dezentral abzurufen und auszuwerten. Der Bitkom ermittelte, dass rund 65 Prozent der deutschen Unternehmen im Jahr 2016 die Möglichkeit nutzten, Software, Speicher oder Rechenleistung aus der Cloud zu nutzen. Die Anforderungen an Cloud-Dienste sind hoch: die Verfügbarkeit der Dienste und Daten soll garantiert werden, ebenso die Unversehrtheit der Daten und ihre Geheimhaltung.

Gerade im Umfeld der industriellen Produktion ist außerdem momentan der Trend zu beobachten, dass nicht nur die oberen Schichten der IT-Hierarchie sondern zunehmend bis hinunter auf die unterste Ebene (Feldbusse, etc.) Steueranlagen mit der Cloud verbunden werden. Diesbezüglich gilt es zum einen, die Notwendigkeit solcher Maßnahmen zu bewerten und gegen die hieraus entstehenden Probleme und Unsicherheiten abzuwägen. Des Weiteren kommen für Cloudverbindungen in der industriellen Produktion zunehmend neuartige Protokolle zum Einsatz, wie beispielsweise OPC UA. Die Sicherheit dieser Protokolle war bisher nicht hinreichend Gegenstand der IT-Sicherheitsforschung. Außerdem können auch diese Protokolle fehlerhaft in Softwarekomponenten verwendet werden. Man muss daher erforschen, wie sich solche Fehler auf Nutzerseite systematisch verhindern lassen.

b) Moderne Authentifizierungsverfahren

Moderne Authentifizierungsverfahren sind in Zeiten von Internet of Things und anderen IT-Infrastrukturen mit Tausenden bis Millionen von Nutzern unerlässlich. Auch eine sichere Realisierung von E-Government Lösungen setzt geeignete und robuste Authentifizierungsverfahren voraus.

Da klassische Authentifizierungsverfahren auf eine eindeutige Identifikation individueller Nutzer abzielen, widerspricht “sichere Authentifizierung" jedoch

oftmals dem Ziel, die Privatsphäre von Nutzern zu schützen. Die eindeutige Identifikation von Individuen macht es möglich, dass sehr genaue Bewegungsprofile von Nutzern erstellt werden können.

Aufgrund von Akzeptanzhürden und durch den Nutzerwunsch nach besserem Datenschutz stellt dies ein Hindernis dar, welches insbesondere die Digitalisierung von Anwendungen erschwert, bei denen Nutzer mobil sind und Authentifizierungsvorgänge von ihrem jeweiligen Aufenthaltsort aus durchführen. Das ist zum Beispiel in modernen Crowd Sensing Systemen, Car-2-Grid Lösungen oder digitalen Bezahlsystemen für den Personennahverkehr der Fall.

In den letzten Jahren wurden mit sehr großem Erfolg die Grundlagen für neue Verfahren entwickelt, welche sichere Authentifikation ermöglichen und gleichzeitig die Privatsphäre von Nutzern effektiv schützen können. Dazu gehören zum Beispiel *attributbasierte* Authentifizierungsprotokolle. Der technologische Reifegrad dieser Verfahren überschreitet gerade die Schwelle der praktischen Einsetzbarkeit und bietet dadurch ein immenses Innovationspotenzial.

Um jedoch erfolgreich für die Entwicklung innovativer Lösungen einsetzbar sein zu können, müssen diese Techniken nun für Anwendungsentwickler zugänglich gemacht werden. Durch Entwicklung geeigneter Proof-of-Concept und Demonstrator-Realisierungen muss praktische Erfahrung in der Umsetzung dieser innovativen Techniken gesammelt werden. Dies ermöglicht innovative Anwendungskonzepte, welche die Privatheit von Bürgern in einer zunehmend digitalisierten Gesellschaft effektiv schützen.

c) Datenschutz durch Technik

Großes Innovationspotenzial besteht auch im Bereich des Datenschutzes durch Technik, z. B. durch die EU-Datenschutzgrundverordnung, die im Mai 2018 in Kraft tritt. Hierbei gilt es, Unternehmen darin zu befähigen, angemessene Lösungen zum Privacy Preserving Data Mining aktiv umzusetzen. Dabei muss auch die Frage beantwortet werden, wie Daten sinnvoll anonymisiert

werden, so dass keine Rückschlüsse auf Einzelpersonen durch Data Mining Verfahren möglich sind.

d) Security and Privacy by Design

Gerade Cyber Physical Systems sind oft auf eine Nutzungsdauer von mehreren Jahrzehnten hin ausgelegt. Zudem ist die in ihnen enthaltene Software oft nur schwer zu aktualisieren, da die Systeme beispielsweise in Echtzeitregelungen eingebunden sind, die nicht einfach unterbrochen werden können. Diese Eigenschaften machen es umso wichtiger, die Notwendigkeit für Software- oder gar Hardwareaktualisierungen so gering wie nötig zu halten. Der einzige Weg, dies zu erreichen ist ein systematischer Systems Engineering-Prozess, der Privacy by Design berücksichtigt. Dabei ist beispielsweise zu erforschen, wie Bedrohungsanalysen für CPS systematisiert werden können. Ebenso benötigen Anwender in der Praxis einfach anwendbare architekturelle Entwurfsmuster, die das jeweilige Softwaresystem nachweislich mit bestimmten Privacy- und Security-Eigenschaften ausstatten. Insbesondere sind hier Werkzeuge notwendig, um Softwarekomponenten modularer zu gestalten, so dass Einzelmodule mit den jeweils geringstmöglichen Privilegien ausgeführt werden können.

Auf Ebene des Programmcode ist *Security Code* von *Secure Code* zu unterscheiden. Security Code implementiert Security-Features (beispielsweise Kryptografie oder Zugriffskontrolle). Hierbei müssen Methoden und Werkzeuge erforscht werden, um die korrekte Implementierung aber vor allem auch Nutzung dieser Features sicherzustellen. Zudem muss der gesamte Softwarestack mit Secure Code implementiert werden. Das heißt, man muss Methoden und Werkzeuge erforschen, um bei der Programmierung dieser Software gängige Softwareschwachstellen systematisch zu vermeiden.

Um eine sicherere Separierung einzelner Softwareschichten zu erreichen, ist es vonnöten, Mittel und Wege zu erforschen, die es erlauben, Daten durchgängig und dennoch effizient auf jeder einzelnen Softwareschicht zu verschlüsseln. So sind beispielsweise Daten in der Applikationsschicht auch dann noch gesichert, wenn das Dateisystem kompromittiert wird.

Ein weiteres wichtiges Thema in Verbindung mit der Problematik der Langzeitsicherheit ist die Sicherstellung der durchgängigen Aktualisierbarkeit von Software. Hierzu bedarf es weiterer Forschung, wie man auch langfristig sichere Updatekanäle schaffen kann, die nicht von Dritten kompromittiert werden können.

e) Blockchain

Damit eine Blockchain sicher und vertrauenswürdig langfristig genutzt werden kann, müssen die folgenden Aspekte weiter erforscht werden:

Das verwendete Public-Key-Verfahren und Hashfunktionen müssen dem Stand der Technik genügen und neue Verfahren und passende Schlüssellängen müssen entsprechend regelmäßig angepasst werden. Dies ist bei Blockchains eine besondere Herausforderung, da diese ohne zentrale Instanz arbeiten. Dazu müssen geeignete Konzepte und Mechanismen erforscht werden.

Die Sicherheit der Blockchain-Technologie hängt auch von der Geheimhaltung der privaten Schlüssel der Public-Key-Verfahren in der Wallet ab. Der private Schlüssel muss immer geheim bleiben. Der Schutz des privaten Schlüssels selber sollte mit Hilfe von modernen Hardware-Security-Modulen realisiert werden. Zusätzlich muss eine unberechtigte Nutzung aktiv verhindert werden. Für die unberechtigte Nutzung von Schlüsseln müssen geeignete Protokolle und Konzepte erforscht werden.

Zusätzlich werden für die unterschiedlichen Anwendungen passende Konsensfindungsverfahren für die Vertrauensbildung notwendig, deren Randbedingungen kontinuierlich überprüft werden müssen.

Wenn die Blockchain an sich eine hohe Sicherheit bietet, werden die Angreifer über die eigentliche Anwendung, die die Blockchain nutzt, angreifen. Daher muss auch die Blockchain-Anwendung manipulationssicher sein, damit keine erfolgreichen Angriffe umgesetzt werden können. Dazu müssen Konzepte und Schnittstellen, z. B. vertrauenswürdige Blockchain-Viewer, erforscht werden.

Zwei Herausforderungen erschweren derzeit den nachhaltigen Einsatz von Blockchain-Technologie:

1. Der immense Energieverbrauch von Proof-of-Work-basierten Blockchains stellt versteckte Kosten bei Nutzung von Blockchaintechnologie dar und wird derzeit sogar als Gefahr für die Erreichung von Klimazielen angesehen: Alleine der Energieverbrauch der größten Kryptowährung Bitcoin ist derzeit ungefähr vergleichbar mit dem Energieverbrauch von ganz Neuseeland und steigt stetig. Dies entspricht einem Energieverbrauch von ungefähr 346 KWh pro durchgeführter Bitcoin-Transaktion.[vi] Um das Potenzial von Blockchains nachhaltig nutzen zu können, müssen daher alternative Ansätze entwickelt und untersucht werden. Vielversprechende Kandidaten dafür sind Proof-of-Stake basierte Blockchains oder alternative Konsensprotokolle.
2. Aufgrund des großen Interesses an Kryptowährungen stiegen die Auslastung des Netzwerkes und die Transaktionsgebühren vieler Währungen kürzlich derart an, dass sie aktuell kaum als Zahlungsmittel genutzt werden können. Hier werden Lösungen gebraucht, die es erlauben, Blockchain-basierte Kryptowährungen langfristig praktisch einzusetzen.

Blockchains bieten durch ihre dezentralisierte Infrastruktur und der Möglichkeit der Nutzung von Smart Contracts ein immenses Potenzial zur Realisierung smarter Cyber Physical Systems. Durch Lösung der beschriebenen Probleme kann dieses Potenzial genutzt werden.

3. Einschätzung durch die Wirtschaft

Der Digitalisierungsprozess wird weiter voranschreiten. Immer mehr Branchen in der Industrie, Handwerksbetriebe und kommunale Einrichtungen werden die Vorteile der zunehmenden Digitalisierung nutzen. Den Mehrwerten der neuen technischen Möglichkeiten stehen aber auch zunehmende Herausforderungen gegenüber. Der volkswirtschaftliche Schaden durch fehlende IT-Sicherheit ist enorm.

Dass die Bereitschaft zum Schutz des eigenen Unternehmens durchaus vorhanden ist, zeigen die Ergebnisse einer Befragung von CPS.HUB NRW, networker NRW und Bitkom vom Sommer 2016. Darin schätzten die nordrhein-westfälischen Unternehmen den Themenkomplex IT-Sicherheit als sehr wichtig ein. Ebenfalls zeigte sich, dass die Bereitschaft zur Investition auf Unternehmensseite groß ist. Insbesondere zielen Unternehmen darauf ab, eine langfristige IT-Sicherheitsstrategie zu entwickeln, enge Kooperationen mit geeigneten Dienstleistern einzugehen oder gut ausgebildete, spezialisierte Mitarbeiter einzustellen. Datenschutz, Sensibilisierung von Mitarbeitern, Schadsoftware im Web und Verschlüsselung von Daten haben laut der Befragung den höchsten Stellenwert bei den IT-Sicherheitsthemen. Die Erwartungen der Wirtschaft an das Land Nordrhein-Westfalen sind vor allem die Durchführung von Sicherheitsinitiativen, der Ausbau der Förderung für Forschung und Entwicklung, Medienkampagnen zur Sensibilisierung der Anwender und die Erhöhung der Nutzerakzeptanz von IT-Sicherheit.

Darüber hinaus sind die Entwicklung einer Weiterbildungsplattform im Bereich IT-Sicherheit sowie vorgelagerte Aktivitäten wie die Stärkung der Digitalkompetenz inklusive der IT-Sicherheit bereits in den Schulen und Hochschulen empfehlenswert.

Nordrhein-Westfalen hat zahlreiche Unternehmen, die im Bereich IT-Sicherheit aktiv sind und Produkte sowie Dienstleistungen auf dem modernsten

Stand der Technik anbieten. Das gute und enge Zusammenspiel zwischen Wirtschaft und Wissenschaft wird künftig noch wichtiger und ein wesentlicher Baustein für den weiteren Erfolg der Unternehmen sein. Die bislang geschaffenen Strukturen und Netzwerke bilden dazu eine hervorragende Ausgangslage, die es gilt, künftig weiter auszubauen.

Im Rahmen eines weiteren Workshops mit ausgewählten Experten der IT-Security-Branche Nordrhein-Westfalens wurden aus domänenspezifischer Sichtweise die Chancen und Herausforderungen identifiziert und analysiert. Perspektivisch wurde erarbeitet, wie sich die IT-Security Branche als Leitmarkt für Nordrhein-Westfalen weiter etablieren kann.
Folgende Ergebnisse spiegeln die domänenspezifische Sichtweise der IT-Sicherheitsexperten aus der Wirtschaft wider:

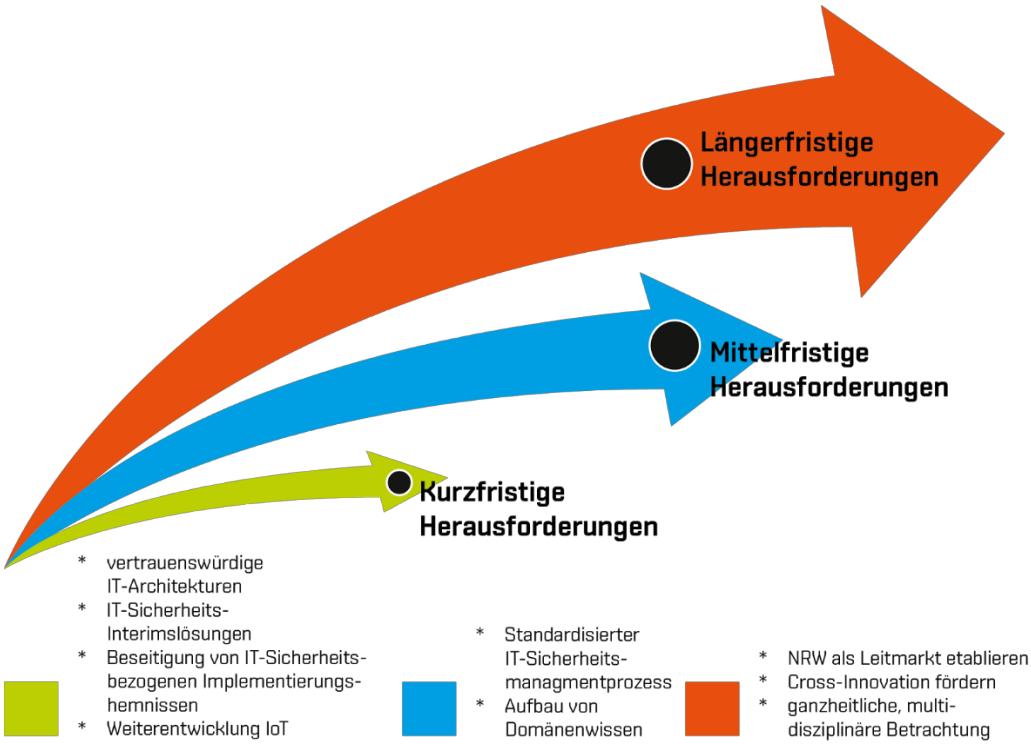

Abbildung 2: Einschätzungen durch die Wirtschaft - Die Herausforderungen im zeitlichen Horizont. Eigene Darstellung.

3.1. Längerfristige Herausforderungen

Nordrhein-Westfalen ist bereits das führende Bundesland für IoT und industrielle Produktion. Jetzt bietet sich die Chance, NRW auch als Leitmarkt für IT-Sicherheitslösungen bekannter zu machen. Hierzu gilt es, Cross-Innovationen oder die Entwicklung von IT-Sicherheitslösungen gezielt vorantreiben zu können. NRW soll eine Führungsrolle auf dem Gebiet der IT-Sicherheit beanspruchen, deshalb bedarf es einer ganzheitlichen, multidisziplinären Betrachtung: technische, ethische, wirtschaftliche, politische und gesellschaftliche Herausforderungen müssen erarbeitet werden.

3.2. Mittelfristige Herausforderungen

Bislang können Wirtschaft und Gesellschaft nicht auf einen standardisierten IT-Sicherheitsmanagementprozess zurückgreifen, es fehlt schlichtweg an Standards. Die schnelle Weiterentwicklung von aktuellen IT-Sicherheitslösungen und standardisierten IT-Sicherheitsmanagementprozessen ist daher dringend erforderlich. Hierzu gilt es, die Kooperation von nordrhein-westfälischen IT-Unternehmen proaktiv zu fördern, um auf diese Weise Synergieeffekte durch Domänenwissen zu nutzen. Um die Weiterentwicklung von aktuellen IT-Sicherheitslösungen vorantreiben zu können, braucht es zudem eine bessere Markttransparenz insbesondere für KMU, um die Qualität von Software im Hinblick auf ihre Sicherheit schnellstmöglich zu verbessern. Offene Fragen sind u. a.: Wie kann ein Maßnahmen- / Kriterienkatalog entwickelt werden, der Mindeststandards und -anforderungen für IT-Sicherheitslösungen formuliert? Wie kann Domänenwissen geschaffen werden? Wo liegen aktuell die technischen Grenzen von IT-Sicherheitslösungen?

3.3. Aktuelle Innovationsbedarfe

Die Komplexität der technologischen, wirtschaftlichen und gesellschaftlichen Handlungsfelder erzeugt insbesondere bei Unternehmen einen hohen Innovationsdruck. Sie benötigen innovative, sichere und vertrauenswürdige IT-Architekturen, um den Digitalisierungsprozess erfolgreich und nachhaltig umsetzen zu können. Dabei sind neue Ansätze aus dem Feld künstliche Intelligenz (maschinelles Lernen, Datenanalyse u.v.m.) vielversprechend, erfordern aber noch intensive F&E-Aktivitäten bis zur Marktreife. So ist auch die Frage zu klären, welche sinnvollen Interimslösungen es bis zur Marktreife geben kann. Die rasant verlaufende Vernetzung zu Cyber Physical Production Systems (CPPS), Industrie 4.0 und Industrial Internet, die Weiterentwicklung des Internet of Things, Internet of Services und Internet of Everything erfordert neue, große technische Systeme von Systemen umfassende Ansätze als integrale Cyber Physical Security Konzepte. Eine entscheidende Frage ist dabei, wie vorhandene IT-Sicherheits-bezogene Implementierungshemmnisse im Bereich von Industrie 4.0 und Cyber Physical Production Systems identifiziert und beseitigt werden können. Ebenso gilt es zu analysieren, wie die Weiterentwicklung des Internet of Things, Internet of Services und Internet of Everythings langfristig gesichert werden kann, um den daraus entstehenden Wettbewerbsvorteil für NRW nutzbar zu machen.

4. LITERATURVERZEICHNIS

[1] Gartner, Inc. (2017): Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016. Unter: https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016, Zugriffsdatum: 12.06.2018.

[2] Bitkom Research (2017): Wirtschaftsschutz in der digitalen Welt. Unter: https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/07-Juli/Bitkom-Charts-Wirtschaftsschutz-in-der-digitalen-Welt-21-07-2017.pdf, Zugriffsdatum: 13. Juni 2018.

[3] Bitkom e. V. (2018): Attacken auf deutsche Industrie verursachten 43 Milliarden Euro Schaden. Unter: https://www.bitkom.org/Presse/Presseinformation/Attacken-auf-deutsche-Industrie-verursachten-43-Milliarden-Euro-Schaden.html, Zugriffsdatum: 19.09.2018.

[4] nrw.uniTS (2018): Netzwerkpartner für IT-Sicherheit. Unter: https://www.nrw-units.de/nrw-units/, Zugriffsdatum: 13. Juni 2018.

[5] „Marktplatz IT-Sicherheit (2018): Anbieterverzeichnis. Unter: https://www.it-sicherheit.de/de/anbieter/anbieter-suchen/, Zugriffsdatum: 14.06.2018.

[6] Digiconomist (2018): Bitcoin Energy Consumption Index. Unter: https://digiconomist.net/bitcoin-energy-consumption, Zugriffsdatum: 14.06.2018.