IT-Sicherheit für Kritische Infrastrukturen

Steffi Rudel[1] · Matthias Rass[2] · Max Jalowski[2]

[1]Universität der Bundeswehr München
steffi.rudel@unibw.de

[2]Friedrich-Alexander-Universität Erlangen-Nürnberg
{matthias.rass | max.jalowski}@fau.de

Zusammenfassung

Durch die zunehmende Digitalisierung und Vernetzung gewinnt auch die Sicherheit der zugrundeliegenden Informationstechnik an Bedeutung. Besondere Relevanz haben hierbei die *Kritischen Infrastrukturen*. Aus diesem Grund gibt es den Förderschwerpunkt „IT-Sicherheit für Kritische Infrastrukturen“ (ITS|KRITIS) des Bundesministeriums für Bildung und Forschung (BMBF), in dem 13 Projekte an Maßnahmen und Werkzeugen zum Schutz der *Kritischen Infrastrukturen* in Deutschland forschen. Teil dieses Förderschwerpunkts ist das Begleitforschungsprojekt „Vernetzte IT-Sicherheit Kritischer Infrastrukturen“ (VeSiKi). Der vorliegende Beitrag gibt zunächst einen Überblick über die Arbeitsschwerpunkte der Verbundprojekte im Förderschwerpunkt ITS|KRITIS. Anschließend werden verschiedene Werkzeuge und Maßnahmen zur Vernetzung der Verbundprojekte durch das Begleitforschungsprojekt VeSiKi vorgestellt. Ein Einblick in die praxisnahe Forschung von VeSiKi rundet den Beitrag ab.

1 Einleitung und Motivation

Die fortschreitende Digitalisierung in Gesellschaft und Arbeitswelt birgt zahlreiche Potenziale, bringt aber auch eine Reihe neuer Herausforderungen mit sich. Je stärker sich Menschen und Organisationen in ihrem Alltag auf Informationstechnik (IT) verlassen, desto mehr rückt die Frage der Sicherheit dieser Technik in den Fokus. Dabei geht es sowohl um ein fehlerfreies Funktionieren als auch um den Schutz dieser Technologien vor gezielten Angriffen. Besonders bedeutend sind diese Themen in Bezug auf die IT-Sicherheit in *Kritischen Infrastrukturen* (KRITIS). Solche *Kritischen Infrastrukturen* sind Institutionen, die für die Aufrechterhaltung des täglichen Lebens wichtig sind [Gesc14], wie bspw. Energieversorger, Wasserversorger, Lebensmittelhandel oder auch Banken [BuBu09].

Fragen wie „Welchen besonderen Schutz benötigen Kritische Infrastrukturen?" und „Was ist zu tun, wenn eine Kritische Infrastruktur aufgrund eines Sicherheitsvorfalls nur noch eingeschränkt zur Verfügung steht oder gar vollständig ausfällt?“ sind nicht erst seit dem 2015 in Kraft getretenen IT-Sicherheitsgesetz [Bund15] drängend. Diese Themen finden aktuell jedoch zunehmend die Beachtung der Öffentlichkeit.

P. Schartner · A. Baumann (Hrsg.) · D•A•CH Security 2017 · syssec (2017) 269-277.

Kritische Infrastrukturen stelle die IT-Sicherheit häufig vor besondere Herausforderungen. So sind beispielsweise Legacy-Systeme in bestimmten Bereichen weniger die Ausnahme als vielmehr die Regel. Umso wichtiger ist hier die ganzheitliche Betrachtung der Faktoren Technik, Organisation und Mensch.

Bereits seit 2015 existiert der vom Bundesministerium für Bildung und Forschung (BMBF) etablierte Förderschwerpunkt „IT-Sicherheit für Kritische Infrastrukturen“, kurz ITS|KRITIS. In diesem Förderschwerpunkt arbeiten Forscher sowie Entwickler und Anwender von IT-Sicherheitslösungen für den Bereich *Kritischer Infrastrukturen* in 13 Verbundprojekten zusammen und adressieren dabei die relevanten Teilaspekte Technik, Organisation und Mensch jeweils aus verschiedenen Perspektiven. Eines dieser Projekte ist das Begleitforschungsprojekt „Vernetzte IT-Sicherheit Kritischer Infrastrukturen“ (VeSiKi).

2 Die Verbundprojekte im Förderschwerpunkt

Im Förderschwerpunkt ITS|KRITIS sind (neben der Begleitforschung VeSiKi) die Verbundprojekte AQUA-IT-Lab, Cyber-Safe, INDI, ITS.APT, MoSaIK, PREVENT, PortSec, RiskViz, SecMaaS, SICIA, SIDATE und SURF vertreten. Diese Verbundprojekte forschen mit unterschiedlichen Schwerpunkten und Zielstellungen in verschiedenen Bereichen für die IT-Sicherheit von *Kritischen Infrastrukturen*.

Das Projekt AQUA-IT-Lab setzt seinen Fokus insbesondere auf die Entwicklung von Lösungsansätzen zum Schutz vor Cyber-Angriffen für kleine und mittlere Betreiber von *Kritischen Infrastrukturen* am Beispiel der Wasserversorgung. In dem Projekt arbeiten die Projektpartner Universität Potsdam, HiSolutions GA, Pretherm GmbH, Stadtwerke Brandenburg/Havel GmbH, Wasser- und Abwasserzweckverband Calau, Berliner Wasserbetriebe und Abwasser Calau (WAC) zusammen.

Das Projekt Cyber-Safe fokussiert in seiner Forschung auf die Erhöhung der IT-Sicherheit in Verkehrsleitzentralen und den Schutz vor Cyber-Angriffen. In dem Projekt arbeiten die Projektpartner Bundesanstalt für Straßenwesen (BASt), STUVA e.V., Ruhr-Universität Bochum, Landesbetrieb Straßenbau NRW sowie DÜRR Group GmbH zusammen.

Das Projekt INDI besteht aus den Projektpartnern Technische Universität Braunschweig, Brandenburgische Technische Universität Cottbus-Senftenberg, genua GmbH sowie Vattenfall Europe Generation KG und hat sich der Erforschung einer neuartigen Technologie zur Erkennung und Eindämmung von Cyber-Angriffen in Industrienetzwerken verschrieben.

Im Projekt ITS.APT forschen die Projektpartner ERNW Enno Rey Netzwerke GmbH, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Universität Bonn, Universität Duisburg-Essen, Westfälische Wilhelms-Universität Münster sowie das Universitätsklinikum Schleswig-Holstein zusammen an einer Erweiterung klassischer Testmethoden für die Bewertung der IT-Sicherheit durch das Einbeziehen des Sicherheitsbewusstseins durch den Benutzer.

Im Projekt MoSaIK wird an Methoden für eine effiziente Risikoanalyse *Kritischer Infrastrukturen* und der Bewertung des Sicherheitsniveaus geforscht. In dem Projekt arbeiten die Projektpartner Stadtwerk Haßfurt, m-privacy, Stadt Gera sowie das Fraunhofer AISEC zusammen.

Das Projekt PREVENT vereint die Projektpartner Wincor NIXDORF, xiv-consult, Fraunhofer FOKUS und UniCredit. Zusammen wird an der Konzeption, Entwicklung und Implementierung einer in Rechenzentren integrierbaren Software für präventives Risiko- und Krisenmanagement gearbeitet.

Das Projekt PortSec befasst sich mit der Erforschung eines systematischen und umfassenden IT-Risikomanagements in der Hafentelematik. Als Projektpartner arbeiten hier ISL Institut für Seeverkehrswirtschaft und Logistik, dbh Logistics IT AG, datenschutz cert GmbH sowie die Universität Bremen zusammen.

Im Projekt RiskViz forschen die Projektpartner Hochschule Augsburg, Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH (BIGS), Munich RE AG, Technologie Centrum Westbayern, genua GmbH, LEW Verteilnetz GmbH, KORAMIS GmbH sowie die Freie Universität Berlin zusammen an einer Suchmaschine zum Auffinden industrieller Kontrollsysteme (ICS) und zur Bewertung der Risiken.

Das Projekt SecMaaS erarbeitet im Konsortium mit den Projektpartnern Stadt Saarbrücken, KommWIS GmbH, Hochschule Darmstadt, Stadt Siegburg sowie der Bundesdruckerei GmbH an Lösungswegen für die Gewährleistung von IT-Sicherheit in der öffentlichen Verwaltung.

SICIA ist ein Projekt der Partner Brandenburgische Technische Universität Cottbus-Senftenberg, LEAG Lausitz Energie Kraftwerke AG, RWE AG und innogy SE und entwickelt ein neuartiges Verfahren zur Ermittlung des Ist-Zustandes der IT-Sicherheit bis auf die Geräteebene.

Im Projekt SIDATE werden Konzepte und Werkzeuge für eine schnelle Einschätzung und Verbesserung des vorhandenen Sicherheitsniveaus besonders für kleine und mittlere Energiebetreiber erforscht. Hier arbeiten die Projektpartner Universität Siegen, Goethe-Universität Frankfurt, Regio iT, TÜV Rheinland i-sec GmbH und die ASEW zusammen.

Das Projekt SURF besteht aus den Projektpartnern Airbus Defence, Flughafen München, Fraunhofer SIT, Hirschmann, Infineon Technologies AG, Technische Hochschule Deggendorf und der Technischen Universität München und befasst sich mit der Entwicklung einer ganzheitlichen Lösung zur Verbesserung der Schutzsysteme in *Kritischen Infrastrukturen*.

3 Das Begleitforschungsprojekt

Das Begleitforschungsprojekt VeSiKi vernetzt zum einen die Verbundprojekte im Förderschwerpunkt und unterstützt so den kooperativen Forschungsprozess. Zum anderen unterstützt VeSiKi die Außendarstellung des Förderschwerpunkts und die Sichtbarkeit der Aktivitäten und Ergebnisse in der Öffentlichkeit und damit den Transfer in die Praxis. Darüber hinaus leistet VeSiKi noch eigene, die Arbeiten der anderen Verbünde flankierende, Forschungsbeiträge.

Im Begleitforschungsprojekt VeSiKi arbeiten Forscher vom Institut für Informatik der Universität der Bundeswehr München, dem Lehrstuhl für Wirtschaftsinformatik, insbesondere Innovation und Wertschöpfung, der Friedrich-Alexander-Universität Erlangen-Nürnberg, dem Institut für Rechtswissenschaften der Universität Bremen sowie der Fachbereich Standardisierung und Innovation des DKE|VDE in Frankfurt zusammen.

3.1 Vernetzung der Verbundprojekte

Im Rahmen des Projekts VeSiKi wurde zur Unterstützung des Wissenstransfers sowohl innerhalb des Förderschwerpunkts als auch zwischen dem Förderschwerpunkt und der Öffentlichkeit die Plattform itskritis.de konzipiert und implementiert. Sie unterstützt Vernetzung, Kommunikation und Kollaboration und gliedert sich, den verschiedenen Aufgaben und Zielen des Projekts entsprechend, in einen öffentlichen und einen internen Bereich. Das Konzept der Bereiche mit seinen Kerninhalten ist in Abbildung 1 dargestellt.

Abb. 1: Übersicht über die zwei Bereiche der Vernetzungsplattform

Der öffentliche Bereich der Plattform dient primär der Präsentation des gesamten Förderschwerpunkts ITS|KRITIS nach außen. Die interessierte Öffentlichkeit sowie Betreiber *Kritischer Infrastrukturen* können sich hier über aktuelle Aktivitäten und bisherige Ergebnisse informieren oder eine Erstberatung zu bestimmten Themen einholen. Dafür steht aktuell z.B. eine Normenlandschaft mit relevanten Normen und Standards im Themenfeld IT-Sicherheit zur Verfügung. Zukünftig werden auch ein rechtlicher Überblick im Themenfeld, Fallstudien sowie Handlungsempfehlungen unter anderem zu Strategie und Innovation bereitgestellt. Außerdem bietet die Plattform eine Übersicht über relevante Einrichtungen und Personen im Themenfeld „IT-Sicherheit für Kritische Infrastrukturen“. Dies soll die Erstberatung ergänzen und die Herstellung eines Kontakts zu Organisationen und Experten erleichtern.

Diese Informationen sind auf den Gelben Seiten der Plattform abrufbar. Dort sind alle am Förderschwerpunkt beteiligten Einrichtungen und weitere relevante Organisationen hinterlegt. Zur erleichterten Auffindbarkeit sind alle Einträge mit Kategorien versehen und können mit Hilfe einer Tag Cloud und einer Suchmaske gefiltert werden. Abbildung 2 zeigt die Standorte beispielhafter Einrichtungen auf einer Landkarte.

Auf weiteren Service-Seiten werden Aktivitäten im Förderschwerpunkt aufbereitet, wie beispielsweise Informationen zu den etablierten Fachgruppen und der in Abschnitt 3.2 beschriebenen ergänzenden praxisnahen Forschung. Die Wegweiser-Sektion ergänzt die Gelben Seiten um tiefergehende Informationen zu aktuellen Thematiken, zum Beispiel Ransomware, und zu möglichen Ansprechpartnern. Ein Pressebereich bietet regelmäßig zusammenfassende Meldungen über den Fortschritt im gesamten Förderschwerpunkt.

Das Angebot wird durch eine Darstellung und Aufarbeitung der Ergebnisse, die im Rahmen des Projekts entstanden sind, abgerundet. So sind unter anderem die Broschüre des "Monitor

IT-Sicherheit Kritischer Infrastrukturen" (siehe dazu auch Abschnitt 3.2), Webinare der DKE zum Thema Normung und Standardisierung und rechtliche Beurteilungen frei verfügbar.

Abb. 2: Landkarte der Gelben Seiten

Für die Verbundprojekte des Förderschwerpunkts sind jeweils eigene Bereiche vorgesehen, die zentrale Informationen zu den jeweiligen Forschungsvorhaben bieten. Darüber hinaus können die Projekte über ihre Aktivitäten, Publikationen, Veranstaltungen und Forschungsergebnisse informieren. Die Plattform dient somit auch als Orientierungshilfe im Förderschwerpunkt und gibt Auskunft, wer zu welchen Themen arbeitet und Kompetenzen aufzuweisen hat.

Der interne Bereich der Vernetzungsplattform wendet sich vorrangig an die Mitglieder der im Förderschwerpunkt zusammengefassten Projekte und soll die Vernetzung aller Beteiligten unterstützen. Dazu wird zum Beispiel ein Kontaktverzeichnis aller angemeldeten Nutzer angeboten. Zusätzlich sind Informationen zur Projektzugehörigkeit sowie den eigenen Forschungsinteressen und Kompetenzen vorhanden.

Die zentralen Komponenten des internen Bereichs sind die Startseite und der Marktplatz. Auf der Startseite dieses internen Bereichs werden die aktuellsten für den Nutzer relevanten Informationen aus den verschiedenen Bereichen dargestellt. Ergänzend dazu werden bei jedem Aufruf verschiedene Personen als Kontaktvorschlag mit ihren Kompetenzen und Forschungsinteressen angezeigt.

Auf den Jahreskonferenzen wurden regelmäßig Suche-/Biete-Sessions angeboten, die auf der Webplattform weitergeführt werden. Der daraus entstandene Marktplatz ist ein Kernelement der Vernetzung innerhalb des Förderschwerpunkts. Er ist als Schwarzes Brett konzipiert, auf

dem die Nutzer Suche-/Biete-Anfragen und Stellenangebote teilen können (siehe Abbildung 3). Hierdurch wird beispielsweise die Suche nach Experten zu bestimmten Themengebieten oder nach Teilnehmern an einer Studie stark vereinfacht.

Abb. 3: Beispielhafte Anfrage auf dem Schwarzen Brett der Plattform

Als eine weitere Maßnahme zur Vernetzung werden durch VeSiKi gemeinsame wissenschaftliche Veröffentlichungen der Verbundprojekte gefördert. So entstand beispielsweise im Frühjahr 2017 ein Beitrag zur „Risikobeurteilung in der IT-Sicherheit Kritischer Infrastrukturen“ [GGK+17]. In dem Beitrag werden Methoden zur Risikobeurteilung im Förderschwerpunkt ITS|KRITIS durch mehrere Verbundprojekte vorgestellt. So wird vom Projekt MoSaIK eine Methode zur Risikoanalyse und -bewertung in KRITIS mit möglichst geringem Ressourcenaufwand für die Betreiber, vom Projekt AQUA-IT-Lab ein branchenspezifischer Schnelltest zur Bewertung der Sicherheit im KRITIS-Sektor Wasser und von PREVENT eine Methode und ein Werkzeug zum systematischen Risikomanagement für den operativen Betrieb von Banken vorgestellt.

3.2 Ergänzende, praxisnahe Forschung

Das Begleitforschungsprojekt VeSiKi wurde vom BMBF ins Leben gerufen, um die Verbundprojekte im Förderschwerpunkt ITS|KRITIS zu vernetzen und zu unterstützen. Darüber hinaus verfolgt VeSiKi eigene Forschungsziele.

So wurde vom Projektteam im Herbst 2016 eine Umfrage zur Lage der IT-Sicherheit in *Kritischen Infrastrukturen* durchgeführt. Die Ergebnisse dieser Umfrage wurden den Verbundprojekten sowie der Öffentlichkeit im Frühjahr 2017 über verschiedene Kanäle zugänglich gemacht [Lech17]. Genaueres zu der Umfrage wird in dem Beitrag "Monitor IT-Sicherheit Kritischer Infrastrukturen" von Tamara Gurschler, Sebastian Dännart und Ulrike Lechner dieses Konferenzbandes vorgestellt. Für die zweite Jahreshälfte 2017 ist ein weiterer, vertiefender Monitor geplant, dessen Ergebnisse sicherlich wieder für spannende Erkenntnisse und wertvolle Ausblicke in die Zukunft der *IT-Sicherheit für Kritische Infrastrukturen* sorgen werden.

Des Weiteren beschäftigen sich die Forscher in VeSiKi mit Open Innovation und den Herausforderungen und Potenzialen offener und kollaborativer Innovations- bzw. Forschungs- und

Entwicklungsprozesse. Open Innovation beschreibt ein Paradigma, in dem Organisationen ihren Innovationsprozess über die Organisationsgrenzen hinweg öffnen und sowohl Wissen und andere Ressourcen von externen Quellen einbeziehen als auch internes Wissen und interne Entwicklungen nicht intern weiter nutzen, sondern außerhalb der Organisation bzw. deren Markt kommerzialisieren [Ches03]. Bei den in Open-Innovation-Ansätzen relevanten Akteuren außerhalb der Organisation kann es sich beispielsweise um Forschungseinrichtungen, Zulieferer oder andere Unternehmen, gegebenenfalls sogar Konkurrenten handeln. Zunehmend erkennen Unternehmen auch die Bedeutung der Einbindung von Kunden und Nutzern in verschiedene Phasen des Innovationsprozesses. Manche Forscher sprechen hierbei auch von interaktiver Wertschöpfung [RePi09]. Ein weiteres Forschungsgebiet, das in diesem Zusammenhang von Relevanz ist, ist User Innovation. Hier wird weniger die Perspektive von Unternehmen eingenommen und mehr der Nutzer in den Vordergrund gestellt. Von Hippel [Hipp05] spricht von einer Demokratisierung der Innovation und beschreibt, wie Nutzer Lösungen für ihre eigenen Problemstellungen entwickeln und so Technologien, Produkte und Dienstleistungen entstehen, die letztlich für weitere Personenkreise relevant sind. Häufig arbeiten Nutzer dabei auch gemeinsam an Lösungen, so dass durch eine konkrete Problemstellung getrieben Netzwerke und Communities entstehen. Das Beispiel von Open Source Software Communities zeigt, wie hierbei markt- und konkurrenzfähige Lösungen entstehen können. Aktuelle Ansätze wie Crowdsourcing oder Citizen Science folgen in Teilen einem ähnlichen Prinzip wie die oben beschriebenen Konzepte und bauen darauf auf, Personen mit unterschiedlichen Hintergründen bei der Lösung von Problemen einzubinden. Die Beiträge bzw. Aufgaben jedes Einzelnen können dabei je nach Ausgestaltung sehr einfach aber auch sehr komplex sein.

Ein konkretes Beispiel für Projektaktivitäten im hier skizzierten Bereich ist die dreimonatige Präsenz in Form einer Themeninsel im JOSEPHS®, einem offenen Innovationslabor in der Nürnberger Innenstadt. Die Präsenz verfolgt dabei in erster Linie zwei Ziele. Einerseits soll das Bewusstsein für das für den Bürger eher abstrakte Thema erhöht und über die Aktivitäten des ITS|KRITIS-Förderschwerpunkts informiert werden. Andererseits werden die Besucher aktiv in Projektfragestellungen eingebunden und bringen ihre Ideen, Lösungsvorschläge und Ansichten ein. Die Themeninsel wird begleitet von einer Veranstaltungsreihe zum Thema IT-Sicherheit, in der mehrere Workshops, ein IT Security Matchplay, ein Live Hacking und ein IT Security Youth Camp verschiedene Teilaspekte adressieren.

Im Rahmen von VeSiKi wurden weiterhin die IT Security Matchplays als eine spielerische Methode entwickelt, Mitarbeiter für das Thema IT-Sicherheit zu sensibilisieren. Hier geht es insbesondere darum, die Kombination technischer Lösungen mit den Faktoren Organisation und Mensch zu beleuchten. Eine Ausprägung der IT Security Matchplays ist die "Operation Digitale Schlange", welche auf der Infrastruktur eines Krankenhauses basiert. Die *Operation Digitale Schlange* wurde im Mai 2017 an der Universität der Bundeswehr öffentlich mit Vertretern aus KRITIS sowie aus den Verbundprojekten gespielt. Für Ende 2017 ist eine weitere öffentliche Veranstaltung hierzu geplant. Ausführlicher werden die IT Security Matchplays in den Beiträgen [RHL+17] und [RuRi17] vorgestellt.

Um Betreibern von KRITIS sowie Unternehmen Good Practices an die Hand zu geben, wie IT-Sicherheit in *Kritischen Infrastrukturen* gut und praxisnah umgesetzt werden kann, werden von VeSiKi in Zusammenarbeit mit den Verbundprojekten Fallstudien erstellt. Die Fallstudien werden nach Fertigstellung auf der Vernetzungsplattform itskritis.de sowohl den Verbundprojekten als auch der Öffentlichkeit zur Verfügung gestellt. Die Fallstudien basieren auf der eXperience-Methodik [WöSQ07] und beleuchten eine Lösung praxisorientiert in verschiedenen Sichten. So wird die Geschäftssicht, die Prozesssicht, die Anwendungssicht und die technische Sicht nach

einem einheitlichen Fallstudienraster erläutert. Der Fokus der Fallstudien liegt zum einen darauf, Betreibern von KRITIS Beispiele an die Hand zu geben, zum anderen ist aber auch die Verwendung in der Hochschullehre vorgesehen. Hier eignen sich die Fallstudien ausgezeichnet, um Studenten bei der Verknüpfung der Theorie mit der Praxis zu unterstützen. Im Förderschwerpunkt entstanden so bisher unter anderem Fallstudien zum Thema sichere Fernwartung, zur Erstellung eines Lagebildes für das Management in Banken-Rechenzentren, zur Ransomware-Abwehr in Krankenhäusern oder auch zur Umsetzung von IT-Sicherheit in einer Kommune. Weitere Fallstudien sind bis Ende 2017 geplant.

Um insbesondere KMU, die im KRITIS-Bereich arbeiten, eine effektive und praxisnahe Hilfestellung bei der Anwendung von Rechtsvorschriften sowie technischen Normen und Standards im Bereich der IT-Sicherheit zu geben, wird vom VeSiKi-Team in Zusammenarbeit mit dem Deutschen Institut für Normung (DIN) in Berlin der IT Security Navigator erarbeitet. Dieser wird ebenfalls in die Vernetzungsplattform itskritis.de integriert.

Zusammen mit dem gesamten Förderschwerpunkt erstellt das VeSiKi-Team des Weiteren ein Rahmenwerk zur *IT-Sicherheit für Kritische Infrastrukturen*. In diesem Rahmenwerk werden nicht nur die Ergebnisse der Forschungsprojekte herausgestellt, sondern die relevanten Themen der IT-Sicherheit auch aus verschiedenen Blickwinkeln beleuchtet. Um sowohl Wissenschaftlern im Bereich IT-Sicherheit als auch Betreibern von KRITIS gerecht zu werden, wird das Rahmenwerk in fünf verschiedene Sektoren untergliedert werden. Die erste Sektion soll die 13 Forschungsprojekte im Förderschwerpunkt ITS|KRITIS sowie die Akteure in den Projekten genauer vorstellen. In der zweiten Sektion werden dann Bausteine, Gefährdungen und Maßnahmen (angelehnt an der Struktur der BSI-Grundschutzkataloge) beschrieben. Die Sektion drei geht auf die Sektorenspezifika der einzelnen KRITIS-Sektoren ein. Sektion vier adressiert den Transfer in die Praxis, hier wird beschrieben welche Werkzeuge und Maßnahmen die Forschungsprojekte des Förderschwerpunktes für den Transfer in die Praxis bereitstellen. In Sektion fünf werden abschließend Referenzimplementierungen aufgezeigt sowie ein Ausblick in die Zukunft gegeben.

4 Ausblick

Der Förderschwerpunkt ITS|KRITIS geht im Jahr 2017 auf die Zielgerade. In allen Verbundprojekten werden Lösungen und Ergebnisse für KRITIS erarbeitet – dabei legt jedes Projekt seinen Fokus auf die besonderen Bedürfnisse seiner Zielgruppe. Gerade der Transfer dieser erarbeiteten Lösungen in die Praxis macht den Förderschwerpunkt so interessant.

Mit der Plattform itskritis.de, den Fallstudien, dem Monitor, dem IT Security Navigator, dem Rahmenwerk sowie den weiteren Ergebnissen stellt die Begleitforschung des Projekts VeSiKi eine Vielzahl von Instrumenten zur Verfügung, um den Transfer der wissenschaftlich erarbeiteten Lösungen in die Praxis der Betreiber zu unterstützen und zu fördern.

Danksagung

Wir danken dem Bundesministerium für Bildung und Forschung (BMBF) für die Möglichkeit der Forschung im Rahmen des Projekts VeSiKi, Förderkennzeichen 16KIS0213 bis 16KIS0216.

Literatur

[BuBu09] Bundesamt für Sicherheit in der Informationstechnik; Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Hg.) (2009): Sektoren- und Brancheneinteilung Kritischer Infrastrukturen. Online verfügbar unter http://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/sektoren_node.html, zuletzt geprüft am 24.05.2017.

[Bund15] Bundestag (2015): Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). BSI-Gesetz. Online verfügbar unter https://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/it-sicherheitsgesetz.pdf?__blob=publicationFile, zuletzt geprüft am 24.05.2017.

[Ches03] Chesbrough, H. W. (2003). Open Innovation: The New Imperative for Creating and Profiting from Technology. Boston, MA: Harvard Business School Press.

[Gesc14] Geschäftsstelle des UP KRITIS (Hg.) (2014): UP KRITIS. Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen – Grundlagen und Ziele –. Online verfügbar unter http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/UP_KRITIS_Fortschreibungsdokument.pdf?__blob=publicationFile, zuletzt geprüft am 24.05.2017.

[GGK+17] Gurschler, T., Großmann, J., Kotarski, D., Teichmann, C., Thim, C., Eichler, J., Göllner, J., Gronau, N., Lechner, U. (2017): Risikobeurteilung in der IT-Sicherheit Kritischer Infrastrukturen – Eine Analyse der Risikobeurteilung im Förderschwerpunkt ITS|KRITIS. In: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Digitale Gesellschaft zwischen Risikobereitschaft und Sicherheitsbedürfnisse. Tagungsband zum 15. Deutschen IT-Sicherheitskongress, 16.-18.5.2017 in Bonn. SecuMedia: Gau-Algesheim 2017, S. 395-410.

[Hipp05] von Hippel, E. (2005). Democratizing Innovation. Cambridge, MA: MIT Press

[Lech17] Lechner, U. (Hg.) (2017): Monitor IT-Sicherheit Kritischer Infrastrukturen. Online verfügbar unter https://monitor.itskritis.de, zuletzt geprüft am 24.05.2017.

[RePi09] Reichwald, R., & Piller, F. (2009). Interaktive Wertschöpfung: Open Innovation, Individualisierung und neue Formen der Arbeitsteilung. Wiesbaden: Gabler

[RHL+17] Rieb, A.; Hofmann, M.; Laux, A.; Rudel, S.; Lechner, U. (2017): Wie IT-Security Matchplays als Awarenessmaßnahme die IT-Sicherheit verbessern können, in Leimeister, J.M., Brenner, W. (Hrsg.): Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017), 12.-15.2.2017 in St. Gallen, Schweiz, S. 867-881.

[RuRi17] Rudel, S., Rieb, A. (2017): Technik vs. Mensch: Was nutzt ein hoher technischer Standard, wenn die Schwachstelle Mensch umgangen wird? In: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Digitale Gesellschaft zwischen Risikobereitschaft und Sicherheitsbedürfnisse. Tagungsband zum 15. Deutschen IT-Sicherheitskongress, 16.-18.5.2017 in Bonn. SecuMedia: Gau-Algesheim 2017, S. 345-352.

[WöSQ07] Wölfle, Ralf; Schubert, Petra; Quade, Michael (2007): Handbuch für Fallstudienautoren – Fallstudien schreiben mit der eXperience Methodik, Basel: Fachhochschule Nordwestschweiz FHNW, Institut für Wirtschaftsinformatik, 2007.