Ein Rahmenwerk zur Erfassung von IT-Sicherheit als Service-System

Max Jalowski[1] und Albrecht Fritzsche[1]

[1] Friedrich-Alexander-Universität Erlangen-Nürnberg, Lehrstuhl für Wirtschaftsinformatik, insb. Innovation und Wertschöpfung, {max.jalowski, albrecht.fritzsche}@fau.de

Abstract

IT-Sicherheit wird meist auf der Basis geschlossener Systemlandschaften diskutiert. Gerade kritische Infrastrukturen erfordern einen anderen Ansatz, mit dem Beiträge externer Experten und anderer Parteien besser berücksichtigt werden können. Das vorliegende Papier entwickelt einen solchen Ansatz auf der Basis aktueller Überlegungen zu Service-Systemen und kollaborativer Wertschöpfung aus der Dienstleistungsforschung. Es wird ein Rahmenwerk für die Analyse und Gestaltung von Systemen zur IT-Sicherheit entwickelt und beispielhaft auf seine Anwendbarkeit hin überprüft. Das Rahmenwerk erlaubt es insbesondere, Angreifer und Verteidiger gleichermaßen als Akteure im System zu erfassen und weitergehende Aktivitäten rund um die technischen Installationen mit einzubeziehen. Durch die Differenzierung verschiedener Formen von Kopplung zwischen den Aktivitäten entstehen weitergehende Möglichkeiten der Analyse.

1 Einführung

Als kritische Infrastrukturen werden Organisationen und Einrichtungen bezeichnet, die grundlegend für ein funktionierendes Gemeinwesen sind. Das deutsche Bundesministerium des Inneren unterscheidet dabei zwischen technischen Basisinfrastrukturen und sozioökonomischen Dienstleistungsinfrastrukturen (BMI 2009).

Technische Basisinfrastrukturen	Sozioökonomische Dienstleistungsinfrastrukturen
• Energieversorgung • Informations- und Kommunikationstechnologie • Transport und Verkehr • (Trink-) Wasserversorgung und Abwasserentsorgung	• Gesundheitswesen, Ernährung • Notfall- und Rettungswesen, Katastrophenschutz • Parlament, Regierung, öffentliche Verwaltung, Justizeinrichtungen • Finanz- und Versicherungswesen • Medien und Kulturgüter

Tabelle 1: Übersicht über kritische Infrastrukturen (vgl. BMI 2009)

Während der vergangenen Jahre wurden weltweit zahlreiche Anstrengungen unternommen, um den Schutz dieser Infrastrukturen zu erhöhen. Herausragende Beispiele sind das Europäische Programm

Critical Infrastructure Protection (EPCIP) und die Presidential Directive PDD-63 in den USA. Jede Institution, die Verantwortung für eine Installation im Bereich kritischer Infrastrukturen trägt, muss besondere Auflagen im Hinblick auf Katastrophenvorsorge, Abwehr von Angriffen und Behebung von Störungen erfüllen. Dies betrifft im Besonderen auch die IT-Systeme, die in den Institutionen verwendet werden.

Berichte über die Folgen von Schadsoftware wie Stuxnet und Duqu oder Hackerangriffen auf den französischen Fernsehsender TV5Monde und Regierungseinrichtungen in den USA oder Korea illustrieren die Herausforderungen für IT-Sicherheit, denen sich Betreiber kritischer Infrastrukturen stellen müssen. Gerade in Deutschland ist dabei zu bedenken, dass für die meisten Objekte im Bereich kritischer Infrastrukturen kommunale Institutionen oder mittelständische Unternehmen zuständig sind, denen oftmals nicht bewusst ist, dass auch sie im Fokus von Angreifern stehen könnten. Deshalb fehlt es solchen Unternehmen unter anderem an Ressourcen, Kompetenzen, klaren Verantwortlichkeiten (z.B. Benennung eines CSO) oder auch an finanziellen Mitteln, um die IT-(Sicherheits-) Infrastruktur auf- und auszubauen (Harsch et al. 2014). Gleichzeitig macht die zunehmende Verbreitung privater IT-Geräte mit eigener Netzwerkverbindung auch vor kritischen Infrastrukturen nicht halt. So verfügen auch dort immer mehr Menschen, die sich innerhalb der Betriebsgelände aufhalten, über eigene Smartphones, Tablets usw., die in Kontakt mit den Systemen vor Ort kommen können.

Die Informationstechnologie in kritischen Infrastrukturen hat deshalb generell einen offenen Charakter. Sie ist in vieler Hinsicht äußeren Einflüssen ausgesetzt und kann nur mit besonderer Anstrengung in spezifischen Bereichen zeitweise von der Umgebung isoliert werden. Diese Situation erfordert die Entwicklung ausgereifter Sicherheitskonzepte. Hier ist gerade die Wirtschaftsinformatik als Verbindungsglied zwischen Ökonomie und Technik gefordert, da die konzipierten Lösungen nicht nur technisch einwandfrei, sondern vor allem auch praktisch nutzbar und wirtschaftlich betreibbar sein müssen, um tatsächlich korrekt angewendet werden zu können.

Das Themengebiet IT-Sicherheit für kritische Infrastrukturen bietet allerdings auch Chancen: da die erforderlichen Lösungen sehr spezifische Anwendungsbereiche und Anforderungen haben, gibt es zunehmenden Bedarf an Experten mit besonderen Fachkenntnissen, die in diesem Bereich tätig werden. In den kommenden Jahren kann man deshalb von einem erheblichen Wachstum in diesem Bereich ausgehen, von dem gerade kleinere und mittelständische Unternehmen mit einem speziellen Fokus profitieren können. Hier ist ebenfalls die Wirtschaftsinformatik gefordert, Entwicklungsvorschläge zu machen und in der Umsetzung zu begleiten.

Was dabei fehlt, ist vor allem eine theoretische Grundlegung, die den Bereich der IT-Sicherheit in ein weitergehendes ökonomisches Konzept einfügt und auch Verbindungen zu Aspekten schafft, die nicht originär technischer Natur sind, wie zum Beispiel Mitarbeiterverhalten, Schulung oder Zutrittsregelung, die ihrerseits wesentlichen Einfluss auf das Gefahrenpotential für die IT kritischer Infrastrukturen haben. Das Ziel dieses Papiers ist es, eine solche theoretische Grundlegung auf der Basis vorhandener Konzepte der Dienstleistungsforschung zu skizzieren. Dazu werden zunächst die wichtigsten Überlegungen aus der Forschung zum Thema IT-Sicherheit aus technischer Sicht erläutert. Diese Überlegungen werden anschließend in Beziehung zu der aktuellen Diskussion über Service-Systeme gebracht, die im Einzelnen zu erläutern sind. Auf dieser Basis erfolgt schließlich die Entwicklung eines Rahmenwerks für IT-Sicherheit aus der Perspektive der Dienstleistungsforschung, das für kritische Infrastrukturen geeignet erscheint. Abschließend wird ein Ausblick auf konkrete Anwendungsmöglichkeiten gegeben, wobei der Schwerpunkt auf Innovationsaktivitäten gerichtet ist.

2 Stand der Forschung

2.1 IT-Sicherheit in offenen Systemen

IT-Sicherheit hat sich während der vergangenen Jahre in ein breit gefächertes und höchst dynamisches Forschungsfeld verwandelt. Neben der traditionellen Kryptographie, die bereits auf eine lange Geschichte zurückblicken kann, gibt es mittlerweile eine ganze Reihe weiterer Themengebiete, auf denen systematisch geforscht wird. Blake und Ayyagari (2012) nennen fünf übergeordnete Teilbereiche der Forschung: Sicherheitsdesign und -management, Business Operations Security, Verhaltensaspekte, Authentifikations- und Integritätskontrolle, sowie Vermeidung und Erkennung von kritischen Vorfällen. Die ersten beiden Kategorien beinhalten vor allem strategische Überlegungen zur Konstruktion von Sicherheitssystemen und Risikomanagement. Den letzten zwei Kategorien werden insbesondere operative Maßnahmen bei Eingriffen und die Minimierung von Risiken zugeordnet. Crossler et al. (2013) betrachten das Verhalten des Menschen als wichtiges zukünftiges Themengebiet für IT-Sicherheit, insbesondere im Bezug auf Compliance-Überlegungen und die Integration interdisziplinärer Ansätze.

Die meisten Arbeiten gehen bisher von der Annahme aus, dass die betroffenen Systeme in sich geschlossen sind und IT-Sicherheit deshalb nach den Gesichtspunkten des Perimeterschutzes betrieben werden kann (vgl. Johnston 2009). Die Aufgabenstellung besteht demnach darin, unberechtigten Zugriff zu blockieren und bereits von Schädlingen betroffene Systeme wieder in einen unversehrten Zustand zurückzubringen. Ob dies in der Praxis jedoch überhaupt möglich ist, bleibt oft völlig unklar (Locasto et al. 2009; Oberheide et al. 2008; siehe auch Cohen 1987). Erst seit jüngerer Zeit mehren sich die Überlegungen, die einen Systemzustand voraussetzen, in dem ständig Beeinträchtigungen vorhanden sind. Harsch et al. (2014) betrachten ein solches System als Kreislauf, mit dem kontinuierlich auf Vorfälle reagiert wird. Aycock et al. (2014) haben in diesem Zusammenhang die Bezeichnung „cosecure systems“ für Einheiten mit beeinträchtigten und nicht beeinträchtigten Teilbereichen vorgeschlagen. Es erscheint gerechtfertigt, offene Systeme, auf die zahlreiche Parteien auf verschiedene Weise Zugriff haben, dieser Kategorie zuzuordnen.

Risikobetrachtungen zu IT-Sicherheit widmen sich dem Phänomen vielfältiger äußerer Einflüsse auf verschiedene Weise. Gordon et al. (2005) betonen, dass Sicherheitsrisiken oft gar nicht an den explizit vorgesehenen Außengrenzen der IT-Landschaft eines Unternehmen entstehen, sondern vielmehr an den Stellen, wo Mitarbeiter und andere Personen auf Einrichtungen innerhalb des Betriebsgeländes Zugriff haben. Die kann insbesondere durch den Anschluss von infizierten USB-Sticks und anderen Datenträgern geschehen. Dabei stellen organisationale Faktoren wie Arbeitsbelastung, Unternehmenskultur oder habitualisierte Verhaltensweisen der Mitarbeiter bekanntermaßen wichtige Einflussgrößen dar, weil sie den Umgang mit den vorgesehenen Sicherheitsmechanismen im Unternehmen bestimmen (Halliday et al. 1996; Straub und Welke 1998). Systemnutzer und Betreiber müssen jedoch nicht unbedingt nur als Risiken betrachtet werden. Gerade dort, wo Beeinträchtigungen als unabwendbar angenommen werden, können sie vielmehr auch als aktive Beteiligte am Sicherheitsmanagement gelten, die Schwächen identifizieren und mit ihrem Verhalten zum Schutz beitragen (Spears und Barki 2010).

IT-Sicherheit ergibt sich also aus dem Zusammenwirken verschiedener technischer, organisationaler und personaler Faktoren. In technischer Hinsicht müssen nach Hawkey et al. (2008) neben den expliziten Schwachstellen des Systems auch die mobilen Zugriffe und die insgesamt vorhandene Komplexität der Anlagen berücksichtigt werden. Organisational spielen eine ganze Reihe unterschiedlicher Faktoren eine Rolle, die miteinander in Wechselwirkung stehen.

Neben der Priorisierung von IT-Sicherheit und der resultierenden Zeitpläne und Budgets gehören dazu insbesondere Sicherheitswahrnehmung, Zugangskontrolle, Interaktion mit anderen Organisationen, Aufbau des IT Managements und die Wahrnehmung von Risiken. Letztere steht nach Hawkey et al. (2008) auch im Zusammenhang mit den personalen Faktoren, wozu neben Ausbildung und Kultur auch Kommunikation und Sensibilität für Risiken zählen. Kesh und Ratnasingam (2007) zählen in Summe acht Dimensionen eines erfolgreichen Sicherheitsmanagements auf: Planung der Informationssicherheit, Vorgehensweisen und Projektmanagement, IT-Architekturen für Sicherheitsmanagement, Modelle und Praktiken, Risikomanagement, Schutzmechanismen, personalbezogene Sicherheit, sowie Gesetze und ethische Richtlinien. IT-Sicherheit ist demzufolge nicht nur eine Frage datentechnischer Instrumente und individueller Kompetenzen, sondern steht in enger Beziehung zum Aufbau eines Unternehmens und seinen internen und externen Ressourcen. Neben expliziten Strukturelementen spielen dabei auch implizite Aspekte eine Rolle, insbesondere die interpersonelle Zusammenarbeit (Fenz et al. 2011).

2.2 Value Co-Creation und Service-Systeme

In dieser Gemengelage bietet sich aus ökonomischer Sicht eine Betrachtungsweise an, die sich genauer mit den Beiträgen unterschiedlicher Beteiligter in Wertschöpfungsprozessen (Value Co-Creation) auseinandersetzt. Überlegungen in dieser Hinsicht wurden in den vergangenen Jahren aus ganz unterschiedlichen Richtungen vorangetrieben (z.B. Toffler 1980; Wikström 1996; Prahalad und Ramaswamy 2004). In Zusammenfassung der gesamten Diskussion beschreiben Ranjan und Read (2014) zwei verschiedene Zugänge zu diesem Phänomen:

1. Co-Production

   Überlegungen zu Co-Production befassen sich mit der Einbeziehung von Konsumenten in den Prozess der Herstellung eines Produkts oder der Bereitstellung einer Dienstleistung. Dies ist insbesondere aufgrund der zunehmenden Individualisierung von Angeboten zu einem wichtigen Thema der Forschung geworden und hat in der Wirtschaftsinformatik vor allem dort Niederschlag gefunden, wo es um Customizing und Produktkonfiguratoren geht (z.B. Piller 2004).

2. Value-In-Use

   Anders als bei Co-Production steht hinter der Idee der Value-In-Use ein neues Verständnis des Wertschöpfungsprozesses an sich, bei dem die Aktivitäten auf Seiten desjenigen, der das jeweilige Angebot in Anspruch nimmt, den Schwerpunkt bilden. Wertschöpfung kann demnach nicht durch den Anbieter determiniert werden, sondern ergibt sich erst aus den Handlungen der Abnehmer. Value-In-Use hat sich vor allem in der Marketingforschung als fruchtbares Konzept erwiesen und wurde dort durch die Service-Dominant Logic von Vargo und Lusch (2004; 2008) geprägt.

Die Service-Dominant Logic betrachtet Produkte und Dienstleistungen nicht als unterschiedliche Varianten von Wertentstehung in ökonomischen Interaktionen, sondern vielmehr als komplementäre Perspektiven auf den Prozess der Wertentstehung selbst. Dabei drückt sich im Begriff der Dienstleistung ein systemisches Verständnis aus, das allen Beteiligten an der Interaktion eine aktive Rolle zugesteht (Maglio et al. 2009). Neben den eigentlichen Handlungsträgern schließt dies auch Ressourcen wie Technologie und Information ein, die Auswirkungen auf das entstehende Resultat haben. Hieraus haben sich neue Anknüpfungspunkte der Wirtschaftsinformatik an die Dienstleistungsforschung ergeben, sowohl aus analytischer Sicht wie auch aus Sicht des

Systemdesigns (Alter 2012; Böhmann et al. 2014). Darüber hinaus hat der Ansatz jedoch auch viele andere Anwendungsfelder gefunden, bis hin zur Analyse sozialer Brennpunkte in Städten (Ng und Andreu 2012; Kieliszewski et al 2012).

3 Forschungsdesign

3.1 Methodologische Basis

Die folgenden Überlegungen orientieren sich an den Prinzipien der gestaltungsorientierten Forschung, die insbesondere in Deutschland eine lange Tradition hat (Witte 1981). Sie eignet sich insbesondere dort für das wissenschaftliche Arbeiten, wo neuartige Phänomene und Aufgabenstellungen behandelt werden, für die noch keine klar strukturierten experimentellen Settings zugänglich sind (vgl. Thomke 2003). Auch international erhalten gestaltungsorientierte Ansätze in der Wirtschaftsinformatik seit einigen Jahren als Design Science Research zunehmende Aufmerksamkeit (vgl. z.B. Hevner et al. 2004).

Gestaltungsorientierte Forschung nutzt die Erstellung von Artefakten in einem strukturierten Problemlösungsprozess als Methode des Erkenntnisgewinns (vgl. Simon 1996). Durch die Reflexion der dabei entstehenden Resultate hinsichtlich der ursprünglichen Problemstellung ergeben sich weitere Einsichten in den Forschungsgegenstand, die auf unterschiedlichen Abstraktionsebenen formuliert werden können, von der Beschreibung des konkreten Anwendungsfalls über weitergehende Designregeln bis hin zu einer allgemeinen Theorie (Gregor und Hevner 2011). Als Artefakte kommen dabei sowohl materiell als auch formal verfasste Gegenstände infrage.

Beim hier zu erstellenden Artefakt handelt es sich um ein Rahmenwerk für das Management von IT-Sicherheit offener Systeme. Nach der Formulierung wird das Rahmenwerk auf seine Anwendbarkeit für kritische Infrastrukturen überprüft, um daraus Erkenntnisse für die weitere Forschung abzuleiten. Zur theoretischen Grundlegung des Rahmenwerks wird das Konzept des Service-Systems aus der Dienstleistungsforschung zur kollaborativen Wertschöpfung herangezogen.

3.2 Fachlicher Ansatz

Die Darstellung des Stands der Forschung hat deutlich gemacht, dass IT-Sicherheit von den Beiträgen zahlreicher unterschiedlicher Handlungsträger abhängt. Demzufolge liegt es nahe, bei der weiteren Modellierung von einem kollaborativen Wertschöpfungsprozesses auszugehen. Im Sinne von Value-In-Use ergibt sich IT-Sicherheit dabei aus dem Nutzen, der in Summe durch die Zusammenarbeit entsteht. IT-Sicherheit muss demnach als eine systemische Leistung gelten. Sie wird durch das reibungslose Funktionieren der Informationstechnologie im Unternehmen bestimmt. IT-Sicherheit gewährleistet, dass ein störungsfreier Betrieb stattfinden kann, wobei die betrachteten Risiken aber nicht wie bei anderen operativen Ansätzen auf Konstruktionsfehler fokussiert sind, sondern die aktive Verursachung von Schäden in den Mittelpunkt gestellt wird.

Auf der Grundlage dieser Überlegungen betrachten wir IT-Sicherheit im Folgenden als Service-System. In Einklang mit Kieliszewski et al. (2012) unterscheiden wir bei der Modellierung drei Arten von Kopplung einzelner Aktivitäten (siehe dazu auch Tan et al. 2012):

- Integration
  Es ist keine Trennung einzelner Beiträge möglich, sondern nur eine Gesamtbetrachtung, weil beispielsweise gemeinsame Ressourcen verwendet werden.
- Feste Kopplung
  Hier ist es möglich unterschiedliche Beiträge einzelner Beteiligter zu identifizieren. Sie werden jedoch als operative Einheit mit einem erkennbaren Gesamtergebnis betrachtet.
- Lose Kopplung
  Die Aktivitäten sind trennbar und austauschbar. Die Zusammenarbeit kann in unterschiedlichen Konstellationen erfolgen.

Es ist dabei wichtig zu verstehen, dass IT-Sicherheit selbst wiederum Teil eines Gesamtsystems ist, dessen Gemeinschaftsleistung im Betrieb der kritischen Infrastruktur besteht. Es ist also eine mehrstufige Modellierung von Service-Systemen nötig (vgl. Böhmann et al. 2014).

4 Rahmenwerk

4.1 Struktur

Unser Rahmenwerk zur IT-Sicherheit verknüpft zwei Darstellungsweisen. Dabei handelt es sich zunächst um eine Akteursmatrix, die es erlaubt, unterschiedliche Formen der Kopplung zu identifizieren. Um einen Überblick über die ablaufenden Wertschöpfungsprozesse zu bekommen, können die Inhalte der Matrix weiterhin in ein Systemschaubild übertragen werden, das ähnlich wie bei Kieliszewski et al. (2012) die verschiedenen operativen Einheiten sichtbar macht.

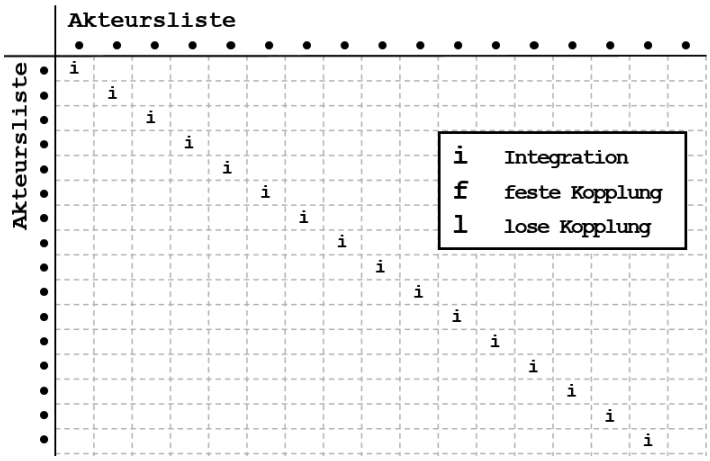

Bild 1: Akteursmatrix

Bild 1 stellt die Akteursmatrix dar. In dieser Matrix werden alle beteiligten Akteure in zwei Dimensionen aufgelistet. Die Zellen der Matrix geben die Art der Kopplung an, die mit den Buchstaben i für integriert, f für fest und l für lose bezeichnet werden. Es werden zwei Entscheidungskriterien herangezogen, um die Art der Kopplung zu bestimmen (vgl. dazu auch Kesh und Ratnasingam (2007):

- physikalisches Setting der Operationen
- verwendetes Wissen bei den Operationen

Aus Gründen der Einfachheit werden diese Kriterien in der Matrix jedoch nicht kenntlich gemacht. Die Matrix beschränkt sich auf die Angabe der Kopplung. In der Diagonale der Matrix kann vorab bereits der Buchstabe i gesetzt werden, da alle Operationen in Bezug auf sich selbst sowohl hinsichtlich des physikalischen Settings, als auch des verwendeten Wissens übereinstimmen.

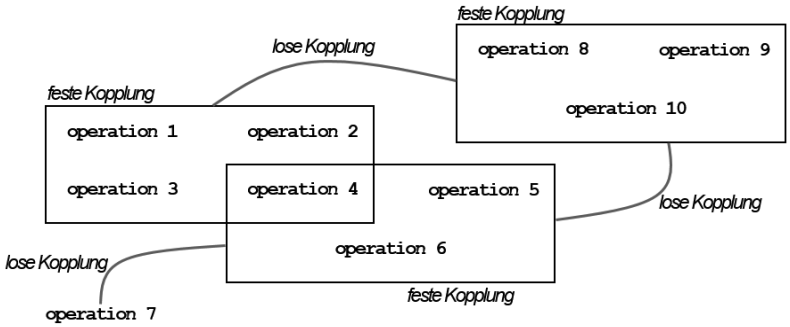

Bild 2: Schaubild Kopplungen

Die zweite Darstellungsform gruppiert die Operationen nach Art der Kopplung (vgl. Bild 2). Einzelne Operationen und Cluster integrierter Operationen werden dabei gleich behandelt. Um diese Entitäten herum sind gekoppelte Operationen dargestellt. Feste Kopplungen erscheinen als Kästen, lose Kopplungen als Verbindungslinien zwischen Elementen. Kästen mit fester Kopplung können sich überlagern.

4.2 Inhalt

Um das Rahmenwerk inhaltlich zu befüllen, ist es notwendig, die verschiedenen Operationen, die zu IT-Sicherheit beitragen, aufzuzählen. Aus diesen Operatoren werden die Akteure abgeleitet, die in der Matrix darzustellen sind. Es ist dabei möglich, dass eine Person in mehreren Rollen als Akteur auftritt. Auch in diesem Fall werden die einzelnen Rollen aber als separate Akteure dargestellt. Die Ausführung in Personalunion wird dann als operative Integration oder feste Kopplung angeführt. Dies ist entscheidend für die spätere Systemanalyse und Suche nach Optimierungen.

Die Darstellung der einzelnen Aktivitäten zur Abwehr von Angriffen in der Literatur ist recht divers (vgl. insbesondere Hawkey et al. 2008; Harsch et al. 2014) und hängt auch vom Anwendungsfall ab, der ggf. spezifische Maßnahmen erfordert. Die folgende Tabelle nimmt darauf aufbauend eine vereinfachende Typisierung vor. Darüber hinaus werden die verschiedenen Typen von Aktivitäten der Angreifer dargestellt, auf die in der Diskussion von Abwehrmaßnahmen Bezug genommen wird. Wenn IT-Sicherheit im Sinne von Value-In-Use verstanden wird, ist es unumgänglich, auch diese Aktivitäten als Beitrag zur Wertschöpfung darzustellen, da sie ebenfalls essentiell für den entstehenden Nutzen der Sicherheitsmaßnahmen sind.

Aktivitäten zur Abwehr		**Aktivitäten beim Angriff**	
Vorbeugung	ID-Management	Spionage	Anlagen auffinden
	Zugangskontrolle		Beteiligte kennenlernen
	Authentifizierung		Architekturbild erzeugen
	Durchführung Backups		Schwachstellen abschätzen
	Logging der Vorgänge		Abwehr austesten
	Wissenserwerb		Informationen ausspähen

Aktivitäten zur Abwehr		Aktivitäten beim Angriff	
Detektion	System-Monitoring	Aufrüsten	Kompetenz aufbauen
	Identifikation von Gefahren		Instrumente akquirieren
	Benachrichtigung		Programme schreiben
Analyse	Dokumentation des Falls		Material beschaffen
	Bewertung der Situation	Angreifen	Status verfolgen
	Vorgehensweise, Priorisierung		Zugang verschaffen
	Weitergabe, Information		Programm starten
Reaktion	Eingrenzen, kenntlich machen	Ausnutzen	Schaden verursachen
	Eliminieren		Kontrolle übernehmen
	Berichten		Werte abschöpfen
	Wiederherstellen		Zurschaustellen

Tabelle 2: Übersicht über Typen von Sicherheitsaktivitäten (eigene Darstellung)

Die Inhalte der Tabelle sind stets auf Vollständigkeit und Anwendbarkeit zu überprüfen und bei Bedarf entsprechend anzupassen. Ebenso muss bei der Ableitung der Systemakteure entschieden werden, wo menschliche Handlungsträger und wo artifizielle Funktionseinheiten Berücksichtigung finden, die nach der Logik der Service-Systeme auch die Rolle von Akteuren annehmen können.

5 Analyse

5.1 Anwendung des Rahmenwerks

Das Rahmenwerk wird nun gemäß den Prinzipien gestaltungsorientierter Forschung zur Anwendung gebracht und dabei auf seine Nutzbarkeit hin untersucht. Aufgrund der Längenvorgabe für diesen Konferenzbeitrag beschränken wir uns auf ein vergleichsweise einfaches Szenario, in dem es um eine Abwassereinrichtung geht, deren Nutzung von IT auf ein Minimum reduziert ist. Es werden lediglich die folgenden Funktionen damit abgedeckt:

- Speicherung des Werteverlaufs
- Berichterstattung an zentrale Stellen
- Personaleinsatzplan und andere administrative Aktivitäten

Die Einrichtung verfügt infolgedessen auch nur über handelsübliche IT-Lösungen, wie sie auch von Privatpersonen verwendet werden. Die Mitarbeiter, die aufgrund der geringen Größe der Einrichtung alle persönlich miteinander bekannt sind, verfügen über keine besondere Kompetenz zur Informationssicherheit und verlassen sich in diesem Themengebiet vollständig auf die automatischen Mechanismen, die auf ihren Geräten eingerichtet sind. Für diese Einrichtung sind sie auf Experten angewiesen, die von außen hinzugezogen werden.

Trotz der Einfachheit der Situation müssen jedoch auch hier schon so viele einzelne Operationen im System bedacht werden, dass die Matrixdarstellung des Rahmenwerks im vorliegenden Dokumentenformat nicht geeignet umsetzbar ist, sondern nur bei direkter Nutzung geeigneter Tabellenprogramme. Wir beschränken uns deshalb auf die Angabe des Schaubilds zur Interaktion, das Aufschluss über die unterschiedlich gekoppelten Bereiche gibt (vgl. Bild 3).

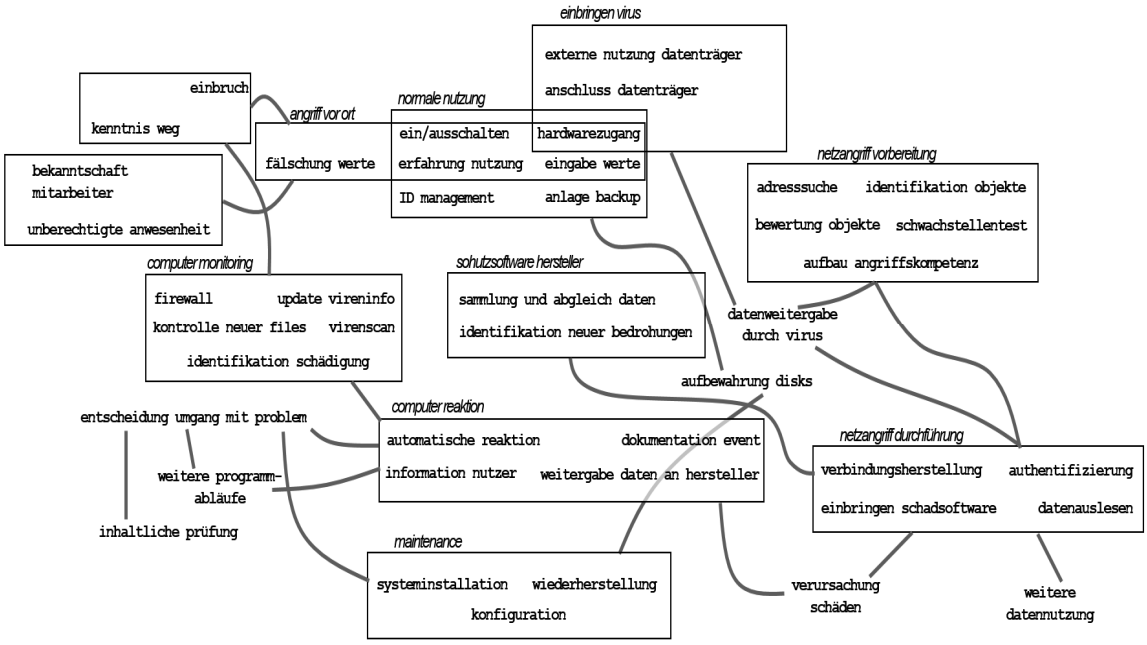

Bild 3: Anwendung Schaubild auf Fallstudie Abwassereinrichtung

Die im Schaubild berücksichtigten Schadensfälle beziehen sich auf den Totalausfall der IT und auf die Fälschung oder Vernichtung von Werten, die dort dokumentiert werden und die wesentlich für die weitergehende Kontrolle des Verlaufs der Wasserqualität sind. Obwohl es also bei dieser Einreichung keine unmittelbaren Verbindungen zwischen der IT vor Ort und dem Funktionieren der kritischen Infrastruktur gibt, spielen solche Ausfälle mittelbar trotzdem eine Rolle und illustrieren damit die Angreifbarkeit der Gesamtstruktur.

5.2 Diskussion

Durch die Anwendung des hier vorgestellten Rahmenwerks ergibt sich ein anderes Bild von IT-Sicherheit, als es in bisherigen Forschungsbeiträgen deutlich geworden ist. Die wichtigste Neuerung besteht darin, dass die Dynamik zwischen Angreifern und Verteidigern besser erfassbar wird. Beide sind zunächst Teile des Gesamtsystems. Wertfrei betrachtet tragen sie alle in gleicher Weise zur Entwicklung des Systems bei. Ihre Aktivitäten bedingen sich gegenseitig und können im Hinblick auf ihre Wirkung nicht unabhängig voneinander verstanden werden. Eben darin kommt die Besonderheit des Konzepts von Value-In-Use zur Geltung.

Weiterhin erhöht die Anwendung des Rahmenwerks die Transparenz über die verschiedenen Arten der Kopplung von Vorgängen, die für IT-Sicherheit eine Rolle spielen. Auffällig ist dabei die Überlagerung fester Kopplungen rund um die normale Arbeit vor Ort. Dies ist als Folge der geringen Größe der Einrichtung zu verstehen, derentwegen die Mitarbeiter zahlreiche sicherheitsrelevante Themen gleichzeitig im Auge behalten müssen. Bei größeren Einrichtungen mit einem stärkeren organisationalen Differenzierungsgrad sähe das Schaubild anders aus.

Darüber hinaus ist zu erkennen, dass die technischen Operationen in vielfältiger Weise mit anderen Aktivitäten zusammenhängen, die sowohl außerhalb der Einrichtung als auch innerhalb stattfinden können. Viele davon sind nur lose mit anderen gekoppelt, was wiederum als Hinweis darauf gedeutet werden kann, dass sie bisher organisational noch keine weitere Aufmerksamkeit erfahren haben und weder systematisch gesteuert noch überwacht werden. Auch hier ergibt sich damit Entwicklungspotential, das über die bisherigen Ansätze hinausgeht.

Auf der anderen Seite ist festzustellen, dass aus dem Rahmenwerk keine organisationalen Lösungen für Sicherheitsprobleme ablesbar sind. Hierzu sind weitere Überlegungen notwendig, die nicht nur die Kopplung von Aktivitäten, sondern auch ihre Zuordnung zu verschiedenen Kompetenzbereichen und ihre Reihenfolge in der Abwicklung berücksichtigen. Das ist auf der Grundlage des existierenden Rahmenwerks nicht möglich, führt jedoch auch weit über die Zielsetzungen hinaus, die bisher normalerweise mit Anwendungen des Konzepts von Value-In-Use verbunden sind. Obendrein ist zu berücksichtigen, dass über die dargestellten Aktivitäten zum Teil große Unsicherheit herrscht. Vor allem die Beschreibung dessen, was auf Seiten der Angreifer passiert, beruht auf Annahmen und Rekonstruktionen rationaler Vorgehensweisen, ohne dass sie konkret überprüft werden könnten.

6 Schluss

Das Ziel des vorliegenden Papiers war es, eine theoretische Grundlegung für die Diskussion von IT-Sicherheit von einem weitergehenden wirtschaftswissenschaftlichen Standpunkt aus voranzubringen. Dazu orientierte sich das Papier an den Arbeiten der jüngeren Dienstleistungsforschung zu kollaborativer Wertschöpfung. Im Sinne von Value-In-Use wurde dabei ein pragmatischer Zugang zu IT-Sicherheit entwickelt, der die operative Betriebsfähigkeit in den Mittelpunkt stellt. Dieser Zugang kann auch dort Verwendung finden, wo nicht mehr voraussetzbar ist, dass schädliche Komponenten vom System ferngehalten werden, sondern von deren ständiger Gegenwart ausgegangen werden muss. Für diese Sachlage wurde der Begriff „cosecure systems“ vorgeschlagen. Anders könnte man auch von Systemen mit einem großen Offenheitsgrad oder verkürzt schlichtweg von offenen Systemen sprechen, denn unter der Annahme, dass Schadsoftware stets existiert und verbreitet wird, ist es nur eine Frage des Abschlusses, ob sie konzeptuell berücksichtigt werden muss oder nicht.

Im weiteren Verlauf wurde ein Rahmenwerk entwickelt, das bisherige Ansätze zur Analyse von Service-Systemen auf den Themenbereich IT-Sicherheit überträgt. Als Besonderheit ist hier die Einbeziehung der Angreifer als Teile des Systems zu betonen. Eine Unterscheidung zwischen positiven und negativen Beiträgen zur IT-Sicherheit muss nicht a priori vorausgesetzt werden. Dies erlaubt es auch, Grauzonen zu adressieren, in denen man nicht weiß, wie die entsprechenden Vorgänge zu interpretieren sind, oder widersprüchliche Vorstellungen davon existieren, ob etwas schädlich ist oder nicht – je nachdem, welcher Standpunkt bei der Analyse eingenommen wird.

Gerade hier scheint die vorgestellte Lösung Potential zu haben, das Forschungsgebiet in neue Richtungen weiterzuentwickeln, in denen die Wirtschaftsinformatik wichtige Beiträge liefern kann. So wäre es beispielsweise vorstellbar, neue Innovationsansätze zu entwickeln, die mehr Wert auf die Einbeziehung aller Parteien legen und nicht nur im Denkmuster der Offensive und Defensive verharren. Bevor dies verwirklicht werden kann, sind jedoch zweifellos weitere Überlegungen zur Verfeinerung des Rahmenwerks und zusätzliche Anwendungsbeispiele nötig, um sowohl die Aufgabenstellung als auch die Lösungsmöglichkeiten noch besser greifbar zu machen.

Danksagung:

Dieses Papier ist im Rahmen des Begleitforschungsprojekts „VeSiKi“ im Förderschwerpunkt des BMBF zur IT-Sicherheit kritischer Infrastrukturen unter dem FKZ 16KIS0214 entstanden. Die Autoren danken allen Beteiligten für die Unterstützung ihrer Forschung.

7 Literatur

Alter S (2012) Metamodel for Service Analysis and Design Based on an Operational View of Service and Service Systems. In: Service Science 4(3): 218–235.

Aycock J, Somayaji A, Sullins J (2014) The Ethics of Coexistence: Can I Learn to Stop Worrying and Love the Logic Bomb? In: IEEE Symposium in Ethics in Science, Technology and Engineering.

Blake R, Ayyagari R (2012) Analyzing information systems security research to find key topics, trends, and opportunities. In: Journal of Information Privacy & Security: 8(3): 37-67.

BMI (2009) Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.html. Abgerufen am 21.3.2015.

Böhmann T, Leimeister JM, Möslein KM (2014) Service-Systems-Engineering. In: BISE Business & Information Systems Engineering 56(2): 83-90.

Cohen F (1987) Computer viruses: theory & experiments. In: Computers & Security 6(1): 22-35.

Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M., Baskerville R. (2013) Future directions for behavioral information security research. In: computers & security 32: 90-101.

Fenz S, Parkin S, van Moorsel A (2011) A community knowledge base for IT security. In: IT Professional 13(3): 24-30.

Gordon, LA, Loeb, MP, Lucyshyn, W, Richardson, R (2005) CSI/FBI Computer Crime and Security Survey, Computer Security Institute.

Gregor S and Hevner A (2011) Introduction to the special issue on design science. In: Information Systems and e-Business Management 9: 1-9.

Halliday S, Badenhorst K, von Solms R (1996) A Business Approach to Effective Information Technology Risk Analysis and Management. In: Information Management & Computer Security 4(1): 19-31.

Harsch A, Idler S, Thurner S (2014) Assuming a state of compromise. In: IT Security Incident Management & IT Forensics (IMF), 2014 Eighth International Conference on IT Security Incident Management & IT Forensics: 76-84.

Hawkey K, Botta D, Werlinger R, Muldner K, Gagne A, Beznosov K (2008) Human, organizational, and technological factors of IT security. In: CHI'08 Human Factors in Computing Systems. ACM: 3639-3644.

Hevner A, March S, Park J and Ram S (2004) Design Science Research in Information Systems. In: MIS Quarterly 28(1): 75-105.

Johnston J (2009) Technological Turf Wars: A Case Study of the Computer Antivirus Industry. Temple University Press.

Kesh S, Ratnasingam P (2007) A knowledge architecture for IT security. In: Communications of the ACM 50(7): 103-108.

Kieliszewski CA, Maglio PP, Cefkin M. (2012) On modeling value constellations to understand complex service system interactions. In: European Management Journal 30: 438-450.

Locasto ME, Bratus S, Schulte, B (2009) Bickering in-depth: Rethinking the composition of competing security systems, In: IEEE Security & Privacy, November/Dezember: 77-81.

Maglio PP, Vargo SL, Caswell N, Spohrer J (2009) The service system is the basic abstraction of service science. In: Information Systems and e-Business Management 7(4): 395-406.

Ng I, Andreu L (2012) Special Issue: Research perspectives in the management of complex service systems. In: European Management Journal 30: 405-409.

Oberheide J, Cooke E, Jahanian F (2008) CloudAV: N-version antivirus in the network cloud. In 17th USENIX Security Symposium: 91-106.

Piller F (2004). Mass customization: reflections on the state of the concept. In: International Journal of Flexible Manufacturing Systems 16(4): 313-334.

Prahalad C, Ramaswamy V (2004) Co-creation experiences: the next practice in value creation. In: Journal of Interactive Marketing 18(3): 5-14.

Ranjan KR, Read S (2014) Value co-creation: concept and measurement. In: Journal of the Academy of Marketing Science: 1-26.

Simon HA (1996) The Sciences of the Artificial (3rded.). MIT Press, Cambridge.

Spears JL, Barki H (2010) User participation in information systems security risk management. In: MIS Quarterly 34(3): 503-522.

Straub D, Welke R. (1998) Coping with Systems Risk: Security Planning Models for Management Decision Making. In: MIS Quarterly 22(4): 441-469.

Tan WC, Haas PJ, Mak RL, Kieliszewski CA, Selinger P, Maglio PP, Li Y. (2012) Splash: A platform for analysis and simulation of health. In: Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium. Miami: 543–552.

Thomke SH (2003) Experimentation Matters. Unlocking the Potential of New Technologies for Innovation. Harvard Business School Press, Boston.

Toffler A (1980) The Third Wave: The Classic Study of Tomorrow. Bantam, New York.

Vargo SL, Lusch RF (2008) Service-dominant logic: continuing the evolution. In: Journal of the Academy of Marketing Science 36(1): 1-10.

Vargo SL, Lusch RF (2004) Evolving to a new dominant logic for marketing. In: Journal of Marketing 68(1): 1-17.

Wikstroem S (1996) The customer as coproducer. In: European Journal of Marketing 30(4): 6-19.

Witte E (1981) Nutzungsanspruch und Nutzungsvielfalt. In: Witte, E. (Hrsg.): Der praktische Nutzen empirischer Forschung. Tübingen: 13-40.