IT-Sicherheit in Kritischen Infrastrukturen – eine Fallstudien-basierte Analyse von Praxisbeispielen

Sebastian Dännart[1], Thomas Diefenbach[1], Manfred Hofmeier[1], Andreas Rieb[1], Ulrike Lechner[1]

[1] Universität der Bundeswehr München, Fakultät für Informatik, 85577 Neubiberg
{Sebastian.Daennart, Thomas.Diefenbach, Manfred.Hofmeier, Andreas.Rieb, Ulrike.Lechner}@unibw.de

Abstract. Die wachsende Bedeutung von IT-Sicherheit in Organisationen aufgrund einer vielfältigen Bedrohungslage ist unbestritten. Dies gilt insbesondere für Kritische Infrastrukturen mit hoher Bedeutung für das staatliche Gemeinwesen. In diesem Beitrag werden Beispiele erfolgreicher Umsetzungen von IT-Sicherheitsprojekten und -konzepten untersucht sowie Gemeinsamkeiten und Unterschiede bei den vorherrschenden kontextualen Rahmenbedingungen analysiert. Sieben Fallstudien wurden im Rahmen des Forschungsprojekts *Vernetzte IT-Sicherheit Kritischer Infrastrukturen* (VeSiKi*)* aus dem durch das BMBF geförderten Förderschwerpunkt *IT-Sicherheit für Kritische Infrastrukturen* (ITS|KRITIS) erhoben. Auf dieser Fallstudienserie aufbauend wurde eine Cross Case-Analyse durchgeführt. Die Ergebnisse zeigen, dass IT-Sicherheitsmaßnahmen nicht isoliert betrachtet werden können, sondern aufgrund der Einbindung in bestehende Geschäftsprozesse auch eine Anpassung organisationaler und personeller Aspekte wesentliche Erfolgsfaktoren sind.

Keywords: Kritische Infrastrukturen, IT-Sicherheit, Cross Case-Analyse

1 Einleitung

IT-Sicherheit Kritischer Infrastrukturen ist ein vergleichsweise neues Themenfeld, das mit Stuxnet, einer IT-Sicherheitsbedrohung für Industrieanlagen, im Jahr 2010 ins Bewusstsein der Öffentlichkeit drang [1]: Eine Schadsoftware konnte über längere Zeit hinweg unbemerkt Steuerungsanlagen und Leittechnik in der Uranaufbereitungsanlage Natanz und dem Kernkraftwerk Buschehr stören. Eine neuere und ebenfalls prominente Schadsoftware ist das Mirai-Botnetz mit dem Distributed Denial of Service-Angriffe organisiert werden und das im Jahr 2016 auch Router in Privathaushalten in Deutschland betraf. Die Blackouts von 2015 und 2016 in der Ukraine werden der Schadsoftware Industroyer zugeschrieben [2]. Verschiedene Versionen von Ransomware haben in den Jahren 2015 und 2016 sowohl Privatpersonen als auch Universitäten, Krankenhäuser und Behörden betroffen [3]. Fake News sowie die Diskussion über Manipulationsmöglichkeiten von demokratischen Wahlen in 2016 und 2017 sind weitere Beispiele für Verwundbarkeiten der Zivilgesellschaft.

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

Kritische Infrastrukturen (KRITIS) sind „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden“ [4]. Funktionierende Informations- und Kommunikationsstrukturen sind Voraussetzung und IT-Sicherheit der Lebensnerv für medienbruchfreie Geschäftsprozesse oder Leitbilder der Zukunft wie autonome Fahrzeuge und Data Driven X (http://mkwi2018.leuphana.de).

Um die IT-Sicherheit Kritischer Infrastrukturen zu studieren, wurde eine Fallstudienserie durchgeführt. In diesem Beitrag wird die Fallstudienserie mit Methodik und durchgeführten Fallstudien vorgestellt (Kapitel 2 und 3) sowie eine Cross Case-Analyse (Kapitel 4) präsentiert. Ziel des Beitrags ist es, Erfolgsfaktoren von Projekten der IT-Sicherheit Kritischer Infrastrukturen zu identifizieren und die Implikationen von IT-Sicherheitsverfahren auf den Kontext zu studieren, um so einen Beitrag zum Verständnis der IT-Sicherheit Kritischer Infrastrukturen zu leisten.

2 Methodik

Da die Einführung von IT-Sicherheitsmaßnahmen zumeist einen Eingriff in bestehende Geschäftsprozesse erfordert, stellen komplexe und schwer voneinander abzugrenzende Zusammenhänge und Folgen eine große Herausforderung dar. Fallstudien bieten eine Forschungsstrategie zur Datenerhebung [5], die sich sehr gut dazu eignet, diese komplexen Phänomene in ihrem natürlichen Kontext darzustellen [6]. Dazu werden Methoden der qualitativen Datenanalyse verwendet, um Prozessabläufe und die Dynamik in konkreten Situationen zu verstehen [7].

Um die Forscher bei der einheitlichen Erstellung der Fallstudien zu unterstützen und deren Arbeiten im Anschluss vergleichbar zu machen, orientieren wir uns an der eXperience Methodik [8]. Die eXperience Methodik will authentisches Wissen rund um E-Business und IT-Management vermitteln und stellt dazu ein Raster und Vorgehensmodell sowie begleitende Materialien bereit. Angelehnt an diese Methodik wurden ein Rahmen für Fallstudien zum Thema „IT-Sicherheit Kritischer Infrastrukturen“ und ein Prozess zur Erhebung der notwendigen Daten entwickelt und mit den Projekten im Förderschwerpunkt *IT-Sicherheit für Kritische Infrastrukturen* des Bundesministeriums für Bildung und Forschung im Jahr 2015 verfeinert. Drei Fallstudientemplates bieten dabei einen Leitfaden zur Darstellung unterschiedlicher Arten von IT-Sicherheitsfallstudien:

- **projektbezogene Fallstudien** beziehen sich auf ein IT-Sicherheitsprojekt,
- **produktbezogene Fallstudien**, die die Implementierung oder den Einsatz von speziellen, innovativen IT-Sicherheitstechnologien beschreiben und
- **unternehmensbezogene Fallstudien**, die die gelebte IT-Sicherheit einer Organisation aus verschiedenen Perspektiven erfassen.

Nach zwei ersten Fallstudien im Jahr 2015 wurden weitere Fallstudien im Jahr 2016 und 2017 durchgeführt und verfasst. Dabei erfolgte die Datenerhebung auf Basis von leitfadengestützten Experteninterviews.

Eine Cross Case-Analyse ermöglicht die analysierten Daten zu kategorisieren und Aussagen mehr Aussagekraft zu geben [9]. Nach Mayring [10] wurde dazu eine Kodierung entwickelt und die Fallstudien qualitativ analysiert, sodass Kernaussagen extrahiert werden konnten. Nach einem Review der Codes wurden die Extrakte als Basis für die vorliegende Cross Case-Analyse genutzt. In der Datenanalyse wurden Rephrasierungen und Aussagen von den Autoren der Fallstudien und dem Autorenteam dieses Beitrags reflektiert, um Verfälschungen auszuschließen.

3 Die Fallstudien

Als Partner für die Erstellung der Fallstudien wurden zunächst Verbundprojekte aus dem Förderschwerpunkt ITS|KRITIS gefragt, darüber hinaus aber auch weitere Betreiber Kritischer Infrastrukturen oder KRITIS-relevante Zulieferer eingebunden. Die Fallstudien wurden in den Jahren 2015 bis 2017 entwickelt und stellen den Stand vor Inkrafttreten des IT-Sicherheitsgesetzes (Bundestag-Drucksache 18/4096 und 18/5121) [11] dar. Für diesen Beitrag wurden sieben Fallstudien ausgewählt, die eine große Bandbreite Kritischer Infrastrukturen und IT-Sicherheitsprojekten abdecken. In diesem Kapitel werden die Fallstudien einzeln vorgestellt.

Tabelle 1. Übersicht über die Fallstudien[1]

Nr.	*Organisation*	*Titel*	*Autor(en)*	*Art*
1	***	Fernwartung Kritischer Infrastrukturen	A. Rieb	Produkt
2	***	Ein sicherer Standardprozess für die Digitale Tatortfotografie	S. Lücking, S. Dännart	Projekt
3	kbo	Ausgewogenes Risikomanagement für nachhaltige IT-Sicherheit	T. Kehr, S. Dännart	Projekt
4	PREVENT	IT-Sicherheit für Geschäftsprozesse im Finanzsektor – die Managementlösung PREVENT	S. Rudel, T. Bollen	Projekt
5	SAP SE	Informationssicherheit bei SAP SE: Die längste Human Firewall der Welt	U. Lechner, T. Gurschler, A. Rieb	Unternehmen
6	ugarbe.de software	Informationssicherheit durch IT-gestützte Klassifizierung von Dokumenten und E-Mails	A. Rieb	Produkt
7	***	IT-Sicherheit in der Nahrungsmittelindustrie: Tradition und Hochverfügbarkeit	S. Dännart	Unternehmen

Fallstudie 1: Fernwartung Kritischer Infrastrukturen. Die Fallstudie thematisiert Risiken der Fernwartung industrieller Kontroll- und Steuerungssysteme in Kritischen

[1] Einige Fallstudien sind anonymisiert; Kennzeichnung mit ***

Infrastrukturen und stellt den Ansatz eines Herstellers vor: eine Fernwartungslösung, die es erlaubt, Fernwartungszugänge kontrolliert zu öffnen und abgesicherten Zugang zur Kritischen Infrastruktur zu ermöglichen. Ein Wildwuchs an Fernwartungszugängen oder „geheime“ Zugänge für IT-Mitarbeiter zu Kritischen Infrastrukturen sind klassische IT-Sicherheitsthemen Kritischer Infrastrukturen. Die Lösung in Form von Hard- und Software ermöglicht die Administration von Wartungsobjekten aus der Ferne und kann insbesondere für die Sicherheit existierender Infrastrukturen eingesetzt werden.

Es werden sowohl unternehmensinterne als auch -übergreifende Herausforderungen beschrieben, die für erfolgreiche Implementierungen gelöst werden müssen.

Fallstudie 2: Ein sicherer Standardprozess für die Digitale Tatortfotografie. In dieser Fallstudie wird die Digitalisierung der Tatortfotografie – ein Prozess der Polizeiarbeit – vorgestellt. Beschrieben wird die lückenlose, justiziable Absicherung des gesamten Prozesses von der Beweismittelaufnahme bis zur Verhandlung vor Gericht.

Der digitalisierte Prozess der Tatortfotografie hat durch die neue Systemarchitektur zudem Vorteile in der polizeilichen Arbeit. Die Zulassung aller fototauglichen Geräte erleichtert die tägliche Polizeiarbeit und ermöglicht effiziente Beschaffungsvorgänge, während die Informationssicherheit der Fotos durch eine automatisch erstellte und zentral überwachte Signatur unmittelbar nach Anschließen des Datenträgers gewährleistet wird. Auch finanziell ist das Projekt ein Erfolg: Bereits drei Jahre nach Implementierung waren die Investitionskosten amortisiert.

Der digitale Prozess ist nicht nur moderner sondern auch anwenderfreundlicher als der tradierte analoge Prozess, der das Ausdrucken von Bildern für analoge Akten vorsah. Die Einbindung aller Stakeholder und deren Sensibilisierung für die Anforderungen der Informationssicherheit vom unmittelbaren Beginn des Projekts an waren für die erfolgreiche Umsetzung wichtig.

Fallstudie 3: Ausgewogenes Risikomanagement für nachhaltige IT-Sicherheit. Den Kern der Fallstudie bildet die Reaktion auf Ransomware-Angriffe auf Krankenhäuser Anfang 2016, die Impuls waren, um geplante Maßnahmen beschleunigt umsetzen zu können. Beschrieben werden die ersten Reaktionen, wie die vollständige Trennung vom Internet oder Deaktivierung von aktiven Inhalten sowie die daraus resultierenden Auswirkungen wie fehlende Unterstützung für medizinische Recherchen, Medikamentenbestellungen und die Erstellung von Arztbriefen.

Zentrales Thema der Fallstudie ist der Prozess der Freigabe von IT-Projekten, der alle Stakeholder im Klinikverbund und IT-Sicherheitsexperten miteinbezieht. Die Umsetzung eines nachhaltigen IT-Sicherheitskonzepts ist ein weiteres Thema. Die kbo erweiterten in diesem Prozess ihre Fähigkeiten mit Bedrohungen umzugehen. Organisatorisch wurden ein IT-Sicherheitskomitee, die offene Zusammenarbeit zwischen Mitarbeitern und der IT sowie der Einbezug externer Partner implementiert. Die konsequente Handlungsweise und die Maßnahmen führten dazu, dass gezielte Angriffe auf den Verbund abgewehrt werden konnten.

Fallstudie 4: IT-Sicherheit für Geschäftsprozesse im Finanzsektor – die Managementlösung PREVENT. Die Fallstudie beschreibt am Beispiel der fiktiven FutureBank und des ebenfalls fiktiven Dienstleisters FutureRZ die technische Lösung PREVENT, die das Risikomanagement in Banken unterstützt, indem ein Dashboard zur Verfügung gestellt wird, das die Daten aus einer Vielzahl an Quellen aggregiert und aufbereitet. Es entsteht eine Datenbasis, die die Wechselwirkungen zwischen verschiedenen Ebenen – Geschäfts- und Serviceprozesse, Funktionen, IT-Systeme und Netzwerk – abbilden kann und aus der verschiedene Sichten bedarfsgerecht erzeugt werden.

Dies erlaubt neue einheitliche Risikobewertungen und löst heterogene Risikomanagementlandschaften ab. Nun können von der Managementebene aggregierte Risiken erkannt werden, die über dem als kritisch eingestuften Schwellenwert der Bank liegen und die zuvor als Einzelrisiken nicht im Fokus von Minimierungsmaßnahmen waren. So soll die Entscheidungsfindung für Verantwortliche verbessert werden.

Fallstudie 5: Informationssicherheit bei SAP SE – Die längste Human Firewall der Welt. Die Human Firewall ist eine Kampagne zur Informationssicherheit der SAP SE. Key Visual ist eine Kette von Mitarbeitern von SAP mit verschränkten Armen – ein Symbol dafür, dass die Mitarbeiter keine Bedrohung zu SAP durchlassen. Mitarbeiter absolvieren eine Schulung zur Informationssicherheit und können mit ihrem Foto und einem individuellen Statement Teil der Human Firewall werden.

Die Fallstudie thematisiert Vertrauen in Mitarbeiter und Awareness zur Informationssicherheit: Kunden können das Vertrauen in SAP und seine Produkte und Dienstleistungen verlieren, wenn Mitarbeiter mit Fragestellungen der IT-Sicherheit nicht sensibel umgehen. Die Fallstudie thematisiert die Einbindung dieser Kampagne in verschiedene IT-Sicherheitsmaßnahmen, genau wie Spaß und Unterhaltung durch die einzelnen Elemente, die Messung der Awareness der Mitarbeiter sowie den Erfolg.

Fallstudie 6: Informationssicherheit durch IT-gestützte Klassifizierung von Dokumenten und E-Mails. ClassifyIt von ugarbe.de software ist ein PlugIn für Microsoft Office. Es unterstützt Nutzer bei der Klassifikation von Dokumenten und E-Mails. Die Software kann so konfiguriert werden, dass die Firewall sicherstellt, dass nur Dokumente und E-Mails mit entsprechender Klassifikation eine Organisation verlassen und dass dem Sicherheitsniveau entsprechende Verschlüsselungen gewählt werden.

Die Fallstudie beschreibt, dass ca. 60% bis 75% aller Dokumente in einer Organisation sensitiver Natur und 5% bis 10% sogar „echte kritische Informationen“ sind. ClassifyIt adressiert Risiken, die mit Sorglosigkeit im Umgang mit Informationen oder Weitergabe von Informationen an Unberechtigte einhergehen und letzten Endes einen Vertraulichkeits- oder Integritätsverlust von Daten bedeuten können. Die Software wird über Standard-Softwareverteilungstools in einer Organisation ausgerollt, die Einstellungen und Sicherheitsniveaus können von der Organisation direkt angepasst werden.

Die Fallstudie beschreibt einen wichtigen Erfolgsfaktor: das IT-Sicherheitsprodukt passt sich an die Organisation an – und nicht umgekehrt. So bietet ClassifyIt ein Höchstmaß an Flexibilität, das zudem mit einer hohen Nutzerfreundlichkeit einhergeht.

Fallstudie 7: IT-Sicherheit in der Nahrungsmittelindustrie: Tradition und Hochverfügbarkeit. Ein Nahrungsmittelhersteller steht vor besonderen Herausforderungen der IT-Sicherheit: Die Verarbeitung von sensiblen Rohstoffen wie etwa Milch erfordert eine Hochverfügbarkeit der Produktionsanlagen. Im Beispiel setzt der IT-Verantwortliche eine Strategie um, in der traditionelle organisatorische Maßnahmen um moderne Maßnahmen zur Datensicherung und Prozessautomatisierung ergänzt werden. Den Mitarbeitern in der IT und ihrer Ausbildung kommt dabei eine zentrale Rolle zu.

Themen der Fallstudie sind die IT-Sicherheitsphilosophie und Aspekte der Echtzeitsicherung des SAP-Systems, die VLAN-Kapselung der Produktionsanlagen zur Gewährleistung sicherer Fernwartung und die Integration der Mitarbeiter in IT-Prozesse.

4 Cross Case-Analyse

Die Fallstudien decken unterschiedliche Kritische Infrastrukturen und unterschiedliche IT-Sicherheitsthemen ab. Im Zuge einer übergreifenden Qualitativen Inhaltsanalyse war es das Ziel, in den Fallstudien Muster, Gemeinsamkeiten und Unterschiede zu identifizieren, die Rückschlüsse auf allgemeingültige Zusammenhänge, bewährtes Vorgehen und für den Erfolg relevante Rahmenumstände erlauben.

Die Zieldimension „IT-Sicherheit“ motiviert die ersten vier Codes: Angelehnt an die Themen des Förderschwerpunkts ITS|KRITIS ist es von besonderem Interesse aus der Praxis Erkenntnisse zu den Themenschwerpunkten *Neue Ansätze zur Beurteilung von IT-Sicherheit* sowie *Neue Ansätze zur Verbesserung der IT-Sicherheit* zu erlangen, gerade im Hinblick auf die Notwendigkeit *einfacher und kosteneffizienter* Lösungen für kleine und mittlere Unternehmen. Dies wird durch die Codes *Beurteilung und Messung von IT-Sicherheit*, *Erhöhung der IT-Sicherheit*, *Einfachheit der Maßnahme* und *Kosteneffizienz der Maßnahme* erfasst.

Tabelle 2. Übersicht über ausgewählte Codes der Qualitativen Inhaltsanalyse

Nr.	*Thema*	*Code*
1	Zieldimension „IT-Sicherheit“	Beurteilung und Messung von IT-Sicherheit
2		Erhöhung der IT-Sicherheit
3		Einfachheit der Maßnahme
4		Kosteneffizienz der Maßnahme
5	Kontext	Nebeneffekte
5.1		Wechselwirkungen mit anderen IT-Sicherheitsmaßnahmen
5.2		Einflüsse auf andere Geschäftsprozesse
6		Erfolgsfaktoren für die Implementierung
8		IT-Sicherheitsphilosophie
8.1		Vertrauensfokus in TOM
8.2		Aspekt Organisationskultur

Darüber hinaus interessieren uns auch praktische Aspekte der Implementierung von IT-Sicherheitsmaßnahmen oder -konzepten in einem Unternehmen, sodass neben den bisher genannten Codes – welche sich auf eine Sicherheitsmaßnahme im engeren Sinne

fokussieren – auch auf andere Bereiche des Unternehmens übergreifende Sachverhalte untersucht werden. Dies ist Motivation für die weiteren Codes *Nebeneffekte*, *Erfolgsfaktoren für die Implementierung*, *Treiber und Auslöser*, *IT-Sicherheitsphilosophie* und *Adressierte Risiken*. Ausgewählte Codes sind in Tabelle 2 aufgeführt.

4.1 Ergebnisse Zieldimension „IT-Sicherheit“ (Codes 1 bis 4)

Beurteilung und Messung von IT-Sicherheit (Code 1). Die Aufrechterhaltung der Informationssicherheit einer Organisation erfordert eine kontinuierliche Verbesserung, die wiederum eine fortwährende Messung und Beurteilung notwendig macht [12]. In den Fallstudien werden Methoden der Praxis in Nr. 3, Nr. 4 und Nr. 5 beschrieben. Es ist zu erkennen, dass sowohl qualitative als auch quantitative Daten erhoben werden. So nutzt SAP bspw. Fragebögen, um die Einschätzung der Mitarbeiter hinsichtlich ihrer Awareness zur Informationssicherheit zu erheben.

Zur Überprüfung der Eignung und Wirksamkeit von Maßnahmen beziehen die kbo sowohl interne IT-Experten als auch externe Dienstleister bspw. für Penetrationstests mit ein. Ferner werden bei kbo zur Beurteilung und Messung der IT-Sicherheit Metriken wie die Erkennungsrate von Malware, Anzahl an Incidents u.a. berücksichtigt. Die Ergebnisse solcher Messungen und Einschätzungen können entsprechend der adressierten Zielgruppe aufbereitet werden (z.B. Effektivitätsmessungen, Berichte). Das Bundesamt für Sicherheit in der Informationstechnik (BSI) sieht hier vorrangig das Management und insbesondere das Sicherheitsmanagement als Adressat der Ergebnisse [13], „um seinen Lenkungs- und Steuerungsaufgaben nachkommen zu können“ [12].

Erhöhung der IT-Sicherheit (Code 2). Das BSI empfiehlt im Zuge eines ganzheitlichen Informationssicherheitsansatzes in den IT-Grundschutz Katalogen sowohl präventive Maßnahmen als auch Maßnahmen zur Behebung von Sicherheitsvorfällen [14]. Als Hilfestellung für Betreiber von KRITIS und Nicht-KRITIS ist der Standard 100-4 zu nennen, der das Notfallmanagement adressiert [15]. Ebenso bietet das National Institute of Standards and Technology zu diesem Thema eine Publikation an [16].

In der Analyse der Fallstudien wird ersichtlich, dass die beschriebenen Maßnahmen primär präventive Maßnahmen sind, in Teilen aber auch Maßnahmen des Notfallmanagements berücksichtigen. Exemplarisch ist hier Fallstudie Nr. 7 hervorzuheben: „Die Rechenzentren […] beinhalten jeweils ein komplettes physisches Serversystem für SAP […]. Im Backup-Rechenzentrum läuft parallel ein zweites, baugleiches SAP-System, auf das zur Absicherung mit einem Zeitversatz […], auf Transaktionsebene alle Bewegungen des Systems übertragen werden“. Unter der Notwendigkeit der Hochverfügbarkeit in der Nahrungsmittelverarbeitung ist in dieser Fallstudie Redundanz ein wichtiges Thema.

Das BSI schreibt in [17] von organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsmaßnahmen, die auch in den Fallstudien wiederzufinden sind. So beschreibt Fallstudie Nr. 5 Maßnahmen, die den Faktor Mensch adressieren. Maß-

nahmen wie die o.a. Redundanz (Nr. 7) oder die Schaffung eines Gremiums zur Bewertung der IT-Bedrohungslage (Nr. 3) fokussieren mehr organisatorische Aspekte, können aber durch personelle und technische Maßnahmen unterstützt werden.

Darüber hinaus beschreiben die Fallstudien Nr. 1, 2 und 6 primär technische Maßnahmen, wie eine Software zur Datenklassifikation, eine Fernwartungslösung oder eine Software zur Absicherung des Standardprozesses für die digitale Tatortfotografie.

IT-Sicherheitsmaßnahmen wirken unterschiedlich auf IT-Risiken. Die Risikobehandlung ist nach Definition der DIN ISO IEC 27000 ein „Prozess der Auswahl und Umsetzung von Maßnahmen zur Modifizierung des Risikos“ [18] und Organisationen stehen nach BSI-Standard 100-3 [13] verschiedene Möglichkeiten offen, mit Risiken umzugehen. Während die Software ClassifyIt eine ergänzende Schutzmaßnahme darstellt, ist die Nutzung von Thin Clients (Nr. 7) der Risikovermeidung zu zuordnen.

Ein weiterer Punkt, der in der Analyse festgestellt wurde, ist der unterschiedliche Adressatenkreis durch die IT-Sicherheitsmaßnahmen. In Summe adressieren die Maßnahmen in den Fallstudien alle Mitarbeiter, ausgewählte IT-Nutzer, IT-Fachpersonal, die Managementebene oder externe Firmen wie Zulieferer, Hersteller oder Partner.

Einfachheit der Maßnahme (Code 3). Mit diesem Code werden in den Fallstudien jene Textstellen codiert, die Aussagen zur Komplexität, dem eingesetzten bzw. zukünftig zu erwartenden Aufwand und alles weitere hinsichtlich der Einfachheit einer IT-Sicherheitsmaßnahme treffen. So entsteht eine konkrete Vorstellung davon, was eine einfache IT-Sicherheitsmaßnahme in der Praxis für Unternehmen ausmacht. In der Analyse zeigte sich, dass sich eine Einteilung in drei Kategorien anbietet; so waren in den Fallstudien mehrere Erwähnungen im Kontext der Einfachheit hinsichtlich *Nutzerfreundlichkeit*, *Implementierungsaufwand* sowie den für die Maßnahme erforderlichen *Schulungsaufwand* (sowohl für Nutzer als auch für die Administration) vorhanden.

Auffallend ist, dass in allen Fallstudien die Nutzerfreundlichkeit und Einfachheit der Implementierung der betrachteten Maßnahme mehrfach betont wird. Darüber hinaus ist zu erkennen, dass die Integration von neuen IT-Sicherheitsmaßnahmen in bestehende Prozesse – welche weder eine organisationale Anpassung von Geschäftsprozessen oder besondere Maßnahmen von Anwendern erforderten – besonders reibungsarm eingeführt werden konnten (Nr. 1, 2, 5, 6). Auch eine Implementierung in bestehende technische Anlagen und die Einbindung in vorhandene Software sowie leichte und transparente Konfiguration wurden als Merkmale der Einfachheit erwähnt.

Kosteneffizienz der Maßnahme (Code 4). Wie in jeder unternehmerischen Entscheidung spielen ebenso bei IT-Sicherheitsmaßnahmen finanzielle, personelle und zeitliche Ressourcen eine Rolle [1]. Auch wenn das IT-Sicherheitsbudget in den meisten Unternehmen wächst [19], bindet die Erreichung und Erhaltung eines bestimmten Sicherheitsniveaus in allen drei Bereichen Ressourcen. Daher muss das Ziel auch hier eine kostenbewusste Lösung sein. Gordon und Loeb stellen zudem die Verwundbarkeit von Informationen und den möglichen Schaden ins Verhältnis zu den nötigen Ausgaben, stellen jedoch nicht zwingend eine Verbesserung der IT-Sicherheit durch mehr Ausga-

ben in diesem Bereich fest [20]. Für die Kosteneffizienz von Projekten oder Umsetzungen steht zunächst offensichtlich eine schnelle Amortisation der Investitionen im Vordergrund. In der Regel ist es bei IT-Sicherheitsinvestitionen jedoch nicht möglich, eine exakte Kalkulation der Wirtschaftlichkeit für IT-Sicherheitsprojekte durchzuführen, da ihr Ertrag eben nicht unmittelbar messbar ist [21].

Die Fallstudien thematisieren die Kosteneffizienz unterschiedlich. In der Fallstudie zum Standardprozess in der digitalen Tatortfotografie wird Kosteneffizienz durch direkte monetäre Einsparungen erreicht und ist damit sehr gut belegbar (Nr. 2). Typischer ist eine schwierige Bezifferung der Einsparungen, wie im Beispiel der Fallstudie Nr. 1, in der eine gut realisierte Fernwartung Kosten reduziert, was jedoch kaum exakt messbar ist. Eine weitere Möglichkeit Kosteneffizienz zu gewährleisten ist die Reduktion des Schulungsaufwands wie dies bei ugarbe.de software vorgesehen ist (Nr. 6).

Gerade vor dem Hintergrund, dass Unternehmen regelmäßig nur einen Bruchteil des zu erwartenden Schadens investieren [20], fällt auf, dass insgesamt auch in den Unternehmen der untersuchten Beispiele wenig Augenmerk auf das Verhältnis zwischen Kosten und dem zu erwartenden Schaden gelegt wird.

4.2 Kontext (Codes 5, 6 und 8)

Die Implementierung einer Maßnahme zur Förderung der IT-Sicherheit in einem Unternehmen kann nicht isoliert betrachtet werden. Da IT-Sicherheit gerade nicht nur ein AddOn zu bestehenden Abläufen einer Organisation ist, sondern nahezu immer einen Eingriff in bestehende Geschäftsprozesse – technisch oder organisational – bedeutet bzw. erfordert, werden in diesem Abschnitt die Ergebnisse der Analyse der kontextualen Dimensionen der Sicherheitsmaßnahmen in den Fallstudien beschrieben.

Diesbezüglich werden Fallstudien nach Aussagen zu Wechselwirkungen, zur IT-Sicherheitsphilosophie sowie damit zusammenhängenden Erfolgsfaktoren für die Implementierung einer IT-Sicherheitsmaßnahme analysiert. Die Analyse zeigt auf, dass die Betrachtung der organisationalen IT-Sicherheit stets ganzheitlich mit Anpassungen bei Personal und Organisation erfolgen muss – selbst dann, wenn nur eine technische Maßnahme in das Unternehmen eingeführt wird.

Nebeneffekte (Code 5). Das BSI empfiehlt in der Vorgehensweise gemäß IT-Grundschutz die Anwendung von organisatorischen, infrastrukturellen, personellen und technischen Sicherheitsmaßnahmen [17]. Dabei kann es Wechselwirkungen der IT-Sicherheitsmaßnahmen mit anderen IT-Sicherheitsmaßnahmen geben.

In Fallstudie Nr. 6 kann die Software ClassifyIt, die als Microsoft Office PlugIn Anwender in der Klassifikation von Dokumenten unterstützt, durch die Firewall unterstützt werden: die Firewall erlaubt nur das Versenden von Dokumenten, die die Organisationsgrenzen verlassen dürfen. Hier ist ClassifyIt von anderen IT-Sicherheitsmaßnahmen abhängig. Die Fernwartungslösung aus Fallstudie Nr. 1 hingegen ist technisch von anderen IT-Sicherheitsmaßnahmen unabhängig, bedarf neben der technischen Implementierung jedoch Maßnahmen auf organisatorischer und personeller Ebene.

Das BSI beschreibt die Rolle von IT-Sicherheitsmanagement wie folgt: „Die Schaffung von Informationssicherheit ist kein Selbstzweck. […] Informations- und Kommunikationstechnik soll die Ziele einer Institution sinnvoll unterstützen und dient zur Unterstützung von Geschäftsprozessen“ [12]. In der Analyse der Fallstudien konnten verschiedene Geschäftsprozesse erhoben werden, die unmittelbar von den Maßnahmen der IT-Sicherheit beeinflusst werden: Beschaffung, Change Management, Dokumentenmanagement, Informationspolitik (intern), IT-Support, Öffentlichkeitsarbeit, Personalverwaltung, Wartung, Zahlungsverkehr (in alphabetischer Reihenfolge).

Maßnahmen der IT-Sicherheit oder Informationssicherheit hören – genau wie Geschäftsprozesse – nicht an einer Organisationsgrenze auf. Auch die Schnittstellen von Geschäftsprozessen Dritter müssen mitbetrachtet werden.

IT-Sicherheitsphilosophie (Code 8). Das BSI nennt als Faktoren, die bei der Konzeption und Planung von Sicherheitsprozessen berücksichtigt werden sollen, u.a. Umwelteinflüsse in Form von sozialen und kulturellen Rahmenbedingungen [17]. IT-Sicherheit, wenn sie gelebt wird, wird Teil der Organisationskultur und die Maßnahmen können die Kultur mitprägen [22].

Die Human Firewall von SAP (Nr. 5) fördert neben der Awareness das Commitment der Mitarbeiter und fließt in die gelebte Organisationskultur ein. Im Unternehmen aus Fallstudie Nr. 7 dagegen gilt neben Einsatzbereitschaft und langjähriger Beschäftigung das Commitment als wichtiger Erfolgsfaktor für die Umsetzung von IT-Sicherheit.

Die Fallstudie kbo (Nr. 3) thematisiert, dass sich aller Einsatz von IT nach den Bedürfnissen des Patienten und dem Datenschutz zu richten hat, was der IT-Sicherheit ambivalent gegenübersteht. In der Fallstudie Nr. 1 wird auf Kompetenzstreitigkeiten oder Machtverlust als Resultat der IT-Sicherheitsmaßnahmen hingewiesen, während die Fallstudie SAP (Nr. 5) Vertrauen in die Mitarbeiter aber auch Vertrauen der Kunden in SAP als zentralen Bestandteil hervorhebt.

Ein Thema der Unternehmensphilosophie ist der „Faktor Mensch“ – der Mensch als mögliche Fehlerquelle oder Risiko der IT-Sicherheit. In der Balance zwischen dem Vertrauen in den Menschen und der Kontrolle durch Technik gibt es Unterschiede in den Ansätzen. In den Fallstudien zu ClassifyIt von ugarbe.de software, der Human Firewall von SAP und der IT-Sicherheitsstrategie beim Nahrungsmittelproduzenten (Nr. 7) wird der Faktor Mensch thematisiert und als potenzielles Risiko bewertet.

Die Ansätze von Fallstudie Nr. 6 und Nr. 7 adressieren das Risiko durch den Menschen mit technischen Maßnahmen, während SAP (Nr. 5) direkt beim Menschen ansetzt.

In den Fallstudien sind die Zusammenhänge zwischen Organisationskultur, dem Faktor Mensch und IT-Sicherheit vielfältig. Dennoch ist Kultur immer ein Bestandteil des Rahmens, in dem IT-Sicherheit stattfindet.

Erfolgsfaktoren für die Implementierung (Code 6). In den untersuchten Fallstudien ergeben sich Gemeinsamkeiten in Bezug auf Faktoren, die eine erfolgreiche Implementierung begünstigen oder sogar Voraussetzung dafür sind. So ist in vier Fallstudien ein erfolgreiches Einbinden der Management-Ebene ein wichtiger Faktor (Nr. 1, 4, 5, 6).

Daneben wird als weiterer Faktor die Akzeptanz der Maßnahme (Nr. 1, 4, 6, 7), die durch Nutzerfreundlichkeit der Maßnahme gefördert werden kann (Nr. 6), identifiziert.

Insgesamt zeichnet sich ab, dass es wichtig ist, alle entscheidenden Organisationseinheiten einzubeziehen und „an einem Strang zu ziehen". So ist es wichtig, alle involvierten Parteien einzubeziehen (Nr. 1, 3) und eine effektive Zusammenarbeit zu ermöglichen (Nr. 2). Dies steht auch im Einklang mit der Empfehlung des BSI, dass ein Realisierungsplan für die Umsetzung eines Sicherheitskonzepts neben der Bereitstellung von Ressourcen durch das Management auch die Festlegung von Verantwortlichkeiten enthalten sollte [12]. Dabei soll laut BSI auch die Informationssicherheit in die Abläufe und Prozesse der jeweiligen Organisation integriert werden.

5 Zusammenfassung und Diskussion

Wir haben sieben Fallstudien durchgeführt, die entweder Projekte zur Erhöhung der IT-Sicherheit, IT-Sicherheitskonzepte von Unternehmen oder einzelne IT-Sicherheitsmaßnahmen eines Dienstleisters qualitativ untersucht haben.

Bei den betrachteten Unternehmen kamen sowohl technische als auch organisatorische IT-Sicherheitsmaßnahmen zum Einsatz, die teilweise Angriffe von außen, teilweise das mögliche Fehlverhalten eigener Mitarbeiter adressieren.

Um Muster in der Fallstudienserie zu erkennen, haben wir nach Fertigstellung der Fallstudien eine Cross Case-Analyse in Form einer Qualitativen Inhaltsanalyse nach Mayring durchgeführt. Die Auswahl der Codes folgte dabei einerseits der Untersuchung von Aspekten der einzelnen IT-Sicherheitsmaßnahmen, andererseits der Betrachtung kontextueller Dimensionen bei der Implementierung der neuen Maßnahme in den untersuchten Organisationen.

Dieser Artikel leistet einen Beitrag zum Verständnis zu den Gesamtzusammenhängen von erfolgreichen IT-Sicherheitsprojekten und Implementierungen von IT-Sicherheitskonzepten. Die Codes selbst stellen einen Analyserahmen für IT-Sicherheitsprojekte dar und sollen bei der Erstellung zukünftiger Fallstudien im Kontext der IT-Sicherheit von Unternehmen und Kritischen Infrastrukturen Impulse für die Auswahl des Untersuchungsgegenstands und der Entwicklung von Forschungsfragen bieten.

Für die vorliegende Arbeit gelten die methodeninhärenten Limitationen von Fallstudien. Die Generalisierbarkeit der Ergebnisse ist durch Anzahl und Auswahl der Fallstudien eingeschränkt möglich; es bleibt jedoch abzuwarten, inwiefern darauf aufbauende qualitative und auch quantitative Forschung die gefundenen Gemeinsamkeiten und Unterschiede bestätigt oder Grenzen der Ergebnisse aufzeigt.

6 Acknowledgements

Wir bedanken uns bei allen Fallstudienpartnern und Interviewpartnern für die Fallstudien, den weiteren Autoren der Fallstudien T. Bollen, T. Gurschler, T. Kehr, S. Lücking sowie bei unseren Kollegen im Projekt VeSiKi. Den Gutachtern sind wir für die hilfreichen und konstruktiven Kommentare dankbar. Wir bedanken uns beim BMBF für die Förderung des Projekts VeSiKi mit den Fallstudien (FKZ: 16KIS0213).

References

1. Zetter, K.: Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown Publishers, New York (2014).
2. Strathmann, M.: Malware führte zum Blackout, http://www.zeit.de/digital/internet/2016-01/stromausfall-hacker-ukraine-blackenergy.
3. BSI: Die Lage der IT-Sicherheit in Deutschland 2016. , Bonn (2016).
4. BMI: Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), (2009).
5. Yin, R.K.: The Case Study Crisis: Some Answers. Adm. Sci. Q. 26, 58–65 (1981).
6. Wilde, T., Hess, T.: Methodenspektrum der Wirtschaftsinformatik: Überblick und Portfoliobildung, http://www.wim.bwl.uni-muenchen.de/download/epub/ab_2006_02.pdf, (2006).
7. Eisenhardt, K.M.: Building theories from case study research. Acad. Manag. Rev. 532–550 (1989).
8. Schubert, P., Wölfle, R.: The Experience Methodology For Writing IS Case Studies. Am. Conf. Inf. Syst. 19–30 (2006).
9. Yin, R.K.: Case Study Research - Design and Methods. SAGE Publications Inc., Thousand Oaks, London, New Delhi (2003).
10. Mayring, P.: Qualitative Inhaltsanalyse. Grundlagen und Techniken. Beltz (2008).
11. Bundesgesetzblatt: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz, Bundesgesetzblatt Jahrgang 2015 Teil I Nr. 31), (2015).
12. BSI: BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS), (2008).
13. BSI: BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz, (2008).
14. BSI: IT-Grundschutz-Kataloge - 15. Ergänzungslieferung, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/GSTOOL/gstool-html_el15_zip.zip.
15. BSI: BSI-Standard 100-4: Notfallmanagement, (2008).
16. Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witte, G., Scarfone, K.: NIST Special Publication 800-184: Guide for Cybersecurity Event Recovery. (2016).
17. BSI: BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, http://www.bsi.bund.de/gshb, (2008).
18. DIN: DIN ISO/IEC 27000, (2011).
19. VeSiKi: Monitor IT-Sicherheit Kritischer Infrastrukturen, https://monitor.itskritis.de/monitor1/, (2017).
20. Gordon, L. a., Loeb, M.P.: The economics of information security investment. ACM Trans. Inf. Syst. Secur. 5, 438–457 (2002).
21. Stöwer, M.: Beispiele für die Wirtschaftlichkeit von Informationssicherheit, (2011).
22. Helisch, M., Pokoyski, D., Beyer, M., Haucke, A., Prantner, K.: Security Awareness - Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung. Vieweg+Teubner Verlag, Wiesbaden (2009).