Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen

Ulrike Lechner · Manfred Hofmeier · Steffi Rudel · Sebastian Dännart

Universität der Bundeswehr München
{ulrike.lechner | manfred.hofmeier | steffi.rudel | sebastian.daennart}@unibw.de

Zusammenfassung

Um die IT-Sicherheit Kritischer Infrastrukturen zu studieren, wurde im Rahmen des Forschungsprojektes VeSiKi im Förderschwerpunkt ITS|KRITIS die CASE|KRITIS Fallstudienserie durchgeführt. Sie bietet Erfahrungen aus erster Hand und berichtet über bewährte Strategien zur Umsetzung von IT-Sicherheit in verschiedenen Organisationen. Die Fallstudienserie besteht aus neun Fallstudien und einer vergleichenden Cross-Case-Analyse. Dieser Beitrag stellt den Kontext von drei Fallstudien dar, die als Kurzbeiträge im Rahmen eines Workshops auf der D·A·CH Security 2018 präsentiert werden. Ziel des Beitrags sowie der Fallstudienserie 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. Die vollständigen Fallstudien sowie detaillierte Beschreibungen der Methodik und der Ergebnisse der Cross-Case-Analyse sind in dem Buch CASE|KRITIS [LDR+18] enthalten.

1 Einleitung

IT-Sicherheit ist in Kritischen Infrastrukturen (KRITIS) ein großes Thema – das ergibt sich häufig alleine schon aus den rechtlichen Anforderungen. Jedoch ist es nicht zielführend, IT-Sicherheit auf die technischen Aspekte zu reduzieren – vielmehr muss das Thema ganzheitlich in den Dimensionen Technik, Organisation und Mensch („TOM“) betrachtet werden. Fallstudien sind unsere Methode, Lösungen der IT-Sicherheit im konkreten Einsatz in Kritischen Infrastrukturen zu studieren.

Für viele Organisationen stellt sich die Frage, wie IT-Sicherheit konkret umgesetzt werden kann – das ist unsere Motivation. Um hier Hilfestellung zu leisten, hat das Forschungsprojekt Vernetzte IT-Sicherheit Kritischer Infrastrukturen (VeSiKi) im Rahmen des Förderschwerpunktes IT-Sicherheit für Kritische Infrastrukturen (ITS|KRITIS) Fallstudien erstellt. Diese Fallstudien beschreiben Lösungen zur IT-Sicherheit, wie sie konkret in Organisationen angewendet und umgesetzt werden und sollen als Good Practices dienen.

1.1 IT-Sicherheit in Kritischen Infrastrukturen

Das Bundesministerium des Innern (BMI) gibt in der Nationalen Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) eine offizielle Definition für KRITIS vor: demnach sind Kritische Infrastrukturen: „Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 240-251.

Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden“ [BMI09]. Das IT-Sicherheitsgesetz [Bund15] ist hier anwendbar auf die KRITIS-Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen, nicht jedoch „Medien und Kultur“ und „Staat und Verwaltung“, die vom BMI ebenfalls zu KRITIS-Sektoren gezählt werden. Die BSI-Kritisverordnung (BSI-KritisV) [BMI17] legt fest, welche Organisationen unter das IT-Sicherheitsgesetz fallen.

1.2 Der Förderschwerpunkt ITS|KRITIS und VeSiKi

Im Rahmen der Hightech Strategie der Bundesregierung und des Bundesministeriums für Bildung und Forschung (BMBF) begann im Jahr 2014 die Forschung im Förderschwerpunkt ITS|KRITIS. Im Förderschwerpunkt forschen dreizehn Projekte für die IT-Sicherheit der Kritischen Infrastrukturen in Deutschland: AQUA-IT-Lab, Cyber-Safe, INDI, ITS.APT, MoSaIK, PREVENT, PortSec, RiskViz, SecMaaS, SICIA, SIDATE, SURF und VeSiKi.

Abb. 1: Ergebnisse des kooperativen Forschungsprozesses in ITS|KRITIS

Das Begleitforschungsprojekt VeSiKi vernetzt die Verbundprojekte im Förderschwerpunkt ITS|KRITIS, unterstützt die Projekte im kooperativen Forschungsprozess sowie die Außendarstellung des Förderschwerpunkts und die Sichtbarkeit der Aktivitäten und Ergebnisse in der Öffentlichkeit und damit den Transfer in die Praxis. Ein Ergebnis aus der Arbeit von VeSiKi sind unter anderem die in dem vorliegenden Beitrag vorgestellten Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen (Abbildung 1). Eine erste Version der Cross-Case-Analyse mit 7 Fallstudien wurde auf der MKWI 2018 veröffentlicht [DDH+18].

2 Die Methode der CASE|KRITIS Fallstudien

Die Methodik für die Fallstudien orientiert sich an der eXperience-Methodik [ScWo06]. Die eXperience-Methodik will authentisches Wissen rund um E-Business und IT-Management vermitteln und stellt dazu ein Raster und Vorgehensmodell für Fallstudien sowie begleitende Materialien bereit. Angelehnt an diese Methodik wurden ein Rahmen für Fallstudien zum Thema IT-Sicherheit Kritischer Infrastrukturen sowie ein Prozess zur Erhebung der notwendigen Daten entwickelt und mit den Projekten im Förderschwerpunkt ITS|KRITIS im Jahr 2015 verfeinert. Die Datenerhebung stützt sich dabei auf Experteninterviews, Beobachtungen vor Ort und ergänzende Literaturrecherchen (Abbildung 2).

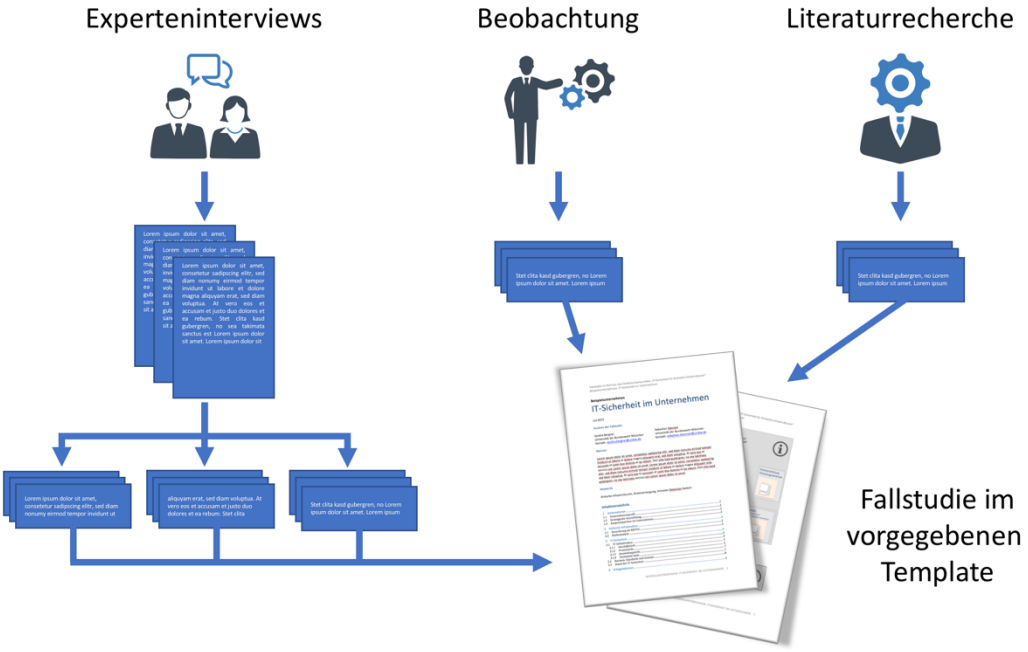

Abb. 2: Inhaltliche Quellen der Fallstudien (Quelle: [LDR+18])

Die CASE|KRITIS Fallstudienserie verwendet drei Arten von IT-Sicherheitsfallstudien.

- **Unternehmensbezogene Fallstudien** erfassen die gelebte IT-Sicherheit einer Organisation. Sie ermöglichen es, beispielgebende Umsetzungen von IT-Sicherheit in Unternehmen verständlich und strukturiert aufzuarbeiten. Die Fallstudien betrachten das Unternehmen ganzheitlich – immer aus der IT-Sicherheitsperspektive heraus. Dazu werden neben dem Unternehmen selbst unter anderem die Geschäftssicht, die relevante Anwendungslandschaft und die technische Sicht sowie bei Bedarf konkrete Prozesse vorgestellt.

- **Projektbezogene Fallstudien** beziehen sich auf ein konkretes IT-Sicherheitsprojekt. Die Fallstudien zu IT-Sicherheitsprojekten thematisieren die Implikationen von Projekten – von neuen Benutzeroberflächen über Schnittstellenprobleme bis hin zu prozessualen Änderungen in der Produktion und den Kosten-Nutzen-Betrachtungen solcher Projekte. Da die projektspezifischen Rahmenbedingungen – wie zeitlicher Rahmen oder Projektbudget – jedoch elementar für das Verständnis der fallspezifisch auftretenden Herausforderungen sind, wurde eine Projektsicht entwickelt, die sowohl die kontextbezogenen Rahmenbedingungen wie auch die IT-sicherheitsrelevanten Sichten in die Fallstudie integriert.
- **Produktbezogene Fallstudien** beschreiben die Implementierung oder den Einsatz von speziellen innovativen IT-Sicherheitstechnologien. Ist ein bestimmtes Produkt oder der Einsatz einer bestimmten Technologie von besonderer Bedeutung, thematisiert eine Fallstudie Prozesse, Anwendungssicht und Wechselwirkungen mit anderen Organisationsbereichen sowie Kosten/Nutzen dieses Produkts.

In der Cross-Case-Analyse wurden die Fallstudien auf Muster, Unterschiede und Gemeinsamkeiten untersucht [Yin03]. Dazu wurden alle Fallstudien einer Qualitativen Inhaltsanalyse nach Mayring unterzogen [Mayr15]. Die verwendenden Codes wurden deduktiv hergeleitet. Das Codeschema wurde in einem ersten Schritt iterativ in drei Workshops definiert. In der zweiten Phase wurden die Fallstudien jeweils zwei Mitarbeitern zugewiesen, die diese unabhängig voneinander mit dem entwickelten Codeschema analysierten und codierten. Der wesentliche Teil der Cross-Case-Analyse fand im sich anschließenden dritten Schritt statt. Die codierten Abschnitte der Fallstudien wurden vom Ursprungsmaterial losgelöst und stattdessen als Summe aller Aussagen zu einem jeweiligen Code betrachtet. Dazu wurden die codierten Aussagen aller Fallstudien miteinander verglichen und auf Muster, Gemeinsamkeiten und Unterschiede hin analysiert. Weiterhin fand auch ein Vergleich mit wissenschaftlicher sowie grauer Literatur zum durch den Code betrachteten Aspekt statt. So konnten abschließend die sich ggf. aufzeigenden Indizien für zugrunde liegende Zusammenhänge extrahiert und aufbereitet werden.

3 Fallstudien zur IT-Sicherheit

Die erstellten Fallstudien werden im Folgenden jeweils kurz vorgestellt. Die vollständigen Fallstudien sind in [LDR+18] enthalten. Die Fallstudien zu den Kliniken des Bezirks Oberbayern, zur Managementlösung PREVENT sowie zur Zentralen Leitstelle Ostthüringen werden in gesonderten Beiträgen im vorliegenden Konferenzband sowie im Rahmen eines Workshops auf der D·A·CH Security 2018 detaillierter vorgestellt.

3.1 Bundeswehr: AG IT-SecAwBw

Die Kampagne PIA (Durch Partnerschaft sicher – IT-Security Awareness) zielt auf die Erhöhung der IT-Sicherheit in der Bundeswehr ab. Key Visual dieser Kampagne ist ein Netzwerkstecker mit Gesicht – ein Symbol dafür, dass IT-Sicherheit nicht nur technische Maßnahmen umfasst, sondern auch den Human Factor adressiert. Die Arbeitsgruppe IT-Security Awareness der Bundeswehr (AG IT-SecAwBw) entwickelt(e) im Rahmen dieser Kampagne verschiedene Tools, die den IT-Sicherheitsbeauftragten der Dienststellen zur Verfügung gestellt werden, um die IT-Sicherheit sowohl im Inland als auch im Ausland für Soldaten und zivile Mitarbeiter der Bundeswehr zu erhöhen.

3.2 genua gmbh: Fernwartung Kritischer Infrastrukturen

Die Fallstudie thematisiert Risiken der Fernwartung industrieller Kontroll- und Steuerungssysteme in Kritischen 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.

3.3 itWatch GmbH: 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 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.

3.4 Kliniken des Bezirks Oberbayern: Risikomanagement

Den Kern der Fallstudie bildet die Reaktion der Kliniken des Bezirks Oberbayern (kbo) 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.

3.5 IT-Sicherheit in der Molkerei

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.

3.6 Die Managementlösung PREVENT für den Banksektor

Die Fallstudie beschreibt 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.

3.7 SAP SE: Die Human Firewall

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.

3.8 IT-Sicherheit in der Zentralen Leitstelle Ostthüringen

Der Alarmierungsprozess vom Absetzen eines Notrufs bis zur Alarmierung der Rettungskräfte muss auch bei Ausfall von IT-Komponenten möglich sein. Die Fallstudie betrachtet die Rückfallebenen und Redundanzen sowie die IT-Sicherheitskonzepte, um die Hochverfügbarkeit der Notrufnummer 112 mit dem Rettungswesen sicherzustellen, und zeigt die Fragen bei der Weiterentwicklung der Informations- und Kommunikationstechnologie einer Leitstelle auf. Wesentliche Erfolgsfaktoren in der täglichen Arbeit und der strategischen Weiterentwicklung sind

der Wille der Belegschaft der Leitstelle, die Infrastruktur mit ihren IT-Komponenten nicht nur zu kennen, sondern auch zu verstehen und allen Problemen auf den Grund zu gehen, um sie zu lösen.

3.9 Klassifizierung von Dokumenten und E-Mails

Die Fallstudie beschreibt die Software ClassifyIt, die IT-gestützt Dokumente und E-Mails klassifiziert und den Datentransfer zwischen Mitarbeitern und zwischen Organisationen absichert. Im Durchschnitt sind ca. 60% bis 75% aller Dokumente in einer Organisation sensitiver Natur, 5% bis 10% sogar „echte kritische Informationen“. ClassifyIt adressiert Risiken, die mit Sorglosigkeit im Umgang mit Informationen, Weitergabe von Informationen an Unberechtigte einhergehen und letzten Endes einen Vertraulichkeits- oder Integritätsverlust von Daten bedeuten können.

4 Erfolgreiche IT-Sicherheit: Cross-Case-Analyse

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. Im Folgenden werden ausgewählte Ergebnisse der Cross-Case-Analyse vorgestellt.

4.1 Beurteilung und Messung von IT-Sicherheit

Die Aufrechterhaltung der Informationssicherheit einer Organisation erfordert eine kontinuierliche Verbesserung, die wiederum eine fortwährende Messung und Beurteilung notwendig macht [BSI08a].

Es ist zu erkennen, dass sowohl qualitative als auch quantitative Daten erhoben werden. So nutzt SAP beispielsweise 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 beispielsweise 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).

4.2 Erhöhung der IT-Sicherheit

In der Analyse der Fallstudien wird ersichtlich, dass die beschriebenen Maßnahmen primär präventive Maßnahmen sind, in Teilen aber auch Maßnahmen des Notfallmanagements berücksichtigen.

Das BSI schreibt in [BSI08b] von organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsmaßnahmen, die auch in den Fallstudien wiederzufinden sind. So beschreibt die Fallstudie zur Human Firewall Maßnahmen, die den Faktor Mensch adressieren. Maßnahmen wie Redundanz oder die Schaffung eines Gremiums zur Bewertung der IT-Bedrohungslage fokussieren mehr organisatorische Aspekte, können aber durch personelle und technische Maßnahmen unterstützt werden.

Darüber hinaus werden in den Fallstudien technische Maßnahmen beschrieben, 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“ [DIN11] und Organisationen stehen nach BSI-Standard 100-3 [BSI08c] verschiedene Möglichkeiten offen, mit Risiken umzugehen. Während die Software ClassifyIt eine ergänzende Schutzmaßnahme darstellt, ist die Nutzung von Thin Clients 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.

4.3 Einfachheit der Maßnahme

In der Cross-Case-Analyse werden auch Passagen betrachtet, 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 zeigt sich, dass sich eine Einteilung in drei Kategorien anbietet; so sind 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. Auch eine Implementierung in bestehende technische Anlagen und die Einbindung in vorhandene Software sowie leichte und transparente Konfiguration wurden als Merkmale der Einfachheit erwähnt.

4.4 Kosteneffizienz der Maßnahme

Die Erreichung und Erhaltung eines bestimmten Sicherheitsniveaus bindet Ressourcen, wobei in dem meisten Organisationen das Budget für die IT-Sicherheit als zu gering eingeschätzt wird [VeSi17, VeSi18]. Daher muss das Ziel eine kostenbewusste Lösung sein.

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. Typischer ist eine schwierige Bezifferung der Einsparungen, wie im Beispiel der Fallstudie zur Fernwartung Kritischer Infrastrukturen, 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 ClassifyIt vorgesehen ist.

Gerade vor dem Hintergrund, dass Unternehmen regelmäßig nur einen Bruchteil des zu erwartenden Schadens investieren [GoLo02], 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.

4.5 Nebeneffekte

Das BSI empfiehlt in der Vorgehensweise gemäß IT-Grundschutz die Anwendung von organisatorischen, infrastrukturellen, personellen und technischen Sicherheitsmaßnahmen [BSI08b]. Dabei kann es Wechselwirkungen der IT-Sicherheitsmaßnahmen mit anderen IT-Sicherheitsmaßnahmen geben.

In der Analyse der Fallstudien wird sichtbar, dass IT-Sicherheitsmaßnahmen von anderen technischen und nicht-technischen IT-Sicherheitsmaßnahmen abhängig sein können, wie etwa im Fall der Klassifikationssoftware ClassifyIt. Umgekehrt 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.

4.6 Erfolgsfaktoren für die Implementierung

In den analysierten Fallstudien finden sich Gemeinsamkeiten bei Faktoren, die eine erfolgreiche Implementierung von IT-Sicherheitsmaßnahmen begünstigen oder sogar Voraussetzung dafür sind. Hier sind folgende Faktoren bedeutend.

Die Management-Ebene muss die Notwendigkeit der Maßnahmen erkennen und deren Umsetzung dann auch aktiv unterstützen, wie es auch vom BSI gefordert wird [BSI13].

Ein weiterer Faktor ist die Akzeptanz der Maßnahmen durch die Mitarbeiter bzw. die Anwender. Denn bei der Implementierung von Systemen oder Prozessen besteht immer das Risiko, dass sich Widerstände dagegen bilden.

Zudem sind Engagement und Commitment ein wesentlicher Faktor. So wollen beispielsweise die Mitarbeiter Probleme nicht einfach nur erkennen, sondern den Ursachen auf den Grund gehen, um Probleme dauerhaft zu verhindern.

Übergreifend zeichnet sich ab, dass es wichtig ist, alle entscheidenden Organisationseinheiten einzubeziehen und „an einem Strang zu ziehen“.

Insgesamt entsprechen die Erfolgsfaktoren für die erfolgreiche Implementierung von IT-Sicherheitsmaßnahmen weitgehend den Erfolgsfaktoren von Projekten im Allgemeinen. Besonders sind hier aber vor allem die Bedeutung der Bereitschaft, Ursachen und Zusammenhängen wirklich auf den Grund zu gehen, und die besondere Bedeutung des Managements.

4.7 Treiber und Auslöser

In der fallstudienübergreifenden Analyse hat sich gezeigt, dass eine Unterteilung in interne und externe Treiber bzw. Auslöser sinnvoll ist.

Allen in den Fallstudien mit einem Unternehmenskontext betrachteten Sicherheitskonzepten ist als einer der externen Treiber gemein, dass die Unternehmen sich den teilweise erhöhten gesetzlichen Anforderungen anpassen. Compliance konnte somit als wichtiger Treiber der betrachten Organisationen identifiziert werden. Dies ist insbesondere bei den Fallstudien mit einem KRITIS-Bezug deutlich zu erkennen.

Als weiterer externer Treiber sind bei zwei Fallstudien auch mögliche Reputationsverluste im Falle von IT-Sicherheitsvorfällen erwähnt worden, während eine veränderte Bedrohungslage oder Informationen zu IT-Angriffen auf Organisationen in derselben Branche nur in der Fallstudie zu den kbo ausschlaggebend waren.

Darüber hinaus konnten aber auch bei knapp der Hälfte der Fallstudien mehrere interne Treiber identifiziert werden. Diese reichten wiederum von einem allgemein hohen moralischen Selbstverständnis bzw. Verantwortungsbewusstsein für die eigenen Kunden, über effizienzbegründeten Vereinfachungen und Optimieren von Prozessen bis hin zum Vermeiden von Wissensverlusten.

Abschließend bleibt festzuhalten, dass die Heterogenität auch im Bereich der Treiber und Auslöser deutlich zu erkennen ist und jeder Anwendungskontext individuelle Rahmenbedingungen vorweist, die für Maßnahmen der IT-Sicherheit ausschlaggebend sein können.

4.8 IT-Sicherheitsphilosophie

Der Zusammenhang von IT-Sicherheit und kulturellen Aspekten ist wechselseitig. So sollen laut BSI unter anderem soziale und kulturelle Rahmenbedingungen wie regionale Kulturprägung und organisationale Aspekte bei der Planung von IT-Sicherheitsprozessen betrachtet werden [BSI08b]. Umgekehrt wird IT-Sicherheit, wenn sie gelebt wird, Teil der Organisationskultur und die Maßnahmen können die Kultur mitprägen [HePo09]. Auch in den Fallstudien findet sich diese wechselseitige Beziehung, etwa in Form von organisationskulturellen Faktoren, wie Commitment, welche den Erfolg von IT-Sicherheitsmaßnahmen begünstigen, oder in Form von Maßnahmen, die fester Bestandteil der Unternehmenskultur werden, so wie es beispielsweise bei der Human Firewall von SAP der Fall ist.

Ein Thema der IT-Sicherheit, das auch die Organisationskultur betrifft, ist der Faktor Mensch – der Mensch als Risiko für die IT-Sicherheit. Hier gibt es verschiedene Ansätze, diesem Risiko zu begegnen. Teils wird dieses Risiko mit technischen Maßnahmen adressiert, teils wird direkt beim Menschen angesetzt, wie etwa mit Maßnahmen zur IT-Sicherheitsawareness.

Die Zusammenhänge zwischen Organisationskultur, dem Faktor Mensch und IT-Sicherheit sind vielfältig. Dennoch ist Kultur immer ein Bestandteil des Rahmens, in dem IT-Sicherheit stattfindet, und sollte daher in Betrachtungen mit einbezogen werden.

4.9 Adressierte Risiken

Als Ergebnis des Vergleichs und der Analyse sämtlicher Textpassagen zu adressierten Risiken in den Fallstudien wurde eine deutliche Heterogenität festgestellt. Dies verdeutlicht, dass die unterschiedlichen Herangehensweisen der Unternehmen und vorgestellten Produkte nicht nur aufgrund der organisationalen und technologischen Unterschiede begründet sind, sondern auch initiale Beweggründe der zu begegnenden IT-Sicherheitsrisiken auch trotz der Gemeinsamkeiten Kritischer Infrastrukturen von Organisation zu Organisation sehr unterschiedlich wahrge-

nommen werden. So wurde die zugrundeliegende Vermutung, dass die Verfügbarkeit einer Kritischen Infrastruktur das über die gesamte Lieferkette im Vordergrund stehende Schutzziel aller beteiligten Organisationen sei, durch ein differenzierteres Verständnis der in den vorliegenden Fallstudien adressierten Risiken ersetzt bzw. um weitere heterogene Aspekte erweitert. Tatsächlich variieren die relevanten Gefährdungen bzw. Risiken in den Fallstudien deutlich; fast alle Bereiche des BSI-Gefährdungskatalogs finden dabei Beachtung.

Insgesamt ließen sich Erkenntnisse darüber gewinnen, wie in Unternehmen sowohl Auswirkungen auf den Produktivbetrieb, Schäden bei Kunden und auch die Sorge um Vertraulichkeits- und Integritätsverluste von Daten und Informationen eine bewusst getroffene Relevanz zugesprochen wird. Diese kann je nach Anwendungskontext Grundlage für Entscheidungen innerhalb des IT-Sicherheitsmanagements sein. Ebenfalls ist an dieser Stelle zu erwähnen, dass auch weiterreichende Folgen und Konsequenzen für die Wahl von Maßnahmen maßgeblich sein können: so ist auch ein möglicher Reputationsverlust als adressiertes Risiko für eine IT-Sicherheitsmaßnahme genannt worden.

5 Fazit

In den neun Fallstudien spielt die IT-Sicherheit die Hauptrolle. Auch vergegenwärtigen die Fallstudien die strategische Bedeutung von IT-Sicherheit für ein Unternehmen im Kontext von Innovation und Digitalisierung. Die Fallstudien sollen als Good Practices Mut machen, das gerade von kleinen und mittleren Unternehmen als abstrakt und schwierig wahrgenommene Thema der IT-Sicherheit anzugehen.

In der Cross-Case-Analyse wurde eine code-individuelle Betrachtung der Umsetzung von IT-Sicherheit durchgeführt. Die Ergebnisse der Analyse können als positive Erfahrungen der gegenwärtigen Praxis das Verständnis der Gesamtzusammenhänge erfolgreicher IT-Sicherheitsprojekte unterstützen. So können die Erkenntnisse der Cross-Case-Analyse für die Planung zukünftiger Einführungen von IT- Sicherheitsmaßnahmen als Inspiration dienen.

Das Buch CASE|KRITIS [LDR+18] rundet die Thematik der IT-Sicherheit in Kritischen Infrastrukturen durch weitere Fachbeiträge zu gesetzlichen Anforderungen, dem Stand der Technik, dem Themenschwerpunkt Innovation sowie einer Interviewserie zu Zukunftsstrategien in der IT-Sicherheit ab.

Danksagung

Wir danken dem Bundesministerium für Bildung und Forschung (BMBF) für die Möglichkeit der Forschung im Rahmen des Projektes VeSiKi, Förderkennzeichen 16KIS0213K. Wir bedanken uns bei Torsten Bollen, Thomas Diefenbach, Tamara Gurschler, Andreas Rieb und allen anderen Fallstudienautoren für die Erstellung der Fallstudien und vor allem bei allen Fallstudienpartnern und Interviewpartnern für die Zusammenarbeit.

Literatur

[BMI09] BMI: Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) (2009).

[BMI17] BMI: Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) vom 22. April 2016 (BGBl. I S.

958), geändert durch Artikel 1 der Verordnung vom 21. Juni 2017 (BGBl. I S. 1903) (2017).

[BSI08a]: BSI-Standard 100-1: Managementsysteme für Informationssicherheit (2008).

[BSI08b] BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise. 2.0 (2008).

[BSI08c] BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz (2008).

[BSI13] BSI: IT-Grundschutz - M 3.44 Sensibilisierung des Managements für Informationssicherheit (2013). https:// www. bsi. bund. de/ DE/ Themen/ ITGrundschutz/ ITGrundschutzKataloge/Inhalt/_content/m/m03/m03044.html?nn=6604926 [Zugegriffen November 27, 2017].

[Bund15] Bundesgesetzblatt: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). Bundesgesetzblatt Jahrgang 2015 Teil I Nr. 31.

[DDH+18] S. Dännart, T. Diefenbach, M. Hofmeier, A. Rieb, U. Lechner: IT-Sicherheit in Kritischen Infrastrukturen – eine Fallstudien-basierte Analyse von Praxisbeispielen. In: Tagungsband Multikonferenz Wirtschaftsinformatik (2018) 1357-1368.

[DIN11] DIN ISO/IEC 27000 (2011).

[GoLo02] L. A. Gordon, M. P. Loeb: The economics of information security investment. ACM Trans. Inf. Syst. Secur. 5, (2002) 438-457.

[HePo09] M. Helisch, D. Pokoyski: Security Awareness – Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung. Vieweg+Teubner (2009).

[LDR+18] U. Lechner, S. Dännart, A. Rieb, S. Rudel: CASE KRITIS – Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen, Logos (2018).

[Mayr15] P. Mayring: Qualitative Inhaltsanalyse – Grundlagen und Techniken, 12. Aufl., Beltz (2015).

[ScWo06] P. Schubert, R. Wölfle: The eXperience Methodology For Writing IS Case Studies. In: R. Wölfle, P. Schubert (Hrsg.): Americas Conference on Information Systems (AMCIS) (2006) 19-30.

[VeSi17] VeSiKi: Monitor IT-Sicherheit Kritischer Infrastrukturen (2017). https:// monitor.itskritis.de/monitor1.

[VeSi18] VeSiKi: Monitor 2.0 IT-Sicherheit Kritischer Infrastrukturen (2018). https:// monitor.itskritis.de/monitor2.

[Yin03] R. K. Yin: Case Study Research – Design and Methods. SAGE Publications, 26(1), (2003) 93–96.