Ulrike Lechner | Sebastian Dännart
Andreas Rieb | Steffi Rudel

CASE KRITIS

Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen

λογος

Ulrike Lechner | Sebastian Dännart | Andreas Rieb | Steffi Rudel

CASE|KRITIS

Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen

λογος

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Lektorat: Dr. Heiner Lohmann, www.lektorat-lohmann.de

Coverdesign: Artes Advertising, www.artes.de

© Coverbild: iStockphoto

© Copyright Logos Verlag Berlin GmbH 2018

Alle Rechte vorbehalten.

ISBN 978-3-8325-4727-1

Logos Verlag Berlin GmbH
Comeniushof, Gubener Str. 47,
10243 Berlin
Tel.: +49 (0)30 42 85 10 90
Fax: +49 (0)30 42 85 10 92
INTERNET: http://www.logos-verlag.de

Vorwort

Die Kritischen Infrastrukturen in Deutschland sind sicher: Die Produkte und Dienstleistungen für die moderne Zivilgesellschaft stehen zur Verfügung. Und das soll auch in Zukunft so bleiben. Das stellt gleichermaßen die großen wie auch kleinere Unternehmen als Betreiber Kritischer Infrastrukturen vor große Aufgaben. Denn nicht mehr nur IT-Landschaften in Büros und Verwaltung müssen sicher sein, sondern Informations- und Kommunikationstechnologien als Teil von Produktionsanlagen, ganze Geschäftsprozesse zur Erbringung von Dienstleistungen oder in der Verwaltung müssen abgesichert werden. Jedes Unternehmen und jeder der Sektoren Kritischer Infrastrukturen hat eigene kritische Geschäftsprozesse, spezifische Industriestrukturen, eine Vielzahl von Normen, Standards und nationale, europäische und internationale gesetzliche Vorgaben, die eingehalten und in Auditierungen nachgewiesen werden müssen, und jede Organisation eine eigene Kultur gelebter Sicherheit. Diese Komplexität des Themas IT-Sicherheit in einer Kritischen Infrastruktur müssen Unternehmen und Behörden angesichts einer Bedrohungslage mit einer steigenden Anzahl, Vielfalt und Professionalität von Cyberangriffen in praktikable und innovative Lösungen umsetzen: IT-Sicherheitsmaßnahmen müssen eingeführt, Technologien ausgewählt und im Unternehmen implementiert werden und das Thema IT-Sicherheit muss in Strategien und der täglichen Agenda die notwendige Priorität erhalten.

Hier setzt dieses Buch mit einer Fallstudienserie von neun Fallstudien an. Fallstudien sind wie gute Geschichten – in diesem Buch sind es gute Geschichten über erfolgreiche IT-Sicherheit. Diese berichten über erfolgreiche IT-Sicherheitsprojekte, innovative Lösungen und gelebte Unternehmenskulturen. Sicherheitskonzepte und Technologien bleiben nicht abstrakt. Die Fallstudien zeigen auf, wie die IT-Sicherheit verbessert werden kann, aber auch welche Tricks und Kniffe, welche Ressourcen dafür notwendig sind. Die Fallstudien gehen über die IT-Sicherheit hinaus und illustrieren, was erfolgreiche Praxis der IT-Sicherheit für Strategie und Geschäftsmodell bedeutet.

Mit einer Einführung in das Thema IT-Sicherheit in Kritischen Infrastrukturen mit ausgewählten Cyberbedrohungen, typischen Schwachstellen Kritischer Infrastrukturen sowie Gesetzen, Standards und Normen und der Methode der CASE|KRITIS-Fallstudien beginnt dieses Buch im Teil I.

Eine Fallstudienserie mit neun Fallstudien in Teil II berichtet über erfolgreiche Projekte der IT-Sicherheit, innovative IT-Sicherheitslösungen und gelebte Unternehmenskulturen. Die Fallstudien thematisieren jeweils das, was für eine erfolgreiche IT-Sicherheitsmaßnahme notwendig ist: Führungs- und Managementkompetenz, neue effiziente Prozesse, innovative IT-Sicherheitstechnologie und neue Ansatzpunkte für Risikomanagement und IT-Sicherheitsmanagementsysteme.

Eine vergleichende Analyse der Fallstudien mit einer Gegenüberstellung zur Literatur in Teil III zeigt das auf, was viele Organisationen bewegt: das Messen von IT-Sicherheit, Kosten und Nutzen von IT-Sicherheitslösungen, Auslöser und Treiber von IT-Sicherheitsvorhaben sowie die Wechselwirkungen von IT-Sicherheitsvorhaben mit anderen Prozessen oder Or-

ganisationseinheiten. Kommentare aus und Instrumente für die Praxis sowie ein Impuls zur Innovation in der IT-Sicherheit schließen die Analyse der Fallstudien ab.

Wir bedanken uns beim Bundesministerium für Bildung und Forschung (BMBF) für die Förderung dieser Forschung. Das vorliegende Buch mit den Fallstudien ist als Aktivität im Förderschwerpunkt *IT-Sicherheit für Kritische Infrastrukturen ITS|KRITIS* entstanden. Das Projekt Vernetzte IT-Sicherheit Kritischer Infrastrukturen (VeSiKi) mit den Förderkennzeichen 16KIS0213K bis 16KIS0216 hat diese Fallstudienserie initiiert und durchgeführt. Neben dem Forschungsprojekt VeSiKi sind Vertreter der Forschungskonsortien von PREVENT, MoSaIK sowie von INDI und RiskViz mit Fallstudien an der vorliegenden Fallstudienserie beteiligt. Gemeinsam mit den Forschungsprojekten INDI und SICIA wurde eine zusätzliche Fallstudie durchgeführt.

Wir bedanken uns auch bei allen Organisationen, die mit uns eine Fallstudie erstellt und uns Einblicke in die gelebte Praxis der IT-Sicherheit Kritischer Infrastrukturen gewährt haben, allen Interviewpartnern, die zu einer Fallstudie beigetragen haben, und den Autoren, die Fallstudien verfasst haben. Wir bedanken uns bei Mitgliedern des Beirats, die in Interviews mit Einsichten aus der Praxis und zur Strategie die Ergebnisse der Fallstudien bereichert haben. Nicht alle Interviewpartner und Organisationen können in diesem Buch namentlich genannt werden – einige Organisationen haben um Anonymität gebeten und auch ihnen gilt unser besonderer Dank. Wir bedanken uns bei Prof. Dr. Petra Schubert, mit der wir die von ihr entwickelte Fallstudienmethodik eXperience für das Thema IT-Sicherheit in Kritischen Infrastrukturen verfeinern konnten.

Wir – die Editoren und Autoren – wünschen den Lesern eine informative Lektüre und hoffen, dass wir zusammen mit Ihnen einen Beitrag zur Sicherheit leisten können.

Ulrike Lechner, Sebastian Dännart, Andreas Rieb und Steffi Rudel

Über dieses Buch

Wer sollte dieses Buch zu Fallstudien der IT-Sicherheit Kritischer Infrastrukturen lesen? Das vorliegende Buch gibt Betreibern Kritischer Infrastrukturen und IT-Professionals Hinweise zur erfolgreichen Umsetzung von IT-Sicherheitsprojekten und zu Lösungen, die sich in der Praxis bewährt haben. Studierenden und Dozierenden in Studiengängen wie Wirtschaftsinformatik, Informatik und IT-Sicherheit geben die Fallstudien einen Einblick in die Praxis der IT-Sicherheit in Organisationen und einen Überblick über das neue Themenfeld der IT-Sicherheit. Studierende aus anderen Disziplinen werden für Fragen der IT-Sicherheit und der Digitalisierung in ihren eigenen Disziplinen sensibilisiert.

Was muss ich zu CASE|KRITIS wissen? Die Fallstudien wurden im Zeitraum von 2015 bis 2017 erstellt, die vergleichende Fallstudienanalyse wurde von 2017 bis Anfang 2018 durchgeführt. In diesem Zeitraum traten das Gesetz zur Erhöhung der Sicherheit informationstechnischer Anlagen und die KRITIS-Verordnung in Kraft und die gesetzlichen Anforderungen an die Betreiber Kritischer Infrastrukturen wurden klar. Die Themen der Fallstudien nehmen die Anforderungen des IT-Sicherheitsgesetzes bereits auf.

In die Zeit der Erstellung der Fallstudien in diesem Buch fallen auch öffentlichkeitswirksame IT-Sicherheitsvorfälle: Ransomware wurde für Unternehmen und Behörden ein wichtiges Thema, die Telekommunikationsinfrastruktur in Unternehmen und Privathaushalten war von dem Botnet Mirai betroffen und die Fake-News-Debatte hat die Verwundbarkeit von Medien und demokratischen Wahlen eindrücklich vor Augen geführt. Die geopolitischen Entwicklungen lassen nicht erwarten, dass sich das Thema der Cybersicherheit in der Zukunft entschärfen wird.

Zu diesem Buch gibt es unter *www.itskritis.de* – der Webseite des Förderschwerpunkts IT-Sicherheit für Kritische Infrastrukturen – Materialien zu den Fallstudien in diesem Buch sowie eine Fortsetzung der Fallstudienserie.

Editoren und Autoren

Die Fallstudienserie CASE|KRITIS wurde von den Mitgliedern des Forschungsprojekts Vernetzte IT-Sicherheit Kritischer Infrastrukturen (VeSiKi) initiiert, konzipiert und zusammen mit Co-Autoren durchgeführt. Die Beiträge, in die die Fallstudienserie eingebettet ist, wurden von Mitgliedern des VeSiKi-Teams verfasst, das Gesamtwerk wurde von ihnen editiert und online bereitgestellt.

Torsten Bollen arbeitet bei Diebold Nixdorf seit mehr als 15 Jahren im Bereich IT. Zu seinen Schwerpunktthemen gehören die Datenübertragung und die IT-Sicherheit. Aktuell arbeitet er im Forschungsbereich von Diebold Nixdorf als Projektmanager im Bereich Datenanalyse, Cloud-Services und IT-Zertifizierung.

Prof. Dr. Benedikt Buchner ist geschäftsführender Direktor des Instituts für Informations-, Gesundheits- und Medizinrecht (IGMR) und Professor für Bürgerliches Recht an der Universität Bremen; sein Forschungsschwerpunkt liegt auf dem Informationsrecht und seinen Schnittstellen zu anderen Rechtsgebieten. Benedikt Buchner ist Vorstandsmitglied der Deutschen Stiftung für Recht und Informatik (DSRI) sowie Vorsitzender der Ethikkommission der Universität Bremen.

Sebastian Dännart ist IT-Sicherheitsberater und freiberuflicher Wissenschaftler, außerdem ist er Lehrbeauftragter für IT-Governance und IT-Management an der Universität der Bundeswehr München. Seine Themenschwerpunkte sind IT-Governance, IT-Sicherheitsmanagement sowie die IT-Sicherheit Kritischer Infrastrukturen.

Thomas Diefenbach ist Militärischer Wissenschaftlicher Mitarbeiter an der Universität der Bundeswehr München. Sein Forschungsschwerpunkt liegt in der Anwendbarkeit von Methoden des Enterprise Architecting in Kontexten des Risk Managements sowie der IT-Sicherheit.

Dr. Dr. Albrecht Fritzsche habilitiert am Lehrstuhl für Wirtschaftsinformatik, insb. Innovation und Wertschöpfung, an der Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU). Er hat in den Fächern Industriebetriebslehre und Technikphilosophie promoviert und war in der produzierenden Industrie als Systemexperte und Technologieberater tätig. Seine Forschungsarbeiten decken ein weites Spektrum von Themen im Zusammenhang mit Digitalisierung und Innovation ab und richten sich an Experten verschiedenster Disziplinen.

Tamara Gurschler war Wissenschaftliche Mitarbeiterin an der Universität der Bundeswehr in München. Heute ist sie Information Security Consultant bei CGI. Ihre Forschungsschwerpunkte sind IT-Security-Awareness und Risikomanagement.

Manfred Hofmeier ist Wissenschaftlicher Mitarbeiter an der Universität der Bundeswehr München und Mitgründer eines IT-Startups. Seine Forschungsschwerpunkte sind IT-Sicherheit Kritischer Infrastrukturen, Bedrohungslagen und soziokulturelle Aspekte der IT-Sicherheit.

Max Jalowski ist Wissenschaftlicher Mitarbeiter am Lehrstuhl für Wirtschaftsinformatik, insb. Innovation und Wertschöpfung, an der Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU). In seiner Forschung beschäftigt er sich mit dem Einsatz von persuasiven Technologien in Innovationsprozessen.

Toni Kehr hat an der Universität der Bundeswehr München studiert und langjährig im Projekt VeSiKi mitgearbeitet. Zu seinen Forschungsschwerpunkten zählen die IT-Sicherheit Kritischer Infrastrukturen und das IT-Sicherheitsmanagement.

Dr. Dennis-Kenji Kipker Wissenschaftlicher Geschäftsführer des IGMR an der Universität Bremen. Vorstand der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) in Berlin. Projektmanager beim VDE e. V. in Frankfurt am Main, CERT@VDE. Mitglied in der AG Recht des Bundesverbandes für IT-Sicherheit TeleTrusT. Forschungsaufenthalte unter anderem in Tokyo, Moskau, Nizza und Los Angeles.

Prof. Dr. Ulrike Lechner ist Inhaberin des Lehrstuhls für Wirtschaftsinformatik an der Universität der Bundeswehr München. Sie leitet das Forschungsprojekt Vernetzte IT-Sicherheit Kritischer Infrastrukturen (VeSiKi). Ihre Themen in Forschung und Lehre sind Unternehmensarchitekturen, Krisenmanagement und IT-Sicherheit für Kritische Infrastrukturen.

Prof. Dr. Kathrin Möslein ist Vizepräsidentin der Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Inhaberin des FAU-Lehrstuhls für Wirtschaftsinformatik, insb. Innovation und Wertschöpfung, und Forschungsprofessorin an der HHL Leipzig Graduate School of Management. Ihre Forschungs- und Tätigkeitsschwerpunkte liegen im Bereich der strategischen Innovation, Kooperation und Führung im Kontext der digitalen Transformation.

Sven Müller ist derzeit Projektmanager für IT-Security in Kritischen Infrastrukturen beim VDE Verband e. V. in Frankfurt am Main. Er verfügt über eine umfangreiche Wissensbasis in den Bereichen Elektrotechnik und Automatisierung, welche er durch Studien der Betriebswirtschaftslehre und Pädagogik ergänzt hat.

Gerrit Opper ist als Cyber-Security-Analyst im Kommando Cyber- und Informationsraum (KdoCIR) beim Chief Information Security Officer der Bundeswehr (CISOBw) im Bereich des operativen Schutzes und des strategischen Cyberlagebildes tätig. Im Bereich der Cyberawareness leitet er stellvertretend die Arbeitsgruppe InfoSecurity Awareness in der Bundeswehr.

Matthias Raß ist Wissenschaftlicher Mitarbeiter am Lehrstuhl für Wirtschaftsinformatik, insb. Innovation und Wertschöpfung, an der Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU). In seiner Forschung beschäftigt er sich vor allem mit Open Innovation, intra- und interorganisationalen Netzwerken und sozialem Kapital.

Tim Reimers ist Wissenschaftlicher Mitarbeiter am Institut für Angewandte Informatik an der Universität der Bundeswehr München. Seine Forschungsschwerpunkte liegen in der Anwendbarkeit der Distributed-Ledger-Technologie in Wertschöpfungsnetzwerken.

Dr. Andreas Rieb war bis 03/2018 Wissenschaftlicher Mitarbeiter an der Universität der Bundeswehr München sowie freiberuflicher IT-Security Berater. Seit 04/2018 ist er IT-Security Specialist bei Airbus CyberSecurity. Seine Aufgabengebiete und Forschungsschwerpunkte sind IT-Sicherheit Kritischer Infrastrukturen, IT-Security-Awareness und Serious Gaming.

Dr. Steffi Rudel ist Wissenschaftliche Mitarbeiterin an der Universität der Bundeswehr München und im Projekt VeSiKi als Projektleiterin tätig. Ihre Forschungsschwerpunkte sind IT-Sicherheit Kritischer Infrastrukturen, Industrielle Digitalisierung / Industrie 4.0 sowie Geschäftsmodelle.

Inhaltsverzeichnis

Teil I

Eine kurze Einführung in das Thema IT-Sicherheit für Kritische Infrastrukturen

Das Bewusstsein für den Wert der sogenannten Kritischen Infrastrukturen und die Rolle von Informations- und Kommunikationstechnologien für die moderne Zivilgesellschaft ist heute geschärft. Produkte und Dienstleistungen müssen verfügbar und sicher sein, die Dienstleistungsqualität muss gewährleistet und Schaden für die Zivilgesellschaft durch nicht korrekt funktionierende Produktionsanlagen, Verletzung der Privatsphäre und unkorrekte Informationen abgewendet werden. Das Thema IT-Sicherheit für Kritische Infrastrukturen ist ein vergleichsweise neues Themenfeld: Erst mit Stuxnet, einer Schadsoftware auf industriellen Produktions- und Steuerungsanlagen, gelangte das Thema der IT-Sicherheit industrieller Anlagen in den Fokus einer breiten Öffentlichkeit. Die Gesetzgebung hat mit dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme und den KRITIS-Verordnungen reagiert und die Kriterien, welche Betreiber Kritischer Infrastrukturen für die Sicherheit der Zivilgesellschaft relevant sind, konnten festgelegt und die Betreiber somit aufgefordert werden, die IT-Sicherheit und damit die Sicherheit ihrer Unternehmen zu gewährleisten. Vor diesem Hintergrund – ein neues Thema mit neuen Anforderungen an Unternehmen – wurde eine Fallstudienserie initiiert mit dem Ziel, erfolgreiche IT-Sicherheitsprojekte, innovative IT-Sicherheitstechnologien und Lösungen genau wie gelebte Organisationskulturen der IT-Sicherheit zu analysieren und zu dokumentieren.

Die neun Fallstudien bilden zusammen mit einer fallstudienübergreifenden Analyse den inhaltlichen Schwerpunkt dieses Buches. In diesem einleitenden Teil I gibt ein Streifzug durch die prägenden Themen der IT-Sicherheit einen Einblick in Kritische Infrastrukturen und ihre Technologie zusammen mit den relevanten Gesetzen, Normen und Standards, in die Bedrohungen der IT-Sicherheit Kritischer Infrastrukturen und in die eingesetzte Methodik der Fallstudien. Motiviert ist die Auswahl dieser Themen durch die Erfahrung im Forschungsprojekt VeSiKi, sie hat das Ziel, Leser ohne vertieftes Wissen über Kritische Infrastrukturen oder IT-Sicherheit zu informieren und vor allem die Spezifika des Themenfelds IT-Sicherheit Kritischer Infrastrukturen im Gegensatz zur klassischen IT zu vermitteln.

1 IT-Sicherheit für Kritische Infrastrukturen

Mit einer Einführung des Begriffs „Kritische Infrastruktur", einem Überblick über die gesetzlichen Grundlagen zur IT-Sicherheit für Kritische Infrastrukturen und über die relevanten Normen und Standards beginnt die Einführung in das Thema IT-Sicherheit für Kritische Infrastrukturen. Das vorliegende Buch will für die Praxis relevant sein und so beziehen sich die wichtigen Definitionen bewusst auf die Referenzdokumente des Bundesamtes für Sicherheit in der Informationstechnik (BSI) mit dem Ziel, die Brücke von den Ergebnissen der Fallstudien in die Praxis zu schlagen.

1.1 Kritische Infrastrukturen und ihre Technologie

Ulrike Lechner, Universität der Bundeswehr München
Andreas Rieb, Universität der Bundeswehr München

„Kritische Infrastrukturen 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" (BMI 2009b). Dieser Definition folgen die Bundesbehörden und entsprechend dieser Definition klassifiziert das Bundesministerium des Innern die Kritischen Infrastrukturen (BMI) nach Sektoren und Branchen (siehe Tabelle 1).

Tabelle 1: Sektoren- und Brancheneinteilung Kritischer Infrastrukturen gemäß BMI, 2009a

Sektoren	Branchen
Energie	• Elektrizität • Gas • Mineralöl
Informationstechnik und Telekommunikation	• Telekommunikation • Informationstechnik
Transport und Verkehr	• Luftfahrt • Seeschifffahrt • Binnenschifffahrt • Schienenverkehr • Straßenverkehr • Logistik
Gesundheit	• Medizinische Versorgung • Arzneimittel und Impfstoffe • Labore
Wasser	• Öffentliche Wasserversorgung • Öffentliche Abwasserbeseitigung
Ernährung	• Ernährungswirtschaft • Lebensmittelhandel

Finanz- und Versicherungswesen	• Banken • Börsen • Versicherungen • Finanzdienstleister
Staat und Verwaltung	• Regierung und Verwaltung • Parlament • Justizeinrichtungen • Notfall- / Rettungswesen einschließlich Katastrophenschutz
Medien und Kultur	• Rundfunk (Fernsehen und Radio), gedruckte und elektronische Presse • Kulturgut • Symbolträchtige Bauwerke

Kritische Infrastrukturen im Sinne des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) und der KRITIS-Verordnung (vgl. Kap. 1.3) sind Infrastrukturen, die mit ihrer Versorgungsleistung die sektorenspezifisch definierten Schwellwerte in Bezug auf die versorgte Bevölkerung überschreiten (vgl. Kap. 1.3). Die Sektoren „Medien und Kultur" sowie „Staat und Verwaltung" unterliegen nicht der Gesetzgebungskompetenz des Bundes und sind entsprechend von der gesetzlichen Regelung durch das IT-Sicherheitsgesetz nicht betroffen.

Die Sektoren Kritischer Infrastrukturen sind traditionell unterschiedlich und einer der grundlegenden Unterschiede betrifft die Industriestrukturen mit ihren Traditionen der Sicherheit: Im Sektor Energie finden sich z. B. mit Kraftwerken große Anbieter mit einer langen Tradition in Sicherheitsthemen, während im Sektor Wasser – der Wasserversorgung und Abwasserbeseitigung beinhaltet – viele kleine und mittlere Betreiber Kritischer Infrastrukturen auf kommunaler Ebene tätig sind. Spezifisch für den Sektor Wasser sind z. B. Regelungen wie die 10%-Regel, das Multibarrierenprinzip mit mehreren Barrieren zum Schutz des Trinkwassers und das Minimierungsprinzip. Bei der Trinkwasseraufbereitung und Verteilung dürfen durch die Aufbereitungschemikalien und die verwendeten Materialien nur so wenig Verunreinigungen wie technisch möglich und wirtschaftlich vertretbar in das Trinkwasser übergehen (Umweltbundesamt 2016). Solche Prinzipien müssen zunehmend nicht nur in der Mechanik der Trinkwasserversorgung, sondern auch in der smarten, vernetzten Steuerung der Anlagen zur Trinkwasserversorgung umgesetzt werden. Einen weiteren Unterschied zwischen den Sektoren stellt die Penetration mit Informations- und Kommunikationstechnologie dar: Während z. B. im Gesundheitswesen viele Arbeitsplätze natürlicherweise mit IT-Infrastruktur ausgestattet sind, muss die IT für die Arbeitnehmer im Straßenbau, in der Produktion von Lebensmitteln oder auf Baustellen robust sein und IT-Kompetenzen stellen keine Selbstverständlichkeit dar.

Ein typischer Netzplan Kritischer Infrastrukturen ist in Abbildung 1-1 dargestellt. Typische Elemente eines Netzwerks Kritischer Infrastrukturen sind Firewalls an der Schnittstelle zwischen Internet und Kritischer Infrastruktur. In der Demilitarisierten Zone finden sich Webserver mit den Datenbanken. Zwischen der Demilitarisierten Zone (DMZ) und dem Netzwerk

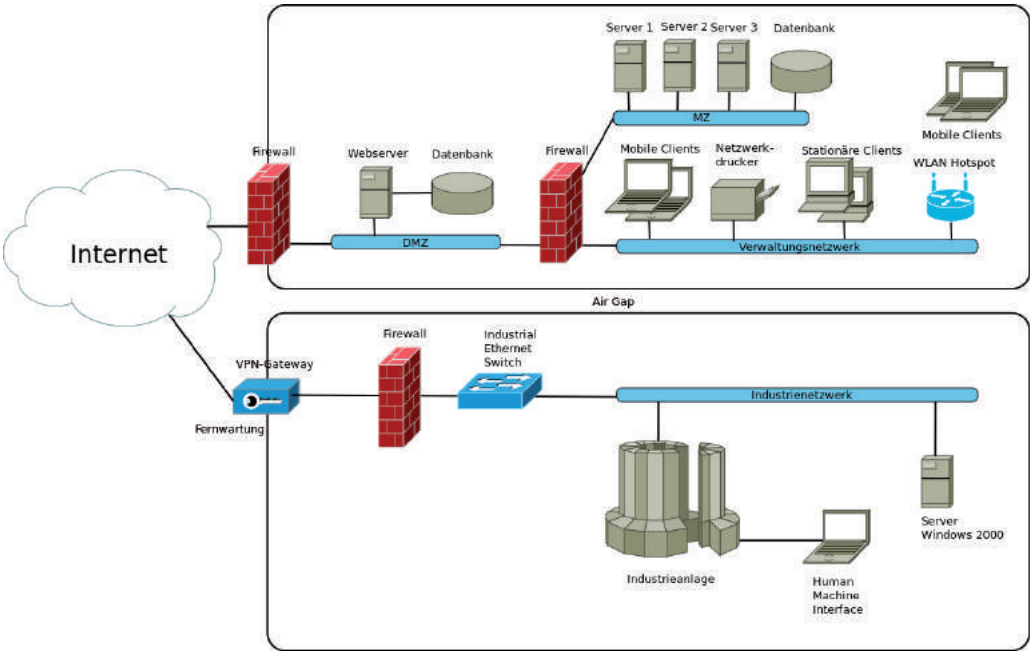


Abbildung 1-1: Netzplan (fiktiver) Kritischer Infrastrukturen mit typischen Elementen

der Infrastruktur finden sich wieder IT-Sicherheitsmaßnahmen wie Firewalls. Das Netz mit der Office-IT enthält Server, Datenbanken, stationäre und mobile Clients, Netzwerkdrucker und WLAN-Netze mit WLAN-Hotspots.

Ein Industrienetzwerk enthält Produktionsanlagen bzw. Industrieanlagen mit Benutzerschnittstellen (Human Machine Interfaces), Server (die häufig noch auf älteren Windows-Versionen basieren), Switche für die Verbindung der Netze. Diese Netzwerke sind wieder durch eine Firewall geschützt und Fernwartungszugänge bspw. mit VPN-Technologie erlauben Zugang von außen auf die Industrieanlagen. Dieses Beispiel eines Netzplans symbolisiert eine Kritische Infrastruktur mit einer Industrieanlage, wie sie in Sektoren wie Energie, Transport und Logistik, Wasser oder auch Ernährung zu finden ist. Im Sektor Gesundheit würden sich in diesem „industriellen" Teil, z. B. eines Krankenhauses, medizintechnische Geräte, Labore mit ihrer Ausstattung sowie der gesamte Bereich der Hygiene, Wäsche und der Versorgung mit Nahrungsmitteln finden. Im Bereich Medien wäre in diesem Teil des Netzes alles von der journalistischen Aufbereitung über Layout bis hin zum Druck und der Distribution von Filmen zu finden.

In Bezug auf die IT sind industrielle Kontrollsysteme (Industrial Control Systems oder kurz ICS) ein typisches, wenn nicht gar das für die IT-Sicherheit zentrale Element der IT in Kritischen Infrastrukturen – und werden aber in der „klassischen" IT-Sicherheit kaum betrachtet. Wie auch z. B. in Knapp (Knapp 2011) und dem National Institute of Standards and Technology (NIST) (Stouffer u. a. 2014) beschrieben, nutzen Kritische Infrastrukturen und vor allem Industrie, wie z. B. die Automobilindustrie, Industrial Control Systems. Der Begriff der Industrial Control Systems umfasst z. B. Supervisory Control and Data Acqui-

sition (SCADA) Systeme, Distributed Control Systems (DCS), Human Machine Interfaces (HMIs) oder andere Kontrollsysteme, wie Programmable Logic Controllers (PLC). Ein ICS besteht aus einer Kombination der oben aufgeführten Systeme und anderen elektronischen, mechanischen oder hydraulischen Komponenten in der Erfüllung industrieller Aufgaben, z. B. Herstellung, Energiegewinnung, Wasserversorgung oder Transport (Stouffer u. a. 2014).

Nicht nur die IT-Technik, wie z. B. die der ICS-Systeme, ist spezifisch für Kritische Infrastrukturen. Technik und Informationstechnik haben unterschiedliche Lebenszyklen: während Informations- und Kommunikationstechnik häufig nach 3 Jahren als veraltet abgeschrieben ist und nach wenigen Jahren durch die Hersteller nicht mehr unterstützt wird, haben z. B. Kraftwerksblöcke, Steuerung von Verkehrsanlagen, Schiffe oder andere Transportmittel deutlich längere Lebenszyklen. Wartungsfenster, in denen ein Update oder Patch eingespielt werden darf, sind bei Kritischen Infrastrukturen, wie z. B. Produktionsanlagen, selten – während in der Office-IT Updates de facto laufend eingespielt werden können und so der Stand der Sicherheit leichter angepasst werden kann.

Dieses erste Kapitel hat den Begriff der Kritischen Infrastruktur eingeführt, die Unterschiede zwischen Sektoren Kritischer Infrastrukturen thematisiert und die relevanten Technologien wie ICS-Systeme mit Netzplänen skizziert. Die Materialität der Technik Kritischer Infrastrukturen prägt die Anforderungen an die IT-Sicherheit. Das folgende Kapitel gibt eine kurze Einführung in die IT-Sicherheit für Kritische Infrastrukturen.

1.2 IT-Sicherheit in Kritischen Infrastrukturen

Ulrike Lechner, Universität der Bundeswehr München
Andreas Rieb, Universität der Bundeswehr München

In Fragen der IT-Sicherheit entwickelt das Bundesamt für Sicherheit in der Informationstechnik (BSI) De-facto-Standards für die Unternehmen und diese maßgeblichen Definitionen des BSI sollen im vorliegenden Buch die Analysen leiten. „IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind“ (BSI 2018b). Der Begriff der Informationssicherheit geht ein Stück weiter als IT-Sicherheit: „Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung“ (BSI 2018b). Das BSI argumentiert in seinem Glossar, dass beide Begriffe synonym verwendet werden – auch wenn der Begriff der Informationssicherheit weiter gefasst ist. „Cyber-Sicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der klassischen IT-Sicherheit wird dabei auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und

schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein“ (BSI 2018a).

Das „Herz der Informationssicherheit“ bilden die sogenannten CIA-Kriterien von

- Confidentiality (Vertraulichkeit)
- Integrity (Integrität)
- Availability (Verfügbarkeit).

Diese drei Kriterien der Informationssicherheit können nach ISO Definitionen ergänzt werden um weitere Schutzziele bzw. Eigenschaften wie Authentizität (Authenticity), Verbindlichkeit (Accountability), Nachweisbarkeit oder Nicht-Abstreitbarkeit (Non-Repudiation) und Zuverlässigkeit (Reliability) (DIN, 2009).

In den Definitionen von Kritischen Infrastrukturen wird die Verfügbarkeit von Produkten und Dienstleistungen für die moderne Zivilgesellschaft als wesentliches Ziel thematisiert und diese Schwerpunktsetzung wird als ein Unterschied zur „klassischen“ IT-Sicherheit genannt. Integrität und Vertraulichkeit von Informationen und Systemen sind jedoch wesentliche Voraussetzung für die Verfügbarkeit.

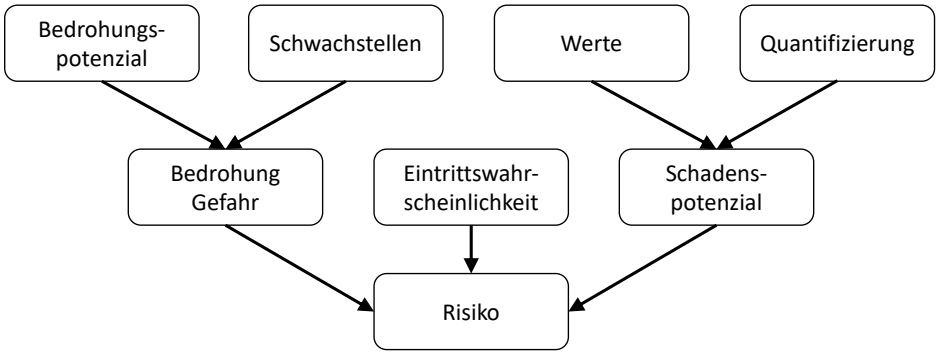


Abbildung 1-2: Zusammenhang zwischen Schwachstellen, Bedrohungen und Risiko; Quelle Eckert, 2013

Eine Bedrohung (engl. threat) des Systems zielt darauf ab, eine oder mehrere Schwachstellen oder Verwundbarkeiten auszunutzen, um einen Verlust der Datenintegrität, der Informationsvertraulichkeit oder der Verfügbarkeit zu erreichen oder um die Authentizität von Subjekten zu gefährden (Eckert 2013). Unter einem Angriff (engl. attack) versteht man einen nicht autorisierten Zugriff bzw. einen nicht autorisierten Zugriffsversuch auf das System. Passive Angriffe betreffen die unautorisierte Informationsgewinnung und zielen auf den Verlust der Vertraulichkeit ab. Aktive Angriffe betreffen die unautorisierte Modifikation von Datenobjekten und richten sich somit gegen die Datenintegrität oder Verfügbarkeit eines IT-Systems (Eckert, 2013). Den Zusammenhang zwischen Schwachstellen, Bedrohungen und Risiko illustriert Abbildung 1-2.

Das Risikomanagement hat eine besondere Rolle: Es schlägt die Brücke zwischen limitierten Ressourcen und Investitionsentscheidungen einerseits und den Bedrohungspotenzialen

andererseits. Prof. Dr. Claudia Eckert formuliert hierzu: „Lösungen der IT-Sicherheit haben zum einen Wegbereiter-Funktion, da neue Anwendungen häufig nur eingesetzt und akzeptiert werden, wenn die Sicherheit der Daten gewährleistet wird. Zum anderen hat die IT-Sicherheit natürlich die bekannte Schutzfunktion. Gezielt und korrekt eingesetzte Maßnahmen der IT-Sicherheit reduzieren die Risiken wirtschaftlicher Schäden, die zum Beispiel durch eine unautorisierte Weitergabe von Daten oder durch kriminelle Aktivitäten wie Wirtschaftsspionage entstehen können. Maßnahmen der IT-Sicherheit sind aber auch notwendig, um vor Schäden an Leib und Leben zu schützen, die zum Beispiel durch manipulierte Gesundheitsdaten oder durch manipulierte Fahrzeugsensorik entstehen können" (Eckert 2013). Während die Bedrohungspotenziale speziell in Kritischen Infrastrukturen hoch sein können, werden die Eintrittswahrscheinlichkeiten eines erheblichen Schadens häufig als sehr gering eingeschätzt. Die Motivation für viele IT-Sicherheitsmaßnahmen kommt damit nicht so sehr aus der betriebswirtschaftlichen Sicht, sondern aus der Verantwortung der Betreiber Kritischer Infrastrukturen und den gesetzlichen Regelungen, wie dem IT-Sicherheitsgesetz. Auch hier ist das Themenfeld der IT-Sicherheit Kritischer Infrastrukturen von neuen Entwicklungen speziell in der Gesetzgebung geprägt.

1.3 Gesetzliche Anforderungen an die IT-Sicherheit in Deutschland und Europa

Dennis-Kenji Kipker, Universität Bremen
Benedikt Buchner, Universität Bremen

Während sich früher die Verpflichtung zur Realisierung angemessener IT-Sicherheitsmaßnahmen vorwiegend aus allgemeinen gesetzlichen Rahmenvorschriften ergab und zur Einhaltung nicht näher bestimmter Sorgfaltspflichten, die keinen unmittelbaren IT-Sicherheitsbezug aufwiesen, gehörte, hat insbesondere seit dem Jahr 2015 eine umfassende rechtliche Regulierung speziell der IT-Sicherheit stattgefunden, die in politischer Hinsicht auf den deutschen und europäischen Cybersicherheitsstrategien basiert. Seither ist es erstmals möglich, insbesondere auch für den Schutz von Einrichtungen, denen für das Funktionieren des Gemeinwesens eine besonders hohe Bedeutung zukommt – den sogenannten Kritischen Infrastrukturen – einen einheitlichen Rechtsrahmen vorzuhalten.

Auf nationaler und europäischer Ebene sind in diesem Zusammenhang im Wesentlichen bisher vier Rechtsakte zu benennen, die unter Gesichtspunkten der Cybersicherheit eine besondere Aufmerksamkeit verdienen: das deutsche IT-Sicherheitsgesetz (IT-SiG) aus 2015; die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) aus 2016 und 2017; die EU-Richtlinie 2016/1148 „über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union" (EU NIS-RL) aus 2016, die im Jahr 2017 durch ein Umsetzungsgesetz in das deutsche Recht implementiert wurde, sowie der Entwurf einer Verordnung über die „EU-Cybersicherheitsagentur" (ENISA) sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit").

Das deutsche IT-SiG war der erste Rechtsakt, der einen Fokus auf die IT-Sicherheit speziell der Kritischen Infrastrukturen legte. Basierend auf der Cybersicherheitsstrategie der Bundesregierung aus dem Jahr 2011 trat das Gesetz am 25. Juli 2015 in Kraft und zielt auf eine „signifikante Verbesserung der Sicherheit informationstechnischer Systeme in Deutschland" ab. Zu solchen IT-Systemen gehören aber nicht nur große Unternehmensnetzwerke, sondern auch der vernetzte Anwender-PC, sodass unter anderem auch der Verbraucher in die Betrachtung ganzheitlicher Cybersecurity einbezogen wird. Zur allgemeinen Verbesserung der Cybersecurity wird das Bundesamt für Sicherheit in der Informationstechnik (BSI) als zentrale deutsche Informationssicherheitsbehörde gestärkt und erfährt einen laufenden Ausbau. In praktischer Hinsicht ist anzumerken, dass die Verpflichtungen aus dem IT-SiG keine unmittelbare Wirkkraft gegenüber Unternehmen und Bürger entfalten: Da es sich bei dem IT-SiG um ein Artikelgesetz handelt, werden durch dieses lediglich verschiedene und bereits bestehende einzelgesetzliche Vorschriften modifiziert und ergänzt, zum Beispiel das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), das Telekommunikationsgesetz (TKG) und das Telemediengesetz (TMG). Dies hat zur Folge, dass trotz der Regelungen des IT-SiG weiterhin auf die bestehenden Einzelgesetze zur IT-Sicherheit Bezug genommen wird. Die umfangreichsten Anpassungen durch das IT-SiG hat das BSIG erfahren. So werden neuerdings in § 2 Abs. 10 BSIG Kritische Infrastrukturen definiert als Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation (IuK), Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder durch ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Die Betreiber der in diesem Sinne bestimmten Infrastrukturen trifft eine Reihe von Pflichten zur Verbesserung der IT-Sicherheit. Zentral sind hier die Änderungen, die durch die §§ 8a und 8b BSIG vorgegeben werden: Zuvorderst besteht die Anforderung, angemessene organisatorische und technische Vorkehrungen (TOV) zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der betriebenen Kritischen Infrastruktur maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Dieser unbestimmte Rechtsbegriff ist vor allem durch die technische Normung und Standardisierung auszufüllen (Kipker, 2016c)[1]. § 8b BSIG regelt über die in § 8a BSIG normierten TOV hinausgehend den Umgang mit IT-Sicherheitsinformationen. Dazu hat das BSI einen Ausbau als zentrale Meldestelle für Betreiber unter anderem von Kritischen Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik erfahren. So hat die Behörde auch die Aufgabe, die für die Abwehr von Gefahren für die IT-Sicherheit relevanten Informationen zu sammeln und auszuwerten und die Betreiber sowie die (Aufsichts-)Behörden über kritische Vorgänge zu informieren. Damit korrespondierend trifft die Betreiber die Verpflichtung, eine Kontaktstelle einzurichten, um für die Unterrichtungen des BSI jederzeit erreichbar zu sein.

1 Ein Tool zur Bestimmung des „Standes der Technik" für einzelne Sektoren und Branchen im Umfeld von Industrie 4.0 und KRITIS stellt der „IT-Security NAVIGATOR" dar (ITSKRITIS 2017).

Diese Kontaktstelle dient aber nicht nur der Informationsentgegennahme, sondern ebenso der Durchführung von eigenständigen Meldungen an das BSI, zu denen die neuen gesetzlichen Vorgaben verpflichten. Demgemäß haben die Betreiber unverzüglich Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastruktur geführt haben, oder erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastruktur führen können, zu melden. Die Meldung kann grundsätzlich pseudonym[2], also ohne direkte Namensnennung des Betreibers, erfolgen, es sei denn, dass die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat. Die Meldung an das BSI muss unter anderem Angaben zur Störung, zu den Auswirkungen und zu den technischen Rahmenbedingungen sowie zur vermuteten oder tatsächlichen Ursache enthalten, soweit diese Informationen dem Betreiber in der konkreten Situation zur Verfügung stehen.

Das IT-SiG umschreibt zwar die wesentlichen rechtlichen Anforderungen, die für die Betreiber der Kritischen Infrastrukturen gelten, legt jedoch nicht fest, welche Betreiber und Anlagen im Einzelnen unter die gesetzlichen Vorgaben fallen. Hier beschränkt sich das Gesetz in § 2 Abs. 10 BSIG auf die bloße Benennung von einzelnen Sektoren. Nach Inkrafttreten des IT-SiG gab es deshalb einen erheblichen Raum für Spekulationen, welche Unternehmen tatsächlich von den neuen Vorgaben betroffen sein würden. Klärung hat hier die BSI-KritisV gebracht, die vom Bundesministerium des Innern (BMI) nach Maßgabe des § 10 Abs. 1 S. 1 BSIG erlassen wurde. Basierend auf den sogenannten Sektorstudien des BSI, welche die Bereiche Energie, Ernährung und Wasser, Gesundheit, Finanz- und Versicherungswesen, Informationstechnik und Telekommunikation, Transport und Verkehr, Logistik sowie Medien und Kultur abdecken, wurde anhand der Berechnung von sogenannten Schwellenwerten ermittelt, welche Anlagenkategorien im Einzelnen als Kritische Infrastrukturen im Sinne des IT-SiG anzusehen sind (Kipker, 2016a). Zunächst wird dabei im Rahmen eines dreistufigen Verfahrens ermittelt, welche der im jeweiligen Sektor erbrachten Dienstleistungen aufgrund ihrer Bedeutung generell als kritisch anzusehen sind. In einem zweiten Schritt werden diejenigen Kategorien von Anlagen identifiziert, die für die Erbringung der zuvor ermittelten kritischen Dienstleistung erforderlich sind. Im dritten und zugleich letzten Schritt wird ermittelt, welche konkreten Anlagen oder Teile davon einen aus gesamtgesellschaftlicher Sicht bedeutenden Versorgungsgrad aufweisen; dies sowohl unter Qualitäts- wie auch unter Quantitätsgesichtspunkten. Bewusst hat der Gesetzgeber für die Bestimmung der konkreten Kritischen Infrastrukturen das Rechtsinstrument der Verordnung gewählt, da diese als untergesetzlicher, ministerieller Rechtsakt in der Lage ist, schneller auf eine Änderung der technischen Rahmenbedingungen zu reagieren, als dies durch ein formelles Parlamentsgesetz möglich ist. Die

2 In Abgrenzung zur anonymen Meldung, die gesetzlich jedoch nicht vorgesehen ist, ermöglicht die pseudonyme Meldung für die Behörde aber immer noch die Zuordnung des individuellen Betreibers.

BSI-KritisV zur Konkretisierung des Anwendungsbereiches der aus dem IT-SiG folgenden Regelungen erschien in zwei sogenannten Körben, wovon der zweite mit den Sektoren Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr erst am 30. Juni 2017 seine Rechtskraft entfaltet hat, wohingegen der Entwurf des ersten Korbes schon zu Beginn 2016 veröffentlicht wurde (Kipker, 2017b).

Die Europäische Union verfolgt bei der gesetzlichen Regulierung der IT-Sicherheit einen Ansatz, der über die Kritischen Infrastrukturen des deutschen Rechts hinausgeht und im Besonderen auch auf den Schutz des digitalen europäischen Binnenmarktes abzielt. Im Mittelpunkt steht dabei die EU NIS-RL, die als Wegbereiter zur Umsetzung der europäischen Cybersicherheitsstrategien von 2013 und 2017 gesehen werden kann. Neben neuen Anforderungen an die Betreiber von „wesentlichen Diensten", die maßgeblich den deutschen Kritischen Infrastrukturen entsprechen, zielt die NIS-RL vor allem auch auf digitale Dienste ab und geht damit zumindest in ihrem Anwendungsbereich zunächst über das nationale Recht hinaus (Kipker 2016b). Als europäische Richtlinie, die im Gegensatz zum EU-Rechtsetzungsakt der Verordnung gemäß Art. 288 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) keine unmittelbare Geltung in den Mitgliedstaaten besitzt, sondern nur hinsichtlich des zu erreichenden Ziels verbindlich ist, den Mitgliedstaaten aber die Wahl der Form und der Mittel zur Zielerreichung offenlässt, muss die NIS-RL durch ein Umsetzungsgesetz in den nationalen Rechtsrahmen überführt werden, um dort grundsätzlich Wirksamkeit zu entfalten. Für Deutschland ist dies durch das „Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union" geschehen. Das Umsetzungsgesetz zur EU NIS-RL hat am 27. April 2017 den Deutschen Bundestag passiert, wodurch einige der Rechtsvorschriften, die bereits durch das IT-SiG neu geschaffen oder novelliert worden waren, eine weitere Anpassung erfuhren (Kipker 2017c). Im Mittelpunkt stehen dabei die neuen Anforderungen für digitale Dienste: Nach § 2 Abs. 11 BSIG sind hierunter vor allem solche Dienste der Informationsgesellschaft zu verstehen, die es Verbrauchern oder Unternehmern ermöglichen, Kauf- oder Dienstleistungsverträge auf Online-Marktplätzen abzuschließen, und Dienste, die es Nutzern gestatten, bestimmte Suchanfragen im Internet durchzuführen – Online-Suchmaschinen –, sowie Cloud-Computing-Dienste, die den Zugang zu einem skalierbaren und elastischen Pool von gemeinsam genutzten Rechenressourcen gewährleisten. Kleinstunternehmen und kleine Unternehmen im Sinne der Empfehlung 2003/361/EG der EU-Kommission sind gemäß Art. 16 Abs. 11 EU NIS-RL hiervon aber ausgenommen. Für die betroffenen Anbieter von digitalen Diensten gelten nach den neuen, in das deutsche Recht umgesetzten europarechtlichen Vorgaben mit Kritischen Infrastrukturen vergleichbare Anforderungen. So sind gemäß § 8c BSIG angemessene technische und organisatorische Maßnahmen (TOM) zu treffen, um die Funktionsfähigkeit der digitalen Dienste in der EU sicherzustellen, ebenso besteht nach Realisierung erheblicher IT-Sicherheitsvorfälle eine Meldepflicht an das BSI.

Auf Basis der EU NIS-RL hat die Europäische Union im Herbst 2017 den Entwurf eines weiteren Rechtsakts im Bereich der Cybersicherheit veröffentlicht, die Verordnung über die „EU-Cybersicherheitsagentur" (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013

sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit"), die gemeinhin auch als „Cybersecurity-Verordnung" bezeichnet wird. Als Verordnung, die einen Kernbestandteil der neuen europäischen Cybersicherheitsstrategie (Kipker 2017d) darstellt, gilt das neue Gesetz unmittelbar in allen Mitgliedstaaten der Europäischen Union und bedarf deshalb keines nationalen Umsetzungsaktes mehr, wie dies noch für die EU NIS-RL der Fall gewesen ist. Die Anforderungen der Cybersecurity-Verordnung gehen inhaltlich weit über Kritische Infrastrukturen hinaus und zielen auf die Regulierung des gesamteuropäischen, digitalen Binnenmarktes ab. Im Mittelpunkt steht dabei die Schaffung eines europaweit einheitlichen Zertifizierungsrahmens für die IT-Sicherheit von Produkten und Diensten der Informations- und Kommunikationstechnik, sodass das Anbieten grenzüberschreitender digitaler Dienste in Zukunft eine deutliche Erleichterung erfahren wird. Hierbei wird die ENISA als Marktbeobachtungsstelle fungieren und unter anderem auch neue Normen zur Cybersicherheit aktiv mitgestalten (Kipker 2017e).

Im Ergebnis ist festzustellen, dass nicht nur die nationale, sondern auch die EU-weite rechtliche Regulierung von Cybersicherheit zunehmend an Fahrt gewinnt. Während zunächst vor allem die Kritischen Infrastrukturen zentraler Anknüpfungspunkt des gesetzgeberischen Handelns waren, werden die neuen Vorgaben zunehmend branchenübergreifend realisiert und stellen vor allem wirtschaftliche Schutzgüter in den Vordergrund – dies nicht nur im Bereich des produzierenden Gewerbes der Industrie 4.0, sondern auch speziell bezogen auf digitale Dienste, die mittlerweile einen erheblichen Anteil des europäischen Binnenmarktes ausmachen. Doch nicht nur in Deutschland und der EU haben die Gesetzgeber die hohe Bedeutung von funktionierenden IT-Systemen erkannt – so finden sich neue Regulierungsansätze auch in China (Kipker 2017a) und in Japan. Insbesondere in Japan, wo bisher keine speziellen IT-Sicherheitsgesetze existierten, steht die Sicherheit von Produkten des Internet of Things (IoT) im Vordergrund.[3] Darüber hinausgehend übernimmt der britische Gesetzgeber trotz des Austritts aus der EU wesentliche Vorgaben der neuen europäischen IT-Sicherheitsgesetzgebung (Kipker & Stelter, 2017). Mit der EU Datenschutz-Grundverordnung (EU DS-GVO), die vor allem in Art. 32 wesentliche Datensicherheitsanforderungen bestimmt und ab dem 25. Mai 2018 anzuwenden ist, rückt zudem die Verknüpfung von technischer IT-Sicherheit und Datenschutz immer weiter in den Vordergrund. Diese Entwicklung verdeutlicht, dass das Thema der IT-Sicherheit nicht nur zunehmend an Bedeutung gewinnt, sondern zugleich ein domänenübergreifendes und vorwiegend interdisziplinär geprägtes Arbeitsfeld darstellt, das eine rein branchenspezifische Betrachtung von Bedrohungslage und Gegenmaßnahmen obsolet macht.

Der Begriff des „Stands der Technik" beschreibt, welchen Anforderungen Unternehmen zur Erfüllung des IT-SiG genügen müssen. In einem dynamischen Umfeld wie dem der Cybersicherheit spielen bei dieser Festlegung des State of the Art Normen und Standards eine wichtige Rolle – nicht zuletzt auch deswegen, weil Technologieanbieter und Kunden gleichermaßen für ihre Lösungen Nachhaltigkeit und Investitionsschutz anstreben.

3 Ein Katalog zur IoT-Sicherheit wurde im Juli 2016 in Zusammenarbeit mit dem japanischen Ministry of Internal Affairs and Communications und dem Ministry of Economy, Trade and Industry erarbeitet (siehe IoTAC, 2016).

1.4 Normen, Standards und der Stand der Technik in der IT-Sicherheit Kritischer Infrastrukturen

Sven Müller, Deutsche Kommission Elektrotechnik Elektronik Informationstechnik

Voraussetzung für eine wirksame Absicherung von Netzen und IT-Systemen in Unternehmen, Behörden und anderen Organisationen ist gerade angesichts der hochdynamischen Entwicklung der Bedrohungslage im Cyber-Raum eine möglichst präzise Kenntnis der eigenen Betroffenheit. Einen pragmatischen Ansatz, diese Betroffenheit anhand nachvollziehbarer Maßstäbe zu bestimmen, bildet die Cyber-Sicherheits-Exposition vom Bundesamt für Sicherheit in der Informationstechnik (BSI 2012a). Um den zahlreichen aus Perspektive der Cyber-Sicherheit entstehenden Anforderungen gerecht zu werden, bieten nationale und internationale Normen, Standards, Leitfäden und Handlungsempfehlungen den Verantwortlichen für IT-Planung und -Betrieb mögliche Vorgehensweisen an (BSI 2012b).

Die Nutzung moderner IT zur Bewältigung von betriebswirtschaftlichen, logistischen und technischen Geschäftsprozessen sowie der Anschluss an das Internet sind heute ebenso unabdingbare Erfordernisse, um im weltweiten Wettbewerb bestehen zu können. Digitalisierung und Vernetzung bergen jedoch auch neue Gefahren, die Unternehmen in ihrem Risikomanagement berücksichtigen müssen. Eine gut organisierte Informationssicherheit vermindert die Anzahl der Schwachstellen, verringert die verbleibenden Risiken und begrenzt dadurch potenzielle Schäden für das Unternehmen. Für diese Abwehr neuer Gefahren hat die VdS Schadenverhütung GmbH die Richtlinie 3473, ein auf kleine und mittlere Unternehmen (KMU) zugeschnittenes Verfahren für die Etablierung und Aufrechterhaltung einer angemessenen Informationssicherheit, entwickelt (VdS 2015). Die Einhaltung der verschiedenen Anforderungen muss in jedem Prozess des Unternehmens sichergestellt werden. Änderungen an Verordnungen oder Gesetzen können gravierende Auswirkungen auf bestehende Geschäftsprozesse haben und neue Herausforderungen für das Risikomanagement bedeuten. Ein organisierter Datenschutz nach der VdS-Richtlinie 10010 vermindert die Anzahl an Schwachstellen, verringert das verbleibende Risiko, schützt dadurch die Rechte der Betroffenen und begrenzt potenzielle Schäden für das Unternehmen (VdS, 2017).

Aufgrund der Komplexität eines Informationssicherheitsmanagementsystems (ISMS) auf Basis der ISO/IEC 27001 wird diese Managementnorm noch in wenigen Klein- und Mittelständischen Unternehmen eingesetzt. Daher fehlt auch die darauf basierende Zertifizierung des ISMS nach ISO/IEC 27001.

Die DIN EN ISO/IEC 27001 geht auf ältere britische Standards (BS 7799:1995) zurück. Dieser nationale Standard wurde von der British Standard Institution herausgegeben und durch viele Guidelines ergänzt (Kersten, 2016). In englischer Sprache erschien die ISO/IEC 27001 im Jahre 2005 (deutsche Fassung 2008), sodann in 2013 in neuer überarbeiteter Fassung. Im März 2015 wurde die entsprechende Neufassung auch in deutscher Sprache herausgegeben.

Die Normenreihe ISO 2700 ist sehr umfangreich und wird ständig weiter ausgebaut. Neben der Hauptnorm 27001 und den unterstützenden Normen 27002 bis 27007, die bestimmte Aspekte der Hauptnorm vertiefen, existiert eine umfangreiche Sammlung von Normen zu

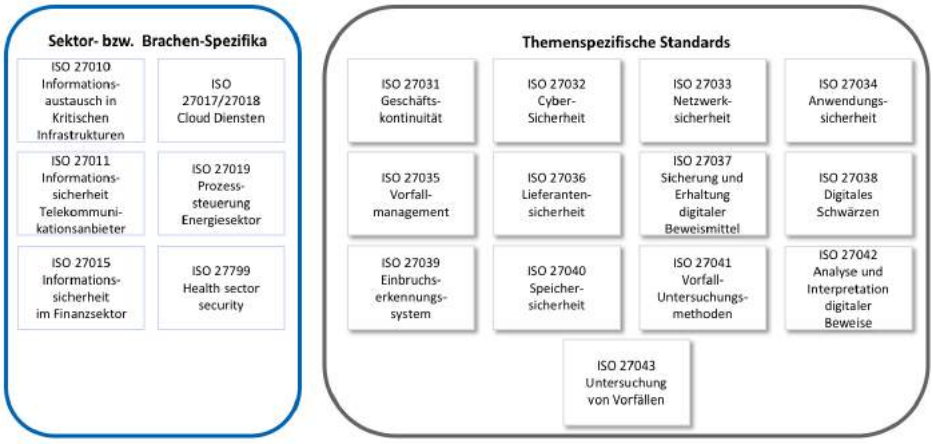


Abbildung 1-3: Normenreihe ISO/IEC 27000 Sektor- / branchenspezifische Normen; Quelle: eigene Darstellung

branchen- bzw. sektorspezifischen Aspekten sowie zu andern Sicherheitsthemen (in der Abbildung 1-3 werden die Titel der Normen nur verkürzt wiedergegeben).

Der IT-Grundschutz bietet eine Methodik für Sicherheitsmanagement mit konkreten Maßnahmenempfehlungen und deckt nicht nur technische, sondern auch organisatorische, personelle und infrastrukturelle Aspekte ab. Ursprünglich für Behörden konzipiert, hat sich der IT-Grundschutz seit 1994 für alle Branchen als ein schnelles und wirtschaftliches Instrument für Informationssicherheit erwiesen und steht Instituten jeglicher Art und aller Größen kostenlos zur Verfügung. Daher ist der IT-Grundschutz im deutschsprachigen Raum zu einer Art „offizieller Messlatte" für Informationssicherheit geworden. Teilweise wird sogar in Regularien, wie etwa den Mindestanforderungen für das Risikomanagement (MaRisk) der Bundesanstalt für Finanzaufsicht (BaFin), explizit auf den IT-Grundschutz referenziert. Deutsche Behörden verlangen bei vielen Projekten mit Dienstleistern aus der Privatwirtschaft die Umsetzung des IT-Grundschutzes. Der IT-Grundschutz vom Bundesamt für Sicherheit in der Informationstechnik (BSI) ist in zwei große Bereiche aufgeteilt, die BSI-Standards und die IT-Grundschutz-Kataloge.

Derzeit gibt es vier BSI-Standards zur Informationssicherheit:

- BSI-Standard 200-1 „Managementsysteme für Informationssicherheit"
  Hier werden die allgemeinen Anforderungen an ein Managementsystem für Informationssicherheit (ISMS) definiert.
- BSI-Standard 200-2 „IT-Grundschutz-Vorgehensweise"
  In diesem Standard zur IT-Grundschutz-Vorgehensweise wird Schritt für Schritt erklärt, wie ein Managementsystem für Informationssicherheit in der Praxis aufgebaut und beschrieben werden kann.
- BSI-Standard 200-3 „Risikoanalyse auf der Basis von IT-Grundschutz"
  In diesem Standard wird eine Methodik für Risikoanalyse vorgestellt, die sich anbietet, wenn in der Institution nach IT-Grundschutz gearbeitet wird.
- BSI-Standard 100-4 „Notfallmanagement"
  Dieser Standard beschreibt Aufbau und Aufgaben eines Notfallmanagementsystems.

Die IT-Grundschutz-Kataloge sind in Bausteine gegliedert, die jeweils ein spezifisches organisatorisches, technisches oder infrastrukturelles Thema behandeln. Dies können zum Beispiel Schutzmaßnahmen für eine konkrete technische Plattform, Anforderungen an Schulungsmaßnahmen oder Sicherheitsaspekte für einen Serverraum sein. In jedem Baustein wird die Thematik zunächst inhaltlich umrissen, dann werden Gefährdungen aufgezeigt, die die Sicherheit des betrachteten Objektes beeinträchtigen können, und schließlich wird auf Maßnahmen verwiesen, die diesen Gefährdungen entgegenwirken (BSI, 2016a).

Für Betreiber von KRITIS sieht das Bundesamt für Sicherheit in der Informationstechnik eine Registrierung beim BSI vor. Das BSI teilt dem registrierten Unternehmen im Gegenzug sämtliche es betreffenden Informationen zu Gefahren für die IT-Sicherheit mit. Die betroffenen Unternehmen müssen dafür sorgen, dass die Systeme, Komponenten und Prozesse ihrer Kritischen Infrastruktur organisatorisch und technisch gesichert sind. Dabei soll der Stand der Technik eingehalten werden. Die Definition dieser Sicherheitsstandards kann vor KRITIS-Betreibern selbst bzw. von ihren Branchenverbänden für ihre Branche vorgeschlagen werden. Das BSI prüft diese auf Antrag und entscheidet, ob diese branchenspezifischen Sicherheitsstandards (B3S) den gesetzlichen Anforderungen genügen (Kaspersky Lab 2017).

Die Normenreihe IEC 62443 befasst sich mit den IT-Sicherheitsanforderungen an Integratoren und Instandhaltungsdienstleister von industriellen Automatisierungssystemen (industrielles Automatisierungssystem) (VDE, 2017a). Der Begriff „industrielles Automatisierungssystem“ umfasst alle Bestandteile, die für den zuverlässigen und sicheren Betrieb einer automatisierten Produktionsanlage erforderlich sind. Das sind auf der einen Seite vernetzte Komponenten, die eine Automatisierungslösung realisieren, wie z. B. Gateways. Dazu gehören auch alle Softwarekomponenten und Applikationen, die zur Automatisierung einer Produktionsanlage eingesetzt werden. Obwohl die Norm ursprünglich von der Automatisierungstechnik in der Prozessindustrie getrieben wurde, deckt ihr Anwendungsbereich nahezu alle Industriebereiche ab, zum Beispiel die diskrete Fertigung, dazu auch die Gebäudeautomation, verteilte Versorgungssysteme für Energie und Wasser sowie Pipelines und die Öl- und Gas-Produktion. Auch andere Branchen, die automatisierte oder ferngesteuerte Einrichtungen einsetzen, fallen in den Anwendungsbereich der IEC 62443 (Kobes 2016).

Die Anwendungsregel VDE-AR-E 2802-10-1 „Zusammenhang zwischen funktionaler Sicherheit und Informationssicherheit am Beispiel der Industrieautomation Teil 1: Grundlagen“ gibt Empfehlungen zur systematischen Harmonisierung der Themen Informationssicherheit und funktionale Sicherheit für Systeme vor allem in der Industrieautomation (DIN EN 61508; VDE 0803 (alle Teile)), künftige Normenreihe DIN EN 62443 (VDE 0802). Sie unterstützt sowohl Hersteller, Integratoren als auch Betreiber. Nach derzeitigem Stand sind im Rahmen der Anwendungsregel VDE-AR-E 2802-10 die folgenden vier Teile geplant:

- Teil 1: Grundlagen
- Teil 2: Referenzarchitektur
- Teil 3: Risiko- und Anforderungsanalyse, Entwicklung von Maßnahmen und Nachweisbarkeit
- Teil 4: Anwendungsbeispiele

Das Anliegen aller Teile ist die Unterstützung der systematischen Ermittlung der Anforderungen und der systematischen Gestaltung effizienter Lösungen, bei denen die Informationssicherheit zur Erreichung der funktionalen Sicherheit notwendig ist. Gleichzeitig ist sie eine Grundlage für weitere Diskussionen (VDE, 2017b).

2 Bedrohungen der IT-Sicherheit Kritischer Infrastrukturen

Andreas Rieb, Universität der Bundeswehr München
Ulrike Lechner, Universität der Bundeswehr München

Die Technik Kritischer Infrastrukturen prägt das Thema IT-Sicherheit Kritischer Infrastrukturen genau wie Gesetze, Normen und Standards. Dieser zweite Abschnitt im einführenden Kapitel beleuchtet die Bedrohungen der IT-Sicherheit in Kritischen Infrastrukturen und beginnt mit einem Abschnitt über ausgewählte Beispiele, während im zweiten Kapitel allgemeine Schwachstellen thematisiert werden.

2.1 Beispiele von IT-Sicherheitsvorfällen in Kritischen Infrastrukturen

Digitalisierung und zunehmende Vernetzung der IT-Systeme in Kritischen Infrastrukturen sowie über Organisationsgrenzen hinweg bedeuten für Betreiber und IT-Sicherheitsverantwortliche neue Herausforderungen. In diesem Abschnitt illustrieren einige Beispiele – neben Stuxnet (Zetter 2014) – typische Bedrohungsszenarien.

Stuxnet ist ein Computerwurm, der 2009 erstmals verwendet und 2010 entdeckt wurde (Raiu 2012). In den späteren Analysen der Experten wurde deutlich, dass zum ersten Mal eine staatliche bzw. militärische Organisation hinter einer Cyberoperation stand (Gaycken 2010). Unter den betroffenen Systemen waren u. a. SCADA-Anlagen in den USA, Großbritannien, Südkorea, Iran und anderen Nationen (Symantec 2011). Das vermutete Hauptziel war nach Ansicht der Experten wie Langner und Gaycken die Störung des iranischen Atomprogramms. Besonders betroffen waren hier die Urananreicherungsanlage in Natanz sowie das Kernkraftwerk Bushehr (Langner 2013; Gaycken 2010).

Für Kritische Infrastrukturen sieht der IT-Sicherheitsexperte Langner eine weitere Gefahr: Stuxnet ist eine Blaupause für andere Angreifer (Langner, 2013). „Seit Stuxnet weiß man, dass die Sabotage von Maschinen und Einrichtungen durch Cyber-Angriffe nicht nur denkbar ist, sondern tatsächlich durchgeführt wird“ (BSI 2015).

So auch Ende 2017: Triton ist eine Malware, die wie Stuxnet ICS-Anlagen Kritischer Infrastrukturen kompromittiert und das Potenzial besitzt, Operationen Kritischer Infrastrukturen zu stören oder gar zu unterbrechen und physischen Schaden anzurichten. Um ein Entdecken der Schadsoftware und der Manipulation laufender Operationen zu verhindern, kompromittiert Triton SIS (Safety Instrumented Systems), die im regulären Betrieb laufende Operationen überwachen und im Falle von „unsafe conditions“, wie zu hohem Druck oder zu hohen Temperaturen, diese Operationen beenden sollen (Symantec, 2017). FireEye vermutet, dass die Angreifer Interesse daran haben, einen Angriff mit hohem Impact und physikalischen Konsequenzen durch die Zerstörung der Anlagen durchzuführen, und vermutet wie bei Stuxnet staatliche Akteure hinter Triton (Johnson u. a. 2017).

Während Malware wie Stuxnet ICS-Anlagen mithilfe von USB-Sticks kompromittierte, da die Anlagen selbst in autarken Netzwerken installiert waren, birgt die Anbindung von ICS-Anlagen an das Internet Gefahren. Denn durch die Anbindung können solche Anlagen

aus Angreifersicht leicht aufgeklärt werden. Hierzu bietet sich die Suchmaschine Shodan[4] an, die sich auf das Aufklären von Geräten spezialisiert hat. Mithilfe dieser Suchmaschine können bspw. Ampelanlagen, Heizsysteme, Router und andere Kontrollanlagen identifiziert werden (Stouffer u. a. 2014). Diese Informationen können Ausgangspunkt für sowohl ungezielte als auch gezielte Cyberangriffe sein. Ein Beispiel eines gezielten Cyberangriffs, bei dem die Angreifer Shodan im Zuge der Informationsbeschaffung nutzten, ist der Angriff auf einen Staudamm in den USA: Staatliche Angreifer nutzten Shodan, um ein veraltetes Betriebssystem innerhalb der Kritischen Infrastruktur aufzuklären, und verschafften sich mit weiteren Angriffsvektoren Zugang in das Netzwerk (Kovacs 2016).

Ein weiterer Trend bzw. ein daraus resultierendes Risiko im Bereich der Kritischen Infrastrukturen und Industrie ist der zunehmende Einsatz von Commercial-of-the-Shelf-Produkten (COTS), die individuelle IT-Lösungen ersetzen (Dacier u. a. 2012; None 2013). Als Beispiel ist hier ein Experiment von Forschern am Lemgoer Fraunhofer-Anwendungszentrum Industrial Automation zu nennen, die eine Smartwatch für die Steuerung einer komplexen Industrieanlage einsetzen (None 2014; None o. J.). Die Nutzung von COTS-Produkten, die u. a. das Monitoring erleichtern, die Wartung vereinfachen, Kosten senken und andere Vorteile mit sich bringen, birgt jedoch auch das Risiko, dass Malware und Angriffsvektoren, die vorrangig weit verbreitete IT-Lösungen bedrohen, zukünftig vermehrt auch ein Risiko für Kritische Infrastrukturen und Industrie darstellen werden (Dacier u. a. 2012).

Neben all diesen Trends haben Kritische Infrastrukturen zudem weitere Herausforderungen, die in herkömmlichen Business-IT-Netzwerken eher selten anzutreffen sind. IT-Systeme in Kritischen Infrastrukturen sind auf eine lange Laufzeit ausgelegt. Das bedeutet, dass veraltete Betriebssysteme, wie z. B. Windows NT 3.5, Windows 95 oder Windows XP, noch immer eingesetzt werden. Solche veralteten Betriebssysteme werden nach Kaspersky Lab u. a. in Krankenhäusern eingesetzt (Kaspersky Lab 2016). Hochspezialisierte medizinische Geräte sind IT-gestützt und speichern alle Informationen in einem digitalen Format ab. Darüber hinaus sind Fachkräfte wie Ärzte von der Funktionsfähigkeit der Geräte abhängig und vertrauen auf die Korrektheit der Daten. Die Geräte selbst basieren jedoch teilweise auf alten Betriebssystemen, wie Windows XP, sind nicht mit aktuellen Patches ausgestattet oder haben gesetzte Default-Passwörter (Kaspersky Lab, 2016). Letzteres Problem wird zudem verschärft, wenn Default-Passwörter nicht geändert werden können, was häufig bei IT-Systemen im Umfeld Kritischer Infrastrukturen der Fall ist. So warnte z. B. das ICS CERT 2013 vor 300 medizinischen Geräten von insgesamt 40 Herstellern, die eine Schwachstelle mittels hard-coded Passwörtern beinhalteten (ICS-CERT 2013). Ein anderes Beispiel ist die Industriesteuerungsanlage S7-300, die in bestimmten Modellen Passwort und Benutzernamen unveränderlich in die Hardware eingebrannt hat (Kremp 2011). Solche Probleme und Schwachstellen stellen im Zuge von Digitalisierung und damit Vernetzung Risiken dar (z. B. ein veraltetes Betriebssystem mit unveränderlichem Default-Passwort, das im Zuge der Vernetzung nun an andere Netzwerke angeschlossen wird), diese Kombination bedeutet für den Angreifer ein ungeahntes Angriffspotenzial mit weitreichenden Konsequenzen.

4 https://www.shodan.io/.

Neben den genannten Beispielen, in denen die Angreifer zielgerichtet Anlagen und Systeme Kritischer Infrastrukturen kompromittierten, sind Betreiber Kritischer Infrastrukturen zusätzlich Bedrohungsszenarien ausgesetzt, die vorrangig Privatnutzer oder Nicht-Kritische Infrastrukturen adressieren. An dieser Stelle sind die beiden Schadsoftware-Produkte Mirai und WannaCry zu erwähnen. Mirai ist ein Werkzeug, das internetfähige Devices wie Router, Überwachungskameras, Fernseher oder Digital-Video-Recorder zu einem Botnet zusammenschaltet, um Distributed-Denial-of-Service-Attacken organisieren und ausführen zu können. Die Opfer hatten als Folge des Angriffs einen mehrtägigen Ausfall von Telefon, Internet und TV hinzunehmen (Kremp 2016). WannaCry ist ein Schadprogramm, das im Mai 2017 weltweit mehr als 200.000 Windows-Systeme mit einem Krypto-Trojaner infizierte und Daten verschlüsselte. Dazu nutzte WannaCry eine Schwachstelle, die durch EternalBlue ausgenutzt werden kann und bereits wenige Monate zuvor von Microsoft behoben worden war (Perakalin 2017). Obgleich WannaCry nicht als gezielte Attacke betrachtet werden kann, wurden dennoch Kritische Infrastrukturen verschiedener Sektoren Opfer dieses Angriffs (Beer 2017).

Diese Beispiele illustrieren, dass IT-Sicherheit ein zentrales Thema für die Gesellschaft und vor allem für Betreiber Kritischer Infrastrukturen ist. Der schnelle Wandel und die fortschreitende Vernetzung erfordern ein hohes Maß an Security-Awareness, ein ständiges Weiterentwickeln von Sicherheitsarchitekturen und -konzepten sowie eine fortlaufende Betrachtung und Analyse aktueller Bedrohungen.

2.2 Bedrohungen, Gefährdungen und Schwachstellen der IT in Kritischen Infrastrukturen

Das Bundesamt für IT-Sicherheit in der Informationstechnik analysiert die Bedrohungen für Industrielle Kontroll- und Steuerungssysteme in dedizierten Statistiken (BSI 2016c).

Tabelle 2: Die Top 10 der kritischen Bedrohungen von ICS-Systemen; Quelle: nach BSI 2016c

Nr.	Bedrohung
1	Social Engineering und Phishing
2	Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
3	Infektion mit Schadsoftware über Internet und Intranet
4	Einbruch über Fernwartungszugänge
5	Menschliches Fehlverhalten und Sabotage
6	Internet-verbundene Steuerungskomponenten
7	Technisches Fehlverhalten und höhere Gewalt
8	Kompromittierung von Extranet und Cloud-Komponenten
9	(D)DoS-Angriffe
10	Kompromittierung von Smartphones im Produktionsumfeld

Tabelle 2 fasst diese Bedrohungen von ICS-Systemen zusammen und bezieht sich auf die primären Angriffe. In der Systematik des BSI nutzt der Primärangriff einer Angriffskette eine Schwachstelle aus, um ein Netzwerk zu kompromittieren, in dem Folgeangriffe den An- oder Zugriff auf weitere interne Systeme erlauben. Diese Folgeangriffe nutzen Informationen oder Zugriffsrechte aus dem Primärangriff und können sich häufig ohne große Hürden im internen Netz einer Kritischen Infrastruktur weiterverbreiten. Die Erläuterungen der Top-10-Bedrohungen können dem Bericht des BSI zur Sicherheit industrieller Kontrollsysteme entnommen werden (Bundesamt für Sicherheit in der Informationstechnik 2016).

Die oben genannten Top 10 der kritischen Bedrohungen werden vom BSI auf eine Reihe von Schwachstellen von ICS-Systemen und ICS-Komponenten zurückgeführt. Das BSI hat eine Sammlung von Gefährdungen von ICS-Systemen, wie sie in Audits festgestellt wurden, veröffentlicht (BSI 2017b).

Tabelle 3: Auditergebnisse zur aktuellen Gefährdungslage; Quelle nach BSI 2017b

ICS-Komponente	Sicherheitsrelevante Beobachtungen
Netz	• Anbindung unbekannter Systeme zur Datensicherung
Firewall / Router	• Regeln nicht ausreichend restriktiv • Undokumentierte Regeleinträge • Offenbar nicht mehr benötigte Datenflüsse • Bypass im Routing • IP-Forwarding auf Servern
Modems	• Ungeschützter Zugang • Anschluss nicht dokumentiert • Ständige Verbindung (always-on)
Fernwartung	• Anschluss direkt in Feldebene
Betriebssysteme / Härtung	• Betriebssystemkomponenten nicht gehärtet • Nicht benötigte Dienste angeboten • Nicht-unterstütze neue Betriebssystem-Version und fehlende Patches
Funkverbindungen	• Fehlende Verschlüsselung • Veraltete Netzelemente
Industrie-Switche	• Fehlende Robustheit gegen unerwartete bzw. nicht-standardkonforme Kommunikation • Backdoors (z. B. hart-codierte Passwörter)
Veraltete Netzelemente	• Administrativer, web-basierter Zugang ohne Absicherung (z. B. SSL) • Fehlende Protokollunterstützung (z. B. nur Telnet-Zugang)

Auf die Frage, wer Kritische Infrastrukturen angreift bzw. von welchen Threat Actors ein hohes Schadenspotenzial für Kritische Infrastrukturen ausgeht, nennt das BSI folgende Tätergruppen: politisch motivierte Hacktivisten, Nation States sowie Cyber Criminals mit wirtschaftlichen Interessen. Ransomware ist seit 2015 als Bedrohung für Kritische Infrastrukturen aktuell geworden (BSI 2016b).

Die IT-Bedrohungslage für Kritische Infrastrukturen unterliegt einem stetigen Wandel und erfordert eine ständige Überprüfung des IT-Sicherheitskonzepts und implementierter

IT-Sicherheitsmaßnahmen. Um IT-Sicherheit wirksam betreiben zu können, müssen sich Kritische Infrastrukturen über ihre (kritischen) Geschäftsprozesse und (kritischen) Assets im Klaren sein. Das bedeutet, dass die Frage „Welche Informationen sind besonders wichtig und damit in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit schützenswert und warum (z. B. personenbezogene Daten, Kundendaten, strategische Informationen, Geheimnisse wie Entwicklungsdaten, Patente, Verfahrensbeschreibungen)?“ (BSI 2008) kontinuierlich im Rahmen der Schutzbedarfsfeststellung gestellt werden muss. Das BSI bezeichnet solche kritischen Geschäftsprozesse und Assets im Community Draft des neuen IT-Grundschutzes als „Kronjuwelen“ (BSI, 2017a), denen unter Berücksichtigung der möglichen Auswirkungen auf die Gesellschaft im Falle einer Beeinträchtigung besondere Bedeutung zuteilwerden muss. Denn wie das Beispiel von Ransomware in einem Krankenhaus gezeigt hat, reicht eine Kompromittierung weniger Daten aus, um die Verfügbarkeit elementarer Geschäftsprozesse wie die Aufnahme von Patienten oder die Durchführung von Operationen zu beeinträchtigen (Grass, 2016). Wie auch in vielen anderen Fällen wurde die Ransomware in die IT-Infrastruktur via E-Mail eingebracht (Classen, 2016). Das BSI bezeichnet diese Bedrohung als „Infektion mit Schadsoftware über Internet und Intranet“, sie ist eines von zehn Themen, mit denen sich IT-Sicherheitsverantwortliche und Betreiber Kritischer Infrastrukturen intensiv auseinandersetzen müssen (vgl. Tabelle 2).

Dieser Abschnitt über Gefährdungen und Bedrohungen speziell für Kritische Infrastrukturen mit ihren typischen IT-Elementen gibt einen Eindruck von der Vielfalt, aber auch von den Anstrengungen, die es bedeutet, diese Infrastrukturen zu schützen und diesen Schutz laufend an die aktuelle IT-Sicherheitslage anzupassen.

3 Erfahrungen aus der Praxis – Die Methode der CASE|KRITIS-Fallstudien

Sebastian Dännart, Universität der Bundeswehr München

Die CASE|KRITIS-Fallstudien bieten Erfahrungen aus erster Hand und berichten über erfolgreiche Projekte und bewährte Strategien – Ideen für IT-Sicherheitsprojekte, die über die Verbesserung der Sicherheit und über bewährte Kniffe berichten, mit denen Unternehmen abstrakte Konzepte für sich handhabbar machen.

Da die Einführung von IT-Sicherheitsmaßnahmen zumeist einen Eingriff in bestehende Geschäftsprozesse erfordert, stellen komplexe und schwer voneinander abzugrenzende Zusammenhänge sowie Folgen der Einführung eine große Herausforderung dar. Fallstudien bieten eine Forschungsstrategie zur Datenerhebung, die sich sehr gut dazu eignet, diese komplexen Phänomene in ihrem natürlichen Kontext darzustellen (Eisenhardt 1989; Wilde & Hess 2006; Yin 2003).

Die Methodik für die Fallstudien orientiert sich dabei an der eXperience-Methodik (Schubert & Wölfle 2006). 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 *IT-Sicherheit für Kritische Infrastrukturen ITS|KRITIS* des Bundesministeriums für Bildung und Forschung (BMBF) im Jahr 2015 verfeinert.

3.1 Drei Arten der CASE|KRITIS-Fallstudien

Um den verschiedenen Anforderungen an unterschiedliche Betrachtungsobjekte gerecht zu werden, unterscheiden wir drei Arten von IT-Sicherheitsfallstudien:

- **Unternehmensbezogene Fallstudien**, die die gelebte IT-Sicherheit einer Organisation aus verschiedenen Perspektiven erfassen: Sie ermöglichen es, beispielgebende Umsetzungen von IT-Sicherheit in bestimmten Unternehmen verständlich und strukturiert aufzuarbeiten. Die grundlegendste Art, eine solche Fallstudie zu gestalten, ist die Darstellung eben jener etablierten und erfolgreichen IT-Sicherheitsstrukturen auf das jeweilige Unternehmen bezogen. 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**, die sich auf ein konkretes IT-Sicherheitsprojekt beziehen: 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**, die die Implementierung oder den Einsatz von speziellen innovativen IT-Sicherheitstechnologien beschreiben: 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.

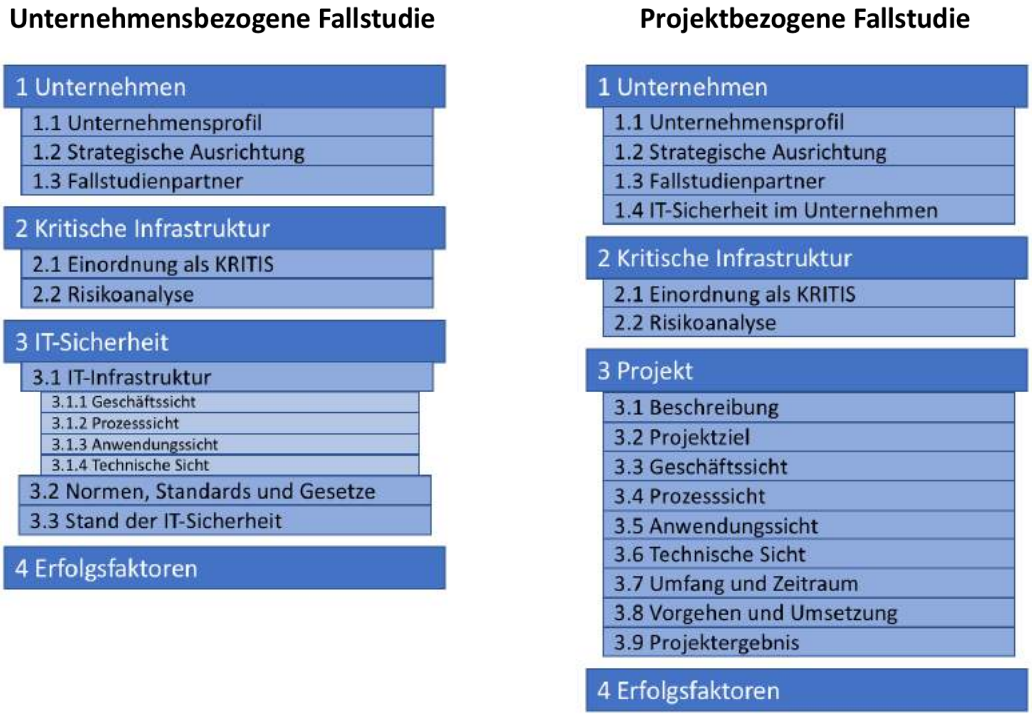


Abbildung 3-1: Grundgliederung der Fallstudientemplates

Die grundlegenden Gliederungen, nach denen unternehmensbezogene sowie projektbezogene Fallstudien strukturiert werden, sind in Abbildung 3-1 aufgeführt. Fallstudien, die nach dem produktbezogenen Ansatz erstellt werden, bedienen sich als Grundlage eines der beiden anderen Leitfäden und passen diesen jeweils spezifisch an die gegebenen Bedürfnisse an. In *Kapitel 16* werden die Fallstudientemplates genauer beschrieben.

3.2 Die Perspektiven der CASE|KRITIS-Fallstudien

Im Zentrum der Fallstudien stehen Unternehmen mit ihren Prozessen und in vier Sichten werden Projekte, Produkte und Unternehmenskulturen dargestellt:

- **Geschäftssicht**
- **Prozesssicht**
- **Anwendungssicht**
- **Technische Sicht**

Im Folgenden werden die Sichten kurz erläutert und beispielhaft visualisiert. Die Beispiele dazu stammen aus den Fallstudien in Teil II dieses Buches, sodass die Beispiele in den direkten Kontext der Fallstudie gesetzt werden können.

3.2.1 Geschäftssicht

Die Geschäftssicht dient dazu, die Organisation sowie die für die IT-Sicherheit relevanten Anspruchsgruppen und Organisationseinheiten zu modellieren und in Relation zueinander zu setzen. So werden hier klassischerweise neben dem IT-Bereich und seinen Unterstrukturen auch relevante Gremien und Dienstleister bzw. externe Anspruchsgruppen mit betrachtet.

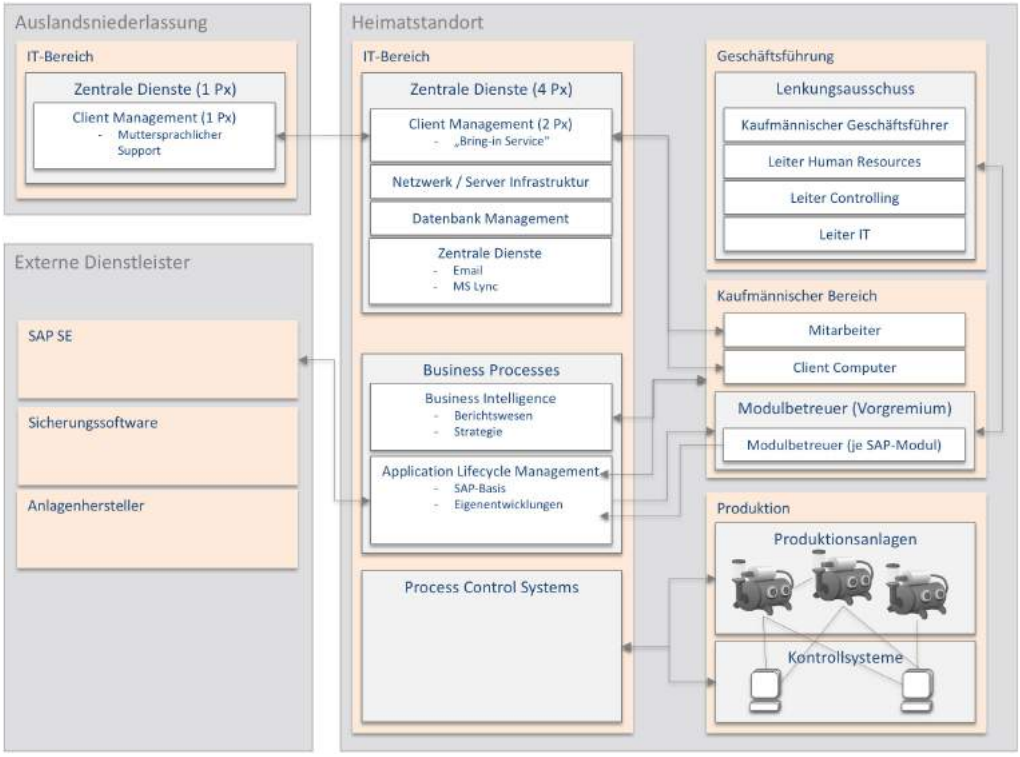


Abbildung 3-2: Beispiel für die Abbildung einer Geschäftssicht; Quelle: Abbildung 8-1: Sicht auf die IT-relevanten Geschäftsbereiche der Molkerei

3.2.2 Prozesssicht

Die Prozesssicht stellt einen oder mehrere für die Fallstudie zentrale Prozesse dar. Beispielsweise können in dieser Sicht konkrete Prozesse der organisationalen Sicherheit, wie die Sicherheitsüberprüfung neuer Mitarbeiter oder die Realisierung von Fernwartungszugängen, aber auch Change-Management-Prozesse zur Änderung im SAP-System – wie in Abbildung 3-3 zu sehen – visualisiert werden. Es ist dabei vom Fokus der Fallstudie abhängig, ob ganze Prozesslandschaften, einzelne Prozesse oder nur Teilprozesse thematisiert werden. In den Fallstudien wird für die Modellierung eine an ereignisgesteuerte Prozessketten (EPK) angelehnte Notation verwendet.

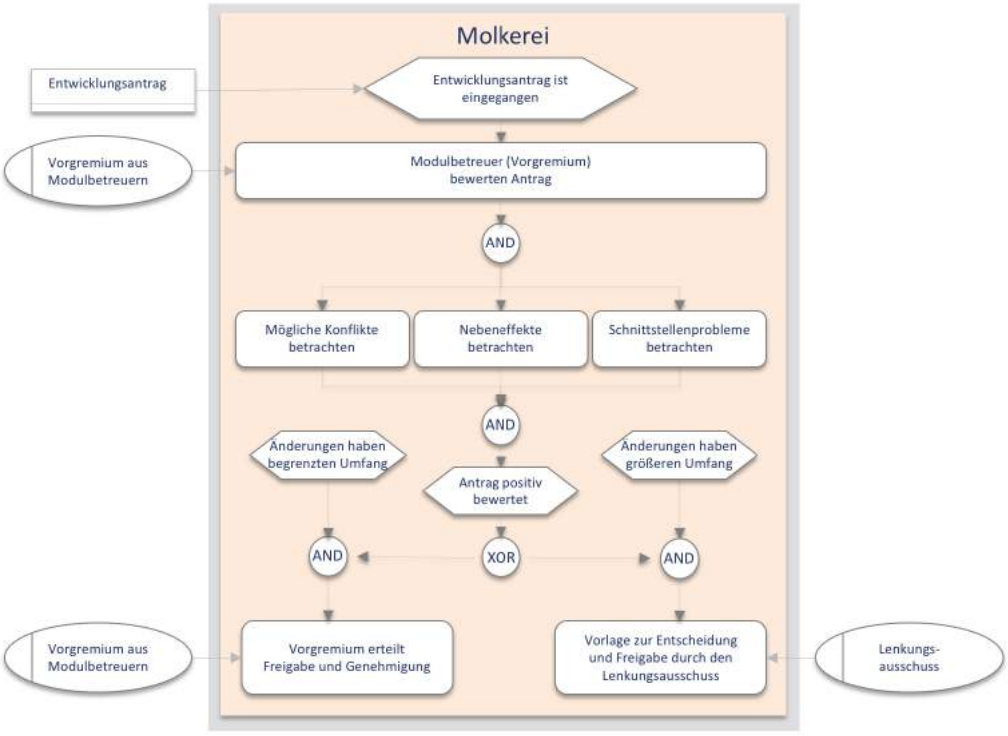


Abbildung 3-3: Beispiel für die Abbildung einer Prozesssicht; Quelle: Abbildung 8-2: Change-Management-Prozess für Entwicklungsanträge

3.2.3 Anwendungssicht

Einen wesentlichen Bestandteil des IT-Systems einer Organisation (und für den Mitarbeiter häufig die sichtbarste Schicht) bilden die Anwendungen. In der Darstellung variieren die Fallstudien zwischen exemplarischen Anwendungsbeispielen bis hin zum Anwendungsportfolio einer Organisation.

Abbildung 3-4 zeigt zum Beispiel die Besonderheit einer Zwei-Säulen-Architektur, die in der Fallstudie für die Auswahl und den Einsatz von Anwendungen eine besondere Rolle spielt.

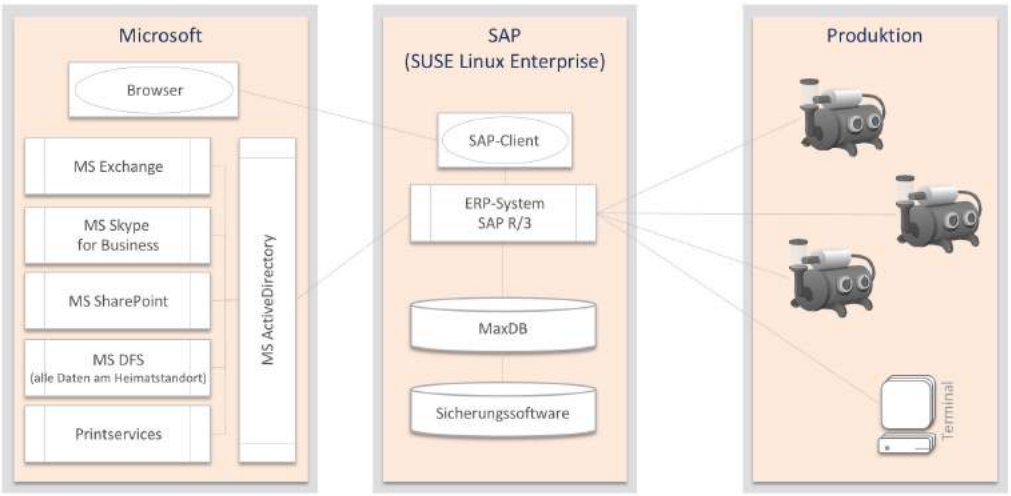


Abbildung 3-4: Beispiel für die Abbildung einer Anwendungssicht; Quelle: Abbildung 8-4: Sicht auf die Anwendungslandschaft der Molkerei

3.2.4 Technische Sicht

Für das Verständnis des Konzeptes der IT-Sicherheit werden die technischen Gegebenheiten in Form eines (vereinfachten) Netzplans dargestellt. Das Beispiel in Abbildung 3-5 zeigt einen schematischen Netzplan der Infrastruktur mit wichtigen IT-Sicherheitsbausteinen.

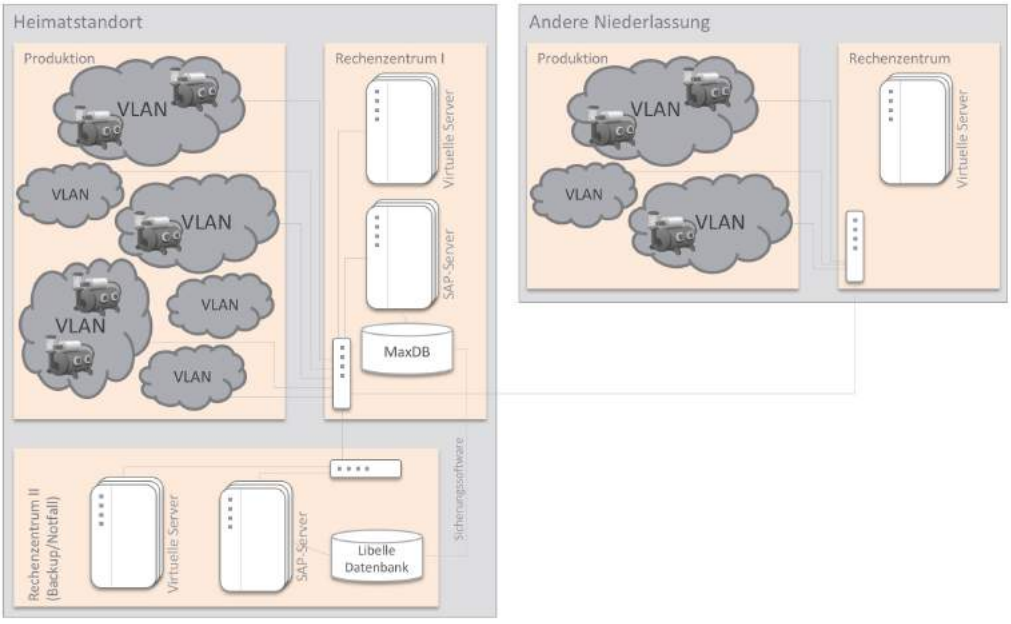


Abbildung 3-5: Beispiel für die Abbildung einer Technischen Sicht; Quelle: Abbildung 8-5: Technische Sicht auf die IT-Infrastruktur der Molkerei

3.3 Vorgehensmodell

Die CASE|KRITIS-Vorgehensweise wird in Abbildung 3-6 dargestellt und die einzelnen Schritte werden im Folgenden kurz erläutert.

Abbildung 3-6: Vorgehen bei der Erstellung der Fallstudien

3.3.1 Auswahl des Objektes

In dieser Phase werden sowohl die Art der Fallstudie (unternehmens-, projekt- oder produktbezogen) als auch der Fokus der Fallstudie in Bezug auf Technologie, Organisation oder Mensch festgelegt. Das soll die weitere Planung der Datenerhebung und das Verfassen der Fallstudien erleichtern.

3.3.2 Vorbereitung der Feldstudie

Über Literaturrecherchen in Veröffentlichungen der Organisation oder offen im Internet können Informationen gewonnen und zur Vorbereitung der Interviews und Datenerhebungen genutzt werden. Die Orientierung an Templates bietet hier einen guten Anhalt, um die Ergebnisse zu strukturieren. In Vorgespräche werden zudem das Vorgehen der Feldstudie, Veröffentlichung und Freigabe besprochen. Weitere Vorgespräche informieren Interviewpartner über Fokus und Zielsetzung der Fallstudie.

3.3.3 Durchführung der Feldstudie

In dieser Phase der Feldstudie werden die Daten erhoben. Dazu werden primär Interviews durchgeführt, aber auch teilnehmende Beobachtung kann die Datenerhebung ergänzen. Besonders wichtig sind in dieser Phase der Feldstudie Vor-Ort-Termine bei der betrachteten Organisation. Es werden in dieser Phase alle Informationen für die Fallstudie zusammengetragen. Die Struktur der Templates kann Hinweise für die Strukturierung der Daten geben.

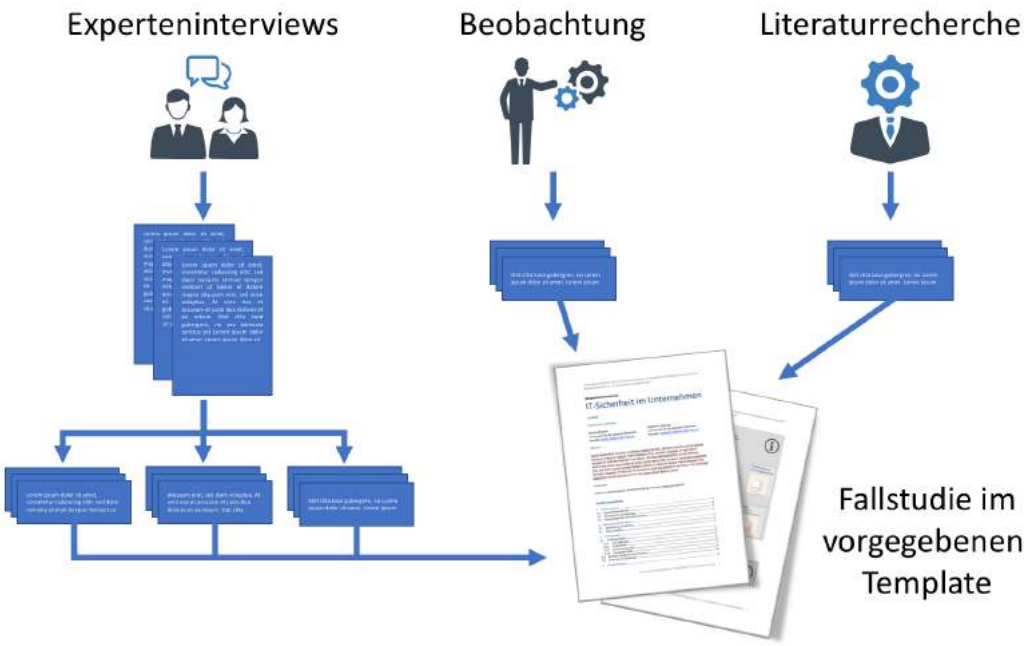


Abbildung 3-7: Inhaltliche Quellen für die Fallstudie

3.3.4 Analyse der Ergebnisse

Da sowohl Interviewtexte als auch Beobachtung regelmäßig wenig strukturiert sind, empfiehlt es sich, durch eine Inhaltsanalyse über alle relevanten Daten hinweg eine Analysebasis zu schaffen. Methoden der qualitativen Inhaltsanalyse können in dieser Phase angewendet werden (vgl. z. B. Mayring 2008; Gläser & Laudel 2010). In dieser Phase der Analyse treten offene Punkte und Unklarheiten auf, welche gesammelt in Rückfragen an die Interviewpartner oder die Verantwortlichen in der Organisation sowie in weiteren Recherchen geklärt werden sollten.

3.3.5 Verfassen der Fallstudie

Auf der Basis der gesammelten und nun strukturiert aufbereiteten sowie analysierten Informationen wird die Fallstudie verfasst.

3.3.6 Freigabe durch Praxispartner

Der Fallstudienpartner gibt die Fallstudie frei und kann im Prozess der Freigabe Änderungen oder Korrekturen an der Fallstudie erwarten. Eine Fallstudie kann in dieser Phase – auf Wunsch des Partners – auch anonymisiert werden. Dabei muss auch eine anonymisierte Fallstudie vom Fallstudienpartner freigegeben werden.

3.4 Cross-Case-Analyse

Über verschiedene Fallstudien hinweg werden in einer Datenanalyse Muster, Gemeinsamkeiten und Unterschiede identifiziert. Verschiedene Autoren (wie Mayring 2008; Eisenhardt 1989; Yin 2003) geben methodische Hinweise zur Durchführung von vergleichenden Fallstudienanalysen.

Informationen zu Methode und Details und das Ergebnis der Cross-Case-Analyse für die Fallstudien dieses Buches sind in *Kapitel 13* enthalten.

3.5 Die Durchführung der Fallstudienserie CASE|KRITIS

Die CASE|KRITIS-Fallstudien in Teil II dieses Buches wurden im Zeitraum von September 2015 bis Januar 2018 durchgeführt und nach dem in diesem Kapitel beschriebenen Vorgehensmodell unter Verwendung des jeweils passenden Templates verfasst.

Literaturverzeichnis Teil I

Beer, K., 2017. Nach WannaCry-Attacke: Dobrindt für schärferes IT-Sicherheitsgesetz. Verfügbar unter: https://www.heise.de/newsticker/meldung/Nach-WannaCry-Attacke-Dobrindt-fuer-schaerferes-IT-Sicherheitsgesetz-3713755.html [zugegriffen: 22-Dez-2017].

BSI, 2008. BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, 2.0, S. 1–90. Verfügbar unter: http://www.bsi.bund.de/gshb [zugegriffen: 7-Juni-2018].

BMI, 2009a. Definition „Kritische Infrastrukturen“, 2009. Verfügbar unter: https://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/BevoelkerungKrisen/Sektoreneinteilung.pdf?__blob=publicationFile%5CnBundesministerium des Innern 2009 – Definition Kritische Infrastrukturen.pdf.

BMI, 2009b. Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), S. 1–16.

BSI, 2012a. BSI-CS 013.

BSI, 2012b. BSI-CS 066.

BSI, 2015. Die Lage der IT-Sicherheit in Deutschland 2015. Bonn.

BSI, 2016a. BSI-MIBro16/811: Überblick IT-Grundschutz Entscheidungshilfe für Manager, S. 1–28.

BSI, 2016b. Die Lage der IT-Sicherheit in Deutschland 2016. Bonn.

BSI, 2016c. Industrial Control System Security: Top 10 Bedrohungen und Gegenmaßnahmen 2016, S. 1–20.

BSI, 2017a. BSI-Standard 200-2, IT-Grundschutz-Methodik, S. 1–139.

BSI, 2017b. ICS-Security-Kompendium. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Empfehlungen/ICS/empfehlungen_node.html [zugegriffen: 7-Juni-2018].

BSI, 2018a. Definition Cybersicherheit. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cyber-sicherheit_node.html [zugegriffen: 7-Juni-2018].

BSI, 2018b. Glossar. IT-Grundschutz: Glossar und Begriffsdefinitionen. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html [zugegriffen: 7-Juni-2018].

Bundesamt für Sicherheit in der Informationstechnik, 2016. Industrial Control System Security, Top 10 Bedrohungen und Gegenmaßnahmen.

Classen, G., 2016. Krisenstab gebildet – OPs verschoben! Hacker-Angriff legt Lukaskrankenhaus Neuss lahm. Express. Verfügbar unter: https://www.express.de/duesseldorf/krisenstab-gebildet-ops-verschoben--hacker-angriff-legt-lukaskrankenhaus-neuss-lahm-23506218 [zugegriffen: 12-Dez-2017].

Dacier, M.; Kargl, F.; Valdes, A., 2012. Securing Critical Infrastructures from Targeted Attacks, S. 49–53. Verfügbar unter: http://doc.utwente.nl/88719/ [zugegriffen: 7-Juni-2018].

DIN, 2009. ISO/IEC 27000:2009.

Eckert, C., 2013. IT-Sicherheit: Konzepte – Verfahren – Protokolle, 8., aktualisierte Ausgabe. Oldenbourg Wissenschaftsverlag GmbH.

Eisenhardt, K. M., 1989. Building theories from case study research. The Academy of Management Review, (4), S. 532–550.

Gaycken, S., 2010. Cyberwar: Das Internet als Kriegsschauplatz, 1. Auflage. Open Source Press.

Gläser, J.; Laudel, G., 2010. Experteninterviews und qualitative Inhaltsanalyse, 4. Auflage. Springer VS.

Grass, K., 2016. Ransomware: Wir haben Eure Daten! Zeit. Verfügbar unter: http://www.zeit.de/2016/11/ransomware-cyberkriminalitaet-patientendaten-krankenhaus-erpressung [zugegriffen: 7-März-2016].

ICS-CERT, 2013. Alert (ICS-ALERT-13-164-01): Medical Devices Hard-Coded Passwords. Verfügbar unter: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01 [zugegriffen: 28-März-2017].

IoTAC, 2016. IoT Security Guidelines, S. 1–66. Verfügbar unter: http://www.iotac.jp/wp-content/uploads/2016/01/IoT-Security-Guidelines_ver.1.0.pdf [zugegriffen: 7-Juni-2018].

ITSKRITIS, 2017. IT-Security Navigator. Verfügbar unter: https://www.itsecuritynavigator.de/ [zugegriffen: 12-Jan-2018].

Johnson, B. u. a., 2017. Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure. Verfügbar unter: https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html [zugegriffen: 22-Dez-2017].

Kaspersky Lab, 2016. How I Hacked a Hospital: Kaspersky Lab Finds Security Weaknesses in Health IT. Kaspersky Lab. Verfügbar unter: https://www.kaspersky.com/about/press-releases/2016_how-i-hacked-a-hospital-kaspersky-lab-finds-security-weaknesses-in-health-it [zugegriffen: 17-Mai-2016].

KasperskyLabs, 2017. Das IT-Sicherheitsgesetz – Was bedeutet es für Unternehmen – ein Leitfaden. Verfügbar unter: https://www.security-insider.de/das-it-sicherheitsgesetz-v-38693-13274/ [zugegriffen: 7-Juni-2018].

Kersten, H., 2016. IT-Sicherheitsmanagement nach der neuen ISO 27001, 1. Auflage. Wiesbaden: Springer Vieweg.

Kipker, D.-K., 2016a. Der Referentenentwurf des BMI zur BSI-Kritis-Verordnung (BSI-KritisV) vom 13.1.2016. MMR, S. VII–VIII.

Kipker, D.-K., 2016b. Die NIS-RL der EU im Vergleich zum deutschen IT-Sicherheitsgesetz. ZD-Aktuell, S. VII–X.

Kipker, D.-K., 2016c. Unbestimmte Rechtsbegriffe. Datenschutz und Datensicherheit, S. 610.

Kipker, D.-K., 2017a. Das neue chinesische Cybersecurity Law. MMR (November 2016), S. 455–460.

Kipker, D.-K., 2017b. Der 2. Korb der BSI-Kritisverordnung tritt in Kraft. MMR, S. V–VIII.

Kipker, D.-K., 2017c. Der BMI-Referentenentwurf zur Umsetzung der NIS-RL. MMR, S. 143–147.

Kipker, D.-K., 2017d. Massiver Ausbau der EU-Cyber-Sicherheitskapazitäten – Jahresansprache 2017 des EU-Kommissionspräsidenten Juncker und Veröffentlichung der neuen europäischen Cyber-Sicherheitsstrategie. MMR, S. VI–VII.

Kipker, D.-K., 2017e. Neuer Verordnungsentwurf für ein einheitliches europäisches IT-Sicherheitsnetzwerk. MMR, S. V–VII.

Kipker, D.-K.; Stelter, M., 2017. Trotz Brexit: Britische Regierung plant langfristige Umsetzung der EU NIS-Richtlinie. MMR, S. X–XIII.

Knapp, E., 2011. Industrial Network Security. Verfügbar unter: http://www.sciencedirect.com/science/article/pii/B9781597496452000100 [zugegriffen: 7-Juni-2018].

Kobes, P., 2016. Leitfaden Industrial Security, VDE Verlag.

Kovacs, E., 2016. Iranian Hacked Computer Controlling US Dam: Prosecutors. Security Week. Verfügbar unter: http://www.securityweek.com/iranian-hacked-computer-controlling-us-dam-prosecutors?utm_source=dlvr.it&utm_medium=twitter [zugegriffen: 4-April-2016].

Kremp, M., 2011. Sicherheitsmängel in Siemens-Anlagen: Hacker, hereinspaziert! Spiegel Online. Verfügbar unter: http://www.spiegel.de/netzwelt/web/sicherheitsmaengel-in-siemens-anlagen-hacker-hereinspaziert-a-778333.html [zugegriffen: 20-März-2017].

Kremp, M., 2016. Telekom-Hack hätte viel schlimmer kommen können. Verfügbar unter: http://www.spiegel.de/netzwelt/web/deutsche-telekom-stoerung-war-misslungener-botnet-angriff-a-1123544.html [zugegriffen: 22-Dez-2017].

Langner, R., 2013. To Kill a Centrifuge: A Technical Analysis of What Stuxnet’s Creators Tried to Achieve. Verfügbar unter: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf. [zugegriffen: 7-Juni-2018].

Mayring, P., 2008. Qualitative Inhaltsanalyse. Grundlagen und Techniken, 10. Auflage. Beltz.

None, 2013. Verschmelzung von Business- und Industrienetzen. IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, S. 56–57.

None, 2014. Cyber-Sicherheit in Produktion und kritischen Infrastrukturen. IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, S. 42–44.

None, 2017. Smartwatch steuert Maschinen. Neue Westfälische. Verfügbar unter: http://www.nw.de/nachrichten/wirtschaft/11285251_Smartwatch_steuert_Maschinen.html [zugegriffen: 3-Jan-2017].

Perakalin, A., 2017. WannaCry: Are you safe? Verfügbar unter: https://www.kaspersky.com/blog/wannacry-ransomware/16518/ [zugegriffen: 22-Dez-2017].

Raiu, C., 2012. The Day The Stuxnet Died. Verfügbar unter: https://securelist.com/blog/events/33206/the-day-the-stuxnet-died-27/ [zugegriffen: 24-Dez-2015].

Schubert, P.; Wölfle, R., 2006. The Experience Methodology For Writing IS Case Studies R. Wölfle; P. Schubert (Hrsg.). Americas Conference on Information Systems (AMCIS), S. 19–30.

Stouffer, K. u. a., 2014. Guide to Industrial Control Systems (ICS) Security. Gaithersburg. Verfügbar unter: http://industryconsulting.org/pdfFiles/NIST Draft-SP800-82.pdf.

Symantec, 2017. Triton: New Malware Threatens Industrial Safety Systems. Verfügbar unter: https://www.symantec.com/blogs/threat-intelligence/triton-malware-ics [zugegriffen: 22-Dez-2017].

Symantec, 2011. What You Need to Know About the „Duqu“ Threat. Verfügbar unter: https://www.symantec.com/en/ca/articles/article.jsp?aid=20110311_duqu_threat [zugegriffen: 16-Mai-2014].

Umweltbundesamt, 2016. Trinkwasserversorgung. Verfügbar unter: https://www.umweltbundesamt.de/trinkwasserversorung#textpart-1 [zugegriffen: 22-Dez-2017].

VDE, 2017a. E DIN IEC 62443-2-4 VDE 0802-2-4:2017-01 IT-Sicherheit für industrielle Automatisierungssysteme. Verfügbar unter: https://www.vde-verlag.de/normen/1800319/e-din-iec-62443-2-4-vde-0802-2-4-2017-01.html [zugegriffen: 7-Juni-2018].

VDE, 2017b. VDE-AR-E 2802-10-1:2017-04 VDE-AR-E 2802-10-1. Anwendungsregel: 2017-04, Zusammenhang zwischen funktionaler Sicherheit und Informationssicherheit am Beispiel der Industrieautomation.

VdS, 2017. VdS 10010: VdS-Richtlinien zur Umsetzung der DSGVO, S. 1–32.

VdS, 2015. VdS 3473: Cyber-Security für kleine und mittlere Unternehmen (KMU), S. 1–38.

Wilde, T.; Hess, T., 2006. Methodenspektrum der Wirtschaftsinformatik: Überblick und Portfoliobildung. Arbeitsbericht 2006/2: Institut für Wirtschaftsinformatik und Neue Medien der Ludwig-Maximilians-Universität München (2), S. 1–20. Verfügbar unter: http://www.wim.bwl.uni-muenchen.de/download/epub/ab_2006_02.pdf [zugegriffen: 7-Juni-2018].

Yin, R. K., 2003. Case Study Research – Design and Methods, 3. Auflage. Thousand Oaks, London, New Delhi: SAGE Publications Inc.

Zetter, K., 2014. Countdown to Zero Day, Crown.

Teil II

Fallstudien

Dieser Teil des Buches enthält eine Sammlung von Fallstudien, die im Rahmen und Kontext des Förderschwerpunkts ITS|KRITIS entstanden. Sie wurden nach der in Kapitel 3 beschriebenen Methodik angefertigt und stellen verschiedene erfolgreiche Projekte und beispielhafte Umsetzungen von Informations- und IT-Sicherheit vor. Die Fallstudien dienen als Good Practices im Bereich der IT-Sicherheit Kritischer Infrastrukturen.

Kapitel	Organisation	Titel der Fallstudie	Autor(en)	Art der Fallstudie
4	Bundeswehr	AG IT-SecAwBw – Wie eine Arbeitsgruppe IT-Security-Awareness im In- und Ausland fördert	A. Rieb, G. Opper	Produkt
5	genua mbH	Fernwartung Kritischer Infrastrukturen	A. Rieb	Projekt
6	itWatch GmbH	Ein sicherer Standardprozess für die digitale Tatortfotografie mit DeviceWatch	S. Lücking, S. Dännart	Projekt
7	kbo	Ausgewogenes Risikomanagement für nachhaltige Sicherheit	T. Kehr, S. Dännart	Projekt
8	Molkerei	IT-Sicherheit in der Molkerei: Familientradition und Hochverfügbarkeit	S. Dännart	Unternehmen
9	PREVENT	IT-Sicherheit für Geschäftsprozesse im Finanzsektor: die Managementlösung PREVENT	S. Rudel, T. Bollen	Projekt
10	SAP SE	Informationssicherheit bei SAP SE: Die längste Human Firewall der Welt	U. Lechner, A. Rieb T. Gurschler,	Unternehmen
11	Stadt Gera	Zentrale Leitstelle Ostthüringen: IT-Sicherheit in einer Leitstelle	T. Gurschler, A. Rieb, M. Hofmeier	Unternehmen
12	ugarbe.de software	Informationssicherheit durch ClassifyIt: Informationssicherheit durch gestützte Klassifizierung von Dokumenten und E-Mails	A. Rieb	Produkt

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 in der Regel den Stand vor Inkrafttreten des IT-Sicherheitsgesetzes und dessen Umsetzung dar. Für diesen Beitrag wurden neun Fallstudien ausgewählt, die eine große Bandbreite Kritischer Infrastrukturen und IT-Sicherheitsprojekten abdecken. In diesem Kapitel werden die Fallstudien einzeln vorgestellt.

4 Bundeswehr: AG IT-SecAwBw – Wie eine Arbeitsgruppe IT-Security-Awareness im In- und Ausland fördert

Andreas Rieb, Universität der Bundeswehr München
Gerrit Opper, Bundeswehr

Die PIA-Kampagne 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.

Keywords: Sektor Staat und Verwaltung, Mitarbeitersensibilisierung, IT-Security-Awareness, Informationssicherheit, Human Factor

4.1 Unternehmen

4.1.1 Unternehmensprofil

Die Bundeswehr hatte zum Zeitpunkt der Erstellung der Fallstudie (11/2017) ca. 170.000 Berufs- und Zeitsoldaten und ca. 8.600 Freiwillig Wehrdienstleistende. Ebenfalls gehören die zivile Verwaltung und der gesamte nachgeordnete Geschäftsbereich des Bundesministeriums der Verteidigung (BMVg) zur Bundeswehr. Die primären Aufträge der Bundeswehr sind es, Deutschland und seine Bürger zu schützen, die außenpolitische Handlungsfähigkeit Deutschlands zu sichern, zur Verteidigung der Verbündeten beizutragen, einen Beitrag zu Stabilität und Partnerschaft im internationalen Rahmen zu leisten sowie die multinationale Zusammenarbeit und die europäische Integration zu fördern.

4.1.2 Strategische Ausrichtung

Mit der Aufstellung des Kommandos Cyber- und Informationsraum (KdoCIR) hat die Bundeswehr im Jahr 2017 einen neuen Organisationsbereich geschaffen, um der zunehmenden Relevanz des Themas IT-Sicherheit für die außenpolitische Handlungsfähigkeit und den Schutz der Bürger Rechnung zu tragen. Auch die North Atlantic Treaty Organization (NATO) behandelt den Cyber-Raum (engl. „Cyber Domain") als einen eigenen Operationsraum [1] und auch viele Partnerländer prägen Cyber-Fähigkeiten in eigenen Organisationsformen aus. Auch die Bundeswehr verbessert ihre Cyber-Fähigkeiten, um als zunehmend digitalisierte Großorganisation die Chancen der Digitalisierung zu nutzen, aber auch, um den Bedrohungen aus dem Cyber- und Informationsraum begegnen zu können.

Die Bundeswehr ist ein Element der Sicherheitsarchitektur Deutschlands und das Weißbuch formuliert die aktuelle Sicherheitslage und legt strategische Entwicklungen fest. Die

Trendwende im Personalkörper und die Modernisierung der Bundeswehr, ihrer Personalpolitik und ihrer Beschaffungsprozesse sind wesentliche Elemente, die strategischen Vorgaben zu erreichen. Für die Bundeswehr sind Kurswechsel immer längerfristig und benötigen in Anbetracht der Größe der Organisation für die Umsetzung Zeit.

4.1.3 Fallstudienpartner

Name	Position im Unternehmen
Ralf Fornefeld	Fregattenkapitän, AG IT-SecAwBw, Bundeswehr
Gerrit Opper	Hauptmann, AG IT-SecAwBw, Bundeswehr
Andreas Rieb	Wissenschaftlicher Mitarbeiter, Universität der Bundeswehr München

4.1.4 IT-Sicherheit im Unternehmen

Die IT-Sicherheitsorganisation ist hierarchisch aufgebaut und hat das Ressort des Chief Information Security Officers (CISO Ressort) an der Spitze im BMVg, gefolgt vom Chief Information Security Officer der Bundeswehr (CISOBw) im KdoCIR, der die strategische Steuerung der Informationssicherheit in der Bundeswehr durchführt. Zusätzlich hält die Bundeswehr enge Verbindung zum Bundesamt für Sicherheit in der Informationstechnik (BSI). Die Bundeswehr hat in den Gremien des BSI eigene Vertreter und ist im nationalen Cyberabwehrzentrum vertreten.

Durch Erlasse und Weisungen werden die IT-Sicherheitsbeauftragten der Organisationsbereiche (IT-SiBeOrgBer) gesteuert, die bis auf die Ebene der einzelnen Dienststellen im Fachstrang die IT- / Informationssicherheit in ihren Dienststellen sicherstellen. Operativ ist das Cyber Security Operations Center der Bundeswehr (CSOCBw) im Zentrum Cybersicherheit der Bundeswehr (ZCSBw) für Incident Response zuständig. Das CSOCBw hält enge Arbeitsbeziehungen zum Bundesamt für den Militärischen Abschirmdienst (BAMAD) und zur BWI, die Großteile der IT-Infrastruktur der Bundeswehr, neben dem Betriebszentrum IT-System der Bundeswehr (BtrbZ IT-SysBw), betreut. Die Deutsche militärische Security Accreditation Authority (DEUmilSAA) ist für die Akkreditierung (adäquat zum BSI) von VS-verarbeitenden IT-Systemen zuständig und berät dahingehend die Projekte im Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw). Die DEUmilSAA ist organisatorisch im ZCSBw des IT-Kommandos der Bundeswehr (ITKdoBw) im KdoCIR verortet.

Die Bundeswehr lehnt sich an die Standards des BSI-IT-Grundschutzes und somit an die ISO 27001 an. Das Bundesdatenschutzgesetz (BDSG) und ab Mai 2018 die Europäische Datenschutz-Grundverordnung (EU DSGVO) sowie die Vorgaben für den Geheimschutz aus dem Bundesministerium des Innern (BMI) sind im Ressort des Geschäftsbereichs des BMVg verbindlich. Meldeverpflichtungen an das BSI leiten sich aus dem § 4 BSI-Gesetz (BSIG) ab. Die IT Infrastructure Library (ITIL) als Sammlung vordefinierter Prozesse, Funktionen und Rollen innerhalb der IT-Infrastruktur wird im IT-Betrieb und beim zentralen IT-Dienstleister BWI, der mitunter für die IT-Sicherheit in der Bundeswehr verantwortlich ist, verwendet.

Die IT-Infrastruktur der Bundeswehr ist heterogen. In der Bürokommunikationslandschaft mit herkömmlichen Softwareprodukten von Microsoft werden auch verschiedene andere IT- und Führungs- und Informationssysteme genutzt. Nicht zu vergessen sind die Industry Control Systems (ICS), wie bspw. Anlagen für die Rollfeldbeleuchtung bei diversen Luftwaffenstützpunkten. ICS müssen in der Betrachtung der Sicherheitsaspekte im Rahmen von neuer Beschaffung und alter Infrastruktur besonders berücksichtigt werden.

Aufgrund der Verarbeitung schützenswerter Informationen im Geschäftsbereich BMVg wird die IT entsprechend klassifiziert und gegebenenfalls physikalisch getrennt. Auch Lösungen für Übergänge zu Netzen mit unterschiedlichen Sicherheitsniveaus sind im Einsatz. Grundsätzlich ist der Ansatz gewählt, dass IT-Systeme mit gleichem Sicherheitsniveau vernetzt werden können. Das Bürokommunikationsnetzwerk hat zudem für jeden Nutzer einen personalisierten, kontrollierten Zugang über einen Proxy-Server in das Internet.

Teilweise haben akkreditierte Unternehmen internetbasierten Zugriff auf IT-Systeme der Bundeswehr. Dies ist vor allem dann notwendig, wenn diese IT-Systeme ferngewartet oder fernadministriert werden müssen. Solche VPN-basierte Zugriffe auf IT-Systeme kommen vor allem in den Bereichen der Luft- und Raumfahrt sowie des Sanitätsdienstes vor.

In einer komplexen Organisation wie der Bundeswehr sind nicht nur die Risiken von technischen Schwachstellen, die Fehler in Prozessen der Beschaffung, im Einsatz, in der Wartung, sondern auch im Besonderen Risiken des „Faktors Mensch“ zu sehen. Soldaten und zivile Mitarbeiter können potenziell bewusst oder auch unbewusst Fehler machen. Diese Fehler können weitreichende Auswirkungen haben, die im schlimmsten Falle Leib und Leben von Soldaten oder auch Zivilisten gefährden.

4.2 Kritische Infrastruktur

4.2.1 Einordnung als KRITIS

Die Bundeswehr ist nicht als Kritische Infrastruktur (KRITIS) im Sinne des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme eingestuft; auch wenn KRITIS-Kriterien für den Betrieb der Bundeswehrzentralkrankenhäuser oder im Auslandseinsatz ersichtlich sind. Als kritisch zu betrachten sind alle Assets, die im Rahmen der Informationsgewinnung oder Destabilisierung ein lohnendes Ziel darstellen können. Ganz klar werden hier exemplarisch die Infrastruktur von Einrichtungen mit Flugbetrieb (Lufthoheit in Deutschland) sowie der Anteil von wichtigen logistischen Mitteln und medizinischer Versorgung gesehen.

4.2.2 Risikoanalyse

IT-Sicherheit Kritischer Infrastrukturen ist ein neues Thema in der IT-Sicherheit, das die Absicherung von Produktionsanlagen, Logistikketten o. a. thematisiert. Stuxnet hat das Thema IT-Sicherheit für Kritische Infrastrukturen bekannt gemacht. So ist es notwendig, dass sich Mitarbeiter mit dem Thema IT-Sicherheit auseinandersetzen, die bisher die IT lediglich als Enabler im Rahmen der Unternehmensprozesse genutzt haben. Ebenso müssen sich IT-Professionals über IT-Sicherheit von Anlagen Gedanken machen, die bisher nicht als

IT-Sicherheitsrisiko betrachtet wurden. Im Spannungsfeld von unpopulärer IT-Sicherheit und drängender Notwendigkeit, Organisationen abzusichern, soll IT-Security-Awareness Mitarbeiter sensibilisieren und befähigen, adäquat auf Bedrohungen der IT-Sicherheit zu reagieren. „Um den Mitarbeitern das nötige Wissen zu vermitteln, sind gleichermaßen Sensibilisierungs- und Schulungsmaßnahmen erforderlich. Ziel der Sensibilisierung für Informationssicherheit ist es, die Wahrnehmung der Mitarbeiter für sicherheitskritische Situationen und der potentiellen Auswirkungen ihrer Handlungen zu schärfen. Durch Schulungen zur Informationssicherheit sollen die Mitarbeiter die notwendigen Kenntnisse und Kompetenzen für sicherheitsbewusstes Verhalten erwerben“ [2]. Das BSI sieht IT-Security-Awareness als zentrales Element, um Gefährdungen durch organisatorische Mängel (*G 2.2 Unzureichende Kenntnis über Regelungen*), menschlichen Fehlhandlungen (z. B. *G 3.44 Sorglosigkeit im Umgang mit Informationen*, *G 3.8 Fehlerhafte Nutzung von IT-Systemen*) oder vorsätzlichen Handlungen (z. B. *G 5.9 Unberechtigte IT-Nutzung*) zu begegnen [2] [3].

Als Beispiel für die fehlerhafte Nutzung von IT-Systemen in Kombination mit der Nichtbeachtung von Sicherheitsmaßnahmen wird die Nutzung von dienstlichen USB-Sticks an privaten IT-Geräten genannt. Wenn die USB-Sticks im Anschluss an eine private Nutzung wieder für dienstliche Zwecke genutzt werden, hat das häufig eine Infektion der IT-Systeme der Bundeswehr zur Folge.

Weitere Risiken ergeben sich für die Bundeswehr zudem durch den Einzug der Social Media und die private Nutzung Sozialer Netzwerke, in denen auch dienstliche Detailinformationen (z. B. aus dem Einsatz) veröffentlicht werden.

Auch in den Führungsebenen gibt es Risiken, vor allem wenn Entscheider im Umgang mit den Gefahren im und aus dem Cyber-Raum unsicher sind. Aus Sicht des BSI spielt die Managementebene im Kontext der Informationssicherheit eine besondere Rolle und bietet mit der Maßnahme *M 3.44 Sensibilisierung des Managements für Informationssicherheit* explizite Hilfestellungen für zielgruppengerechte Sensibilisierungsmaßnahmen [4].

4.3 Projekt

Der Grundgedanke, Erfahrungen aus der Praxis für die Praxis mit den pädagogischen Fertigkeiten zu verknüpfen, wurde mit dem ersten IT-Security-Awareness-Tag der Bundeswehr 2010 im BMVg in Bonn geboren. Aus einer Interessengemeinschaft von ca. 25 Personen, meist IT-Sicherheitsbeauftragte einzelner Dienststelle, haben diese sich neben ihrer eigentlichen Tätigkeit in der jeweiligen Dienststelle dazu bereit erklärt, Informationsmaterialien für Schulungszwecke zu entwickeln und bereitzustellen.

Unter der Schirmherrschaft des damaligen stellvertretenden IT-Sicherheitsbeauftragten der Bundeswehr, Herrn Brigadegeneral Klaus Veit, wurde im März 2011 die Arbeitsgruppe IT-Security-Awareness der Bundeswehr (AG IT-SecAwBw) ins Leben gerufen und die Erstellung und Bereitstellung von IT-Security-Awareness-Informationen und -materialien zentralisiert.

In einem Pilotprojekt wurde 2012 die PIA-Kampagne (PIA = Durch Partnerschaft sicher – IT-Security-Awareness) als Sensibilisierungskampagne im Bundeswehrstandort Köln-Wahn mit ca. 12.000 Bundeswehrangehörigen und Bediensteten getestet.

Abbildung 4-1: Logo der PIA-Kampagne; Quelle: Bundeswehr

Seitdem werden Inhalte dieser Kampagne erfolgreich auch für alle anderen Bundeswehrstandorte und Dienststellen bereitgestellt und aktiv genutzt. Zu den Inhalten dieser Kampagne zählen bspw. ein von der Arbeitsgruppe produzierter Ausbildungsfilm sowie kurze Filmclips, die je nach Ausbildungsziel verwendet werden können.

Diese und weitere Materialien bietet die Bundeswehr im „PIA-Werkzeugkasten" an, der über das Intranet allen Soldaten und zivilen Mitarbeitern der Bundeswehr frei zugänglich ist und im Rahmen der Sensibilisierung genutzt werden kann.

Die Durchführung einer Nutzersensibilisierung innerhalb der Bundeswehr ist für alle Dienststellen Pflicht. So fordert die Zentrale Dienstvorschrift A-960/1 „IT-Sicherheit in der Bundeswehr": „Die Sensibilisierung und Schaffung eines Risikobewusstseins (Awareness) der Mitarbeiter und Mitarbeiterinnen zur IT-Sicherheit ist eine allgemeine Führungsaufgabe aller Vorgesetzten" [5]. Ferner fordert die Vorschrift:

- Kontinuierliche Information und Aufklärung über aktuelle Entwicklungen im Bereich IT-Security Awareness.
- Regelmäßige Durchführung eines ‚IT-Security-Awareness-Tages' in Verantwortung des bzw. der IT-SiBeBw (jetzt CISOBw).
- Regelmäßige Durchführung von ‚IT-Security-Awareness-Tagen / Nutzersensibilisierungsmaßnahmen' aller DSt / EinsKtg in ihrem Zuständigkeitsbereich.
- Ständige Überprüfung der Meldesysteme und deren Wege bei einem IT-Sicherheitsvorfall.
- Auswertung der Ergebnisse von Überwachungsmaßnahmen, um eigene IT-Security-Awareness-Maßnahmen zielgerichtet zu aktualisieren.

Mit der Aufstellung des KdoCIR am 01.04.2017 ist das Aufgabenspektrum des IT-Sicherheitsbeauftragten der Bundeswehr auf den CISOBw übertragen worden.

4.3.1 Projektziel

Ziel ist es, eine flächendeckende Sensibilisierung für Gefahren im Cyber-Raum für die Zielgruppe der IT-Nutzer auf verschiedenen Hierarchieebenen der Dienstgradstruktur zu bewirken. Dabei sollen für Soldaten und zivile Bedienstete der Bundeswehr ein Interesse für die Thematik der IT-Sicherheit und damit ein Bewusstsein für dieses Thema geschaffen werden.

Durch die multimedialen Tools im Werkzeugkasten sollen diese Ziele zeitgemäß erreicht werden und bewirken, dass IT-Sicherheit nicht als „Hürde" im Dienstbetrieb wahrgenommen wird.

Abhängig von der Größe und dem Auftrag der einzelnen Dienststellen sowie von aktuellen Bedürfnissen der Bundeswehr werden die Tools im Werkzeugkasten modular bereitgestellt und kontinuierlich erweitert.

4.3.2 Geschäftssicht

Die AG IT-SecAw wird von Fregattenkapitän Ralf Fornefeld geleitet und ordnet sich im Aufgabenbereich des CISOBw ein.

Neben dem Leiter besteht die Arbeitsgruppe aus freiwilligen Offizieren und Unteroffizieren sowie zivilen Bediensteten der Bundeswehr. Seit Gründung der Arbeitsgruppe wurde stets darauf geachtet, dass die Mitgliederstruktur ein breites Spektrum an Teilstreitkräften, Führungsebenen und Dienststellen abbildet, die in der Bundeswehr existieren. So sind bspw. für den Bereich Ausbildung / Lehre / akademische Ausbildung die Helmut-Schmidt-Universität – Universität der Bundeswehr Hamburg sowie die Schule Informationstechnik der Bundeswehr (ITSBw) und die Führungsakademie der Bundeswehr (FüAkBw) vertreten. Die Arbeitsgruppe profitiert von dem Wissen der Teilnehmer dieser Organisationen, denn einerseits findet ein regelmäßiger Informationsaustausch im Themenfeld der IT-Sicherheit mit Dozenten, wie bspw. im Lehrgang für den Generalstabsdienst / Admiralstabsdienst national (LGAN), statt. Andererseits können über die Dozenten der o. g. Organisationen die Ideen, die Ansätze sowie die Materialien den entsprechenden Lehrgangsteilnehmern, wie bspw. Führungskräften und IT-Sicherheitsbeauftragten, präsentiert werden.

Neben den Ausbildungsorganisationen sind in der AG IT-SecAw weitere Verbände, wie Kampftruppen, Marineunterstützung, Sanitätsdienst und Verwaltung, vertreten. Durch die vielseitige Expertise können bereits in der Entwicklung von Kampagnenelementen sowohl Informationen und Bedürfnisse unterschiedlicher Verbände als auch zielgruppenspezifische Belange berücksichtigt werden. Denn neben unterschiedlichen Dienstgradstrukturen und Bildungsniveaus müssen unterschiedliche Kulturen innerhalb der Bundeswehr berücksichtigt werden. So z. B. können IT-Security-Awareness-Maßnahmen und inhalte für Verwaltungsmitarbeiter nicht 1:1 auf Kampftruppen übertragen werden.

4.3.3 Prozesssicht

Dienststellen können zu jeder Zeit eine Awareness-Kampagne auf Grundlage der Vorschrift A-960/1 initiieren. Der PIA-Kampagnenfahrplan gibt den Dienststellen einen Anhalt für den Ablauf, der die einzelnen Phasen von Vorbereitung, Durchführung und Nachbereitung einer Awareness-Kampagne in Form einer Checkliste aufgeführt. Neben der Checkliste enthält der PIA-Kampagnenfahrplan weitere Hinweise und Tipps für eine erfolgreiche Sensibilisierung unter Berücksichtigung der einzelnen Tools des Werkzeugkastens, wie bspw. Poster und Newsletter. Somit garantiert der PIA-Kampagnenfahrplan ein gewisses Maß an Standardisierung, lässt den Dienststellen aber zeitgleich genügend Spielraum, eine standort-eigene Awareness-Kampagne zu gestalten, die genau auf die Bedürfnisse des Personals und die Risiken vor Ort zugeschnitten ist.

Innerhalb einer Awareness-Kampagne einer Dienststelle initiiert der IT-SiBeDSt meist eine Awareness-Veranstaltung, die wenige Stunden bis zu einen Tag in Anspruch nimmt. In der Regel sind diese Awareness-Veranstaltungen mit Vorträgen ausgestaltet, in denen der Dienststellenleiter sowie der IT-SiBeDSt über die aktuelle Bedrohungslage in der IT-Sicherheit referieren. Abgerundet werden die Vorträge meist mit Live-Hackings, die entweder durch das IT-Fachpersonal vor Ort oder durch externe Referenten durchgeführt werden.

Sofern externe Referenten in die Awareness-Veranstaltung integriert sind, müssen die Dienststellen Haushaltsmittel aus dem Haushaltstitel der Dienststelle beantragen bzw. bereitstellen.

Eine Kennzahlenermittlung und Qualitätssicherung zur Messung von Awareness wurde zum Zeitpunkt der Erstellung der Fallstudie noch nicht praktiziert. Jeder Durchführende ist zu einem Feedback seiner Veranstaltung an KdoCIR InfoSecAwareness angehalten.

Neben den Awareness-Veranstaltungen einzelner Dienststellen findet jährlich der IT-Security-Awareness-Tag der Bundeswehr statt, an dem IT-Sicherheitsbeauftragte und Führungskräfte aller Dienststellen teilnehmen können. Dieses Event dient neben der Möglichkeit des Networkings auch der Präsentation aktueller und neuer Tools des Werkzeugkastens sowie der Weiterbildung. So wurde z. B. auf dem IT-Security-Awareness-Tag der Bundeswehr 2017 ein spielerisches Format zur Awareness-Steigerung für IT-Fachpersonal durch Dr. Andreas Rieb [6] sowie die Ergebnisse der Monitorumfrage des Forschungsprojekts *Vernetzte IT-Sicherheit Kritischer Infrastrukturen* (VeSiKi) durch Prof. Dr. Ulrike Lechner präsentiert [7].

Die Inhalte für die jährlich stattfindenden IT-Security-Awareness-Tage der Bundeswehr sowie die Konspiration neuer Ideen zur Sensibilisierung werden in den quartalsweise stattfindenden Arbeitsgruppentreffen besprochen, an denen die Mitglieder der Arbeitsgruppe teilnehmen. Die Anstöße kommen dabei aus den querschnittlichen Erfahrungen der AG-Mitglieder und aus dem Feedback der IT-SiBeDSt. Zudem orientiert man sich an den Bedrohungslagen und Meldungen aus dem BSI und statistischen Meldungen zum eigenen Incident Response. Als Verbreitungsmedium für neue Tools, Erkenntnisse und übergreifende Veranstaltungen werden die Kanäle des Intranets (Ausbildungsforum, ConnectBw, WikiBw, E-Mail, Intranetseite) verwendet, auf die bei anderen Veranstaltungen hingewiesen wird.

4.3.4 Anwendungssicht

Der Werkzeugkasten adressiert primär die IT-Sicherheitsbeauftragten der Dienststellen, die gemäß der Vorschrift die IT-Security-Awareness in ihren Dienststellen aufrechterhalten oder gar verbessern sollen. Die Ziele, die in den einzelnen Dienststellen im Rahmen der IT-Security-Awareness verfolgt werden, obliegen dem IT-SiBeDst in enger Zusammenarbeit mit dem Dienststellenleiter. Je nachdem, welches Ziel verfolgt wird, kann sich der IT-SiBeDst die entsprechenden Tools auf der Website im Intranet herunterladen und einsetzen. Dazu zählen exemplarisch, Informationsschriften, Plakate (siehe Abbildung 4-2) und Aufsteller, Flyer, Filme, Kalender, Give Aways, Quiz, Feedbackbögen, Visitenkarten u. a. Materialien.

Inhaltlich richten sich die Botschaften der oben aufgeführten Tools vorrangig an IT-Nutzer und erfüllen unterschiedliche Einsatzzwecke: So sollen z. B. die Visitenkarten, die

Abbildung 4-2: Poster zum Thema Malwareprävention; Quelle: Bundeswehr

vom IT-SiBeDst in nicht-abgesperrten Büros verteilt werden können, die Sichtbarkeit der Awareness-Kampagne erhöhen und auf die Bedrohungssituation hinweisen. Materialien, wie Informationsschriften, sollen themenspezifisch Wissen über gängige Angriffsmethoden, allgemeine Schutzmaßnahmen, aber auch Bundeswehr-interne Richtlinien vermitteln. Filme sollen neben einer Verbesserung der Risikowahrnehmung und Wissensvermittlung zusätzlich eine Verhaltensänderung initiieren.

Im Hinblick auf die verschiedenen Tools und die damit einhergehenden Ziele hat die AG SecAw neben den o. g. Materialien einen PIA-Kampagnenfahrplan entwickelt. In Form einer Checkliste mit weiterführenden Informationen unterstützt der Fahrplan IT-SiBes sowohl in der Planung als auch in der Durchführung von IT-Security-Awareness-Kampagnen und im Einsatz einzelner Maßnahmen (siehe Abbildung 4-3).

Ungeachtet der Form einer Checkliste ist der PIA-Kampagnenfahrplan kein Instrument, um eine einheitliche Awareness-Veranstaltung in allen Dienststellen sicherzustellen. Er ist lediglich als Hilfestellung und Inspiration zu sehen und bietet IT-SiBes ferner die Möglichkeit, auch Tools und Maßnahmen in ihre Kampagne zu integrieren, die über die bereitgestellten

Tools des Werkzeugkastens hinausgehen. So wurde z. B. in einigen Dienststellen ein Planspiel zum Thema IT-Sicherheit als Instrument zur Verbesserung der Awareness für IT-Fachpersonal in einer Awareness-Kampagne integriert (siehe [6]).

Abbildung 4-3: Auszug aus dem PIA-Kampagnenfahrplan; Quelle: Bundeswehr

Abbildung 4-4: Planspiel zur IT-Sicherheit; Quelle: [8]

Der Dreiklang der unterschiedlichen Zieldimensionen der Materialien des PIA-Werkzeugkastens steht somit im Einklang mit der wissenschaftlichen Untersuchung nach Hansch und Benenson [8], die in einer Literaturübersicht den Begriff der IT-Security-Awareness nach folgenden drei Dimensionen klassifizieren: *Perception* mit der Fähigkeit, *to recognize threats*, *Protection* mit der Fähigkeit, *to know solutions,* sowie *Behavior* mit der Fähigkeit, *to act right*.

4.3.5 Technische Sicht

Der im Intranet der Bundeswehr bereitgestellte Werkzeugkasten enthält kein Tracking der Besucher und keinen Counter, der feststellt, wie oft ein Produkt heruntergeladen wurde.

Sofern bei einer Awareness-Veranstaltung in einer Dienststelle ein Live-Hacking durchgeführt wird, muss die IT-Infrastruktur für die Präsentation entsprechend vorbereitet werden. Es ist zu erwähnen, dass ein solches Live-Hacking keine Form des Penetrationtestings darstellt. Live-Hacking im Kontext eines Awareness-Vortrags findet immer auf autarken – nicht mit der Produktivumgebung verbundenen – IT-Systemen statt, die für die Darstellung der Angriffsvektoren entsprechend vorbereitet sind.

In den seltensten Fällen wird das Live-Hacking vom IT-SiBeDSt selbst durchgeführt, sondern typischerweise von externen Referenten, die sich auf solche Vorträge spezialisiert haben. Je nach Wunsch und Bedarf der Dienststelle werden in den Live-Hacking-Vorträgen unterschiedliche Angriffsvektoren vorgestellt, z. B.:

- Social Engineering
- Webserverattacken durch Code-Injections
- Kompromittierung eines Win7-Systems durch einen USB-Stick mit einem automatischen Download von Software
- Man-in-the-Middle zum Abfangen von Passwörtern in https-Verbindungen
- Ransomware
- Wiederherstellung gelöschter Dateien

Für die technische Umsetzung zur Demonstration der Angriffsvektoren werden i. d. R. virtuelle Betriebssysteme eingesetzt, die von den (externen) Referenten administriert und zur Awareness-Veranstaltung mitgebracht werden.

4.3.6 Umfang und Zeitraum

IT-Security-Awareness ist ein fortlaufender Prozess auf verschiedenen Ebenen, an dem über die Arbeitsgruppe hinaus noch weitere Instanzen beteiligt sind. Hierzu zählt die Erarbeitung von strategischen Zielvorgaben der Leitung BMVg (siehe Strategische Leitlinie Cyberverteidigung[5] [9]), die Anpassung an die Vorschriftenlandschaft der Bundeswehr (A-960/1) sowie übergreifende Weisungen zur IT-Sicherheit. Aufgrund der Matrixorganisation der Arbeitsgruppe gehen die Personalkosten in anderen Bereichen auf. Kosten, wie Infrastruktur und

5 Die Strategische Leitlinie wurde mit Billigung von BMVg Referatsleiter CIT I 1 am 10.04.2017 auf OFFEN (nicht öffentlich) heruntergestuft und liegt vor.

materielle Ausstattung, sind bestehende Betriebskosten der Dienststellen. Eine Betrachtung der Wirkung und des Mitteleinsatzes wird zwar angenommen, aber nicht im betriebswirtschaftlichen Sinne eines Mittelrückflusses angestrebt.

4.3.7 Vorgehen und Umsetzung

Der Projektplan der Arbeitsgruppe sieht jährliche Meilensteine vor. Die Leitung der Arbeitsgruppe steuert die Arbeitstreffen und fasst Ergebnisse zusammen. Die Ansätze der Vorgehensweise waren anfangs nach dem Big-Bang-Modell aufgestellt. Das bedeutet, dass ein Arbeitsergebnis in Form eines Tools erst vollständig ausgearbeitet und in einem endgültigen Zustand zur Veröffentlichung, z. B. beim Awareness-Tag der Bundeswehr, freigegeben wurde. Durch ein neues Tool im Werkzeugkasten sollte das Interesse der Nutzer „auf einen Schlag" geweckt werden. Aufgrund der beschränkten Ressourcen der AG konnten teilweise Ergebnisse nicht zu den gewünschten Terminen fertiggestellt werden. Zum Zeitpunkt der Erstellung der Fallstudie wird ein an Scrum angelehntes Verfahren für das Projektmanagement verwendet. Der Product Owner ist nun das KdoCIR und priorisiert eine Liste mit den Anforderungen für die Awareness im Geschäftsbereich des BMVg. Operativ wird in Zukunft das ZCSBw die Arbeitsgruppe koordinieren. Dadurch kann sich die Arbeitsgruppe, die in gleicher Zusammensetzung bestehen bleibt, auf den Kern ihrer Arbeit konzentrieren. Dies bietet nun die Möglichkeit, sich schneller an Situationen oder Vorgaben der Leitung anzupassen und ad hoc Arbeitstreffen zu bilden.

Im Laufe der Jahre wurde dadurch die IT-Security Awareness als fester Bestandteil in der Vorschriftenlage etabliert, sodass auch in der Struktur des KdoCIR Dienstposten und feste Stellen für die Sensibilisierung geschaffen wurden. An der Organisation und Struktur der Arbeitsgruppe hat sich durch die Umstrukturierung nichts geändert. Wie bisher können Interessierte aus allen Bereichen ihr Wissen der Bundeswehr bereitstellen und sich in der Arbeitsgruppe engagieren. Neue Mitglieder werden meist über Mund-zu-Mund-Propaganda sowie Vorträge innerhalb der Bundeswehr, in denen die Ergebnisse der Arbeitsgruppe und die Gruppe selbst vorgestellt werden, akquiriert.

4.3.8 Projektergebnis

Die Bundeswehr hat mit der PIA-Kampagne ein sichtbares Zeichen für IT-Sicherheit in der Organisation im In- und Ausland setzen können. Sensibilisierte Mitarbeiter sind für die IT-Sicherheit in der Bundeswehr ebenso wichtig wie technische Schutzmaßnahmen – dieses Bewusstsein für den menschlichen Faktor will die IT-Security-Awareness-Kampagne schaffen. Der Werkzeugkasten, den die Arbeitsgruppe über mehrere Jahre unter ständiger Rücksprache mit der Zielgruppe – den IT-SiBeDst – entwickelt und zusammengestellt hat, bietet IT-SiBeDst hilfreiche Tools, mit denen das Thema IT-Sicherheit den Soldaten und zivilen Mitarbeitern der Bundeswehr zeitgemäß präsentiert werden kann.

Exemplarisch sind hier noch einmal folgende Tools des Werkzeugkastens hervorzuheben: die Erstellung eines eigenen Films und Printprodukte für die Sensibilisierung sowie der PIA-Kampagnenfahrplan für die Durchführung von Veranstaltungen. Des Weiteren hat die

Arbeitsgruppe das Drehbuch für den Awareness-Anteil des Online-Cyber-Hygiene-Check-Ups entworfen und beigesteuert.

Fornefeld und Opper geben an, dass die Resonanz zu den einzelnen Materialien sehr unterschiedlich ist und geben als wichtigen Einflussfaktoren die Unternehmenskultur sowie Alter und Vorkenntnisse der Ausbildungsgruppe an. „Was in der einen Ausbildungsgruppe akzeptiert wird und gut funktioniert, kann in einer ähnlichen Gruppe abgelehnt werden." Unabhängig von der Qualität einzelner Awareness-Maßnahmen oder der ganzen Kampagne werden in der Bundeswehr über die einzelnen Dienststellen hinaus keine Ergebnisse veröffentlicht. Die Ergebnisse werden lediglich für die interne Revision genutzt, da die Dienststellen nicht einem Vergleich ausgesetzt werden sollen.

Über die Laufzeit der Kampagne hat die IT-Sicherheit und im Speziellen der Faktor Mensch als Risiko der IT-Sicherheit zunehmend an Bedeutung gewonnen. Dienststellenleiter erkennen zunehmend die Notwendigkeit dieser Thematik und initiieren in enger Zusammenarbeit mit ihren IT-Sicherheitsbeauftragten IT-Security-Awareness-Kampagnen oder vereinzelte Maßnahmen. Durch die Rückmeldungen von Teilnehmern und Durchführenden aus den einzelnen Dienststellen konnte die Arbeitsgruppe feststellen, dass die Akzeptanz der IT-Sicherheit – vor allem auf den Führungsebenen – gestiegen ist. Dieser Akzeptanzgewinn ist besonders wichtig. Denn gerade eine fehlende Vorbildfunktion von Führungskräften hinsichtlich IT-Sicherheit war bis zum Beginn des Projekts eine besondere Hürde, die es zu nehmen galt.

4.4 Erfolgsfaktoren

Die PIA-Kampagne mit dem Key Visual des Netzwerksteckers ist in der Bundeswehr sowohl im Inland als auch im Ausland ein sichtbares Symbol für IT-Sicherheit mit einem hohen Wiedererkennungswert.

IT-Sicherheit wird in der PIA-Kampagne im Werkzeugkasten durch vielseitige Tools und Maßnahmen präsentiert und in den Dienststellen angewendet. Der PIA-Kampagnenfahrplan unterstützt Dienststellen dabei, schnell und wirksam IT-Security für den „Human Factor" herzustellen.

Die AG IT-SecAwBw war zum Zeitpunkt der Erstellung der Fallstudie bereits mehrere Jahre aktiv. Für den Erfolg der Arbeitsgruppe sind sowohl ein langer Atem als auch die Unterstützung durch das Top-Management der Bundeswehr ausschlaggebend. Ebenso hat sich die Matrixorganisation der Arbeitsgruppe bewährt. So ist es der großen Flexibilität und den innovativen Ansätzen geschuldet, dass trotz der Größe und hierarchischen Prägung der Bundeswehr Ideen und Werkzeuge entwickelt werden können. Das Wissen über die unterschiedlichen Zielgruppen und Kulturen innerhalb der Bundeswehr sowie die Vielseitigkeit der Arbeitsgruppe durch die Mitglieder waren und sind für die Mission, IT-Sicherheit für die Soldaten und zivilen Mitarbeiter der Bundeswehr zu schaffen, sehr gewinnbringend.

Zu guter Letzt ist als Erfolgsfaktor das hohe Engagement der Arbeitsgruppe zu nennen. Denn ursprünglich wurde die Arbeitsgruppe aus intrinsischer Motivation weniger Personen gegründet, die IT-Security-Awareness als wesentlichen Schlüssel für ganzheitliche IT-Sicher-

heit erkannt haben. Aus dieser Bewegung und Arbeit über das eigentliche Dienstgeschäft hinaus konnten im Laufe der Zeit immer mehr Freiwillige gewonnen werden, die sich für IT-Security-Awareness in der Bundeswehr engagieren.

Mit Aufstellung des KdoCIR und der Neuorganisation der IT-Sicherheit in der Bundeswehr wurde die IT-Sicherheit zur Informationssicherheit (engl. „Information Security“) erweitert. Diesem Schritt wird auch die AG IT-Security-Awareness folgen und ab dem 01.01.2018 unter dem neuen Namen **AG InfoSec Awareness** firmieren. Der jährlich Anfang Juli am Bildungszentrum der Bundeswehr (BiZBw) in Mannheim stattfindende IT-Security-Awareness-Tag der Bundeswehr wird somit ab 2018 zum **InfoSec Awareness-Tag der Bundeswehr**.

4.5 Danksagung

Wir danken dem Bundesministerium für Bildung und Forschung (BMBF) für die Möglichkeit der Forschung im Rahmen des Projektes VeSiKi, Förderkennzeichen 16KIS0213K.

4.6 Literaturverzeichnis

[1] NATO 2017. Cyber defence. Verfügbar unter: https://www.nato.int/cps/en/natohq/topics_78170.htm [zugegriffen: 30-Nov-2017].

[2] BSI, 2014. IT-Grundschutz: B 1.13 Sensibilisierung und Schulung zur Informationssicherheit, Bundesamt für Sicherheit in der Informationstechnik. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b01/b01013.html [zugegriffen: 23-Aug-2016].

[3] BSI, 2016. IT-Grundschutz: ORP.3 Sensibilisierung und Schulung, IT-Grundschutz. BSI, Bonn.

[4] BSI, 2013. IT-Grundschutz – M 3.44 Sensibilisierung des Managements für Informationssicherheit, 2013. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m03/m03044.html?nn=6604926 [zugegriffen: 27-Nov-2017].

[5] BMV, 2016. Zentrale Dienstvorschrift A-960/1: IT-Sicherheit in der Bundeswehr, S. 1–269.

[6] A. Rieb; U. Lechner, 2016. Towards a Cybersecurity Game: Operation Digital Chameleon, in: Conference proceedings CRITIS 2016, S. 283–295.

[7] VeSiKi, 2017. Monitor IT-Sicherheit Kritischer Infrastrukturen, 1. Auflage. Neubiberg: Universität der Bundeswehr München.

[8] N. Hansch; Z. Benenson, 2014. Specifying IT security awareness, in: *P*roceedings – International Workshop on Database and Expert Systems Applications, DEXA, S. 326–330.

[9] Bundesregierung, 2015. Krieg im „Cyber-Raum“ – offensive und defensive Cyberstrategie des Bundesministeriums der Verteidigung (Drucksache 18/6989). Bundesregierung.

5 genua gmbh: Fernwartung Kritischer Infrastrukturen

Andreas Rieb, Universität der Bundeswehr München

Die vorliegende Fallstudie beschreibt Risiken, die auf den Verzicht oder mangelhafte Implementierung von Fernwartungslösungen zurückzuführen sind. Darauf basierend werden Chancen und Vorteile erörtert, die durch eine hochwertige Implementierung einer Fernwartungslösung genutzt werden können. Diese Ansätze werden anhand der Dienstleistungen und Produkte der Firma genua beschrieben. Darüber hinaus werden mögliche Implementierungen behandelt und diese aus unterschiedlichen Perspektiven unter Berücksichtigung aller involvierten Parteien betrachtet.

Keywords: Fernwartung, Fernadministration, Remote-Access

5.1 Unternehmen

5.1.1 Unternehmensprofil

Die genua gmbh (kurz genua) wurde 1992 gegründet und ist ein deutscher Anbieter für IT-Sicherheitslösungen. genua ist seit 2015 ein Unternehmen der Bundesdruckerei-Gruppe und zählt ca. 250 Mitarbeiter an vier Standorten (Berlin, Köln, Stuttgart, Kirchheim bei München [Hauptsitz]).

genua will „hochwertige Lösungen entwickeln, um bei unseren Kunden für zuverlässige IT-Sicherheit zu sorgen“ [1]. Das Portfolio an IT-Sicherheitslösungen von genua reicht von Lösungen für Netzwerk-Sicherheit, wie Datendioden und Firewalls, bis hin zu Lösungen zur Absicherung von Automatisierung, Industrial Monitoring oder auch der Fernwartung von Maschinen und IT-Systemen. genua legt besonderen Wert darauf, dass alle Lösungen in Deutschland entwickelt, produziert und auf hohe Sicherheitsanforderungen, wie z. B. die des Bundesamts für Sicherheit in der Informationstechnik (BSI), hin ausgerichtet sind. Zahlreiche Zertifikate sowie Zulassungen für den Geheimschutzbereich sind besonders für Kunden mit hohen Sicherheitsanforderungen aus Industrie und Öffentlicher Verwaltung ein wesentliches Kriterium der IT-Sicherheitslösungen von genua.

5.1.2 Strategische Ausrichtung

Die Vision von genua ist es, auch in Zukunft hochwertige Lösungen zu entwickeln, um sowohl bei nationalen als auch bei internationalen Kunden für zuverlässige IT-Sicherheit zu sorgen. Aus diesem Grund legt genua großen Wert auf Innovationsfähigkeit: „Um richtig gute Lösungen zu finden, ist es häufig sinnvoll, verschiedene Kompetenzen, Sichtweisen und Ressourcen zu bündeln“ [2]. Aus dieser Überzeugung heraus arbeitet genua eng mit Universitäten, Forschungsinstituten und anderen Unternehmen zusammen, um gemeinsam grundlegende Probleme der IT-Sicherheit zu lösen.

Im Marktsegment von genua gibt es nur wenige Anbieter und die Auswahl der Anbieter gerade für den öffentlichen Bereich ist strikt geregelt. So verzeichnet genua ca. 60 %

der Kunden aus dem öffentlichen Bereich und 40 % der Kunden aus der Privatwirtschaft. Die Privatwirtschaft präferiert günstigere Anbieter und hat weniger Auflagen hinsichtlich etwaiger Zulassungsbestimmungen einzusetzender Lösungen. Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) erhöht die Anforderungen an IT-Sicherheit in der Privatwirtschaft, speziell für die als Kritische Infrastruktur (KRITIS) eingestuften Unternehmen. Strategisch gesehen soll sich das Verhältnis zwischen dem öffentlichen Bereich und der Privatwirtschaft auf ein ausgeglichenes Verhältnis von 50:50 einpendeln.

5.1.3 Fallstudienpartner

Name	Position im Unternehmen
Andreas Leinfelder	Public Sales (PSA) innere und äußere Sicherheit, genua
Hans Hein	Leiter Enterprise Solutions und Fernwartungsspezialist, genua
Andreas Rieb	Wissenschaftlicher Mitarbeiter, Universität der Bundeswehr München

5.2 Kritische Infrastruktur

5.2.1 Einordnung als KRITIS

Als IT-Dienstleister ist genua selbst keine Kritische Infrastruktur gemäß dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) und der ersten KRITIS-Verordnung. Das Leistungsspektrum von genua beinhaltet die Absicherung sensibler Schnittstellen von Behörden und Industrie bis hin zur Vernetzung Kritischer Infrastrukturen. Die Lösungen von genua werden in mehreren Sektoren Kritischer Infrastrukturen, wie z. B. Energie, Gesundheit, Ernährung, Staat und Verwaltung, eingesetzt. So realisierte genua z. B. sichere Fernwartungslösungen zur Steuerung der Gebäudetechnik bei staatlichen Kunden oder sichere Netztrennung zwischen zwei Konzernbereichen.

5.2.2 Risikoanalyse

Nach Ansicht des BSI sind Systeme zur Prozesssteuerung, Fertigung und Automatisierung, die häufig im Bereich der Kritischen Infrastrukturen Anwendung finden, ähnlichen Bedrohungen ausgesetzt wie konventionelle IT-Systeme [3]. Erschwerend kommt hinzu, dass diese Maschinen, Anlagen und IT-Systeme (im Laufe der Fallstudie allgemein als Wartungsobjekte bezeichnet) z. T. bereits Fernwartungsmöglichkeiten implementiert haben. Damit sind Informationen über den Zustand der Anlage jederzeit abrufbar und Fernzugriffe durch den Hersteller grundsätzlich jederzeit möglich. Aus betrieblichen oder wirtschaftlichen Gründen muss hier das IT-Netzwerk des Betreibers gegenüber dem Hersteller teilweise geöffnet werden, was wiederum zu einem Anstieg der Bedrohungen führen kann [3].

Fernwartung birgt aus Sicht der IT-Sicherheit Risiken, jedoch ist ohne Fernwartung in der heutigen Zeit nicht mehr auszukommen: Wartungsaufgaben müssen gemacht werden. Ein kompletter Verzicht oder gar ein Verbot seitens des Managements hinsichtlich Fernwartung

ist erfahrungsgemäß kontraproduktiv. Es muss angenommen werden, dass sich Techniker oder IT-Fachleute, die z. B. für das reibungslose Funktionieren des Wartungsobjekts verantwortlich sind, einen (geheimen) Weg suchen, das Wartungsobjekt über die Ferne dauerhaft oder temporär anzubinden. Das begünstigt Wildwuchs in der IT-Landschaft einer Organisation und ein trügerisches Gefühl der IT-Sicherheit.

Ein weiteres Risiko stellt die Unkenntnis vieler Betreiber Kritischer Infrastrukturen hinsichtlich ihrer eingesetzten Wartungsobjekte und der darin verbauten Komponenten dar. So gibt es z. B. Wartungsobjekte, die vonseiten des Herstellers ein GSM-Modem integriert haben, das für die notwendigen Aktionen wie Störungsbeseitigung oder Einspielen von Updates eine Fernwartungsverbindung zum Hersteller aufbaut. Damit entsteht ein weiterer Zugang zu einem Wartungsobjekt und dem Netzwerk, der am zentralen Netzwerkübergang in Richtung Internet vorbeigeht. Betrachtet man diesen Aspekt für Kritische Infrastrukturen in realistischen, größeren Dimensionen und über einen längeren Zeitraum hinweg, muss davon ausgegangen werden, dass eine Vielzahl unkontrollierter Netzwerkzugänge zum Internet entstehen kann. Dieses Risiko wird verschärft, wenn diese Netzwerkzugänge unzureichend oder gar nicht dokumentiert und geregelt werden. Man muss die Möglichkeit bedenken, dass der Hersteller eines Wartungsobjekts bei einem Fernwartungsvorgang ungenügend oder gar nicht authentisiert wird. Das bedingt das Risiko, dass Fernwartungszugänge durch Angreifer abgehört oder gar übernommen werden. Implementierungs- und Konfigurationsfehler im Wartungsobjekt, im Netzwerk oder der Firewall können so das Risiko eines Zugriff auf andere Assets in anderen Bereiche des Netzwerkes (z. B. in das Netzwerk der Office-IT oder andere Anlagen) erhöhen.

Bei einer Umstellung von „lokaler" Wartung auf Fernwartung – einem Thema für viele Unternehmen von Kritischen Infrastrukturen – entfallen die herkömmlichen Sicherheitsmechanismen. Eine „lokale" Wartung durch einen externen Mitarbeiter kann durch einen (eigenen) Mitarbeiter der Organisation überwacht werden – ganz gleich, ob er die auszuführenden Wartungsarbeiten kognitiv nachvollziehen kann oder nicht. Dieses Gefühl der Sicherheit wird psychologisch verstärkt, wenn der Wartungsmitarbeiter bereits bekannt ist „und man sich kennt". Der Wegfall dieser bekannten und bewährten Sicherheitsmechanismen stellt eine erhebliche Anforderung an eine Fernwartungslösung dar: Alle Arbeiten müssen nachvollziehbar sein und gegebenenfalls überwacht werden können.

In der Zukunft werden Themen wie „Netztrennung" im Rahmen von Szenarien wie Industrie 4.0 zunehmend an Bedeutung gewinnen. Eine sichere Lösung wäre an dieser Stelle eine Separierung der unterschiedlichen Netzwerke. Häufig sind sowohl Office- als auch Produktionsnetze historisch gewachsen und Netzsegmente eng miteinander gekoppelt. Eine Separierung würde einen erheblichen Eingriff in die IT-Infrastruktur bedeuten und ist nicht immer die bevorzugte Wahl des Kunden. Eine praktikable Lösung kann vorsehen, die Netzübergänge zu sichern, Netzwerkbereiche, wie z. B. Industrieanlagen mit ihren veralteten Betriebssystemen wie Windows XP abzusichern und darüber hinaus eine sichere Möglichkeit zu schaffen, eine Netzwerkanbindung zum Hersteller für Wartungszwecke zu gewährleisten.

5.2.3 Chancenanalyse

Sofern Fernwartung sicher umgesetzt wird, kann sie für Betreiber Kritischer Infrastrukturen Chancen und Vorteile bieten. Die bewusste und kontrollierte Öffnung des Perimeters für Fernwartungszwecke verhindert die heimliche Installation und Implementierung alternativer Zugänge. Eine gut realisierte Fernwartung trägt zur Kontrolle und Transparenz bei und reduziert Kosten. Die Reduktion von Kosten ist vor allem dann relevant, wenn der Zugang nicht nur für Fernwartungszwecke, sondern auch zur Optimierung der Einstellungen oder für das Monitoring von Verschleißteilen eingesetzt wird. Ein rechtzeitiges Versenden von Ersatzteilen – gerade in geografisch schwer zugänglichen Gebieten – senkt potenziell drastisch die Ausfallzeiten von Wartungsobjekten.

Ein weiterer Vorteil von sicher umgesetzter Fernwartung betrifft primär den öffentlichen Bereich mit einer potenziell hohen Fluktuation der Mitarbeiter, z. B. durch Versetzungen. Eine lokale Wartung durch speziell ausgebildete eigene Mitarbeiter bringt nur so lange IT-Sicherheit, wie diese vor Ort sind. Da jedoch häufig nur eine geringe Einarbeitungszeit für Nachfolger eingeräumt wird oder keine rechtzeitige Nachbesetzung möglich ist, geht viel Wissen verloren – zulasten der IT-Sicherheit.

Fernwartung ist ein wichtiges Instrument, über das die Hersteller der Wartungsobjekte Support leisten und das neue Servicemöglichkeiten und neue Geschäftsmodelle für die Hersteller der Wartungsobjekte unterstützt. Eine sichere Umsetzung von Fernwartung ist Voraussetzung – gerade im Hinblick auf neue Szenarien im Bereich der Industrie 4.0 genau wie für Kritische Infrastrukturen.

5.3 Projekt

Während für Office-IT in der Regel internationale Dienstleister die Software – zum Teil auch herstellerübergreifend – verwalten und Sicherheitsupdates einspielen, gibt es im Industriebereich solche Dienstleister (noch) nicht. Hier ist es die Aufgabe des Herstellers, einerseits die Wartungsdienste in festgelegten Wartungsfenstern durchzuführen und andererseits die Wartungsobjekte ggf. auch zu modifizieren und zu optimieren. Besteht zudem das Wartungsobjekt aus Komponenten unterschiedlicher Hersteller bzw. Zulieferer, muss auch diesen Parteien die Möglichkeit eingeräumt werden, auf das Wartungsobjekt oder lediglich auf Komponenten des Wartungsobjekts zugreifen zu können. Die Anbindung der Wartungsobjekte mit all ihren Sicherheitskomponenten an das Internet stellt an dieser Stelle ein „Vehikel" dar – eine Voraussetzung für die vielfältigen Supportbeziehungen zwischen Herstellern und Zulieferern einerseits und Betreibern andererseits.

Eine sichere Umsetzung einer Fernwartungslösung ist nicht nur aus technischer, sondern auch aus organisatorischer und vertragsrechtlicher Perspektive eine umfangreiche Aufgabe.

5.3.1 Projektziel

In einem Projekt zur Realisierung einer sicheren Fernwartungslösung haben die Kunden, also die Betreiber, sehr unterschiedliche Zielvorstellungen: So soll exemplarisch „Wildwuchs"

verhindert werden, der entstehen kann, wenn z. B. Fernwartung nicht von der Organisation unterstützt wird, sich die IT-Mitarbeiter jedoch „geheime“ Lösungen einfallen lassen oder wenn Fernwartung prinzipiell erlaubt ist, aber nicht an zentraler Stelle geregelt, dokumentiert und überwacht wird. Potenzielle Schwachstellen beinhalten nicht-dokumentierte IT-Sicherheitseinstellungen, wie z. B. offene Ports an der Firewall, zu freizügig eingerichtete Rechte oder falsch definierte Rollen. Die bewusste Öffnung der IT-Infrastruktur für das Internet mit der Möglichkeit der Fernwartung sehen viele Betreiber an dieser Stelle als eine transparente, zentralisierte und sichere Option, die Funktionsfähigkeit der Wartungsobjekte zu gewährleisten. Ein weiteres Ziel von Kunden kann es sein, Fernwartung erstmalig zu etablieren. Die Gründe hierfür können vielfältig sein, z. B. weil Wartungsarbeiten bisher lediglich lokal durchgeführt wurden oder weil Wartungsobjekte in geografisch schwer erreichbaren Regionen der Welt installiert werden sollen.

5.3.2 Geschäftssicht

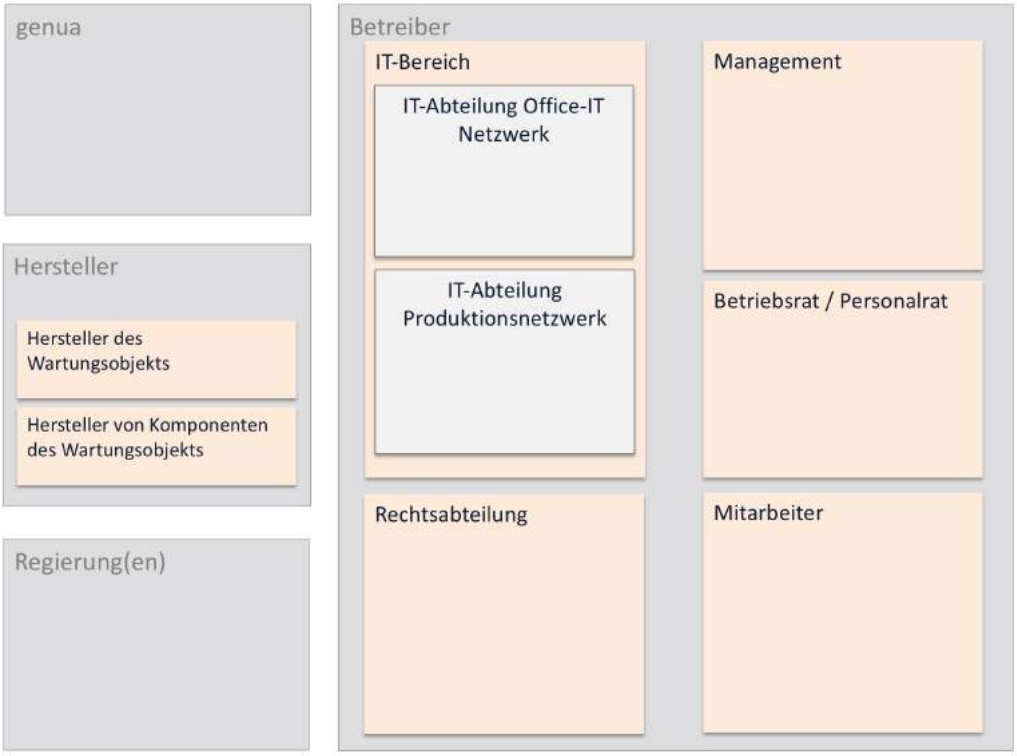


Abbildung 5-1: Geschäftssicht

Wie in Abbildung 5-1 zu sehen, sind aus Geschäftssicht mehrere Parteien in die Realisierung einer sicheren Fernwartungslösung involviert.

Das Management muss die finanziellen Mittel bereitstellen und die strategische Ausrichtung der Organisation vorgeben. Denn ein Fernwartungsprojekt kann einen Schritt in

Richtung Industrie 4.0 oder Smart Factories darstellen. Aus organisatorischer Sicht müssen Aufgabengebiete und Verantwortlichkeiten neu strukturiert werden. Dies ist z. B. der Fall, wenn es separate, autarke IT- und IT-Sicherheitsabteilungen gibt und diese z. B. bei einer Anbindung des Produktionsnetzwerks an das Office-IT-Netzwerk zur Nutzung des Internetzugangs des Office-IT-Netzwerks Rechte für den Zugriff auf die Firewall am Netzwerkübergang neu regeln und untereinander abstimmen müssen. Themen aus organisatorischer Sicht sind Kompetenzstreitigkeiten, Machtverluste, Stellenstreichungen durch Zusammenführung von IT-Abteilungen und Kompetenzstreitigkeiten.

Die Rechtsabteilung bzw. der Datenschutzbeauftragte kann in einem Fernwartungsprojekt zusätzlich involviert sein. Werden z. B. auf dem Wartungsobjekt, wie einer medizinischen Anlage, personenbezogene Daten verarbeitet, achten interne Rechtsabteilungen bzw. Datenschutzbeauftragte auf eine datenschutzkonforme Lösung. Seitens der Rechtsabteilung sind im Vorfeld des Projekts weitere Fragen zu klären: Wer haftet, wenn bei einer Fernwartung über eine VPN-Verbindung Probleme oder Fehler auftreten? Welche Regelungen sind anwendbar, wenn ein Hersteller aus einem anderen Land ein Wartungsobjekt fernwartet? Die Zulässigkeit von Verschlüsselungsverfahren sowie Import bzw. Export von Kryptografie sind in vielen Ländern, wie z. B. Ägypten, gesetzlich streng geregelt. An dieser Stelle bedarf es häufig Einzelfallprüfungen staatlicher Stellen. Es müssen außerdem Vereinbarungen über IT-Sicherheitsanforderungen an den Fernwarter und seine IT getroffen werden.

Fernwartung ist die Grundlage dafür, dass die Hersteller der Wartungsobjekte Support leisten können. Aus Geschäftssicht bedeutet das, dass genua mit dem Kunden gemeinsam die Fernwartungslösung in die vorhandene IT-Infrastruktur integriert. Der Hersteller des Wartungsobjekts – als weitere Partei in der Geschäftssicht – nutzt die technische Lösung eines IT-Dienstleisters, um auf die Wartungsobjekte remote zugreifen zu können. Je nach Konfiguration können unterschiedliche Verfahren zum Aufbau einer Fernwartungsverbindung zum Einsatz kommen. Es muss auf Herstellerseite geregelt werden, wie etwaige Zulieferer wartungsbedürftiger Komponenten die Fernwartungsleitung mitnutzen können.

Auf der Seite des Betreibers und somit am anderen Ende der Fernwartungsleitung stehen die Mitarbeiter, die für die Wartungsobjekte lokal verantwortlich sind und gegebenenfalls eine spezielle Schulung oder Einweisung benötigen. Wenn die Mitarbeiter des Betreibers die Fernwartungslösung nutzen, um remote (z. B. aus dem Home Office) das Wartungsobjekt zu administrieren, müssen Betriebsrat oder Personalrat involviert werden. Der Grund dafür ist, dass zwar eine lückenlose Aufzeichnung der Fernwartungsarbeiten durch den Hersteller u. a. Vorteile hinsichtlich Haftungsfragen bringt, aber diese Aufzeichnungen für hauseigene Mitarbeiter eine Überwachung möglich macht. Dieser Interessenkonflikt muss somit vom Betriebs- oder Personalrat im Vorfeld geregelt werden.

5.3.3 Prozesssicht

Die Implementierung einer sicheren Fernwartungslösung durch genua wird in Abbildung 5-2 dargestellt. In der vorliegenden Variante wird der Rendezvous-Server über eine genubox realisiert und befindet sich in der Demilitarisierten Zone hinter einer Firewall auf Herstel-

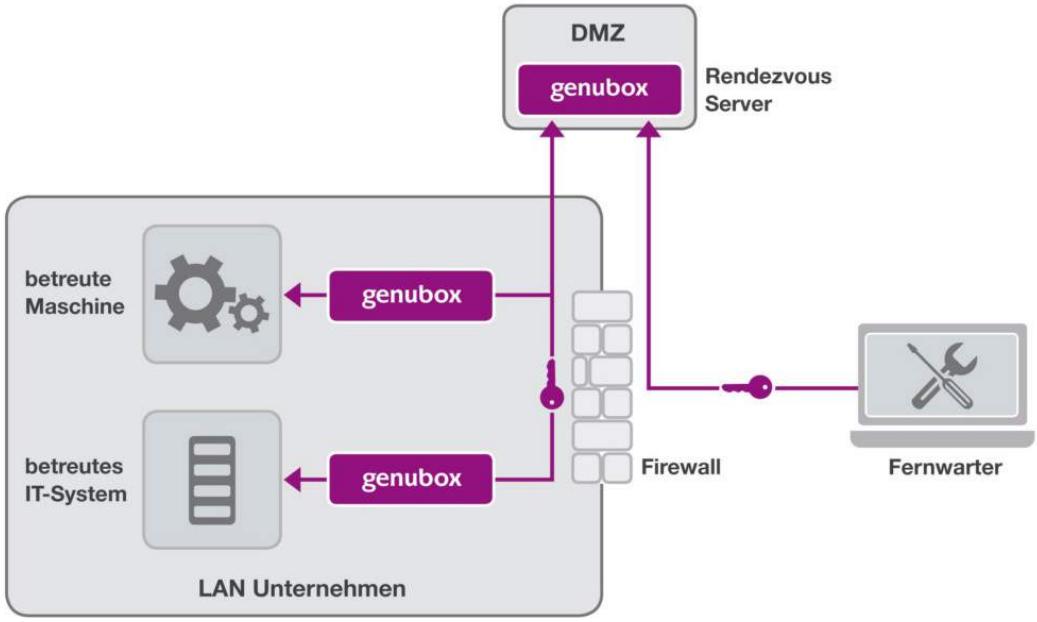


Abbildung 5-2: Prozesssicht; Quelle: [4]

lerseite. Die genubox als robuste Appliance ermöglicht hochsichere Fernwartungszugriffe an nahezu jedem Ort und kann z. B. an Industrierobotern, Windrädern oder auch einfach in Serverräumen installiert werden.

Der Hersteller initiiert als ersten Schritt über seinen Fernwartungs-PC eine Anfrage in Richtung Rendezvous-Server. Je nach Konfiguration des Rendezvous-Servers erhält der Mitarbeiter des Betreibers, der für das Wartungsobjekt verantwortlich ist, im Anschluss eine Mitteilung auf seinem PC. Diese Mitteilung dient lediglich der Information, dass der Hersteller in diesem Moment plant, auf das Wartungsobjekt remote zuzugreifen – die Fernwartungsanfrage selbst ist jedoch zu diesem Zeitpunkt im „Wartemodus" innerhalb des Rendezvous-Servers.

Wenn der Mitarbeiter des Betreibers der Fernwartungsanfrage einwilligt, ist der Hersteller in der Lage, remote auf das Wartungsobjekt zuzugreifen. Hierzu bestätigt der Mitarbeiter des Betreibers zunächst die Fernwartungsanfrage für das entsprechende Wartungsobjekt (z. B. gemäß Abbildung 5-2: betreute Maschine oder betreutes IT-System).

Mit dieser Einwilligung baut die am Wartungsobjekt vorgelagerte genubox eine Verbindung in Richtung Rendezvous-Server auf, wo nun die Verbindungen beider Parteien (Fernwartungsanfrage und Einwilligung) zusammengeführt werden. Nachdem die Verbindung zwischen Hersteller und Betreiber zustande gekommen ist, kann der Hersteller die Fernwartung sicher am Wartungsobjekt durchführen.

Die genubox, die entweder im Netzsegment des Wartungsobjekts oder direkt im Wartungsobjekt implementiert ist, sichert die Fernwartungsverbindung gegenüber Zugriffen auf andere Wartungsobjekte ab.

5.3.4 Anwendungssicht

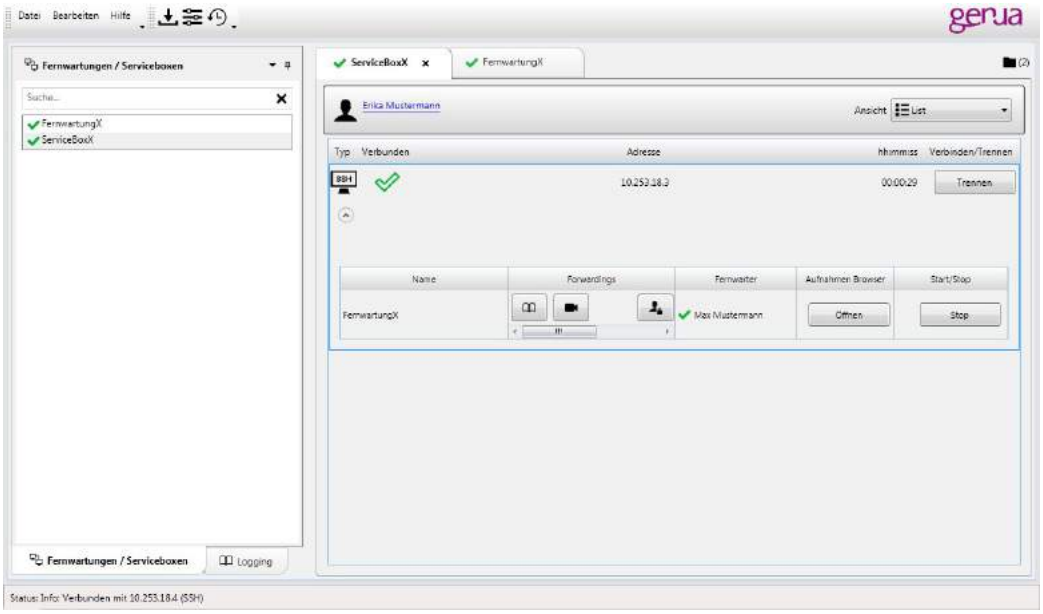


Abbildung 5-3: Anwendungssicht; Quelle: [4]

Die Fernwartung von genua kann mit unterschiedlichen Anwendungen umgesetzt werden. Um bspw. die Fernwartungsverbindung herstellerseitig zu initiieren, kann der Mitarbeiter entweder die Fernwartungs-App (siehe Abbildung 5-3) oder herkömmliche Anwendungen, wie z. B. Putty zum Aufbau einer VPN-Verbindung nutzen. Die Fernwartungs-App kann auf der Webseite von genua frei heruntergeladen und an den Hersteller übergeben werden. Zudem können in diese App Netzwerkkonfigurations- oder Authentifizierungsdaten integriert werden, welche über das genucenter erstellt werden. Ebenso ist eine Personalisierung der Fernwartungs-App über die Konfigurationsdatei möglich, sodass immer nachvollzogen werden kann, wer welche Änderungen auf Herstellerseite gemacht hat. Damit diese Konfigurationsdateien nicht Hersteller-intern zwischen Mitarbeitern weitergegeben werden, können die Mitarbeiter vertraglich verpflichtet werden, die individualisierten Konfigurationsdateien nicht weiterzugeben. Der Inhaber einer Konfigurationsdatei kann bei vorsätzlichen Verstößen auch persönlich für den entstandenen Schaden haftbar gemacht werden. Diese Personalisierung kann die Nachweiskraft von Aufzeichnungen und Protokollierungen erhöhen und IT-Sicherheitsrisiken reduzieren.

Neben dem Einsatz auf Herstellerseite ist auch der Einsatz der Fernwartungs-App auf Betreiberseite in einer Implementierung möglich. Da die Verantwortlichen für ein Wartungsobjekt nicht immer ausgebildete IT-Administratoren sind, kann auch hier eine Fernwartungs-App mit den benötigten Netzwerkkonfigurations- und Authentifizierungsdaten generiert und genutzt werden. So wird den eigenen Mitarbeitern ein einfacher und fehlerresistenter Zugriff auf das Wartungsobjekt ermöglicht. Damit die Verbindungen problemlos aufgebaut werden

können, ist eine Konfiguration der Netzwerke erforderlich. Diese Konfiguration wird einerseits über die genuboxen realisiert, die über die Web-Oberfläche des genucenters zentral administriert werden können. Andererseits müssen die Firewalls (über Web-Oberflächen) konfiguriert werden, sodass die Verbindungen die Firewalls passieren dürfen.

5.3.5 Technische Sicht

Für den Fernwartungszugriff baut der Hersteller zunächst einen SSH-Tunnel zum Rendezvous-Server auf. Dabei werden für alle von der Wartungssoftware benötigten TCP-Ports entsprechende Local-forwarding-Einträge auf dem Rendezvous-Server konfiguriert. Nach erfolgreicher Authentifizierung wird ein VPN-Tunnel zwischen dem Rechner des Fernwarters auf Herstellerseite und dem Rendezvous Server aufgebaut.

Auf der Seite des Betreibers startet der Verantwortliche für das Wartungsobjekt ebenfalls eine VPN-Verbindungsanfrage in Richtung Rendezvous-Server. Die von der Wartungssoftware benötigten TCP-Ports werden hierbei als Remote-forwarding-Einträge auf das Wartungsobjekt konfiguriert. Bevor die Fernwartungsverbindung via VPN zwischen beiden Parteien aufgebaut wird, ersetzt die genubox vor dem Wartungsobjekt ihren Filtersatz für den Produktiveinsatz durch einen Wartungsfiltersatz. Dieser isoliert das Wartungsobjekt vom restlichen Netzwerk und verhindert einen direkten Zugriff des Fernwarters auf Objekte, die sich nicht im Bereich des Wartungsobjekts befinden. Nachdem dieser Regelwechsel durchgeführt und die Fernwartungsverbindung etabliert wurde, muss sich der Fernwarter ein weiteres Mal authentifizieren, nämlich am Wartungsobjekt. Nachdem dieser Schritt erfolgreich vollzogen ist, können die eigentlichen Arbeiten der Fernwartung beginnen.

Nach Abschluss der Wartungsarbeiten über die Fernwartungsleitung beendet der Fernwarter die Verbindung zum Wartungsobjekt und im Anschluss die Verbindung zum Rendezvous-Server. Auf Betreiberseite muss der Verantwortliche für das Wartungsobjekt die Verbindung zum Rendezvous-Server ebenfalls beenden. Damit sind dann alle Verbindungen abgebaut und alle Möglichkeiten genommen, auf das Wartungsobjekt von außen zuzugreifen.

5.3.6 Vorgehen und Umsetzung

Das Vorgehen der Implementierung einer Fernwartungslösung aus technischer Sicht gestaltet sich in der Regel wie folgt: genua wird von einem Betreiber beauftragt, eine Fernwartungslösung zu implementieren. Hierzu sieht genua vor, einen Testaufbau auf Betreiberseite zu implementieren. Da ein Testsetting (im Laborsinn) aus verschiedenen Gründen, wie z. B. Knappheit an redundanten Maschinen, die aus dem produktiven Betrieb herausgelöst werden können, nicht möglich ist, findet der Testaufbau häufig im Live-Betrieb statt.

In enger Kooperation mit dem Betreiber werden im Produktionsnetzwerk potenzielle Wartungsobjekte identifiziert, die in den Testaufbau zur Fernwartung integriert werden können. Da der Hersteller remote auf das Wartungsobjekt zugreifen muss, muss auf Betreiberseite eine entsprechende Gegenstelle eingerichtet werden: die genubox. Um den Aufwand der Implementierung so stark wie möglich zu reduzieren, bereitet genua die genubox weitestgehend hinsichtlich der Konfiguration vor, sodass diese lediglich noch an das Netzwerk angeschlossen

werden muss. Je nach Konfiguration der Firewall des Betreibers müssen die ausgehenden Verbindungen in Richtung Rendezvous-Server auf der Firewall zugelassen werden.

Damit ist aus technischer Sicht die Fernwartungslösung als Testaufbau fertig eingerichtet und kann nach erfolgreicher Erprobung für weitere Wartungsobjekte ausgerollt werden. Damit die IT-Administratoren die Fernwartungslösung in eigener Hand administrieren können, sieht genua zudem eine Schulung über 2,5 Tage vor, in der z. B. der Umgang mit den Produkten, die Erstellung der Konfigurationsdateien für die Fernwartungs-App und das Fernwartungskonzept behandelt werden. Für Mitarbeiter, die die nutzerfreundlichen Fernwartungs-Apps erhalten und zukünftig nutzen werden, sieht genua eine Einweisung als ausreichend an.

5.4 Erfolgsfaktoren

Veränderung bedeutet Abwehr! Wenn lokale Wartung oder selbst entwickelte, nicht sichere Möglichkeiten des Zugriffs auf Systeme durch eine sichere Fernwartungslösung ersetzt werden, ist das Management gefordert, alle involvierten Parteien in das Projekt einzubinden, die Vorteile dieser Veränderung aufzuzeigen und das für IT-Sicherheit notwendige Bewusstsein zu schaffen. Die Unterstützung des Vorstands, des CIOs und des CISOs ist ein elementarer Erfolgsfaktor.

Sobald diese organisatorischen Aspekte geklärt wurden und die Fernwartung erfolgreich implementiert ist, ergeben sich für den Kunden fünf wesentliche Vorteile: (1) Vermeidung von Cyber-Angriffen, (2) Schutz sensibler Produktionsdaten, (3) Verhinderung der Ausbreitung von Schadsoftware, (4) Behalten der Kontrolle sowie (5) Gewährleistung von Usability und komfortabler Administration.

(1) Vermeidung von Cyber-Angriffen. Das Management der Fernwartungslösung unterstützt an zentraler Stelle den Kunden dabei, unzureichende Authentifizierungsmethoden, offene Ports in der Firewall oder zu freizügig eingeräumte Zugriffsrechte auf das Wartungsobjekt zu vermeiden. Damit wird die Angriffsfläche für Cyber-Angreifer minimiert und das Risiko von Produktionsstörungen reduziert.
(2) Schutz sensibler Produktionsdaten. Mittels Fernwartung ist ein Auslesen sensibler Produktionsdaten prinzipiell möglich. Die Fernwartungslösung von genua bietet die Möglichkeiten, einseitige Fernwartungszugriffe zu unterbinden, die Kommunikation über VPNs zu realisieren und für Dritte den Zugriff auf den für die Arbeit notwendigen Bereich zu limitieren. Ein Zugriff über Netzsegmente hinaus ist dem Fernwartungsunternehmen somit versperrt.
(3) Verhinderung der Ausbreitung von Schadsoftware. Das Risiko der absichtlichen oder unbeabsichtigten Infektion der IT-Systeme mittels Schadsoftware durch einen Angreifer oder durch den Dienstleister wird durch starke Authentifizierungsmechanismen und kontrollierte Zugriffsrechte minimiert. Die Kapselung des Wartungsobjektes in einem minimalen Netzwerksegment sorgt zudem für Sicherheit – vor allem dann, wenn es Schadsoftware gelingen sollte, trotz Schutzmaßnahmen in das Netzwerk des Betreibers einzudringen.
(4) Behalten der Kontrolle. Fernwartungszugriffe können in Echtzeit mitverfolgt werden und alle Aktionen können von der genubox protokolliert, per Video direkt auf der

genubox aufgezeichnet und auf dem lokalen Graphical User Interface der genubox übersichtlich dargestellt werden. So ist es dem Kunden möglich, jederzeit nachzuvollziehen, wer wann auf welches Wartungsobjekt im Rahmen der Fernwartung zugegriffen hat. Diese Transparenz und Dokumentation ist vor allem bei Haftungsfragen von Vorteil.

(5) Gewährleistung von Usability und komfortabler Administration. Die Umsetzung einer Fernwartungslösung erfordert weitere IT-Komponenten in der IT-Infrastruktur, die damit noch komplexer und heterogener sowie möglicherweise störanfälliger wird. Die Fernwartungslösung ist einfach in bestehende IT-Netzwerke integrierbar, zentral administrierbar und über die ggf. von anderen genua-Produkten bekannten Bedienoberflächen steuerbar. Mit nur wenigen Mausklicks können Sessions zur Fernwartung freigegeben, durchgeführt und abgeschlossen werden.

genua sieht sich als ein Dienstleister für Lösungen und nicht als Produkthersteller mit einer „Hit and Run"-Strategie und hat die Kompetenzen und die Technologie, Fernwartungszugänge individuell an die Bedürfnisse von Betreibern, Wartungsfirmen und Zulieferern anzupassen und so Nutzenpotenziale zu realisieren.

Die Lösungen von genua werden in verschiedenen Branchen und für verschiedene Systeme (Wartungsobjekte) von unterschiedlichen Herstellern eingesetzt. genua stellt seinen Kunden nicht nur Wissen über Fernwartungslösungen, sondern auch Wissen zu IT-Sicherheit über Sektoren und Technologieanbieter hinweg zur Verfügung. Damit kann die Lösung von genua dazu beitragen, die Heterogenität im IT-Sicherheitsmanagement – gerade bei größeren Betreibern Kritischer Infrastrukturen – zu verringern und einheitliche Standards der IT-Sicherheit in diesem spezifischen Bereich zu etablieren. genua kann dadurch, dass die gesamte Entwicklung in Deutschland stattfindet, eine hohe Qualität der Produkte sicherstellen, dies durch Zertifikate nachweisen und kommt daher als Anbieter für sicherheitskritische Systeme infrage. Darüber hinaus ist genua nicht nur in der Forschung mit Partnern, sondern auch in den Gremien zur Standardisierung und Normung im Bereich der IT-Sicherheit aktiv und leistet damit einen Beitrag, die IT-Sicherheit Kritischer Infrastrukturen zu erhöhen.

5.5 Danksagung

Wir danken dem Bundesministerium für Bildung und Forschung (BMBF) für die Möglichkeit der Forschung im Rahmen des Projektes VeSiKi, Förderkennzeichen 16KIS0213K.

5.6 Literaturverzeichnis

[1] genua, genua – Über uns. Verfügbar unter: https://www.genua.de/ueber-uns.html [zugegriffen: 17-Jan-2016].

[2] genua, „genua – Unsere Forschungsprojekte". Verfügbar unter: https://www.genua.de/ueber-uns/unsere-forschungsprojekte.html [zugegriffen: 17-Jan-2017].

[3] BSI, 2015. Fernwartung im industriellen Umfeld. Bundesamt für Sicherheit in der Informationstechnik, S. 1–4.

[4] genua, genubox. Hochsichere Fernwartungs-Appliance. Technische Informationen. Verfügbar unter: https://www.genua.de/fileadmin/download/produkte/genubox-broschuere.pdf [zugegriffen: 11-Mai-2018].

6 itWatch GmbH: Ein sicherer Standardprozess für die digitale Tatortfotografie mit DeviceWatch

Sebastian Lücking, Universität der Bundeswehr München
Sebastian Dännart, Universität der Bundeswehr München

Die Bayerische Polizei hat einen bayernweiten Standardprozess für die Umsetzung der digitalen Tatortfotografie in der Polizeiarbeit eingeführt. Dieser Prozess ermöglicht eine gerichtsfeste Verarbeitung der Bilder mit einer regelbasierten Endgeräteüberwachung als zentralem Sicherheitskonzept. Die Lösung lässt unter diesem Gesichtspunkt nicht nur die Nutzung aller digitalen Geräte mit Fotofunktion zu, sondern kontrolliert in einem sicheren Prozess ebenso die Schnittstellen der Geräte. Durch den einheitlichen Ablauf der Verarbeitung von Tatortfotos konnten vonseiten der Bayerischen Polizei Kosteneinsparungspotenziale realisiert und der administrative Anteil der Polizeiarbeit verringert werden.

Keywords: Sektor Staat und Verwaltung, Behörde, Prozesssicherheit, Endgerätesicherheit

6.1 Unternehmen

6.1.1 Unternehmensprofile

Die Bayerische Polizei zählt mit ca. 41.000 Beschäftigten zu den größten Polizeiverbänden in Deutschland. Strafverfolgung und Gefahrenabwehr mit dem Schutz der Bevölkerung sowie die Bekämpfung und Aufklärung von Straftaten stellen wesentliche Aufgabenbereiche dar. Dieser Aufgaben nimmt man sich im Landeskriminalamt, den verschiedenen Dienststellen und den Polizeipräsidien an. Die Ausstattung der Polizeidienststellen und Behörden mit moderner Informations- und Kommunikationstechnologie und die Umsetzung moderner Konzepte des E-Government mit digitalen Akten sind dabei strategische Themen der Bayerischen Staatsregierung.

Das Unternehmen itWatch, mit Sitz in München, ist Weltmarktführer im sicheren Device-Management und entwickelt innovative, maßgeschneiderte IT-Sicherheitslösungen, unter anderem für Behörden. Das Unternehmen wurde 2002 gegründet und ist im Jahr 2016 mit über 15 verschiedenen Softwarelösungen am Markt. Die Lösungen der itWatch Enterprise Security Suite werden – ohne Zukauf von außen – ausschließlich im Unternehmen selbst entwickelt. Auf diese Weise kann das Unternehmen die Sicherheit seiner Produkte jederzeit garantieren. Die laufende Weiterentwicklung der Produkte sichert den Kunden gleichzeitig den Zugang zu technischen Innovationen sowie Investitionsschutz.

6.1.2 Strategische Ausrichtung

Zu den Zielen der Polizei gehört nicht nur die Gewährleistung von Sicherheit, sondern auch die professionelle Durchsetzung des Rechts. Für die Erfüllung der Polizeiaufgaben ist eine

technisch aktuelle und gut funktionierende IT notwendig. Strategische Ziele für die IT in Polizeibehörden bilden unter anderem die Umsetzung von E-Government mit modernen, effizienten Prozessen und papierlose, digitale Akten.

Das Projekt Digitale Fotografie (DiFo) (Metzger 2004; Metzger 2006) soll die Digitalisierung der Prozesse der Polizeiarbeit weiter vorantreiben und so das tägliche Polizeigeschäft erleichtern. Ebenso soll durch das Projekt der Papier- und Verwaltungsaufwand reduziert werden und Kosteneinsparungspotenziale realisiert werden können. Bei der Planung und Einführung neuer Prozesse ist vorrangig darauf zu achten, dass alle Prozesse der Polizeiarbeit vor Gericht Bestand haben müssen. Aus diesem Grund ist für das Projekt DiFo die Datenintegrität der digitalen Tatortfotografien essenziell.

6.1.3 Fallstudienpartner

Name	Position im Unternehmen
Ramon Mörl	Geschäftsführer itWatch
Sebastian Dännart	Wissenschaftlicher Mitarbeiter, Universität der Bundeswehr München
Sebastian Lücking	Studierender der Wirtschaftsinformatik, Universität der Bundeswehr München

6.2 Kritische Infrastruktur

6.2.1 Einordnung als KRITIS

Die Polizei Bayern ist dem Sektor „Staat und Verwaltung“ zuzuordnen. Dieser ist entsprechend der ressortübergreifenden KRITIS-Definition des Bundesministeriums des Innern (BMI) ein Sektor der Kritischen Infrastrukturen. Durch eine Beeinträchtigung der Arbeit der Polizei würde eine Gefährdung der öffentlichen Sicherheit eintreten.

Das IT-Sicherheitsgesetz findet jedoch keine Anwendung auf Landespolizeibehörden, wie die Polizei Bayern und das Bayerische Landeskriminalamt, da der Begriff der Kritischen Infrastruktur hier enger gefasst ist und den Sektor „Staat und Verwaltung“ nicht umfasst.

6.2.2 Risikoanalyse

Bei jedem Prozess der Aufnahme von Beweisen besteht das Risiko der Beweisfälschung. Sowohl bei der Aufnahme als auch bei der Bearbeitung und Verwendung der Bilder liegen hier potenzielle Schwachstellen. Durch die lückenlose Dokumentation vom Import der Aufnahme vom Datenträger bis zur digitalen Ablage auf dem Fileserver, ist jeder Prozessschritt nachvollziehbar und das Risiko der unrechtmäßigen Beeinflussung minimiert.

Ein weiteres Risiko ist die Zulassung unterschiedlicher Datenträger. Diese erhöht jedoch die flexible Verfügbarkeit von Bildaufnahmegeräten und stellt eine visuelle Aufnahme des Tatorts sicher. Wird eine dienstliche Kamera unbrauchbar und ist daher kurzfristig im Einsatz nicht mehr nutzbar, kann der Polizeibeamte jede beliebige dienstlich gekaufte Kamera, auch spontan nach Verlust neu erworbene, für die Beweisaufnahme heranziehen. Dem Risiko durch die Zulassung beliebiger Datenträger wird, zugunsten einer höheren Verfügbarkeit

und besserer Einkaufspreise durch COTS-Produkte („Commercial off the Shelf"), mit einer besseren Prozesssicherheit begegnet. Die nötigen Maßnahmen werden in dieser Fallstudie beschrieben.

Das Projekt selbst konzipierte einen völlig neuen, digital unterstützen Prozess. Dieser hatte keinen Einfluss auf den alten „analogen" Prozess und wurde erst aktiv ausgerollt, nachdem alle Tests erfolgreich durchgeführt worden waren. Ein Scheitern wäre also mit geringem Risiko verbunden gewesen.

6.3 Projekt

Die Tatortfotografie weist eine Reihe von unterschiedlichen Anwendungsfeldern auf: Ermittlungen der Kriminalpolizei oder Dokumentation von Verkehrsunfällen sind nur zwei Anwendungsbeispiele der Fotografie im Rahmen der Polizeiarbeit.

Das Hauptrisiko der digitalen Tatortfotografie liegt in der Datenintegrität der digitalen Bilder. Es muss sichergestellt werden, dass die Fotos bis zur richterlichen Nutzung als Beweismaterial keinerlei Manipulation unterliegen können. Der gesamte Prozess – von der Erstellung der Tatortfotografien über die Archivierung und die Weiterverarbeitung in digitalen Akten, der „Übergabe" der digitalen Akten der Polizei an die Richter bis hin zu richterlichen Entscheidung – muss deshalb gegenüber unbefugter Eingriffe abgesichert werden. In der aktuellen Polizeiarbeit wird auch von digitaler Asservatenkammer gesprochen, wenn digitales Beweismaterial für die richterliche Würdigung aufbewahrt wird.

Es wurden 2005 bei der beschriebenen Projektierung mehrere Optionen der Realisierung der Nutzung von digitaler Tatortfotografie in Erwägung gezogen. Im „analogen" Prozess, mit Polaroids, hat der Polizist die Authentizität des Fotos durch eine Unterschrift auf der Rückseite verifiziert und das unterschriebene Foto wurde mit den Angaben zur Herkunft in der Akte abgelegt. Für die Kopie einer Akte, um diese an Gericht und Richter zu übergeben, beauftragte die Polizei eines von fünf zertifizierten Kopierlabors, die sicherstellten, dass die Kopie dem Original entspricht.

Die Projektleitung entschied sich dazu, einen gänzlich neuen Prozess zu definieren, also keinesfalls den „analogen" Prozess mit digitalen Bildern zu imitieren – digitale Bilder ausdrucken, unterschrieben und in einer Akte ablegen. Mithilfe des digitalen Prozesses sollen Kosteneffizienz- und Synergiepotenziale genutzt werden können.

Der erste Lösungsansatz sah vor, dass jede Kamera und jeder dazugehörige Datenträger einzeln für das System freigegeben werden müssten. Das Projektmanagement entschied, dass diese Lösung nicht nur mit einem hohen administrativen Aufwand verbunden ist, sondern der Beschaffungsprozess für Kameras zu kompliziert und langsam durchführbar wäre. Jedes Kameramodell müsste zentral zugelassen, anschließend müssten Kameras über entsprechende Ausschreibungen und Rahmenverträge beschafft und anschließend von einem Administrator freigegeben werden. Erst dann könnte die Kamera im Dienst genutzt werden. Sollte eine Kamera allerdings während eines Einsatzes nicht mehr funktionstüchtig sein, müsste ein Polizeibeamter zur Dienststelle fahren und sich eine neue Kamera aus dem Lager holen. Das bedingt, dass jede Polizeidienststelle Kameras vorrätig halten müsste. Kameras und speziell

Digitalkameras sind jedoch ein kurzlebiges Produkt, mit kurzen Weiterentwicklungszyklen. Deshalb müsste für neue Kameramodelle ständig geprüft werden, ob sie zulassungsfähig wären, ob sie beschafft werden könnten und ehe die Modelle im Polizeidienst real eingesetzt werden könnten, wären sie bereits veraltet. Mit einem solchen Prozess wären nicht nur Einsparungen und Modernisierungspotenziale von papierlosen und digitalen Akten nicht ausgeschöpft, sondern ebenso die Nutzung von fototauglichen Geräten eingegrenzt worden. Der Projektleitung war es aber ein Anliegen der Zukunftssicherheit, dass nicht nur Digitalkameras, sondern jedes fototaugliche Gerät für die Polizeiarbeit verwendet werden kann.

Im Rahmen der Polizeiarbeit sollte jeder Polizist in der Lage sein, die Bilder selbst am Arbeitsplatz in der digitalen Akte zu nutzen. Manipulation der digitalen Bilder und die Datenübertragungen zwischen Kameras, Arbeitsplatzrechnern und Servern der Polizei wurden als wesentliche Risiken identifiziert. Weitere Risiken bestehen darin, dass bei offenen Ports für die Datenübertragung Dateien illegal kopiert oder Schadsoftware in das Netz der Bayerischen Polizei eingebracht werden können. Die Ports der Windows-Arbeitsplatzrechner können „mit Bordmitteln" bezüglich der verfügbaren Rechtegranularität nur unzureichend geschützt werden. BIOS, Registry und der Plug-and-Play-Mechanismus von Windows, dem wesentlichen Betriebssystem in Polizeibehörden, lassen es jedoch nicht zuverlässig zu, Ports für einzelne Geräte und Dateitypen (hier Bilder) zu öffnen und die Sicherung der Ports adäquat zu verwalten. Daher musste hier auf spezielle Software zurückgegriffen werden.

Die Projektleitung entschied, einen neuen Prozess mit neuen Konzepten der Endgeräte-Kontrolle und einem regelbasierten System zuzulassen, das eine Kontrolle der Geräte genau wie die einfache Integration neuer Geräte in die Polizeiarbeit möglich macht. Es war notwendig, IT-Sicherheit von Beginn der Neukonzeption des Prozesses zu betrachten und hier ein System einzuführen, das die Kontrolle der Schnittstellen der Polizeiarbeitsrechner zu externen Geräten über USB-Schnittstellen feingranular übernimmt.

Im Oktober 2000 wurde eine Projektgruppe eingerichtet, die ein Fachkonzept unter Beteiligung der Justizbehörden erstellte. Das Fachkonzept wurde im Juli 2002 vorgestellt, woraufhin das Projekt DiFo im Jahr 2004 beginnen konnte. Mit dem Projektstart wurde auch die Ausschreibung der für die DiFo notwendigen Bildübertragungssoftware, der Bildverwaltungssoftware sowie der Schnittstellensicherung und des Content-Filters initiiert. Das Bildübertragungsprogramm wird von T-Systems als Individualsoftware und das Bildverwaltungsprogramm von Pixelboxx als Standard-Software gestellt. Für die Schnittstellenabsicherung und den Content-Filter entschied man sich für die Software „DeviceWatch" von itWatch. Diese Software wurde mit dem Plug-in SecureDIFO erweitert.

Eine der Herausforderungen für das Projekt DiFo war die Ausstattung der Dienststellen mit dem Betriebssystem Windows. Erst mit Windows XP war die neue USB-Technologie für Plug-and-Play und die Absicherung von Schnittstellen vorhanden. Das Projekt „PC REA 3", zur Einführung von Windows XP in den Dienststellen, musste vor dem Projekt DiFo realisiert werden.

Die Ergebnisse des Projekts DiFo waren die Einsatzfähigkeit eines einzigen Standardprozesses in allen Anwendungsbereichen der Tatortfotografie der Bayerischen Polizei, große Effizienzgewinne und Synergieeffekte, Kosteneinsparung von über einer Million Euro pro Jahr sowie die Amortisation des Investments nach bereits drei Jahren.

6.3.1 Projektziel

Das Projekt sollte bei der Bayerischen Polizei die analoge durch die digitale Fotografie ablösen. Besonderes Augenmerk wurde auf die Schutzziele der Informationssicherheit mit Vertraulichkeit, Verfügbarkeit und Integrität der Bilddaten gelegt. Die Bilddaten müssen insbesondere vor Manipulation geschützt werden, damit sie in Straf- und Ordnungswidrigkeitsverfahren als Beweismittel vor Gericht anerkannt werden.

Weitere Ziele des Projekts waren es, eine kosteneffiziente Lösung zu erreichen sowie Prozesse einzuführen, die den Betrieb in den Dienststellen nicht belasten. Die Polizei wollte eine moderne Lösung, die es erlaubt, digitale Kameras einfach zu beschaffen und uneingeschränkt zu nutzen, sodass sie ohne weitere Zulassungsverfahren einfach im Polizeidienst genutzt werden können.

6.3.2 Geschäftssicht

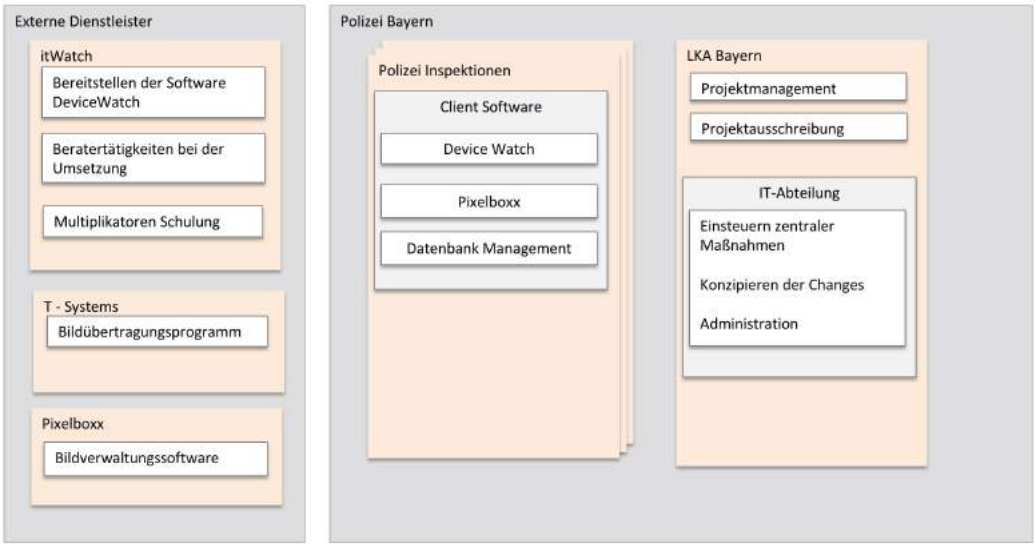


Abbildung 6-1: Geschäftssicht

Nach der Initialisierung des Projektes durch das Landeskriminalamt (LKA) Bayern übernahm dieses das Projektmanagement sowie die Projektausschreibung mit den zur Realisierung notwendigen Ausschreibungen für Hard- und Software. Mit dem Projekt sollte ein landesweiter Standardprozess eingeführt werden und so hat das LKA Bayern über seine IT-Abteilung alle Maßnahmen und das notwendige Changemanagement koordiniert. Die einzelnen Polizeipräsidien und Inspektionen der Regierungsbezirke Bayerns beteiligten sich durch Vertreter an dem Projekt. Das Gesamtprojekt wurde in Teilprojekte zerlegt, die neben dem täglichen Dienst durchgeführt wurden. Im Projekt DiFo standen die Leiter der Schnittstellenprojekte von itWatch, T-Systems und Pixelboxx als externe Berater zur Verfügung.

6.3.3 Prozesssicht

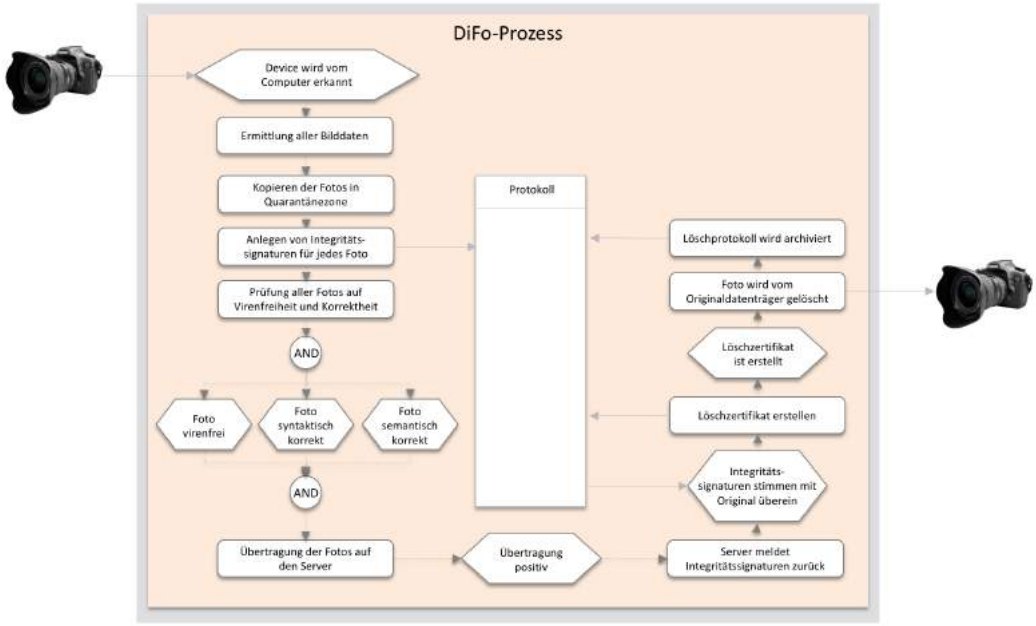


Abbildung 6-2: Prozesssicht

Der bereits beschriebene alte, „analoge" Prozess zielte darauf ab, Bilder als verwertbare Beweismittel zu hinterlegen, wobei die Unterschrift des Beamten die Verifikation der Echtheit des Bildes dokumentieren sollte. Der Grundgedanke bleibt im digitalen Prozess derselbe, jedoch entschieden die Projektmanager sich bewusst dafür, einen komplett neuen, an die neuen Gegebenheiten und Bedürfnisse angepassten Prozess zu entwerfen.

Ziel des neuen Prozesses waren im Wesentlichen zwei Merkmale:

- möglichst einfache Handhabung für den Beamten, der das Bild automatisch in seinem Workflow in der elektronischen Akte sehen soll, und
- Sicherstellung der gerichtsfesten Beweiseignung der Bilder.

Nach dem Einsetzen eines Datenträgers beliebiger Art an einem Arbeitsplatz-PC oder dem Anstecken einer Digitalkamera an einem USB-Port überprüft die Software DeviceWatch diesen Datenträger auf zulässige Fotoformate (z. B. JPEG, TIFF oder Rohformate der Hersteller), ohne andere Datenformate zu berücksichtigen. Die Überprüfung erfolgt dabei mittels eines Content-Filters.

Die Dateien werden anschließend zur genaueren Untersuchung in eine Quarantänezone kopiert. Hier erhält jedes Foto eine Integritätssignatur, die in einem Protokoll vermerkt wird. Ebenso wird hier jede Bilddatei auf Virenfreiheit sowie semantische und syntaktische Korrektheit geprüft.

Ist diese Überprüfung erfolgreich, werden die Fotodateien zum Server übertragen. Der Server signiert das Foto und sendet eine Erfolgsmeldung. Nun werden die Integritätssigna-

turen vom Server geprüft. Nur wenn die Signatur des Servers mit der Signatur des Originals übereinstimmt, wird ein Löschzertifikat erstellt. Wurde das Löschzertifikat erstellt, wird das Foto von dem Originaldatenträger gelöscht und das Löschprotokoll archiviert. Die gesamte Kommunikation erfolgt über abgesicherte Kanäle und die Ablage der Logfiles ist revisionssicher.

Bis zu diesem Punkt hat der Beamte vor dem Arbeitsplatz-PC lediglich das Speichermedium verbunden. Alle weiteren Prozessschritte geschehen automatisch. Mit dieser Vereinfachung ist dem ersten angestrebten Merkmal des Prozesses Rechnung getragen, nämlich den Importvorgang für den Beamten zu vereinfachen und zu automatisieren.

Durch die Integritätssignaturen ist auch für eine spätere, weitere Verarbeitung die Authentizität der Daten sichergestellt und die Voraussetzungen für eine Verwendung als Beweis vor Gericht sind gegeben.

Der neue landesweite Standardprozess ist in Abbildung 6-2 dargestellt.

6.3.4 Anwendungssicht

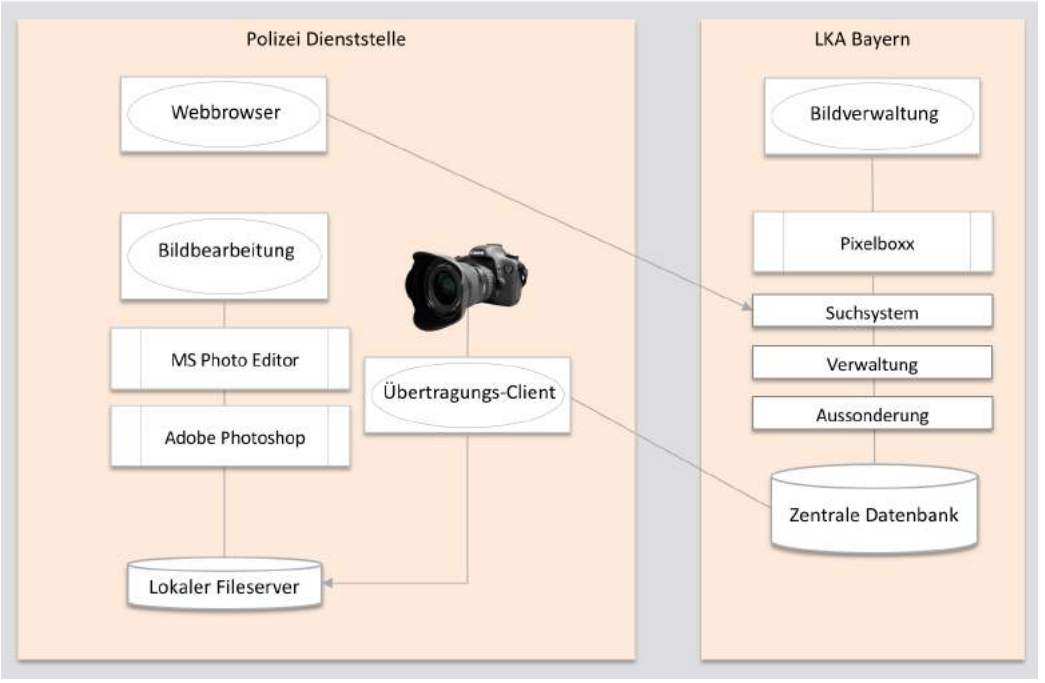


Abbildung 6-3: Anwendungssicht

Das Projekt DiFo entwickelte eine Standardanwendung, die für alle Bereiche der polizeilichen Tätigkeit, bei der gerichtsfestes Bildmaterial zu erfassen ist, genutzt wird. Für die Tatortarbeit der Schutz- und Kriminalpolizei, die Spuren- und Sachfotografie, das Täterbildverfahren, die Verkehrsunfallbearbeitung, die Fahndungs- und Dokumentenfotografie kommt diese eine Standardanwendung zum Einsatz.

Die Hauptanwendung befindet sich auf den Clients in den Polizeidienststellen. Die Anwendung besteht im Wesentlichen aus einer Bildbearbeitungssoftware sowie einem Übertragungs-Client.
Der Übertragungs-Client dient nicht nur dem Versenden und Archivieren der Originalbilder, sondern stellt zudem Kopien der Originalbilder für eine Weiterverwendung der Bilddaten in der polizeilichen Tätigkeit zur Verfügung. Der in Kapitel 6.3.3 beschriebene Prozess wird von dem Übertragungs-Client durchgeführt.

Für die Bildbearbeitung stehen die Programme Photo Editor von MS Office und Photoshop zur Verfügung. Die gesamte Bildbearbeitung findet auf einem lokalen Fileserver statt, dieser stellt Kopien der Originaldateien über den Übertragungs-Client bereit. So wird sichergestellt, dass die Originaldateien während der Polizeiarbeit nicht verändert werden.

Die Polizeibeamten können über einen Webbrowser die Bildverwaltungssoftware Pixelboxx nutzen. Die Software erlaubt die Suche nach Bildern sowie das Einsehen von Metadaten zu den Bildern. Ein authentifizierter Nutzer kann zudem die Informationen der Bilder anpassen. Pixelboxx arbeitet auf dem zentralen Datenbankserver beim LKA Bayern und führt die Standardverwaltung und Aussonderung gemäß den vorgeschriebenen Bestimmungen durch.

6.3.5 Technische Sicht

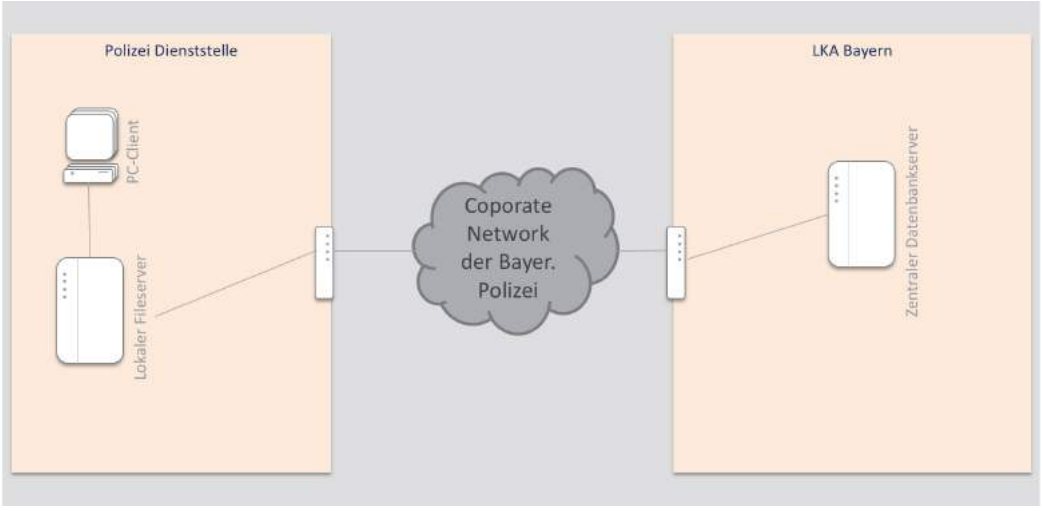


Abbildung 6-4: Technische Sicht

Die Lösung zur Datenhaltung besteht aus einem zentralen Datenbankserver mit fünf Datenbanken (und entsprechenden Datenbankservern), die sich beim LKA Bayern befinden:

- Eine Transferdatenbank ist für die Übertragung zwischen LKA und dem Fileserver der Polizeidienststellen zuständig.
- Eine Konfigurationsdatenbank beinhaltet die Sicherheitsrichtlinien und Regeln für die Clients.

- Eine Aussonderungsdatenbank, die für die Umsetzung der gesetzlichen Lösch- und Aussonderungsbestimmungen zuständig ist.
- Eine Metadaten- und Userdatenbank stellt die Informationen für die Bildverwaltung bereit.
- Eine Beschäftigtendatenbank hält die Daten für die Authentifikation der Nutzer bereit.

Die einzelnen Polizeidienststellen sind durch das Corporate Network der Bayerischen Polizei mit dem LKA verbunden. Insgesamt verfügen alle Dienststellen zusammen über 30.000 PCs, die mit der Bildübertragungssoftware und der Schnittstellenabsicherung von itWatch ausgestattet sind. Wie in Kapitel 6.3.4 beschrieben, findet der Zugriff auf die Bildverwaltung mittels Webbrowser und Webinterface statt und jede Dienststelle verfügt über einen lokalen Fileserver.

Der Ressourcenaufwand in personeller Hinsicht beläuft sich bei dem LKA für die Administration auf zwei Administratoren, die je zu 50 % an der Verwaltung des DiFo-Prozesses arbeiten. Dezentral wird der personelle Aufwand auf die einmalige Erfassung der Übertragungs- und Aussonderungsclients begrenzt.

6.3.6 Umfang und Zeitraum

Die Projektplanung räumte dem Projekt DiFo, von der Haushaltsmittelzusage bis zum endgültigen Roll-out, eine Projektlaufzeit von zwei Jahren ein. Die Realisierung der Schnittstellenabsicherung, des Content-Filters mit dem Software-Plug-in SecureDIFO wurde mit zwei Monaten angesetzt.

Die Kosten des Projekts betrugen ca. drei Millionen Euro und nach drei Jahren hatten sich diese Kosten bereits amortisiert. Die Kosten für die zertifizierten Labore, die Abzüge von den analogen Fotografien anfertigen, konnten um 80 % reduziert werden, da nur noch eines der ehemaligen fünf Labore weiterbetrieben werden muss.

6.3.7 Vorgehen und Umsetzung

Die Projektplanung begann mit der Zusage der Haushaltsmittel im Februar 2004, im April erfolgte die Ausschreibung des Projekts und im September der Zuschlag. Die Anpassung der Software von itWatch startete mit Oktober 2004. Im Februar 2005 konnten bereits die ersten Piloten des Modells eingeführt werden. Im selben Jahr fanden die Piloten noch flächendeckenden Einsatz und im März 2006 erfolgte schließlich der vollständige Roll-out.

Das Projektmanagement der Polizei wurde von einem erfahrenen Projektleiter übernommen. Dieser erwies sich bei der Implementierung der digitalen Fotografie als professionell, ziel- und kostenorientiert. Sowohl Planung als auch Eskalationsmanagement werden als beispielhaft angesehen. Neben dem DiFo-Projekt mussten Testlabore und Testumgebungen für funktionale Abnahmetests eingerichtet und die Versorgung der Dienststellen mit Windows XP sichergestellt werden.

Die Umsetzung des Projekts selbst erfolgte mittels Friendly-User-Tests. Kleinere Einheiten von geschulten Polizeibeamten wurden mit dem System gekoppelt.

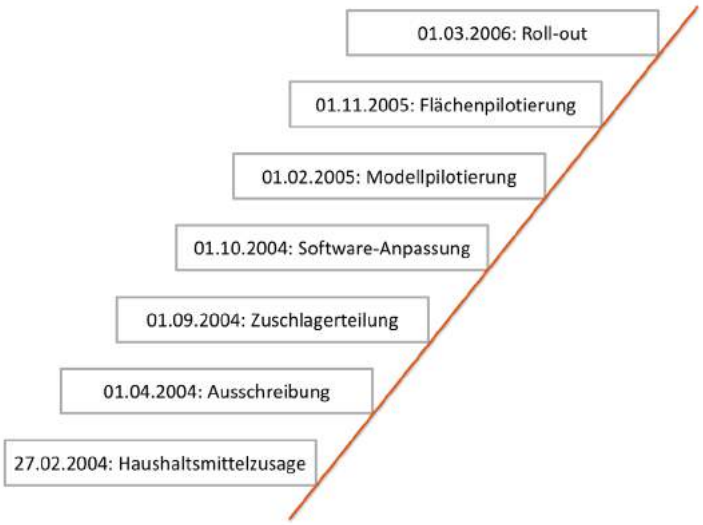


Abbildung 6-5: Projektplanung des DiFo-Projektes

Die Einführung der digitalen Fotografie ermöglichte die Ablösung der Prozesse für die analoge Erstellung, Speicherung und Verwaltung von Bildern durch einen integrierten digitalen Prozess.

Die vorhandene Systemarchitektur wurde durch DiFo im Hinblick auf die Server- und Datenbankarchitektur erweitert. Die Anwendungslandschaft wurde um die Bildbearbeitungssoftware sowie die Bildverwaltung mittels Webinterface ergänzt.

Die Schulung auf das neue System erfolgte in einem vierstufigen Multiplikatorensystem. Zunächst wurden die Fachlehrer des Fortbildungsinstituts der Bayerischen Polizei durch externe Referenten über drei Tage geschult. Für die nächsten beiden Ebenen dauerten die Schulungen einen Tag bzw. drei Tage. Hier waren pro Dienststelle mindestens zwei Multiplikatoren vorgesehen. Die Mitarbeiter der Ebene drei schulten die Endanwender ihrer Dienststellen in individuell ausgerichteten Workshops und Dienstunterrichten von ca. zwei Stunden.

6.3.8 Projektergebnis

Ergebnis des Projekts ist ein bayernweiter, neuer digitaler Standardprozess für die Verarbeitung und Verwaltung von digitalen Fotografien in der Polizeiarbeit. Dieser Prozess wurde konzeptioniert, umgesetzt und für alle Dienststellen der Polizei in Bayern eingeführt. Das Projekt gilt allgemein als ein Erfolg.

Trotzdem gibt es noch Potenziale für weitere sichere digitale Prozesse. Während es für die digitale Fotografie ein bayernweites Standardverfahren gibt, gibt es keinen Standard für die Übergabe von digitalen Bildern von Privatpersonen an die Polizei, bspw. bei einer Anzeige oder wenn Bürger Handybilder von Verbrechen als Beweis übergeben möchten. Die Dienststellen lösen in individuellen Verfahren, wie ihnen Bürger Bilder als Beweismaterial übergeben können. Weitere vergleichbare Folgeprojekte wie z. B. ein digitaler Prozess für Audiomaterial wurden bisher nicht umgesetzt.

6.4 Erfolgsfaktoren

Die digitale Fotografie wurde, zu dem Zeitpunkt, zu dem diese Fallstudie verfasst wurde, bereits seit mehreren Jahren in den Prozessen der Polizeiarbeit der Bayerischen Polizei erfolgreich genutzt und ist auch unter Windows 8 identisch im Einsatz. Das Projekt wird als durchweg positiv angesehen. Die IT-Sicherheit hat in diesen Jahren nie eine auffällige Rolle gespielt; es wurden keine IT-Sicherheitsvorfälle verzeichnet.

Der wesentliche Erfolgsfaktor des Projektes ist sicherlich die einfache Nutzbarkeit für die Anwender. Der Polizeibeamte kann ohne wahrnehmbare Einschränkungen jedes Medium als Quelle für gerichtsfeste, digitale Tatortfotografien nutzen, dabei durchläuft der Vorgang weder langwierige Genehmigungsverfahren noch ist der ursprüngliche Vervielfältigungsaufwand für die Weitergabe von Bildern oder Akten im Rahmen der Polizeiarbeit nötig. Gleichzeitig sind alle Anforderungen an die IT-Sicherheit gewahrt, was in diesem Fallbeispiel eine kritische Voraussetzung ist.

Es konnte ein neuer, bayernweiter Standardprozess mithilfe von DeviceWatch definiert werden und es wurde nicht der bestehende „analoge" Prozess der Fotografie übernommen.

Im Bereich der Projektplanung und -durchführung waren die effektive Zusammenarbeit innerhalb des Projektes und vor allem die herausragende Rolle des Projektleiters ein Schlüssel zum Erfolg. Dieser hat nicht nur alle Stakeholder frühzeitig in die Planung mit einbezogen, sondern der Rolle der IT-Sicherheit von Beginn besondere Aufmerksamkeit beigemessen.

Das Projekt DiFo kann deshalb als Referenz für andere IT-Projekte von KRITIS-Betreibern gelten. Vorzugsweise ist hier nicht nur die Projektplanung an sich, sondern vor allem auch die Einbeziehung der IT-Sicherheit im gesamten Projektverlauf hervorzuheben.

6.5 Danksagung

Wir danken dem Bundesministerium für Bildung und Forschung (BMBF) für die Möglichkeit der Forschung im Rahmen des Projektes VeSiKi, Förderkennzeichen 16KIS0213K.

6.6 Literaturverzeichnis

Metzger, F., 2004. Digitale Fotografie bei der Bayer. Polizei. Polizei in Bayern, S. 30–35.

Metzger F.; Wust, W., 2006. Digitale Fotografie, in: Polizeikongress, Bad Homburg.

7 Die Kliniken des Bezirks Oberbayern: Ausgewogenes Risikomanagement für nachhaltige Sicherheit

Toni Kehr, Universität der Bundeswehr München
Sebastian Dännart, Universität der Bundeswehr München

Der Schutz der Patientendaten in Kliniken ist ein wichtiges Thema in der IT-Sicherheit. Die Kliniken des Bezirks Oberbayern haben im Rahmen einer laufenden Aktivität zur Erhöhung der IT-Sicherheit auf eine Bedrohung der IT-Sicherheit durch Ransomware kurzfristig reagiert und diesen Impuls in eine nachhaltige Steigerung der IT-Sicherheit und des Bewusstseins für IT-Sicherheit umgesetzt. kbo (Kliniken des Bezirks Oberbayern) setzt dabei auf eine Strategie des ausgewogenen Risikomanagements in der IT-Sicherheit. Wichtige Elemente des IT-Sicherheitsmanagements sind ein multiprofessionelles IT-Sicherheitskomitee mit Prozessen, die externe Kompetenzen einbinden, Verantwortungsdruck für Mitarbeiter vermeiden sowie schnelle, transparente Entscheidungen von IT und Anwendern gemeinsam ermöglichen.

Keywords: Sektor Gesundheit, Branche Medizinische Versorgung, Ransomware, IT-Sicherheitsmanagement, Risikomanagement

7.1 Unternehmen

7.1.1 Unternehmensprofil

kbo ist ein Verbund von ambulanten und stationären Einrichtungen, die seit 2007 als Kommunalunternehmen zusammenarbeiten. Mit 6.700 Mitarbeitern werden jährlich 110.000 Patienten stationär, teilstationär und ambulant behandelt, gepflegt und betreut. An den über 22 Standorten umfassen die medizinischen Leistungen neben Psychiatrie, Psychotherapie, Psychosomatik auch Neurologie und Sozialpädiatrie für Kinder, Jugendliche und Erwachsene. Dafür stehen in den Kliniken des Unternehmensverbundes insgesamt 3.000 Betten zur Verfügung. Zur kbo gehört auch eine forensische Psychiatrie mit 200 Maßregelvollzugsbetten.

Die gemeinnützigen GmbHs kbo-Isar-Amper-Klinikum, kbo-Inn-Salzach-Klinikum, kbo-Heckscher-Klinikum, kbo-Kinderzentrum München, kbo-Sozialpsychiatrisches Zentrum, Ambulante Psychiatrische Pflegedienst München und die kbo-Lech-Mangfall-Kliniken werden als Tochtergesellschaften geführt. Darüber hinaus ist das Kommunalunternehmen Mitgesellschafter des Autismuskompetenzzentrums Oberbayern gGmbH, der kbo-Service GmbH und Anteilseigner (51 %) der IT des Bezirks Oberbayern GmbH.

Die IT des Bezirks Oberbayern GmbH erbringt Managementleistungen in den Bereichen Informations- und Kommunikationstechnik – sowohl für den Bezirk Oberbayern, seine Eigenbetriebe, kameralen Einrichtungen und Dienststellen als auch für das Kommunalunternehmen und seine Tochtergesellschaften. Die strategische Steuerung der IT aller Tochtergesellschaften liegt bei der IT GmbH. Hier werden Vorgaben und Anforderungen an die IT entwickelt und die Umsetzung der Vorgaben an die IT und vor allem auch im Themenfeld

IT-Sicherheit kontrolliert. Das Verbundrechenzentrum der kbo, das am kbo-Isar-Amper-Klinikum angesiedelt ist, ist für den operativen Betrieb und für die produktive Sicherheit zuständig. Diese Struktur realisiert ein ausgewogenes Risikomanagement und hilft, ein einheitliches Niveau im IT-Betrieb mit einheitlichen Strukturen und in der IT-Sicherheit darzustellen und von Synergieeffekten gerade in der Beschaffung zu profitieren. Die IT-Governance, also die strategische Steuerung, ist vom IT-Betrieb getrennt.

7.1.2 Strategische Ausrichtung

Die IT-Strategie der Kliniken des Bezirks Oberbayern und der IT des Bezirks Oberbayern GmbH richtet sich an der Gesamtstrategie aus. Ein Leitbild beschreibt diese Gesamtstrategie:

> **„Was uns wichtig ist**
> *Wir gehen auf die persönlichen und vielfältigen Lebenssituationen der Menschen ein. Patienten, Klienten und Mitarbeiter erfahren Achtung, Wohlwollen und Anerkennung. Wir handeln verantwortungsvoll, arbeiten offen, glaubwürdig und verlässlich zusammen und gehen konstruktiv mit unseren Fehlern um. So lernen wir voneinander und miteinander, um uns stetig zu verbessern.*" (kbo 2012)
>
> **„Wo wir hinwollen**
> *Wir streben eine erfolgreiche Zukunft an, damit wir den Bedürfnissen der Menschen in einer sich ändernden Gesellschaft gerecht werden.*
> *Wir wollen zukunftsfähige Einrichtungen und Behandlungskonzepte mit einer ausgewogenen und nachvollziehbaren Finanzplanung, dabei prägt Nachhaltigkeit unsere Entscheidung.*
> *Wir wollen eine flexible Arbeitsplatzgestaltung, damit wir auf individuelle Lebenssituationen des Mitarbeiters eingehen können, denn zufriedene und motivierte Mitarbeiter sind der Schlüssel für unseren Erfolg.*" (kbo 2012)

Die Strategie der IT wird in der IT des Bezirks Oberbayern GmbH festgelegt und unterstützt die Gesamtstrategie der Träger. Im Themenfeld des Klinikverbundes bedeutet das für den Vorstand der kbo: „IT ist wichtig und IT-Sicherheit ist noch wichtiger!". So werden alle IT-Maßnahmen an den Notwendigkeiten der medizinischen Behandlung ausgerichtet. Bewusst sind viele der Prozesse und auch Teile der Patientenakten noch analog, denn für Patienten von kbo kann IT einen Faktor darstellen, der der Behandlung nicht förderlich ist und so ist außer gewöhnlichen Bildschirmen keine IT im Patientenbereich sichtbar. Aller Einsatz von IT wird an dem Datenschutz und den Bedürfnissen der Patienten ausgerichtet: Personenbezogene Daten, welche z. B. mit dem medizinischen Dienst der Krankenkassen ausgetauscht werden müssen, werden ausschließlich auf einem verschlüsselten Kommunikationskanal ausgetauscht.

Die Träger von kbo müssen die Ressourcen für die IT und die IT-Sicherheitsmaßnahmen freigeben.

7.1.3 Fallstudienpartner

Name	Position im Unternehmen
Nikolaus Schrenk	Datenschutzbeauftragter, kbo
Matthias Lehner	IT-Sicherheitsbeauftragter, kbo
Toni Kehr	Studierender der Wirtschaftsinformatik, Universität der Bundeswehr München
Sebastian Dännart	Wissenschaftlicher Mitarbeiter, Universität der Bundeswehr München
Tamara Gurschler	Wissenschaftliche Mitarbeiterin, Universität der Bundeswehr München

7.1.4 IT-Sicherheit im Unternehmen

Der Schutz der Patientendaten ist das oberste Gebot bei kbo und auch bei dem IT-Dienstleister „IT des Bezirks Oberbayern GmbH". Das Gesamtsystem mit seinen Schnittstellen zu anderen Unternehmen, wie Banken oder Apotheken für beispielsweise Gehaltsabrechnungen und Medikamentenbestellungen, muss geschützt sein.

Ein IT-Sicherheitskomitee ist das Bindeglied zwischen der IT, dem Anwender und dem Konzernvorstand und setzt sich aus Vertretern der verschiedenen Funktionsbereiche des Unternehmens zusammen. Mitglieder sind der Geschäftsführer IT, der IT-Compliance Officer und die drei Bereichsleiter der Bereiche Service-Management, Applikationen und Infrastruktur sowie der Datenschutzbeauftragte und der IT-Sicherheitsbeauftragte. Das IT-Sicherheitskomitee trifft Entscheidungen zur IT-Sicherheit immer gemeinsam mit IT und Anwendern. Im Fall von Cyberangriffen werden im IT-Sicherheitskomitee die Maßnahmen abgestimmt und freigegeben.

Grundlage für viele Entscheidungen im Themenfeld IT-Sicherheit bilden die unternehmensweit eingeführten und zertifizierten Grundkomponenten von ISO 27001, ITIL sowie eine für das Gesundheitswesen adaptierte Variante von COBIT 5. COBIT 5 dient hier den Standards aus ITIL und ISO 27001. Als IT-Sicherheitsmaßnahme wurde ein „Anforderungskonzept an die IT-Sicherheit" mit Teilen der Rahmenwerke, der Norm (ISO 27001) sowie einem IT-Grundschutz-Katalog vom BSI erstellt. Die Sicherheitsanforderungen werden mindestens einmal jährlich überprüft und dies wird durch den IT-Sicherheitsbeauftragten kontrolliert. Jährlich erfolgt zudem ein Penetrationstest: Ein externer Dienstleister wird beauftragt, die Firewall zu überwinden und an die Unternehmensdaten (u. a. Patientendaten) zu gelangen.

Der IT-Sicherheitsbeauftragte von kbo definiert das IT-Sicherheitskonzept und legt damit auch wichtige Aspekte des Risikomanagements fest. Das IT-Sicherheitskonzept wird durch den Vorstand freigegeben. Dieses Risikomanagement basiert auf Prozessen und Controls von COBIT.

7.2 Kritische Infrastruktur

7.2.1 Einordnung als KRITIS

Als Verbund von Einrichtungen des Gesundheitswesens lässt sich kbo dem Sektor „Gesundheit" und der Branche „Medizinische Versorgung" als Kritische Infrastruktur zuordnen. Die

Rechtslage sieht entsprechend dem IT-Sicherheitsgesetz mit der KRITIS-Verordnung (BSI 2016a) einen Schwellenwert von 30.000 stationären Fällen pro Krankenhaus für Kritische Infrastrukturen vor. kbo erreicht diesen Schwellenwert nur im Verbund und wird daher nach dem IT-Sicherheitsgesetz und der KRITIS-Verordnung nicht als KRITIS-Betreiber angesehen. Bereiche, wie die Forensik (Maßregelvollzug) mit über 200 Betten, können nicht einfach von anderen Kliniken oder Institutionen übernommen werden, daher sieht sich kbo jedoch selbst als Kritische Infrastruktur und die IT würde sich auch eine gesetzliche Anerkennung als KRITIS wünschen. Es wäre ein wichtiges Signal an die Bevölkerung, dass der Staat die Sicherheit beispielsweise der Forensik kontrolliert. Es wäre auch ein wichtiges Signal an die Träger von kbo, die für IT-Sicherheitsmaßnahmen notwendigen Ressourcen bereitzustellen.

7.2.2 Risikoanalyse

Als Verbund von ambulanten und stationären Einrichtungen und Klinken kommt kbo eine besondere Rolle zu. Können chirurgische Eingriffe oftmals von anderen Kliniken übernommen werden, so stoßen konventionelle Krankenhäuser und staatliche Institutionen bei einer geschlossenen Unterbringung und dem Maßregelvollzug an ihre Grenzen. Patienten im Maßregelvollzug bedürfen nicht nur einer speziellen Betreuung, sondern auch einer separaten Unterbringung, da Fremd- und Eigengefährdung vorliegen können. Müsste beispielsweise der Maßregelvollzug geräumt werden, so wäre eine Unterbringung der Patienten im Raum München nur in Kooperation mit staatlichen Institutionen möglich.

Für kbo selbst gibt es verschiedene Abhängigkeiten von Kritischen Infrastrukturen: Der Verbund kbo verfügt nur über begrenzte Vorräte an Medikamenten und Medikamentenbestellungen werden online durchgeführt. Somit ist kbo nicht nur auf Laboreinrichtungen, sondern auch auf Apotheken und Transportdienstleister angewiesen. Fällt die Versorgung mit Strom durch Energieversorger aus, so kann es z. B. im Bereich des Maßregelvollzuges zu starken Beeinträchtigungen kommen, denn die gesicherten Türen der Patientenzimmer müssten trotz Notstromversorgung mit einem Schlüssel jeweils einzeln geöffnet werden.

Das IT-Sicherheitsgesetz (Bundesgesetzblatt 2015) und auch gesetzliche Regelungen zur Verschwiegenheitspflicht von Ärzten und medizinischen Einrichtungen (§ 203 StGB) erfordern, dass alle Patientendaten besonders geschützt sind.

Im Jahr 2016 hat sich die Bedrohungslage augenscheinlich für kbo verändert. Verschiedene Institutionen wie Universitäten, Behörden und eben Krankenhäuser, sowohl in Deutschland als auch international, werden mit Ransomware angegriffen. Die Patientendaten sind damit deutlich stärker gefährdet, als das bis vor Kurzem angenommen werden konnte. Bisher galten E-Mail-Anhänge und Social Engineering als wesentliche Angriffsvektoren und bei dem Ransomware-Angriff von 2016 war der Angriffspfad zunächst unklar.

7.3 Projekt

7.3.1 Beschreibung

kbo hatte bereits mit der Planung und Umsetzung von Maßnahmen zur Erhöhung der IT-Sicherheit begonnen, als im Februar 2016 ein Krankenhaus in Neuss von Ransomware betroffen war (Borchers 2016). In Reaktion auf Informationen über diesen Vorfall wurden mehrere Maßnahmenpakete kurzfristig beschlossen und umgesetzt. Damit konnte auch eine nachhaltige Verbesserung der IT-Sicherheit erreicht werden.

7.3.2 Projektziel

Mit Unterstützung des Vorstandes von kbo sollten gezielte zweckgerichtete Maßnahmen ergriffen werden, um die IT-Sicherheit im Unternehmen zu erhöhen, da die implementierten Schutzmaßnahmen nicht mehr State of the Art waren und vor allem der veränderten Risikosituation nicht gerecht wurden.

Zur Erhöhung der IT-Sicherheit sollten die interne Organisation und IT-relevante Sicherheitsvorgänge überprüft und gegebenenfalls geändert werden. Möglichkeiten für Gegenmaßnahmen standen ebenso auf der Agenda wie ein Upgrade der IT-Infrastruktur mit Hardware und Software.

7.3.3 Geschäftssicht

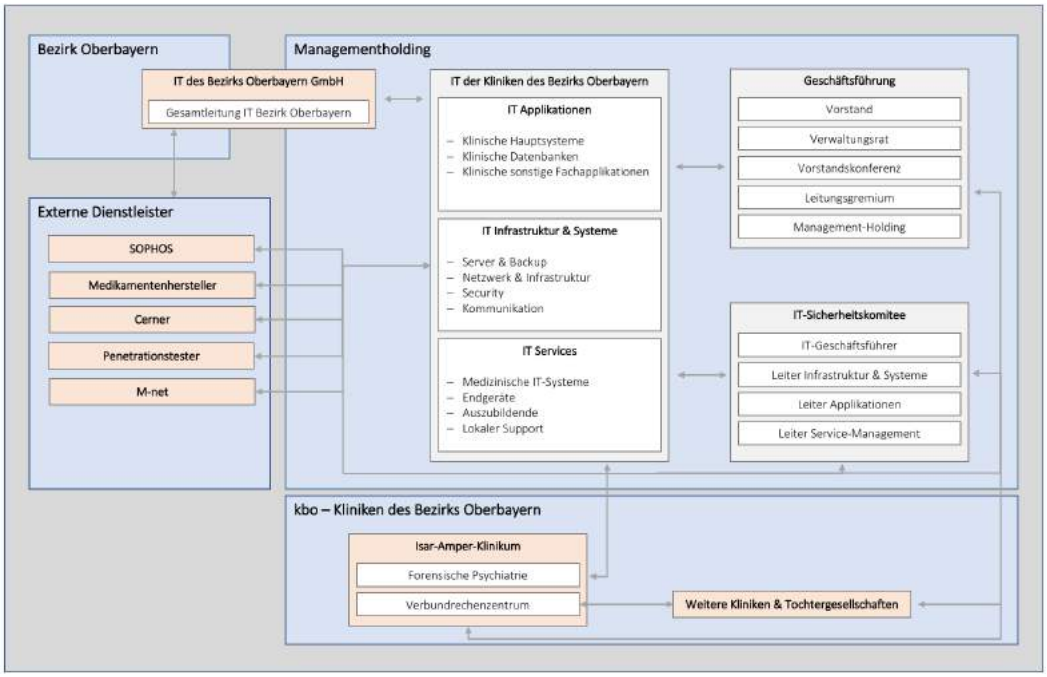


Abbildung 7-1: Sicht auf die IT-relevanten Geschäftsbereiche von kbo

Die Grundstruktur der Verwaltung und anderer Funktionsbereiche von kbo entspricht der Grundstruktur von kommunalen Krankenhauskonzernen: Es gibt eine Geschäftsführung mit Vorstand, Verwaltungsrat, Vorstandskonferenz und Leitungsgremium innerhalb der Management-Holding. Eine Besonderheit stellt die Struktur des IT-Betriebs dar (Abbildung 7-1):

Die „IT des Bezirks Oberbayern GmbH" bündelt den IT-Betrieb des Bezirks Oberbayern mit seinen kameralen Einrichtungen und den Kliniken. Die IT strukturiert sich in IT-Applikationen, IT-Infrastruktur & Systeme und IT-Services. Am kbo-Isar-Amper-Klinikum sind u. a. eine Forensische Psychiatrie und das Verbundrechenzentrum für die Kliniken der kbo angesiedelt.

Die Abteilung „IT Applikationen" ist für die klinischen Hauptsysteme, klinischen Fachapplikationen und klinischen Datenbanken zuständig. Die Fähigkeiten der Mitarbeiter werden in einer Skill-Level-Matrix geführt und dem Training-on-the-Job kommt eine zentrale Rolle zu.

Die Abteilung „IT Infrastruktur & Systeme" betreut Server und Backups und auch die zentrale Firewall von kbo. Zum Aufgabenbereich gehören Netzwerke und Infrastruktur sowie Security und Kommunikation.

Die Abteilung „IT Services" betreut medizinische IT-Systeme und Endgeräte und sorgt für den Vor-Ort-Support. Die Ausbildung von Auszubildenden ist diesem Bereich angegliedert und in diesem Bereich erfolgt die IT-Koordination mit den Kliniken.

Das IT-Sicherheitskomitee ist direkt unter dem Vorstand verankert und übernimmt die Bewältigung von IT-Vorfällen in der Organisation.

Das kbo-Isar-Amper-Klinikum agiert mit dem Verbundrechenzentrum als Schnittstelle zwischen der IT und den Anwendern in den weiteren Kliniken und Tochtergesellschaften.

7.3.4 Prozesssicht

Das Changemanagement und die Überprüfung von E-Mails mit ihren Anhängen sind zwei zentrale Prozesse im IT-Sicherheitsmanagement von kbo.

Change Management für IT-Sicherheitsmaßnahmen

Wie in Abbildung 7-2 dargestellt, werden Entwicklungen und Vorschläge zu Änderungen im Zusammenhang mit IT-Sicherheitsvorfällen in Form von Änderungsanträgen eingereicht und bearbeitet. Ein Antrag wird sowohl von der IT selbst, dem IT-Sicherheitskomitee als auch von den beteiligten externen Dienstleistern bewertet und letztendlich genehmigt. Sollte nur eine Partei dem Antrag nicht zustimmen, erfolgt keine Freigabe und der Änderungsantrag würde dann überarbeitet und neu eingereicht werden müssen.

Dieser Prozess bezieht mehrere Parteien in die Entscheidung mit ein und soll die Gefahr von Fehlentscheidungen verringern. Besonders die externen Dienstleister sind Experten auf ihrem Gebiet und kennen Anforderungen ebenso wie technische Entwicklungen. Mit dem IT-Sicherheitskomitee hat die Expertise der verschiedenen Anspruchsgruppen zum Thema IT-Sicherheit im Changemanagement-Prozess eine gleichberechtigte Rolle zu IT und zu den IT-Dienstleistern.

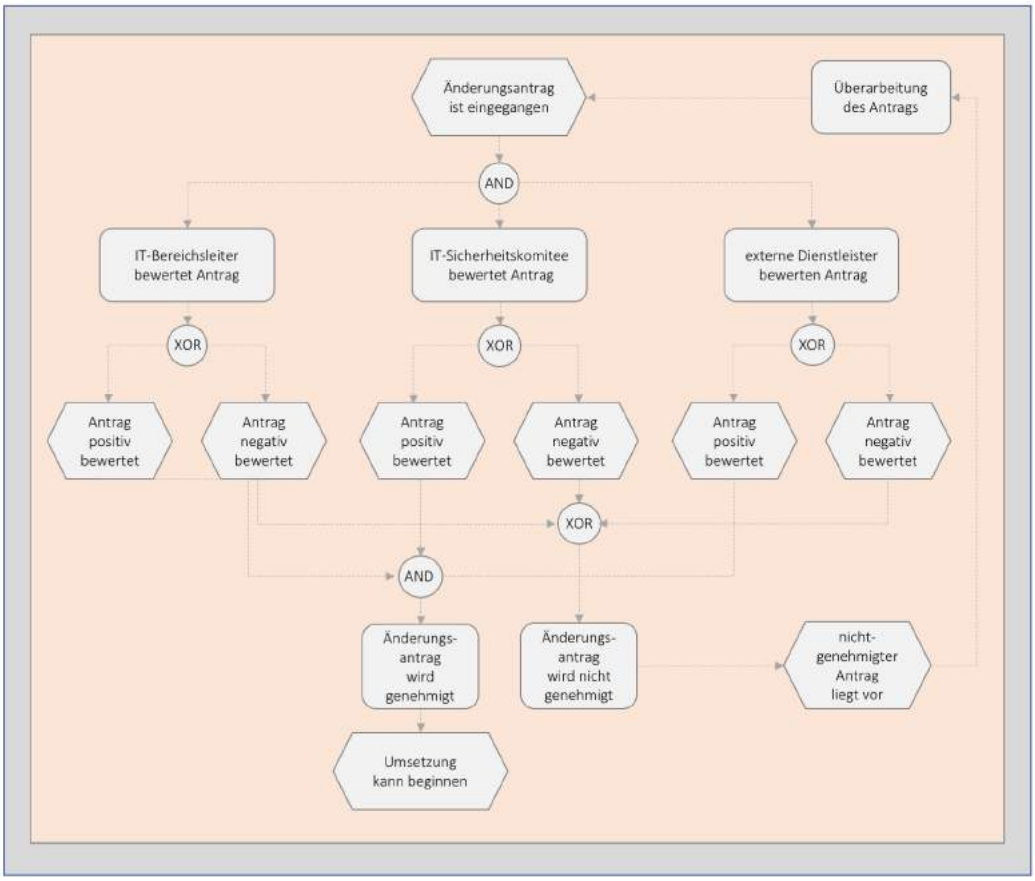


Abbildung 7-2: Changemanagement-Prozess für Änderungsanträge in der IT-Sicherheit

E-Mail-Überprüfungsprozess

In der Reaktion auf die geänderte Risikolage wurde ein Prozess definiert (Abbildung 7-3), der das Risiko von E-Mails und Anhängen reduziert.

Bevor E-Mails in das interne Netz von kbo gelangen, wird von MNet Email Relay ein ReCheck vollzogen. Dabei gehen alle E-Mails zunächst an den Herkunftsserver zurück und werden bei Spam-Mails in der Regel nicht noch einmal zugestellt. Somit werden hier bereits 90 % der E-Mails als Spam erkannt und herausgefiltert. Vor der Übergabe an das interne E-Mailsystem wird eine Verschlüsselungsprüfung in der Demilitarisierten Zone (DMZ) durchgeführt. Erst wenn diese erfolgreich war und noch vor der Zustellung der E-Mail wird der Anhang darauf überprüft, ob die Dateien die erlaubten Formate wie PDF, MS Office oder Ähnliches erfüllen. Bei Bedarf wird der Anhang in einem Schleusen-PC mit drei zusätzlichen Virenscannern überprüft. Wenn diese Virenscanner keine Schadsoftware entdecken, können die Anhänge den Empfängern zugehen. Schlagen hingegen die Scanner an, so wird die Mail aus der Quarantäne gelöscht und der Empfänger informiert.

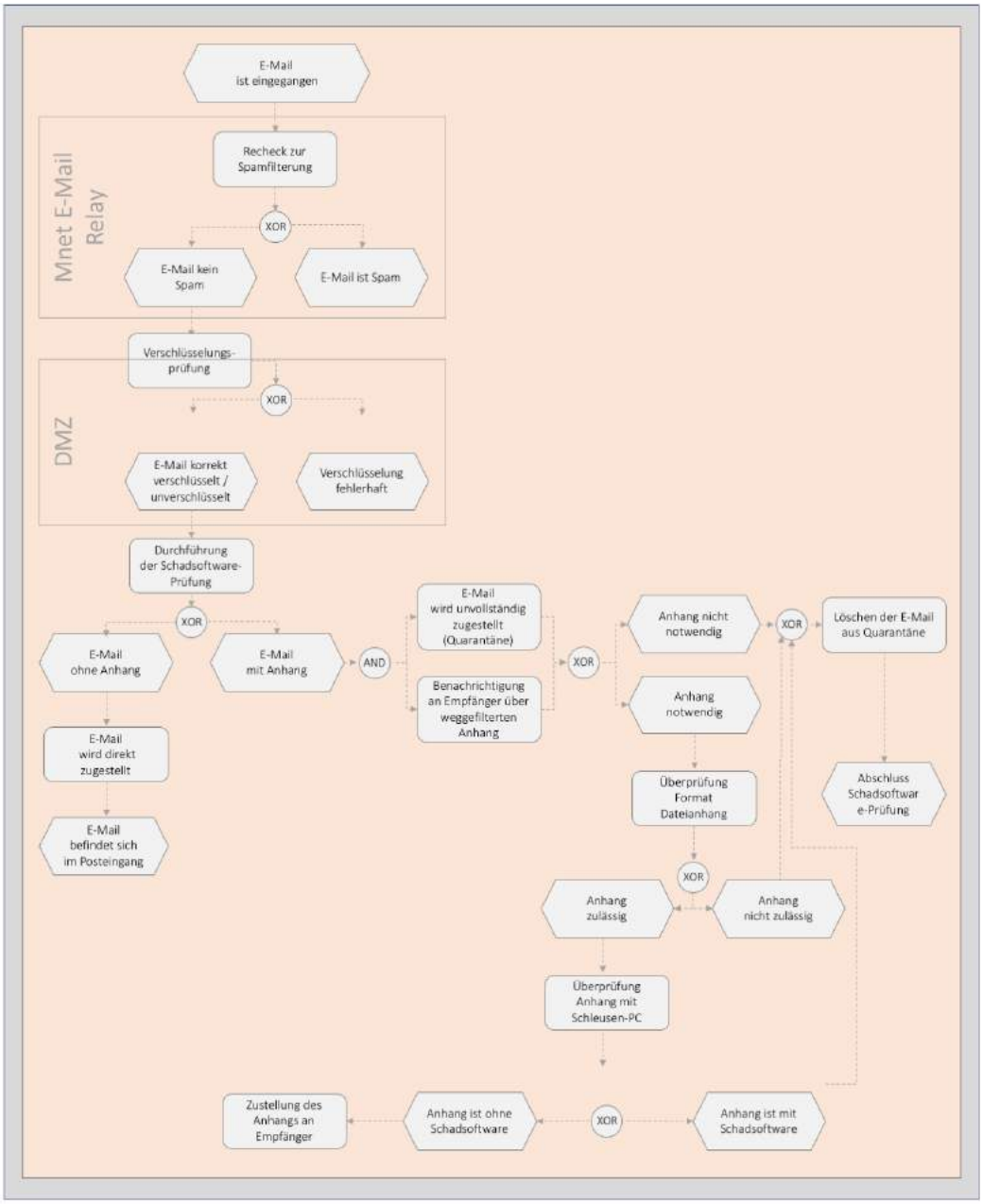


Abbildung 7-3: Überprüfungsprozess für E-Mail-Anhänge

Dieses Verfahren schützt vor Angriffen über E-Mails und besonders Fake-Bewerbungen sind immer wieder Träger von Schadsoftware. kbo sucht laufend neue Mitarbeiter und Initiativbewerbungen sind üblich und daher ist dieser Prozess sinnvoll, um einerseits Bewerbungen und andere Dokumente in E-Mails zuzulassen und andererseits den notwendigen Schutz von kbo

zu realisieren. Aufgrund anderer Prozesse müssen Makros in Office-Dateien erlaubt bleiben. Als langfristige Lösung ist hier die Nutzung signierter Makros angedacht. Darüber hinaus soll zukünftig in der DMZ zusätzlich ein Geoblocking stattfinden, um weitere Sicherheit zu gewährleisten.

7.3.5 Anwendungssicht

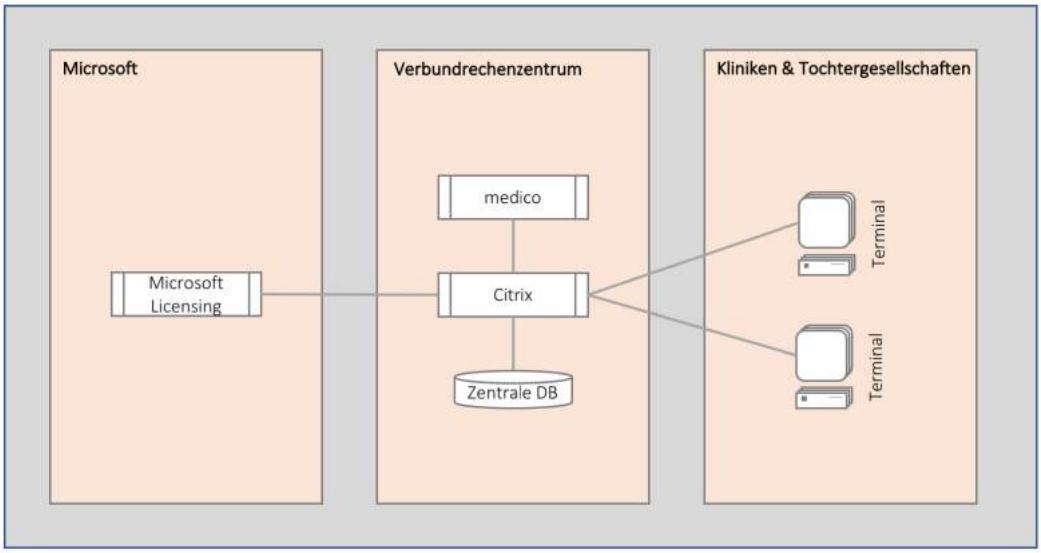


Abbildung 7-4: Anwendungssicht von kbo

Wie in Abbildung 7-4 dargestellt, hostet das Verbundrechenzentrum das Krankenhausinformationssystem (KIS) der Firma Cerner medico sowie weitere Anwendungen und zentrale Datenbanken. Das KIS hat einen großen Funktionsumfang und deckt das notwendige Leistungsspektrum ab. Es wurde speziell für den deutschen Markt entwickelt und seine Stärke ist die Möglichkeit, weitere Drittsysteme anzubinden (Cerner 2016). Über die Citrix-Umgebung werden bei kbo alle Daten und Anwendungen verteilt.

Die Kliniken des Bezirks Oberbayern setzen durchgängig Windows-Produkte und SQL-Server mit Windows ein. Die Windows-Produkte werden über ein Microsoft Licensing Enterprise Agreement bereitgestellt.

7.3.6 Technische Sicht

Die Kliniken des Bezirks Oberbayern betreiben, wie in Abbildung 7-5 dargestellt, ihr eigenes Verbundrechenzentrum am Standort des kbo-Isar-Amper-Klinikums in Haar. Mitarbeiter der Kliniken der kbo sowie Tochtergesellschaften greifen auf die virtuellen Server zu – es nutzen 70 % Thin Clients und 30 % Fat Clients.

Das Verbundrechenzentrum ist der zentrale Speicherort für kbo und das Verbundrechenzentrum erstellt regelmäßig Backups, dazu dient eine zentrale Datenbank. Als kurzfristiges

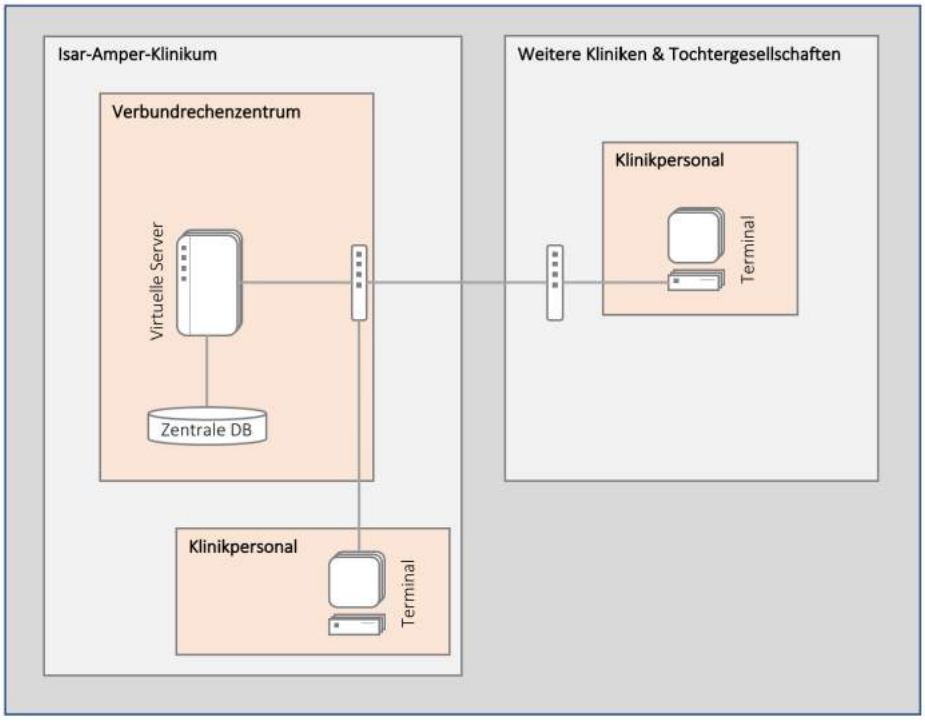


Abbildung 7-5: Sicht auf die technische Landschaft von kbo

Speicherverfahren verwendet man NetApp. Disk-to-Disk-to-Tape (D2D2T) bildet als Langzeitspeicherverfahren das Pendant dazu. Für klinische Anwendungen wie das KIS medico wird Disk-to-FAST LTA verwendet.

7.3.7 Umfang und Zeitraum

Finanzierung von IT-Sicherheit ist in öffentlichen Institutionen ein sensibles Thema – so müssen Investitionen in IT und IT-Sicherheit mit Trägern ausgehandelt werden. Im Rahmen des Möglichen wurden Mittel bereitgestellt, um die IT-Sicherheit in kbo zu erhöhen. In der ersten Hälfte des Jahres 2016 konnten mehrere Maßnahmenpakete realisiert werden. Die Einrichtung des multiprofessionellen IT-Sicherheitskomitees, als ein Hauptaugenmerk, wird beispielsweise im Budget nicht festgehalten und lässt sich so kaum beziffern.

Dabei war die geänderte Risikowahrnehmung nach den Ransomware-Vorfällen stets ein Treiber, jedoch nicht der alleinige Auslöser dafür, dem Ziel der IT-Sicherheit einen höheren Stellenwert zukommen zu lassen.

7.3.8 Vorgehen und Umsetzung

Zu Beginn des Jahres 2016 begann mit der Erhöhung des IT-Sicherheitslevels. Es wurde begonnen eine neue Firewall zu implementieren. Zudem wurde das IT-Sicherheitskomitee ein-

gerichtet. Weitere Maßnahmen sollten Schritt für Schritt ausgeplant und umgesetzt werden.

Der Angriff mit Ransomware auf Krankenhäuser war vier Wochen später im Februar 2016 Anlass für kbo, das Sicherheitsniveau kurzfristig zu erhöhen und IT-Sicherheitsmaßnahmen sofort vorzunehmen bzw. geplante IT-Sicherheitsmaßnahmen vorzuziehen.

Auf Grundlage der bedenklichen Situation eines den Kliniken der kbo vergleichbaren Krankenhauses wurde sofort vom IT-Geschäftsführer das IT-Sicherheitskomitee einberufen und es wurden parallel Informationen zum Angriffsvektor gesammelt. Ziel war es, geeignete Maßnahmen zu treffen. Das Risiko, dass das betroffene Krankenhaus in Neuss nicht das einzige Ziel sein könnte, wurde als realistisch eingeschätzt – speziell nachdem auch in Bayern ein Fall von Ransomware bekannt wurde. Keinesfalls sollten die gleichen Auswirkungen wie in dem betroffenen Krankenhaus – Entlassung von Patienten, Arbeiten wie vor 20 Jahren (u. a. handschriftliche Dokumentation von Patientenakten) etc. – auftreten.

Es wurden Informationen zum Angriff mit Ransomware eingeholt: Es handelte sich um einen Angriff mittels Schadsoftware-behafteten E-Mail-Anhängen. Nach den Erstmaßnahmen, wie der Abschaltung der Internetverbindung und der kompletten Sperrung des E-Mail-Systems, wurde als Folgemaßnahme die neue Firewall vier Wochen früher als geplant implementiert.

Des Weiteren wurde durch die IT kommuniziert, dass es einen Cyberangriff auf das Gesundheitswesen gibt und daher keine Internetaufrufe getätigt werden sollten und E-Mail Anhänge nicht geöffnet werden sollten. Durch diese gute Kommunikation war das Verständnis für die Maßnahmen zunächst gegeben.

Am nächsten Tag war diese organisatorische Maßnahme auch technisch umgesetzt und das Internet gesperrt. Binnen eines Werktages wurden diverse Dateiformate im E-Mail-Empfang gesperrt. Es wurden weitere Maßnahmen, wie eine Überprüfung und Aktualisierung des Virenscanners, durchgeführt. Parallel dazu wurde der IT-Sicherheitsdienstleister, der mit den Penetrationstests beauftragt wird, einbezogen. Der Dienstleister überprüft alle IT-Sicherheitsmaßnahmen z. B. auf Konfigurationen und Parametereinstellungen, bevor das IT-Sicherheitskomitee eine Maßnahme freigibt.

Die Sperrung des Internet musste nach zwei Tagen auf Druck der Anwender wieder aufgehoben werden: Die gesamte automatische Serverkommunikation, wie Medikamentenbestellungen und Gehaltsüberweisungen, war nicht mehr möglich und Informationen für Behandlungen konnten nicht mehr eingeholt werden. Die IT-Dienstleister konnten auf Nachfrage jedoch keine 100%-Schutzmaßnahmen gegen Ransomware anbieten. Der Angreifer in Neuss nutzte Zero-Day-Exploits, um die Infrastruktur zu infizieren, und Gegenmaßnahmen waren für kbo zu dieser Zeit nicht verfügbar. Daher mussten intern organisatorische und technische Maßnahmen erarbeitet werden.

> *„Wenn es die Profis in der IT-Sicherheit nicht schaffen, den Angriff mit den Schutzsystemen zu verhindern – wie können wir uns trotzdem schützen?“*
>
> *– Leiter Governance Consulting kbo*

Eigene IT-Sicherheitsanalysen wurden durchgeführt und ergaben, dass vor allem Systemadministratoren als Ziel von Cyber-Angriffen prädestiniert sind. Um dieses Risiko zu re-

duzieren, wurden die Administrator-Konten vom Internet und von Outlook getrennt. Die Anwenderrechte der Mitarbeiter wurden außerdem mittels eines selbst geschriebenen Skripts überprüft, den Mitarbeitern insbesondere lokale Administratorrechte entzogen und die Anwenderrechte wurden auf die notwendigen Rechte zurückgesetzt.

Bevor man mit kbo wieder online gehen wollte, standen auch die Fernzugänge auf dem Prüfstand. Diesem Thema war bis dato wenig Beachtung geschenkt worden. Das Firmenzugangsverfahren wurde als Schwachstelle identifiziert und die Fernzugänge wurden überprüft, beschränkt und weitere Maßnahmen ergriffen.

Der Druck vonseiten der Anwender, wieder Zugang zum Internet zu erhalten, stieg parallel weiter an, daher wurde das Internet wieder freigegeben – zugleich aber eine strenge Internet-Policy implementiert. Zuerst konnten nur einige bestimmte Seiten auf Antrag hin wieder aufgerufen werden. Das war vor allem für Spezialrecherchen der Ärzte nicht ausreichend. Dann wurde ein Content-Filter eingerichtet und Seiten konnten aufgrund von Blacklists mit Begriffen wie Pornografie, Glücksspiel oder Sexsucht nicht mehr aufgerufen werden. Das erschwerte die Recherchen für Ärzte, denn in der Forensik oder in Suchtzentren sind diese Begriffe elementare Bestandteile der Recherche. Mit dem Verfahren, einzelne Seiten für einzelne Mitarbeiter freizugeben, kam man schnell nicht mehr weiter. Der Druck wurde größer und das Arbeiten stellte sich stellenweise als sehr umständlich dar.

„Wir haben dann die Internet-Policy im größeren Maße wieder aufweichen müssen."
– Datenschutzbeauftragter kbo

Im Zuge der Restriktionen des Zugriffs auf das Internet wurde der Zugriff auf alle aktiven Inhalte untersagt, um Drive-by-Attacken auszuschließen. Dies hatte jedoch zur Folge, dass beispielsweise Webformulare nicht mehr korrekt angezeigt wurden.

Eine weitere wichtige Maßnahme war die Einführung des Überprüfungsprozesses für E-Mail-Anhänge (vgl. Kapitel 7.3.4). Es wurde außerdem festgelegt, dass sich PCs innerhalb von 180 Tagen einmal im Netzwerk anmelden müssen, da ansonsten ihr IT-Sicherheitsschutz (Anti Virus, Microsoft-Updates etc.) nicht mehr aktuell genug wäre und sie eine Gefahr für das Netz von kbo darstellen würden. PCs, die sich mehr als 180 Tage nicht im Netz angemeldet haben, werden gesperrt und müssen manuell unter Beteiligung der IT entsperrt werden.

Nach der Erstbewältigung der Krisensituation entschied sich kbo für die Umsetzung des Maßnahmenkataloges zur Ransomware für Krankenhäuser des BSI (BSI 2016b). kbo setzte diesen Katalog mit 20 technischen Maßnahmen soweit wie möglich um. Der IT-Sicherheitsbeauftragte wurde damit beauftragt, in regelmäßigen Abständen Sonderprüfungen der durchgeführten Maßnahmen vorzunehmen. Diese Überprüfung finden direkt in der IT und damit am Terminal statt. Damit erhielt der Vorstand neben dem Berichtswesen eine weitere, direkte Rückmeldung zu den IT-Sicherheitsmaßnahmen und ihrer Umsetzung.

Die Durchführung einzelner Maßnahmen war für die Mitarbeiter eine Herausforderung – stellenweise fehlte der Überblick und Mitarbeiter der IT wussten teilweise nicht, welche „Knöpfe wo zu drücken sind".

7.3.9 Projektergebnis

Folgende Maßnahmen wurden im Rahmen der Erhöhung der IT-Sicherheit umgesetzt:

- **IT-Sicherheitskomitee in Verbindung mit Changemanagement**: Die wohl wichtigste Maßnahme war die Schaffung des multiprofessionellen IT-Sicherheitskomitees mit Prozessen wie dem Changemanagement im Zusammenhang mit IT-Sicherheitsvorfällen, die Verantwortungsteilung, genaue, schnelle, transparente Prozesse implementiert und dabei den externen IT-Sicherheitsdienstleister einbezieht.
- **Überprüfungsprozess für E-Mail-Anhänge**: Der Prozess sorgt für einen wirkungsvollen Schutz vor Schadsoftware und schützt gegen die üblichen Angriffsvektoren Phishing und Spear-Phishing und auch gegen Fake-Bewerbungen als Träger von Schadsoftware und damit Ransomware. Anhänge mit PDFs und einigen Bauplanformaten können im Gegensatz zu Zip-Files oder Exe-Files in Anhängen zugestellt werden. Die Virenscanner im Schleusen-PC, mit dem Anhänge überprüft werden, schlägt häufig an und trägt zur Vertrauensbildung in die IT im Allgemeinen und die IT-Sicherheitsmaßnahmen bei.
- **Internet-Policy und aktive Inhalt**e: Die Internet-Policy wurde verschärft, jedoch aufgrund von Anforderungen aus den Fachbereichen gelockert. Die Makros für Arztbriefe liegen alle in einem geschützten Bereich und wurden als vertrauenswürdig gekennzeichnet.
- **Sperrung Internetzugriff für Administrator-Konten**: So ist die Gefahr reduziert, dass Administrator-Konten mit Schadsoftware infiltriert werden (beispielsweise über Outlook) und damit direkt das Netzwerks infiziert wird.
- **Management der Fernzugänge:** Der Login in das kbo-Netz von externen Standorten wird überwacht, Zugangskontrollen finden statt und die Zugänge sind auf das Notwendige beschränkt. Es besteht Transparenz darüber, welche medizinischen Geräte Fernzugang z. B. für Wartung benötigen.
- **Maßnahmenkatalog BSI für Krankenhäuser**: Die Expertenempfehlung des BSI wurde, soweit es für kbo machbar war, umgesetzt und gibt so weiteren Schutz vor Schadsoftware.
- **Anwenderrechte**: Mit einem Skript werden die Anwenderrechte überprüft, nicht nötige Anwenderrechte werden entzogen, sodass die Anwenderrechte auf das Notwendige beschränkt sind.
- **PC-Update**: PCs, die sich länger als 180 Tage nicht im Netz von kbo angemeldet haben, werden automatisch gesperrt und müssen durch die IT wieder freigegeben werden. So befinden sich keine Rechner mit veralteten IT-Sicherheitskonfigurationen im Netz.
- **Sonderprüfungen**: Sie stellten den tatsächlichen Stand der Maßnahmen in der IT fest, sodass das IT-Sicherheitskomitee über geplante und genehmigte Maßnahmen zusätzlich zum Berichtswesen Feedback erhält.

Das Abschalten des Internet und die Informationen von dem betroffenen Krankenhaus in Neuss haben die Wichtigkeit der IT für den Betrieb veranschaulicht: Für Unterstützungsprozesse und wieviel Arbeitszeit die IT spart – dass

„ … IT kein Hinderer, sondern auch genauso ein Förderer […] sein kann."
– Datenschutzbeauftragter kbo

Nicht nur den Mitarbeitern im medizinischen Bereich, sondern auch der IT selbst wurde durch das Abschalten des Internet in der Krisensituation bewusst, in welchen Prozessen IT und Internet unverzichtbar sind und welche externen Datenquellen für die Prozesse notwendig sind. Die Key User in den Bereichen hatten viel selbst initiiert und so konnte die Abschaltung des Internet bei den Prozessen für Transparenz sorgen.

Ein Quartal nach dem Auftreten der Ransomware waren die Maßnahmen in den regulären Betrieb überführt und die Arbeitslast der IT-Sicherheitsmaßnahmen stellt sich im laufenden Betrieb als bewältigbar dar.

Dass die Sorge der Kliniken des Bezirks Oberbayern hinsichtlich eines Cyberangriffs nicht unbegründet sein sollte, zeigte sich im September 2016. Seit drei Uhr morgens verzeichnete die IT eine massive Anzahl von Anfragen auf die Firewall. Das war extrem ungewöhnlich für das Krankenhaus. Die neue Firewall war so konfiguriert, dass sie sich im Falle einer Überlast automatisch abschaltet, und so war kbo wieder vom Netz. Die Telekom wurde zurate gezogen, um den Traffic zu analysieren, und konnte diesen Botnetzangriff nach Osteuropa zurückverfolgen. Nach zwei Stunden wurde die Firewall teilweise hochgefahren und in einem durch die Telekom gesicherten Testbetrieb beobachtet. Die Muster des Netzwerkverkehrs entsprachen denen der vorangegangenen Woche und so konnte nach zwei weiteren Stunden in den normalen operativen Betrieb übergegangen werden. Die Mitarbeiter wurden über den Vorfall informiert und IP-Adressen aus dem vermuteten Ursprungsland des Angriffs wurden dauerhaft gesperrt.

Das Bewusstsein für IT-Sicherheit hat sich in kbo sowohl durch die Ereignisse im Februar 2016 als auch durch einen Angriff auf kbo im September 2016 merklich verbessert – Mitarbeiter rufen an, wenn Sie ein IT-Sicherheitsproblem vermuten, aus Versehen einen Anhang oder ein File geöffnet haben, oder senden mögliche Schadsoftware an den IT-Bereich zur Überprüfung auf Schadcode.

Mit der Verwendung von COBIT und der Anlehnung an die Empfehlungen des BSI hat kbo etwa 70 % ISO-27001-Konformität erreicht. Das IT-Sicherheitskomitee dokumentiert das Leben der IT-Sicherheit bei kbo. Zertifiziert wird jedoch aus Kostengründen noch nicht – auch wenn die Organisation als solche bereit für eine Zertifizierung wäre. Ein Teil der ITIL-Prozesse ist implementiert, während vor allem COBIT-Prinzipien, wie eine gesamtheitliche Governance der IT und gemeinsame Verantwortung, realisiert bleiben. So gibt es ein Chief Information Officer (CIO) Board mit einem Medizinischen Direktor, einem Pflegedirektor und den IT-Verantwortlichen (IT-Geschäftsführer oder Datenschutzbeauftragter), das strategische Aufgaben wahrnimmt, während bei der IT-Geschäftsführung die Betriebsverantwortung und die Kostenverantwortung verbleiben. Die Service-Orientierung bleibt ein Thema in Bezug auf Reaktionszeiten und Beschaffungen. In Bezug auf Umsetzung von ITIL oder COBIT werden zunächst keine Weiterentwicklungen angestrebt.

7.4 Erfolgsfaktoren

kbo konnte den Impuls, die IT-Sicherheit zu verbessern, in eine nachhaltige Verbesserung der IT-Sicherheit umsetzen und die Strategie eines ausgewogenen Risikomanagements hat sich in der Praxis bewährt. Die IT-Strategie wird hierbei von einem gemeinsamen Entscheidungsgremium vorgegeben und stellt den organisatorischen Rahmen dar, dieser wird in den einzelnen Abteilungen von der IT dann individuell umgesetzt und realisiert. Durch diese zweistufige Hierarchie kann die finanzielle Argumentation auf einer höheren Ebene erfolgen und lässt den IT-Abteilungen gleichzeitig größtmögliche Freiheit, auf individuelle Bedürfnisse einzugehen.

Wichtig für den Erfolg des Vorhabens, die IT-Sicherheit zu verbessern, war, dass das betroffene Krankenhaus in Neuss, das nicht dem Klinikverbund der kbo angehörte, die Situation – ein erfolgreicher Angriff mit Ransomware auf den laufenden Betrieb – aktiv kommuniziert hat. Dem folgten auch andere von der Ransomware betroffene Institutionen und so konnte kbo kurzfristig Maßnahmen planen und durchsetzen.

Zentrale Erfolgsfaktoren sind die Einrichtung des multiprofessionellen IT-Sicherheitskomitees und die Zusammensetzung dieses Komitees. In der Krisensituation war verlässliche Information wichtig: Die Mitarbeiter wurden mit „einer Information für alle" aufgeklärt. So haben sich die Mitarbeiter informiert gefühlt und „Flurfunk" wurde verhindert. Diese Informations-E-Mails enthielten auch die Informationen, wann die nächste Mitarbeiterinformation erwartet werden konnte – daran hat sich die IT verlässlich gehalten und das hat den Druck von den Mitarbeitern in der IT und dem Sicherheitskomitee genommen. Während der Krisensituation hat E-Mail-Verkehr intern immer funktioniert und konnte für die interne Kommunikation genutzt werden. Die Rückmeldung der Mitarbeiter zur Arbeit der IT und zur Zusammenarbeit war durchweg positiv ebenso wie auch die Rückmeldung zur Zusammenarbeit mit dem Dienstleister – weshalb unter anderem die Mitarbeiter aktiver mit der IT zusammenarbeiten.

Die erfolgreiche Abwehr des Angriffs im September 2016 war ein wichtiges Vertrauenssignal: kbo konnte intern weiterarbeiten, das Sicherheitskomitee und die IT haben die Lage im Griff gehabt und das Frühwarnsystem hat funktioniert. Wichtig war, dass die Entscheidungsprozesse schnell und transparent abliefen: Die IT kann jetzt das Internet für kbo sperren, weil sie weiß, was wieder schnell freigegeben werden muss und wie sie diese Dienste dann auch wieder schnell freigeben kann. Wichtig für die Nachhaltigkeit der IT-Sicherheitsmaßnahmen war die Sonderprüfung mit Bericht an den Vorstand wie bei einem Audit. Im Betrieb – direkt am Terminal – wurden Einstellungen z. B. der Firewall geprüft bzw. überprüft, ob die Anwenderrechte stimmen und die Skripte arbeiten. Das motiviert auch die Administratoren, statt schneller Bugfixes dauerhafte und durchdachte Lösungen zu entwickeln.

Dem IT-Sicherheitskomitee wird es zugeschrieben, dass sich die Maßnahmen in der Praxis bewährt haben. Bewährt haben sich auch die Hinzuziehung des externen Dienstleisters für Penetration-Tests zur Überprüfung aller Sicherheitsmaßnahmen, die transparenten und schnellen Prozesse sowie das Prinzip der Teilung von Verantwortung, das den Verantwortungsdruck von den Mitarbeitern in der IT nimmt. So wird kbo seiner Verantwortung gegenüber den Mitarbeitern in der IT entsprechend dem Leitbild gerecht.

„Wir handeln verantwortungsvoll, arbeiten offen, glaubwürdig und verlässlich zusammen […].

– (kbo 2012)

Das Prinzip des ausgewogenen Risikomanagements wird umgesetzt: Weder IT noch Anwender können Fragen der IT-Sicherheit alleine entscheiden, das Risikomanagement bezieht IT und Anwender gleichermaßen mit ein und Lösungen für IT-Sicherheitsfragen werden gemeinsam getragen.

Insgesamt ermöglichen die Struktur von kbo und die Dienstleistung der IT des Bezirks Oberbayern GmbH mit dem zentralen Rechenzentrum in einer privaten Cloud einen effizienten Betrieb mit nur etwa 100 Mitarbeitern für die IT: In den Kliniken des Verbundes werden IT-Management-Positionen bei gleichzeitiger Erhöhung des IT-Sicherheitsniveaus eingespart – vergleichbare Betriebe und Organisationen benötigen wesentlich mehr IT-Personal.

Das entschlossene Handeln und das pragmatische Umsetzen der nötigen Ad-hoc-Maßnahme und die anschließende Umsetzung der nötigen Maßnahmen in konsequentem Einklang mit den Bedürfnissen der Mitarbeiter ermöglichen kbo eine IT-Sicherheitsstrategie, die bestmöglich auf die Bedürfnisse eines Klinikenverbundes abgestimmt ist. Trotz des angesprochenen Handelns war der tägliche Betrieb auf den Stationen durch die ständige Verfügbarkeit des KIS und der File-Shares, insbesondere die Patientenversorgung, zu jeder Zeit gesichert.

7.5 Danksagung

Wir danken dem Bundesministerium für Bildung und Forschung (BMBF) für die Möglichkeit der Forschung im Rahmen des Projektes VeSiKi, Förderkennzeichen 16KIS0213K.

7.6 Literaturverzeichnis

Borchers, U., 2016. Ransomware-Virus legt Krankenhaus lahm. Verfügbar unter: https://www.heise.de/newsticker/meldung/Ransomware-Virus-legt-Krankenhaus-lahm-3100418.html [zugegriffen: 14-Mai-2018].

Bundesamt für Sicherheit in der Informationstechnik (BSI), 2016a. Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz. Verfügbar unter: https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html [zugegriffen: 03-Aug-2017].

Bundesamt für Sicherheit in der Informationstechnik (BSI), 2016b. Ransomware: Bedrohungslage, Prävention & Reaktion. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/Ransomware/Ransomware_node.html [zugegriffen: 21-Sept-2017].

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

Cerner, 2016. Cerner medico – einfach mehr KIS. Verfügbar unter: https://www.cerner.com/Produkte_und_Services/KIS/medico/?langtype=1031 [zugegriffen: 05-Jan-2016].

kbo (2012). Unser kbo – Leitbild. Verfügbar unter: https://www.kbo-ku.de/fileadmin/_migrated/content_uploads/kbo_leitbild.pdf [zugegriffen: 15-Nov-2016].

8 IT-Sicherheit in der Molkerei: Familientradition und Hochverfügbarkeit[6]

Sebastian Dännart, Universität der Bundeswehr München

Die Molkerei ist ein Familienunternehmen und setzt unternehmensweit auf Nachhaltigkeit. Eine wesentliche Grundlage des Unternehmenserfolges ist eine solide IT-Strategie mit einem effektiven IT-Sicherheitsmanagement, das auf Kompetenz und Verantwortungsbewusstsein der Mitarbeiter setzt. Hier werden modernste Technik mit der Unternehmensphilosophie der alteingesessenen Molkerei verbunden. Die vorliegende Fallstudie bietet einen Einblick in die IT-Sicherheitsstrategie und das IT-Sicherheitsmanagement eines mittelständischen familiengeführten Traditionsunternehmens im Kontext der Kritischen Infrastrukturen.

Keywords: Sektor Ernährung, Branche Ernährungswirtschaft, Mitarbeiterintegration, IT-Sicherheitsmanagement, Datensicherung

8.1 Unternehmen

Seit der Unternehmensgründung liegt der Unternehmenssitz der Molkerei in einem kleinen bayerischen Ort. Die Molkerei ist mit diesem Standort eng verbunden – dort ist der Sitz der Unternehmensführung, wesentliche Produktionsanlagen und andere Unternehmensbereiche.

Wesentliche Herausforderungen sind die zunehmende Diversifizierung des Produktangebotes, die Automatisierung der Produktion aber auch das Themenfeld Food Safety. Die Molkerei setzt verschiedene Produktions- und Sicherheitsstandards um – entsprechend nationalen und europäischen Vorgaben. Das Unternehmen hat auch selbst ein Qualitäts- und Nachhaltigkeitsprogramm zur Tiergesundheit und nachhaltigen Erzeugung von Milch entwickelt.

IT-Sicherheitsmanagement ist in der Molkerei eng mit dem Thema Food Safety verbunden. Der Nachhaltigkeitsstrategie entsprechend strebt das Unternehmen – auch in Hinblick auf die Diskussion über die IT-Sicherheit Kritischer Infrastrukturen – ein hohes Maß an IT-Sicherheit an und verstärkt die IT-Strategie und das IT-Sicherheitsmanagement, um dem Anspruch der eigenen Unternehmensphilosophie sowie der Gesetzgebung in der besonderen Verantwortung als Lebensmittelproduzent gerecht zu werden.

Vor etwa 10 Jahren wechselte die Verantwortung für die Unternehmens-IT. Seitdem stehen das Verständnis und die Motivation aller Mitarbeiter als Schlüsselfaktoren für eine erfolgreiche IT-Sicherheit im Mittelpunkt. In der Unternehmens-IT sind alle Mitarbeiter mit IT-Bezug sowohl aus dem Bereich der Produktion als auch aus dem Bereich der Office-IT zusammengefasst und das einheitliche, an ITIL angelehnte IT-Management der gesamten IT gilt als einer der Schlüsselfaktoren der erfolgreichen IT-Strategie. In den vergangenen zehn Jahren wurde die IT des Unternehmens grundlegend aufgebaut und wichtige sicherheitskritische Projekte,

6 Diese Fallstudie ist anonymisiert.

wie die unternehmensweite Einführung von SAP oder eine „Big Bang"-Umstellung auf eine neue Steuerung des Hochregallagers und der Logistik, erfolgreich umgesetzt.

Die IT-Sicherheitsstrategie der Molkerei setzt auf Kompetenz und Verantwortungsbewusstsein der Mitarbeiter als zentrale Elemente. Sie will neue IT-Technologien schnell und effizient in die produktive Nutzung bringen, bestehende Infrastrukturen auf adäquate IT-Sicherheitsniveaus anheben. Das Ziel ist es, die Vorteile von standardisierten Prozessen im IT-Management mit dem notwendigen Augenmaß in der Atmosphäre eines Familienunternehmens zu verbinden, um die Hochverfügbarkeit einer leistungsfähigen IT sicherzustellen.

8.1.1 Unternehmensprofil

Die Molkerei ist ein bayerisches Familienunternehmen, das seit Jahrzehnten eine Vielzahl von bekannten Milchprodukten herstellt. Das Unternehmen beschäftigte 2017 mehr als 3.000 Mitarbeiter und hatte einen geschätzten Jahresumsatz von über 960 Millionen Euro. Das Unternehmen hat Produktionsstätten im In- und Ausland und ist international vertreten.

8.1.2 Strategische Ausrichtung

Die Molkerei hat sich selbst eine Corporate-Responsibility-Strategie auferlegt. Diese thematisiert neben Rohstoffen und der Umwelt auch die soziale Verantwortung des Unternehmens. Lebensmittelsicherheit und Sicherheit der Produktion sind entsprechend wichtige Themen und so setzt das Unternehmen eine Vielzahl von sicherheitsrelevanten Standards in der Produktion um – nicht zuletzt, weil es die deutschen und europäischen gesetzlichen Vorgaben fordern und explizit von internationale Kunden gefordert wird. Verschiedene Produktlinien haben außerdem ein Halal-Zertifikat. Das Gesamtunternehmen ist nach IFS Food Version 6 zertifiziert und demzufolge ist Food Defense eine verpflichtend umzusetzende Anforderung.[7] Diese Sicherheitsrichtlinie bezieht sich beispielsweise auf unbefugten Zugang zur Produktion von Lebensmitteln und fordert Zugangskontrollen vor Ort. Das Risiko- und Sicherheitsmanagement der Produktion wird entsprechend dem HACCP-Konzept (Hazard-Analysis-Critical-Control-Points-Konzept für Lebensmittelsicherheit[8]) für Lebensmittelsicherheit und Verbraucherschutz durchgeführt. Die Produktionsstätten sind entsprechend zertifiziert.

IT-Sicherheit ist ein zentraler Baustein im Sicherheitskonzept. Da beispielsweise die Produktion sowie auch die Sicherheitsschlösser der Türen zentral über IT gesteuert werden, spielt die IT-Sicherheit auch unmittelbar für die Sicherheit der Lebensmittelproduktion eine wichtige Rolle.

7 Food Defense and Emergency Response (fsis.usda.gov). United States Department of Agriculture. Die Food Defense US-Richtlinie des U.S. State Department of Agriculture bezeichnet den Produktschutz von Lebensmitteln vor mutwilliger Kontamination oder Verfälschung durch biologische, chemische, physikalische oder radioaktive Stoffe. Food Defense betrachtet die dazu relevanten physikalischen, personellen und operativen Sicherheitsmaßnahmen.

8 Die Verordnung der Europäischen Gemeinschaft EG 852/2004 sieht die Anwendung des HACCP-Konzeptes in allen Unternehmen, die mit der Produktion, der Verarbeitung und dem Vertrieb von Lebensmitteln beschäftigt sind, verpflichtend vor.

8.1.3 Fallstudienpartner

Name	Position im Unternehmen
anonymisiert	Leiter IT der Molkerei
Sebastian Dännart	Wissenschaftlicher Mitarbeiter, Universität der Bundeswehr München

8.2 Kritische Infrastruktur

8.2.1 Einordnung als Kritische Infrastruktur (KRITIS)

Die Molkerei liegt mit ihrer Produktionsmenge knapp unter der Grenze für eine Kritische Infrastruktur im Sektor „Ernährung" der Branche „Ernährungswirtschaft".[9] Mit der öffentlichen Diskussion über KRITIS fühlt sich das Unternehmen jedoch dennoch dem Schutz der eigenen Infrastruktur stärker verpflichtet, auch wenn erwartet wird, dass IT-Sicherheit entsprechend der KRITIS-Verordnung für die Lebensmittelindustrie keine große Veränderung der Prozesse bedeutet. Eine Normung oder Standardisierung für IT-Sicherheit Kritischer Infrastrukturen für den Sektor Ernährung wird aus Sicht der Leitung der Unternehmens-IT als wichtig und wegweisend empfunden.

Neben der Verantwortung des Unternehmens für die Kunden ist der Markt der Haupttreiber für Sicherheit. Über die letzten Jahre hinweg konnte der Kundenkreis international ausgeweitet werden und so müssen Produktionsanlagen und Management heute vielen national verschiedenen Sicherheitsanforderungen entsprechen. Beispiele sind sowohl die Food-Defense-Richtlinie als auch Halal-Zertifizierungen.

8.2.2 Risikoanalyse

Bei einem Molkereibetrieb ist – wie in vielen Lebensmittelproduktionen – die Hochverfügbarkeit ein Muss: Bereits ein kurzer Stillstand des Systems oder eine Fehlfunktion in der Steuerung der Produktion können zu einer Veränderung des Produkts führen und kurze Störungen oder Unterbrechungen können zur Folge haben, dass Produkte verunreinigt werden und die Produktion länger unterbrochen werden muss. Speziell in einem Molkereibetrieb würde eine kurze Störung bedeuten, dass Milch, die laufend angeliefert wird, nicht verarbeitet werden kann. Eine Verunreinigung von Produkten kann direkten Einfluss auf die Gesundheit der Konsumenten haben. Ein Risiko für die Produktion stellen beispielsweise Stromausfälle dar. Das Unternehmen wird, um dieses Risiko auszugleichen, nötigenfalls vom Energieversorger mit Notstrom-Aggregaten ausgestattet. Auch hier werden bereits IT-Sicherheitsrisiken der Produktionsanlagen, aber auch der Office-IT betrachtet.

Neben dem Risiko von Verunreinigungen spielen auch die Wahrnehmung der Sicherheit der Produkte und die Reputation des Unternehmens in der Öffentlichkeit eine große Rolle.

9 Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015. Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) vom 22. April 2016.

Vor allem die Herstellung von Kindernahrung bedeutet eine besondere Verantwortung den Konsumenten gegenüber.

Aus diesem Grund ist auch die Dokumentation der Produktionsabläufe mit allen Chargen ein wichtiges Thema – nicht zuletzt, um Produkte zurückrufen zu können und den Dokumentationspflichten der verschiedenen umgesetzten Standards und Anforderungen der Kunden gerecht zu werden.

8.3 IT-Sicherheit

Die zentrale IT-Abteilung plant und verantwortet die gesamte IT des Unternehmens – inklusive der Sicherheit moderner Produktionsanlagen. Mit modernsten Mitteln werden die Voraussetzungen für einen reibungslosen, automatisierten und sicheren Ablauf aller Geschäfts- und Produktionsprozesse geschaffen.

8.3.1 IT-Infrastruktur

Die Molkerei betreibt zwei redundante Rechenzentren, die jeweils die Kapazität haben, die gesamte Systemlast zu tragen. Diese Struktur mit zwei Rechenzentren ist aus einem ursprünglich einzelnen, älterem Rechenzentrum, das nun als Backup-Rechenzentrum fungiert, und einem weiteren Rechenzentrum, welches nach neusten IT-Sicherheitsstandards mit modernen Löschanlagen und unterbrechungsfreier Stromversorgung gebaut wurde, gewachsen.

Die Architektur des nicht-produktiven IT-Systems baut auf einem Zwei-Säulen-Konzept auf. Die erste Säule basiert auf SUSE Linux und umfasst alle SAP-Systeme. Die zweite Säule basiert auf Microsoft-Betriebssystemen und umfasst neben der Kommunikation alle administrativen Bereiche und die klassische Office-IT. Durch diese Heterogenität werden IT-Sicherheitsrisiken in der Regel auf eine der beiden Säulen begrenzt. Dieses Zwei-Säulen-Konzept trägt zu Transparenz und Übersichtlichkeit, zur Wartbarkeit des Systems und zur individuellen Systemkompetenz der Mitarbeiter bei.

Die Grundidee der Systemarchitektur des produktiven Systems ist es, dass Eingaben und Steuerungen an den Produktionsanlagen nur aus der Steuerzentrale (Leitstand) durchgeführt werden können. Die Steuerzentrale ist ein abgeschlossener „gekapselter“ Bereich innerhalb der Produktionshallen und bietet keinerlei Interfaces oder Terminals zum Zugriff außerhalb der Kapselung an. Damit werden ungewollte Zugriffe, auch durch Innentäter, in diesem Bereich wirksam unterbunden. Materialrückmeldungen wie „Wechsel von Chargen“ finden im Produktionsbereich noch händisch an SAP-Eingabemasken durch die Mitarbeiter in der Produktion statt. Durch den fließenden Übergang zwischen den produzierten Chargen verschiedener Produkte ist dazu bislang keine automatisierte Lösung gefunden worden. Es gibt in der Produktion keine PC-Arbeitsplätze, sondern nur Eingabemasken oder Eingabegeräte mit beschränkter Funktionalität, wodurch die Gefahr einer Manipulation über die IT im Produktionsbereich stark reduziert wird. Der Produktionsbereich selbst ist hochautomatisiert und die IT selbst muss mit den (niedrigen) Temperaturen in der Produktion und im Tiefkühlbereich zurechtkommen. Die Etikettendrucker beispielsweise sind Spezialgeräte, die

auch bei sehr niedrigen Temperaturen in Kühlhäusern und der gekühlten Produktion noch funktionsfähig sind.

Konfiguration und Installation von IT-Systemen erfolgen nahezu komplett mit internen Kompetenzen. Bevor ein System im Unternehmen zum Einsatz kommt, wird es unternehmensintern analysiert und studiert.

Die IT setzt sowohl in der Produktion als auch in der Office-IT auf Virtualisierung.

8.3.2 Geschäftssicht

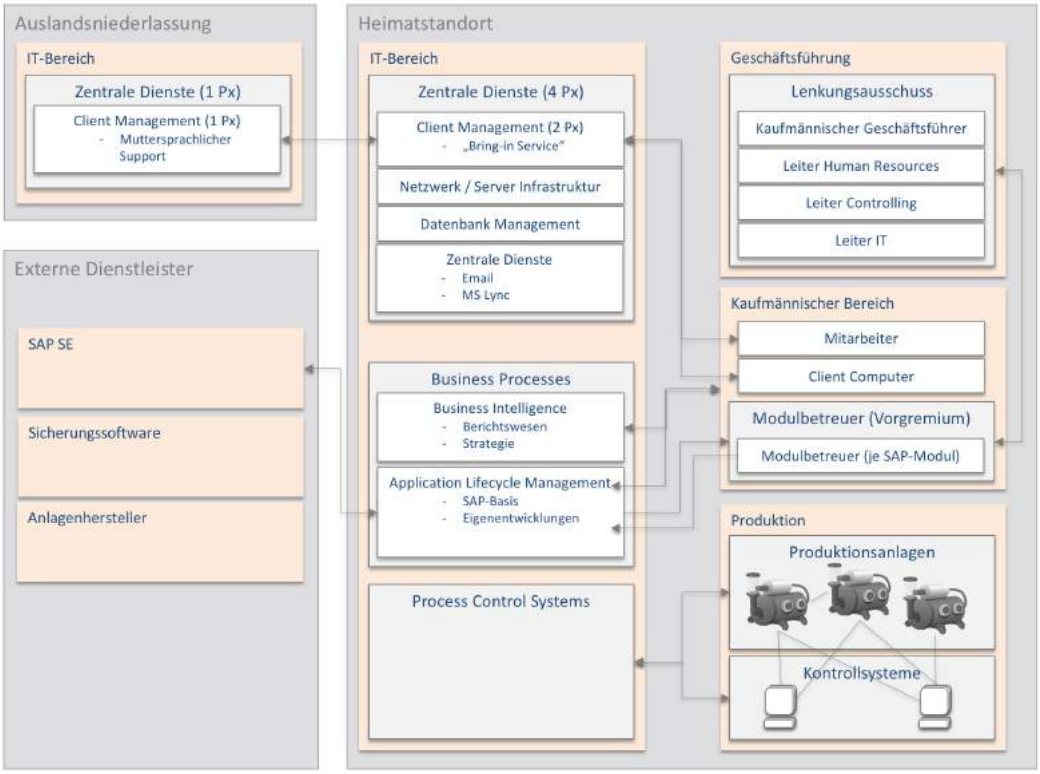


Abbildung 8-1: Sicht auf die IT-relevanten Geschäftsbereiche der Molkerei

Der IT-Bereich ist in drei Abteilungen gegliedert: „Zentrale Dienste", „Business Processes" und „Process Control Systems".

Die Abteilung „Zentrale Dienste" beschäftigt sich mit allem, was Netzwerk, Server und Betriebssysteme betrifft. Zudem fallen in diesen Bereich Client-Management sowie Datenbanken und E-Mail-Dienste. Die Abteilung besteht aus sieben Mitarbeitern, von denen zwei primär für das Client-Management zuständig sind. Diese beiden Mitarbeiter werden durch zwei muttersprachliche Mitarbeiter an den internationalen Standorten unterstützt.

Eine innovative Besonderheit dieser Abteilung ist der Bring-in-Service. Ein Mitarbeiter, der ein Problem mit einem dienstlichen IT-Gerät hat, bringt es selbst in den IT-Service. Dort

erhält der Mitarbeiter entweder ein Austauschgerät oder der Fehler wird behoben. Das minimiert nicht nur Serviceslots und -termine, sondern der Mitarbeiter kommt schnell zu einer Lösung. Dieser Bring-in-Service lässt eine persönliche Verbindung zwischen IT-Bereich und dem übrigen Betrieb entstehen.

„Business Processes" ist die Abteilung, die sich mit der Abbildung der Geschäftsprozesse in der Software beschäftigt. In erster Linie ist dies die gesamte SAP-Umgebung, in zweiter Linie auch Kollaborationssoftware, wie Microsoft SharePoint, und individuell benötigte Geschäftssoftware. Diese Abteilung ist in zwei Arbeitsteams gegliedert. Das Team „Business Intelligence" greift Themen in den Bereichen Berichtswesen und Strategie auf und setzt Projekte in diesem Bereich um. Das zweite Team „Application Lifecycle Management" bewirtschaftet die SAP-Basiskomponenten mit Versionskontrolle und Support Stack. Außerdem sichert das Team die Qualität der Eigenentwicklungen und Erweiterungen im Kontext der Geschäftsprozesse.

Die dritte Abteilung „Process Control Systems" verantwortet die Prozessautomatisierung mit allen Produktionssystemen und Systemen, die in direktem Zusammenhang mit Produktionssystemen stehen. Eine besondere Herausforderung ist es hier, die Konfiguration nach den Vorgaben der Hersteller mit den eigenen Richtlinien in Einklang zu bringen.

Zur Entscheidungsfindung über den IT-Bereich hinaus ist ein Lenkungsausschuss eingesetzt. Dieser Lenkungsausschuss besteht aus dem kaufmännischen Geschäftsführer, dem Leiter Human Resources, dem Leiter Controlling und dem Leiter des IT-Bereichs. Durch diese bereichsübergreifende Kompetenz können Implikationen von Änderungen und Anpassungen identifiziert, im Vorfeld analysiert sowie gegebenenfalls auch gestoppt werden.

Für alle Bereiche des SAP-Systems sind Modulbetreuer in den jeweiligen Abteilungen eingesetzt. Dies sind Mitarbeiter, die sich sehr gut mit den Prozessen, Systemen und Schnittstellen in den Fachabteilungen auskennen, die Prozesse optimieren und bei Fragen zu Änderungen unterstützen.

8.3.3 Prozesssicht

Stellvertretend für die Vielzahl von unterschiedlichen Prozessen im Unternehmen werden in diesem Abschnitt zwei Prozesse herausgegriffen, die den Ansatz des IT-Sicherheitsmanagements illustrieren: Das Change-Management und die Remote-Wartung.

Change-Management

Sowohl im Bereich der Produktion als auch im SAP-Umfeld werden Änderungswünsche und Vorschläge als Entwicklungsanträge eingereicht und bearbeitet. Im Bereich der SAP-Produkte wird dieser Vorgang technisch durch den SAP Solution Manager abgebildet und integriert. Im Produktionsbereich existiert eine solche Unterstützung nicht, die Entwicklungsanträge werden „händisch" organisiert. In beiden Fällen ist der Change-Prozess an das Change-Management aus ITIL angelehnt.

Wird ein Entwicklungsantrag eingereicht, begutachtet diesen zunächst ein Vorgremium aus allen Modulbetreuern. Hier werden mögliche Konflikte, Nebeneffekte oder Schnittstel-

lenprobleme zu jedem Entwicklungsantrag thematisiert. In begrenztem Umfang kann das Vorgremium bereits Änderungen zustimmen oder diese priorisieren und zur Entscheidung und Freigabe an den Lenkungsausschuss weitergeben.

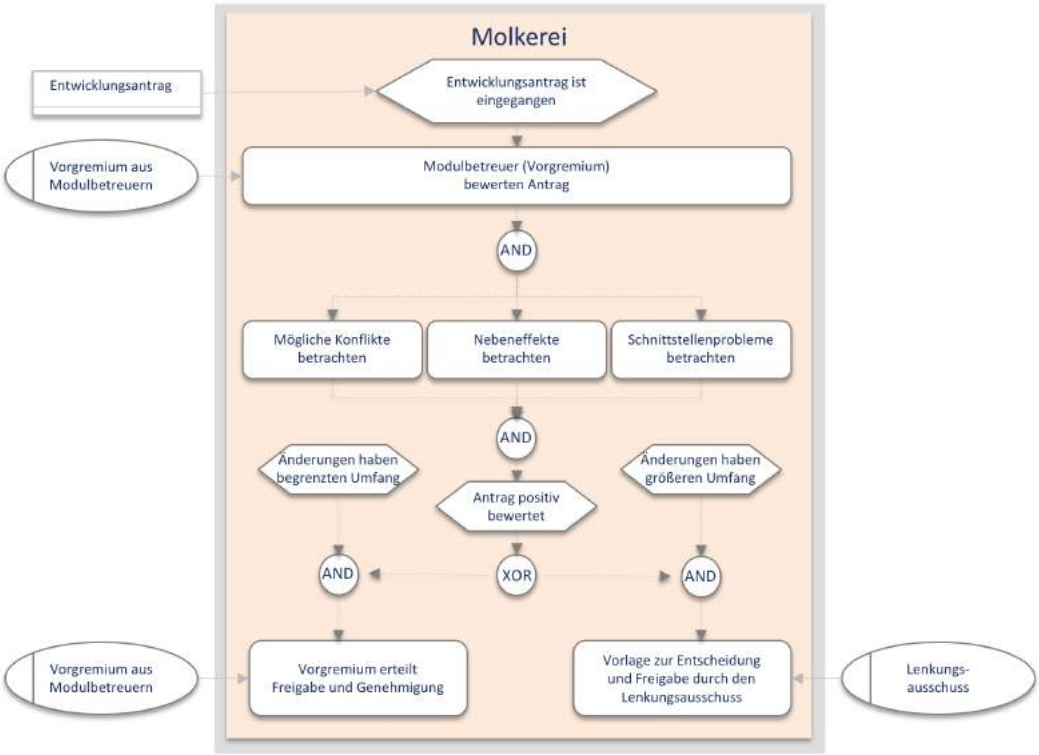


Abbildung 8-2: Change-Management für Entwicklungsanträge

Dieses strukturierte Vorgehen sorgt seit der Einführung vor etwa acht Jahren für Stabilität in der Systemlandschaft der Molkerei.

Remote-Wartung

Hersteller von Produktionsanlagen oder externe Wartungsfirmen müssen die Produktionsanlagen von extern erreichen können. Für Fernwartung werden jeweils einzeln über einen zentralen Eingangsrouter Zugänge zu dem jeweiligen VLAN der benötigten Anlage durch die Abteilung Zentrale Dienste gewährt. So kann kein Zugriff auf andere Anlagen oder andere Unternehmensbereiche erfolgen. Alle Zugriffe werden protokolliert und zeitlich auf ein Minimum begrenzt. Dies reduziert wirkungsvoll die Risiken, die durch die Möglichkeit von Remote-Zugriffen auf die Produktionsanlagen entstehen.

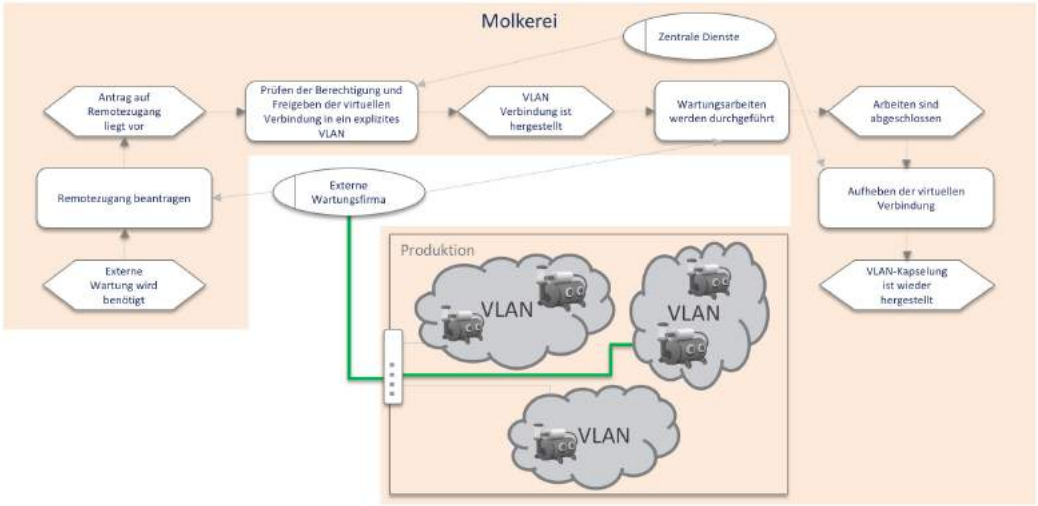


Abbildung 8-3: Remotezugangs-Prozess für Wartungsarbeiten externer Unternehmen

8.3.4 Anwendungssicht

Die Anwendungslandschaft stützt sich im Wesentlichen auf zwei Säulen: eine SAP-Säule und eine Microsoft-Säule. Auf den Bereich der Produktion und die dort verwendeten IT-Systeme sowie deren Sicherheitsniveaus hat das Unternehmen selbst keinen großen Einfluss. Hier geben die Anlagenhersteller in der Regel die verwendeten IT-Systeme vor.

Der Bereich der kaufmännischen Software basiert auf SUSE-Linux-Enterprise-Betriebssystemen und beinhaltet sämtliche SAP-Komponenten. Dies ist im Kern das SAP-ERP-System. Es wurde in kurzer Zeit unternehmensweit für nahezu alle Geschäftsprozesse eingeführt und läuft als OnPremise-Lösung in den hauseigenen Rechenzentren. Dem Ansatz des komplett selbstadministrierten Systems folgend, wurde hier ein Rollout-Konzept samt Template entwickelt, mit dem ein Rollout in den Niederlassungen in nahezu vollständiger Eigenleistung durchgeführt werden kann. Lediglich ein Compliance Berater für die jeweiligen Länder, in denen die Niederlassung eröffnet wird, hilft die nötigen Anpassungen vorzunehmen, bevor das System – basierend auf den SAP-Servern am Heimatstandort – produktiv angeschlossen wird. Im zweiten Rechenzentrum läuft ein zweites baugleiches SAP-System, welches mittels LogFile-Shipping um acht Stunden zeitversetzt läuft und auf SAP-Transaktionsebene alle Änderungen aus dem Live-System übernimmt.

Der Bereich der klassischen Office-IT wird von Microsoft-Systemen abgebildet. Auf virtualisierten Servern werden alle nötigen Dienste aus einer Hand zur Verfügung gestellt. Dies sind neben MS Exchange und MS Skype for Business zur Kommunikation auch MS SharePoint für Kollaboration, MS Printservices sowie die MS DistributedFileServices zur gemeinsamen Datenablage. Letztere stellt auch für alle Tochtergesellschaften die Datenablage dar, sodass alle relevanten Daten am Stammsitz liegen und dort gesichert werden.

In allen Anwendungsbereichen wird stets angestrebt, die aktuellen Versionen zu nutzen; dabei wird weniger Wert auf Homogenität der Anwendungslandschaft gelegt. Kommt bei-

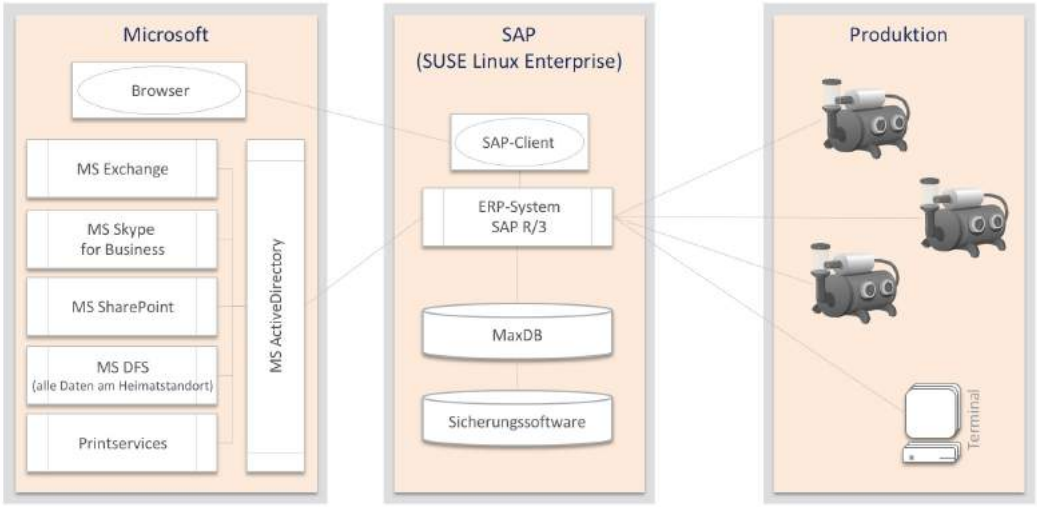


Abbildung 8-4: Sicht auf die Anwendungslandschaft der Molkerei

spielsweise ein neues Betriebssystem von Microsoft auf den Markt, wird es zunächst als Testclient aufgesetzt und dann ausgiebig von den eigenen Mitarbeitern der IT getestet. Wenn diese Tests positiv verlaufen, werden ein neues Installationsbündel erstellt und die neuen und – bei Bedarf – auch die alten Clients umgerüstet.

Im Bereich der Berechtigungen arbeiten die SAP- und die MS-Säule Hand in Hand. Die MS ActiveDirectory fungiert als Identity Container und wird mit den Identitäten des SAP-ERP-Systems synchronisiert. Innerhalb des SAP-HR-Moduls werden Planstellen ausgewiesen und diese dann Mitarbeitern zugewiesen. Diese Planstellen dienen zur Verwaltung der Berechtigungen für das SAP-System und werden an die MS ActiveDirectory weitergegeben und dort in das Rollen- und Rechtekonzept überführt. Auf diese Weise werden auch automatisiert Mitarbeiterinformationen verarbeitet. Automatisierte Aktualisierung der Kontaktdaten und Änderung von Visitenkarten als Beispiel werden so problemlos möglich. Es ist auch eine händische Pflege der Berechtigungen denkbar, wenn bestimmte Rollenkonstrukte nicht durch diesen Wechsel von SAP und MS ActiveDirectory abgebildet werden können oder Sonderberechtigungen nötig sind.

8.3.5 Technische Sicht

An ihrem Heimatstandort betreibt die Molkerei zwei redundante Rechenzentren, die über Core-Switche miteinander verbunden sind. Das ursprüngliche erste Rechenzentrum dient als Backup-Rechenzentrum und ein neu erbautes, modernes Rechenzentrum übernimmt die Funktion des Hauptrechenzentrums. Jedes einzelne Rechenzentrum kann die betriebsnotwendige Last des Systems tragen.

Auch in diesem Bereich setzt das Unternehmen auf die Ausbildung und Systemkenntnis seines eigenen Personals und arbeitet darüber hinaus eng mit den lokalen Behörden zusammen, um Schäden, z. B. durch unsachgemäße Löschung im Brandfall (z. B. durch Löschwas-

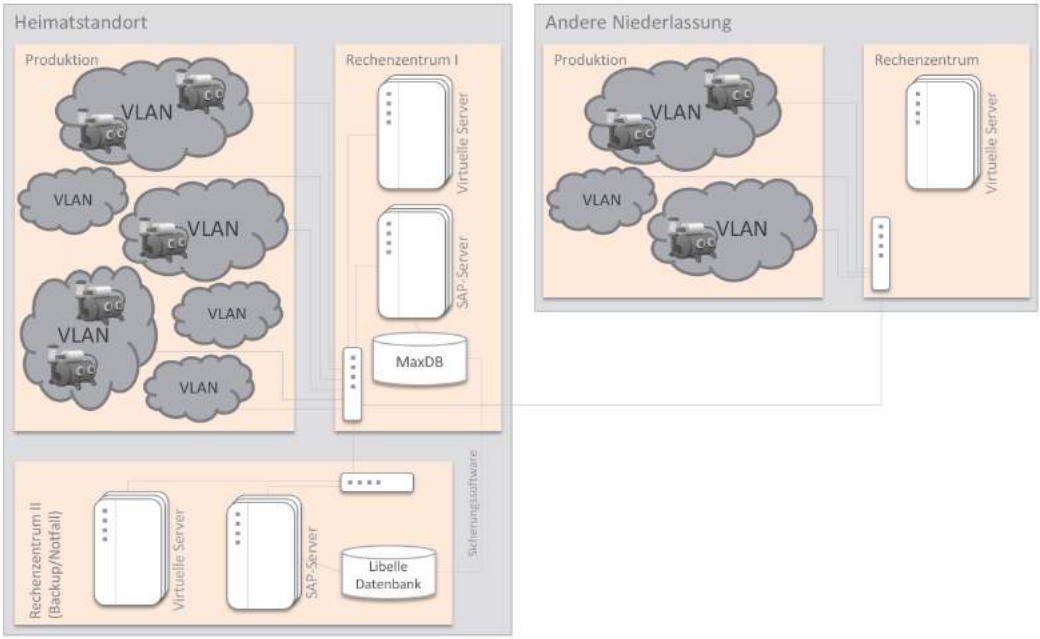


Abbildung 8-5: Technische Sicht auf die IT-Infrastruktur der Molkerei

ser), zu vermeiden. Hier sind moderne Löschanlagen im Rechenzentrum verbaut und der Ernstfall mit der Feuerwehr im Detail geplant.

Die Rechenzentren am Hauptsitz beinhalten jeweils ein komplettes physisches Serversystem für SAP, basierend auf dem SAP-eigenen Datenbanksystem MaxDB. Im Backup-Rechenzentrum läuft parallel ein zweites baugleiches SAP-System (siehe Kapitel 8.3.4). Alle Standorte greifen auf das SAP-System am Heimatstandort zu.

Für alle anderen Systeme beherbergen die Rechenzentren der Außenstandorte zwei weitere physische Server, auf denen mittels MS HyperV jeweils vier Server virtualisiert werden. Dies sind unter anderem ein DHCP-Server und Domain-Controller, ein Printserver, ein WSUS-Server für die Softwareverteilung, ein SCCP-Relay und ein FileServer für das Distributed File System (DFS). Einer der beiden physischen Server ist in der Lage, im Notfall die gesamte Last alleine zu tragen. Diese beiden Systeme sind an jedem Standort vorhanden und identisch aufgebaut. Der jeweilige DFS-Speicher wird in die Rechenzentren am Stammsitz synchronisiert.

Im Bereich der Produktion ist eine so homogene technische Lösung nicht möglich, daher wird hier die Technologie der VLANs genutzt. Jede Produktionsanlage wird in ein eigenes VLAN gekapselt und so werden die Produktionsanlagen virtuell voneinander getrennt. Sollte ein Zugang nötig sein, wird dies über einen Router temporär ermöglicht. Diese virtuelle Separierung erlaubt es, ein gefordertes IT-Sicherheitsniveau in einer Kapsel unabhängig vom IT-Sicherheitsniveau anderer VLANs zu gewährleisten. Ein weiterer Vorteil dieser Separierung ist es, dass einzelne Netzwerke vor unberechtigten Zugriffen aus anderen Netzwerkbereichen geschützt werden.

8.3.6 Normen, Standards und Gesetze

Bisher ist das Unternehmen nach keinem IT-spezifischen Standard zertifiziert, orientiert sich jedoch bei der Ausrichtung der IT-Service-Infrastruktur an Vorschlägen aus ITIL. Während der unternehmensweiten Einführung von SAP hat sich diese Ausrichtung an diesem Best-Practice-Rahmenwerk als zielführend erwiesen.

Neben dem neuen IT-Sicherheitsgesetz und dem Telekommunikationsgesetz beeinflusst eine Reihe weiterer Regelungen die IT des Unternehmens. Die Abteilung „Tax & Legal" unterstützt bei der Umsetzung z. B. von Compliance-Regelungen. Normen der IT-Sicherheit, wie die ISO/IEC 27001, finden bislang keine konkrete Anwendung.

8.3.7 Stand der IT-Sicherheit

Für die Molkerei ist eine solide IT-Sicherheitsstrategie, die die Philosophie des Unternehmens mit den Anforderungen an IT-Sicherheit und hoher Verfügbarkeit verbindet, wichtig für den nachhaltigen Geschäftserfolg. Dieses Kapitel greift ausgewählte Aspekte des IT-Sicherheitsmanagements der Molkerei auf.

Die IT-Abteilung

Die zentrale IT-Abteilung ist auf dem Gelände der Produktion am Heimatstandort platziert und kurze Wege von der IT zu allen Geschäftsbereichen prägen das Klima der Zusammenarbeit. Die Mitarbeiter am Standort sind überwiegend langjährig beschäftigt und dem Unternehmen eng verbunden. Dieses kann sich auf die Loyalität ihrer Mitarbeiter genau wie auf das Verantwortungsbewusstsein der Mitarbeiter für das Unternehmen verlassen. Auch in Krisenfällen setzen sich die Mitarbeiter für ihr Unternehmen ein und würden bei einem Notfall oder Systemausfall jederzeit zur Verfügung stehen.

In die IT-Abteilung wurden auch die technischen Mitarbeiter aus der Produktion integriert, vor dem Hintergrund, dass der IT-Anteil in den Produktionsanlagen zunehmend komplexer wurde und sich für diesen Teil des Unternehmens die Frage stellte, wie Management und Weiterentwicklung aussehen würden. So werden die Rahmenwerke und Standards aus der IT, wie z. B. das ITIL-Rahmenwerk, jetzt auch im Bereich der Produktion eingesetzt, damit die gesamte IT nach einheitlichen Prozessen gemanagt werden kann. Dies ist eine wichtige Voraussetzung, um neue IT-Sicherheitsstandards auch in der Produktion nachhaltig umzusetzen.

Die Mitarbeiter in der IT-Abteilung erhalten Freiräume in der Arbeit, um mit neuen Technologien zu experimentieren oder eigene Projekte durchzuführen, erwerben so eine hohe individuelle Systemkompetenz und bleiben in neuen technischen Entwicklungen auf dem aktuellen Stand.

Notfallsituationen wie das Einspielen von Backups werden als Teil der „normalen" Arbeitsabläufe geübt: Bei der Installation neuer Systeme oder der Wiederherstellung von Systemen wird – wenn möglich – auf Backups zurückgegriffen. Mitarbeiter stellen so sicher, dass die Notfallmechanismen funktionieren, und erwerben individuelle Kompetenz im Notfall- und Krisenmanagement.

Loyalität und Verantwortungsbewusstsein der Mitarbeiter, langjährige Beschäftigungsverhältnisse und hohe individuelle Systemkompetenzen sind die zentrale Säule im IT-Sicherheitsmanagement der Molkerei.

Systemarchitektur

Die Grundidee der Systemarchitektur besteht darin, für das Unternehmen zentrale Informationen und Steuerungsfunktionalitäten am Heimatstandort zu bündeln. Jeglicher Netzwerkverkehr, auch der der Niederlassungen, läuft dort über Proxy-Server und protokolliert den Netzwerkverkehr, der im Rahmen der Internetzugänge der Mitarbeiter, der Telearbeit oder im Rahmen der Fernwartung entsteht. Alle Daten der unternehmensinternen Kollaborationssysteme werden ebenfalls zentral am Heimatstandort gehalten.

Vermeidung externer Dienstleister

Die Produktion der Molkerei ist empfindlich und zeitkritisch. Milch wird laufend angeliefert und bereits kurze Unterbrechungen der Produktion können zu erheblichen Produktionsausfällen und Kosten führen. Wegen der geringen zeitlichen Toleranz bei Systemausfällen oder Systemfehlern, verzichtet das Unternehmen weitgehend auf die Beauftragung externer Dienstleister im Bereich der IT. Externe Dienstleister wären schlicht nicht schnell genug auf dem Werksgelände, um bei einer Störung wirksam eingreifen zu können.

Um zu jeder Tages- und Nachtzeit flexibel reagieren zu können, wird ein Bereitschaftsmodell genutzt, bei dem hauseigene Techniker rund um die Uhr verfügbar sind. Eine Voraussetzung dafür sind sowohl die hohe Systemkompetenz der Mitarbeiter als auch die Loyalität der Mitarbeiter.

Sicherheits- und Anwenderrichtlinien

Das Unternehmen hat für die Nutzung der IT eine Sicherheitsrichtlinie herausgegeben, die durch den Leiter IT erarbeitet wurde. Nachdem diese Richtlinie von der „Tax & Legal"-Abteilung und dem Datenschutzbeauftragten geprüft worden war, erließ die Geschäftsführung diese Richtlinie und führte sie damit unternehmensweit ein.

Das 20 Seiten umfassende Dokument beschreibt unter anderem, wie die Architektur des Gesamtsystems aufgebaut ist, welche Sicherheitsregeln gelten und wer die Verantwortung für die Datenbestände trägt.

Zusätzlich wurden Anwenderrichtlinien herausgegeben. Sie regeln unter anderem die Nutzung von Kommunikationsmitteln, E-Mail und Internet. Die IT erreicht hier alle, auch IT-ferne Mitarbeiter in ihrer Kommunikation: Die Sicherheit von Passwörtern wird den Mitarbeitern durch eine Analogie zu PIN-Nummern einer EC-Karte nahegebracht. Diese Analogie motiviert Mitarbeiter, Passwörter beispielsweise für den Zugang zu Produktionsanlagen nicht weiterzugeben und die Sicherheit der IT-Systeme so zu schützen.

Internetzugänge

Im Bereich der Datenkommunikation werden unter anderem alle eingehenden E-Mails auf Schadsoftware und Auffälligkeiten gescannt. Internetzugang am Arbeitsplatz ist grundsätzlich für alle Mitarbeiter möglich und im Unternehmen gibt es drei Stufen des Internetzugangs:

- Whitelist: Es dürfen nur bestimmte Seiten besucht werden.
- Blacklist: Es dürfen bestimmte Seiten nicht besucht werden.
- Frei: Es ist unbeschränkter Internetzugang möglich.

Die jeweilige Stufe des Internetzugangs legt der Bereichsleiter für die Mitarbeiter individuell fest. Unabhängig von der Stufe laufen alle Zugänge über die zentralen Proxy-Server am Heimatstandort.

Einwahl aus externen Netzen für Mitarbeiter, Smartphone Nutzung und Telearbeit

Alle portablen Geräte sind so konfiguriert, dass sie sich aus jedem unternehmensfremden Netz direkt per MS DirectAccess mit dem Unternehmensnetzwerk verbinden.

Im Bereich der Office-IT werden mobile Geräte, wie Laptops und Smartphones, mittels MS DirectAccess bei jeder Einwahl über externe Netzwerke automatisch mit dem MS DirectAccess-Server am Heimatstandort verbunden und lassen keine Kommunikation über andere Kanäle zu. Jedes IP-basierte Netzwerkpaket, das über portable Geräte versandt wird, geht zwangsweise den Weg über den Proxy. Das bedeutet zwar einen enormen Datenverkehr, ermöglicht aber gleichzeitig lückenlose Protokollierung aller Kommunikation über unternehmenseigene Hardware.

Alle verwendeten Smartphones sind MS Windows Phones. Diese können außerhalb des Unternehmensgeländes zum Abrufen von E-Mails oder für Telearbeit verwendet werden. Dafür werden die Geräte allerdings explizit durch die Administratoren freigegeben und „liegen" bis zur Freigabe in einem Quarantäne-Container. Nach erfolgter manueller Freigabe ist Synchronisation der Daten möglich. Da durchaus sensitive Daten auf diese Geräte gelangen können, ist eine gewisse Passworthärte gefordert und nach Sperrung durch Falscheingabe der PIN erfolgt eine Selbstlöschung der Daten des Smartphones.

Sicherung der SAP-Umgebung

Das Unternehmen verfügt über zwei baugleiche SAP-Systeme, von denen jeweils eines in den beiden Rechenzentren gehostet wird. Basierend auf der SAP-eigenen MaxDB als Datenbank wird mittels LogFile-Shipping jede Transaktion im Primärsystem auf das Backup-System übertragen. Durch einen zeitlichen Versatz von acht Stunden ist es so möglich, neben System- und Softwarefehlern auch falsche Bedienung und Sabotage zeitnah zu identifizieren und transaktionsgenau zu unterbinden.

Durch die Schnelligkeit des Systems ist es bei einem Systemausfall oder einer Systemstörung möglich, den Versatz in ca. 20 Minuten auszugleichen und wieder über ein voll lauf-

fähiges System zu verfügen. Als positiver Nebeneffekt ist eine Archivierung während des Betriebes auf dem Backup-System möglich. Mittels dieser Lösung kann eine Verfügbarkeit von 99,91 % erreicht werden.

Durch den parallelen Betrieb der beiden SAP-Systeme ist eine Wartung im laufenden Betrieb möglich und daher sind auch geplante Wartungszyklen in die Verfügbarkeit eingerechnet.

Berechtigungskonzept

Die Molkerei setzt für sicherheitskritische Prozesse auf das Vier-Augen-Prinzip. Im Einkauf oder dem Kreditorenmanagement lassen sich kritische Berechtigungen, die nicht dem Vier-Augen-Prinzip unterliegen, nicht vermeiden.

Während nicht-kritische Berechtigungen durch die Modulbetreuer vergeben werden, müssen kritische Berechtigungen explizit und bewusst über den Lenkungsausschuss freigegeben werden. Gerade kritische Berechtigungen werden vor der Einrichtung im Produktivsystem zunächst auf einem Testsystem getestet und erst bei konfliktfreiem Ergebnis übertragen.

Die Berechtigungen und das zugrunde liegende Konzept werden jährlich von einem Wirtschaftsprüfer auditiert. Auf die Prozesssteuerung ist dieses Konzept allerdings nicht ohne Weiteres übertragbar.

VLAN-Kapselung der Produktionsanlagen

Produktionsanlagen bringen die Herausforderung mit sich, dass die Systeme durch die Hersteller meist nur unzureichend gegen Zugriffe geschützt sind und außerdem kaum IT-Sicherheitsrichtlinien oder Standards in diesem Bereich existieren. Die Molkerei hat sich für eine einheitliche Lösung für die Netzwerkanbindung aller Anlagen entschieden, die es möglich macht alle Anlagen auf ein einheitliches IT-Sicherheitsniveau anzuheben.

Jede Produktionsanlage wird in einem eigenen VLAN gekapselt. Nötige Verbindungen (z. B. VPN) werden über Router explizit geschaltet und wieder deaktiviert. Bei Bedarf wird ein Remotezugriff für Hersteller oder Wartungsfirmen über VPN freigeschaltet. Durch diese Kapselung wird unerwünschte Kommunikation zwischen den Netzen bzw. Anlagen unterbunden und das Sicherheitsniveau von Produktionsanlagen kann unternehmensweit einheitlich gesteigert werden.

Keine Port Security

In einer Kosten-Nutzen-Abwägung hat sich das Unternehmen gegen die Nutzung von Port Security entschlossen. Das Risiko für Innentäter wird – aufgrund der Unternehmensphilosophie und der gelebten IT-Sicherheitskultur und der Unternehmenskultur – als gering eingestuft. Durch die für Food Defense ohnehin bestehenden physischen Zugangsbeschränkungen und die Vertrauensmentalität ist dieses Risiko tragbar.

Kundenanforderung: PKI-Zertifikate

Kunden fordern häufig PKI-Infrastrukturen zur Verschlüsselung und Authentifikation. Unternehmensintern bedeutete dies auch den Aufbau einer Infrastruktur für die nötigen PKI-Dongle mit dem Nutzermanagement. Die nötigen Mechanismen sind aufwändig, und beispielsweise einen verlorenen Stick wiederherzustellen ist mit erheblichem Aufwand verbunden. Die IT-Abteilung setzt solche Kundenanforderungen bei Bedarf und in Abstimmung mit der Geschäftsführung – wie auch andere Standards und Richtlinien – um.

8.4 Erfolgsfaktoren

Die Mitarbeiter des Unternehmens mit ihrer Kompetenz und ihrer Loyalität sind wesentlich für die IT-Sicherheitsstrategie: Durch die Zugangsregelungen, die z. B. von der Food-Defense-Richtlinie vorgegeben werden, kann die direkte, nicht-netzwerkbasierte Bedrohung durch Innentäter reduziert werden. Das Risiko „Innentäter" wird als eher niedrig beurteilt: Die Molkerei folgt einem offenen, kommunikativen Ansatz und bringt den Mitarbeitern einen Vertrauensvorschuss entgegen.

Die Akzeptanz des Themas IT-Sicherheit ist bei den Mitarbeitern hoch: Die Prozesse, die notwendigen Dokumente und Richtlinien sind außergewöhnlich kompakt, die Systemkompetenz der Mitarbeiter ist hoch und der Bring-in-Service verbindet die zentrale IT mit den übrigen Geschäftsbereichen des Unternehmens. Das Unternehmen setzt zudem auf eigene Mitarbeiter und vermeidet größtenteils den Einsatz von externen Firmen in der IT.

Aufseiten der IT-Abteilung ist ein Erfolgsfaktor die gelebte Abteilungskultur mit der Förderung der individuellen Systemkompetenz der Mitarbeiter, speziell auch in sicherheitskritischen Themen, gefördert durch individuelle Freiräume, mit neuen Technologien zu experimentieren, sowie Verantwortungsbewusstsein und hohe Loyalität der IT-Mitarbeiter dem Unternehmen gegenüber.

Die IT-Abteilung kann eine Historie erfolgreicher Projekte und ein gutes Verhältnis von IT zu allen Bereichen des Geschäfts aufweisen und erhält für die Umsetzung einer nachhaltigen Strategie und der dafür notwendigen IT-Sicherheitsmaßnahmen die notwendigen Mittel und Unterstützung durch das Topmanagement. Die IT-Abteilung wird als internes, helfendes *Beraterhaus* für das Unternehmen verstanden.

Durch die genaue Analyse aller Systeme ist es möglich, intern einen hohen Maßstab an den Standard des gebotenen Service zu legen. Hochverfügbarkeit ist eine wesentliche Forderung an die IT gerade in der Produktion. Hohe Systemkompetenz und Loyalität der Mitarbeiter ebenso wie eine IT-Strategie, die auf moderne Technologien und wohlstrukturierte Einführungsprozesse neuer Technologien angelehnt an ITIL setzt, sind die Schlüsselfaktoren, Hochverfügbarkeit in der Praxis umzusetzen. Die Mitarbeiter bekommen individuellen Freiraum, um eigene Projekte zu verwirklichen, die – sofern sich diese dazu eignen – im Unternehmen umgesetzt werden. Dies erzeugt ein hohes Maß an Mitarbeiterzufriedenheit und Verbundenheit der Mitarbeiter mit der IT des Unternehmens.

8.5 Danksagung

Wir danken dem Bundesministerium für Bildung und Forschung (BMBF) für die Möglichkeit der Forschung im Rahmen des Projektes VeSiKi, Förderkennzeichen 16KIS0213K.

8.6 Literaturverzeichnis

Aufgrund der Anonymisierung wurden die Quellen entfernt.

9 IT-Sicherheit für Geschäftsprozesse im Finanzsektor: Die Managementlösung PREVENT

Steffi Rudel, Universität der Bundeswehr München
Torsten Bollen, Wincor Nixdorf

In der vorliegenden Fallstudie wird die Managementlösung PREVENT vorgestellt, die im Rahmen eines Forschungsprojektes im Förderschwerpunkt "IT-Sicherheit für Kritische Infrastrukturen" ITS|KRITIS entwickelt wird. Die Managementlösung PREVENT stellt Banken Dashboards zur Verfügung, welche durch nutzergerechte Aufbereitung eines Lagebildes bei der Risikoeinschätzung unterstützen. PREVENT soll insbesondere bei der Einschätzung des Risiko-Managements unter Compliance-Aspekten unterstützen. Dieses Lagebild erlaubt ein effektives und effizientes Risikomanagement für systemkritische Geschäftsprozesse.

Keywords: Sektor Finanz- und Versicherungswesen, Branche Banken, Rechenzentrum, Risikomanagement

9.1 Unternehmen

Die vorliegende Fallstudie entstand in dem Forschungsprojekt PREVENT des Förderschwerpunktes „IT-Sicherheit für Kritische Infrastrukturen" des Bundesministeriums für Bildung und Forschung. Die Fallstudie beschreibt ein IT-Sicherheitsmanagementsystem der nächsten Generation für die als kritisch eingestuften Prozesse einer Bank: die Managementlösung PREVENT. Insbesondere bei den stetig steigenden Compliance-Anforderungen an (europäische) Banken soll PREVENT die Entscheider unterstützen.

Akteure der Fallstudie sind ein fiktives Bankenrechenzentrum FutureRZ und die fiktive Bank FutureBank als Referenzmodelle für Banken und ihre Bankrechenzentren (siehe Abbildung 9-1).

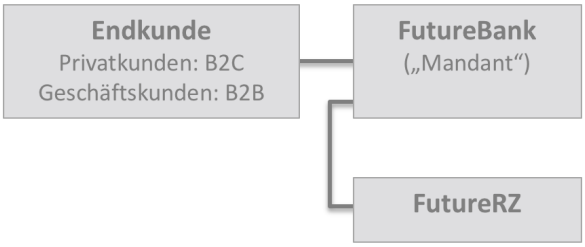


Abbildung 9-1: Zusammenhang FutureBank – Future RZ

9.1.1 Unternehmensprofil

Die FutureBank ist eine in Deutschland agierende Bank, die mit Endkunden sowohl im Bereich Privatkunden (B2C) als auch im Bereich Geschäftskunden (B2B) agiert. Das Bankenrechenzentrum FutureRZ ist ein Dienstleister, der für verschiedene Banken („Mandanten")

arbeitet. Diese Mandanten werden thematisch im FutureRZ strikt getrennt. Das FutureRZ kommt in der Regel nicht in direkten Kontakt mit Endkunden. Kunden des FutureRZ im eigentlichen Sinne sind die Fachabteilungen und die IT-Abteilungen der Mandanten.

Das FutureRZ bietet durch den Einsatz eines mehrstufigen redundanten und zertifizierten Sicherheitskonzeptes höchst mögliche Verfügbarkeit. Dem Kundenwunsch nach nahezu „Zero Downtime“ inkl. „Disaster Recovery“ wird hiermit entsprochen. Besonders wichtig sind dem FurtureRZ hierbei die Verfügbarkeit und die Sicherheit für die anvertrauten Bankdaten. Entsprechend bietet FutureRZ auf Mandanten zugeschnittenes und flexibles Datenmanagement und professionelle Betreuung der Mandanten auch in Fragen von Sicherheit und Verfügbarkeit an und möchte ein professionelles, auf die Bedürfnisse der Stakeholder angepasstes Risikomanagement anbieten. Die aktuellen gesetzlichen Rahmenbedienungen sorgen dafür, dass Risikomanagement bei allen Banken notwendig ist.

Das FutureRZ hat selbst erhebliche Kapazitäten und Kompetenzen, sowohl eigene Systeme zu entwickeln und weiterzuentwickeln wie auch den operativen Betrieb und Innovationen sicherzustellen. Mit seinen ca. 350 Mitarbeitern betreut FurtureRZ mehrere hundert Server und darauf die verschiedensten Anwendungen der Kunden.

9.1.2 Strategische Ausrichtung

Die **FutureBank** agiert in einer gewachsenen Infrastrukturlandschaft im Rahmen starker Regulierung sowie generell dem Sicherheitsanspruch an den Finanzsektor. Daher kann bei der FutureBank nicht so innovativ gearbeitet werden, wie sie es sich wünschen würde.

Das **FutureRZ** sieht sich selbst als hochspezialisierten Dienstleister für Banken und geht eine enge Partnerschaft mit den Banken ein. Das FutureRZ bietet seinen Mandanten, den Banken, Dienstleistungen an. Den Banken, die an die FutureBank mit ihren Rechenzentren Dienste outsourcen, will das FutureRZ nicht nur eine kosteneffiziente, sondern auch eine sichere Option bieten. Als Dienstleistungen werden beispielsweise die folgenden angeboten:

- Bereitstellen einer modernen und flexiblen IT-Infrastruktur zur Unterstützung der Prozesse der Kunden
- Auf Kundenbedürfnisse maßgeschneiderte IT-Lösungen in allen Bereichen (Netzwerk, Server, Datenbanken, Web-Portale usw.)
- Beratung der Kunden u. a. bei der Ausgestaltung von Geschäftsprozessen
- Consulting für Zertifizierungen, Compliance und Security

Zu diesen Leistungen soll nun ein Risikomanagement auf Geschäftsprozessebene für systemkritische Prozesse angeboten werden.

9.1.3 Fallstudienpartner

Name	Position im Unternehmen
Torsten Bollen	Project Manager, Wincor Nixdorf International GmbH
Steffi Rudel	Wissenschaftliche Mitarbeiterin, Universität der Bundeswehr München

9.1.4 IT-Sicherheit im Unternehmen

Sicherheit im Bankwesen wird für ganze Zahlungssysteme oder Geschäftsprozesse betrachtet – diese Sicht interessiert die Regulierungsbehörden ebenso wie das Management der Mandanten. Sowohl die FutureBank als auch das FutureRZ müssen sich daher an den Anforderungen des Gesetzes zur Erhöhung der IT-Sicherheit u. a. gemäß den Richtlinien im IT Grundschutz als Betreiber Kritischer Infrastrukturen orientieren.

Für Banken ist seit Basel II das Risikomanagement von Finanzrisiken ein wichtiges Thema. Diese Finanzrisiken werden vorrangig vom Basler Ausschuss für Bankenaufsicht in Zusammenhang mit der Eigenkapitalquote der Banken gesehen. Zunehmend treten heute jedoch die operativen Risiken in den Vordergrund. Dies sind Risiken, die sich aus Geschäftsprozessen, Menschen und Systemen sowie deren Interaktion miteinander ergeben. Dieser Umstand findet entsprechende Beachtung u. a. in den Katalogen des IT-Grundschutzes vom Bundesamt für Sicherheit in der Informationstechnik (BSI). Neben den bereits genannten Normen und Gesetzen müssen von Banken noch folgende beachtet werden:

- ISO 20000 Security- und Servicemanagementprozesse (IT-Service-Management)
- ISO 27001 (Norm für alle Themen im Kontext der Informationssicherheit)
- ISO 31000 Risikomanagement im Unternehmen
- ISO 50001 (Anforderungen an Energiemanagementsysteme)
- ANSI/TIA-942 (internationaler Standard, definiert Anforderungen an die Qualität von Rechenzentrums-Standorten und der darin umgesetzten Infrastruktur)
- KonTraG (Gesetz zur Kontrolle und Transparenz in Unternehmen)
- Basel I-III (Internationale Konvergenz der Eigenkapitalmessung und Eigenkapitalanforderungen / Anforderungen an die Qualität von Rechenzentrums-Standorten und der darin umgesetzten Infrastruktur)
- KWG (Kreditwesen-Gesetz)
- MaRisk (BaFin: Mindestanforderungen an das Risikomanagement)
- BCBS 239 (Grundsätze für die effektive Aggregation von Risikodaten und die Risikoberichterstattung)

Die **FutureBank** geht offensiv mit dem Thema IT-Sicherheit um und setzt die nötigen IT-Sicherheitsmaßnahmen in den Bereichen Technik, Organisation und Mensch um. Einige Beispiele hierfür sind:

- Einsatz von „State of the Art"-IT-Technik in den Rechenzentren
- Planung von Geschäftsprozessen vornehmlich unter Sicherheitsaspekten
- Fortlaufende Zertifizierung und Rezertifizierung in allen Bereichen
- Überprüfung der eigenen Prozesse durch interne Audits
- Schulungen und Weiterbildungen auf Richtlinien und Prozessen aller Mitarbeiter

Auch im **FutureRZ** wird IT-Sicherheit bereits umfangreich umgesetzt. Dies erfolgt beispielsweise in den folgenden Bereichen:

- Baulich (Gebäudemanagementsysteme, elektronische Zutrittssysteme, USV-Anlagen, Videoüberwachung, Alarmanlage, Notstromaggregate, Löschanlage etc.)

- Organisatorisch (Risikomanagement, Notfallkonzepte, geschultes Personal, standardisierte Prozesse)
- Technisch (Zugriffssicherheit, Rollen- und Berechtigungskonzepte, Firewalls, Antivirensysteme, Verschlüsselungssysteme etc.)
- Proaktives Monitoring der erhobenen Daten, um direkt Auffälligkeiten zu erkennen und ggf. Gegenmaßnahmen einzuleiten

9.2 Kritische Infrastruktur

9.2.1 Einordnung als KRITIS

Kritische Infrastrukturen (KRITIS) werden vom BSI grundsätzlich in verschiedene Sektoren untergliedert. Die Fallstudie mit den beteiligten Playern siedelt sich in dem Sektor Finanz- und Versicherungswesen an [1].

Ausschlaggebend für die Einordnung als KRITIS ist die kritische Versorgungsdienstleistung. Die Abwicklung des Zahlungsverkehrs ist eine kritische Dienstleistung sowohl für Privatpersonen (Erhalt des Gehalts, Bezahlen von Rechnungen, Miete etc.) als auch für Unternehmen. Sie hat damit eine sektorübergreifende Bedeutung und ist daher die wesentliche kritische Versorgungsdienstleistung des Finanzdienstleistungssektors [1].

Der Finanzsektor stellt unter den KRITIS eine Besonderheit dar, da hier die „Finanzmittel – im Gegensatz zu anderen Wirtschaftsbereichen – nicht nur die Rahmenbedingung für das Wirtschaften, sondern den Geschäftsgegenstand selbst darstellen“ [1].

Die besondere Relevanz der Zahlungssysteme für den bankübergreifenden Zahlungsverkehr als KRITIS ist weiterhin daran erkennbar, dass die Zahlungssysteme EURO1, STEP2 (beide EBA-Clearing) und TARGET2 (Eurosystem) durch die Europäische Zentralbank (EZB) als Systemically Important Payment Systems (SIPS) eingestuft wurden. Diese Systeme müssen erhöhte Anforderungen erfüllen und unterliegen der direkten Aufsicht durch die Europäische Zentralbank.

Als weitere Besonderheit sind in Bankenrechenzentren sowohl die Geschäftsprozesse als auch die Infrastruktur kritisch, da ausschließlich mit Daten und nicht mit physischen Waren gehandelt wird.

9.2.2 Risikoanalyse

Die Risikoanalyse zeigt, dass gesellschaftlich starke Abhängigkeiten vom Finanzsektor bestehen. Im äußersten Fall würde der Ausfall der Bankenrechenzentren den dauerhaften Zusammenbruch des Zahlungssystems bedeuten und damit den Ausfall der Versorgung der Gesellschaft mit Zahlungsmitteln zur Folge haben.

Somit stehen andere KRITIS in einer starken Abhängigkeit, wie die folgende Ausführung verdeutlicht (siehe Abbildung 9-2).

So kann im schlimmsten Fall keine Miete nicht mehr überwiesen werden und vom Endkunden nicht mehr auf das Konto zugegriffen werden. In der Folge können keine Nahrungsmittel mehr gekauft werden (KRITIS-Sektor Ernährung), es kann nicht mehr getankt werden

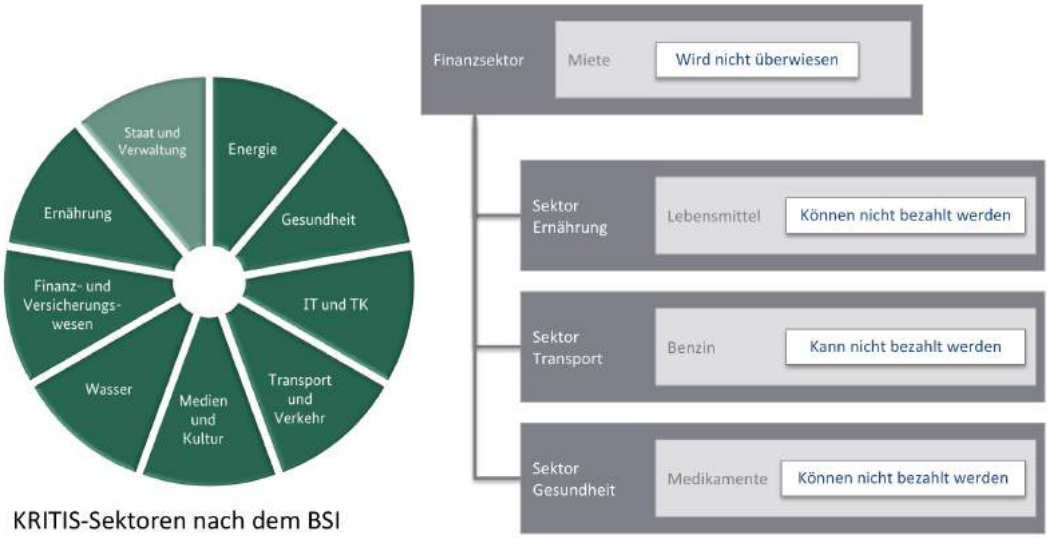


Abbildung 9-2: Auswirkungen eines Ausfalles im Finanzsektor; Quelle linkes Bild: [2]

(Transport und Verkehr), es können keine Medikamente mehr in der Apotheke bezahlt werden (Gesundheit).

Ebenso sind weitere Kaskadeneffekte denkbar. So kann z. B. die Stromversorgung zusammenbrechen, da Strom an der Börse gehandelt wird und dies ebenfalls nicht mehr möglich ist (Energie).

Ein systemkritischer Geschäftsprozess des FutureRZ, der von mehreren Banken als Mandanten genutzt wird, könnte zu einem Ausfall von Finanzdienstleistungen in erheblichem Umfang führen – auch wenn ein Dienstleister wie das FutureRZ auf einem branchenüblichen sehr hohen Sicherheitsniveau arbeitet.

9.3 Managementlösung PREVENT

9.3.1 Hintergrund und Rahmenbedingungen

In Banken sind per Gesetz grundsätzlich die Vorstände für das Risikomanagement verantwortlich und haftbar zu machen. Aus diesem Grund soll dieser Managementebene mit der Managementlösung PREVENT ein Dashboard auf Basis eines Lagebildes (Compliance-Status) zur Verfügung gestellt werden. Dieses soll helfen, Risiken in Echtzeit konkret einzuschätzen und zu bewerten und anschließend geeignete Maßnahmen einzuleiten. Zu den potenziellen Bedrohungen zählen:

- Server- oder Service-Ausfälle
- Attacken von innen und außen (Malware)
- Ransomware-Attacken

Die Managementlösung PREVENT wird als Dienstleistung des FutureRZ für die FutureBank implementiert.

9.3.2 Status quo und gemeinsames Lagebild zur Risikobeurteilung

Mithilfe der Managementlösung PREVENT sollen den Verantwortlichen fundierte Gründe für oder gegen eine Maßnahme zur Entscheidungsunterstützung an die Hand gegeben werden. Wirkungsketten sollen erkannt und potenzielle Aggregationen von Risiken offengelegt werden.

Um dies umzusetzen, unterstützt die Managementlösung PREVENT bei

- der Modellierung von Businessprozessen
- der Analyse von Betriebsprozessen
- der Analyse der unterstützenden Infrastruktur auf Funktions-, Software-, Netzwerk- und Hardwareebene

Dabei arbeitet PREVENT mit **einer** zusammengeführten Datenbasis, aus der verschiedene Sichten bedarfsgerecht erzeugt werden. Als Herausforderungen sind hier die Big-Data-Analyse sowie das Erzeugen anwendungsgerechter Sichten zu meistern.

Aktuell existiert eine Vielzahl von Datenquellen und Analysen zur Erkennung und Untersuchung von Sicherheitsproblemen. So schreibt jedes IT-System verschiedene Log-Files. Die verschiedenen Akteure der FutureBank und des FutureRZ nutzen bislang unterschiedliche Werkzeuge, um diese Daten aufzubereiten und anschließend in ein aktuelles Lagebild zu überführen. Auch wurden bisher die verschiedenen Sichten der IT, der Sicherheit und des Business separat abgebildet und Korrelationen zwischen verschiedenen, mit unterschiedlichen Werkzeugen analysierten Daten konnten im Wesentlichen nur bei überlappenden Daten gewonnen werden. Die folgende Abbildung 9-3 verdeutlicht dies.

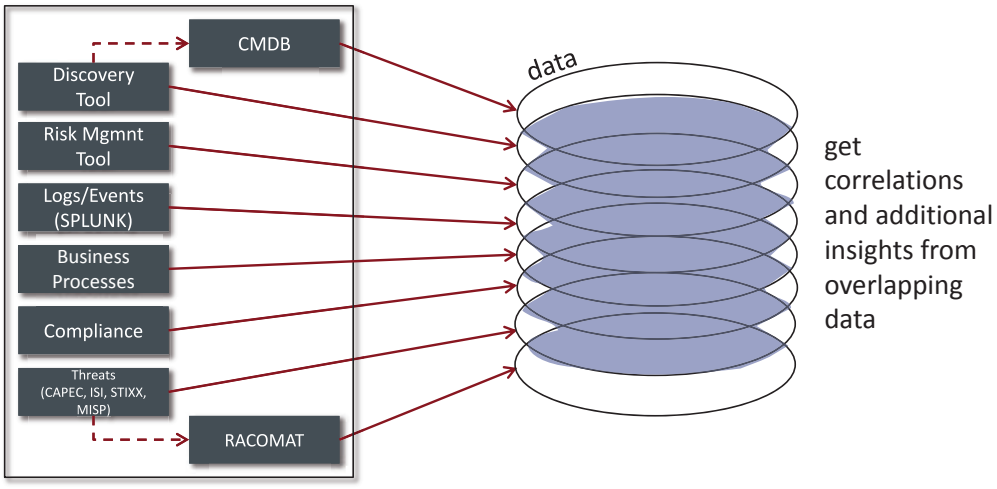


Abbildung 9-3: Aktuelle Situation

Ziel der Managementlösung PREVENT ist es, diese Sichten zu bündeln. Es werden Daten aus SIEM-Systemen ebenso verwendet wie z. B. die Informationen der Zutrittskontrolle. So sollen Bedrohungspotenziale besser und schneller erkannt und im Lagebild abgebildet werden, was die Basis für proaktive Handlungsanweisungen bilden kann. Die folgende Abbildung 9-4 zeigt die implementierte Managementlösung PREVENT.

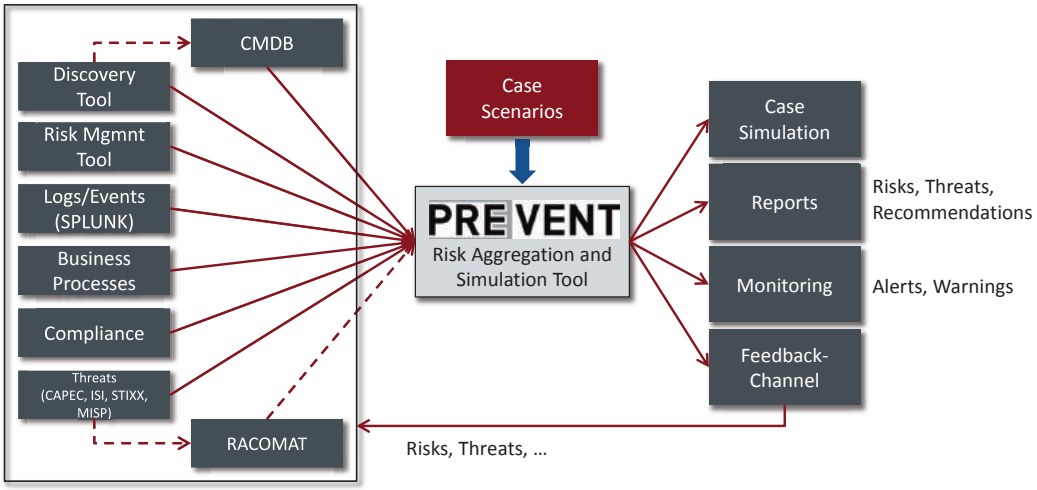


Abbildung 9-4: Implementierte Managementlösung PREVENT

Der Kern des neuen Risikomanagements ist das „Risk Aggregation and Simulation Tool" – es erhält Informationen von der Configuration Management Database (CMDB) sowie einer Reihe von anderen Werkzeugen (die generischen Namen sind in Abbildung 9-4 angegeben). RACOMAT ist ein Werkzeug für das Risiko-Managements, das insbesondere das Risiko-Assessment mit Sicherheitstests kombiniert und damit eine Berechnung von Risiken durchführt. Ergebnisse des Risk-Aggregation- und Simulation-Ansatzes gehen ein in Simulationen von Fällen, Berichten, Monitoring und werden in Feedbackkanäle eingespeist.

9.3.3 Abhängigkeiten zwischen Prozessen und Anwendungen

Grundsätzlich lassen sich die Prozesse und Anwendungen in einem Finanzunternehmen auf verschiedenen Ebenen betrachten. Die folgende Abbildung 9-5 visualisiert diese Ebenen.

Tritt nun ein Vorfall auf einer der Ebenen auf, so darf dieser nicht isoliert auf seiner Ebene betrachtet werden. Vielmehr ist es wichtig, hier die Zusammenhänge zu erfassen. Denn um der Managementebene ein aussagekräftiges Lagebild zur Verfügung stellen zu können, müssen die Risiken über alle Ebenen aggregiert werden.

Die folgende Abbildung 9-6 visualisiert daher den Zusammenhang zwischen den Ebenen und welche Auswirkungen ein Vorfall auf der Netzwerkebene auf die anderen Ebenen haben kann.

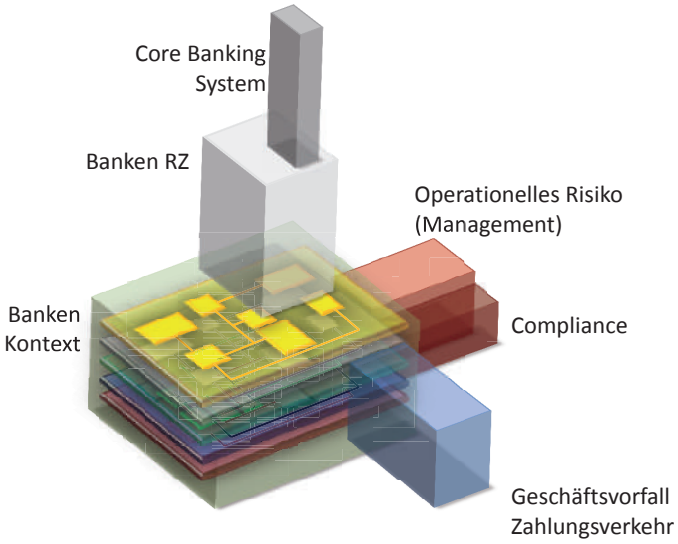


Abbildung 9-5: Ebenen eines Finanzunternehmens

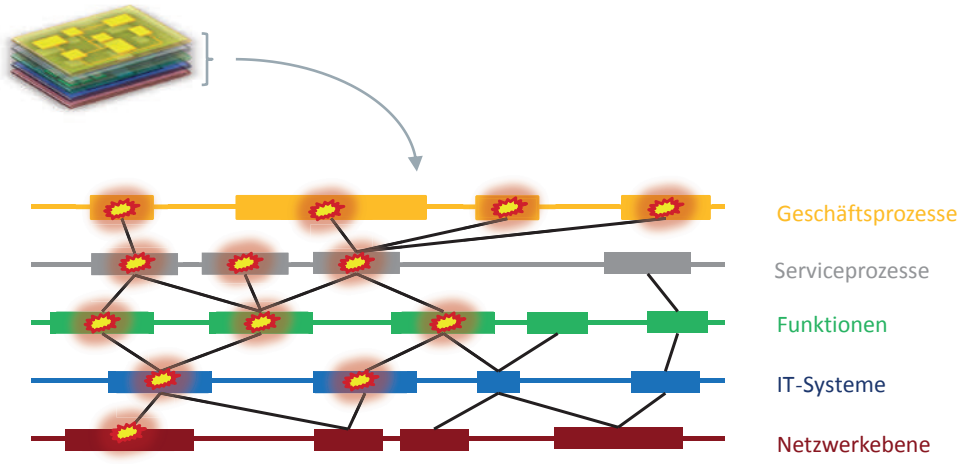


Abbildung 9-6: Wechselwirkungen zwischen den Ebenen

Es ist zu beachten, dass alle Ebenen unterhalb der Geschäftsprozesse (Serviceprozesse, Funktionen, IT Systeme und Netzwerkebene) vom FutureRZ betreut und abgewickelt werden.

9.4 Konkret betrachtetes Szenario

Die Fallstudie ist auf den Prozess des Zahlungsverkehrs fokussiert. Konkret wird als Referenzprozess eine Überweisung innerhalb Deutschlands herausgegriffen, was einen typischen Geschäftsprozess der FutureBank darstellt.

Es wird betrachtet, wie sich der Ausfall eines Switches (= Netzwerkebene) auf den Überweisungsprozess (= Geschäftsprozesse) auswirkt.

9.4.1 Mögliche Risiken

Ein Ausfall eines Switches kann verschiedene Gründe haben. Eine mögliche Ursache stellen dabei Hacker-Angriffe auf die Software der Switche dar. Eine andere denkbare Ursache wäre ein Defekt der Hardware des Switches. Fällt ein Switch aus, können sich daraus verschiedene Risiken ergeben. Einige davon sind im Folgenden beispielhaft aufgelistet:

- Kurzfristiger Ausfall von Hardware
- Software-Probleme beim Neustart der Systeme
- Datenleitungen nicht erreichbar (Server, Router, andere RZ)

Switches sind aus Kostengründen oft nicht redundant ausgelegt und bei einem Fehler der Firmware bzw. bei einem Exploit einer Schwachstelle der Firmware eines Switches kann erfahrungsgemäß schnell ein ganzes Rechenzentrum betroffen sein.

9.4.2 Geschäftssicht

In der folgenden Abbildung 9-7 wird der konkrete Geschäftsprozess einer Überweisung mit den beteiligten Institutionen visualisiert.

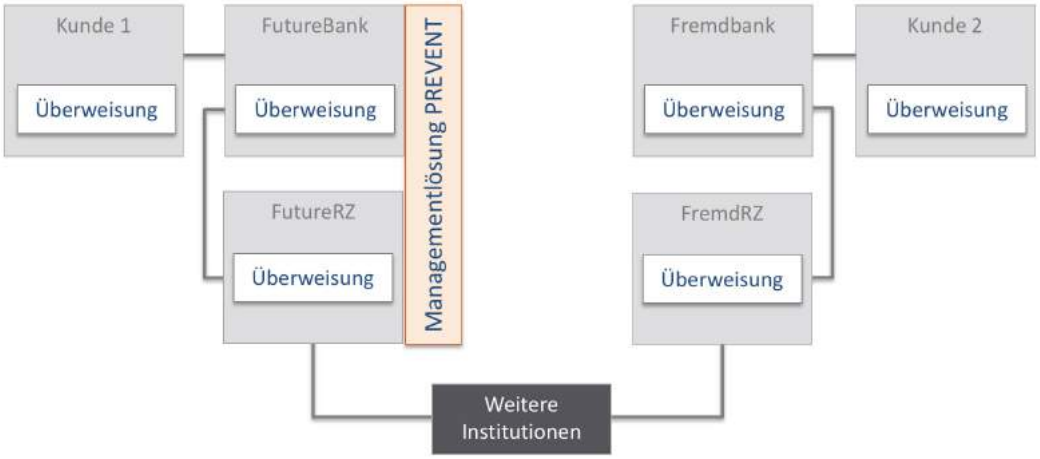


Abbildung 9-7: Konkreter Geschäftsprozess Überweisung

Um den Geschäftsprozess in den Kontext zu setzten, werden in der folgenden Abbildung 9-8 die Instanzen, welche an dem Prozess einer Überweisung beteiligt sind, aufgezeigt. Um die Komplexität des Prozesses zu verdeutlichen, wird hier der Zahlungsverkehr innerhalb Europas dargestellt.

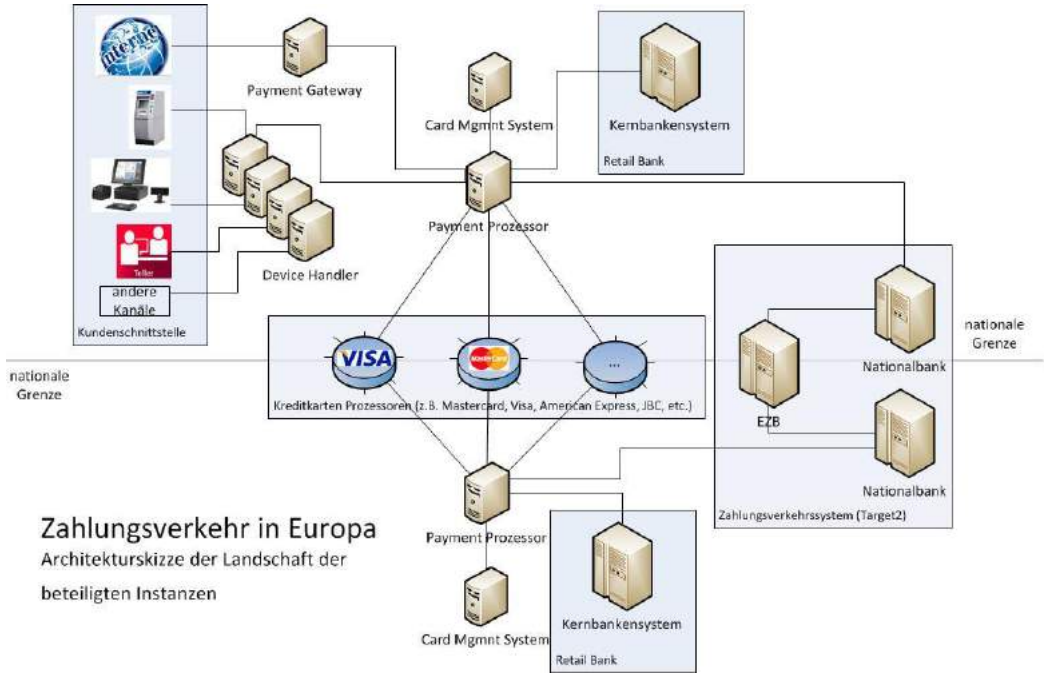


Abbildung 9-8: Die am Referenzprozess beteiligten Instanzen

Fällt nun auf der Netzwerkebene der Switch aus, kann dies Auswirkungen bis auf die Ebene der Geschäftsprozesse haben. In der folgenden Abbildung 9-9 wird die Sicht auf die verschiedenen Ebenen aus Abbildung 9-6 aufgegriffen und die möglichen Auswirkungen des Ausfalles eines Switches werden visualisiert.

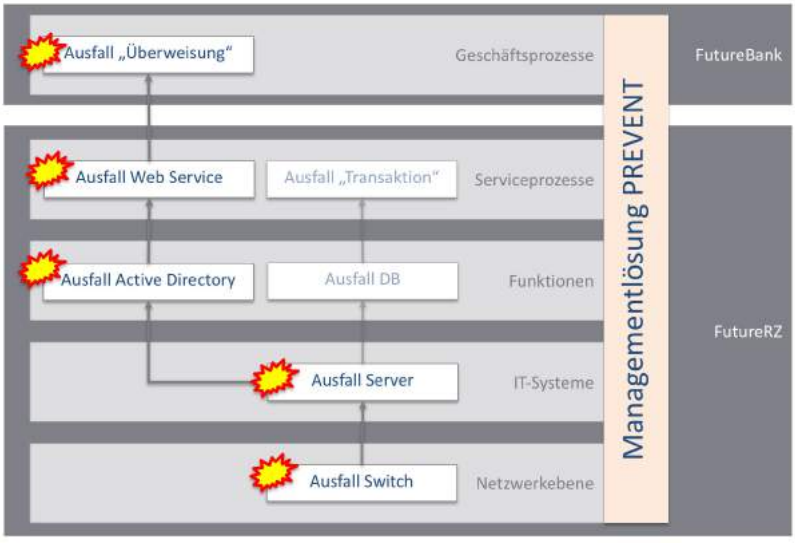


Abbildung 9-9: Auswirkungen eines Ausfalls des Switches auf die verschiedenen Ebenen

9.4.3 Anwendungs- und technische Sicht

Die folgende Abbildung 9-10 der Infrastruktursicht setzt das FutureRZ in den Kontext der angebundenen Netzwerke und Institutionen. Abbildung 9-10 illustriert das Prinzip von Redundanz von Rechenzentren mit den Abhängigkeiten von Strom- und Wasserversorgung und dem Internet.

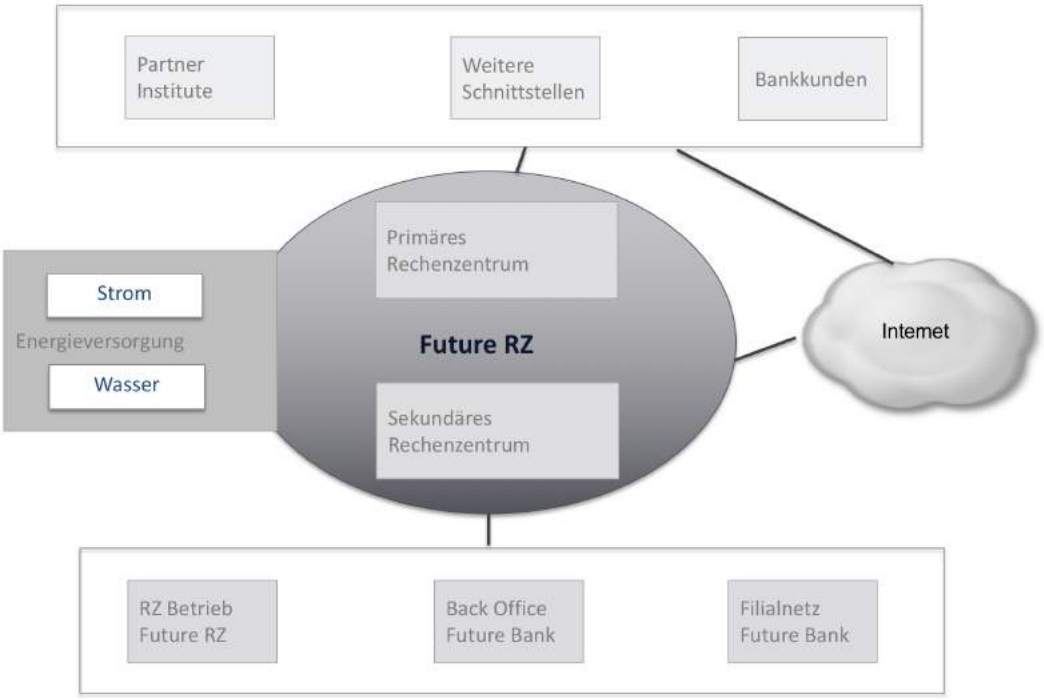


Abbildung 9-10: FutureRZ und angebundene Netzwerke

9.5 Modernes IT-Risk-Management mit PREVENT

9.5.1 Zusammenfassung

Die IT-Sicherheit ist im Finanzsektor ein wichtiges Thema. Dies trifft insbesondere auf systemrelevante Bereiche wie die Bankenrechenzentren zu.

Ziel der Managementlösung PREVENT ist die gezielte Information (Dashboarding) unterschiedlicher Nutzergruppen im Unternehmen. So soll der Vorstand genauso über die aktuelle Lage informiert werden wie ein Administrator.

Die Managementlösung PREVENT erlaubt neue Risikobewertungen von Aspekten und Zusammenhängen, die bisher nicht betrachtet wurden, und löst damit die alten, oft heterogenen Risikomanagementlandschaften bei den Banken ab.

Als wesentliches Ergebnis der Einführung der Managementlösung PREVENT können nun von der Managementebene aggregierte Risiken erkannt werden, die über dem als kritisch

eingestuften Schwellwert der Bank liegen und die zuvor als Einzelrisiken nicht im Fokus von Minimierungsmaßnahmen waren. Die Managementlösung PREVENT hat damit eine Sensibilität für relevante Sicherheitsrisiken geschaffen, die nun aktiv optimiert werden können.

9.5.2 Einführungsstrategie

Die Managementlösung PREVENT wird als Projekt vom Rechenzentren Hand in Hand mit den Banken eingeführt. Alle Fachbereiche der Bank müssen einbezogen sein. Hier kommt dem Rechenzentrum als Dienstleister auch eine starke vernetzende Funktion zu, da alle betreffenden Fachabteilungen der Banken an einen Tisch gebracht werden müssen.

Da ein zentrales System dafür verantwortlich ist, die Funktionen der Managementlösung PREVENT zu übernehmen, erwartet das Projektteam eine einfache Implementierung des Systems in die vorhandene Infrastruktur. Die offenen Schnittstellen ermöglichen zudem die Hinzunahme von Systemen, die klassisch getrennt behandelt werden, z. B. Gefahren-Managementsysteme, Gebäudeleittechnik.

Der angestrebte Ansatz von PREVENT ist generisch und modular. Daher wird die Managementlösung PREVENT nicht in einem Schritt für alle Bereiche gleichzeitig umgesetzt, sondern es wird vielmehr zunächst ein Referenzprozess als Pilotprojekt in einem Geschäftsbereich durchgeführt, der stark betroffen ist. So können schnelle Effekte erzielt und andere Bereiche von der Managementlösung PREVENT überzeugt werden.

Ebenfalls bedingt durch den generischen Ansatz kann der Ansatz später auch auf andere Geschäftsprozesse der Banken (neben dem im Pilotprojekt betrachteten Zahlungsverkehr) übertragen werden.

9.5.3 Erfolgsfaktoren

Da sich die Managementlösung PREVENT an die Management-Ebene wendet, muss diese für Erfolg des Projektes frühzeitig eingebunden und für das Projekt gewonnen werden.

Um die Akzeptanz für die Managementlösung PREVENT zu erhöhen, wird weiterhin so wenig Einfluss wie möglich auf bestehende Prozesse genommen.

9.5.4 Ausblick

Als Ausblick bleibt zu sagen, dass die Managementlösung PREVENT nicht auf Bankenrechenzentren limitiert ist, sondern vielmehr überall dort eingesetzt werden kann, wo Business-Prozesse mithilfe von IT-Systemen unterstützt werden.

Die Managementlösung PREVENT soll in seiner Gesamtlösung weitere Dashboards enthalten, die z. B. Security- & Compliance-Mitarbeiter mit Daten für ihre Arbeit unterstützen.

Sinnvoll erscheinen hier z. B. folgende Nutzergruppen-gerechte Dashboards:

- Business Process Owner
- Compliance bzw. Security Officer
- Administrator

9.6 Danksagung

Wir danken dem Bundesministerium für Bildung und Forschung (BMBF) für die Möglichkeit der Forschung im Rahmen des Projektes VeSiKi, Förderkennzeichen 16KIS0213K und des Projektes PREVENT, Förderkennzeichen 16KIS0182K.

9.7 Literaturverzeichnis

[1] BSI, 2015. KRITIS-Sektorstudie Finanz- und Versicherungswesen – Analyse Kritischer Infrastrukturen in Deutschland, Bonn.

[2] BSI und BBK (Hrsg.), 2009. Sektoren- und Brancheneinteilung Kritischer Infrastrukturen. Verfügbar unter: https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/sektoren_node.html [zugegriffen: 29-Apr-2018].

10 Informationssicherheit bei SAP SE: Die längste Human Firewall der Welt

Ulrike Lechner, Universität der Bundeswehr München
Andreas Rieb, Universität der Bundeswehr München
Tamara Gurschler, Universität der Bundeswehr München

Die Human Firewall ist eine Kampagne zur Informationssicherheit der SAP SE (kurz SAP). Key Visual dieser Kampagne 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 dann mit ihrem Foto zusammen mit einem individuellen Statement zur Informationssicherheit Teil der Human Firewall werden. Die längste Human Firewall der Welt ist ein starkes Signal der Verpflichtung der Mitarbeiter dem Thema Informationssicherheit gegenüber. Angestrebt wird ein Eintrag ins Guinness-Buch der Rekorde für die längste Human Firewall der Welt.

Keywords: Mitarbeitersensibilisierung, Awareness, Informationssicherheit, Human Factor, Konzernsicherheit

10.1 Unternehmen

10.1.1 Unternehmensprofil

Die SAP SE (kurz SAP) ist im Bereich Unternehmensanwendungen weltweit der umsatzstärkste Anbieter von Software und Softwareservices und gemessen an der Marktkapitalisierung der weltweit drittgrößte unabhängige Softwarehersteller. Die SAP hat mehr als 345.000 Kunden in mehr als 180 Ländern, mehr als 88.000 Mitarbeiter in über 130 Ländern und mehr als 87 % der Forbes-Global-2.000-Unternehmen sind SAP-Kunden.

Softwareprodukte und Services von SAP sind SAP S/4HANA und SAP Business One. Im Portfolio von SAP nehmen Dienstleistungen und Cloud-basierte Lösungen eine immer wichtigere Rolle ein und so sind der Schutz der eigenen Informationen ebenso wie der Schutz der Daten der Kunden ein zentrales Thema der SAP. Vertrauen der Kunden in SAP sowie in die Produkte und Dienstleistungen von SAP ist für SAP essenziell: „Vertrauen ist die ultimative Währung". So erfüllt SAP als internationaler Konzern und vor allem als Anbieter von Cloud-basierten Lösungen ebenso wie auch seine Kunden vielfältige Anforderungen in Bezug auf Informationssicherheit und Compliance. „Protect yourself! Protect SAP! Protect the Cloud! Protect the Customer!" [1] beschreibt die Rolle, die der Einzelne für die Sicherheit von SAP, der Cloud und der Kunden hat.

Die Mitarbeiter der SAP haben eine zentrale Rolle für den Schutz der Daten des Unternehmens. „Der Mensch ist und bleibt das wichtigste Glied in der Security Kette!" [3] Ein einziger Mitarbeiter, der Sicherheitsrichtlinien nicht einhält, kann SAP verwundbar machen und – wenn ein Kunde mangelnde Sorgfalt im Umgang mit Informationen oder Sicherheits-

richtlinien bemerkt – das Vertrauen der Kunden in SAP mit seine Produkten und Dienstleistungen erschüttern. Eine Unaufmerksamkeit eines Mitarbeiters kann genügen, dass das Unternehmen für eine Schadsoftware verwundbar wird. Dieser menschliche Faktor der Informationssicherheit ist das Thema dieser Fallstudie entsprechend einem Motto „Sicherheit beginnt im Kopf“ [1] der Informationssicherheit von SAP.

Die Human Firewall ist ein zentrales Element der SAP-internen Kampagne zur Informationssicherheit und ein Symbol dafür, dass die Mitarbeiter die SAP mit ihren Informationen und den Informationen der Kunden schützen: Mitarbeiter bilden mit verschränkten Armen eine Kette, die keine Bedrohung zu SAP durchlässt (Abbildung 10-1). Dieses Key Visual der Human Firewall ist ein Symbol für das Bewusstsein für Informationssicherheit bei SAP und macht das Thema Informationssicherheit nach innen und nach außen hin sichtbar.

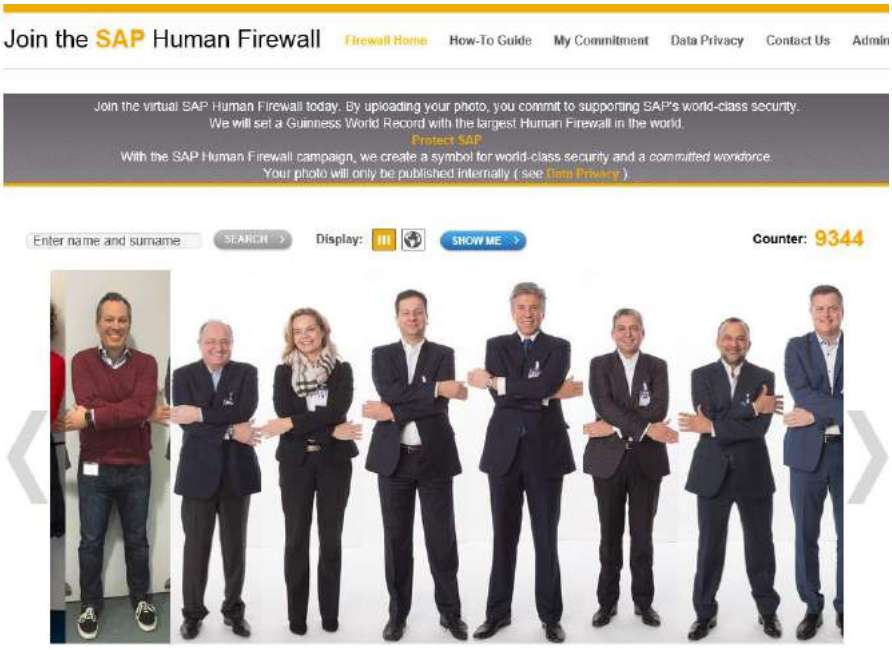


Abbildung 10-1: Human Firewall der SAP; Quelle: SAP SE

Mitarbeiter werden im Kontext von Schulungen zur Informationssicherheit, Aktionen auf Events oder z. B. über eine Fotobox eingeladen, sich an der Human Firewall mit der Fotokampagne zu beteiligen und sich aktiv für die Informationssicherheit von SAP zu engagieren.

Die Kampagne Human Firewall wird von der Abteilung Informationssicherheit als Teil des Bereichs Konzernsicherheit durchgeführt. Neben der Kampagne Human Firewall führt die Abteilung Informationssicherheit weitere Aktionen durch: Diese sind u. a. (verpflichtende) Schulungen zur Informationssicherheit, der Awareness-Check als ein Survey mit fünf Fragen zur Awareness sowie ein Webportal als zentrale Anlaufstelle mit Informationen zur Informationssicherheit.

10.1.2 Strategische Ausrichtung

SAP will Unternehmen dabei unterstützen, sich dem digitalen Wandel zu stellen, um nachhaltig wettbewerbsfähig und zukunftsorientiert zu sein. „Wir helfen, die Abläufe der weltweiten Wirtschaft und das Leben von Menschen zu verbessern", lautet die Vision von SAP [2]. SAP prognostiziert einen Wandel durch digitale Transformation, der sowohl die Nutzung von Technologie als auch die Gesellschaft verändert. Als Beispiele werden von SAP Technologietrends wie Hyperkonnektivität, Cloud Computing und Big Data, aber auch wirtschaftliche Entwicklungen wie Urbanisierung, die Ökonomie des Teilens, demografische Veränderungen und die Ressourcenknappheit genannt.

Die Services der SAP sollen den Kunden eine Plattform für deren digitale Strategie und digitale Geschäftsprozesse bieten – und das stets unter dem Aspekt der Anpassungsfähigkeit an den digitalen Wandel. Die Bedeutung der Dienstleistungen, wie z. B. die auf der Hana Plattform basierten Cloud Services, wächst und damit auch die Kritikalität der Produkte und Dienstleistungen von SAP [2], [3].

10.1.3 Fallstudienpartner

Name	Position im Unternehmen
Julia Langlouis	Director Global Security Awareness, Training & Communication, SAP SE, Walldorf
Ulrike Lechner	Professorin für Wirtschaftsinformatik, Universität der Bundeswehr München
Andreas Rieb	Wissenschaftlicher Mitarbeiter, Universität der Bundeswehr München
Tamara Gurschler	Wissenschaftliche Mitarbeiterin, Universität der Bundeswehr München

10.1.4 Informationssicherheit im Unternehmen

Die Informationen von SAP müssen ebenso wie die Informationen der Kunden in den Systemen und den Cloud Services der SAP geschützt werden. Dadurch ist SAP – ebenso wie ihre Kunden auch – verpflichtet, eine Vielzahl von Compliance-Anforderungen zu erfüllen. So fordert z. B. das IT-Sicherheitsgesetz von den Betreibern Kritischer Infrastrukturen ein IT-Sicherheitsmanagement. Neben der organisatorischen IT-Sicherheit ist IT-Sicherheit zudem ein wichtiges Thema hinsichtlich der angebotenen Produkte und Dienstleistungen der SAP: So bietet SAP z. B. integrierte Sicherheitsservices der SAP Cloud-Plattform mit sicherer Authentifizierung, Single-Sign-on-Funktionen, On-Premise-Integration sowie Self-Services wie die Registrierung und das Zurücksetzen von Passwörtern für Mitarbeiter, Kunden, Partner und Benutzer sowie Lösungen für IT-Sicherheitsmanagement an. SAP will mit seinen Produkten und Dienstleistungen den Anteil an Geschäftsprozessen, der über SAP-Systeme gesteuert wird, erhöhen und zunehmend Cloud Services anbieten.

Informationssicherheit ist ein zentrales Thema der gesamten SAP. Als Anbieter von unternehmenskritischen Softwareprodukten und Dienstleistungen ist Vertrauen die ultimative Währung (vgl. Abbildung 10-2) – diese Einstellung wird zudem durch den Slogan „Trust, Security, SAP" öffentlich illustriert und untermauert hier den Stellenwert der Sicherheit für SAP. Mehrere Betriebsbereiche nehmen sich der Themen rund um die Informationssicherheit an.

So gibt es Bereiche für die konzernweite Informationssicherheit, aber auch Cybersicherheit und IT-Sicherheit. Neben der Fotokampagne, wie die Human Firewall zum Aufgabengebiet Informationssicherheit, die sich weltweit an alle Mitarbeiter der SAP richtet, gibt es spezielle Aktivitäten zur IT-Sicherheit, die z. B. speziell auf das Management oder die Software-Entwickler abzielen.

Jeder Mitarbeiter des Unternehmens SAP ist für Vertrauen und Sicherheit zuständig – das ist ein Thema, das die Abteilung Informationssicherheit mit ihrer Kampagne zur Informationssicherheit kommuniziert. Die Informationssicherheit adressiert weltweit alle Mitarbeiter der SAP. Die Informationssicherheitskampagne umfasst seit 2012 eine einstündige Pflichtschulung zur Informationssicherheit für alle Mitarbeiter des Unternehmens. Andere Maßnahmen zur Informationssicherheit sind Tip of the Month, 100-Sekunden-Videos zu unterschiedlichsten Themen der Informationssicherheit, E-Books, Quiz sowie ein Incident Reporting Tool mit aktuellen Hinweisen und Informationen, was bei einem Incident zu tun ist. Neben diesen Maßnahmen wurde ferner der im Oktober stattfindende „Cyber Security Month" 2016 erstmalig bei der SAP mit einer Reihe von Events gelebt. Im Awareness-Check – einer Umfrage zum Thema Informationssicherheit und Awareness – werden seit 2012 die dieselben fünf Fragen gestellt und so das Bewusstsein für Informationssicherheit bei SAP evaluiert. Die Maßnahmen zur Informationssicherheit sind in einem Webportal gebündelt für alle Mitarbeiter zugänglich (siehe Abbildung 10-4).

10.2 Kritische Infrastruktur

10.2.1 Einordnung als KRITIS

Die SAP ist entsprechend dem IT-Sicherheitsgesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom Juli 2015 nicht als Kritische Infrastruktur einzustufen. Allerdings verwenden viele Betreiber Kritischer Infrastrukturen SAP-Systeme. Ein Ausfall von SAP-Systemen bei einem oder auch bei mehreren Anwendern könnte zu einer weitreichenden Beeinträchtigung des öffentlichen Lebens und der öffentlichen Sicherheit führen.

10.2.2 Risikoanalyse

Die Unternehmenssoftware von SAP wird in vielen Unternehmen, die entsprechend dem IT-Sicherheitsgesetz als Kritische Infrastruktur eingestuft sind, eingesetzt. In SAP-Systemen liegen u. a. Kundendaten oder es werden Dokumente und sensible Informationen verwaltet. Solche Informationen sind ein lukratives Angriffsziel für Hacker. Darüber hinaus steuern SAP-Systeme ganze Unternehmen hinsichtlich ihrer Geschäftsprozesse und Anwendungen in Echtzeit. Ein Ausfall oder eine Beeinträchtigung dieser Systeme kann damit (un-)mittelbar zu einer Beeinträchtigung von Produkten, Dienstleistungen oder sogar Ausfällen von Kritischen Infrastrukturen führen.

Vor dem Hintergrund dieser Kritikalität von SAP-Systemen für die Steuerung von Unternehmen in Echtzeit gewinnt das Thema Informationssicherheit immer mehr an Bedeutung. Vertrauen in das Unternehmen und seine Produkte und Dienstleistungen ist für SAP essen-

ziell. Mitarbeiter sind für die Informationssicherheit wichtig; denn Mitarbeiter benötigten nicht nur Informationen, sondern sollen aktiviert werden, selbst zur Informationssicherheit beizutragen. Dies soll durch die Kampagne erreicht werden. Kunden können das Vertrauen in SAP und seine Produkte und Dienstleistungen schnell verlieren, wenn die Mitarbeiter von SAP keine Awareness hinsichtlich Informationssicherheit zeigen oder gegen Sicherheitsrichtlinien verstoßen. Deshalb will SAP unternehmensintern und auch gegenüber den Kunden demonstrieren, dass sowohl die Produkte als auch die Mitarbeiter sicher sind.

10.3 Das Projekt Human Firewall

Im Jahr 2012 hat SAP mit verpflichtenden Schulungen zur Informationssicherheit begonnen und die Human Firewall als Fotokampagne innerhalb der Informationssicherheitskampagne initiiert. Das Key Visual der Human Firewall ist ein Bild von Mitarbeitern mit verschränkten Armen. Mitarbeiter fotografieren sich mit verschränkten Armen. Eine Anwendung erstellt anschließend aus den Einzelbildern dynamisch neue „Firewalls", die im Intranet abrufbar sind (vgl. Abbildung 10-2 und Abbildung 10-3). Zudem können Mitarbeiter ihre Teilnahme an der Human Firewall mit einer individuellen Aussage zur Informationssicherheit verknüpfen.

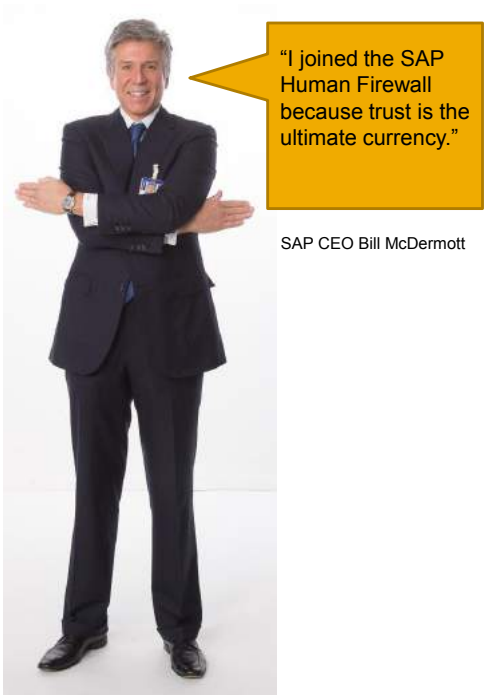


Abbildung 10-2: Eine Human Firewall mit Poster der Vorstandsmitglieder und Mitarbeiter von SAP als Human Firewall; Quelle linkes und rechtes Bild: SAP SE

Abbildung 10-2 zeigt verschiedene Varianten des Key Visuals der Human Firewall. Abbildung 10-2 (links) zeigt das Top-Management von SAP und die Leiterin der Abteilung Informationssicherheit als SAP Human Firewall auf einem Poster: Mit diesen Bildern und Postern werden die Mitarbeiter von SAP eingeladen, sich der Human Firewall anzuschließen: „Join the SAP Human Firewall". Abbildung 10-2 (rechts) zeigt den CEO von SAP mit seiner Aussage „Vertrauen ist die ultimative Währung".

Abbildung 10-3: Ausschnitt aus einer Präsentation mit Human-Firewall-Bild und Anleitung für die Fotografien zur Human Firewall; Quelle: SAP SE

Die Human Firewall ist auf der Intranetplattform ein zentrales Element mit hohem Aufmerksamkeits- und Identifikationswert für die Mitarbeiter. Abbildung 10-3 zeigt eine dynamisch von der Anwendung zusammengesetzte Human Firewall von Mitarbeitern, Vorständen und Leiterin des Bereichs Informationssicherheit sowie die Anleitungen für das Foto für die Human Firewall.

Die Aktionen der Abteilung Informationssicherheit sind auf einem Webportal gebündelt (siehe Abbildung 10-4). Das Webportal zur Informationssicherheit zeigt das Key Visual der Fotokampagne Human Firewall und beinhaltet weitere Informationsangebote zur Informationssicherheit. Ein großes Thema ist „Faktor Mensch" mit Hinweisen zu dem aktuellen Thema „Social Engineering". Im Webportal befindet sich auch der Zugang zum verpflichtenden Informationssicherheitstraining. Außerdem befindet sich im Webportal ein Link zu einem Incident Reporting Tool mit Blogfunktion. Dieser Blog enthält Informationen zur aktuellen Bedrohungslage, z. B. über Ransomware.

Neben der Human Firewall sind eine verpflichtende Schulung zur Informationssicherheit und eine Umfrage zu Informationssicherheit und Awareness bei SAP wichtige Elemente der Informationssicherheitskampagne. Nach der Teilnahme an der verpflichtenden Schulung als E-Learning-Modul und einer bestandenen Überprüfung des Wissens zur Informationssicherheit können die Mitarbeiter optional an der Human Firewall mit ihrem Foto teilnehmen.

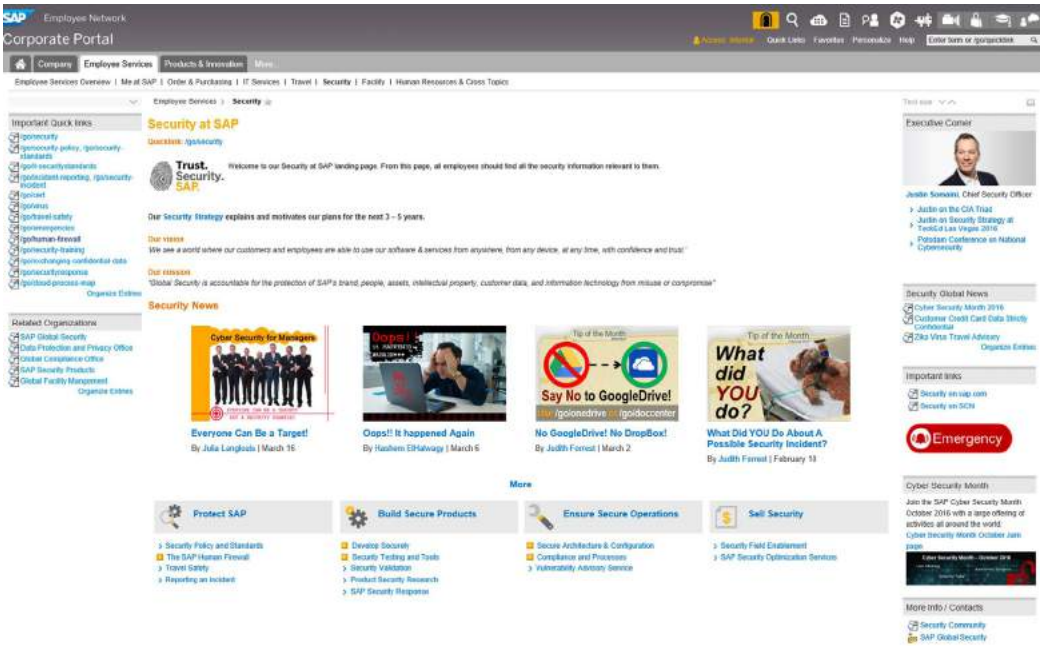


Abbildung 10-4: Intranet-Portal der Konzernsicherheit bei SAP; Quelle: SAP SE

Wechselnde Poster, Spiegeldisplays und Broschüren steigern zudem die Sichtbarkeit der Kampagne und liefern weitere Informationen zur Informationssicherheit. In einem Spiegeldisplay sieht ein Mitarbeiter von SAP den „Most important Security Officer at SAP" – nämlich sich selbst. Dazu ist jede Toilette mit einem solchen Spiegel ausgestattet. Das soll für 100 % Aufmerksamkeit sorgen – und das jeden Tag. Andere Maßnahmen machen die Mitarbeiter auf die Gefahren von Social Media aufmerksam – die Nutzung von Twitter kann Mitarbeiter als Ziel für Angriffe exponieren. Der internationale „Cyber Security Month" im Oktober 2016 wurde bei SAP mit vielen Aktionen, wie z. B. Konferenzen, Vorträgen oder Live-Hackings, „gelebt". Diese Aktionen wurden nicht nur am Hauptstandort von SAP durchgeführt, sondern global. Exemplarisch sind Informationssicherheitsevents in Palo Alto und Shanghai mit verschiedenen Themen der Informations- und IT-Sicherheit. Zudem wurden diese Events per Video aufgezeichnet und über das Webportal im Intranet für alle Mitarbeiter publiziert. Weitere Aktionen wenden sich gezielt an Manager: Das Online-Training „Everyone can be a target" will Manager für das Thema Informationssicherheit auf Reisen sensibilisieren. Für Softwareentwickler und Techniker bei SAP gibt es spezielle Angebote wie Hackathons oder Capture-the-Flag-Events.

Das Ziel der Informationssicherheitskampagne ist es, alle Mitarbeiter der SAP für das Thema Informationssicherheit zu sensibilisieren. Alle Mitarbeiter der SAP sind in der Fotoaktion der Human Firewall vereint und lassen symbolisch keinen Angreifer „an der Firewall" vorbei ins Unternehmen gelangen. Das Key Visual erhöht Sichtbarkeit, Akzeptanz der Informationssicherheit und demonstriert den Mitarbeitern ebenso wie den Kunden das Commitment der SAP-Mitarbeiter zum Unternehmen und seiner Sicherheit.

Die zusätzlichen Maßnahmen neben der Human Firewall als Key Visual wie eine Umfrage zu IT-Security-Awareness, Schulungen zur Informationssicherheit sowie die Analyse der Awareness und die Teilnehmerquoten an Schulung und Awareness-Umfrage sind ein Teil des IT-Sicherheitsmanagements, wie es z. B. vom IT-Sicherheitsgesetz gefordert wird.

10.3.1 Geschäftssicht

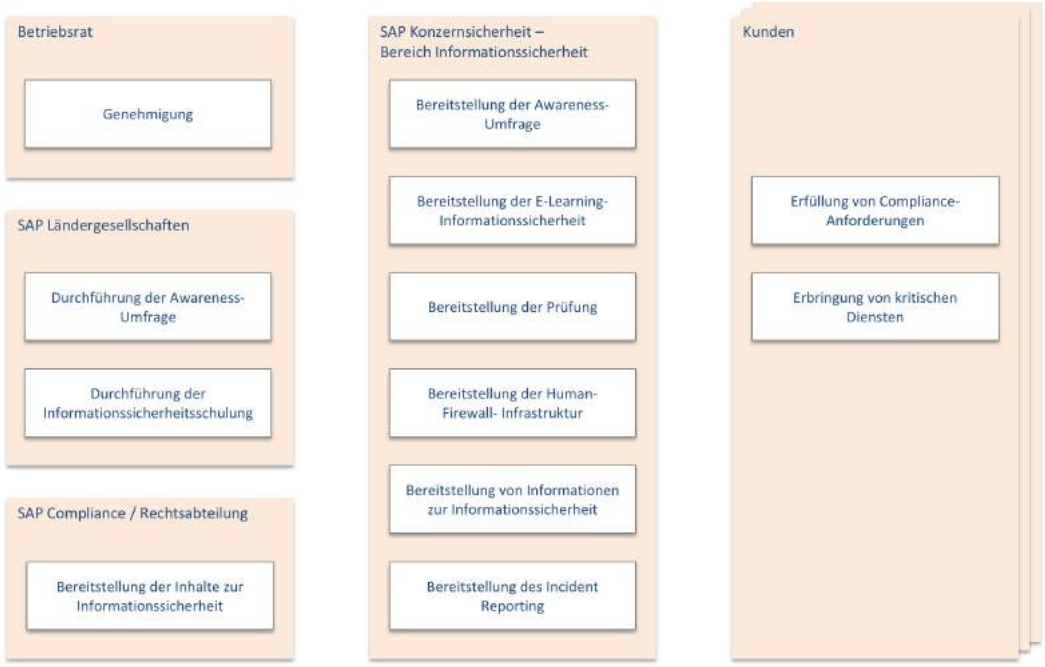


Abbildung 10-5: Geschäftssicht SAP Informationssicherheit

Die Fotokampagne Human Firewall ist eine von vielen Maßnahmen zur Steigerung der Informationssicherheit von der gleichnamigen Abteilung, Informationssicherheit, als Teil der Konzernsicherheit der IT. Die Abteilung Informationssicherheit verantwortet das Portal im Intranet, die Inhalte zur Informationssicherheit, wie die 100-Sekunden-Videos, den aktuellen Tipp zur Informationssicherheit sowie die Inhalte zum Incident-Management und verschiedene Aktionen, wie die Fotobox.

Der Betriebsrat muss die verpflichtende Informationssicherheitsschulung und die Wissensüberprüfung genehmigen, nicht aber den freiwilligen Awareness-Check, die freiwillige Teilnahme mit Foto und Statement an der Human Firewall. Die Compliance-Abteilung erhält die Informationen zur Durchführung der Informationssicherheitsschulung mit Antworten und den Teilnahmequoten der verschiedenen Funktionen und Ländergesellschaften / Regionen.

Die Regionalgesellschaften und die verschiedenen (funktionalen) Abteilungen führen die Informationssicherheitskampagne durch.

Die Rechtsabteilung trägt Informationen sowie eine Datenschutzerklärung bei, die die Mitarbeiter ausfüllen, sodass SAP die Bilder im Intranet verwenden kann. Informationen über die Kampagne mit den Bildern werden in der Kommunikation zu den Kunden verwendet, um das Commitment der SAP-Mitarbeiter zu SAP und der Informationssicherheit zu signalisieren.

In die Gestaltung der Inhalte und die Schwerpunktsetzung der Inhalte auf dem Webportal der Informationssicherheit werden Informationen der anderen Abteilungen und insbesondere des Incident-Managements bei der SAP miteinbezogen.

10.3.2 Prozesssicht

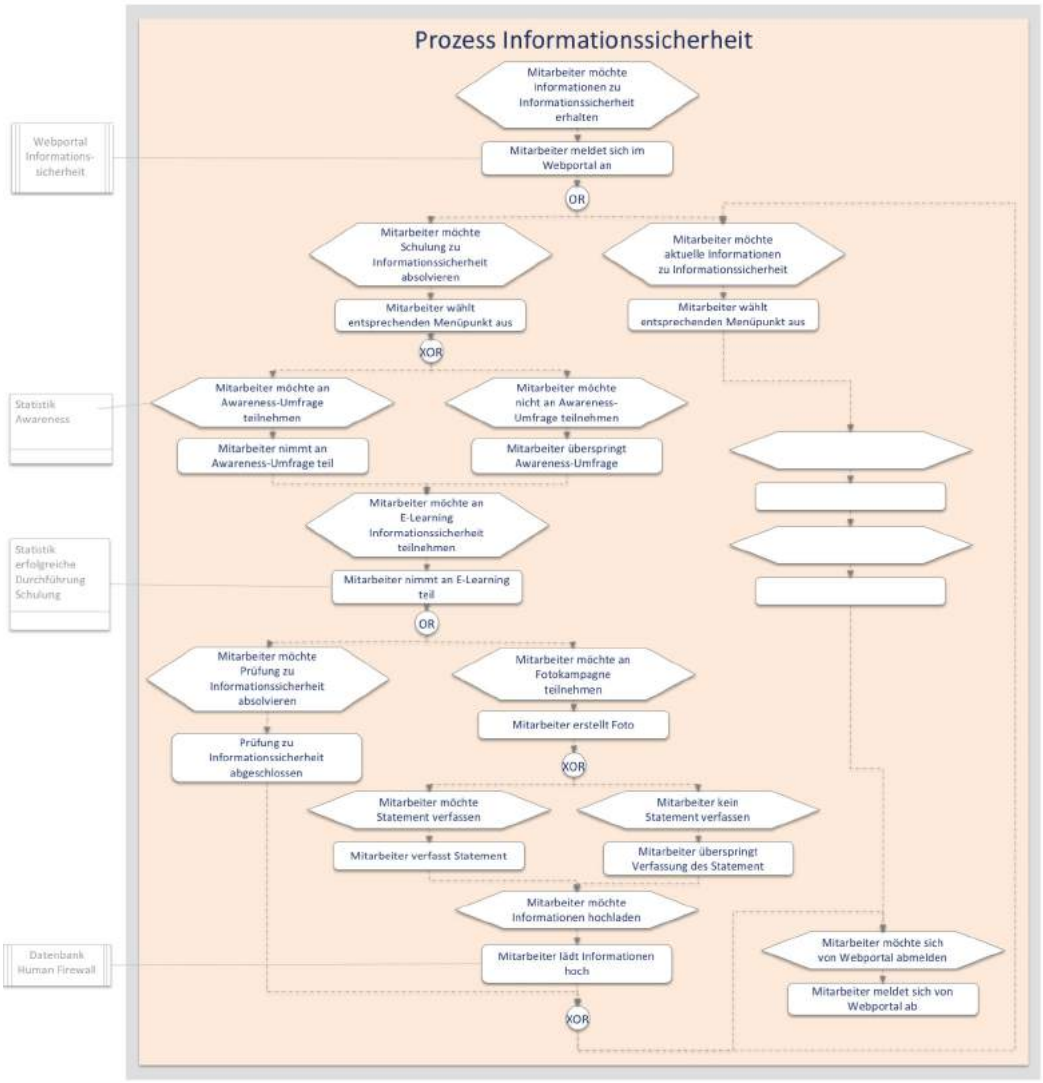


Abbildung 10-6: Prozess in der Informationssicherheit mit verpflichtender Informationssicherheitsschulung und der freiwilligen Teilnahme an der Human Firewall

Der Standardprozess, wie ein Mitarbeiter Teil der Human Firewall wird, ist in Abbildung 10-6 dargestellt. Mitarbeiter loggen sich in der Anwendung über das Webportal der Informationssicherheit ein. Sie absolvieren (freiwillig) den Awareness-Check; dies ist eine Umfrage zur Informationssicherheit mit fünf Fragen. Sie nehmen dann an einer Schulung zur Informationssicherheit – realisiert als E-Learning – teil und absolvieren einen Multiple-Choice Test. Wenn Mitarbeiter diesen Test bestehen, können sie (optional) ein Foto für die Human Firewall von sich machen, dieses Foto über das Webportal hochladen und ein individuelles Statement zur Informationssicherheit abgeben.

Die Anwendung setzt dynamisch immer wieder neue Human Firewalls aus den Fotos der Mitarbeiter zusammen – für die Darstellung im Webportal der Informationssicherheit und in anderen Anwendungskontexten.

Aus den Teilnahmen an der Umfrage und der Schulung werden Statistiken über die Awareness, Informationssicherheit und die erfolgreiche Teilnahme an den Informationssicherheitsschulungen generiert – z. B. nach Funktionsbereichen der SAP und nach Ländern bzw. Regionen.

10.3.3 Anwendungssicht

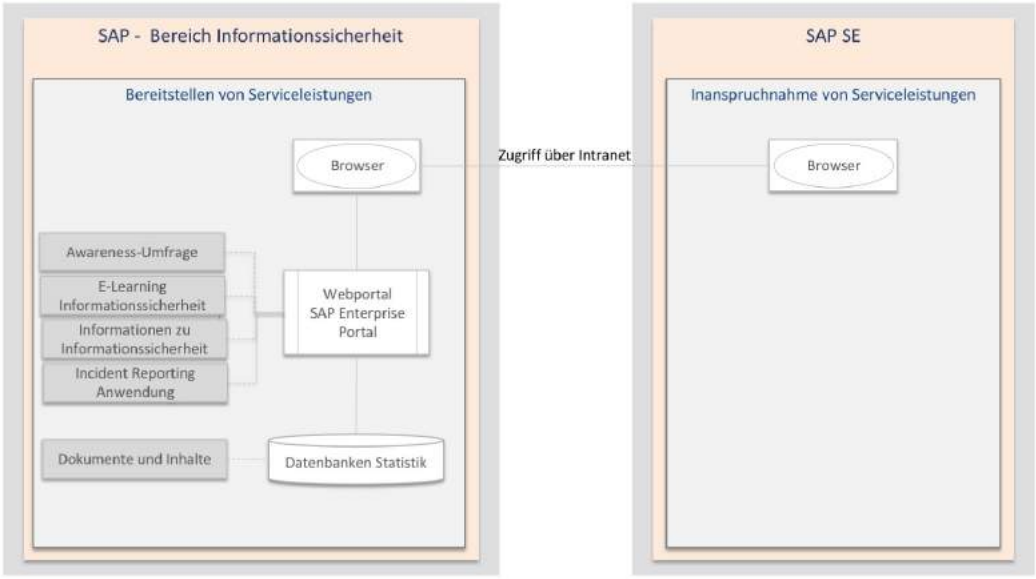


Abbildung 10-7: Anwendungssicht Informationssicherheit bei der SAP

Mitarbeiter können der Human Firewall über das Webportal beitreten und an den Umfragen und dem E-Learning zur Informationssicherheit teilnehmen. Sie können darüber hinaus über das Webportal auf Informationsangebote wie den Tipp des Monats, Multi-Media-Anwendungen, wie die 100-Sekunden-Videos, oder auch auf das Incident Reporting Tool zugreifen.

Eine Datenbank registriert die Teilnehmer, archiviert die hochgeladenen Fotos für die Human Firewall, lässt einen Zähler zur Anzahl der Mitglieder der Human Firewall „mitlaufen“

und wertet die Teilnahme an den Informationssicherheitsschulungen (E-Learning-Modulen) in Heatmaps über Teilnehmer nach Funktionsbereichen und Ländergesellschaften aus.

In die Datenbank wird ein „Bestanden" bei einem erfolgreichen Test im Anschluss an das E-Learning-Modul eingetragen. Es findet kein Tracking von Besuchern auf dem Webportal der Informationssicherheit statt.

Mitarbeiter werden per E-Mail aufgefordert, sich an der Informationssicherheitsschulung zu beteiligen, und es wird mit einem automatischen Reminder per E-Mail an die Teilnahme an der Informationssicherheitsschulung erinnert.

10.3.4 Technische Sicht

Das Webportal der Informationssicherheit mit all den Inhalten und den E-Learning-Modulen sowie die Human Firewall sind nur über das Intranet der SAP zugänglich. Externe Mitarbeiter werden ebenfalls zu Themen der Sicherheit geschult – hier gibt es auch von außen zugängliche Informationen und Schulungen, die Voraussetzung dafür sind, dass diese Mitarbeiter einen Zugang zur IT-Infrastruktur der SAP erhalten.

10.3.5 Umfang und Zeitraum

Die Aktion der Human Firewall wurde 2015 begonnen. Seit 2012 gibt es eine Kampagne zur Informationssicherheit mit verpflichtenden Schulungen als E-Learning-Modul. Die Human Firewall wird als Maßnahme zur Steigerung des Informationssicherheitsbewusstseins auf Konferenzen, wie z. B. dem International Security Forum (ISF), beworben. Die dabei entstehenden Fotografien haben den Vorteil, dass sie sowohl die Innen- als auch die Außenwirkung der Kampagne zusätzlich steigern.

In der Abteilung Informationssicherheit sind zum Zeitpunkt der Datenerhebung für diese Fallstudie 1,5 Mitarbeiterstellen angesiedelt, die neben der Kampagne Human Firewall auch andere Informationssicherheitsmaßnahmen entwickeln und durchführen.

10.3.6 Vorgehen und Umsetzung

Die Abteilung Informationssicherheit agiert entsprechend der Strategie „Sicherheitsbewusstsein muss mit regelmäßigem Training und ständiger Kommunikation aufgebaut und gestützt werden" [3]. Die Fotokampagne der Human Firewall wurde im Jahr 2015 mit dem Key Visual der Menschenkette der SAP-Mitarbeiter mit verschränkten Armen entwickelt und eingeführt. Dieses Key Visual fördert das Bewusstsein für Informationssicherheit und die Sichtbarkeit der Informationssicherheitskampagne. Mitarbeiter werden in die Informationssicherheit aktiv einbezogen und sollen sich so mit dem Thema identifizieren und mindestens ein Bewusstsein für die Informationssicherheit entwickeln.

Die Kampagne wird immer wieder durch neue Aktionen aufgefrischt: Einmalig wurde eine Fotobox für die Bilder der Mitarbeiter am Standort Walldorf aufgestellt, Security-Clowns greifen Themen der Informationssicherheit auf und präsentieren sie eindrücklich und unterhaltsam.

Es ist wichtig, dass die Human Firewall ebenso wie andere Kampagnen der Informationssicherheit Mitarbeiter aktiviert. Mitarbeiter werden dazu eingeladen, sich selbst zu beteiligen,

gemeinsam für Bilder zu posieren und Poster oder Spiegel sind für jeden Mitarbeiter sichtbar. Das Statement lädt Mitarbeiter ein, sich selbst mit dem Thema Informationssicherheit auseinanderzusetzen.

Die Informationssicherheitsschulung ist verpflichtend und Informationen zum Bewusstsein für Informationssicherheit bei der SAP werden laufend erhoben. Es sind Informationen verfügbar, wie viele Mitarbeiter die Schulung zur Informationssicherheit durchgeführt haben und wie sie Fragen zur Informationssicherheit des Unternehmens SAP ebenso wie zu ihrem eigenen Sicherheitsverhalten und dem Verhalten ihrer Vorgesetzten beantwortet haben.

10.3.7 Projektergebnis

SAP hat mit der Human Firewall als Key Visual eine Marke für Informationssicherheit im Unternehmen entwickeln können. Die Human Firewall ist für die Informationssicherheit im Unternehmen genauso wichtig wie die technische Firewall – dieses Bewusstsein für den menschlichen Faktor will die Informationssicherheit schaffen. Neben der Human Firewall gibt es eine Reihe von anderen Aktivitäten, die das Thema Informationssicherheit ins Bewusstsein der Mitarbeiter rücken.

Dem E-Learning-Modul ist eine Befragung zum Thema Informationssicherheit vorgeschaltet, die über die Jahre hinweg einen Hinweis auf die Entwicklung des Bewusstseins für Informationssicherheit bei Mitarbeitern und auch im Management erlaubt: Das Bewusstsein für Informationssicherheit im Unternehmen ist gestiegen. Über die Laufzeit der Kampagne und der Informationssicherheitsschulung hat das Thema Informationssicherheit für die Mitarbeiter bei SAP an Bedeutung gewonnen. Der Anteil der Mitarbeiter, die SAP als eine sichere Unternehmung ansehen und die der Meinung sind, dass SAP für die Sicherheit genug tut, ist gestiegen. Der Anteil der Mitarbeiter, die denken, dass SAP zwar Sicherheit ernst nimmt, aber mehr tun müsste, ist hingegen gesunken. Außerdem ist das Interesse an Themen der Informationssicherheit in der SAP gestiegen. Mitarbeiter berichten, dass ihre Vorgesetzten das Thema Informationssicherheit adressieren und immer mehr Mitarbeiter schätzen den Informationssicherheitslevel auf Managementebene als hoch ein – jedoch mit Unterschieden zwischen Geschäftsbereichen und Regionen. Diese Informationen basieren auf dem Awareness-Check der optionalen Umfrage zur Informationssicherheit, die der Schulung und dem Bild für das Key Visual vorgeschaltet ist.

Die Mitarbeiter sind bereit, sich für das Thema der Informationssicherheit zu engagieren und so hat der Awareness-Check als freiwilliger Fragebogen zu Informationssicherheit eine Teilnahmequote von 50 %. Mehr als 95 % der Mitarbeiter haben an den Schulungen zu Informationssicherheit teilgenommen.

Mindestens ein anderes DAX-Unternehmen hat zum Zeitpunkt der Erstellung dieser Fallstudie die Idee der Human Firewall von SAP aufgegriffen und Vergleichbares gestartet.

SAP will mit der Fotokampagne der längsten Firewall der Welt ins Guinness-Buch der Rekorde. Im März 2017 sind ca. 9.500 Mitarbeiter mit ihren Bildern Teil der Human Firewall von SAP. Mit ca. 10.000 Mitarbeitern soll die Human Firewall ins Guinness-Buch der Rekorde aufgenommen werden.

10.4 Erfolgsfaktoren

Die Human Firewall von SAP mit dem Key Visual der Mitarbeiterkette ist nach innen und über die Unternehmensgrenzen hinweg ein starkes und sichtbares Symbol für Informationssicherheit von SAP und dem Commitment der Mitarbeiter.

Informationssicherheit wird in dieser Kampagne als unterhaltsames und interaktives Thema präsentiert: Die Mitarbeiter lachen auf den Bildern, Security-Clowns vermitteln auf unterhaltsame Weise Themen der Informationssicherheit und die Mitarbeiter werden durch die Teilnahme an der Human Firewall mit Bild und Statement aktiviert und entscheiden sich, Teil dieses Themas bei der SAP zu sein.

Wichtig für den Erfolg der Human-Firewall-Aktion ist die Einbindung des Topmanagements: Das Topmanagement ist als Poster ebenso wie in der Human Firewall im Webportal präsent. Informationssicherheit wird darüber hinaus in einem hierarchischen Ansatz ausgerollt und so wird z. B. auch – als Teil der Umfrage zu Awareness – erhoben, ob Vorgesetzte Themen der Informationssicherheit gegenüber Mitarbeitern aktiv ansprechen.

Die Fotokampagne der Human Firewall ist zum Zeitpunkt der Erstellung der Fallstudie bereits mehrere Jahre aktiv – wichtig für den Erfolg der Kampagne waren das Key Visual und ein langer Atem mit einer Finanzierung von ca. 1,5 Vollzeitäquivalenten Mitarbeiterstellen über mehrere Jahre. Wesentlich für den Erfolg der Kampagne Human Firewall ist die Vielzahl der damit verknüpften und auch wechselnden Aktionen – die Poster, die Spiegelbilder, die Clowns ebenso wie die Fotoboxen und vor allem die E-Learning-Schulungen, durch die alle Mitarbeiter auf die Human Firewall gestoßen werden. Denn „Sicherheitsbewußtsein muß mit regelmäßigem Training und ständiger Kommunikation aufgebaut und gestützt werden." [1]

Die Präsenz des Themas der Informationssicherheit hat bei der SAP zugenommen – das zeigen die Ergebnisse des Awareness-Checks. Inwieweit das auf die Kampagne der Human Firewall zurückzuführen ist, muss naturgemäß ein Stück unklar bleiben, denn schließlich war das Thema Informationssicherheit während der Human-Firewall-Kampagne auch auf anderen Ebenen sowie in der Öffentlichkeit präsent.

10.5 Danksagung

Wir danken dem Bundesministerium für Bildung und Forschung (BMBF) für die Möglichkeit der Forschung im Rahmen des Projektes VeSiKi, Förderkennzeichen 16KIS0213K.

10.6 Literaturverzeichnis

[1] Langlois, J.; Schimmer, K., 2015. Sicherheit beginnt im Kopf – Die Human Firewall.

[2] SAP, 2015. Strategie und Geschäftsmodell, SAP Integrierter Bericht 2015. Verfügbar unter: https://www.sap.com/integrated-reports/2015/de/strategy/strategy-and-business-model.html [zugegriffen: 13-Apr-2017].

[3] Saueressig, T., 2017. Digitale Transformation am Beispiel der SAP. Vortrag auf der Konferenz Wirtschaftsinformatik 2017. St. Gallen.

11 Zentrale Leitstelle Ostthüringen: IT-Sicherheit in einer Leitstelle

Tamara Gurschler, Universität der Bundeswehr München
Andreas Rieb, Universität der Bundeswehr München
Manfred Hofmeier, Universität der Bundeswehr München

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 bei 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.

Keywords: Sektor Staat und Verwaltung, Branche Notfall-/Rettungswesen, Zentrale Leitstelle, Informationssicherheit, Ausfallsicherheit

11.1 Unternehmen

11.1.1 Unternehmensprofil

Die Stadt Gera betreibt im Auftrag des Rettungsdienstzweckverbands Ostthüringen die Zentrale Leitstelle Ostthüringen für Rettungsdienst, Feuerwehr und Katastrophenschutz in Form einer integrierten Regionalleitstelle. Das Versorgungsgebiet sind die Gebietskörperschaften der kreisfreien Stadt Gera sowie seit mehr als 20 Jahren die Landkreise Altenburger Land und Greiz. Es leben 298.000 Menschen in 550 Ortschaften und 16 Städten im Zuständigkeitsbereich der Leitstelle Ostthüringen. Die Leitstelle in Gera ist nach den Leitstellen Erfurt und Jena die drittgrößte Leitstelle der dreizehn Leitstellen im Bundesland Thüringen.

Die Zentrale Leitstelle ist 365 Tage im Jahr und 24 Stunden pro Tag besetzt und beschäftigt insgesamt 22 Disponenten sowie drei Mitarbeiter für Führung und Verwaltung. Die Mitarbeiter disponieren jährlich über 90.000 Einsätze. Die Leitstelle vermittelt Einsätze von Rettungsdienst, Krankentransport, kassenärztlichem Notfalldienst und der Feuerwehr (vgl. Abbildung 11-1). Ein Notruf unter der Notrufnummer 112 muss in der Leitstelle innerhalb von 10 Sekunden angenommen sein und innerhalb von 60 Sekunden muss eine Alarmierung der Rettungskräfte erfolgen.

Die konzeptionelle Arbeit in der Leitstelle und die Weiterentwicklung der IT-Systeme finden statt im Spannungsfeld zwischen dem Wunsch, alle Anrufe bestmöglich zu vermitteln, den gesetzlichen Grundlagen, die die Antwortzeiten und Aufgaben der Leitstelle vorgeben, neuen technischen Entwicklungen und der Haushaltslage der Kommunen sowie einer aktuellen Diskussion über strategische Zusammenlegung von Leitstellen im Bundesland.

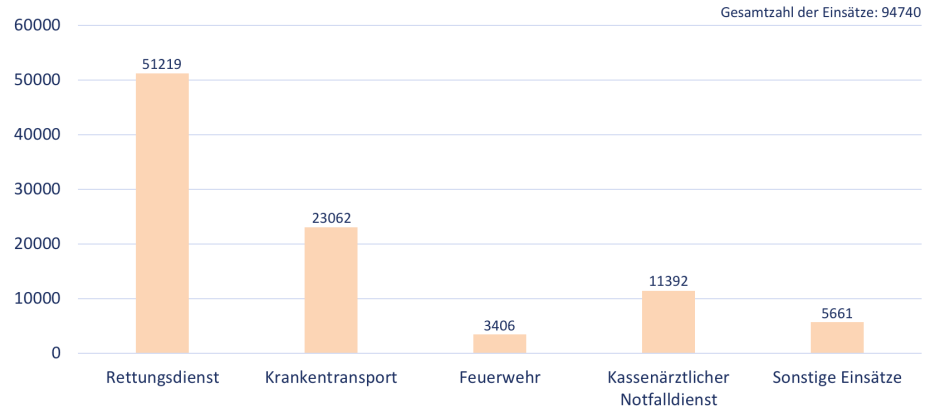


Abbildung 11-1: Vermittelte Einsätze der Zentralen Leitstelle Ostthüringen 2016

11.1.2 Strategische Ausrichtung

Regionalisierung von Leitstellen ist in Deutschland ein Thema und auch Thüringen möchte in einer Leitstellenstrukturreform Skaleneffekte im Bereich der Notfallversorgung erreichen, die letztlich auch im Kontext einer Gebietsreform des Freistaates steht. Dies könnte in Thüringen so auf lange Sicht zu vier bis sieben Leitstellen führen. Synergien zwischen Leitstellen sowie geübtere Disponenten sind Argumente für diese Regionalisierung, während die nötigen Regionalkenntnisse der Disponenten ein Argument für einen lokalen Betrieb der Leitstellen ist.

Die Erweiterung der Zentralen Leitstelle Ostthüringen um einen bis zwei Landkreise (auf etwa 400.000 Menschen) verspricht Synergieeffekte und könnte ohne wesentliche Investitionen verwirklicht werden. Vorbilder sind Leitstellen, die bis zu einer Million Menschen versorgen. Die personellen, technischen und räumlichen Entfaltungsmöglichkeiten am Standort Gera werden geprüft. Geprüft wird auch die Ausstattung der Leitstelle mit weiteren Stellen, vor dem Hintergrund von neuen Aufgaben, wie Risikomanagement, werden dabei ebenso die Anzahl der administrativen Mitarbeiter und die Führungsfunktionen betrachtet. Bisher sind dafür in der Leitstelle drei vollzeitäquivalente Dienstposten vorgesehen.

Auf technischer Seite gehören zu den strategischen Überlegungen unter anderem eine Homogenisierung der Software nach dem Vorbild des Bundeslands Sachsen: Einheitliche Software erlaubt eine problemlose Zusammenarbeit und die Möglichkeit, ohne Medienbrüche ad hoc Rückfallebenen in den Live-Betrieb zu überführen. Darüber hinaus wird die Einführung von Digitalfunk ein strategischer Bereich der Weiterentwicklung des Rettungswesens in Thüringen sein.

11.1.3 Fallstudienpartner

Name	Position im Unternehmen
Cornell Zergiebel	Fachgebietsleiter Zentrale Leitstelle Ostthüringen
Matthias Schönbach	Sachbearbeiter Einsatzvorbereitung – Stellvertreter Fachgebietsleiter Zentrale Leitstelle Ostthüringen

Steven Müller	Fachgebietsleiter Information und Kommunikation – Stadtverwaltung Gera
Sebastian Dännart	Wissenschaftlicher Mitarbeiter, Universität der Bundeswehr München
Tamara Gurschler	Wissenschaftliche Mitarbeiterin, Universität der Bundeswehr München
Andreas Rieb	Wissenschaftlicher Mitarbeiter, Universität der Bundeswehr München
Manfred Hofmeier	Wissenschaftlicher Mitarbeiter, Universität der Bundeswehr München

11.2 Kritische Infrastruktur

11.2.1 Einordnung als KRITIS

Die kritischste Dienstleistung einer Zentralen Leitstelle besteht in der Bereitstellung des Notrufgeschehens. Ein Notruf über die Notrufnummer 112 kommt in der Zentralen Leitstelle Ostthüringen an und muss jederzeit angenommen und weitervermittelt werden können. Gemäß Artikel 1 Absatz 2 des IT-Sicherheitsgesetzes sind „Einrichtungen, Anlagen oder Teile davon, die den Sektoren [...] Gesundheit [...] angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden", Kritische Infrastrukturen (KRITIS). Laut dieser Definition sind alle (integrierten) Leitstellen, die von Behörden und Organisationen mit Sicherheitsaufgaben betrieben werden, Kritische Infrastrukturen. Die Leitstellen können sowohl dem KRITIS-Sektor Gesundheit und der Branche medizinische Versorgung als auch dem Sektor Staat und Verwaltung in der Branche Notfall- und Rettungswesen einschließlich Katastrophenschutz zugeordnet werden. Es bestehen Abhängigkeiten und Schnittstellen zu den Sektoren Informationstechnik und Telekommunikation sowie Energie. Der Sektor Staat und Verwaltung ist allerdings nicht dem IT-Sicherheitsgesetz unterworfen.

Die Leitstelle sieht sich selbst – ungeachtet der Rechtslage – als Kritische Infrastruktur.

11.2.2 Risikoanalyse

Das Projekt MoSaIK[10] aus dem Forschungsschwerpunkt *IT-Sicherheit für Kritische Infrastrukturen* hat im Rahmen der Forschung eine Strukturanalyse sowie eine Risikoanalyse durchgeführt, die auf dem fundierten Wissen der Mitarbeiter der Leitstelle über vorhandene Systemkomponenten, Architekturen und Prozesse der Leitstelle basieren. Die Risikoanalyse definiert die Notrufannahme als den Baustein mit dem höchsten Schutzbedarf. Hier sind nur extrem kurze Ausfallzeiten tolerierbar. Dem nachgeordnet werden Prozesse der Notfallbehandlung gesehen. Eine sehr geringe Priorität haben selbstverständlich administrative Prozesse wie Abrechnung und Auswertung.

In einer Zentralen Leitstelle gibt es Schnittstellen und signifikante Abhängigkeiten von anderen Sektoren von Kritischen Infrastrukturen. Beispielsweise hängt die Aufrechterhaltung des Notrufgeschehens von der Ausfallsicherheit des Telekommunikationsanbieters und des

10 https://www.itskritis.de/mosaik.html.

Energieversorgers ab. Zudem hängt das Funktionieren einer integrierten Leitstelle von der Verfügbarkeit von Informationssystemen ab.

Für Wartung und Fernwartung der Informationssysteme werden VPN-Verbindungen zu den Herstellern der Systeme unterhalten. Solche Fernwartungszugänge sind in den Wartungsverträgen festgelegt, um die regelmäßige Wartung der Systeme zu gewährleisten. Es gibt eine Wartungsschnittstelle für das Kommunikationssystem, eine Wartungsschnittstelle für das Einsatzleitsystem und eine Schnittstelle zum Rettungsdienstzweckverband, um Abrechnungen durchzuführen. All diese Wartungsschnittstellen sind potenzielle Risiken.

Es gibt mehrere Rückfallebenen für das IT-System bzw. den allgemeinen Betrieb der Leitstelle. Die letzte Instanz dieser Rückfallebenen – bei einem Komplettausfall der Zentralen Leitstelle Ostthüringen – sind die Gebietskörperschaften mit Unterleitstellen, die die Alarmierung von Notrufkräften in diesem Fall übernehmen. Die Unterleitstellen haben keine Schnittstelle zur Zentralen Leitstelle Ostthüringen.

11.3 IT-Sicherheit

Die IT-Sicherheit ist ein priorisiertes Thema in der Zentralen Leistelle Ostthüringen. Ein eigener Mitarbeiter ist mit der Planung, Anschaffung, Inbetriebnahme, Wartung, Instandhaltung und anderen Aufgaben rund um die Informationstechnik beauftragt. Zudem arbeitet die IT-Abteilung der Stadtverwaltung Gera eng mit der Leitstelle zusammen.

11.3.1 IT-Infrastruktur

Die IT-Infrastruktur der Zentralen Leitstelle Ostthüringen ist historisch gewachsen und stellt eine von der IT der Stadtverwaltung losgelöste Insellösung dar. Die IT-Infrastruktur der Leitstelle ist in sich geschlossen und hat nur wenige Schnittstellen nach außen, da die meisten Kernfunktionalitäten der Leitstelle nur das geschlossene Netzwerk erfordern.

Der Internetzugang für die Mitarbeiter wird über ein Remote Controlled Browser System (ReCoBS) verwirklicht, sodass Infektionen über den Browser kein Risiko für die Arbeitsplatz-PCs darstellen. Zusätzlich wird der Zugriff auf Ressourcen im Internet protokolliert.

Daneben gibt es Wartungsschnittstellen zu externen Dienstleistern – etwa für das Kommunikationssystem und das Einsatzleitsystem, die entsprechend den Wartungsverträgen erforderlich sind. Diese Schnittstellen sind via VPN-Verbindungen realisiert. Eine gleichartige Schnittstelle zum Rettungsdienstzweckverband ist ebenfalls vorhanden.

Das Netzwerk der Leitstelle gliedert sich in zwei Subnetze: das Kommunikationsnetz, in dem sich die Komponenten mit Telekommunikationsbezug befinden, und das Datennetz, in dem sich die Disponenten-Arbeitsplatz-PCs, die Systeme zur Einsatzunterstützung sowie Alarmdrucker und Brandmeldeanlage befinden. Beide Subnetze sind über ein Gateway miteinander verbunden.

Den zentralen Baustein im Kommunikationsnetz bilden die HiPath-TK-Anlage und das Vermittlungs- und Abfragesystem (VAS), bestehend aus einem VAS-B-Server und den VAS-B-Clients für die Disponenten. Zudem befinden sich im Kommunikationsnetz auch die Ge-

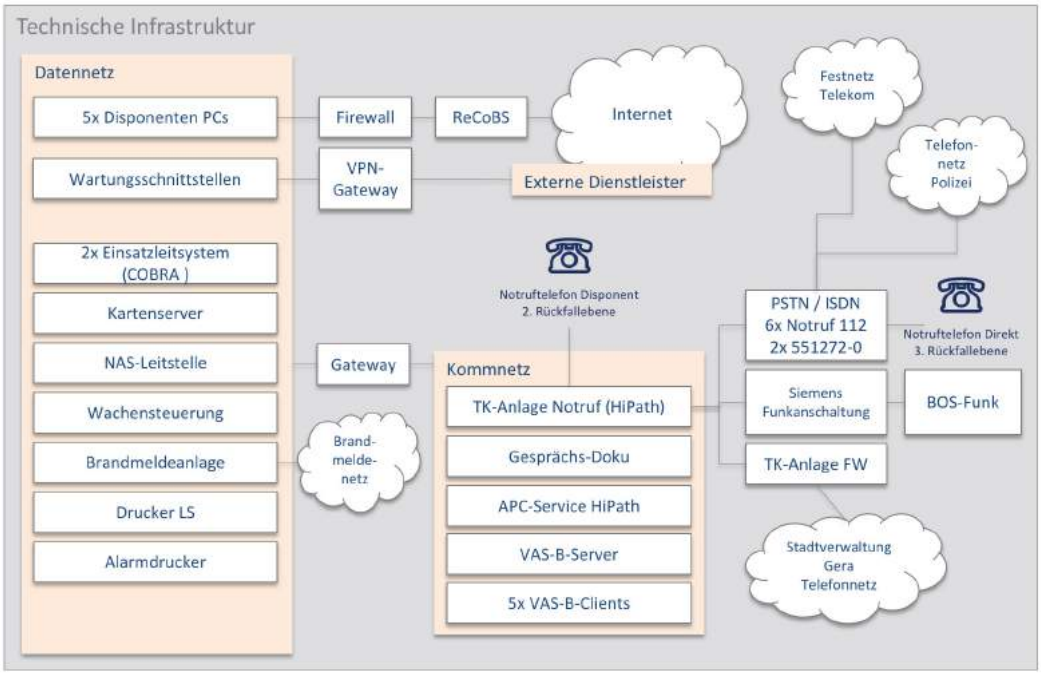


Abbildung 11-2: IT-Infrastruktur der Zentralen Leitstelle Ostthüringen

sprächsdokumentation, die die Kommunikation der Disponenten mit den Hilfeersuchenden aufzeichnet, und ein PC zur Administration der HiPath-TK-Anlage.

Die HiPath-TK-Anlage ist der Knotenpunkt für die Kommunikation. Sie ist am PSTN-/ISDN-Anschluss angeschlossen, an dem auch die Notrufersuche eingehen. Weiter ist auch eine Siemens Funkanschaltung (SiFa) angeschlossen, welche die HiPath-TK-Anlage mit dem Funk für Behörden und Organisationen mit Sicherheitsaufgaben (BOS-Funk) verbindet. Über diesen Funk können unter anderem die Einsatzkräfte kontaktiert werden.

An die HiPath-Anlage sind Disponententelefone direkt angeschlossen, über die Notrufe angenommen werden können, wenn das VAS ausfällt (2. Rückfallebene). Das geschieht automatisch. Sollte die HiPath selbst ausfallen, übernimmt ein Telefon, das direkt am Telefonanschluss angegliedert ist (3. Rückfallebene).

Das Datennetz umfasst neben den Anwendungsservern und Druckern die Disponenten-PCs. Diese sind einmal pro Disponenten-Arbeitsplatz vorhanden und befinden sich zusammen mit der Server-Infrastruktur im Serverraum. Die Eingabe- und Ausgabegeräte der Disponenten sind per Remote-Extender angebunden.

Auf das Internet können die Disponenten nur über ReCoBS zugreifen. Dabei wird der Browser in einem abgeschotteten System ausgeführt, während auf dem Disponenten-PC nur Eingabe und Anzeige erfolgen. Der ReCoBS-Server ist vom Netzwerk durch eine Firewall getrennt und bildet als gehärtetes System die Schnittstelle ins Internet.

11.3.2 Geschäftssicht

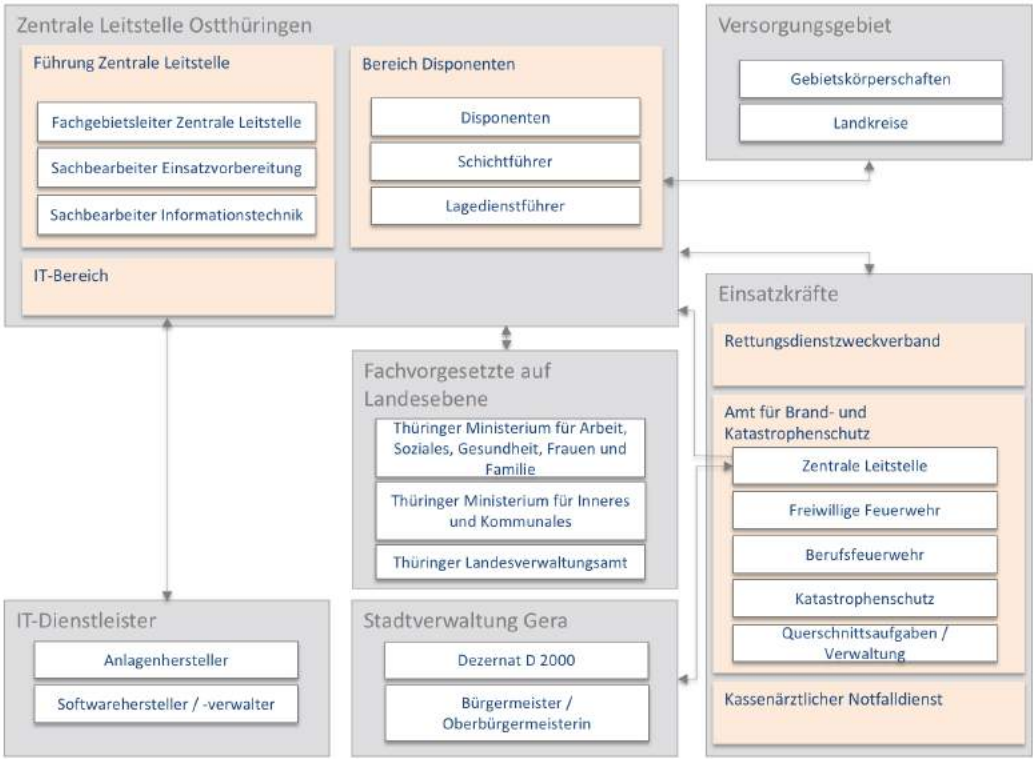


Abbildung 11-3: Geschäftssicht

Die Zentrale Leitstelle Ostthüringen ist eines von mehreren Fachgebieten des Amts für Brand- und Katastrophenschutz. Als integrierte Regionalleitstelle versorgt dieses Fachgebiet ein Gebiet von 298.000 Menschen in 550 Ortschaften und 16 Städten. Eingehende Notrufe der Hilfesuchenden in diesem Versorgungsgebiet werden von den Disponenten entgegengenommen und bearbeitet – 365 Tage im Jahr, 24 Stunden am Tag. Der Regelbetrieb sieht für die Disponenten einen Schichtdienst vor, bei dem vier Disponenten Notrufe entgegennehmen. Entsprechend dem Einsatzaufkommen am Wochenende und in der Nacht kann die Zahl der Disponenten abweichen. Der Schichtführer im Leitstellendienst trägt die Verantwortung für die Lenkung der Einsätze während der Schicht. Ebenso stellt der Schichtführer sicher, dass eingehende Notrufe zu jeder Tageszeit angenommen, die zuständigen Einsatzkräfte alarmiert werden und dass die benötigten Einsatzkräfte mit ihren Einsatzfahrzeugen, -geräten und Rettungsmitteln ausrücken.

Eine weitere Funktion im Bereich der Disponenten ist die des Lagedienstführers. Seine Aufgaben umfassen unter anderem die Gewährleistung der ständigen Arbeitsfähigkeit der Leitstelle, die Koordinierung der Datenpflege in den Einsatzunterlagen der Leitstelle, Planung von Aus- und Weiterbildungen, Sicherung der Arbeitsqualität der Disponenten in der Dienstschicht.

Fachlich ist die Zentrale Leitstelle Ostthüringen dem Land Thüringen unterstellt. Genauer dem Thüringer Ministerium für Inneres und Kommunales, dem Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie sowie dem Thüringer Landesverwaltungsamt. Neben der fachlichen Regelung ist die Zentrale Leitstelle Ostthüringen der Fachgebietsleitung des Amts für Brand- und Katastrophenschutz im Fachgebiet Zentrale Leitstelle unterstellt. Das Fachgebiet Zentrale Leitstelle ist wiederum der Stadtverwaltung Gera mit ihrem Dezernat D 2000 und der Oberbürgermeisterin unterstellt.

Der Rettungsdienstzweckverband ist Träger der Zentralen Leitstelle Ostthüringen und ein kommunaler Zusammenschluss, um die Aufgabe „Rettungsdienst" im definierten Versorgungsgebiet zu bewältigen. Dazu zählen z. B. Krankentransporte, Notarzt- und Rettungseinsätze.

Der kassenärztliche Notfalldienst leistet die flächendeckende ambulante vertragsärztliche Versorgung während der sprechstundenfreien Zeiten, insbesondere in der Nacht sowie an Sonn- und Feiertagen.

Ebenso zählen zu den Einsatzkräften die weiteren Fachgebiete des Amts für Brand- und Katastrophenschutz der Freiwilligen Feuerwehr, der Berufsfeuerwehr, des Katastrophenschutzes und der Querschnittsaufgaben / Verwaltung [15].

Insgesamt gibt es im Leitstellengebiet zehn Rettungswachen, die mit Rettungswagen, Notarzt-Einsatzfahrzeugen und auch Krankentransportwagen ausgestattet sind. Zudem gibt es im Versorgungsgebiet mehrere 100 Gerätehäuser und Standorte von Berufs- und Freiwilligen Feuerwehren, die von der Zentralen Leitstelle betreut werden. In Summe umfassen diese Standorte ca. 200 Feuerwachen und ca. 400 Einsatzfahrzeuge sowie das entsprechend ausgebildete Personal.

Eine weitere Gruppe, die in der Abbildung dargestellt ist, umfasst Anlagenhersteller sowie Softwarehersteller und -verwalter. Im Zuge der Wartung greifen diese auf die IT-Infrastruktur der Zentralen Leitstelle zu, um Fehler zu beheben, Updates einzuspielen oder die Systeme zu optimieren. Ebenso erfolgt der Zugriff in die andere Richtung, etwa wenn der Disponent im Rahmen der Notrufbearbeitung Informationen über verschiedene Datenbanken abrufen muss. Beide Anwendungsfälle werden in den nachfolgenden Sichten näher erläutert.

11.3.3 Prozesssicht

In nur 10 Sekunden muss ein Notruf spätestens entgegengenommen werden und in maximal 60 Sekunden wird aus dem Notfall ein Einsatzbefehl. Diese Anforderungen stellen sowohl für den Disponenten als auch für die IT-Infrastruktur besondere Herausforderungen dar, die es einerseits mit geschulten Mitarbeitern und andererseits mit einem ausgeklügelten Konzept an Rückfallebenen und Redundanzen zu bewältigen gilt.

Neben der telefonischen Notrufalarmierung können Hilfesuchende – speziell Hörgeschädigte – auch auf anderem Wege mit dem Disponenten in Kontakt treten. Wie auch andere Leitstellen ist die Zentrale Leitstelle Ostthüringen auch via Alarmfax und Schreibtelefone erreichbar. Da diese Art der Alarmierung für die Zentrale Leitstelle Ostthüringen nur selten der Fall ist, stellt Abbildung 11-4 den Prozess eines eingehenden Notrufs per Telefon bis zur Alarmierung der Einsatzkräfte schematisch dar.

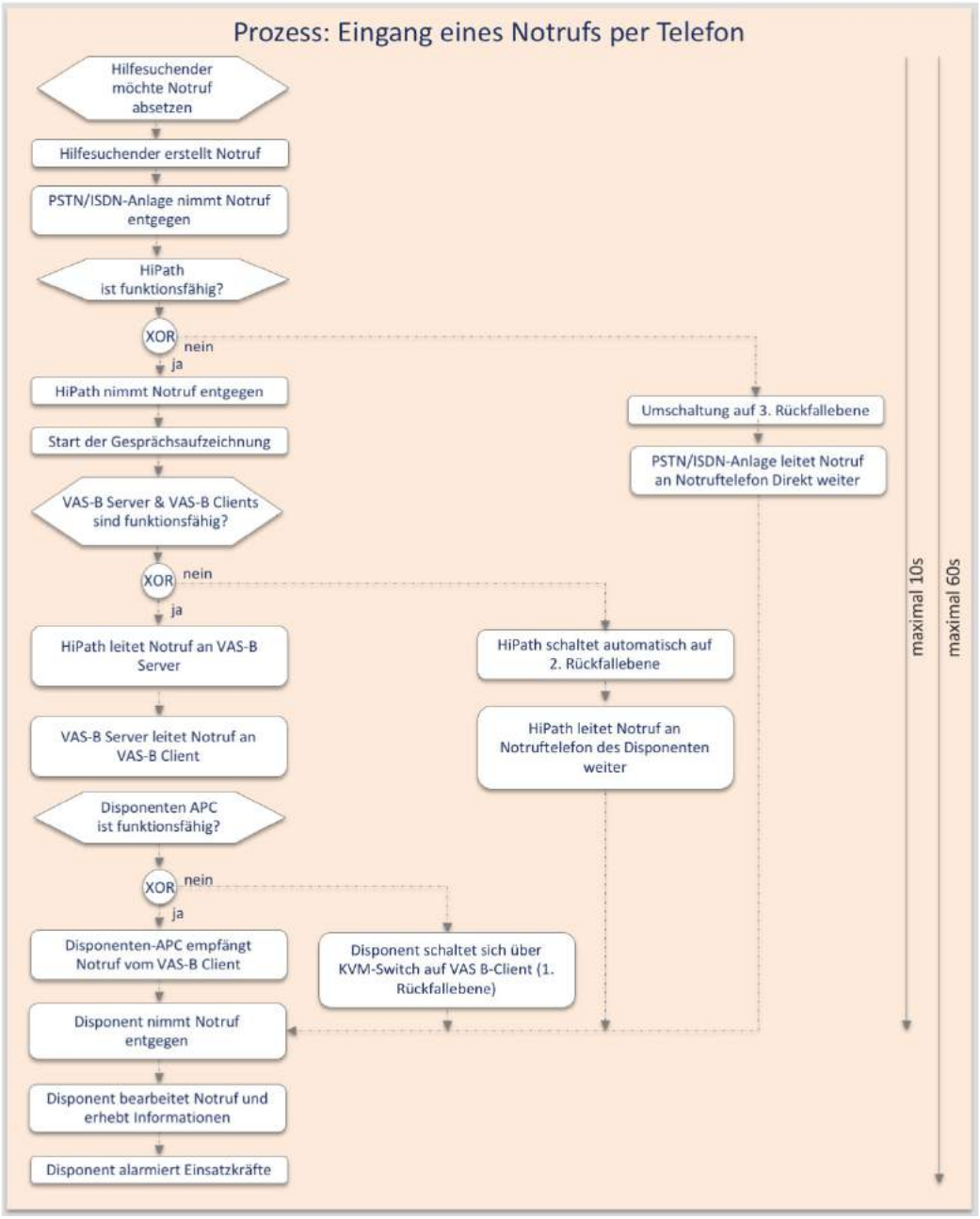


Abbildung 11-4: Prozess zum Eingang eines Notrufs per Telefon

Im Regelbetrieb stehen dem Disponenten alle Funktionen, Dienste und Geräte zur Verfügung, um dem Hilfesuchenden die bestmögliche Hilfe zu bieten. Ein eingehender Notruf per Telefon wird zu Beginn von der PSTN- / ISDN-Anlage entgegengenommen und an das Kommunikationssystem HiPath weitergeleitet. Unmittelbar im Anschluss erfolgt die Gespräch-

saufzeichnung, zu der Leitstellen gesetzlich verpflichtet sind. Das Kommunikationssystem HiPath stellt dann den Notruf an den VAS-B-Server zur Vermittlung und Abfrage durch. Der Disponent kann daraufhin über seinen Disponenten-Arbeitsplatz-PC auf den eingehenden Notruf zugreifen, diesen annehmen und bearbeiten.

An diesem Prozess sind mehrere IT-Systeme unterschiedlicher Hersteller beteiligt und unterliegen zudem dem Risiko, dass einzelne Komponenten oder gar ganze Systeme zeitweise oder langfristig ausfallen. Aus diesem Grund identifizierte die Zentrale Leitstelle Ostthüringen Worst-Case-Szenarien und entwickelte daraufhin ein IT-Infrastrukturkonzept, das mehrere Rückfallebenen und Redundanzen vorsieht:

- **Rückfallebene 1:** Für den Fall, dass ein Arbeitsplatz-PC ausfällt, kann sich der Disponent direkt auf den VAS-B-Client aufschalten und den Notruf wie gewohnt entgegennehmen.
- **Rückfallebene 2:** Die zweite Rückfallebene sieht vor, dass im Falle eines Ausfalls des VAS-B-Servers oder Clients ein Notruf per Telefon an den Disponenten zugestellt wird. Für diesen Fall hat jeder Disponent an seinem Arbeitsplatz ein zusätzliches Telefon, das mit der HiPath verbunden ist und im Falle des o. g. Ausfalls aktiviert wird.
- **Rückfallebene 3:** Die dritte Rückfallebene geht im Schadensszenario davon aus, dass die HiPath-Anlage nicht einsatzbereit ist. In diesem Fall leitet die PSTN- / ISDN-Anlage den Notruf nicht an die HiPath-Anlage weiter, sondern an ein einzelnes Notruftelefon, das für alle Disponenten in der Leitstelle bereitsteht. In diesem Szenario stehen den Disponenten die gewohnten Services, die im nachfolgenden Abschnitt beschrieben werden, nicht zur Verfügung. Um jedoch eine funktionierende Betriebsvariante gewährleisten zu können, hält die Zentrale Leitstelle Ostthüringen eine papiergebundene Lösung bereit. Damit die Disponenten im Ernstfall eine solche Betriebsvariante reibungslos aufrechterhalten können, sind intensive Schulungen, fortwährende Weiterbildungen und praktische Übungen notwendig.

Die Gewährleistung eines reibungslosen Betriebs in unterschiedlichen Betriebsvarianten erfordert von den Disponenten eine hohe Flexibilität und Einsatzbereitschaft. Damit es jedoch (wenn möglich) gar nicht erst so weit kommt, dass die Disponenten auf eine papiergebundene Variante zurückgreifen müssen, sind die IT-Mitarbeiter stets bemüht, die Anlagen und IT-Komponenten regelmäßig zu überprüfen, zu testen und zu warten. Diese Arbeiten finden zum einen im Rahmen der täglichen Arbeit statt, in der auch auftretenden Problemen auf den Grund gegangen wird, um diese langfristig zu beseitigen. Zum anderen finden in der Zentralen Leitstelle Ostthüringen regelmäßig Notfallübungen statt, bei denen die Rückfallebenen getestet werden, um die Funktionsfähigkeit der IT-Infrastruktur sicherzustellen.

11.3.4 Anwendungssicht

Das Einsatzleitsystem COBRA der Firma ISE unterstützt die Disponenten bei der Abwicklung eines kompletten Auftrags von der Notrufannahme bis zum Einsatzende. Während der gesamten Abwicklung ist es wichtig, dass die Disponenten die Lage, den Einsatzort sowie die verfügbaren Rettungsmittel und Einsatzkräfte schnell erfassen können. Ebenso muss das

Einsatzleitsystem in der Lage sein, strukturiert Informationen und Abläufe in Echtzeit zu erheben und klare Handlungsaufforderungen zu geben, um eine effektive Durchführung eines Einsatzes gewährleisten zu können.

Das Einsatzleitsystem der Zentralen Leitstelle Ostthüringen ist als Serversystem realisiert, auf das die Disponenten über ihre Clients zugreifen. Die Anwendungen, die zur Erfüllung der verschiedenen Aufgaben benötigt werden, sind in der Leitstelle Ostthüringen teilweise lokal installiert und teilweise über eine Webanwendung realisiert und werden jedem Disponenten über vier Monitore dargestellt (siehe Abbildung 11-5).

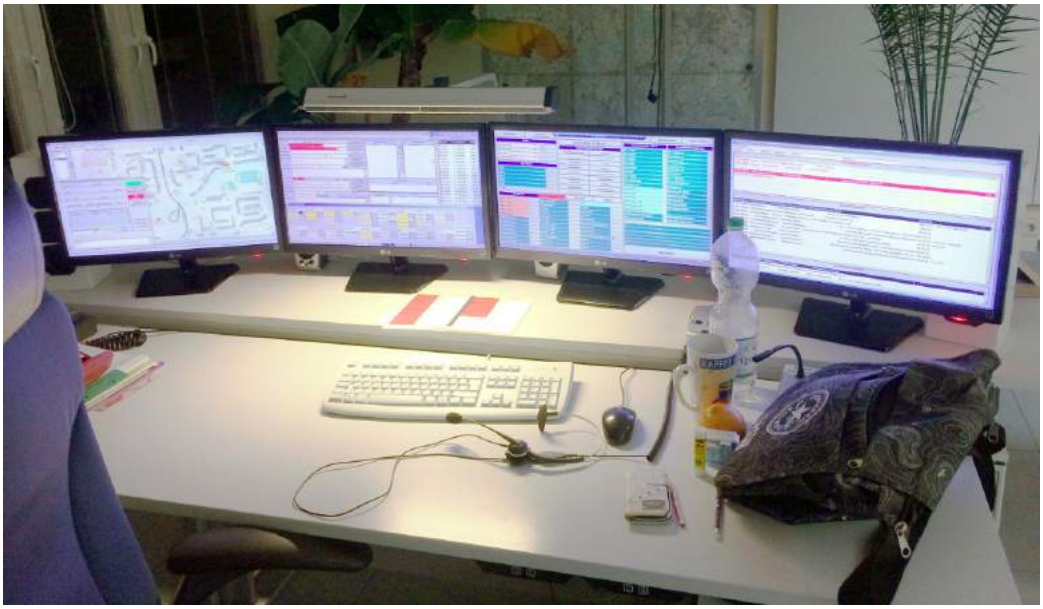


Abbildung 11-5: Arbeitsplatz eines Disponenten der Zentralen Leitstelle Ostthüringen; Foto: Sebastian Dännart)

Für die Disponenten stellt das Einsatzleitsystem eine Schnittstelle zwischen dem Hilfesuchenden und den Einsatzkräften dar, die binnen 60 Sekunden nach Eingang des Notrufs alarmiert werden müssen. In dieser Zeit müssen die Disponenten wichtige Informationen aus unterschiedlichen Quellen erheben, den Überblick behalten und wichtige Entscheidungen, z. B. „Welche Mittel kommen in Frage?“ oder „Wer muss verständigt werden?“, treffen. Aus diesen Gründen ist es wichtig, dass den Disponenten nutzerfreundliche Anwendungen mit intuitiver Bedienoberfläche und hochwertige Hardware zur Verfügung stehen. Im Hinblick auf die einzelnen Aufgaben werden nachfolgend ausgewählte Anwendungen vorgestellt.

Entgegennahme von Notrufen

Im Regelbetrieb stellt das Einsatzleitsystem die Notrufe automatisch an die Disponenten in der Zentralen Leitstelle Ostthüringen durch. Automatisierte Abläufe, die durch das Einsatzleitsystem abgebildet sind, helfen den Disponenten dabei, den Notruf entgegenzunehmen

und zu bearbeiten. Diese Prozesse werden vollständig durch die IT-Infrastruktur abgebildet, sodass eine „vorsintflutliche Papierlösung“ der Vergangenheit angehört. Zwar existiert in der Leitstelle noch eine papiergebundene Lösung mit „Papier und Stift“, jedoch stellt diese Lösung lediglich den Worst Case dar, wenn trotz Redundanzen und Rückfallebenen der IT-Infrastruktur der IT-gestützte Betrieb nicht gewährleistet werden kann.

Im Normalbetrieb sind die Disponenten aufgrund der hohen Anzahl an Notrufen in der Leitstelle einer permanenten Geräuschkulisse ausgesetzt und so arbeiten die Disponenten in der Leitstelle mit hochwertigen Headsets. Die Disponenten haben damit beide Hände frei, um Informationen in Datenbanken zu erheben und in das Einsatzleitsystem einzutragen (siehe Abbildung 11-6). So können sich die Disponenten auf den Notfall konzentrieren und wertvolle Zeit sparen.

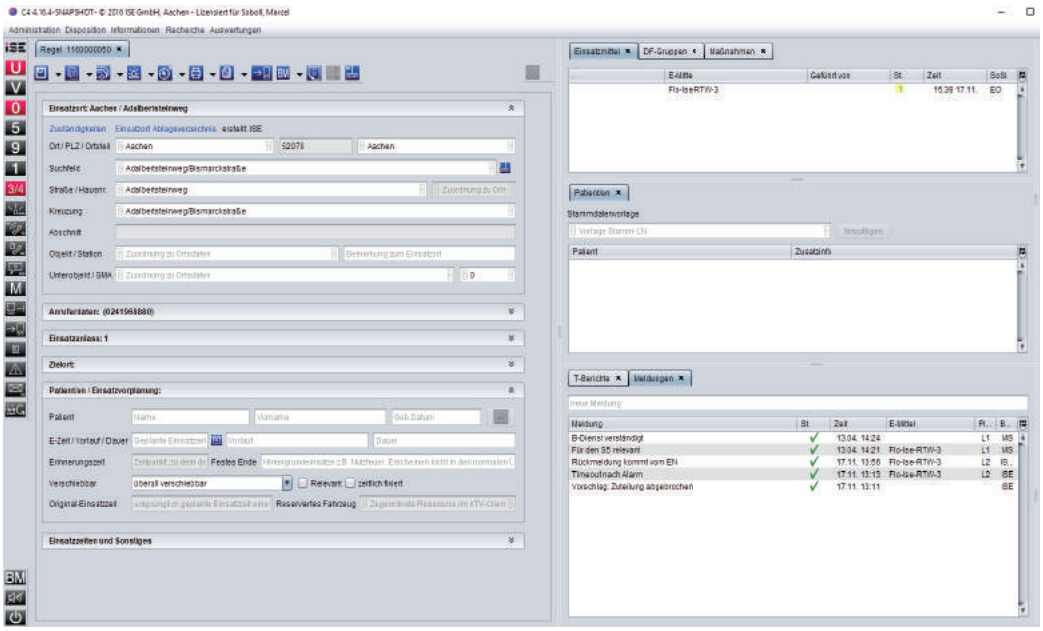


Abbildung 11-6: Einsatzleitsystem COBRA; Quelle: [2]

Die für den Notruf notwendigen Daten tragen die Disponenten via Tastatur und Maus in eine Eingabemaske des Einsatzleitsystems ein. Dazu zählen z. B. Einsatzort, Art des Einsatzes, z. B. Verkehrsunfall, oder Informationen über verletzte Personen.

Führen einer Übersicht der Einsatzmittel

Über eine Datenbank werden den Disponenten Informationen über Ausrüstung, Fahrzeuge und Hubschrauber im Dienstbereich der Leitstelle zur Verfügung gestellt. Diese Informationen beinhalten einerseits die Art des Einsatzmittels, z. B. Löschfahrzeug oder Rettungswagen, andererseits aber auch deren Status, z. B. „frei“ oder „im Einsatz“.

Die Software rescuetrack erlaubt es neben der Prüfung der Verfügbarkeit von Fahrzeugen und Hubschraubern auch, deren Position zu ermitteln, d. h., die Disponenten sehen in Echtzeit die Position der Einsatzmittel auf einer Karte. So können die Disponenten eine Situation sofort erfassen, die am günstigsten stationierten Einsatzkräfte alarmieren und so Ressourcen optimal einsetzen.

Dokumentation von Einsätzen

Eine separate Anwendung zeichnet die Gespräche (Funk, Telefon) entsprechend den gesetzlichen Vorgaben in digitaler Form auf und löscht diese Aufzeichnungen nach 180 Tagen vollautomatisch. Die Dokumentation von Einsätzen ist notwendig für die Erstellung von Statistiken und wichtig für die laufende Prozessoptimierung in der Leitstelle.

Visualisierung mittels Karten

Eine spezielle Anwendung stellt Straßen- und Ortskarten sowie Einsatzpläne zur Verfügung, sodass sich die Disponenten einen Überblick über die Lage verschaffen können (siehe Abbildung 11-7).

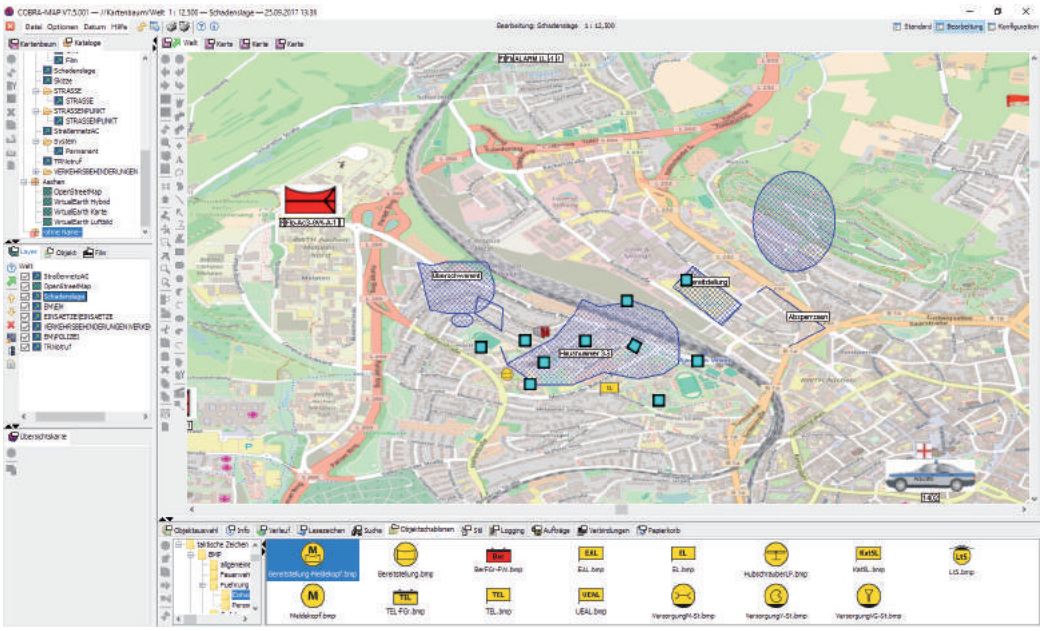


Abbildung 11-7: Lagedarstellung mittels COBRA; Quelle: [2]

Die Darstellung geografischer Gegebenheiten berücksichtigt auch Informationen zu Straßensperren, die im Zuge der täglichen Arbeit per E-Mail eintreffen und von der Leitstelle individuell bewertet werden.

Recherche

Über das Geoinformationssystem (GIS), das in der Stadtverwaltung gehostet wird, können die Disponenten Adressen und Personendaten abfragen. Dies ist z. B. notwendig, wenn der Eigentümer eines einsturzgefährdeten Hauses identifiziert werden muss oder wenn im Zuge eines Bombenfundes erhoben wird, wie viele Personen im Radius betroffen sind.

Darüber hinaus steht den Disponenten ein medizinisches Online-Wörterbuch zur Verfügung, über das Fachbegriffe in Erfahrung gebracht werden können.

Eine weitere Webanwendung stellt die kennzeichengestützte Abfrage von Rettungsdatenblättern dar. Diese Anwendung, die vom Bundeskraftfahramt bereitgestellt wird, bietet Informationen für Einsatzkräfte vor Ort z. B. im Umgang mit Unfallfahrzeugen. Die Rettungsdatenblätter beinhalten standardisierte Informationen über verbaute technische Systeme, wie Airbags oder Gurtstraffer, Besonderheiten zur Karosserie oder zum Fahrzeugantrieb.

Eine weitere Datenbank ermöglicht es den Disponenten, Informationen über Gefahrgüter zu erheben. Über die UN-Nummer, die bei Gefahrguttransporten auf einer orangefarbenen Tafel aufgeführt ist, können die Disponenten das Gefahrgut ermitteln und die Gefährdung bewerten. Das Spektrum der Gefahrguteinsätze beinhaltet radioaktive, chemische oder biologische Stoffe, die jeweils eigene Rettungs- und Hilfsmittel erfordern.

Alarmierung der Einsatzkräfte

Das Einsatzleitsystem unterstützt die Disponenten beim Alarmieren der Einsatzkräfte und stellt ihnen Kommunikationsmöglichkeiten in Form von Telefon, Funk und Datenleitungen zur Verfügung.

Über die Datenleitung werden Informationen an den Einsatzleiter gesendet, die im Zuge der Notrufbearbeitung ermittelt wurden. Dazu gehören die Rettungsdatenblätter von Unfallfahrzeugen, damit die Einsatzkräfte wissen, welche Stellen am Unfallfahrzeug gegebenenfalls nicht aufgeschnitten werden dürfen.

Darüber hinaus können die Disponenten die an Bord der Rettungsmittel befindlichen Navigationsgeräte kontaktieren, um Informationstexte und Zielkoordinaten zu senden, die die Fahrer sicher zur Einsatzstelle führen. Über diesen Kommunikationsweg werden auch Statusmeldungen, wie z. B. „Brand unter Kontrolle“, direkt vom Einsatzort an die Disponenten gesendet.

Über die bidirektionale Kommunikation zwischen Leitstand und Einsatzkräften können zudem ohne große Zeitverzögerung weitere Mittel, wie z. B. Rettungshubschrauber oder spezielle Hilfsmittel, z. B. Sonderlöschmittel, angefordert werden.

11.3.5 Technische Sicht

Wie bereits beschrieben ist das Netzwerk der Leitstelle ein geschlossenes, nach außen abgeschottetes Netzwerk. Verbindungen nach außen werden lediglich über ReCoBS, TightGate-Pro oder über VPN-Verbindungen zwischen Wartungsschnittstellen und Dienstleistern realisiert. Auch das Netzwerk selbst ist in Subnetze untergliedert, die Kommunikationsanlagen von den Anwendungsservern und Arbeitsplatz-PCs trennen.

Die Disponenten mit ihren Arbeitsplätzen und die technische Infrastruktur sind zusätzlich räumlich getrennt. So befinden sich an den Arbeitsplätzen nur die Eingabe- und Ausgabegeräte, während die Disponenten-PCs im Serverraum stehen. Die Verbindung wird über Remote-Extender realisiert.

Auch an den Arbeitsplätzen wird auf Ausfallsicherheit geachtet. So ist jeder Arbeitsplatz gleich ausgestattet, sodass jeder Disponent an jedem Platz gleich arbeiten kann. Je Arbeitsplatz kann für den Fall, dass der Disponenten-PC ausfällt, über ein KVM-Switch direkt auf den jeweiligen VAS-B-Client zugegriffen werden, sodass die digital unterstützte Kommunikation weiterhin funktioniert (Abbildung 11-8); dies bildet die 1. Rückfallebene.

USB-Sticks können durch die Disponenten aufgrund der physischen Trennung nicht angeschlossen werden, was die Gefahr durch BadUSB-Angriffe minimiert.

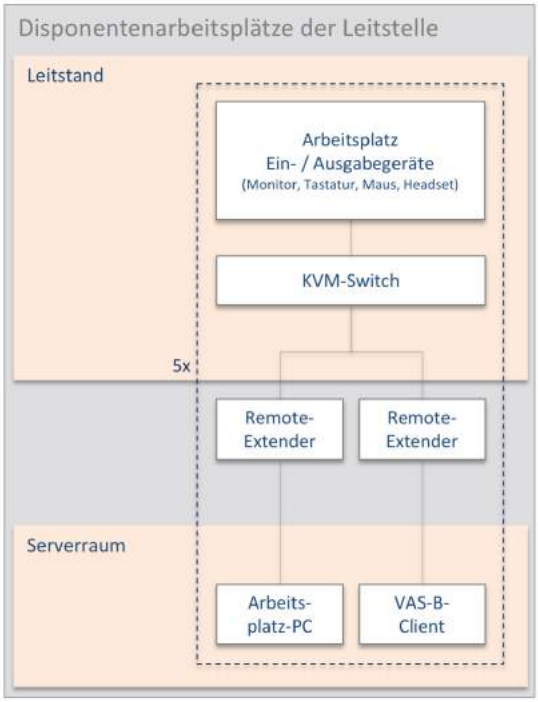


Abbildung 11-8: Anbindung der Disponentenarbeitsplätze

Für den COBRA-Server gibt es zudem eine Reserve in Form eines PCs mit lokaler COBRA-Installation, der sich in einem komplett separierten Netzwerk befindet. Neben der Kaltreserve existiert eine weitere Reserve in Form einer lokalen Installation auf einem PC. Die Datenbank der lokalen Installation wird manuell mehrmals im Monat aktualisiert.

Weitere redundante Reserven hält die Leitstelle zudem für weitere IT-Infrastrukturkomponenten, wie z. B. Router / Switche oder ISDN-Anlage vor. Diese sind als Kaltreserve realisiert und bereits in die Serverracks integriert, sodass im Falle eines Ausfalls einer Komponente lediglich ein manueller Anschluss erfolgen muss. Ebenso ist die PSTN- / ISDN-Anlage hin-

sichtlich ihrer Zubringerleitungen redundant angebunden. Hier wurde die Anbindung über Leitungen unterschiedlicher Straßen und Gebietszüge realisiert.

Da in der Leitstelle Ausfallsicherheit eine wichtige Rolle spielt, wird zudem die Temperatur im Serverraum durchgehend überwacht und Ausfälle durch Kurzschlüsse werden durch Steckdosen mit Einzelplatzsicherungen und Flintensicherungen an jedem Computer verhindert.

Um Daten auf die Rechensysteme zu transferieren, wird eine Schleuse eingesetzt. Auf dem Schleusenrechner befinden sich verschiedene Detektionssysteme, wie etwa ein Stickdetektor. Von dort werden die Daten dann per eigenem – immer gleichbleibendem – USB-Stick, der vor und nach Datentransfers Checks durchläuft, auf die entsprechenden Systeme transferiert.

11.3.6 Normen, Standards und Gesetze

Eine Leitstelle unterliegt neben allgemeinen Normen und Gesetzen auch solchen, die durch die Leitstellentätigkeit oder die Verwendung von Telekommunikation und Funk bedingt sind.

Die Leitstelle Ostthüringen unterliegt also zum einen allgemeinen Gesetzen, wie dem Telekommunikationsgesetz, der Funkrichtlinie und dem Datenschutzgesetz. In Zukunft – nach der Umstellung auf Digitalfunk – wird auch die Digitalfunkrichtlinie eine Rolle spielen. Zum anderen unterliegt die Leitstelle auch Gesetzen und Richtlinien mit Bezug auf die Leitstellentätigkeit. Dazu gehören das Thüringer Brand- und Katastrophenschutzgesetz, das die Grundlage der Arbeit der Leitstelle Ostthüringen bildet, die Polizeidienstvorschrift 810 sowie die Notrufverordnung. Dazu gehören Anforderungen an den Betrieb einer Notrufabfragestelle. Eine dieser Anforderungen ist beispielsweise ein niedriger Geräuschpegel am Leitstand, sodass die Konzentrationsfähigkeit der Disponenten nicht beeinträchtigt wird. Das ist einer der Gründe für die Trennung der Ein- und Ausgabegeräte von den Disponenten-PCs, die im Serverraum stehen. Weitere zentrale Anforderungen sind eine ständige Verfügbarkeit und niedrige Reaktionszeiten für Notrufannahme und Alarmierung der Einsatzkräfte.

Die Zentrale Leitstelle Ostthüringen verwendet als Standard für die IT-Sicherheit den BSI-Grundschutz, wobei sie noch nicht durchgängig zertifiziert ist. Ein einheitliches Niveau wird aber angestrebt.

11.3.7 Stand der IT-Sicherheit

Die Leitstelle Ostthüringen sieht sich Änderungen in Bedingungen und Anforderungen gegenüber und so ist auch die IT der Leitstelle ständig im Wandel begriffen. Zum Zeitpunkt der Erstellung der Fallstudie waren die meisten Prozesse automatisiert und auf modernem Stand.

Die Ausfallsicherheit des Alarmierungsprozesses ist das wesentliche Ziel in der IT-Sicherheit. Um die Ausfallsicherheit zu gewährleisten, existieren drei Rückfallebenen. Die Rückfallebene 1 (Umschalten per KVM-Switch direkt auf den VAS-Client) besteht für den Fall, dass ein Disponenten-PC ausfällt, Rückfallebene 2 (Telefon an der HiPath-TK-Anlage) bedient den Fall, dass die VAS-B-Komponenten ausfallen, und die 3. Rückfallebene (Telefon direkt an der Leitung) ist für den Fall, dass die computergestützten Komponenten des Alarmierungsprozesses ausfallen.

Schulungen stellen im Betrieb der Leitstelle eine besondere Herausforderung dar, weil während der Dienstzeit eine durchgehende Bereitschaft, Notrufe anzunehmen, gefordert ist.

Daher können Schulungen nur vor Dienstbeginn oder nach Dienstende stattfinden. Trotzdem finden verwaltungsweit regelmäßige Schulungen zur IT-Sicherheit statt und es gibt einen Belehrungsordner für den Fall, dass während des regulären Dienstes Fragen zum Thema IT-Sicherheit oder Datenschutz aufkommen. Systemausfälle und die damit einhergehenden Prozesse werden regelmäßig trainiert.

Für die Zukunft ist in der Zentralen Leitstelle Ostthüringen eine Verbesserung der Ausfallsicherheit durch Virtualisierung und den Einsatz einer webbasierten Software geplant. Des Weiteren ist zum Zeitpunkt der Erstellung dieser Fallstudie ein Gutachten in Arbeit, das die Umstellung der Funkkommunikation auf Digitalfunk bewertet. Eine solche Umstellung würde den Datenschutz verbessern, da analoger Funk im Gegensatz zum Digitalfunk leicht abgehört werden kann. Für Oktober 2017 ist vorgesehen, dass die Leitstelle das eCall-System unterstützt. Bei eCall setzen Fahrzeuge automatisch Notrufe ab, bei denen für die Rettung wichtige Daten mitgesendet werden. Ein Beispiel für solche Daten ist die Fahrzeugidentifikationsnummer (FIN), mit der das Rettungsdatenblatt ermittelt werden kann.

11.4 Erfolgsfaktoren

Die IT-Infrastruktur der Zentralen Leitstelle Ostthüringen muss im Spannungsfeld zwischen neuen Anforderungen, einer Diskussion der strategischen Weiterentwicklung, limitierten Ressourcen der Kommunen weiterentwickelt werden. Hochverfügbarkeit des Alarmierungsprozesses ist für die IT ein zentrales Thema.

Basis-Technologien der Leitstelle wandeln sich: Neue und moderne Herstellerlösungen erhöhen auch die Komplexität der technischen Systeme und der Prozesse in der Zentralen Leitstelle Ostthüringen. Aus diesem Grund ist es wichtig, dass sich das Management für ein Einsatzleitsystem entschieden hat, das hinsichtlich Insellösungen anderer Hersteller kompatibel ist und diese Lösungen modular integrieren kann.

Richtlinien, Gesetze und Verordnungen auf Bundes- und Landesebene fordern zudem höchste Verfügbarkeit, die die Leitstelle Ostthüringen mittels Redundanzen auf mehreren Rückfallebenen, eines modularen Systemaufbaus und Schnittstellen zu Systemen Dritter realisiert. So können Hilfesuchende im Einsatzgebiet der Leitstelle auch bei Ausfällen der IT-Systeme oder gar Netzwerke Notrufe absetzen und erhalten jederzeit die benötigte Hilfe.

Ein wesentlicher Erfolgsfaktor ist das Engagement der Mitarbeiter der Leitstelle, die auch über den eigentlichen Aufgabenbereich Probleme erkennen und Lösungen entwickeln. Die Mitarbeiter der Leitstelle wollen Probleme nicht einfach nur erkennen, sondern den Ursachen auf den Grund zu gehen, um Probleme dauerhaft zu verhindern. Die Mitarbeiter der Leitstelle wollen ihre IT-Infrastruktur nicht nur als Anwender *kennen*, sondern auch die Hintergründe und das Zusammenspiel einzelner Komponenten *verstehen*. Dieses Verständnis trägt in der Leitstelle maßgeblich dazu bei, dass die Belegschaft in der Lage ist, Probleme selbst zu lösen.

Die Belegschaft der Leitstelle verfügt über fundierte IT-Kenntnisse, insbesondere in der grafischen Informationsverarbeitung und -darstellung, Datenbanken und kontextbezogener Prozessautomatisierung und dies trägt zum Erfolg des Gesamtsystems bei.

Zwei weitere Erfolgsfaktoren, die maßgeblich dazu beitragen, dem schnellen Wandel zu begegnen, sind gute Strukturen und festgelegte Prozesse. Diese sind einerseits formal, z. B. in Belehrungen und Weisungen, niedergeschrieben, andererseits werden die Strukturen und Prozesse durch die Belegschaft tagtäglich gelebt. Hohes Engagement, Bereitschaft zur Pflichterfüllung und Commitment zum Arbeitgeber der Belegschaft der Leitstelle Ostthüringen in Gera sind hier essenziell für die erfolgreiche Arbeit der Leitstelle.

In der Zukunft wären dabei einige Punkte für die Leitstelle besonders hilfreich:

- Offene und standardisierte Schnittstellen in Ausschreibungen
- Steigerung der Gesamtwirtschaftlichkeit in Ausschreibungen
- Mehr Einheitlichkeit hinsichtlich der implementierten Lösungen unterschiedlicher Leitstellen und anderer angeschlossenen Organisationen

11.5 Danksagung

Wir danken dem Bundesministerium für Bildung und Forschung (BMBF) für die Möglichkeit der Forschung im Rahmen des Projektes VeSiKi, Förderkennzeichen 16KIS0213K sowie des Projektes MoSaIK, Förderkennzeichen 16KIS0173K.

11.6 Literaturverzeichnis

[1] Gera, Fachdienst 2600 Brand- und Katastrophenschutz. Verfügbar unter: https://www.gera.de/sixcms/detail.php?id=16946 [zugegriffen: 25-Sep-2017].

[2] Soboll, M., 2017. Screenshots von iSE-COBRA-Software. Informatikgesellschaft für Software-Entwicklung mbH, Aachen.

12 Informationssicherheit durch ClassifyIt: Informationssicherheit durch gestützte Klassifizierung von Dokumenten und E-Mails

Andreas Rieb, Universität der Bundeswehr München

Die vorliegende 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.

Keywords: Klassifizierung, Informationssicherheit, Organisationssicherheit, Geheimhaltungsstufen

12.1 Unternehmen

12.1.1 Unternehmensprofil

ugarbe.de software wurde 1995 gegründet und ist ein deutscher Anbieter für Lösungen mit Schwerpunkt auf Informationssicherheit. ugarbe.de software ist ein Einzelunternehmen mit Sitz in Koblenz.

ugarbe.de software unterstützt Organisationen in der Informationssicherheit und adressiert mit dem Tool ClassifyIt alle Organisationen, die mit sensiblen Informationen umgehen und Schutzbedarfe haben. Dazu zählen Organisationen im Government-Bereich, wie Bundeswehr und NATO sowie EU-Behörden.

12.1.2 Strategische Ausrichtung

Die Motivation von ugarbe.de software ist es, Informationssicherheit da zu betreiben, wo sensible Informationen entstehen – beispielsweise, wenn ein Mitarbeiter sensible Informationen generiert, ein Dokument anlegt oder versendet. Die Software von ugarbe.de software ist flexibel und kann an die Organisationsrichtlinien adaptiert werden. Das Selbstbild von ugarbe.de software beschreibt die Philosophie: „Policies müssen Tools machen und nicht umgekehrt". Das Werkzeug ClassifyIt ist seit 2007 erfolgreich im Einsatz und wird im Kontext dieser Fallstudie näher beschrieben.

ugarbe.de software möchte in den nächsten Jahren ClassifyIt in weitere Kritische Infrastrukturen im europäischen Umfeld und hier vor allem in Behörden und kritischen Industrie- und Wirtschaftszweigen ausrollen, um dort die Informationssicherheit zu erhöhen. Darüber hinaus ist geplant, die Funktionalität von ClassifyIt zu erweitern, um z. B. mobile Geräte zu unterstützen, die Software in eine bereits vorhandene Public Key Infrastructure (PKI) in Organisationen zu integrieren und das Dateiformat PDF zu unterstützen.

Neben der Weiterentwicklung von ClassifyIt verfolgt ugarbe.de software langfristig das Ziel, den Kunden Security-as-a-Service anzubieten und Systemberatung sowie Support bei der organisationsspezifischen Richtlinienentwicklung im Themenfeld Informationssicherheit anzubieten.

12.1.3 Fallstudienpartner

Name	Position im Unternehmen
Ralf Ulrich Garbe	Geschäftsführer von ugarbe.de software
Andreas Rieb	Wissenschaftlicher Mitarbeiter, Universität der Bundeswehr München

12.2 Kritische Infrastruktur

12.2.1 Einordnung als KRITIS

Als IT-Dienstleister ist ugarbe.de software selbst keine Kritische Infrastruktur gemäß dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) und den KRITIS-Verordnungen. Jedoch unterstützt ugarbe.de software mit seiner Lösung ClassifyIt viele Kunden im Bereich Kritischer Infrastrukturen im europäischen Raum sowie viele Kunden im Sektor *Staat und Verwaltung*.

12.2.2 Risikoanalyse

Im Durchschnitt sind ca. 60 % bis 75 % aller Dokumente in einer Organisation sensitiver Natur, 5 % bis 10 % sogar „echte kritische Informationen". Die Vergangenheit hat immer wieder gezeigt, dass nicht-markierte Informationen von Nutzern anders wahrgenommen und somit anders behandelt werden. Entweder werden nicht-markierte Informationen fälschlicherweise an nicht-berechtigte Personen weitergegeben oder aber nicht-markierte Informationen werden fälschlicherweise nicht an berechtigte Personen weitergegeben. Beide Varianten stellen ein Risiko dar: „Der Verlust von sensiblen Inhalten kann durch die leichtsinnige Nutzung und Versendung von internen oder aber auch externen Daten immer dann erfolgen, wenn einerseits der Sicherheitsgrad nicht bekannt [sic!], weil fehlende Kennzeichnung, oder aber andererseits bereits vorhandene Klassifizierungsstandards nicht ihre volle Berücksichtigung finden" [1].

Mögliche Auswirkungen eines Verlusts sensibler Daten sind: Regierungsorganisationen können einen enormen Reputationsverlust erleiden, wenn beispielsweise politische Überlegungen vorzeitig in die Medien gelangen. Eine Steigerung ist im militärischen Kontext denkbar, wenn etwa einsatzrelevante, streng geheime Informationen in die Hände des Gegners fallen und Leib und Leben der im Auslandseinsatz befindlichen Soldaten dadurch gefährdet werden. Für kommerzielle Organisationen kann ein Verlust sensibler Informationen hohe monetäre Verluste bedeuten, wenn beispielsweise Entwicklungsdaten in die Hände von Konkurrenten geraten.

Die Gründe für einen solchen Datenverlust sind vielfältig. Exemplarisch genannt sind hier folgende Gefährdungen aus den BSI-IT-Grundschutzkatalogen:

- G 3.44 Sorglosigkeit im Umgang mit Informationen [2]
- G 3.13 Weitergabe falscher oder interner Informationen [3]
- G 3.8 Fehlerhafte Nutzung von IT-Systemen [4]
- G 3.1 Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten [5]

Die Erfahrungen bei Garbe sind vergleichbar: „Opfer von Spear Phishing sind oft Geheimnisträger", und Data Leakages passieren häufig aus Nachlässigkeit (der Mitarbeiter leitet sensible Daten aus Versehen an Dritte weiter) oder weil Daten falsch abgespeichert bzw. klassifiziert wurden. Deshalb ist es wichtig, dass Daten direkt dann klassifiziert werden, wenn sie entstehen – und genau hier unterstützt ClassifyIt die Informationssicherheit. Eine klare Einstufung und Kennzeichnung der Daten unterstützt damit Maßnahmen der Data Loss Prevention (DLP).

12.3 Die Software ClassifyIt

12.3.1 Beschreibung

ClassifyIt verhindert, dass Dokumente ohne eine Sicherheitskennzeichnung erstellt werden, die nicht dem Informationssicherheitskonzept entsprechen. ClassifyIt ist eine Software, die sich als Modul in Microsoft Outlook sowie Microsoft-Office-Applikationen, wie Word, Excel und PowerPoint (ab Version 2010), einbinden lässt. Nach erfolgreicher Einbindung unterstützt ClassifyIt die Mitarbeiter mit einer visuellen und technischen Klassifizierung von Dokumenten und E-Mails und bietet zudem die Möglichkeit der Verschlüsselung von E-Mailanhängen. Je nach Konfiguration kann der Mitarbeiter dazu gezwungen werden, eine Klassifizierung vorzunehmen, wenn Daten erstellt werden. In [1] beschreibt Garbe: „Die Erzwingung ist, wenn auch banal erscheinend, einer der wesentlichsten Kriterien [sic!] um die unkontrollierte Verbreitung von Informationen einzuschränken. Das schwächste Glied in der Kette der Sicherstellung von IT-Sicherheit ist und bleibt der Mensch, der durch ‚Nichtwissen' u. U. vertrauliche Informationen an Nichtberechtigte weitergibt."

Die Klassifizierung der Informationen basiert dabei auf den in der Organisation vorherrschenden Richtlinien bzw. Geheimhaltungsstufen, wie z. B.:

- STRENG GEHEIM
- GEHEIM
- VERSCHLUSSSACHE – VERTRAULICH
- VERSCHLUSSSACHE – NUR FÜR DEN DIENSTGEBRAUCH
- OFFEN

Darüber hinaus kann es weitere Einschränkungen, wie etwa den Zusatz „NUR FÜR DEUTSCHE" geben. Ferner kann es vorkommen, dass Organisationen andere Begriffe für die o. g. Stufen verwenden: z. B. „VERTRAULICHE DIENSTSACHE". Hier bietet ClassifyIt die Flexibilität, die Geheimhaltungsstufen der Organisation exakt so abzubilden, wie sie im Informationssicherheitskonzept dieser Organisation definiert sind.

Zudem kann es sowohl im nationalen sowie im internationalen Kontext vorkommen, dass kooperierende Organisationen unterschiedliche Geheimhaltungsstufen verwenden. Geheim-

haltungsstufen können sich sowohl von den Begriffen als auch in der Anzahl der Stufen unterscheiden. Auch hier unterstützt ClassifyIt dabei, die Geheimhaltungsstufen abzubilden und die Informationen in der Geheimhaltungsstufe der Organisation zu visualisieren. Letzteres ist vor allem dann von großem Interesse, wenn beispielsweise NATO-Partner wie Deutschland und Griechenland Informationen austauschen, die unterschiedliche Alphabete bzw. Zeichensätze verwenden. So würde die deutsche Einstufung „VERSCHLUSSSACHE – VERTRAULICH“ beim Empfänger in der griechischen Organisation entsprechend der Landessprache eingestuft und visualisiert werden.

12.3.2 Geschäftssicht

Aus Geschäftssicht sind mehrere Parteien in die Realisierung einer sicheren Lösung für Informationssicherheit mittels ClassifyIt involviert. Das Management definiert die strategische Ausrichtung und damit auch die Informationssicherheitsstrategie der Organisation und stellt die finanziellen Mittel bereit. Die IT-Sicherheitsexperten und die Datenschutzbeauftragten geben für ClassifyIt die Organisationsrichtlinien und Geheimhaltungsstufen vor. Die Nutzer werden durch das Microsoft-Office-Modul von ClassifyIt unterstützt: Das Modul ist in Microsoft Outlook sowie Microsoft-Office-Applikationen wie Word, Excel und PowerPoint integriert.

Die Software ClassifyIt setzt Organisationsrichtlinien und Geheimhaltungsstufen durch. Organisationsrichtlinien und Geheimhaltungsstufen müssen vor dem Rollout der Software zwischen ugarbe.de software sowie den Datenschutzbeauftragten und IT-Sicherheitsexperten erfasst und in ClassifyIt abgebildet werden. Da in den meisten Fällen solche Richtlinien und Geheimhaltungsstufen in Organisationen bereits existieren, ist der Aufwand eher gering.

Wenn ClassifyIt für den Austausch mit anderen Organisationen genutzt wird, muss eine Abbildung der Geheimhaltungsstufen definiert werden. Dies findet meist in einem Workshop statt, an dem neben ugarbe.de software die Datenschutzbeauftragten und IT-Sicherheitsexperten der beteiligten Organisationen teilnehmen.

Sobald die Organisationsrichtlinien und Geheimhaltungsstufen und ggf. das Mapping durch ugarbe.de software in ClassifyIt umgesetzt sind, rollt die IT-Abteilung der Organisation die Software auf den Clients aus.

Sofern die Funktionalität vorhandene technische Lösungen der Informationssicherheit Dritter berührt, sind diese ebenfalls in die Implementierung involviert. Dritte Parteien sind zudem involviert (sofern die IT-Abteilung der Organisation diese Aufgabe nicht erfüllen kann), wenn mittels ClassifyIt klassifizierte Dokumente an der Firewall oder am E-Mail-Gateway überprüft werden sollen. Die Firewall oder das E-Mail-Gateway können bei geeigneter Konfiguration überprüfen, ob beispielsweise eine als „GEHEIM“ eingestufte E-Mail an Dritte versendet werden darf.

Bei einer Implementierung von ClassifyIt sind aus organisatorischer Sicht nur wenige neue Aufgaben zu bewältigen. Es fallen keine neuen Verantwortlichkeiten an und so ist eine Neu- oder Umstrukturierung einer Organisation nicht erforderlich.

12.3.3 Prozesssicht

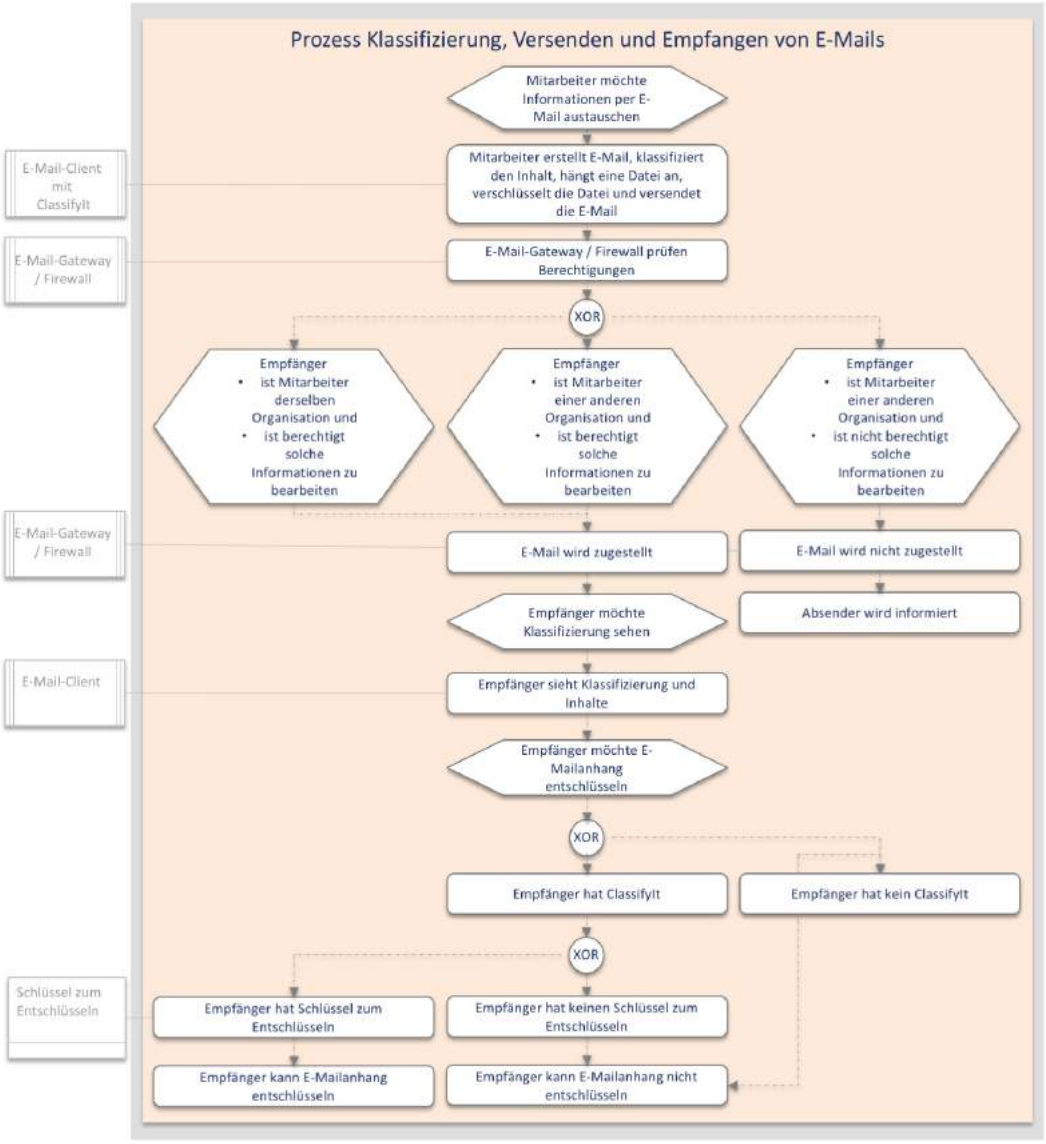


Abbildung 12-1: Prozess Klassifizierung, Versenden und Empfangen von E-Mails

In Abbildung 12-1 wird der Prozess von ClassifyIt vereinfacht dargestellt: Ein Mitarbeiter erstellt eine E-Mail mit sensitiven Inhalten und einem verschlüsselten E-Mail-Anhang. Im Anschluss wird die E-Mail an Personen innerhalb bzw. außerhalb der Organisation gesendet.

Zunächst erstellt der Mitarbeiter die Inhalte der E-Mail und stuft die E-Mail entsprechend den von der Organisation vorgegebenen Geheimhaltungsstufen mit ClassifyIt ein. ClassifyIt klassifiziert die E-Mail sowohl mit einer visuellen Markierung als auch mit Einträgen in den

X-Headern. Sollte ein Mitarbeiter eine solche Klassifizierung vor Absenden oder Speichern einer E-Mail bzw. Datei vergessen, erinnert ClassifyIt den Nutzer daran, dass die Klassifizierung Pflicht ist, und fordert diese vom Nutzer ein.

Neben dieser Einstufung hat der Mitarbeiter die Möglichkeit, den E-Mail-Anhang zu verschlüsseln. Hierzu stehen dem Mitarbeiter in Abhängigkeit von der Implementierung verschiedene Methoden, wie z. B. mittels PIN-basierter Schlüssel, zur Verfügung.

Sobald der Mitarbeiter die E-Mail versendet, wird sie zum E-Mail-Gateway weitergeleitet. Je nach IT-Infrastruktur und Implementierung kann nun geprüft werden, ob der Empfänger berechtigt ist, eine E-Mail entsprechend der vom Absender definierten Geheimhaltungsstufe zugestellt zu bekommen. Das E-Mail-Gateway bzw. die Firewall verwerfen die E-Mail, sofern diese Prüfung ergeben hat, dass der Empfänger für E-Mail-Inhalte dieser Geheimhaltungsstufe nicht berechtigt ist. Andernfalls wird die E-Mail zugestellt.

Die visuelle Markierung durch ClassifyIt ist im Falle einer Zustellung auch für Empfänger sichtbar, die z. B. in Organisationen arbeiten, die ClassifyIt nicht im Einsatz haben. Für Empfänger im internationalen Umfeld ist ClassifyIt zudem in der Lage, diese Markierung in der jeweiligen Landessprache (und im entsprechenden Zeichensatz) anzuzeigen – hier muss zuvor ein entsprechendes Matching der Geheimhaltungsstufen in ClassifyIt implementiert werden.

ClassifyIt bietet die Möglichkeit, E-Mail-Anhänge zu verschlüsseln. ClassifyIt kann Anhänge verschlüsseln und entschlüsseln und bietet drei einfach zu nutzende Methoden an: vordefinierte Schlüssel, PIN-basierte Schlüssel und öffentliche / private Schlüssel (inklusive deren Verwaltungsfunktionen). Sobald ein Empfänger eine E-Mail mit einem verschlüsselten Anhang erhält, ist es zwingend notwendig, dass der Empfänger ebenfalls ClassifyIt nutzt, um den E-Mail-Anhang entschlüsseln zu können. Beim PIN-Verfahren muss der Schlüssel bzw. die PIN über einen separaten Kommunikationsweg übertragen werden.

12.3.4 Anwendungssicht

„Das Tool soll für Nutzer und Administratoren so einfach wie möglich sein in seiner Anwendung" und „es soll selbsterklärend sein" – So lautete die Vision bei der Entwicklung von ClassifyIt. ClassifyIt ist ein nutzerfreundliches Tool, das sich als Modul in Microsoft Outlook sowie Microsoft-Office-Applikationen wie Word, Excel und PowerPoint (ab Version 2010) einbinden lässt (siehe Abbildung 12-2).

ClassifyIt bietet Nutzerfreundlichkeit sowohl für Anwender als auch Administratoren. Für die Nutzer stellt ClassifyIt ein Menü zur Verfügung, bei dem die Klassifizierung des Dokuments ausgewählt wird. Unmittelbar nach der Klassifizierung visualisiert ClassifyIt die entsprechende Geheimhaltungsstufe gut leserlich im Dokument (siehe Abbildung 12-3) bzw. in der E-Mail (siehe Abbildung 12-4).

Wie bereits angesprochen, bietet ClassifyIt die Möglichkeit, E-Mail-Anhänge zu verschlüsseln (siehe Abbildung 12-5). ClassifyIt kann Anhänge verschlüsseln und entschlüsseln und bietet drei einfache Methoden: vordefinierte Schlüssel, Pin-basierter [sic!] Schlüssel und öffentliche / private Schlüssel (inklusive deren Verwaltungsfunktionen)" [1].

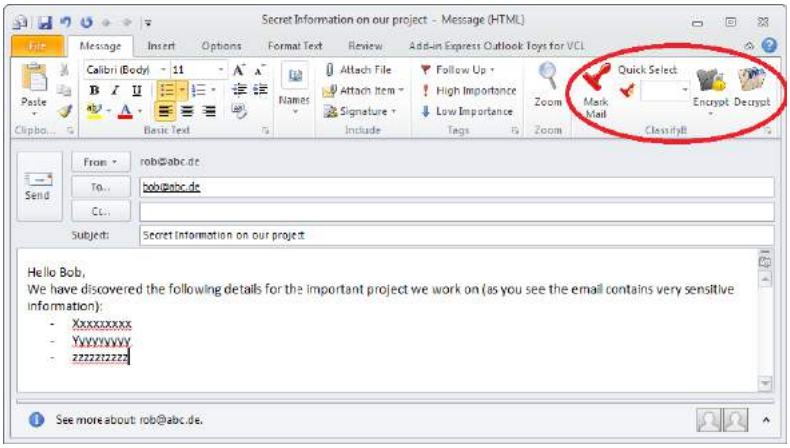


Abbildung 12-2: ClassifyIt in Microsoft Outlook; Quelle: ugarbe.de Software

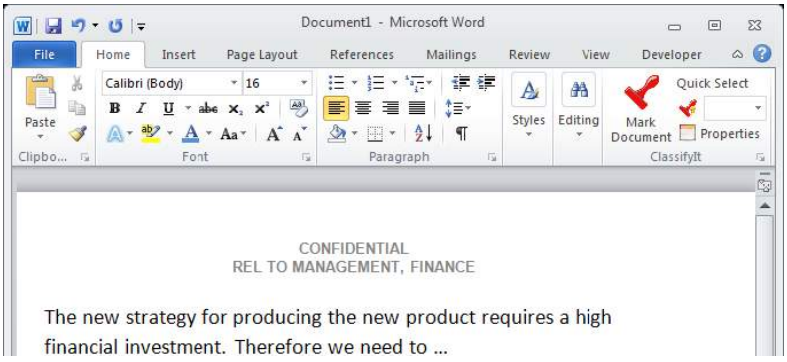


Abbildung 12-3: Visuelle Markierung der Klassifizierung durch ClassifyIt in Microsoft Word; Quelle: ugarbe.de Software

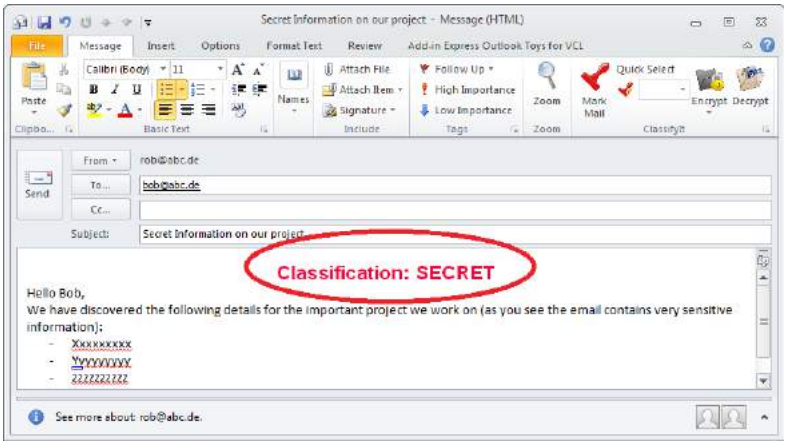


Abbildung 12-4: Visuelle Markierung der Klassifizierung durch ClassifyIt in Microsoft Outlook; Quelle: ugarbe.de Software

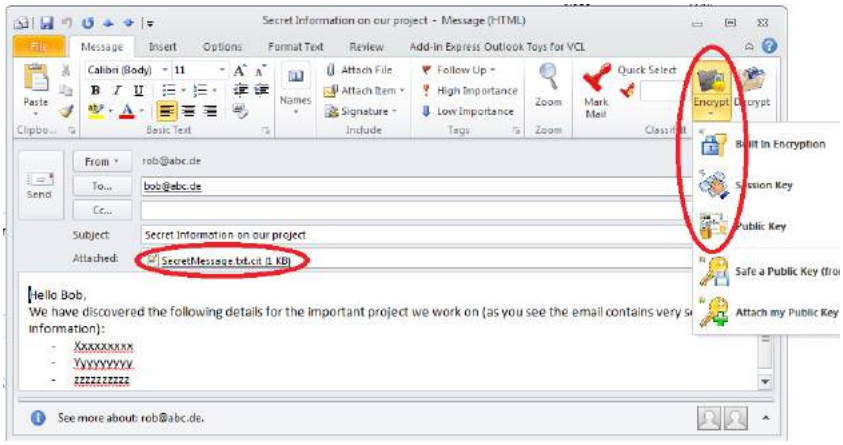


Abbildung 12-5: ClassifyIt in Microsoft Outlook mit der Option zur Verschlüsselung von E-Mail-Anhängen; Quelle: ugarbe.de Software

Während die visuelle Markierung auch für einen Empfänger sichtbar ist, der ClassifyIt nicht nutzt, ist es hier zwingend notwendig, dass die Gegenstelle (der Empfänger) ebenfalls ClassifyIt nutzt, um die E-Mail-Anhänge wieder entschlüsseln zu können.

Zudem unterstützt ClassifyIt bei der Awareness rund um Informationssicherheit, indem Pop-Up-Menüs Anwendern die Geheimhaltungsstufen auch mittels Beispielen erläutern.

12.3.5 Technische Sicht

ClassifyIt ist als Modul in Microsoft Outlook sowie Microsoft-Office-Applikationen, wie Word, Excel und PowerPoint, weitestgehend autark und benötigt keinerlei Internetanbindung, um z. B. neue Konfigurationsdateien zu beziehen.

ClassifyIt selbst wird über das zentrale Softwareverteilungssystem innerhalb einer Organisation ausgerollt. Dasselbe gilt auch für Updates dieser Software, die über die Website von ugarbe.de software bereitgestellt werden. Die Konfiguration von Clients muss vorsehen, dass in den Microsoft Produkten Add-ins aktiv sind und nicht manuell deaktiviert werden können.

Wenn sich Unternehmensrichtlinien, Geheimhaltungsstufen oder die Zusammenarbeit mit externen Organisationen ändern, kann eine Anpassung der Konfigurationsdatei notwendig werden. ugarbe.de software nutzt das JSON-Format, sodass die Konfigurationsdatei mit herkömmlichen Texteditoren beispielsweise von einem Administrator geändert werden kann (siehe Abbildung 12-6).

Nach Änderung der Konfigurationsdatei muss der Administrator (wie bei der initialen Konfigurationsdatei auch) diese Datei auf einem internen Web- oder Fileserver bereitstellen und die Integrität dieser Datei sicherstellen. Dies wird mit dem ConfigFile Signer ermöglicht, in dem die Konfigurationsdatei digital signiert wird (siehe Abbildung 12-7). Das schützt die Konfigurationsdatei vor unautorisierten Änderungen.

```
{
"admin_mode":       false,
"classifications":
        [{"real":    "OPEN",
          "trans":   "OFFEN",
          "color":   "0x000000",
          "x-class": "O",
          "descr":   "no prctection r

         {"real":    "RESTRICTED",
          "trans":   "EINGESCHRÄNKT",
          "color":   "0xFF0000",
          "x-class": "R",
          "descr":   "medium protecti
```

Abbildung 12-6: Auszug einer Konfigurationsdatei, Quelle: ugarbe.de Software

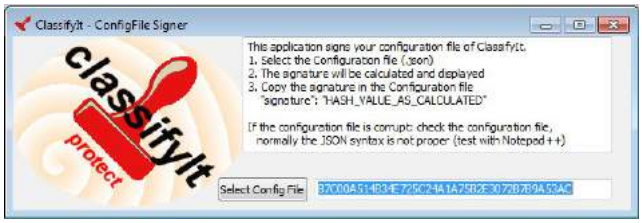


Abbildung 12-7: ConfigFile Signer; Quelle: ugarbe.de Software

Ein Registry-Key in den Clients – der zentral über das Microsoft Active Directory gesetzt werden kann – zeigt hier auf die neue Konfigurationsdatei, die ClassifyIt zukünftig verwenden soll. Somit haben alle Nutzer bei ihrer Arbeit stets denselben Versions- und Konfigurationsstand, was Kompatibilitätsproblemen vorbeugt.

Klassifiziert der Nutzer eine E-Mail, kann ClassifyIt diese Einstufung zudem in die X-Header der Netzwerkpakete schreiben, die nachfolgend von der Firewall oder vom E-Mail-Gateway ausgewertet werden können. So ist z. B. eine Organisationsrichtlinie umsetzbar, dass als „GEHEIM" eingestufte Informationen die Organisation nicht per E-Mail verlassen dürfen. Der Nutzer wird – wenn er eine als „GEHEIM" klassifizierte E-Mail versendet – entsprechend informiert.

Neben dieser erweiterten Überprüfung mittels X-Header-Informationen bietet ClassifyIt die Option, Properties in Office-, Excel- und PowerPoint-Dateien mit individuellen Attributen entsprechend dem Klassifikationsschema zu setzen. Diese Attribute können von Applikationsfirewalls ausgewertet werden, um das Versenden von beispielsweise als „NICHT AUTORISIERT" markierten E-Mails an Außenstehende oder aber auch – entsprechend den internen Informationssicherheitsrichtlinien – an unbefugte Personen zu verhindern.

12.3.6 Vorgehen und Umsetzung

Das Vorgehen der Implementierung dieser Lösung gestaltet sich in der Regel wie folgt: Der interessierte Kunde kann ClassifyIt in einer eingeschränkten Version kostenfrei beziehen und

intern testen. ugarbe.de software unterstützt bei Fragen rund um die Nutzung und Implementierung.

Sobald dieser Test abgeschlossen wurde und sich die Organisation für den Einsatz von ClassifyIt entschieden hat, erfolgt die Entscheidung, welches Lizenzmodell für die Organisation das richtige ist. ugarbe.de software bietet den einmaligen Kauf der Software sowie ein Subscription-Lizenzmodell an, das Software-Updates, neue Versionen und E-Mail-Support beinhaltet.

Im Anschluss erfolgt die individuelle Erstellung der Konfigurationsdateien mit den organisationsinternen Geheimhaltungsstufen, Richtlinien und ggf. Mapping mit anderen Organisationen. Dieser Prozess dauert ein bis wenige Tage – je nachdem, ob die Organisation bereits Richtlinien und Geheimhaltungsstufen definiert hat. Neben der Erstellung der Konfigurationsdateien müssen je nach Einsatzzweck von ClassifyIt Netzwerkkomponenten, wie Firewalls oder E-Mail-Gateways, mit einem erweiterten Regelwerk auf die Konfigurationsdatei abgestimmt werden.

Danach kann ClassifyIt über den bereits vorhandenen Softwareverteilungsprozess in der Organisation installiert werden. Dies schließt auch Änderungen der Konfiguration mit ein, wenn sich z. B. ein Mapping aufgrund einer Erweiterung ändern sollte.

Da geltende Vorschriften, Normen und Standards, wie z. B. die ISO 27001 oder der BSI-IT-Grundschutzkatalog, bereits Awareness in der Informationssicherheit vorsehen und vorgeben, kann der Umgang mit ClassifyIt leicht als Schulungsmaßnahme in Maßnahmen wie Workshops, Rundmails, Web-based Trainings integriert werden. An dieser Stelle stellt ugarbe.de software kostenlos Dokumentationen und Video-Tutorials zur Verfügung (siehe [6] und [7]). Eine spezielle Schulung für IT-Fachpersonal und Nutzer ist nicht vorgesehen – und ist entsprechend den Erfahrungen von urgarbe.de software nicht notwendig.

Darüber hinaus unterstützt ClassifyIt dabei, das vorhandene Wissen der Mitarbeiter über Informationssicherheit aufrechtzuhalten. Mittels optionaler Pop-ups kann ClassifyIt dem Nutzer bei Bedarf aufzeigen, was unter der jeweiligen Geheimhaltungsstufe zu verstehen ist, und kann hier zudem organisationsinterne Beispiele anführen, die Mitarbeitern die Einstufung von Informationen erleichtern.

„Policies müssen Tools machen und nicht umgekehrt". Dieses Motto verdeutlicht, dass die Einführung von ClassifyIt keine großen Prozessänderungen mit sich bringt. Bereits vorhandene Organisationsrichtlinien und Geheimhaltungsstufen werden in ClassifyIt portiert. ClassifyIt wird wiederum in Software integriert, die die Mitarbeiter tagtäglich für ihre Arbeit verwenden.

12.4 Erfolgsfaktoren

„Policies müssen Tools machen und nicht umgekehrt" (Ulrich Garbe)

So bietet ClassifyIt ein Höchstmaß an Flexibilität, das zudem mit einer hohen Nutzerfreundlichkeit einhergeht. Der Bedarf an hoher Nutzerfreundlichkeit von Software sieht ugarbe.de software sowohl bei den Endanwendern als auch bei den Administratoren, die die Installation

pflegen. Der Aufwand für die Einführung und Pflege der Software ist gering: Die Konfigurationsdateien sind einfach zu erstellen und zu verteilen und ClassifyIt lässt sich über die Standardsoftwareverteilung einer Organisation ausrollen. Zudem sind Umorganisationen oder Prozessänderungen nicht notwendig. Die Software fügt sich für die Endanwender nahtlos in die gewohnte Office-Landschaft ein.

Dies sind wesentliche Erfolgsfaktoren für den Einsatz von ClassifyIt. Von zentraler Bedeutung ist die Unterstützung durch das Management: „Das Management muss die Notwendigkeit für Informationssicherheit begreifen und mittragen und einfordern". Erst dann wird eine Organisation gute Richtlinien und gute Geheimhaltungsstufen entwickeln und Richtlinien und Geheimhaltungsstufen den Mitarbeitern vermitteln. Awareness für Fragen der Informationssicherheit bei Anwendern ist zentral für den erfolgreichen Einsatz von ClassifyIt: Die Software alleine kann die Denkprozesse des Endanwenders nicht übernehmen und Geheimhaltungsstufen bei der Erstellung von Dokumenten nicht erkennen. Der Schlüssel für den erfolgreichen Einsatz der Software ist, dass Informationssicherheit genau da erzeugt wird, wo sensible Inhalte erstellt werden. Ab der Klassifizierung von Dokumenten kann ClassifyIt die Informationssicherheit in den Arbeitsprozessen unterstützen.

12.5 Danksagung

Wir danken dem Bundesministerium für Bildung und Forschung (BMBF) für die Möglichkeit der Forschung im Rahmen des Projektes VeSiKi, Förderkennzeichen 16KIS0213K.

12.6 Literaturverzeichnis

[1] Garbe, R. U., ugarbe.de integrierte Softwarelösungen: ClassifyIt. ugarbe.de software, Koblenz, S. 5.

[2] BSI, 2014. IT-Grundschutz: G 3.44 Sorglosigkeit im Umgang mit Informationen, Bundesamt für Sicherheit in der Informationstechnik, 2014. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g03/g03044.html [zugegriffen: 29-Juni-2017].

[3] BSI, 2009. IT-Grundschutz: G 3.13 Weitergabe falscher oder interner Informationen, Bundesamt für Sicherheit in der Informationstechnik. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g03/g03013.html [zugegriffen: 29-Juni-2017].

[4] BSI, 2009. IT-Grundschutz: G 3.8 Fehlerhafte Nutzung von IT-Systemen, Bundesamt für Sicherheit in der Informationstechnik. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g03/g03008.html [zugegriffen: 29-Juni-2017].

[5] BSI, 2009. IT-Grundschutz: G 3.1 Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten, Bundesamt für Sicherheit in der Informationstechnik. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g03/g03001.html [zugegriffen: 29-Juni-2017].

[6] Garbe, R. U. Documentation. Verfügbar unter: http://ugarbe.de/index.php/classifyit-web-page/classifyit-demo.html [zugegriffen: 05-Juli-2017].

[7] Garbe, R. U. ClassifyIT – Multimedia Demonstration. Verfügbar unter: http://ugarbe.de/index.php/classifyit-web-page/classifyit-overview-2.html [zugegriffen: 05-Juli-2017].

Teil III – Implikationen für die Praxis

13 Erfolgreiche IT-Sicherheit konzipieren und umsetzen – Eine Cross-Case-Analyse

Thomas Diefenbach, Universität der Bundeswehr München
Sebastian Dännart, Universität der Bundeswehr München
Manfred Hofmeier, Universität der Bundeswehr München
Tim Reimers, Universität der Bundeswehr München
Andreas Rieb, Universität der Bundeswehr München
Ulrike Lechner, Universität der Bundeswehr München

Die Fallstudien decken unterschiedliche Kritische Infrastrukturen und unterschiedliche IT-Sicherheitsthemen ab und rücken dabei jeweils ein individuelles Beispiel eines IT-Sicherheitsprojekts bzw. -produkts in den Fokus der Betrachtung. Um Erkenntnisse und Lehren auch für zukünftige und losgelöste Projekte in hiervon verschiedenen Rahmenbedingungen gewinnen zu können, wurde über die Fallstudienserie eine übergreifende Qualitative Inhaltsanalyse nach Mayring (2015) durchgeführt. Ziel dieser fallstudienübergreifenden Analyse (*Cross-Case-Analyse*) war es, trotz der unterschiedlichen Betrachtungsgegenstände Muster, Gemeinsamkeiten und auch prominente Unterschiede zu identifizieren, die Rückschlüsse auf allgemeingültige Zusammenhänge erlauben und somit die für einen positiven Projektverlauf relevanten Rahmenumstände und bewährte Vorgehensarten sichtbar machen.

Dieses Kapitel ist so aufgebaut, dass in den nächsten beiden Unterkapiteln zunächst das methodische Vorgehen und die gewählten Codes für die Inhaltsanalyse dargestellt werden, um in den anschließenden Unterkapiteln die jeweiligen Untersuchungsergebnisse vorzustellen.

13.1 Methodik

In diesem Kapitel wird die Methodik der Cross-Case-Analyse beschrieben, welche auf der Fallstudienserie durchgeführt wurde, mit dem Ziel, aus erkannten Mustern, Gemeinsamkeiten und Unterschieden allgemeingültige Rückschlüsse auf andere IT-Sicherheitsprojekte zu ziehen.

Als Methode wurde eine Cross-Case-Analyse deshalb gewählt, weil diese Herangehensweise es ermöglicht, analysierte Daten zu kategorisieren und den enthaltenen Aussagen dadurch mehr Aussagekraft zu geben (Yin 2003). Dazu wurden alle Fallstudien einer Qualitativen Inhaltsanalyse nach Mayring unterzogen (Mayring 2015), jedoch mit der Besonderheit, dass die zu verwendenden Codes im Vorfeld deduktiv hergeleitet und einheitlich definiert worden sind, sodass alle Fallstudien mit Fokus auf die gleichen Aspekte analysiert werden konnten.

Dazu bedurfte es im ersten Schritt der Entwicklung des zu nutzenden Codeschemas. Dies geschah im Zuge eines iterativen Verfahrens in drei Workshops. Teilnehmer der Workshops waren neben mehreren Autoren der Fallstudien auch weitere wissenschaftliche Mitarbeiter der gleichen Forschungsgruppe, die selbst nicht an der Erstellung der Fallstudien mitgewirkt hatten. Während im ersten Workshop neben der initialen Sammlung möglicher Codes die

bestehenden Informationsbedarfe des Forschungskontexts sowie mögliche Mehrwerte einer Cross-Case-Analyse diskutiert wurden und darüber ein einheitliches Verständnis geschaffen wurde, waren im zweiten und dritten Workshop die Erweiterung und Verfeinerung des Codeschemas selbst Schwerpunkte. Durch diesen iterativen Ansatz zweier Reviews der Codes – vom ersten auf den zweiten und vom zweiten auf den dritten Workshop – konnte ein Portfolio an Codes entwickelt werden, das auch in der Retrospektive den Anforderungen gerecht werden konnte. So ist es z. B. in den anschließenden Phasen trotz regelmäßiger Reflexion und Diskussion bisheriger Fortschritte zu keinem Zeitpunkt nötig gewesen, Anpassungen am Codeschema durchzuführen, da die Codes alle wesentlichen Aspekte einer Fallstudie aus Betrachtung der codierenden Mitarbeiter abdecken konnten.

In der zweiten Phase wurden die einzelnen Fallstudien jeweils zwei Mitarbeitern zugewiesen, die diese unabhängig voneinander mit dem entwickelten Codeschema analysierten und codierten. Dabei wurde sichergestellt, dass die für eine Fallstudie ausgewählten Mitarbeiter nicht im Erstellungsprozess dieser jeweiligen Fallstudie mitgewirkt hatten, weder in der Phase der Datenerhebung – z. B. bei den durchgeführten Interviews – noch in einer sich daran anschließenden Phase. Die beiden durch die codierenden Mitarbeiter einer Fallstudie extrahierten Textpassagen wurden miteinander verglichen und Unterschiede zwischen diesen beiden Mitarbeitern diskutiert und vereinheitlicht. Insgesamt konnte mit diesem Vorgehen die Wahrung der Intercoder-Reliabilität sehr gut unterstützt werden. Die codierten Textpassagen konnten folglich weiter analysiert werden.

Der wesentliche Teil der Cross-Case-Analyse fand nun 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. Mitarbeiter der Forschungsgruppe haben jeweils einen oder mehrere Codes zugewiesen bekommen und die dazu codierten Aussagen aus allen Fallstudien miteinander verglichen und auf Muster, Gemeinsamkeiten und Unterschiede hin analysiert. Anhand dieser vergleichenden Betrachtung konnten bereits erste unterteilende Kategorisierungen bei mehreren Codes vorgenommen worden, sofern die Ergebnisse dies nahelegten. An dieser Stelle fand auch der Vergleich mit wissenschaftlicher sowie grauer Literatur zum durch den Code betrachteten Aspekt statt. Sofern eine individuelle Literaturrecherche zum Codeinhalt entsprechende Forschungsergebnisse aufzeigte, konnten die zum jeweiligen Fokus gesammelten Erkenntnisse aus den Praxisbeispielen der Fallstudien mit den anderen Literaturquellen verglichen werden. Diese Vergleiche – sofern möglich – haben aufzeigen können, welche Faktoren in der IT-Sicherheit für den Erfolg von Maßnahmen in der Praxis relevant sind. Nach detaillierter Auswertung und Vergleich der Fallstudien- und Literaturinhalte konnten abschließend die sich ggf. aufzeigenden Indizien für zugrunde liegende Zusammenhänge extrahiert und aufbereitet werden.

Zunächst werden in den beiden folgenden Kapiteln die in der Cross-Case-Analyse betrachteten Fallstudien aufgeführt sowie das für die Untersuchung verwendete Codeschema beschrieben. Die Ergebnisse der einzelnen Codes werden in den darauffolgenden Kapiteln einzeln erörtert.

13.2 Betrachtete Fallstudien

Alle Fallstudien dieses Buchs konnten bei der Cross-Case-Analyse berücksichtigt werden.

Tabelle 4: Betrachtete Fallstudien

Titel der Fallstudie	Kurzbezeichnung
Bundeswehr: AG IT-SecAwBw – Wie eine Arbeitsgruppe IT-Security Awareness im In- und Ausland fördert	Bundeswehr AG Awareness
genua gmbh: Fernwartung Kritischer Infrastrukturen	genua Fernwartungslösung
itWatch GmbH: Ein sicherer Standardprozess für die digitale Tatortfotografiemit DeviceWatch	itWatch Digitale Tatortfotografie
Die Kliniken des Bezirks Oberbayern: Ausgewogenes Risikomanagement für nachhaltige Sicherheit	kbo Risikomanagement
IT-Sicherheit in der Molkerei: Familientradition und Hochverfügbarkeit	Molkerei Hochverfügbarkeit
IT-Sicherheit für Geschäftsprozesse im Finanzsektor: Die Managementlösung PREVENT	PREVENT Managementlösung
Informationssicherheit bei SAP SE: Die längste Human Firewall der Welt	SAP Human Firewall
Zentrale Leitstelle Ostthüringen: IT-Sicherheit in einer Leitstelle	Ostthüringen Leitstelle
Informationssicherheit durch ClassifyIt: Informationssicherheit durch gestützte Klassifizierung von Dokumenten und E-Mails	ugarbe.de software ClassifyIt

Zur Übersicht enthält Tabelle 4 alle Titel der betrachteten Fallstudien. Die zweite Spalte weist außerdem jeder Fallstudie je zwei eindeutige Kurzbezeichnungen zu, die zum einen den Partner der Fallstudie – also die betrachtete Organisation – und zum anderen die Maßnahme, Technologie oder das auszeichnende Paradigma der Fallstudie benennt und das in diesem Kapitel verwendet wird. Um die Lesbarkeit zu erleichtern, sind die Fallstudien in den folgenden Ergebniskapiteln mit diesen Kurzbezeichnungen referenziert.

13.3 Verwendete Codes

Das Vorgehen bei der Entwicklung der Codes für die Qualitative Inhaltsanalyse beinhaltet deduktives und induktives Vorgehen. Neben den dem Forschungsprojekt VeSiKi sowie den Verbundprojekten zugrunde liegenden Forschungsfragen waren für die Entwicklung der Codes auch die Erfahrungen aus der Erstellung der Fallstudien inspirierend.

Es wurden neun Codes festgelegt, die die beiden zentralen Themen *Zieldimension IT-Sicherheit* und *Kontext* der in den Fallstudien betrachteten Maßnahmen beleuchten. Während das erste Thema die Aspekte der IT-Sicherheitsmaßnahme im engeren Sinn im Fokus hat – und somit den inhärenten Stärken und Schwächen einer bestimmten Lösung gewidmet ist, werden im Themenbereich *Kontext* jene Faktoren in den Mittelpunkt gestellt, welche vor al-

lem für die Einführung einer bestimmten Maßnahme und deren Erfolg relevant sind, wie z. B. organisationale und projektbezogene Aspekte. Zwei Codes sind ferner noch in jeweils zwei detailliertere Abstufungen unterteilt worden. Tabelle 5 enthält eine Übersicht über die Codes.

Tabelle 5: Codes der Cross-Case-Analyse

Nr.	Thema	Code
1	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
7		Treiber und Auslöser
8		IT-Sicherheitsphilosophie
8.1		Vertrauensfokus in Technik – Organisation – Mensch
8.2		Organisationskultur
9		Adressierte Risiken

Das Thema *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 Nr. 1 bis 4 *Beurteilung und Messung von IT-Sicherheit*, *Erhöhung der IT-Sicherheit*, *Einfachheit der Maßnahme* und *Kosteneffizienz der Maßnahme* erfasst.

Darüber hinaus sind aber auch jene praktischen Aspekte einer Implementierung von IT-Sicherheitsmaßnahmen oder -konzepten in einer Organisation von Interesse, die im Thema *Kontext* zusammengefasst sind. Die Codes *Nebeneffekte*, *Erfolgsfaktoren für die Implementierung*, *Treiber und Auslöser*, *IT-Sicherheitsphilosophie* und *Adressierte Risiken* sollen deshalb einen Einblick in bzw. Sensibilisierung für jene Rahmenbedingungen innerhalb einer Organisation ermöglichen, die für eine erfolgreiche Umsetzung avisierter IT-Sicherheitslösungen in einer bereits vorhandenen Organisationsstruktur relevant sein können.

In Tabelle 6 sind die Codes noch einmal dargestellt und jeweils um eine Beschreibung ergänzt, um die jeweilige Verwendung in der Qualitativen Inhaltsanalyse zu erläutern. Die folgenden Kapitel enthalten nun die Ergebnisse der Cross-Case-Analyse mit je einem Kapitel pro Code.

Tabelle 6: Beschreibung der Codes

Nr.	Code	Beschreibung
1	Beurteilung und Messung von IT-Sicherheit	Für Aussagen verwendet, die die Messung oder Beurteilung von IT-Sicherheit durch die in der Fallstudie beschriebene Umsetzung betreffen.
2	Erhöhung der IT-Sicherheit	Für Aussagen verwendet, die beschreiben, in welcher Art die IT-Sicherheit durch den in der Fallstudie beschriebenen Ansatz erhöht wird.
3	Einfachheit der Maßnahme	Für Aussagen verwendet, die beschreiben, wie aufwändig die Implementierung oder Betrieb und Nutzung von IT-Sicherheitsmaßnahmen sind.
4	Kosteneffizienz der Maßnahme	Für Aussagen verwendet, die beschreiben, wie kostengünstig die Implementierung oder Betrieb und Nutzung von IT-Sicherheitsmaßnahmen sind.
5	Nebeneffekte	
5.1	Wechselwirkungen mit anderen IT-Sicherheitsmaßnahmen	Für Aussagen verwendet, die beschreiben, welche Wechselwirkungen mit anderen Komponenten oder Bereichen der IT-Sicherheit, wie etwa bereits etablierten IT-Sicherheitsmaßnahmen, bestehen.
5.2	Einflüsse auf andere Geschäftsprozesse	Für Aussagen verwendet, die beschreiben, welche Nebeneffekte oder Einflüsse die Maßnahmen auf Bereiche haben, die nicht IT-Sicherheit im Schwerpunkt behandeln.
6	Erfolgsfaktoren für die Implementierung	Für Aussagen verwendet, die beschreiben, welche Faktoren die Implementierung begünstigt haben oder Voraussetzung dafür waren.
7	Treiber und Auslöser	Für Aussagen verwendet, die beschreiben, was die treibende Kraft oder der Auslöser für die in der Fallstudie beschriebenen Maßnahmen war.
8	IT-Sicherheitsphilosophie	
8.1	Vertrauensfokus in Technik – Organisation – Mensch	Dieser Code wurde verwendet, wenn in der Fallstudie über die Balance zwischen dem Vertrauen in Menschen und der Kontrolle durch Technik geschrieben wird.
8.2	Organisationskultur	Für Aussagen zum Zusammenhang der IT-Sicherheit mit der Organisationskultur verwendet.
9	Adressierte Risiken	Dieser Code wurde bei Textpassagen zu Risiken, die durch die in der Fallstudie beschriebenen Maßnahmen adressiert wurden, verwendet.

13.4 Code 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 (BSI 2008a). Im Kontext der IT-Sicherheitskonzeption finden die Messungen sowie die Beurteilungen in den Phasen der Bedrohungs- und Risikoanalyse statt, deren Ergebnisse wiederum Grundlage für die Entwicklung entsprechender Maßnahmen zur Behandlung der identifizierten Risiken darstellen. Zudem sieht das National Institute of Standards and Technology (NIST) in (Chew u. a. 2008) weitere Vorteile: „*Such measures are used to facilitate decision making, improve performance, and increase accountability through the collection, analysis, and reporting of relevant performance-related data – providing a way to tie the implementation,*

efficiency, and effectiveness of information system and program security controls to an agency's success in achieving its mission."

In den Fallstudien werden Methoden der Praxis in *Bundeswehr*, *kbo*, *PREVENT*, *SAP* und *Ostthüringen* beschrieben. Es ist zu erkennen, dass sowohl qualitative als auch quantitative Daten erhoben werden. So nutzt *SAP* z. B. Fragebögen, um die Einschätzung der Mitarbeiter hinsichtlich ihrer Awareness zur Informationssicherheit zu erheben. In der *Leitstelle* unterstützte das Forschungsprojekt MoSaIK aus dem Forschungsschwerpunkt ITS|KRITIS. Auf Basis bereits vorhandener Unterlagen und Interviews mit den Mitarbeitern wurde eine Strukturanalyse durchgeführt, die eine aktuelle Übersicht über vorhandene Systemkomponenten, Architekturen und Prozesse der *Leitstelle* abbildet. Die anschließende Risikoanalyse sowie die Entwicklung von Worst-Case-Szenarien ermöglichten es, ein IT-Infrastrukturkonzept zu entwickeln, das sowohl mehrere Rückfallebenen als auch Redundanzen vorsieht.

Ähnlich wie die *Leitstelle* beziehen die *kbo* ebenfalls externe IT-Experten z. B. für Penetrationstests in die Überprüfung der Implementierung und Wirksamkeit von Maßnahmen mit ein und unterstützen hier die hausinternen IT-Experten. Ferner werden bei *kbo* zur Beurteilung und Messung der IT-Sicherheit Metriken, wie die Erkennungsrate von Malware, Anzahl an Incidents u. a., berücksichtigt. Diese Kombination aus verschiedenen Methoden zur Messung sowie die unterschiedlichen Fokusse stehen im Einklang mit der Empfehlung des NIST, Kennzahlen für die Implementierung, die Effektivität und Effizienz sowie den Impact von IT-Sicherheitsmaßnahmen zu entwickeln und zu messen (Chew u. a. 2008).

Die Ergebnisse solcher Messungen und Einschätzungen müssen im Anschluss entsprechend der adressierten Zielgruppe aufbereitet und verteilt 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 (BSI 2008c), „*um seinen Lenkungs- und Steuerungsaufgaben nachkommen zu können*" (BSI 2008a). Diesen Kreis adressieren auch die Maßnahme in den Fallstudien *Bundeswehr*, *kbo*, *PREVENT*, *SAP* und *Ostthüringen*.

Aus der Analyse der vorgestellten Fallstudien ist ersichtlich, dass das Messen des IT-Sicherheitsniveaus kein prominentes Thema ist und Maßnahmen meist ohne nachgelagerte Messungen implementiert werden (z. B. *Bundeswehr*). Organisationen wie *SAP* oder *kbo* nutzen hingegen vergleichsweise einfache Instrumente, wie z. B. Fragebögen, um das IT-Sicherheitsniveau festzustellen. Fallstudien wie *PREVENT* zeigen die Komplexität auf, wenn das Risikomanagement mit Datengewinnung und Datenanalyse im Risikomanagement in einem Unternehmen betrachtet wird.

13.5 Code 2: Erhöhung der IT-Sicherheit

Das BSI empfiehlt im Zuge eines ganzheitlichen Informationssicherheitsansatzes in den IT-Grundschutz-Katalogen sowohl präventive Maßnahmen als auch Maßnahmen zur Behebung von Sicherheitsvorfällen (BSI 2016a). Als Hilfestellung für Betreiber von KRITIS und Nicht-KRITIS ist der Standard 100-4 zu nennen, der das Notfallmanagement adressiert (BSI 2008d). Ebenso bietet das National Institute of Standards and Technology (NIST) mehrere Publika-

tionen zu diesem Thema, wie z. B. Bartock u. a. (2016) und NIST (2014) an, wobei letztere Publikation ein Framework zur Verbesserung der IT-Sicherheit in Kritischen Infrastrukturen ist. Dieses Framework unterteilt Maßnahmen zur Erhöhung der IT-Sicherheit in die Funktionsbereiche *Identify*, *Protect*, *Detect*, *Respond* und *Recover*, wie die Abbildung 13-1 illustriert.

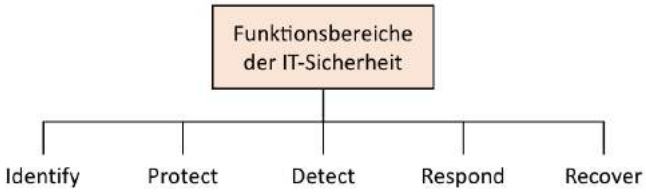


Abbildung 13-1: Funktionsbereiche der IT-Sicherheit gemäß NIST; Quelle: NIST 2014

Die Analyse der Fallstudien macht ersichtlich, dass die beschriebenen Maßnahmen primär präventive Maßnahmen des Funktionsbereichs *Protect* sind, in Teilen aber auch Maßnahmen des Notfallmanagements (*Respond* und *Recover*) berücksichtigen. Exemplarisch ist hier die Fallstudie *Molkerei* 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. So auch in der Fallstudie *Ostthüringen*, in der der Prozess der Notfallannahme und Alarmierung der Rettungskette über mehrere Rückfallebenen durch Redundanzen abgesichert wird. Diese Rückfallebenen sind in der *Leitstelle* einerseits mittels technischer Redundanzen, andererseits auch mithilfe organisatorischer Prozesse realisiert, die im Notfall vollkommen ohne IT-Unterstützung auskommen.

Im Rahmen eines ganzheitlichen Ansatzes zur Gewährleistung einer sicheren IT-Infrastruktur ist dieses Zusammenspiel unterschiedlicher Maßnahmen besonders wichtig. Das BSI schreibt in BSI (2008b) von organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsmaßnahmen. Die Fallstudien thematisieren mehrere dieser Sicherheitsmaßnahmen.

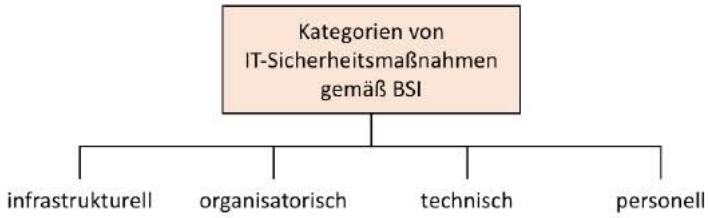


Abbildung 13-2: Kategorien von IT-Sicherheitsmaßnahmen; Quelle: nach BSI 2008b

So beschreiben die Fallstudien *SAP* und *Bundeswehr* Maßnahmen, die den personellen Faktor in Form der IT-Security-Awareness adressieren. Maßnahmen wie die o. a. Redundanz (*Molkerei*, *Ostthüringen*) oder die Schaffung eines Gremiums zur Bewertung der IT-Bedrohungslage

(*kbo*) enthalten mehr organisatorische Aspekte, können aber durch personelle und technische Maßnahmen unterstützt werden.

Darüber hinaus beschreiben die Fallstudien *genua*, *itWatch* und *ugarbe.de software* primär technische Maßnahmen, wie eine Software zur Datenklassifikation, eine *Fernwartungslösung* oder eine Software zur Absicherung des Standardprozesses für die *digitale Tatortfotografie*. An dieser Stelle ist jedoch zu beachten, dass diese Maßnahmen nicht zwangsläufig autark implementiert wurden und betrieben werden, sondern von unterstützenden anderen Maßnahmen abhängig sind (siehe Code 5.1 *Wechselwirkungen mit anderen IT-Sicherheitsmaßnahmen* und Code 5.2 *Einflüsse auf andere Geschäftsprozesse*).

Neben der Unterscheidung der adressierten Funktionsbereiche und Kategorien gemäß BSI können IT-Sicherheitsmaßnahmen unterschiedlich auf IT-Risiken wirken und Organisationen stehen nach BSI-Standard 100-3 (BSI 2008c) verschiedene Möglichkeiten offen, mit den identifizierten Risiken umzugehen:

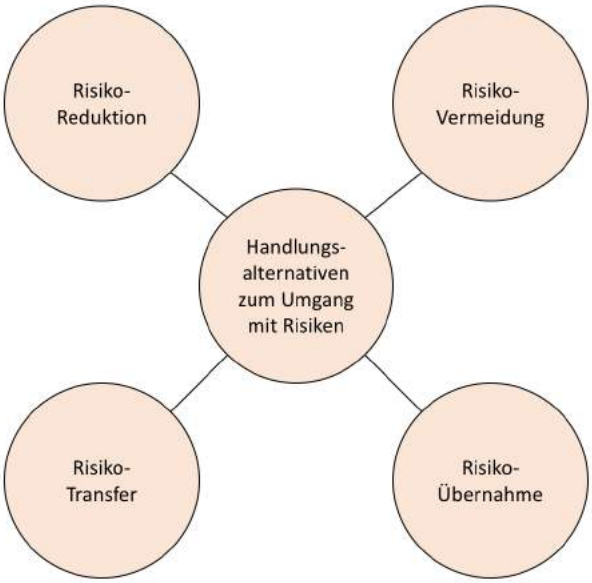


Abbildung 13-3: Handlungsalternativen zum Umgang mit Risiken; Quelle: BSI 2008c

- Risiko-Reduktion: Ergänzende Schutzmaßnahmen wirken den Risiken entsprechend entgegen.
- Risiko-Vermeidung: Durch eine Umstrukturierung von Geschäftsprozessen oder des Informationsverbunds werden bestimmte Risiken fortan vermieden.
- Risiko-Transfer: Durch Abschluss von Versicherungsverträgen oder Outsourcing wird das Risiko auf eine andere Institution übertragen.
- Risiko-Übernahme: Das verbleibende Risiko wird akzeptiert, weil z. B. der Aufwand und die Kosten für wirksame Gegenmaßnahmen den zu schützenden Wert übersteigen würden.

Die Analyse der Fallstudien hat ergeben, dass die IT-Sicherheitsmaßnahmen unterschiedliche Möglichkeiten im Umgang mit Risiken adressieren. Während die Software von *ugarbe.de software* eher eine ergänzende Schutzmaßnahme darstellt, ist die Nutzung von Thin Clients (*Molkerei*, *Ostthüringen*) eher in der Risiko-Vermeidung zu verorten.

Ein weiterer Punkt, der in der Analyse festgestellt wurde, ist der unterschiedliche Adressatenkreis durch die IT-Sicherheitsmaßnahmen in den Fallstudien. In Summe adressieren die Maßnahmen in den Fallstudien alle Mitarbeiter, ausgewählte IT-Nutzer, IT-Fachpersonal, die Managementebene oder externe Firmen, wie z. B. Zulieferer, Hersteller oder Partner. Die Fallstudien zeigen somit ein ganzheitliches Bild von Maßnahmen, die nicht nur verschiedene Zielgruppen adressieren, sondern auch IT-Sicherheit auf unterschiedlichen Ebenen abbilden (organisatorisch, personell, infrastrukturell und technisch).

Dem Stichwort der Verfügbarkeit kommt gerade im Kontext Kritischer Infrastrukturen besondere Bedeutung zu. Denn bei den ausgewählten Fallstudien liegt der Fokus nicht einzig und allein auf präventiven Maßnahmen, sondern auch auf Resilienz, um geschäftskritische Funktionen im Falle eines Cyberangriffs schnellstmöglich wieder „zum Laufen zu bekommen".

Die Perspektiven (Kategorien und Funktionsbereiche, vgl. Abbildung 13-1 und Abbildung 13-2) können Anreize schaffen, um z. B. bereits etablierte IT-Sicherheitsmaßnahmen unter neuen Perspektiven zu betrachten. In den Fallstudien SAP und Bundeswehr werden die Awareness-Maßnahmen primär für die Phase Protection eingesetzt, könnten jedoch prinzipiell auch auf die Phasen Respond und Recover übertragen werden, um z. B. IT-Fachpersonal auf den Schadensfall vorzubereiten.

13.6 Code 3: Einfachheit der Maßnahme

Mit dem Code *Einfachheit der Maßnahme* wurden in den Fallstudien jene Textstellen codiert, die konkrete Aussagen zur Komplexität und dem im Zuge der Einführung eingesetzten bzw. im zukünftigen Betrieb zu erwartenden Aufwand der neuen IT-Sicherheitsmaßnahme beinhalten, sowie aber auch jene Abschnitte, die das Thema der Einfachheit der behandelten Maßnahme zum Inhalt haben. Aus dieser Menge an Aussagen ließ sich ein Spektrum mehrerer Auslegungen des Begriffs der Einfachheit sowie seiner Bedeutung in der Praxis erkennen.

Lösungen und Maßnahmen zur Erhöhung der IT-Sicherheit in Organisationen und speziell in KMU sollen einfach sein. Das fordert bereits die Ausschreibung des Förderschwerpunkts. Die Analyse zu „Einfachheit der Maßnahme" konkretisiert, was eine *einfache* IT-Sicherheitsmaßnahme in der Praxis für Organisationen und KMU tatsächlich bedeutet bzw. im Ergebnis ausmacht.

Die Analyse der Fallstudien hat gezeigt, dass sich eine Einteilung in Kategorien als eine Möglichkeit genau für diese Fragestellung anbietet. So waren in den Fallstudien jeweils mehrere Erwähnungen bzgl. der *Einfachheit der Maßnahme* voneinander zu unterscheiden und den drei Bereichen *Nutzerfreundlichkeit*, *Implementierungsaufwand* sowie dem für die Maßnahme erforderlichen *Schulungsaufwand* – bei der Einführung und im laufenden Betrieb – zuzuordnen (siehe Abbildung 13-4). Vor weiterer Ausführung dieser drei Bereiche und der

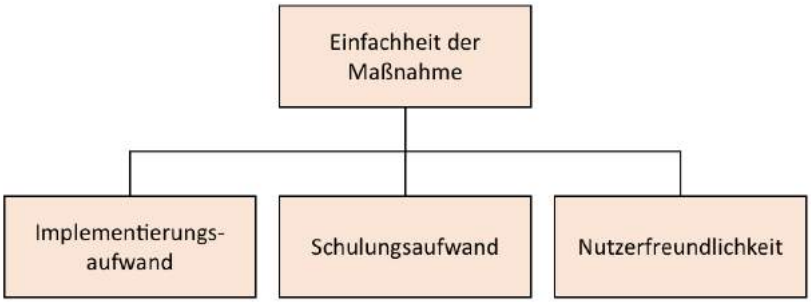


Abbildung 13-4: Kategorien des Codes *Einfachheit der Maßnahme*

jeweilig interessanten Aspekte empfiehlt es sich, zunächst kurz darauf einzugehen, was es bei der Interpretation der zum Begriff der Einfachheit codierten Textstellen zu berücksichtigen galt.

Im Fokus dieses Codes waren die unterschiedlichen Wahrnehmungen und Interpretationen zur *Einfachheit der Maßnahme*. Alle Aussagen zum Thema dieses Kapitels – insbesondere zu den konkret in den Fallstudien betrachteten Maßnahmen, Konzepten und Produkten – spiegeln individuelle und somit subjektive Einschätzungen von Fallstudienautoren und Gesprächspartnern zum Begriff der Einfachheit – bzw. darüber, wie einfach eine eingesetzte Lösung tatsächlich ist – wider. Dies bedeutet deshalb ebenfalls, dass alle Aussagen eine *wahrgenommene* Einfachheit beschreiben. Gleichermaßen wurden aber auch Textstellen ohne explizit hervorhebende Aussagen zur *Einfachheit der Maßnahme* codiert, wenn die zugrunde liegende Beschreibung der Komplexität dies zugelassen hat; gerade bei Fragestellungen der Implementierung ist es selbst für Außenstehende abzuschätzen, ob z. B. eine Awareness-Maßnahme oder eine technische Veränderung der IT-Infrastruktur an mehreren Orten im Zweifel einfacher oder aufwändiger ist. Im Vergleich aller codierten Textpassagen hat sich schließlich die Struktur mit den drei bereits zuvor genannten Kategorien als sinnvoll angeboten, welche nun im Detail erörtert wird.

Als womöglich intuitivste Form der Begriffsauffassung könnte man bei einer *einfachen IT-Sicherheitsmaßnahme* tatsächlich auf den notwendigen *Implementierungsaufwand* der Einführung selbst schließen. Dies war auch bei vier der betrachteten Fallstudien und somit in knapp der Hälfte der Fälle gegeben. Die als einfach beschriebenen Maßnahmen im Zuge der Implementierung reichten hierbei von den Vorzügen einer reibungsarmen Integration in bereits bestehende Systemlandschaften – sowohl bei Hardware als auch Software (*ugarbe.de software*, *PREVENT*, *genua*) – bis hin zum Aufbau der IT-Sicherheitsmaßnahmen im engeren Sinne – also Projekten, bei denen die inhärenten Herausforderungen der Umsetzung und die damit verbundene Risikobehaftung als gering und deshalb *einfacher* als z. B. kompliziertere IT-Infrastrukturprojekte einzustufen sind (*SAP*).

Als weitere Ausprägung der *Einfachheit* hat sich *Nutzerfreundlichkeit* in den Fallstudien herauskristallisiert. In der Fallstudie zu *ugarbe.de software* erfolgte die Einbindung der Softwarelösung in das in Nutzung befindliche Office-Paket, sodass die Veränderungen für den Anwender – trotz der verpflichteten Nutzung des neuen Softwaremoduls – gering gehalten

und Hürden einer ungewohnten Umgebung vermieden werden konnten. Die Lösung der *digitalen Tatortfotografie* bedeutete dagegen zwar einen gänzlich neuen Prozess der Verarbeitung dieser Beweismittel, jedoch ist dieser für alle Nutzergruppen deutlich komfortabler als der zuvor etablierte analoge Prozess, sodass auch in diesem Beispiel die Akzeptanz der Nutzer unterstützt wurde.

Über diese beiden Kategorien hinaus enthielten zwei Fallstudien außerdem Angaben zum erforderlichen *Schulungsaufwand* im Zuge der neu eingeführten Maßnahmen. Bei der *Fernwartungslösung* ist z. B. eine zweieinhalbtägige Schulung für die Administratoren bzw. eine deutlich kürzere Einweisung für die Nutzer vorgesehen. In diesem Beispiel erscheint die mehrtägige Schulung auf den ersten Blick ggf. etwas aufwändig, jedoch liegt im Vergleich zu den zeitlichen Ersparnissen, die im operativen Betrieb entstehen, die Vermutung nahe, dass auch diese Rahmenbedingungen der Maßnahme keinen Aufwand über Gebühr bedingt haben.

Durch die Analysen der positiven Beispiele in den Fallstudien ist somit gut sichtbar geworden, dass Anbieter technischer Lösungen bei der Entwicklung sowie Organisationen bei der Einführung neuer IT-Sicherheitsmaßnahmen die Veränderungen im laufenden Betrieb frühzeitig in die Planung mit einbeziehen. Gerade IT-Sicherheitsmaßnahmen bedürfen für den effektiven Einsatz der Akzeptanz der betroffenen Anwender und des administrierenden IT-Fachpersonals, da sonst die Möglichkeit der Nichtbeachtung bzw. des Umgehens der Maßnahme die beabsichtigte Wirkung gefährden kann. Neben der Akzeptanz – die durch eine erhöhte Nutzerfreundlichkeit gefördert werden kann – werden außerdem Aufwände für Nutzer- und Administrationsschulungen berücksichtigt, um auch zeitliche Mehrbelastungen bei der Entscheidung für eine Lösung einbeziehen zu können. Darüber hinaus ist zu erkennen, dass die Integration von neuen IT-Sicherheitsmaßnahmen in bestehende Prozesse – welche weder eine organisationale Anpassung von Geschäftsprozessen noch besondere Maßnahmen von Anwendern erforderten – besonders reibungsarm eingeführt werden konnten (*ugarbe.de software*, *genua*, *SAP*, *it Watch*). Auch eine Implementierung in bestehende technische Anlagen und die Einbindung in vorhandene Software sowie leichte und transparente Konfiguration wurden als Merkmale der Einfachheit erwähnt, was die Planung in bestehende Strukturen erstrebenswert erscheinen lässt.

Die Fallstudien und die Ergebnisse der Analyse des Codes *Einfachheit der Maßnahme* zeigen auf, wie vielfältig die Interpretationen des Begriffs bzw. das tatsächliche Bedürfnis nach *einfachen* Lösungen sein können. Die untersuchten Praxisbeispiele haben meist mehrere der drei aufgezeigten Kategorien – *Implementierungsaufwand*, *Schulungsaufwand* und *Nutzerfreundlichkeit* – in ihrem individuellen Umfeld ausfüllen können; gleichermaßen können diese aber nur den jeweiligen Anwendungsfall im spezifischen Organisationskontext repräsentieren und eine Übertragung der Ergebnisse ist ggf. nicht ohne Weiteres möglich. Aus Sicht der Autoren sind die Erfahrungen aus den Fallstudien jedoch gute Beispiele, um das eigene Umfeld zu reflektieren und Hemmschwellen für neue technische oder organisationale Maßnahmen bewerten zu können. Auch Anbieter technischer Produkte können Inspiration dazu erhalten, welche Aspekte einer Sicherheitslösung den vielfältigen Kundenbedürfnissen am ehesten entsprechen und welchen in Entscheidungsfindungen der Organisationen somit auch

höhere Relevanzen beigemessen werden können, da bei der *Einfachheit* einer Maßnahme augenscheinlich nicht nur *Bequemlichkeiten* adressiert werden, sondern bei ungünstigen Bedingungen auch der *Erfolg* eines Projekts gefährdet sein kann.

13.7 Code 4: Kosteneffizienz der Maßnahme

Wie in jeder unternehmerischen Entscheidung spielen ebenso bei IT-Sicherheitsmaßnahmen finanzielle, personelle und zeitliche Ressourcen eine Rolle (Zetter 2015). Ein generelles Problem bei der Bestimmung der Kosteneffizienz bzw. Wirtschaftlichkeit von IT-Sicherheitsmaßnahmen besteht darin, dass eine erfolgreiche Maßnahme meist nur zur Verringerung eines Risikos beträgt und damit nur ein indirektes Ergebnis erzielt (Grob u. a. 2008; Cavusoglu u. a. 2004). Zusätzlich zu dem Verringern eines Risikos nennt Stöwer (2011) als mögliche weitere Effekte einer IT-Sicherheitsmaßnahme die Steigerung der Effizienz von Prozessen und Chancen durch neue Geschäftsmodelle. Dabei können für IT-Sicherheitsmaßnahmen dieser Art Standardverfahren der Investitionsrechnung verwendet werden, wie z. B. die Interne Zinssatzmethode oder die Amortisationsdauer (vertiefend: Faisst u. a. 2007).

Währenddessen ist die betriebswirtschaftliche Rechtfertigung des Verringerns eines Risikos mit Herausforderungen verbunden. Diese besteht in der Quantifizierung der Wahrscheinlichkeit des Eintretens sowie in der Quantifizierung der verursachten Kosten des möglichen Schadens (siehe Code 1 *Beurteilung und Messung von IT-Sicherheit*). Dabei ist neben dem Bestimmen der zu erwartenden Kosten die Berechnung des Nutzens einer IT-Sicherheitsmaßnahme eine weitere Herausforderung. Eine oft genutzte Kenngröße, welche diese drei Werte verwendet, ist der vom Return-on-Investment (RoI) abgeleitete Return-on-Security-Investment (RoSI). Dieser setzt die zu erwartenden jährlichen Schäden (ALE – Annual Loss Expectancy) mit dem zu erwartenden Nutzen des Investments in Beziehung zu den Kosten (meist nach dem Prinzip TCO – Total Cost of Ownership) (Sonnenreich u. a. 2006).

Neben der Möglichkeit, die zu erwartenden Kosten mittels Experteninterviews, Szenarioanalysen oder ähnlichen zu schätzen, können Tools wie das von Chehrazi u. a. (2015) entwickelte QUANTSEC oder Monte-Carlo-Simulationen (Kronschnabl 2010) verwendet werden. Umfassende Betrachtungen der Bestimmung der Wirtschaftlichkeit von IT-Sicherheitsinvestitionen bieten das WiBe-Verfahren (Wirtschaftlichkeitsbetrachtung) der Bundesverwaltung und das VOFI-Modell (Vollständige Finanzplanung) von Grob u. a. (2008).

Das WiBe-Verfahren legt den Fokus auf allgemeine IT-Investitionen, jedoch kann es auch für Maßnahmen in der IT-Sicherheit angewendet werden (Stöwer 2011). Bisher genannte Ansätze betrachten jedoch nicht dynamische Entwicklungen in der IT-Sicherheit. Lösungen hierfür bietet zum Beispiel Cavusoglu u. a. (2008) mit einem aus der Spieltheorie abgeleiteten Modell. Es werden dabei ein sequenzieller und simultaner Spielverlauf mit einem klassischen Decision-Theory-Ansatz verglichen. Eine weitere dynamische Methode schlagen Faisst u. a. (2007) vor. Dabei werden über mehrere Zeitperioden die optimalen Investitionszeitpunkte berechnet. Dies wird mit einer um die Berücksichtigung der ökonomischen Eigenkapitalunterlegung für unerwartete Schäden angereicherten klassischen Kapitalwertwertmethode erreicht.

Dabei setzen viele Methoden voraus, dass die zu erwartenden Schäden quantifizierbar sind und die Organisationen einen Trade-off zwischen Kosten und IT-Sicherheit eingehen können (Cavusoglu u. a. 2004), teilweise sogar, dass diese einen bestimmten hohen Schadenswert nicht übersteigen (Gordon & Loeb 2002). Da der Schadensfall in Kritischen Infrastrukturen durchaus direkt oder indirekt Menschenleben betreffen und damit einen nicht quantifizierbaren bzw. hohen Schaden hervorrufen kann mit gleichzeitiger unsicherer bzw. geringer Eintrittswahrscheinlichkeit, sind die Modelle nur bedingt anwendbar. In jedem Fall ist eine passende Auswahl des Instruments immer kontextabhängig und sollte individuell bestimmt werden.

Die Kosteneffizienz wird in den Fallstudien meist nur indirekt thematisiert. Dennoch bietet die Fallstudie zum Standardprozess in der *digitalen Tatortfotografie* ein gutes Beispiel für zusätzliche Chancen für IT-Sicherheitsinvestitionen nach Stöwer (2011). Dabei werden mit der Einführung einer IT-Sicherheitsmaßnahme direkte monetäre Einsparungen erreicht.

Typischer ist eine schwierige Bezifferung der Einsparungen, wie im Beispiel der Fallstudie *genua*, in der eine gut realisierte Fernwartung Kosten reduziert und für sich allein genommen eine betriebswirtschaftlich sinnvolle Maßnahme darstellt. Jedoch sollten bei der Umsetzung einer Remote-Access-Lösung immer die IT-Sicherheitsaspekte und deren Kosten bedacht werden.

Eine Möglichkeit, Kosten bei einer IT-Investition zu senken, ist die Reduktion des Schulungsaufwands für die zukünftigen Nutzer oder Administratoren, wie dies bei *ugarbe.de software* vorgesehen ist; dabei wird ein höherer Nutzen durch ein kostengünstigeres Produkt erreicht. In der Fallstudie *Bundeswehr* werden die Kosten nicht auf das Projekt berechnet, sondern auf andere Organisationseinheiten umverteilt, aus welchen die Mitarbeiter für das Projekt ausgeliehen werden. Es gibt jedoch auch Beispiele bei denen die Kosten für Mitarbeiter direkt einem Projekt zugeordnet werden können (*SAP*). Dabei war es für den Erfolg der *Human Firewall* bei *SAP* essenziell, dass über einen Zeitraum von mehreren Jahren die Mitarbeiter finanziert wurden.

Dabei fällt auf, dass in den untersuchten Beispielen wenig Augenmerk auf das Verhältnis zwischen Kosten und Nutzen sowie dem zu erwartenden Schaden gelegt wird. Das lässt sich dadurch begründen, dass in den Fallstudien neben IT-Sicherheitsprojekten auch konkrete IT-Sicherheitsprodukte und -unternehmen untersucht wurden und der Aspekt der Wirtschaftlichkeit dabei nur am Rande untersucht wurde.

Jedoch hat sich aus den Fallstudien gezeigt, dass durch effektive Maßnahmen eine Verringerung der Kosten einer IT-Sicherheitsinvestition möglich sind. Zum Beispiel sind Synergieeffekte zwischen Optimierung vorhandener Prozesse und gleichzeitiger Erhöhung der Sicherheit möglich und tragen zu einer wirtschaftlichen Lösung bei. Gleichzeitig gibt es auch Maßnahmen, z. B. die Einführung von Fernwartungszugängen, bei denen die IT-Sicherheit Kosten verursacht, aber in der Gesamtbetrachtung eine Einsparung, z. B. von Personal- oder Reisekosten, bedeutet. Eine zusätzliche Möglichkeit, Kosten zu senken, ist die Verringerung von Schulungsaufwand bei der Einführung und Administration von IT-Sicherheitssoftware. Es zeigt sich aber auch, dass eine über den geplanten Projektzeitraum garantierte Finanzierung den Erfolg eines Projektes maßgeblich unterstützen kann.

13.8 Code 5: Nebeneffekte

13.8.1 Code 5.1: Wechselwirkungen mit anderen IT-Sicherheitsmaßnahmen

Das BSI empfiehlt in der Vorgehensweise gemäß IT-Grundschutz die Anwendung von organisatorischen, infrastrukturellen, personellen und technischen Sicherheitsmaßnahmen (BSI 2008b). Dabei kann es Wechselwirkungen der IT-Sicherheitsmaßnahmen mit anderen IT-Sicherheitsmaßnahmen geben.

In der Fallstudie *ugarbe.de software* kann die Software *ClassifyIt*, die vorrangig als Microsoft-Office-Plug-in Anwender bei der Klassifikation von Dokumenten unterstützt, zudem die IT-Sicherheit auf Netzwerkebene verbessern. Durch die Berücksichtigung zusätzlicher Paket-Header klassifizierter Inhalte bei der Untersuchung von Netzwerkpaketen an der Firewall kann z. B. festgelegt werden, welche Dokumente in Abhängigkeit von der Klassifikationsstufe die Organisationsgrenzen verlassen dürfen. Es können also Synergieeffekte zweier unterschiedlicher technischer IT-Sicherheitsmaßnahmen genutzt werden.

Ferner bietet die IT-Sicherheitssoftware *ClassifyIt* die Möglichkeit, Nutzer durch entsprechende Popups zu unterstützen. Diese können z. B. die Klassifikationsstufen noch einmal erläutern und organisationsspezifische Beispiele geben. Der Vorteil an dieser Stelle ist, dass Botschaften der IT-Security-Awareness und geltende IT-Sicherheitsrichtlinien noch einmal aufgegriffen werden und dem Nutzer dann eine Hilfestellung geben, wenn er diese benötigt. In diesem Beispiel kann eine Synergie zwischen der technischen Implementierung einer Software und organisatorischen und personellen Maßnahmen der IT-Security-Awareness kombiniert werden. So auch in der Fallstudie *Bundeswehr*. Hier werden Inhalte der IT-Security-Awareness-Kampagne neben dem primären Zweck der Sensibilisierung an den Standorten der Bundeswehr zudem genutzt, um in Aus- und Weiterbildungen einerseits die Kampagne als solche zu bewerben, andererseits, um die Werkzeuge angehenden oder aktiven IT-Sicherheitsfachkräften und Führungskräften vorzustellen.

Neben diesen optionalen Abhängigkeiten können IT-Sicherheitsmaßnahmen aber auch zwangsläufig voneinander abhängen und bedürfen ggf. einer korrekten Implementierung auf anderer Ebene. So setzt z. B. *ClassifyIt* auf einem System von Einstufungen wie „VS VERTRAULICH“ oder „STRENG GEHEIM“ auf – diese Klassifikationsstufen müssen im Kontext der Sicherheitsrichtlinien einer Organisation bereits existieren. Hier ist *ClassifyIt* von anderen IT-Sicherheitsmaßnahmen abhängig.

Die *Fernwartungslösung* von *genua* ist ein weiteres Beispiel für eine IT-Sicherheitsmaßnahme, die von anderen IT-Sicherheitsmaßnahmen abhängig ist. Die Abhängigkeit besteht hier in Form von notwendigen weiteren Maßnahmen auf organisatorischer und personeller Ebene: „*Aus organisatorischer Sicht müssen Aufgabengebiete und Verantwortlichkeiten neu strukturiert werden. Dies ist beispielsweise der Fall, wenn es separate, autarke IT- und IT-Sicherheitsabteilungen gibt und die bspw. bei einer Anbindung des Produktionsnetzwerks an das Office-IT-Netzwerk zur Nutzung des Internetzugangs des Office-IT-Netzwerks Rechte für den Zugriff auf die Firewall am Netzwerkübergang neu regeln und untereinander abstimmen müssen*“ (*genua*).

Aus den Fallstudien geht hervor, dass IT-Sicherheitsmaßnahmen auf technischer, personeller, infrastruktureller oder organisatorischer Ebene von anderen IT-Sicherheitsmaßnahmen

auf gleicher – oder auch auf anderer – Ebene abhängig sind bzw. sein können. Ferner können IT-Sicherheitsmaßnahmen auf optionaler Basis mit anderen IT-Sicherheitsmaßnahmen kombiniert werden, um Synergieeffekte zu nutzen.

An dieser Stelle empfehlen die Autoren Betreibern und Verantwortlichen für IT-Infrastrukturen eine kritische Betrachtung vorhandener IT-Sicherheitsmaßnahmen auf notwendige und optionale Abhängigkeiten, um die IT-Sicherheit maßgeblich zu verbessern. Diese Empfehlung hat über die IT-Sicherheit zudem den Vorteil, dass Recovery-Prozesse im Falle eines Incidents zielgerichteter durchgeführt werden können und IT-Infrastrukturen resilienter werden. Denn so sieht z. B. das NIST im *Guide for Cybersecurity Event Recovery* (Bartock u. a. 2016) das Verständnis von Zusammenhängen, indirekten und direkten Beziehungen als Notwendigkeit, um einerseits Notfallmanagement effektiv planen und andererseits auch im Falle eines Incidents effektiv umsetzen zu können. Das Wissen über Zusammenhänge „*can help the organization's risk management team prioritize the implementation of adequate security protection mechanism, the incident response team react efficiently during a cyber event and identify the root cause when possible, and the recovery team return the business capabilities in a prioritized and orderly manner*".

Das Verständnis der Zusammenhänge ist gemäß NIST allerdings nicht nur auf IT-Sicherheitsmaßnahmen limitiert, sondern umfasst auch wertschöpfende, organisatorische Prozesse fernab der IT-Sicherheit und umfasst z. B. auch „*applicable regulatory, legal, environmental, and operational requirements*" (Bartock u. a. 2016).

13.8.2 Code 5.2: Einflüsse auf andere Geschäftsprozesse

Das BSI beschreibt die Rolle des IT-Sicherheitsmanagements wie folgt: „Die Schaffung von Informationssicherheit ist kein Selbstzweck. Aktuelle und zuverlässige Informationen sind die Grundlage der meisten Geschäftsprozesse. Informations- und Kommunikationstechnik soll die Ziele einer Institution sinnvoll unterstützen und dient zur Unterstützung von Geschäftsprozessen" (BSI 2008a). Code 5.2 ist diesem Thema gewidmet und soll in der Analyse verwendet werden, wenn beschrieben wird, welche Nebeneffekte oder Einflüsse die Maßnahmen auf Bereiche haben, die nicht im Schwerpunkt mit IT-Sicherheit zu tun haben.

Bei der Analyse der Fallstudien konnten verschiedene interne Geschäftsprozesse erhoben werden, die unmittelbar von den Maßnahmen der IT-Sicherheit beeinflusst werden. Dazu zählen in alphabetischer Reihenfolge Geschäftsprozesse in Beschaffung, Changemanagement, Dokumentenmanagement, Führungsinformationssysteme, Informationspolitik, IT-Support, Öffentlichkeitsarbeit, Personalverwaltung und -entwicklung, Wartung und Zahlungsverkehr. So ermöglicht z. B. die Einführung der IT-Sicherheitslösung in Fallstudie *itWatch* eine hohe Flexibilität bei der täglichen Polizeiarbeit. Denn die Änderung des Prozesses hin zur *digitalen Tatortfotografie* sowie die IT-sicherheitstechnische Absicherung erlaubt eine Verwendung jeglicher fototauglichen Geräte für die Polizeiarbeit. Damit werden nicht nur Kosten reduziert, sondern auch der Beschaffungsprozess vereinfacht.

Ein weiteres Beispiel stellt die *Bundeswehr* dar, bei der die IT-Security-Awareness-Kampagne verschiedene interne Prozesse beeinflusst. Über die Werkzeuge zur Sensibilisierung und

die Kampagnen in den einzelnen Dienststellen hinaus findet ein regelmäßiger Informationsaustausch im Themenfeld der IT-Sicherheit mit Dozenten verschiedener Aus- und Weiterbildungseinrichtungen der Bundeswehr statt. Zudem wurde IT-Security-Awareness fester Bestandteil in den Lehrplänen, wie z. B. im Lehrgang für IT-Sicherheitsbeauftragte der Bundeswehr und auch im Lehrgang für den Generalstabsdienst / Admiralstabsdienst national. Die Arbeitsgruppe sieht diese Synergie als sehr wichtig an, denn einerseits steigert diese Kooperation die Sichtbarkeit der Kampagne als solche sowie deren Werkzeuge, andererseits wird Führungskräften die Notwendigkeit der IT-Sicherheit für den Faktor Mensch über einen weiteren Kanal präsentiert. Und das wiederum steigert die Akzeptanz und die Unterstützung für die Umsetzung von IT-Security-Awareness in den Dienststellen. Aus Sicht des BSI steht dieses Vorgehen ganz im Einklang mit dem BSI-IT-Grundschutz, in dem Sensibilisierung des Managements sogar aktiv gefordert wird und mangelhafte Akzeptanz als wesentliche Bedrohung für erfolgreiche Sensibilisierung gesehen wird (BSI 2016b). „*Eine nachdrückliche und aktive Unterstützung durch die Behörden- bzw. Unternehmensleitung ist essentiell, damit Sicherheitskampagnen für die Mitarbeiter erfolgreich sein können*“ (BSI 2013a). Zudem wird im IT-Grundschutz darauf hingewiesen, dass das Management die Auswirkungen auf die Geschäftsprozesse erkennen muss (BSI 2013a).

Gemäß der Untersuchung der Fallstudien hören die Maßnahmen der IT-Sicherheit oder Informationssicherheit – genau wie Geschäftsprozesse – nicht an einer Organisationsgrenze auf. Auch die Schnittstellen von Geschäftsprozessen Dritter müssen mit betrachtet werden. Beispiele hierfür sind die technischen IT-Sicherheitslösungen der Fallstudien *genua* und *ugarbe.de software*. Die Software *ClassifyIt* zur Klassifikation von Daten erlaubt es, die Geheimhaltungsstufe einer Organisation (z. B. „STRENG GEHEIM“) auf Geheimhaltungsstufen anderer Organisationen abzubilden. Dies ist *„vor allem dann von großem Interesse, wenn beispielsweise NATO-Partner wie Deutschland und Griechenland Informationen austauschen, die unterschiedliche Alphabete bzw. Zeichensätze verwenden“*.

Die *Fernwartungslösung* der Firma *genua* berührt die Implementierung von Prozessen Dritter. Sie ermöglicht es Herstellern (und Komponentenherstellern), technischen Support als kosteneffizienten Service anzubieten und die Verfügbarkeit zu verbessern, denn die *„Reduktion von Kosten ist vor allem dann relevant, wenn der Zugang nicht nur für Fernwartungszwecke, sondern auch zur Optimierung der Einstellungen oder für das Monitoring von Verschleißteilen eingesetzt wird. Ein rechtzeitiges Versenden von Ersatzteilen – gerade in geografisch schwer zugänglichen Gebieten – senkt potenziell drastisch die Ausfallzeiten von Wartungsobjekten“*.

Die Ergebnisse der Analyse der Fallstudien dieses Codes zeigen, dass nicht nur Geschäftsprozesse Einfluss auf andere Geschäftsprozesse haben, sondern auch IT-Sicherheitsmaßnahmen andere Geschäftsprozesse beeinflussen – und das teilweise sogar über die Organisationsgrenze hinaus. Das Wissen von solchen Abhängigkeiten ist besonders im Hinblick auf den Schutz vor Angriffen und insbesondere im Rahmen des Business-Continuity-Managements und der damit einhergehenden Business-Impact-Analyse von besonderer Bedeutung (Hiles 2010; Bartock u. a. 2016). In den Fallstudien zeigt sich, dass IT-Sicherheitsprojekte innerhalb einer Organisation nicht nur von IT-Sicherheitsfachpersonal durchgeführt werden sollten, sondern Fachkompetenzen anderer Geschäftsbereiche und z. B. Process Owner in die Projekt-

teams integriert werden sollten. So können bereits in der Planungsphase Synergien erkannt werden, was einerseits die IT-Sicherheitsprozesse verbessert und andererseits andere Geschäftsprozesse (noch) besser absichert. Ebenso zeigen die Fallstudien, dass es nicht-triviale Abhängigkeiten zwischen IT-Sicherheitsprozessen und anderen Geschäftsprozessen geben kann. Für diesen Fall ist es für Organisationen ratsam, bereits bestehende Geschäftsprozesse kritisch im Hinblick auf mögliche Synergien zu prüfen und ggf. mit bereits bestehenden IT-Sicherheitsprozessen zu kombinieren. An dieser Stelle können die vorgestellten Fallstudien als Inspiration gesehen werden.

13.9 Code 6: Erfolgsfaktoren für die Implementierung

In den untersuchten Fallstudien ergeben sich Gemeinsamkeiten in Bezug auf Faktoren, die eine erfolgreiche Implementierung begünstigen oder sogar Voraussetzung dafür sind. Das Ergebnis der vergleichenden Fallstudienanalyse ist, dass sich vier Faktoren als bedeutend darstellen (Abbildung 13-5).
So ist in fünf Fallstudien ein *erfolgreiches Einbinden* der Management-Ebene ein wichtiger Faktor (*Bundeswehr*, *genua*, *PREVENT*, *SAP*, *ugarbe.de software*). Beispielsweise wird bei der Fallstudie über *ClassifyIt* festgestellt, dass das Management nicht nur die Notwendigkeit von IT-Sicherheit erkennt, sondern sie auch durchsetzen muss. Auch bei den Fallstudien zur *Human Firewall* von *SAP* und zur *Managementlösung* von *PREVENT* wird auf die Bedeutung des frühzeitigen und erfolgreichen Einbindens der Management-Ebene hingewiesen. In der *genua*-Fallstudie wird spezifischer genannt, dass die Unterstützung durch den Vorstand sowie CIO und CISO wichtig ist, während in der Fallstudie *Bundeswehr* die Unterstützung durch das Top-Management der Bundeswehr als ausschlaggebend erkannt wurde. Hierzu passt auch die Forderung des BSI, dass das Management für IT-Sicherheit sensibilisiert werden muss und dafür verantwortlich ist, die Umsetzung von IT-Sicherheitsmaßnahmen nachdrücklich und aktiv zu unterstützen (BSI 2013a).

Ein weiterer Faktor für eine erfolgreiche Implementierung ist die *Akzeptanz der Maßnahmen*. Während bei der Fallstudie zu *ClassifyIt* die Akzeptanz durch Nutzerfreundlichkeit im Vordergrund steht, wird in der Fallstudie zu *genua* die Notwendigkeit gesehen, Widerstände abzubauen. Auch bei der *Molkerei* und bei *PREVENT* wird die Akzeptanz durch die Mitarbeiter (*Molkerei*) bzw. durch die Anwender (*PREVENT*) als wichtiger Erfolgsfaktor betrachtet. Genauso wird auch in der Fallstudie *Bundeswehr* die Akzeptanz der Awareness-Maßnahmen durch die Zielgruppe betrachtet. Denn bei der Implementierung von neuen IT-Sicherheitsmaßnahmen besteht, wie auch generell bei der Implementierung von neuen Systemen und Prozessen, die Gefahr, dass sich Widerstände dagegen bilden.

Daneben identifiziert die Fallstudie zur *Leitstelle* in *Ostthüringen* auch speziell *Engagement* und Bereitschaft zur Pflichterfüllung als wesentlichen Faktor. So wollen z. B. die Mitarbeiter Probleme nicht einfach nur erkennen, sondern den Ursachen auf den Grund gehen, um Probleme dauerhaft zu verhindern. Derselbe Faktor kommt in ähnlicher Form auch in der Fallstudie zur *Molkerei* zum Tragen. In der *Bundeswehr*-Fallstudie spielt Engagement insofern

Abbildung 13-5: Erfolgsfaktoren für die Umsetzung von IT-Sicherheit

eine bedeutende Rolle, als die Arbeit der *AG Awareness* in großen Teilen auf Eigeninitiative und freiwilliger Mitarbeit basiert. So fußen erfolgreiche Implementierungen sowie auch deren Akzeptanz auf dem *Commitment* in der Belegschaft.

Insgesamt zeichnet sich ab, dass es wichtig ist, alle entscheidenden Organisationseinheiten einzubeziehen und „an einem Strang zu ziehen". So wird in der Fallstudie *itWatch* die *effektive Zusammenarbeit* als wichtiger Faktor unterstrichen, welche speziell vom Projektleiter gefördert wird. In der Produktfallstudie *genua* wird ebenfalls auf die Notwendigkeit des Einbindens aller involvierten Parteien hingewiesen, während bei Fallstudie *kbo* die Zusammensetzung des IT-Sicherheitskomitees ausschlaggebend ist. Dies steht auch im Einklang mit der Empfehlung des BSI, dass ein Realisierungsplan für die Umsetzung eines IT-Sicherheitskonzepts neben der Bereitstellung von Ressourcen durch das Management auch die Festlegung von Verantwortlichkeiten enthalten sollte (BSI 2008a). Dabei soll laut BSI auch die Informationssicherheit in die Abläufe und Prozesse der jeweiligen Organisation integriert werden, wobei auftretende Probleme umgehend zu kommunizieren sind.

Insgesamt entsprechen die Erfolgsfaktoren für die erfolgreiche Implementierung von IT-Sicherheitsmaßnahmen weitgehend den Erfolgsfaktoren von Projekten im Allgemeinen. Hervorzuheben ist die Bedeutung der Bereitschaft, Ursachen und Zusammenhängen wirklich auf den Grund zu gehen. Hervorzuheben ist auch die besondere Bedeutung des Managements. Es muss speziell beim Thema IT-Sicherheit die Notwendigkeit erkennen und entsprechend durchsetzen.

13.10 Code 7: Treiber und Auslöser

Mit dem Code *Treiber und Auslöser* wurde der Fokus auf die der Einführung einer IT-Sicherheitsmaßnahme zugrunde liegende Rahmenbedingung gelegt, welche für die Entscheidung für ein Projekt innerhalb eines Unternehmens bzw. die Entwicklung eines Produkts zur Erhöhung der IT-Sicherheit in einem bestimmten Anwendungskontext ursächlich (*Auslöser*) oder zumindest teilweise mit auschlaggebend war (*Treiber*). Diese für die hier vorgestellten Fallstudien relevanten Rahmenbedingungen können demnach entweder allgemeine Umstände widerspiegeln – wie z. B. die Einführung des IT-Sicherheitsgesetzes – oder eine individuelle Besonderheit der die Maßnahme einführenden Organisation sein. Die *Treiber und Auslöser* der IT-Sicherheitsstrategien bzw. -maßnahmen in den Fallstudien variieren dabei je nachdem, ob eine gesamte Organisation, die Einführung einer spezifischen neuen Maßnahme oder aber die Dienstleistung eines externen Anbieters betrachtet wurde. In der fallstudienübergreifenden Analyse hat sich dabei eine Unterteilung in interne und externe Treiber bzw. Auslöser herauskristallisiert.

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 (*SAP*, *Molkerei*, *itWatch*, *PREVENT*, *kbo*), der entweder direkt oder indirekt ausgeprägt gewesen sein kann.[11] Compliance als zentraler Treiber überrascht ggf. auch deshalb nicht, da sich aus den – je nach Branche sehr unterschiedlichen – regulatorischen Vorgaben und Gesetzen nicht nur Verpflichtungen für Mindestanforderungen in der IT-Sicherheit ableiten, sondern auch Haftungsrisiken für die Unternehmensführer von GmbHs oder Vorständen von AGs entstehen können (Grünendahl u. a. 2017).

Als weiterer externer Treiber sind bei zwei Fallstudien auch mögliche *Reputationsverluste* im Falle von IT-Sicherheitsvorfällen erwähnt worden (*SAP*, *Molkerei*), während eine *veränderte Bedrohungslage* sowie die *Informationen zu IT-Angriffen* auf Organisationen in derselben Branche nur in der Fallstudie *kbo* ausschlaggebend waren. Hier war der Angriff mit einer Ransomware auf ein anderes Krankenhaus das auslösende Ereignis, um die eigenen Prozesse und die damit verbundene IT-Sicherheit einer dedizierten Überprüfung zu unterziehen.

Darüber hinaus konnten aber auch bei knapp der Hälfte der Fallstudien mehrere interne Treiber als ausschlaggebende Rahmenbedingungen für die IT-Sicherheitsprojekte und eingeführten IT-Maßnahmen identifiziert werden. Diese reichten wiederum von einem allgemein hohen moralischen Selbstverständnis bzw. *Verantwortungsbewusstsein* für die eigenen Kunden (z. B. *Molkerei*) über effizienzbegründete Vereinfachungen und *Optimieren von Prozessen* bis hin zum *Vermeiden von Wissensverlusten*, welche sich z. B. durch eine erhöhte Personal-

11 Eine indirekte Ausprägung des KRITIS-Bezugs kann z. B. dann gegeben sein, wenn Unternehmen selbst nicht durch die KRITIS-Verordnungen erfasst sind, aber entweder schlicht auf freiwilliger Basis nachkommen möchten oder ähnlichen bzw. äquivalenten Anforderungen durch eigene KRITIS-Kunden gerecht werden müssen.

Abbildung 13-6: Interne und externe Treiber und Auslöser

fluktuation in der Vergangenheit als Herausforderung erwiesen hatten (z. B. *itWatch*, *genua*). Alle in den Fallstudien erkannten Treiber und Auslöser sind in Abbildung 13-6 dargestellt.

Die *Treiber und Auslöser* der Fallstudien haben sich in der Cross-Case-Analyse naturgemäß heterogen dargestellt, da jeder der betrachteten Anwendungskontexte individuelle Rahmenbedingungen vorweist, die auch für Maßnahmen der IT-Sicherheit Bedeutung haben. Auch können die gesetzlichen Vorgaben bzw. die vom Gesetzgeber selbstgesetzten Anforderungen in ihrer Konkretheit unterschiedlich sein: So ist die treibende Vorgabe der Fallstudie *Ostthüringen* – innerhalb 60 Sekunden aus einem Notruf einen Einsatzbefehl zu erzeugen – greifbar, während bei der *Bundeswehr* die Rückschlüsse auf konkrete Maßnahmen auf Basis der allgemein gehaltenen Maxime – die Chancen der Digitalisierung zu nutzen, Bedrohungen aus dem Cyber- und Informationsraum zu begegnen und der außenpolitischen Handlungsfähigkeit und dem Schutz der Bürger Rechnung zu tragen – vermutlich nur mit höherem Aufwand möglich sind. Zahlenmäßig sind in den Fallstudien jedoch die externen Treiber den internen Treibern deutlich überlegen – insbesondere die Compliance zu Veränderungen in der rechtlichen Anforderungslandschaft (siehe dazu auch Kapitel 13.3). Aber auch herausragende Einzelbeispiele, wie z. B. die Fallstudie der *Molkerei*, zeigen auf, dass es neben solchen externen Einflüssen auch wegweisende interne Treiber geben kann, die das moralische Selbstverständnis des Unternehmens abbilden und das Verantwortungsbewusstsein gegenüber dem eigenen Kunden in den Vordergrund stellen. Eine sorgfältige Analyse sämtlicher interner und externer Treiber erscheint jedoch in jedem Fall als eine Notwendigkeit, um nachhaltige Entscheidungen zur IT-Strategie treffen zu können.

13.11 Code 8: IT-Sicherheitsphilosophie

Für die Betrachtung des Codes „IT-Sicherheitsphilosophie" werden die untergeordneten Codes *Vertrauensfokus in Technik – Organisation – Mensch* und *Organisationskultur* zusammengefasst behandelt.

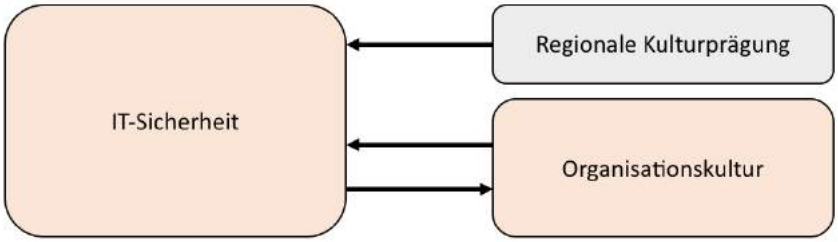


Abbildung 13-7: IT-Sicherheit im Zusammenhang mit kulturellen Aspekten

Das BSI nennt als Faktoren, die bei der Konzeption und Planung von IT-Sicherheitsprozessen berücksichtigt werden sollen, unter anderem Umwelteinflüsse in Form von sozialen und kulturellen Rahmenbedingungen, wie regionale Kulturprägung und organisationale Aspekte (BSI 2008b). Umgekehrt wird IT-Sicherheit, wenn sie gelebt wird, Teil der Organisationskultur und die Maßnahmen können die Kultur mitprägen (Helisch & Pokoyski 2009). Der Zusammenhang von IT-Sicherheit und kulturellen Aspekten ist demnach wechselseitig (Abbildung 13-7).

Es wird in den Fallstudien sichtbar, wie die bestehende Organisationskultur die Grundlage für das Gelingen von IT-Sicherheitsmaßnahmen bildet. So gilt in der Fallstudie *Molkerei* das Commitment neben Einsatzbereitschaft und langjähriger Beschäftigung als wichtiger Erfolgsfaktor für die Umsetzung von IT-Sicherheit. Auch in der Fallstudie *Ostthüringen* spielt die Einsatzbereitschaft des Personals eine entscheidende Rolle. Ähnlich verhält es sich mit der *AG Awareness* in der Fallstudie über die *Bundeswehr*, wo Eigeninitiative und freiwillige Mitarbeit eine große Rolle spielen. Auch die Fallstudie *kbo* thematisiert den Einfluss dieser Bedingungen auf IT-Sicherheitsmaßnahmen, z. B. in der Form, dass sich in den Kliniken jeder Einsatz von IT nach den Bedürfnissen des Patienten und dem Datenschutz zu richten hat, was der IT-Sicherheit ambivalent gegenübersteht. Denn einerseits ist so ein generelles Verständnis für die Belange des Datenschutzes und der IT-Sicherheit gegeben, andererseits kann z. B. durch das Bedürfnis des Patienten, schnell behandelt zu werden, die Sorgfalt zugunsten eines schnellen Handelns vernachlässigt werden. Die Fallstudie *SAP* beschreibt Vertrauen in die Mitarbeiter, aber auch Vertrauen der Kunden in SAP als zentralen Bestandteil. Vertrauen ist hier bereits Bestandteil der Organisationskultur und das drückt sich auch im Kontext der IT-Sicherheit aus, etwa durch das Projekt der *Human Firewall*.

Aber auch für den Einfluss der IT-Sicherheitsmaßnahmen auf die kulturellen Aspekte finden sich Hinweise in den betrachteten Fallstudien. Die *Human Firewall* fördert nämlich nicht nur die Awareness zum Thema Informationssicherheit, sondern nebenbei auch das Commitment der Mitarbeiter und wird mit den Aktionen der Kampagne Teil der Organisationskultur. Denn die Maßnahmen sind nicht nur präsent für die Mitarbeiter, sondern

beeinflussen letztlich auch Verhalten, Handeln und Selbstbild. In der Fallstudie *genua* wird auf Kompetenzstreitigkeiten oder Machtverlust als Resultat der IT-Sicherheitsmaßnahmen hingewiesen. So können Änderungen in IT-Landschaften oder Organisationsprozessen das Machtgefüge in einer Organisation ändern und dadurch zu Unmut in der Belegschaft führen sowie Widerstände gegen diese Änderungen hervorrufen (Markus 1983; Lapointe & Rivard 2005).

Ein Thema der IT-Sicherheit, das auch die Organisationskultur betrifft, 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, die in den Fallstudien beschrieben werden. In den Fallstudien zu *ClassifyIt*, der *Human Firewall*, der *AG Awareness* und der IT-Sicherheitsstrategie der *Molkerei* wird der Faktor Mensch thematisiert und als potenzielles Risiko bewertet: *ugarbe.de software* fokussiert die Nachlässigkeit von Nutzern beim E-Mail-Versand und bei der Klassifizierung von Dokumenten, *SAP* sieht den Mitarbeiter als kritisch für Kundenvertrauen und die *Molkerei* bezieht Innentäter in die Strategie mit ein, auch wenn dort ein Risiko durch Innentäter eher als gering eingestuft wird. Die Ansätze der Fallstudien *Molkerei* und *ugarbe.de software* adressieren das Risiko durch den Menschen mit technischen Maßnahmen, während *SAP* und die *Bundeswehr* dies mit einem umfangreichen Awareness-Maßnahmenpaket adressieren, also beim Menschen direkt ansetzen.

Es ist ersichtlich, dass in den Fallstudien die Zusammenhänge zwischen Organisationskultur, dem Faktor Mensch und IT-Sicherheit vielfältig sind. Dennoch ist Kultur immer ein Bestandteil des Rahmens, in dem IT-Sicherheit stattfindet, und sollte daher in Betrachtungen mit einbezogen werden. Denn es spielt angesichts der Ergebnisse der vergleichenden Fallstudienanalyse eine Rolle, wie gut über die Grenzen einer Organisation hinaus zusammengearbeitet wird, aber auch wie Commitment oder Awareness in einer Organisation ausgestaltet ist. So kann IT-Sicherheit ganzheitlich betrachtet werden, was dann auch die Perspektive der Cybersecurity Culture (CSC) einschließt. ENISA definiert CSC als „*the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest in people's behaviour with information technologies*“ (ENISA 2017a).

13.12 Code 9: Adressierte Risiken

Mit dem Code „Adressierte Risiken“ wurden die in den Fallstudien vorgestellten IT-Sicherheitsmaßnahmen dahingehend untersucht, welchen Konstellationen aus zu schützenden Informationswerten, Bedrohungen und möglichen Angriffsvektoren durch die jeweiligen IT-Sicherheitsprojekte oder -produkte begegnet werden sollte. Dies ist auch deshalb von Interesse, da die möglicherweise in IT-Sicherheitsstrategien oder Produkt- bzw. Projektbeschreibungen *explizit* genannten Risiken ggf. nicht auch alle *implizit* adressierten Risiken der einführenden Organisation abdecken müssen. Die Analyse der Praxisbeispiele hat gezeigt, dass das Feld der *Adressierten Risiken*, denen eine Organisation mit einem IT-Sicherheitskonzept begegnen will, meist ein komplexes Zusammenwirken mehrerer Gefährdungen und unterschiedlicher IT-Sicherheitsmaßnahmen ist, deren Orchestrierung – insbesondere bei gegenläufigen Inte-

ressen der beteiligten Stakeholdergruppen – zu einer Herausforderung werden kann. Bevor die Ergebnisse dieses Codes erläutert werden, empfiehlt sich daher zunächst, einen kurzen Überblick über das Zusammenwirken von Gefährdungen und Maßnahmen voranzustellen.

Maßnahmen zur Förderung der IT-Sicherheit sind in der Regel auf einzelne oder mehrere *Schutzziele* der IT-Sicherheit ausgerichtet. Regelmäßig werden in diesem Zusammenhang die drei anscheinend besonders bedeutsamen Schutzziele *Authentizität* (engl. *Authenticity*), *Datenintegrität* (engl. *Integrity*) sowie *Informationsvertraulichkeit* (engl. *Confidentiality*) hervorgehoben. In der Literatur werden jedoch zudem auch noch weitere Schutzziele thematisiert. So definiert Eckert neben den zuvor genannten ebenfalls *Verfügbarkeit* (engl. *Availability*) und *Verbindlichkeit* (engl. *Non-Repudiation*) als Schutzziele, weist aber darüber hinaus auch auf Aspekte der *Anonymisierung* und *Pseudonymisierung* oder den recht abstrakten Begriff des *Vertrauens* als mögliche Schutzziele hin, welche gerade im Kontext *vernetzter und insbesondere mobiler Systeme* an Bedeutung gewinnen (Eckert 2013). Auch Bedner & Ackermann differenzieren zwischen mehr als zehn verschiedenen Schutzzielen, welche teils auch auf Gegensätzliches ausgerichtet sind. So kann abhängig vom jeweiligen Kontext auch die Gewährleistung größtmöglicher *Transparenz* – als Gegenteil zur *Vertraulichkeit* – die der spezifischen IT-Sicherheit förderlichere Zielmaxime sein (Bedner & Ackermann 2010). In Abbildung 13-8 sind mehrere mögliche Schutzziele der IT-Sicherheit aufgelistet und ein möglicher Zusammenhang zwischen Schutzzielen und Rahmenbedingungen dargestellt.

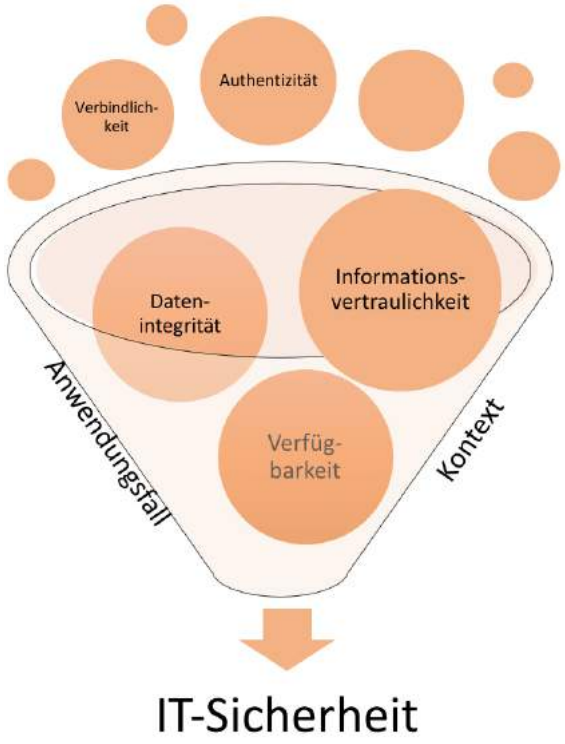


Abbildung 13-8: Kontextabhängige Relevanz verschiedener Schutzziele der IT-Sicherheit

Diese Vielfalt zeigt letztlich auf, dass die Relevanz von Schutzzielen und insbesondere deren Priorisierung hauptsächlich vom zugrunde liegenden Anwendungsfall abhängig sind und eine dies adressierende Analyse Grundlage der initialen Planung und fortlaufenden Gewährleistung von Effektivität und Effizienz einer jeden IT-Sicherheitsstrategie sein sollte; zweites insbesondere deshalb, weil die Wirksamkeit einer Maßnahme auch nur dann gemessen werden kann, wenn ein Bewusstsein über die eingenommene Schutzzielausrichtung besteht.

Schutzziele geben jedoch lediglich die abstrakten Maximen für die Ausrichtung der IT-Sicherheit einer Organisation vor. Verfahren des Risikomanagements bieten Methoden an, um die in einem Anwendungsfall tatsächlich vorliegenden Informationswerte bzw. Assets der IT-Infrastruktur, deren externe und interne Schwachstellen, auf diese Schwachstellen wirkende Gefährdungen und so entstehende Risiken zu erheben. Verfahren des Risikomanagements erlauben es damit, die Eintrittswahrscheinlichkeiten und Schadenspotenziale von Risiken in strukturierter Form zu erheben und derart zu analysieren, dass informierte Entscheidungen getroffen werden können. Je nach verwendeten Verfahren können sich die Prozesse unterscheiden; es ist aber die Regel, dass zu schützende *Assets*, *Schwachstellen* und *Gefährdungen* in Verbindung gesetzt werden, um die erst daraus entstehenden *Risiken* konkret *behandeln* zu können. Diese im Risikomanagement verortete Unterscheidung zwischen ursächlichen Gefährdungen und daraus entstehenden Risiken ist für den hiesig betrachteten Code *Adressierte Risiken* nicht ausschlaggebend gewesen. Extrahierte Aussagen zu behandelten Risiken wurden somit unabhängig von verwendeten Methoden des Risikomanagements als Ergebnis einer *Black Box* betrachtet. Der Code umfasst *sowohl* konkrete Risiken für die IT der Organisation *als* auch durch die Fallstudienpartner aufgezeigte Gefährdungen.

In den Gefährdungskatalogen des IT-Grundschutzes des BSI sind in einem hohen Detaillierungsgrad die vielfältigen Gefährdungen zusammengefasst, die die geschäftsrelevante Informationssicherheit in Unternehmen und Behörden bedrohen. Dabei sind unterschiedliche Gefährdungsarten in die sechs Bereiche *G 0* bis *G 5* gruppiert, die entsprechend für Gefährdungen aus den Themengebieten *Elementare Gefährdungen*, *Höhere Gewalt*, *Organisatorische Mängel*, *Menschliche Fehlhandlungen*, *Technisches Versagen* und *Vorsätzliche Handlungen* stehen (BSI 2016a). Die sechs Bereiche enthalten dabei jeweils einige Dutzende bis mehrere Hundert einzelne Gefährdungen. Die einzelnen Kataloge und beispielhaften Gefährdungen daraus sind in Abbildung 13-9 dargestellt. Für viele Organisationen ist die Auseinandersetzung mit den IT-Grundschutzkatalogen im Ganzen und auch nur mit den Gefährdungskatalogen im Speziellen aufgrund der Fülle an Informationen eine große Herausforderung; gerade für kleinere Unternehmen kann jedoch bereits der Katalog *G 0 Elementare Gefährdungen* eine gute Grundlage für eine individuelle Risikoanalyse bieten (Stetter & Heukrodt-Bauer 2017).

Als Ergebnis des Vergleichs und der Analyse sämtlicher mit dem Code *Adressierte Risiken* codierten Textpassagen in den Fallstudien wurde eine große Breite begegneter Gefährdungen festgestellt. Dies verdeutlicht, dass die unterschiedlichen Herangehensweisen der Unternehmen und der vorgestellten Produkte nicht nur organisational und technologisch begründet sind, sondern auch IT-Sicherheitsrisiken von Organisation zu Organisation unterschiedlich wahrgenommen werden. So wurde die zugrunde liegende Vermutung, dass die *Verfügbarkeit* einer Kritischen Infrastruktur das über die gesamte Lieferkette im Vordergrund stehende Schutzziel

Abbildung 13-9: Gefährdungskataloge (BSI) mit beispielhaften Gefährdungen; Quelle: BSI 2016a

sei, durch ein differenzierteres Verständnis der in den vorliegenden Fallstudien adressierten Risiken erweitert. Tatsächlich variieren die relevanten Gefährdungen bzw. Risiken in den Fallstudien deutlich; fast alle Bereiche der BSI-Gefährdungskataloge finden dabei Beachtung.

Die Art der Erwähnung bzw. Behandlung der explizit und implizit adressierten IT-Sicherheitsrisiken ist in den Fallstudien im Zuge der Vorstellung der IT-Sicherheitsmaßnahmen verschieden. Während zum Beispiel einzig die Fallstudie der *Molkerei* das IT-Sicherheitskonzept möglichst in Gänze beschreibet, werden in den anderen Fallstudien vorwiegend einzelne bzw. kombinierte IT-Sicherheitsmaßnahmen innerhalb der individuellen Gefährdungssituation der Unternehmen vorgestellt. Diese *Adressierten Risiken* ließen sich neben ihrer individuellen Zugehörigkeit zu den verschiedenen Bereichen der BSI-Gefährdungskataloge in der übergreifenden Betrachtung der Fallstudien untereinander außerdem auch in *interne* und *externe* Risiken untergliedern (siehe Abbildung 13-10).

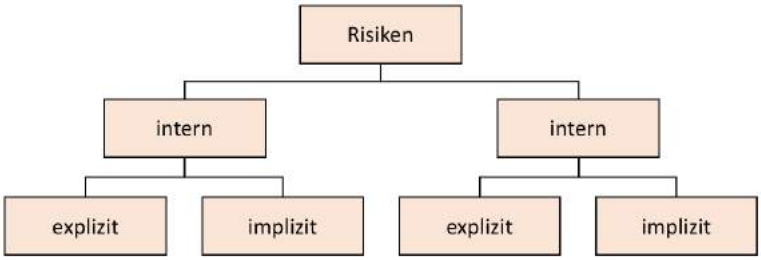


Abbildung 13-10: Möglichkeiten adressierter IT-Sicherheitsrisiken

Das Vermeiden von *Menschlichen Fehlhandlungen* (G 3) war über alle Fallstudien hinweg die hinsichtlich der adressierten Risiken am häufigsten auszumachende Strategie. Der häufig erkannten Gefährdung eines *Vertraulichkeits- oder Integritätsverlustes von Daten durch Fehl-*

verhalten (*G 3.1*) – verursacht z. B. durch die *Nichtbeachtung von Sicherheitsmaßnahmen* (*G 3.3*), die *Weitergabe falscher oder interner Informationen* (*G 3.13*) oder durch *Sorglosigkeit im Umgang mit Informationen* (*G 3.44*) – wird oft durch technische und prozessuale Verbesserungen der Geschäftsabläufe begegnet, wobei die Lösungsansätze unterschiedlich sind. So zielt die technische Maßnahme der Fallstudie zu *ugarbe.de software* unter anderem auf eine bewusste Sensibilisierung der Anwender unmittelbar bei der Verarbeitung von vertraulichen Informationen ab, während die Fallstudie zur *digitalen Tatortfotografie* sich auf einen vollautomatisierten Ablauf außerhalb der Wahrnehmung des Anwenders stützt. Die Fallstudie über die Implementierung einer *Fernwartungslösung* adressiert auch unmittelbar die mögliche Gefährdung, dass Mitarbeiter bei der Durchführung von Routinewartungen sorgloser werden, indem Belastungen durch Anfahrtswege oder aufwendige Prozessabläufe eliminiert werden.

Zwar werden in den Fallstudien auch Sicherheitsmaßnahmen beschrieben, die Gefährdungen durch *Höhere Gewalt* (G 1; *PREVENT*, *Molkerei*), *Technisches Versagen* (G 4; *itWatch*, *Molkerei*) und *Vorsätzliche Handlungen* (G 5; *itWatch*, *genua*) vermeiden sollen, tatsächlich sind interne Maßnahmen zur Vermeidung *Menschlicher Fehlhandlungen* (G 3) jedoch deutlich häufiger zu zählen: entweder durch eine Förderung der IT-Security-Awareness der Anwender (z. B. *ugarbe.de software*, *SAP*) oder durch eine Prozessveränderung jener Art, dass das Risiko eines Anwenderfehlers reduziert oder sogar gänzlich ausgeschlossen ist (z. B. *itWatch*, *Molkerei*, *genua*). Interessant ist in diesem Zusammenhang auch das adressierte Risiko der Fallstudie *Bundeswehr*, die das Risiko einer unausgefüllten Vorbildfunktion durch die der Zielgruppe vorgesetzten Führungskräfte beschreibt. Dieses implizit adressierte Risiko kann am ehesten der Gefährdung G 3.77 *Mangelhafte Akzeptanz von Informationssicherheit* zugeordnet werden. In der Fallstudie *Ostthüringen* liegt stattdessen die Absicherung technischer Systeme und Schnittstellen – welche entweder ausfallen oder Angreifern als Einfallstore dienen können – vorwiegend im Fokus der betrachteten IT-Sicherheitsmaßnahmen. Hier wird deutlich, wie bei einem überschaubaren Anwenderkreis der eingesetzten Disponenten die Gefahr menschlicher Fehlhandlungen eher geringer ist. Angesichts der hohen Anforderungen der *Leitstelle* bezüglich des Schutzziels der *Verfügbarkeit* (interne Risiken durch *Technisches Versagen* (G 4) und externe Risiken durch *Vorsätzliche Handlungen* (G 5)) haben die Härtung der Kommunikations- und Wartungsschnittstellen bzw. der vielen Komponenten unterschiedlicher Hersteller die höchste Priorität im IT-Sicherheitskonzept.

Die Häufung der anwenderausgerichteten Maßnahmen kann vermutlich auch darauf zurückgeführt werden, dass insbesondere Angriffstypen innerhalb des *Social Engineerings* nahezu allen Angriffsakteuren (engl. *threat agents*) offenstehen, während sehr komplexe Angriffe auf IT-Infrastrukturen in der Regel den besonders finanzstarken Angreifern vorbehalten sind (ENISA 2017b). Ebenfalls darf an dieser Stelle nicht unerwähnt bleiben, 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 in einer Fallstudie genannt worden.

Insgesamt ließen sich durch den Code *Adressierte Risiken* Erkenntnisse darüber gewinnen, wie in Unternehmen den Auswirkungen auf den Produktivbetrieb, den Schäden bei Kunden und auch der Sorge um Vertraulichkeits- und Integritätsverluste von Daten und Informati-

onen eine bewusst getroffene Relevanz zugesprochen wird, die je nach Anwendungskontext Grundlage für Entscheidungen innerhalb des IT-Sicherheitsmanagements sein kann. Gerade aufgrund der dargestellten Herausforderung bedingt aus dem Zusammenwirken von implizit und explizit adressierten Risiken hat sich aufgezeigt, dass mit der verwendeten Untersuchungsmethodik eine garantierte Erfassung aller relevanten Gefährdungen und Risiken nicht gegeben sein kann. Die schiere quantitative Menge differenzierbarer Gefährdungen und die nicht in Gänze erfassbaren, für die IT-Sicherheit relevanten Entscheidungsprozesse innerhalb der betrachteten Organisationen lassen Spielraum für weitere – hier unter Umständen nicht erfasste – Risiken offen. Jedoch eignet sich das Ergebnis dieses Codes neben der Analyse der in den Fallstudien adressierten Risiken auch dazu, für die Vielschichtigkeit des Themas zu sensibilisieren. Ohne eine geeignete Methodik des Risikomanagements kann der Erfolg gut gemeinter IT-Sicherheitskonzepte bereits zu Beginn gefährdet sein, daher sollte ein strukturiertes Vorgehen und ein auf den individuellen Anwendungsfall zugeschnittenes IT-Sicherheitskonzept am Anfang jedweder Bemühungen stehen – sowie natürlich auch dessen fortlaufende Aktualisierung.

13.13 Fazit

In dieser Cross-Case-Analyse konnten die neun einzelnen Fallstudien dieses Buchs in ihrer jeweils unterschiedlichen Auseinandersetzung mit dem Thema IT-Sicherheit untersucht werden. Dem qualitativen Charakter einer solchen Analyse entsprechend kann damit keine „Bedienungsanleitung für IT-Sicherheit" gegeben werden. Doch die Hoffnung der die Cross-Case-Analyse durchführenden wissenschaftlichen Mitarbeiter, dass eine solche fallübergreifende Betrachtung interessante, nicht-intuitive und auch spannende Ergebnisse aufzeigen kann, hat sich erfüllt.

Die vorangegangenen Kapitel zu den Ergebnissen der einzelnen Codes der Analyse zeigen insbesondere auf, dass IT-Sicherheit zumindest in den untersuchten Szenarien der neun Fallstudien niemals isoliert betrachtet wurde. Die häufig betonte Maxime, verschiedene Stakeholdergruppen bei einer Maßnahmeneinführung bereits zu Beginn der Planungen mit einzubeziehen, scheint geradezu symptomatisch für das Verständnis, IT-Sicherheit nicht als Zustand oder als eine Verantwortlichkeit einzelner IT-Mitarbeiter, sondern als gelebten Prozess aller mit Informationssystemen einer Organisation in Berührung stehenden Personengruppen zu verstehen. Für erfolgreiche Projekte bedarf es deswegen neben der Auswahl geeigneter technischer Lösungen oder organisationaler Maßnahmen auch insbesondere des Augenmerks auf die Überzeugung und Gewinnung der betroffenen Mitarbeiter – bzw. auch unternehmensexterner Personenkreise – für die mit einer Maßnahme verbundenen möglichen Veränderungen der Geschäftsabläufe. Um dies zu gewährleisten, hat sich die Identifikation und Verpflichtung von Vorgesetzten und des Managements als ein zentraler Faktor herausgestellt. Dies kann außerdem auch dem Verständnis für Investitionen in die IT-Sicherheit dienlich sein; gerade bei diesem Aspekt stoßen klassische Verfahren der Kapitalrentabilität aufgrund der inhärenten Abstraktheit von IT-Sicherheit an Grenzen, sodass Verständnis für monetäre und Opportunitätskosten als kritischer Erfolgsfaktor auf anderen Wegen geschaffen werden muss.

Neben den kontextuellen Ergebnissen u. a. zu Erfolgsfaktoren, zur vorherrschenden IT-Sicherheitsphilosophie in einer Organisation und zu Fragestellungen nach den Kosten von IT-Sicherheit wurden auch Aspekte der IT-Sicherheitslösungen im engeren Sinne betrachtet und verglichen: So bieten die Ergebnisse der Codes einen Einblick in die durch die Projekte adressierten Risiken, die Beurteilung, Messung und Erhöhung von IT-Sicherheit und – last, but not least – die sogenannte Einfachheit einer gewählten Maßnahme. Denn auch hier hat sich gezeigt, dass es vor der Bereitstellung von einfachen Lösungen zunächst auch einer einheitlichen Sprache bzw. eines semantischen Verständnisses bedarf, in welcher Hinsicht z. B. technische Lösungen *einfach* sein müssen, damit sie für Organisationen und vor allem KMU auch tatsächlich attraktiv sind.

So konnten durch die code-individuelle Betrachtung innerhalb der Cross-Case-Analyse mehrere Beiträge zum Verständnis der Gesamtzusammenhänge erfolgreicher IT-Sicherheitsprojekte geleistet werden. Diese Erkenntnisse sollen dabei aber nicht als Gesetzmäßigkeiten missverstanden werden, sondern als positive Erfahrungen der gegenwärtigen Praxis, die für die Planung zukünftiger Einführungen von IT-Sicherheitsmaßnahmen Inspiration bieten können.

13.14 Literaturverzeichnis

Bartock, M. u. a., 2016. NIST Special Publication 800-184: Guide for Cybersecurity Event Recovery, Verfügbar unter: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf [zugegriffen: 7-Juni-2018].

Bedner, M.; Ackermann, T., 2010. Schutzziele der IT-Sicherheit. Datenschutz und Datensicherheit – DuD, 34(5), S. 323–328. Verfügbar unter: http://link.springer.com/10.1007/s11623-010-0096-1 [zugegriffen: 7-Juni-2018]

BMI, 2008. Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement, S. 1–89.

BSI, 2008a. BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS), S. 1–37.

BSI, 2008b. BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, 2.0, S.1–90.

BSI, 2008c. BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz, 2.5, S. 1–23.

BSI, 2008d. BSI-Standard 100-4: Notfallmanagement, S. 1–123.

BSI, 2013a. IT-Grundschutz – M 3.44. Sensibilisierung des Managements für Informationssicherheit. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m03/m03044.html?nn=6604926 [zugegriffen 27-Nov-2017].

BSI, 2013b. Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT, S. 1–74.

BSI, 2016a. IT-Grundschutz-Kataloge – 15. Ergänzungslieferung.

BSI, 2016b. IT-Grundschutz: ORP.3. Sensibilisierung und Schulung. IT-Grundschutz. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/BS_Sensibilisierung_und_Schulung.pdf?__blob=publicationFile&v=2.

Cavusoglu, H.; Mishra, B.; Raghunathan, S., 2004. A model for evaluating IT security investments. Communications of the ACM, 47(7), S. 87–92. Verfügbar unter: http://portal.acm.org/citation.cfm?doid=1005817.1005828 [zugegriffen: 7-Juni-2018].

Cavusoglu, H.; Raghunathan, S.; Yue, W. T., 2008. Decision – Theoretic and Game-Theoretic Approaches to IT Security Investment. Journal of Management Information Systems, 25(2), S. 281–304. Verfügbar unter: http://www.tandfonline.com/doi/full/10.2753/MIS0742-1222250211 [zugegriffen: 7-Juni-2018].

Chehrazi, G.; Schmitz, C.; Hinz, O., 2015. QUANTSEC – Ein Modell zur Nutzenquantifizierung von IT-Sicherheitsmaßnahmen. In: Proceedings der 12. Internationalen Tagung Wirtschaftsinformatik (WI), S. 1131–1145. Verfügbar unter: http://www.wi2015.uni-osnabrueck.de/ [zugegriffen: 7-Juni-2018].

Chew, E. u. a., 2008. NIST Special Publication 800-55: Performance Measurement Guide for Information Security, Gaithersburg.

DIN, 2011. DIN ISO/IEC 27000, S. 1–26.

Ebert, C., 2013. Risikomanagement kompakt – Risiken und Unsicherheiten bewerten und beherrschen, 2. Auflage. Stuttgart: Springer Vieweg.

Eckert, C., 2013. IT-Sicherheit: Konzepte – Verfahren – Protokolle, 8. Auflage. München: Oldenbourg Wissenschaftsverlag GmbH.

ENISA, 2017a. Cyber Security Culture in organisations. Verfügbar unter: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations [zugegriffen: 7-Juni-2018].

ENISA, 2017b. ENISA threat landscape report 2017 – EU Law and Publications. Verfügbar unter: https://publications.europa.eu/en/publication-detail/-/publication/d4d64bd6-0af1-11e8-966a-01aa75ed71a1/language-en/format-PDF/source-66667278 [zugegriffen: 7-Juni-2018].

Faisst, U.; Prokein, O.; Wegmann, N., 2007. Ein Modell zur dynamischen Investitionsrechnung von IT-Sicherheitsmaßnahmen. Zeitschrift für Betriebswirtschaft, 77, S. 511–538. Verfügbar unter: http://link.springer.com/10.1007/s11573-007-0039-y [zugegriffen: 7-Juni-2018].

Gordon, L. A.; Loeb, M. P., 2002. The economics of information security investment. ACM Transactions on Information and System Security, 5(4), S. 438–457.

Grob, H.; Strauch, G.; Buddendick, C., 2008. Konzeption einer VOFI-basierten Methode zur Entscheidungsunterstützung für IS-Sicherheitsinvestitionen. In: Proceedings of Multikonferenz Wirtschaftsinformatik (MKWI) München 26.2.–28.2.2008, S. 1125–1136.

Grünendahl, R.-T.; Steinbacher, A. F.; Will, P. H. L., 2017. Das IT-Gesetz: Compliance in der IT-Sicherheit. Verfügbar unter: http://link.springer.com/10.1007/978-3-658-18205-2 [zugegriffen: 7-Juni-2018].

Helisch, M.; Pokoyski, D., 2009. Security Awareness: Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung, 1. Aufl. Wiesbaden: Vieweg+Teubner Verlag. Verfügbar unter: https://link.springer.com/book/10.1007%2F978-3-8348-9594-3 [zugegriffen: 7-Juni-2018].

Hiles, A., 2010. The Definitive Handbook of Business Continuity Management, 3. Aufl. A. Hiles, Hrsg. John Wiley & Sons.

Johnson, C. S. u. a., 2016. NIST SP 800-150: Guide to Cyber Threat Information Sharing, S. 1–35.

Kronschnabl, S. A., 2010. Konzeption eines Models zur Bestimmung des optimalen Investitionsbeitrags in IT-Sicherheits- bzw. IT-Notfallmaßnahmen unter Berücksichtigung Compliance-bedingter Anforderungen. In: M. Schumann u. a. (Hrsg.), Multikonferenz Wirtschaftsinformatik, {MKWI} 2010, Göttingen, 23.-25.2.2010, Proceedings. Universitätsverlag Göttingen, S. 2181–2192. Verfügbar unter: http://webdoc.sub.gwdg.de/univerlag/2010/mkwi/03_anwendungen/integriertes_ertrags-risikomanagement/05_konzeption_eines_modells_zur_bestimmung_des_optimalen_investitionsbeitrags.pdf [zugegriffen: 7-Juni-2018].

Lapointe, L.; Rivard, S., 2005. A Multilevel Model of Resistance to Information Technology. MIS Quarterly, 29(3), S. 461–491. Verfügbar unter: http://www.jstor.org/stable/25148692 [zugegriffen: 7-Juni-2018].

Markus, M. L., 1983. Power, Politics, and MIS Implementation. Communications of the ACM, 26(6), S. 430–444.

Mayring, P., 2015. Qualitative Inhaltsanalyse – Grundlagen und Techniken, 12. Auflage. Weinheim und Basel: Beltz Verlag.

NIST, 2014. Framework for Improving Critical Infrastructure Cybersecurity, S. 1–39. Verfügbar unter: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf [zugegriffen: 7-Juni-2018].

OWASP, 2017. About The Open Web Application Security Project.

Prokein, O., 2008. IT-Risikomanagement – Identifikation, Quantifizierung und wirtschaftliche Steuerung. Wiesbaden: Springer Gabler.

Sonnenreich, W.; Albanese, J.; Stout, B., 2006. Return on security investment (ROSI) – A practical quantitative model. In: Journal of Research and Practice in Information Technology, S. 45–56.

Stetter, F.; Heukrodt-Bauer, S., 2017. IT-Grundschutzkataloge des BSI – Last oder Mehrwert? Wirtschaftsinformatik & Management, 9(4), S. 62–66. Verfügbar unter: http://link.springer.com/10.1007/s35764-017-0082-6 [zugegriffen: 7-Juni-2018].

Stöwer, M., 2011. Werte schützen, Kosten senken, Erträge steigern – Beispiele für die Wirtschaftlichkeit von Informationssicherheit, Fraunhofer-Institut für Sichere Informationstechnologie. Darmstadt, Sankt Augustin, S. 1–27.

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

Zetter, K., 2015. Countdown to Zero Day : Stuxnet and the launch of the world's first digital weapon. Arms Control Today, 45(2), S. 22–23.

14 Offene Innovationsprozesse für die IT-Sicherheit Kritischer Infrastrukturen – Impulse aus dem Projekt VeSiKi

Matthias Raß, Friedrich-Alexander-Universität Erlangen-Nürnberg
Albrecht Fritzsche, Friedrich-Alexander-Universität Erlangen-Nürnberg
Max Jalowski, Friedrich-Alexander-Universität Erlangen-Nürnberg
Kathrin M. Möslein, Friedrich-Alexander-Universität Erlangen-Nürnberg

14.1 Open Innovation

Unter dem Begriff „Open Innovation" werden heute in Forschung und unternehmerischer Praxis in erster Linie zwei bedeutende Paradigmen diskutiert und praktiziert. Eine der beiden Sichtweisen bezeichnet einen Ansatz, in dem Organisationen ihre Innovationsprozesse zumindest teilweise öffnen und dabei Abteilungs- und Organisationsgrenzen durchlässiger für den Fluss von Wissen und andere Ressourcen gestalten (Chesbrough 2003; Huff, Möslein & Reichwald 2013). Dieser Fluss kann in beide Richtungen stattfinden: von außen nach innen, also z. B. von externen Partnern zur Forschungs- und Entwicklungsabteilung einer Organisation, oder von innen nach außen, also z. B. von dieser Abteilung zu anderen Partnern. Auf diese Weise können externes Wissen, externe Ideen und Lösungsansätze anderer Beteiligter in die Entwicklung eigener Produkte oder Dienstleistungen einfließen, während es umgekehrt genauso möglich ist, dass internes Wissen oder interne Entwicklungen nicht zu marktreifen Produkten oder Dienstleistungen weiterentwickelt, sondern entgeltlich oder unentgeltlich veräußert und außerhalb der Organisation weiterentwickelt und kommerzialisiert werden. Werden beide Prozesse in einer dauerhaften Kooperation miteinander verzahnt, entstehen darüber hinaus noch viele zusätzliche Möglichkeiten für Innovation (Enkel, Gassmann & Chesbrough 2009). Mögliche externe Partner für Open Innovation sind auf institutioneller Ebene z. B. Universitäten und andere Forschungseinrichtungen, Zulieferer oder sogar Konkurrenten des betreffenden Unternehmens. Besonders wichtig sind aber auch Beiträge individueller Kunden oder Nutzer von Produkten und Dienstleistungen, die wertvolles Wissen über Bedürfnisse, praktikable technische Lösungen und die damit verbundenen Wertbeiträge in die Praxis einbringen. Zur Unterstützung von Open Innovation stehen viele verschiedene Instrumente zur Verfügung, die den Interaktionsprozess effizienter und effektiver gestalten (Möslein & Fritzsche 2017). Sie können nicht nur die Innovationsleistung erhöhen, sondern auch noch weitere positive Effekte haben, weil z. B. ein durch den Einsatz dieser Instrumente entstehendes und wachsendes Netzwerk eine für weitere Aktivitäten wertvolle soziale Ressource darstellt (Rass et al. 2013). Während Extremfälle bezüglich ihrer Innovationsaktivitäten völlig geschlossener und völlig offener Organisationen in der Realität kaum existieren, lässt sich doch eine zunehmende Öffnung organisationaler Innovationsaktivitäten feststellen.

Neben der unternehmensgetriebenen Open Innovation wird in der Forschung eine zweite Sichtweise verfolgt, die der ersten nicht widerspricht, aber mehr die Nutzer selbst in den Vordergrund stellt und beschreibt, wie diese auch ohne Unternehmenspartner eigene Lösungen

entwickeln, die für einen gewissen Markt relevant sind und mitunter auch mit Angeboten etablierter Firmen konkurrieren (von Hippel 2005; Huff, Möslein & Reichwald 2013). Diese Form könnte man auch als Proto-Stadium von Open Innovation im Sinne einer nutzergetriebenen Innovation bezeichnen, die später zur Entwicklung neuer institutioneller Strukturen führen kann. Häufig entstehen dabei durch den Austausch und die Zusammenarbeit mehrerer Nutzer obendrein eigene, oft eher informelle Organisationsformen, wie Netzwerke oder Communitys. Auch die Maker-Bewegung ist eine Ausprägung dieser Art offener Innovation. Ansätze wie Citizen Science bauen auf ähnlichen Prinzipien auf und beziehen Personen mit unterschiedlichen Hintergründen in wissenschaftliche Projekte ein. Hier haben sich über die Jahre schon verschiedenste Formen offener Forschung etabliert, die ein neues Verständnis von Experimenten und Labortätigkeit erfordern. Citizen Scientists arbeiten dabei häufig mit wissenschaftlichen Institutionen zusammen, weshalb auch bei diesem Ansatz ersichtlich wird, dass sich die beiden oben genannten Paradigmen nicht widersprechen, sondern lediglich verschiedene Perspektiven einnehmen.

14.2 Das Projekt VeSiKi

Im Bereich der IT-Sicherheit ist es unerlässlich, dass verschiedene Beteiligte über institutionelle Grenzen hinweg zusammenarbeiten. Diese Zusammenarbeit ist ein Kernthema des Begleitforschungsprojekts „Vernetzte IT-Sicherheit Kritischer Infrastrukturen" (VeSiKi) im Förderschwerpunkt „IT-Sicherheit für Kritische Infrastrukturen" (ITS|KRITIS). Im Projekt VeSiKi arbeiten Forscher der Universität der Bundeswehr München, der Friedrich-Alexander-Universität Erlangen-Nürnberg und der Universität Bremen sowie Experten der Deutschen Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE. Das Projekt vernetzt die Verbundprojekte des Förderschwerpunkts ITS|KRITIS und unterstützt den kooperativen Forschungs- und Entwicklungsprozess innerhalb des Förderschwerpunkts sowie die Kommunikation und Kooperation zwischen dem Förderschwerpunkt und der allgemeinen Öffentlichkeit. Darüber hinaus adressieren die Projektpartner in VeSiKi verschiedene eigene Fragestellungen. Der Lehrstuhl für Wirtschaftsinformatik, insbes. Innovation und Wertschöpfung, der Friedrich-Alexander-Universität Erlangen-Nürnberg beschäftigt sich unter anderem mit der Frage, wie über Prinzipien der Open Innovation den Herausforderungen und Potenzialen offener und kollaborativer Innovations- bzw. Forschungs- und Entwicklungsprozesse im Bereich der IT-Sicherheit Kritischer Infrastrukturen begegnet werden kann. Dabei geht es sowohl um die Interaktion zwischen Experten mit einem besonderen institutionellen Bezug zur Aufgabenstellung als auch um den Austausch mit der breiten Öffentlichkeit.

14.3 Das offene Labor als Innovationsmotor für IT-Sicherheit

Zahlreiche Forschungsarbeiten, die in den vergangenen Jahren zu Open Innovation und User Innovation entstanden sind, geben Einblick in die Möglichkeiten der Förderung organisationsübergreifender Forschungs- und Entwicklungstätigkeiten für die IT-Sicherheit kritischer

Infrastrukturen. Grundbedingung dafür ist es, Orte zu schaffen, an denen die Beteiligten sich treffen können. Das Projekt VeSiKi hat aufgezeigt, dass technische Plattformen, auf denen man im Internet miteinander kommunizieren kann, dafür nicht immer ausreichen. Dies erklärt sich durch die besondere Sensibilität des Themas und die Vielzahl der Möglichkeiten, wie das Wissen in diesem Bereich missbraucht und falsch verstanden werden kann. Um Vertrauen zu fördern, ist persönlicher Kontakt unerlässlich. VeSiKi hat dazu viele Möglichkeiten geschaffen, z. B. auf den Jahreskonferenzen des Förderschwerpunkts, weiteren Tagungen und Sonderveranstaltungen zur Förderung von Austausch und Innovation. Eine besondere Rolle spielte die Platzierung des Themas im offenen Innovationslabor JOSEPHS® in Nürnberg. JOSEPHS® ist eine dauerhafte Einrichtung in der Nürnberger Innenstadt, direkt an den Einkaufsmeilen in der Fußgängerzone und offen für alle Besucherinnen und Besucher, die Innovation mitgestalten wollen. Unter diesen „Co-Kreatoren" vor Ort befinden sich infolgedessen Personen mit ganz unterschiedlichen persönlichen und beruflichen Hintergründen, die das Labor gezielt oder auch zufällig betreten. Das Labor stellt einen flexibel nutzbaren Raum zur Verfügung, der auf ganz unterschiedliche Weise zur Umsetzung organisationsübergreifender Innovationsprozesse genutzt werden kann (Roth et. al. 2014).

14.4 Konzeption

Das Begleitforschungsprojekt VeSiKi hat sich der bestehenden Infrastruktur des offenen Innovationslabors JOSEPHS® bedient, um Vernetzung und Wissenstransfer zwischen individuellen und organisationalen Akteuren mit den verschiedensten Hintergründen zu fördern. Dabei wurden einerseits die bestehenden Netzwerke, Formate und Ressourcen des offenen Innovationslabors genutzt, andererseits aber auch gezielt weitere Netzwerke, Formate und Ressourcen integriert. Dieser Ansatz verfolgte mehrere Ziele. Zum einen sollte der Wissenstransfer vom Förderschwerpunkt und seinen Projekten in die Öffentlichkeit unterstützt werden. Zum anderen sollten aber auch Impulse, Ideen und Wissen von außen aufgenommen werden. Ähnliches galt für den Austausch zwischen Experten, der durch Einladung zu speziellen Veranstaltungen vorangetrieben wurde. Für die wissenschaftliche Forschung im Projekt war es natürlich auch von Interesse, aus dieser Art der Integration und Zusammenarbeit weitere Erkenntnisse über die Möglichkeiten offener Innovationsprozesse abzuleiten.

Das Projekt VeSiKi richtete eine Themeninsel ein, die über drei Monate hinweg den Kern der Präsenz im Labor darstellte und dabei einerseits das Bewusstsein der Besucher für das Themenfeld „IT-Sicherheit für Kritische Infrastrukturen" steigern und sie andererseits anregen sollte, eigene Ideen einzubringen. Dabei sollten sowohl die verschiedenen Facetten des Themenfelds und die Aktivitäten des Förderschwerpunkts ITS|KRITIS dargestellt als auch die Besucher in einem interaktiven Ansatz in konkrete Fragestellungen eingebunden werden.

Die Themeninsel bestand aus mehreren Komponenten: einer Simulation zur Einführung in das Thema, einer Interaktionswand mit verschiedenen Fragestellungen und zwei Demonstratoren von Verbundprojekten aus dem Förderschwerpunkt. Mithilfe der Simulation konnte das Eindringen in eine Kritische Infrastruktur und die Manipulation einer Kraftwerkssteuerung durch die Besucher selbst sowie mögliche Auswirkungen dieses Angriffs auf den eigenen

Alltag in einer Modellwelt demonstriert werden. Die Besucher wurden so an die Thematik herangeführt und für sie sensibilisiert. Dies wurde durch eine Faktenwand ergänzt, für die aktuelle Daten zur Lage der IT-Sicherheit Kritischer Infrastrukturen aufbereitet wurden.

Die Interaktionswand bestand aus drei Teilkomponenten: 1) einer Wand zur subjektiven Einschätzung der Relevanz, an der die Besucher quantitatives und qualitatives Feedback zur Bedeutung und zur Bedrohungslage der IT-Sicherheit in den verschiedenen KRITIS-Sektoren geben konnten, 2) einer Lösungswand, an der die Co-Kreatoren Ideen, Lösungsansätze und Problemstellungen beitragen konnten, und 3) einer Wand, an der die Besucher ihre individuellen privaten sowie beruflichen Erfahrungen mit Cyberangriffen berichten und einordnen sollten.

Die beiden Demonstratoren aus zwei Verbundprojekten des Förderschwerpunkts sollten den Besuchern einerseits aktuelle Entwicklungen der Forschung im Themenfeld „IT-Sicherheit für Kritische Infrastrukturen“ aufzeigen, sie andererseits aber auch zum ausgiebigen Test und zum Einbringen eigener Vorschläge motivieren.

Ergänzt wurde die Themeninsel um eine Veranstaltungsreihe zur IT-Sicherheit, in der in praxisnahen Workshops und Vorträgen die verschiedenen Aspekte dieses Forschungsfeldes thematisiert wurden. Die Veranstaltungen adressierten verschiedene Zielgruppen und die Formate reichten von Fachvorträgen z. B. zu den Themen Normung und Standardisierung über eine Live-Hacking-Demonstration für die breite Allgemeinheit bis hin zu einem „IT Security Youth Camp“ für Schüler während der Sommerferien.

14.5 Erkenntnisse

Die verschiedenen Möglichkeiten, wie sich Besucher des JOSEPHS® in das Thema einbringen konnten, boten die Grundlage zur Sammlung wertvoller Erkenntnisse. Zunächst wurde aus den Beiträgen der Besucher klar, dass das Thema IT-Sicherheit durchaus bei der Bevölkerung angekommen ist. Nutzer von IT-Systemen machen sich Gedanken über die Sicherheit ihrer Daten und die funktionale Integrität ihrer Systeme – sowohl im privaten als auch im beruflichen Bereich. Dabei besteht ein deutlich höheres Vertrauen in die Maßnahmen, die auf betrieblicher Seite für IT unternommen werden, als in die eigenen Maßnahmen im häuslichen Umfeld. Aus Gesprächen wurde beispielsweise klar, dass sich viele Menschen bewusst entschieden, wo sie kritische Transaktionen über das Internet durchführen. Den Vorzug erhalten Plattformen, die sie für sicher erachten, insbesondere diejenigen, die sie am Arbeitsplatz vorfinden. Daher haben sie auch ein persönliches Interesse daran, dass diese Plattformen gesichert sind. Dies ist von besonderer Bedeutung, weil die Aufmerksamkeit der Nutzer für Sicherheitsprobleme wesentlich zur Erkennung von Schwächen und Einleitung von Verbesserungsmaßnahmen beitragen kann.

Es zeigte sich allgemein, dass die Relevanz des Themas IT-Sicherheit Kritischer Infrastrukturen von den Besuchern nicht immer sofort eingeordnet werden konnte. Dies schien in erster Linie an dem für die meisten Besucher eher abstrakten Begriff „Kritische Infrastrukturen“ zu liegen. Des Weiteren sind Bedrohungen der IT-Sicherheit Kritischer Infrastrukturen für viele Besucher natürlich nur indirekt von Bedeutung. Eine Beeinträchtigung stellt sich für sie selbst

erst durch die Auswirkungen auf ihren Alltag ein. Die Unsicherheit der Besucher hinsichtlich des Begriffs „Kritische Infrastrukturen" und der Bedeutung des Themas für jeden Bürger konnte durch das Simulationsmodell und die informierenden Bestandteile der Forschungsinsel aufgeklärt werden. Hatten sie sich einmal Bedeutung und Zusammenhänge bewusst gemacht, konnten sie über das Thema diskutieren und eigene Überlegungen einbringen.

14.6 Fazit und Ausblick

Die Öffnung von Innovationsprozessen im Bereich IT-Sicherheit Kritischer Infrastrukturen hat nichts mit der Offenlegung sensibler Daten über den Betrieb der Infrastruktur zu tun, durch die Angreifer mehr Erkenntnisse über die Schwächen der entsprechenden Anlagen sammeln könnten. Vielmehr geht es darum, alle zur Verfügung stehenden Kräfte zur Verbesserung von IT-Sicherheit optimal zu bündeln. Neben Experten spielt auch die breite Bevölkerung dabei eine große Rolle. Kritische Infrastruktur geht alle an, und auch die Informationsnetze kritischer Infrastrukturen sind heute schon in vielen Fällen so gestaltet, dass sie viele Wechselwirkungen und Zugangsmöglichkeiten aus öffentlichen Netzen erlauben. Daher gibt es viele und unterschiedliche Personengruppen, die zu IT-Sicherheit beitragen können, sei es durch aktive Eingriffe in das Verhalten von IT-Systemen, durch Beobachtung oder auch ganz einfach durch die Beschäftigung mit dem Thema, durch die Aufmerksamkeit in der Bevölkerung hergestellt wird (Jalowski & Fritzsche 2016).

Die Nutzung des offenen Innovationslabors JOSEPHS® zeigt zahlreiche Wege auf, wie die Einbindung verschiedener Personengruppen in das Thema IT-Sicherheit vonstattengehen kann. Dabei wird klar, dass die technische Architektur der Systeme nicht im Vordergrund stehen muss. Nutzungs- und Bewertungsfragen hinsichtlich der Systeme sind genauso zu adressieren. Sie tragen ganz entscheidend zur Bestimmung der Stoßrichtung weiterer Sicherheitsmaßnahmen bei, die sich nicht allein aus Sicht der Technik ergibt. Die Innovationsforschung steht deshalb vor der Herausforderung, ganz unterschiedliche und jeweils passgenaue Konzepte von Open Innovation und User Innovation zu entwickeln, die den jeweiligen Anforderungen und dem Grad der Beteiligung entsprechen.

14.7 Danksagung

Wir danken dem Bundesministerium für Bildung und Forschung für die Möglichkeit der Forschung im Rahmen des Projekts VeSiKi (Förderkennzeichen 16KIS0214).

14.8 Literaturverzeichnis

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

Enkel, E.; Gassmann, O.; Chesbrough, H., 2009. Open R&D and Open Innovation: Exploring the Phenomenon. R&D Management, 39, S. 311–316.

Hippel von, E., 2005. Democratizing Innovation. Cambridge, MA: MIT Press.

Huff, A. S.; Möslein, K. M.; Reichwald, R., 2013. Leading Open Innovation. Cambridge, MA: MIT Press.

Jalowski, M.; Fritzsche A., 2016. Ein Rahmenwerk zur Erfassung von IT-Sicherheit als Service-System. Multikonferenz Wirtschaftsinformatik (MKWI).

Möslein, K. M.; Fritzsche, A., 2017. The Evolution of Strategic Options, Actors, Tools and Tensions in Open Innovation. In: Nicole Pfeffermann; Julie Gould (Hrsg.), Strategy and Communication for Innovation. Integrative Perspectives on Innovation in the Digital Economy, S. 61–76.

Rass, M.; Dumbach M.; Danzinger F.; Bullinger A. C.; Möslein K. M., 2013. Open Innovation and Firm Performance: The Mediating Role of Social Capital. Creativity and Innovation Management. 22(2), S. 177–194.

Roth, A.; Fritzsche A.; Jonas J. M.; Danzinger F.; Möslein K. M., 2014. Interaktive Kunden als Herausforderung: Die Fallstudie „JOSEPHS® – Die Service-Manufaktur“. HMD Praxis der Wirtschaftsinformatik. 51, S. 883–895.

15 IT-Sicherheit – Impulse für Innovation, Strategie und Zukunft

Ulrike Lechner, Universität der Bundeswehr München

Die strategische Dimension von IT-Sicherheit ist das Thema dieses Abschnitts, der Themen zu Strategie, Innovation und Zukunft der IT-Sicherheit aufgreift und Impulse setzen will. In den vorherigen Abschnitten des vorliegenden Buches haben neun Fallstudien und eine vergleichende Fallstudienanalyse Themen der IT-Sicherheit adressiert. Dieser Abschnitt schlägt die Brücke zu Strategie, Innovation und zu den strategischen Zukunftsthemen der IT-Sicherheit.

Für die strategischen Zukunftsthemen wurden mit Persönlichkeiten aus dem Beirat „IT-Sicherheit für Kritische Infrastrukturen" mündliche oder schriftliche Interviews geführt, um Informationen über Zukunftsstrategien aus der Sicht eines Betreibers Kritischer Infrastrukturen, über die Perspektive von Standardisierung und Normierung, über strategische Innovation sowie über rechtswissenschaftliche und ethische Positionen zu den Themen zu erhalten. Diese Antworten mit ihren Impulsen sollen in diesem Kapitel für sich stehen. Auf unsere Fragen haben geantwortet:

Florian Haacke ist Leiter Konzernsicherheit bei innogy SE. In dem Beirat „IT-Sicherheit für Kritische Infrastrukturen" vertritt er die Sicht großer Betreiber Kritischer Infrastrukturen und den Sektor Energie.

Andreas Harner leitet das VeSiKi Team bei VDE|DKE. Er hat beim VDE ein CERT für industrielle KMU aufgebaut und mit dem VDE|DKE will er durch Normung und Standardisierung Investitionen langfristig absichern und den Transfer von Forschungsresultaten in die Anwendung ermöglichen.

Prof. Dr. Dirk Heckmann ist Inhaber des Lehrstuhls für Öffentliches Recht, Sicherheitsrecht und Internetrecht an der Universität Passau und Mitglied des Bayerischen Verfassungsgerichtshofes sowie in der Ethikkommission „Vernetztes und Automatisiertes Fahren", die einen vielbeachteten Bericht mit Empfehlungen verfasst hat.

Dr. Uwe Jendricke vertritt beim Bundesamt für Sicherheit in der Informationstechnik (BSI) das Thema IT-Sicherheit Kritischer Infrastrukturen. Er ist in die Erstellung der branchenspezifischen Sicherheitsstandards für Kritische Infrastrukturen sowie den UP KRITIS, die Zusammenarbeit von Wirtschaft und Staat zum Thema Schutz Kritischer Infrastrukturen, involviert.

Prof. Dr. Kathrin Möslein leitet das VeSiKi-Team an der Friedrich-Alexander-Universität Erlangen-Nürnberg. Sie ist Inhaberin des Lehrstuhls für Wirtschaftsinformatik mit Schwerpunkt Innovation und Wertschöpfung und Vizepräsidentin für Forschung der Friedrich-Alexander-Universität Erlangen-Nürnberg.

Prof. Dr. Martin Wirsing ist Vizepräsident an der Ludwig-Maximilians-Universität München und Lehrstuhlinhaber für Programmierung und Softwaretechnik. Prof. Dr. Martin Wirsing ist Sprecher des Beirats „IT-Sicherheit für Kritische Infrastrukturen". Seine Forschung thematisiert formale Methoden und Anwendungen in adaptiven, serviceorientierten und autonomen „Self Aware"-Systemen.

15.1 Impulse zu Strategie „IT-Sicherheit"

In der IT-Sicherheit fühlt man sich an das Spiel von Hase und Igel erinnert. Neue Arten von Schadsoftware erfordern neue Maßnahmen und die Angreifer sind anscheinend der IT-Sicherheit einen Schritt in puncto Innovation und Technologie voraus. Unser Interesse gilt den Leitbildern und Strategien der IT-Sicherheit, die über das Hase-und-Igel-Spiel im täglichen Geschäft der laufenden Anpassung der IT-Sicherheit an die neuesten Bedrohungen hinausgehen.

Herr Prof. Wirsing, wir hören vor allem von kleineren Betreibern Kritischer Infrastrukturen. Jede IT braucht neue IT-Sicherheitsmaßnahmen, und neue IT und neue Sicherheitsmaßnahmen machen nur wieder neue Probleme und erhöhen das Risiko. Meine Steuerung und Regelungen können auch manuell bedient werden – wir brauchen und wollen keine neue IT. Bisher ging es ja auch ohne.

Prof. Dr. Martin Wirsing: Die Frage ist, wie lange Betreiber eine solche "IT-freie" Strategie durchhalten können. *Warum braucht man IT in einer modernen Geschäftswelt? Auch kleine und mittlere Betreiber von Kritischen Infrastrukturen können sich der Digitalisierung auf lange Sicht nicht entziehen, weil wir in einer vernetzten Gesellschaft leben. Je mehr Vernetzung es gibt, desto weniger kann man mit isolierten Lösungen anfangen. Vernetzte Lösungen lassen sich – anders als isolierte Lösungen – nicht mehr mechanisch regeln, dafür ist eine Steuerung mit IT notwendig. Ein Unternehmen, das Geld verdienen möchte, muss heute Aufträge elektronisch verarbeiten können und elektronisch erreichbar sein. Sobald ein Unternehmen aber vernetzt ist, ist es auch den Risiken der IT ausgesetzt.*

Der wesentliche Punkt ist: Eigentlich haben kleine Betriebe jetzt den Vorteil, dass sie Sicherheitsfragen von Beginn an berücksichtigen und ihre IT-Steuerungssysteme im Sinne von „Security-by-Design" entwickeln können. Das ist viel besser, als nachträglich Sicherheit in ein gewachsenes IT-System einbringen zu müssen.

Herrn Prof. Dr. Dirk Heckmann haben wir nach dem von ihm geprägten Begriff der Concordisierung gefragt, mit dem er auf dem Jahreskongress des Förderschwerpunkts ITS|KRITIS 2017 die strategische Relevanz von Sicherheit für die Innovationsfähigkeit beschrieben hat.

Herr Professor Heckmann, Sie haben den Begriff der „Concordisierung" von Technologien geprägt. Mit dem schrecklichen Unfall der Concorde wurde das Zeitalter einer vielbewunderten und vielgeliebten Technologie beendet. Sie beschreiben, eine Schubumkehr, die durch eine Tragödie ausgelöst werden kann und die dann alle Innovation zu diesem Thema als Folge davon undenkbar erscheinen lässt. Ist „Concordisierung" ein Thema für die Betreiber Kritischer Infrastrukturen in Deutschland?

Prof. Dr. Dirk Heckmann: Leider ja. Die vermeintlich nach oben offene Innovationsspirale kann ein jähes Ende finden, wenn das Vertrauen in eine Technologie nachhaltig erschüttert wird. Restrisiken sind beim Einsatz neuer Technologien nur hinnehmbar, wenn deren Realisierung als punktuelles Unglück wahrgenommen wird, das sich nur bedingt wiederholen wird (auch weil man daraus lernen kann) – so wie bei einem tragischen Flugzeugabsturz. Wenn aber etwa gezielte Angriffe auf digitalisierte Operationssäle mehrere Todesopfer zur Folge hätten, würde eine damit zum Ausdruck kommende Hilflosigkeit der Verantwortlichen in den Kliniken die Vertrauensfrage aufwerfen. Nicht zuletzt deshalb wird man in solchen Infrastrukturen angriffssichere Alternativsysteme vorhalten müssen.

Herr Haacke, welche Idee kann eine gleichzeitig zukunftsorientierte und pragmatisch umsetzbare Strategie eines Betreibers Kritischer Infrastrukturen anleiten? Absicherung existierender Infrastrukturen und Innovation – beides scheint wichtig. Was würden Sie Betreibern Kritischer Infrastrukturen empfehlen: erst „Aufräumen" – also alte Systeme ablösen zugunsten von Systemen, die leicht abzusichern sind, die Systeme absichern und dann erst Innovationen in Richtung der strategischen Zukunftsszenare oder Innovation und IT-Sicherheit gleichzeitig betreiben?

Florian Haacke: Alles sicher machen und dann aus dieser guten Position Zukunftsthemen angehen ist sicherlich wünschenswert, aber 100 % Sicherheit sind gerade in diesem dynamischen Umfeld nicht erreichbar. Neben den diversen Präventionsmechanismen einer modernen Sicherheitsarchitektur sind auch die intelligente Detektion und eine professionelle Incident Response ebenso wichtige Bestandteile. Die Erkennung bedingt gerade in komplexen und dynamischen Infrastrukturen eine sehr gute Orchestrierung. Auch hier gilt es, im Partnering mit anderen professionellen Marktteilnehmern stärker zu werden, insbesondere aufgrund der kritischen Komponente Zeit sowie der am Markt immer größer werdenden Komponente Skill Gap / Skill Shortage. Insofern muss gleichzeitig an einer permanenten Verbesserung des Reifegrades der bestehenden Infrastruktur und der konsequenten Implementierung von Security by Design für Innovationen gearbeitet werden, um in die Zukunft gerichtete, sichere Lösungen im Portfolio zu haben.

Herr Dr. Jendricke, in den Fallstudien zur IT-Sicherheit Kritischer Infrastrukturen werden immer wieder folgende Themen genannt: Mitarbeiter, das IT-Sicherheitsbewusstsein und Vertrauen in die Mitarbeiter, veraltete Systeme und veraltete Betriebssysteme ohne aktuelle Sicherheitspatches, Fernwartungszugänge und Schnittstellenüberwachung. Sind das Ihrer Meinung nach die wichtigsten Themen der IT-Sicherheit – dort wo es kurz- und mittelfristig den größten Handlungsbedarf gibt? Gibt es weitere Themen?

Dr. Uwe Jendricke: Großer Handlungsbedarf besteht insbesondere beim Thema veraltete Systeme und veraltete Betriebssysteme. Etwas allgemeiner formuliert ist dies das Thema „Security by design", was besagt, dass bei der Entwicklung von Systemen auch die Informationssicherheit ein zentraler Aspekt sein sollte. Sicherheit sollte nicht nachträglich in ein Produkt integriert werden müssen. Hersteller sollten Sicherheitsfunktionalitäten von

Beginn an vorsehen und über die gesamte Lebensdauer des Produkts unterstützen, z. B. durch verlässliches Patchen beim Bekanntwerden von Schwachstellen und eine klare Dokumentation von sicherheitsrelevanten Eigenschaften des Produkts. Die Bundesregierung unterstützt solche Aktivitäten beispielsweise durch das BSI-Gesetz, das die Entwicklung von branchenspezifischen Sicherheitsstandards für Kritische Infrastrukturen fördert. Hersteller können solche Regelwerke nutzen, um den Betreibern die Umsetzung dieser Standards zu erleichtern und ihre Produkte sicherer zu gestalten.

Frau Prof. Möslein, Innovationsfähigkeit ist ein strategisches Thema für den Wirtschaftsstandort Deutschland. Open Innovation, das ist das Konzept für das Ihr Lehrstuhl und die Service Manufaktur Josephs´ stehen – von den Erfahrungen in Open Innovation können auch Organisationen mit ihren IT-Sicherheitsprojekten lernen. Welche Erfahrungen aus Open Innovation und den Erfahrungen von Josephs´ würden Sie IT-Sicherheitsverantwortlichen für Projekte zur IT-Sicherheit ans Herz legen?

Prof. Dr. Kathrin Möslein: Lösungen zur Verbesserung der IT-Sicherheit werden oft unter strenger Geheimhaltung hinter verschlossenen Türen entwickelt. Damit wird ein immenses Innovationspotenzial verschenkt. Ich möchte die Verantwortlichen ermutigen, den Dialog mit anderen Experten, aber auch der breiten Öffentlichkeit zu suchen. Unsere Arbeiten im Projekt VeSiKi haben gezeigt, dass sich darauf viele neue Erkenntnisse und Impulse für Innovation ergeben können.

15.2 Impulse für „IT-sichere Systeme und Unternehmen“

Impulse zu neuen IT-Sicherheitskonzepten, zu strategisch und wirtschaftlich wichtigen Fragestellungen von Normen und Standards sowie zu einer nächsten Generationen von Technologie bildet den zweiten Abschnitt dieses Kapitels. Die Fragen thematisieren die strategischen Fragestellungen der Interviewpartner.

Herr Haacke, IT-Sicherheit ist ein komplexes Thema – das zeigen auch die Fallstudien zu ganz unterschiedlichen Fragestellungen in der IT-Sicherheit. Wie wählen Sie die IT-Sicherheitsprojekte für innogy aus? Ein Ergebnis der Fallstudien ist, dass IT-Sicherheitsprojekte „einfach“ sein sollen, wenig finanzielle und personelle Ressourcen binden, kaum Schulungsbedarf vorweisen sollen, die Technologie von den Mitarbeitern nicht nur angewandt, sondern beherrscht werden soll und es wenig Interaktion mit anderen Prozessen geben soll. Sind für Sie diese Kriterien auch wichtig – haben Sie andere oder weitere Kriterien für IT-Sicherheitsprojekte?

Florian Haacke: Alle Ihre Punkte sind richtig und wünschenswert und unsere Erfahrung zeigt, dass wir zudem noch auf weitere Punkte achten müssen.

IT in Unternehmen entsteht meist nicht in einem „grüne Wiese“-Ansatz. Sie ist oftmals über Jahrzehnte gewachsen und in Konzernstrukturen manchmal sogar hoch komplex. Unternehmensteile werden veräußert oder hinzugekauft, neue Technologien sind in immer kürzeren Zyklen verfügbar. Ein praktisches Beispiel sind die vielen Cloud-Lösungen.

Wir wählen unsere Sicherheitsprojekte risikobasiert aus. In vielen Fällen ist das leider noch sehr reaktiv. Unser Ziel ist es, Themen proaktiv zu treiben. Zu nennen sind hier Initiativen im Bereich des Mobile-Device-Managements, neue Netzwerkarchitekturen oder wie im Beispiel geschildert die sichere Nutzung von Cloud-Lösungen. Alle Projekte haben ihre individuellen Herausforderungen und bedingen unterschiedliche Herangehensweisen. Nicht nur der Betrieb ist hier von Bedeutung. Auch die heutige Softwareentwicklungslandschaft unterliegt einem großen Wandel. Agile Methoden in der Softwareentwicklung bedürfen neuer Verfahren, um „Security by Design" gewährleisten zu können. Hier unterscheidet sich ein klassisches Wasserfallprojekt doch erheblich von einem SCRUM-Projekt.

Auch wurden in den letzten Jahren in der Industrie immer mehr „Make or Buy"-Entscheidungen zugunsten von „Outsourcing-Partnern" getroffen. Was man früher noch seinem internen IT-Betrieb oder Entwicklungsbereichen einfach vorgegeben hat, muss man heute in der IT-Security Supply Chain vereinbaren, überprüfen und steuern. Hier ist jedes neue Outsourcing-Thema, insbesondere in der Anbahnung, ein eigenes Projekt.

Vergessen wir bei all den neuen Themen bitte nicht, dass Sicherheitsstandards, die einmal etabliert wurden, aufrechterhalten werden müssen. Neue Technologien oder sich sonst ändernde Rahmenbedingungen bedingen, dass wir unsere bestehenden guten Lösungen ständig kritisch hinterfragen müssen.

Es gibt eine Vielzahl von möglichen Projekten in dem sich ständig wandelnden Themenfeld und es ist für uns eine tägliche Herausforderung, stets die richtigen Themen zur richtigen Zeit anzugehen. Bei allen Projekten liegt der Fokus auf der nachhaltigen Steigerung des Reifegrades der Sicherheit bei gleichzeitiger Berücksichtigung der Kosteneffizienz des Projektes sowie der Bedien- und Beherrschbarkeit der Ergebnisse.

Herr Dr. Jendricke, Digitalisierung, Industrie 4.0 oder Autonomes und Vernetztes Fahren sind strategische Themen und Verbraucher sowie die Gesellschaft werden nur sichere Dienste akzeptieren. Absicherung existierender Infrastrukturen und Innovation – beides scheint wichtig. Was würden Sie Betreibern Kritischer Infrastrukturen empfehlen: erst „Aufräumen" – also alte Systeme ablösen zu Gunsten von Systemen die leicht abzusichern sind, die Systeme absichern und dann erst Innovationen in Richtung der strategischen Zukunftsszenare oder Innovation und IT-Sicherheit gleichzeitig betreiben?

Dr. Uwe Jendricke: Kritische Infrastrukturen sollten eher keine „Early Adopters" sein. Ganz neue Technologien weisen oft noch viele Sicherheitslücken auf. Gleichzeitig sollten aber auch keine veralteten Systeme genutzt werden, da die kritischen Dienstleistungen mit hoher Verfügbarkeit erbracht werden sollen. Die ideale Systemumgebung sollte daher aus modernen aber schon erprobten Systemen bestehen, die rechtzeitig vor dem Ende der Lebensdauer (und dem Ende von verfügbaren Sicherheitsupdates) ausgetauscht werden.

Herr Haacke hat mit Nachhaltigkeit, Sicherheit für ganze Supply Chains und sich ändernden Rahmenbedingungen einige – aus Sicht der Betreiber Kritischer Infrastrukturen – zentrale Themen adressiert. Investitionssicherheit durch Normen und Standards. Herr Harner, „Nor-

men und Standards" sind Ihr Thema in der IT-Sicherheit. In den Fallstudien ist immer wieder die Rede davon, dass all die Anforderungen zur IT-Sicherheit nur weitere Anforderungen neben anderen Zertifizierungen und gesetzlichen Regelungen sind. Was zeichnet „Normen und Standards" im Themenfeld der IT-Sicherheit im Gegensatz zum Thema Normen und Standards in anderen Themenfeldern aus?

Andreas Harner: IT-Sicherheit ist ein Prozess, bei dem es notwendig ist, alle Beteiligten entlang den Wertschöpfungsketten an einen Tisch zu bekommen. Es genügt nicht, nur den Betreiber einer KRITIS bzw. den Hersteller oder Integrator die IT-Sicherheit normen zu lassen: es müssen vielmehr alle Rollen involviert werden, um eine durchgängige Sicherheit definieren und umsetzen zu können. Das Involvieren aller Stakeholder gelingt auf der Kollaborationsplattform der Normung. Darüber hinaus sind branchenspezifischer Austausch und Beachtung staatlicher Regelsetzer von großer Wichtigkeit, um Akzeptanz und Anwendung entstehender Normen zu garantieren. Eine Herausforderung für die Normung der Zukunft wird sein, die Anforderungen der „kryptographischen Agilität" in den Normungsprozess zu integrieren.

Herr Dr. Jendricke, das IT-Grundschutzkompendium ist das neue Referenzwerk zur IT-Sicherheit Kritischer Infrastrukturen. Welche drei Bausteine würden Sie den Betreibern Kritischer Infrastrukturen besonders ans Herz legen, weil Sie den größten Gewinn an Sicherheit für die Kritischen Infrastrukturen bringen?

Dr. Uwe Jendricke: Die Auswahl der für eine Organisation relevanten IT-Grundschutz-Bausteine ist einer von mehreren Teilen der Sicherheitskonzeption, die z. B. im BSI-Standard 200-1 beschrieben ist. Welche Bausteine für eine Organisation relevant sind, ergibt sich also aus der Art und dem Aufbau der Organisation, jede Institution wird daher andere Bausteine als besonders wichtig erachten. Aus der Erfahrung mit KRITIS empfehle ich den Betreibern insbesondere die folgenden Bausteine:

- *ISMS.1 Sicherheitsmanagement mit Hinweis auf Produktion: traditionell werden ISMS eher in Office-Umgebungen betrieben. Viele KRITIS-Betreiber erbringen ihre kritischen Dienstleistungen jedoch nicht mit Office-Anwendungen. Oftmals werden Spezialsysteme eingesetzt und viele Anlagen enthalten industrielle Steuerungssysteme (ICS). Es ist jedoch trotz hoher IT-Durchdringung von Produktionsumgebungen noch nicht selbstverständlich, dass diese Anlagen in den Geltungsbereich eines ISMS integriert werden. Um die Cybersicherheit in der Produktion (und damit die Verfügbarkeit der kritischen Dienstleistung) zu gewährleisten, sollte ein ISMS auch die Produktion miterfassen.*
- *DER.1 Detektion von sicherheitsrelevanten Ereignissen: die Analyse von Cybersicherheitsvorfällen zeigt, dass IT-Angriffe oft lange unentdeckt bleiben. Dies ist insbesondere bei professionelleren Angriffen der Fall. Der Schaden ist dann entsprechend hoch, da bereits viel Information abgeflossen sein kann und viele Systeme durch die Angreifer*

verändert wurden. Essenziell ist daher eine zügige Entdeckung von Angriffen, um das Schadensausmaß (und daraus resultierende Ausfälle) gering zu halten.

– *IND: Chance für strukturierte Absicherung von Produktionsumgebungen: Cybersicherheit von Produktionsanlagen ist immernoch ein relativ neues Thema. Traditionell kommt die Cybersicherheit aus der Office-Welt. Die Sicherheitskultur muss in Produktionsanlagen oftmals erst etabliert werden. Insbesondere für KRITIS-Betreiber ist dies essenziell, da die Systeme der kritischen Dienstleistungen möglichst nicht ausfallen dürfen. Industrielle Steuerungssysteme erfordern jedoch andere Cybersicherheitsmaßnahmen als Office-Systeme. So muss beispielsweise oftmals die Echtzeitfähigkeit erhalten bleiben, was u. a. durch Antivirensysteme gestört werden kann. Hier helfen die IND-Bausteine, die Sicherheitsmaßnahmen speziell für Produktionsumgebungen liefern.*

Herr Harner, welche Erfolge konnten in den letzten Jahren im Themenfeld der Normen und Standards erreicht werden und auf welche Themenbereiche der IT-Sicherheit wirken sie sich aus?

Andreas Harner: Im Bereich der Energietechnik konnte aufgrund der deutschen Initiative bei der DKE die internationale Norm ISO/IEC 27019 beim JTC 1 der ISO/IEC erfolgreich eingebracht und umgesetzt werden. Diese sektorspezifische Ableitung der ISO/IEC 27002 hilft Energieunternehmen, das ISMS auch im Bereich der Prozess-IT (Prozess- und Leittechnik) umzusetzen. Darüber hinaus entwickeln sich bei IEC die Normenreihen IEC 62351 („Standard für Sicherheit in Energiemanagementsystemen und zugehörigem Datenaustausch") und 62443 („Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme") zu Pilotnormen, die weit über Ihren Anwendungsbereich Beachtung finden.

Frau Prof. Möslein, die Fallstudien zur IT-Sicherheit Kritischer Infrastrukturen thematisieren Innovationen für mehr Sicherheit – Inwiefern lassen sich die Erfahrungen aus Open Innovation auf Innovationen in der IT-Sicherheit übertragen?

Prof. Dr. Kathrin Möslein: Viele Erkenntnisse, die wir in der Managementforschung über den Einsatz von Open Innovation gewonnen haben, lassen sich auch auf IT-Sicherheit anwenden. Eine Zusammenarbeit über organisationale Grenzen hinweg schafft immer zusätzlichen Aufwand und muss gut geplant und gesteuert werden. Wir wissen inzwischen aber sehr genau, wie man dabei vorgehen muss und an welchen Stellen die Risiken lauern. Bei IT-Sicherheit lässt sich vieles, was wir gelernt haben, genauso gut nutzen wie in anderen Anwendungsfällen, gerade im Ingenieursbereich. Wichtig ist, über den Horizont der technischen Entwicklung hinauszudenken. Innovation ist am Ende des Tages immer auch eine wirtschaftliche und soziale Herausforderung, die nur über die Einbindung unterschiedlicher Interessengruppen erfolgreich gestaltet werden kann.

Herr Prof. Wirsing, neue Technologie adaptiver Systeme ist eines Ihrer Forschungsgebiete. Innovative Technologien für IT-Sicherheit sind Thema der Fallstudienserie. Sehen Sie Chancen für lernende Systeme oder für selbst-adaptive Systeme?

Prof. Dr. Martin Wirsing: Lassen Sie mich zunächst allgemein über den Einsatz lernender Systeme reden und dann auf die Sicherheitsaspekte eingehen.

Lernende Systeme sind immer dann nützlich, wenn der Mensch keine gute Spezifikation erstellen kann oder wenn sich Planungsaufgaben nicht vollständig mit klassischen Algorithmen lösen lassen. Ein Beispiel *ist die dezentrale Energieversorgung, bei der es viele lokale Energieproduzenten gibt, die gleichzeitig auch Energieverbraucher sind. Ein solches System kann nicht mehr a priori zentral gesteuert werden, sondern muss adaptiv an die aktuelle Situation angepasst werden. Ein anderes Beispiel sind große Produktions- und Lagerhallen mit autonom agierenden Robotern. Hier sind lernende Systeme sowohl zur Produktionssteuerung als auch zur Gewährleistung der Sicherheit einsetzbar.*

*Natürlich gibt es noch eine Reihe von Problemen: z. B. ist es schwierig, lernenden Systemen Grenzen zu setzen. Lernende Systeme könnten Strategien lernen, die gegen die Gesetze verstoßen. Ein Beispiel: Alle Bürger einer Stadt zahlen Steuern, mit denen u. a. die Infrastruktur, wie etwa Straßen und Schwimmb*äder, gepflegt wird. *Die Bürger geben Geld und profitieren gleichzeitig von der Infrastruktur;* Bürger, die keine Steuern zahlen, profitieren aber mehr. Für ein lernendes System wäre das optimal und *es würde die Strategie lernen, keine Steuern zu zahlen und so den Profit zu maximieren. Security-by-Design würde in diesem Fall bedeuten, dass man sich die Auswirkungen lernender Systeme* überlegt und ihnen Regeln mitgibt, die falsches Verhalten bestrafen. Auch das ist nicht immer ausreichend; es gibt große *Unternehmen, die lieber eine Strafe zahlen – für sie manchmal „nur Peanuts" –, als die Gesetze einzuhalten. Deshalb sollte man lernende Systeme so gestalten, dass sie sich an die Regeln halten.*

Man kann sich gut vorstellen, dass Angreifer von Kritischen Infrastrukturen lernende Systeme einsetzen. Zum Beispiel könnten in einem großen Netz mit vielen zusammenwirkenden Knoten lernende, adaptive Systeme Angriffe entdecken, die auf subtil unterschiedliche Weise verschiedene Komponenten angreifen, so dass jede einzelne Steuerung zwar noch fast einwandfrei arbeitet, aber die Gesamtheit nicht mehr funktioniert und zusammenbricht. In solchen „emergenten" sicherheitskritischen Situationen sollten die Sicherheitssysteme für Kritische Infrastrukturen selbst Lerntechniken verwenden, um das Angreiferverhalten verstehen zu lernen und sich so gegen lernende Angreifer zu verteidigen. Das Motto ist hier: Lieber einen intelligenten als einen kräftigen Verteidiger, der leicht ausgetrickst werden kann.

15.3 Impulse für Innovationen – die Zukunft der IT-Sicherheit

Die Zukunft der IT-Sicherheit mit den Themen und den offenen Fragen, die Betreiber Kritischer Infrastrukturen, Technologieanbieter und auch die Politik und Gesetzgebung noch adressieren sollten, ist Thema dieses dritten Abschnitts. Zu dem Zeitpunkt, als diese Fragen

gestellt wurden, fanden in Deutschland Sondierungen und Verhandlungen zu einer neuen Regierung statt. Welches Thema müsste in einer gesellschaftlichen Debatte adressiert werden? Welches Thema würden Sie einer Regierung gerne für ihre Agenda empfehlen?

Herr Haacke, Innovation und IT-Sicherheit schließen sich nicht gegenseitig aus – gerade bei den Unternehmen die als Kritische Infrastrukturen spezielle Sicherheitsanforderungen erfüllen müssen. In der Fallstudienserie sticht eine Fallstudie heraus – hier wurde ein innovativer digitaler Prozess umgesetzt, der kosteneffizienter und einfach besser war als der alte Prozess und gleichzeitig sicher. Weitere Fallstudien thematisieren die Absicherung von existierenden Technologien oder generell Sicherheitskulturen. Was zeichnet erfolgreiche Projekte in der IT-Sicherheit aus? Wie ist das Verhältnis von „einfach absichern" zu Projekten, die gleichzeitig „innovativ und sicher" sind?

Florian Haacke: Ich würde hier noch weiter gehen. Nicht nur, dass Innovation und IT-Sicherheit sich nicht gegenseitig ausschließen, sondern dass Innovation ohne Sicherheit nicht funktioniert. Würden Sie sich eine „Smart Home"-Anwendung anschaffen, bei der Sie nicht sicher sind, ob ein Dritter die Steuerung übernehmen kann? Viele Menschen haben das Buch „Blackout" von Marc Elsberg gelesen. Hier wird beschrieben, wie innovative Lösungen im Bereich von Kritischen Infrastrukturen so manipuliert werden, dass die Steuerung des Netzes unmöglich wird und es zu einem großflächigen Stromausfall in nahezu ganz Europa kommt. So ein Angriff wäre vor wenigen Jahrzehnten noch undenkbar und wirklich fiktiv gewesen, da die Netzsteuerung analoger und dezentraler stattfand. Heute haben wir innovative Lösungen, die eine digitale Echtzeitsteuerung ermöglichen. Das hat viele Vorteile, birgt aber auch in Bezug auf Cybersicherheit Risiken, denen wir uns stellen müssen.

Prof. Dr. Katrin Möslein: Das Thema Digitalisierung genießt in der Politik bereits große Aufmerksamkeit. Das ist sehr gut so. Im Bereich der IT-Sicherheit hat das BSI bereits vorbildliche Arbeit geleistet und die neue Regierung tut sicher gut daran, es auch in Zukunft tatkräftig dabei zu unterstützen. Genauso wichtig ist es aber auch, den Aufbau von Fachkompetenz durch neue Studiengänge an den Hochschulen zu unterstützen und die Entwicklung des wachsenden Markts für IT-Sicherheit in Deutschland so anzuleiten, dass hier neue Arbeitsplätze und Verdienstmöglichkeiten entstehen. Auch das ist ein wesentlicher Motor für Innovation!

Prof. Dr. Martin Wirsing: Deutschland ist ein hochtechnisiertes Land, in dem ein großer Teil der wirtschaftlichen Produktivität von IT-Systemen abhängt, die immer mehr vernetzt und deren Angriffsflächen damit immer größer werden. In den letzten Jahren haben wir eine Reihe von Cyberangriffen auf Kritische Infrastrukturen gesehen; manche davon könnten sogar von Nationalstaaten initiiert worden sein.
Darum sollte die Sicherheit von IT-Systemen oberste Priorität besitzen. Es ist wichtig, dass wir an unseren Hochschulen qualifizierte Sicherheitsspezialisten ausbilden, die IT-Systeme möglichst gut schützen können. Wir *brauchen außerdem gesetzliche Anforderungen, die die Entwickler verpflichten, sichere IT-Systeme zu bauen. Notwendig* wäre ein

Gesetz *zur Sicherheit von IT-Systemen in Analogie zur Datenschutzgrundverordnung. Softwareentwickler müssten für jedes IT-System ein bestimmtes Sicherheitsniveau garantieren; bestehende Altsysteme müssten sukzessive auf ein verbessertes Sicherheitsniveau gehoben werden. Gerade bei Kritischen Infrastrukturen wird die Qualität der IT-Sicherheit ein zentrales Thema bleiben – mit großen Herausforderungen und vielen Chancen.*

Prof. Dr. Dirk Heckmann: Ich plädiere für eine unaufgeregte, von akuten Anlässen losgelöste, sachlich abwägende politische und gesellschaftliche Debatte über das „citius, altius, fortius" der Digitalisierung. Wir müssen Risiken offen aussprechen und zugleich über Lösungen nachdenken, die Chancen der Digitalisierung gemeinverträglich zu nutzen. Derzeit gibt es zu viel „Schwarz-Weiß-Malerei", indem etwa die Risiken einseitig verteufelt und die Chancen unkritisch in den Himmel gehoben werden. Die Gewährleistung von IT-Sicherheit zum Beispiel gehört zu den allergrößten Herausforderungen einer digitalen Gesellschaft und einer digitalen Wirtschaft. Im Rahmen eines von Bundesamt für Sicherheit in der Informationstechnik geförderten wissenschaftlichen Projekts erstellen unter meiner Projektleitung die Universität Passau und das Helmholtz Zentrum i. G. Center for IT-Security, Privacy and Accountability in Saarbrücken Leitlinien für eine wirksame IT-Sicherheitsregulierung. Wir werden in diesem Projekt auch eine Debatte mit Akteuren aus Gesellschaft, Wirtschaft und Politik anstoßen.

Andreas Harner: Industrie 4.0 und Digitalisierung eröffnen große Chancen – gerade für den deutschen Wachstumsmotor, den Mittelstand. Zugleich steigt mit der fortschreitenden Vernetzung von Produktionssystemen mittels moderner IKT-Systeme das Risiko von Cyber-Angriffen. Umso wichtiger ist es, IT-Sicherheit als kritischen Erfolgsfaktor für Industrie 4.0 und Digitalisierung zu stärken: zum einen durch eine verbesserte Prävention bei der Systementwicklung, zum anderen durch eine möglichst schnelle, strukturierte und professionelle Reaktion bei Bekanntwerden neuer Sicherheitslücken.

Während große Unternehmen und öffentliche Institutionen über eigene spezialisierte Sicherheits- und Notfallteams (Computer Emergency Response Team, CERT) verfügen, fehlen KMU dafür in aller Regel die notwendigen Ressourcen. Zudem fehlt es dort oft an Routine im Umgang mit Schwachstellen, von der Entgegennahme von Schwachstellen-Meldungen über die weitere Kommunikation mit den Meldenden (z. B. externen Sicherheitsforschern oder sogenannten „White Hat"-Hackern), die Erstellung von Sicherheitswarnmeldungen (Advisories), bis hin zur Koordination mit anderen, ebenfalls betroffenen Herstellern und mit anderen CERTs, wie dem ICS-CERT in den USA.

An dieser Stelle setzt CERT@VDE an, die erste Plattform zur Koordination bei IT-Security-Problemen im Bereich der Industrieautomation: CERT@VDE unterstützt im Umgang mit IT-Sicherheitsschwachstellen über Organisationsgrenzen hinweg. Was das einzelne KMU nicht leisten kann, bietet CERT@VDE durch Kooperation und Vernetzung. Solche Initiativen, die sich direkt an den Mittelstand richten und den Mittelstand unterstützen, ein hohes Niveau der IT-Sicherheit zu erreichen und zu halten, werden immer wichtiger. Solche Initiativen für den Mittelstand müssen gefördert werden.

16 Instrumente für die Beratung und Analyse

Sebastian Dännart, Universität der Bundeswehr München

Grundlage für die Erstellung einer Fallstudie nach der CASE|KRITIS-Methode ist die Datenerhebung in Form von Experteninterviews, teilnehmender Beobachtung und Literaturrecherche. Um diese Daten bereits von Beginn der Feldstudie an zu strukturieren und ihnen einen einheitlichen Rahmen zu geben, werden zwei Templates mit grundlegenden Gliederungen und Hinweisen zur inhaltlichen Gestaltung zur Verfügung gestellt.

Mit diesen Instrumenten ist es möglich, auf effiziente Weise Ist-Aufnahmen und Retrospektiven für die Beratung in Fragen der IT-Sicherheit zu erstellen und zugleich für eine spätere Analyse – auch über mehrere Fallstudien hinweg – eine gute Vergleichbarkeit zu gewährleisten.

Durch die hohe Individualität der einzelnen Fälle und die unterschiedlichen Schwerpunkte bei der Betrachtung, werden die Templates in der Regel nicht unverändert genutzt werden können. Sie bieten hingegen einen Startpunkt und eine Orientierungshilfe, um zu guten Ergebnissen im Prozess der Erstellung von CASE|KRITIS-Fallstudien zu gelangen.

Im Folgenden werden die Templates jeweils mit kurzen Hinweisen zum Inhalt zur Verfügung gestellt. Die CASE|KRITIS-Methode wird in Kapitel 3 dieses Buches beschrieben.

16.1 Template – Typ unternehmensbezogen

Kapitel 1 Unternehmen

Kapitel 1.1 Unternehmensprofil

Inhalt dieses Kapitels

- Unternehmensprofil
- Unternehmensgröße / Mitarbeiterzahl
- Branche / Produkte
- Zielgruppe / Kundenstruktur
- Sektor

Kapitel 1.2 Strategische Ausrichtung

Inhalt dieses Kapitels

- Unternehmensvision
- Internationalisierung
- Selbstbild des Unternehmens
- Innovationsfähigkeit

Kapitel 1.3 Fallstudienpartner

Name	Position im Unternehmen	Kontakt

Kapitel 2 Kritische Infrastruktur

Kapitel 2.1 Einordnung als KRITIS

Inhalt dieses Kapitels

- Kritische Infrastruktur – Warum ist das Unternehmen als kritische Infrastruktur einzustufen?
- Sektor – Zu welchem Sektor der kritischen Infrastrukturen gehört das Unternehmen?
- Kritische Bereiche – Welche Bereiche Ihres Unternehmens stufen Sie als kritisch ein?
- Selbstwahrnehmung – Als wie kritisch stufen Sie ihr Unternehmen ein?

Kapitel 2.2 Risikoanalyse

Inhalt dieses Kapitels

- Abhängigkeiten – Welche Abhängigkeiten / Schnittstellen (zu anderen kritischen Infrastrukturen) gibt es?
- Auswirkungen eines Ausfalls – Unternehmensintern / Gesellschaftlich – Was würde ein Ausfall bestimmter Bereich bedeuten?
- Adressierte Risiken

Kapitel 3 IT-Sicherheit

Kapitel 3.1 IT-Infrastruktur

Inhalt dieses Kapitels

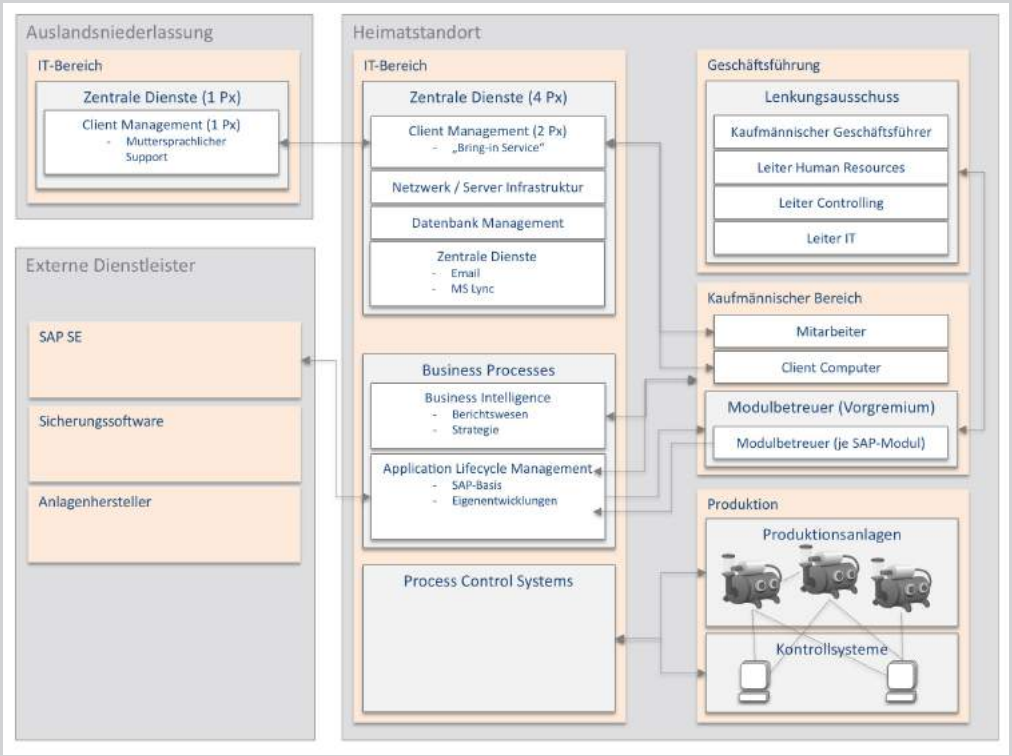
- Wie sieht die IT-Infrastruktur des Unternehmens aus?
- Bitte orientieren Sie sich an den Beispielen in den folgenden Unterkapiteln.

Kapitel 3.2 Geschäftssicht

Inhalt dieses Kapitels

- Wie sieht die IT-Infrastruktur im Unternehmen aus?
- Wie sieht das Zusammenspiel aller Beteiligten aus?
- Welche (externen) Partner sind beteiligt?

Beispielgrafik

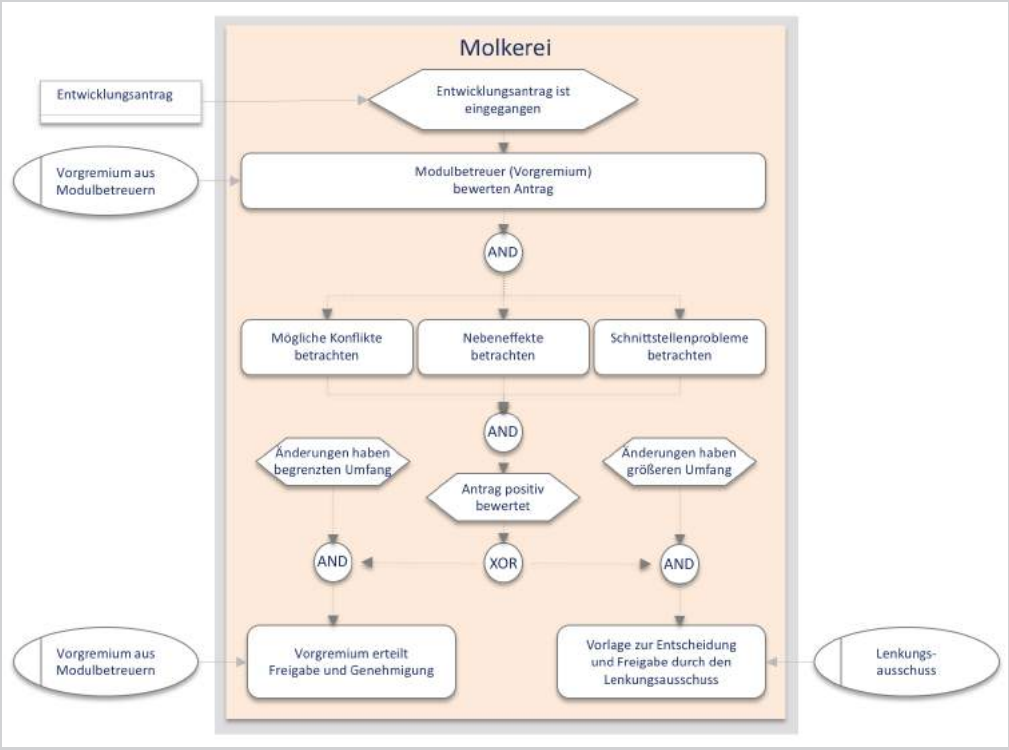


Kapitel 3.3 Prozesssicht

Inhalt dieses Kapitels

- Welche IT-Sicherheitsprozesse gibt es bereits im Unternehmen?
- Welche anderen Prozesse werden von diesen Prozessen beeinflusst?

Beispielgrafik

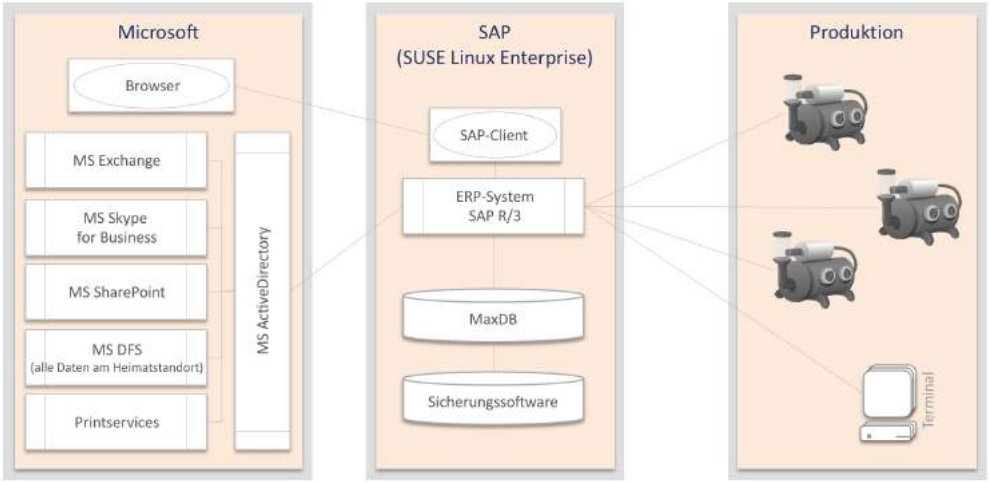


Kapitel 3.4 Anwendungssicht

Inhalt dieses Kapitels

- Wie sieht die IT-Anwendungslandschaft im Unternehmen aus?
- Welche speziellen IT-Sicherheitsanwendungen sind bei Ihnen im Einsatz?
- Welche Schnittstellen gibt es zwischen den Anwendungen und nach außen?

Beispielgrafik

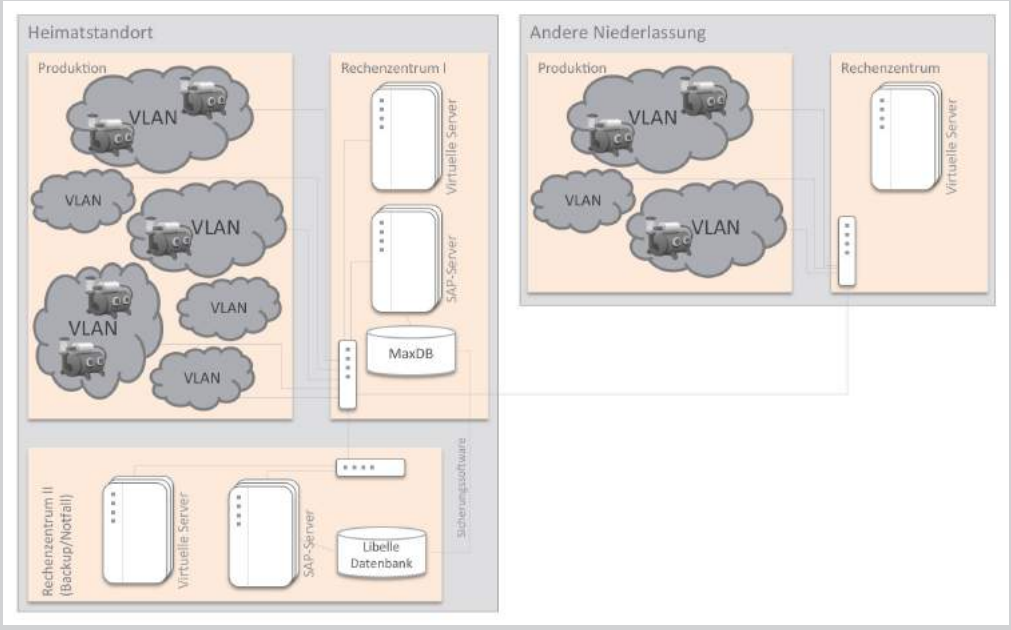


Kapitel 3.5 Technische Sicht

Inhalt dieses Kapitels

- Wie sieht die Verteilung der technischen Komponenten aus?
- Wie sind die verschiedenen Bereiche untereinander vernetzt?
- Wo sind Schnittstellen in andere Netze?
- Welche IT-Sicherheitssysteme sind verbaut?

Beispielgrafik



Kapitel 3.6 Normen, Standards und Gesetze

Inhalt dieses Kapitels

- Compliance – Welche Normen und Gesetze finden im Unternehmen bereits Anwendung? (ISOs, ITSiG etc.)
- Rahmenwerke – Ist Ihre IT nach gängigen Rahmenwerken organisiert? (CoBiT, ITIL, BSI etc.)
- Evaluation – Auditing / PenTesting / Zertifizierung

Kapitel 3.7 Stand der IT-Sicherheit

Inhalt dieses Kapitels

- Umsetzung – Wie wird die IT-Sicherheit umgesetzt?
- Risiken – Welche IT-Sicherheitsrisiken sehen Sie speziell in Ihrem Unternehmen?
- Maßnahmen – Welche IT-Sicherheitsmaßnahmen werden bereits aktiv umgesetzt?
- Maßnahmenebene – Auf welcher Ebene wurde die Maßnahme durchgeführt?
- Sicherheitsvorfälle – Gab es bereits Sicherheitsvorfälle? Welche? Wie wurden sie abgewehrt?
- Projekte – Sind bislang bereits Projekte abgeschlossen? Werden aktuell Projekte durchgeführt oder sind zukünftig Projekte geplant?
- Projekte – Was waren / sind die Auslöser für diese Projekte? (Sicherheitsvorfall, neuer Threat, Infrastrukturumstellung etc.)
- Awareness – Werden Mitarbeiterschulungen durchgeführt?

Kapitel 4 Erfolgsfaktoren

Inhalt dieses Kapitels

- Praxisrelevanz – Haben sich die bisherigen Maßnahmen in der Praxis bewährt?
- Anwenderakzeptanz – Wie wird die IT-Sicherheit im Unternehmen gelebt?
- Lessons Learned – Gibt es spezielle Besonderheiten in dieser Fallstudie?
- Best Practice – Kann die Lösung für andere KRITIS ein Vorbild sein?

16.2 Template – Typ projektbezogen

Kapitel 1 Unternehmen

Kapitel 1.1 Unternehmensprofil

Inhalt dieses Kapitels

- Unternehmensprofil
- Unternehmensgröße / Mitarbeiterzahl
- Branche / Produkte
- Zielgruppe / Kundenstruktur
- Sektor

Kapitel 1.2 Strategische Ausrichtung

Inhalt dieses Kapitels

- Unternehmensvision
- Internationalisierung
- Selbstbild des Unternehmens
- Innovationsfähigkeit

Kapitel 1.3 Fallstudienpartner

Name	Position im Unternehmen	Kontakt

Kapitel 1.4 IT-Sicherheit im Unternehmen

Inhalt dieses Kapitels

- Welche verschiedenen IT-Systeme nutzen Sie im Unternehmen? (ICS, ERP, Office-IT, Kommunikation etc.)
- Wie sind die Systeme untereinander vernetzt? Bestehen Schnittstellen zu anderen Unternehmen und ins Internet?
- Compliance – Welche Normen und Gesetze finden im Unternehmen bereits Anwendung? (ISOs, ITSiG etc.) Ist Ihre IT nach gängigen Rahmenwerken organisiert? (CoBiT, ITIL, BSI etc.)
- Umsetzung – Wie wird die IT-Sicherheit umgesetzt?
- Risiken – Welche IT-Sicherheitsrisiken sehen Sie speziell in Ihrem Unternehmen?
- Maßnahmen – Welche IT-Sicherheitsmaßnahmen werden bereits aktiv umgesetzt?
- Awareness – Werden Mitarbeiterschulungen durchgeführt?

Kapitel 2 Kritische Infrastruktur

Kapitel 2.1 Einordnung als KRITIS

Inhalt dieses Kapitels

- Kritische Infrastruktur – Warum ist das Unternehmen als kritische Infrastruktur einzustufen?
- Sektor – Zu welchem Sektor der kritischen Infrastrukturen gehört das Unternehmen?
- Kritische Bereiche – Welche Bereiche Ihres Unternehmens stufen Sie als kritisch ein?
- Selbstwahrnehmung – Als wie kritisch stufen Sie ihr Unternehmen ein?

Kapitel 2.2 Risikoanalyse

Inhalt dieses Kapitels

- Abhängigkeiten – Welche Abhängigkeiten / Schnittstellen (zu anderen kritischen Infrastrukturen) gibt es?
- Auswirkungen eines Ausfalls – unternehmensintern / gesellschaftlich – Was würde ein Ausfall bestimmter Bereich bedeuten?
- Adressierte Risiken

Kapitel 3 Projekt

Kapitel 3.1 Beschreibung

Inhalt dieses Kapitels

- Freie Beschreibung des Projektes
- Wird das Projekt intern oder mit externer Hilfe durchgeführt?

Kapitel 3.2 Projektziel

Inhalt dieses Kapitels

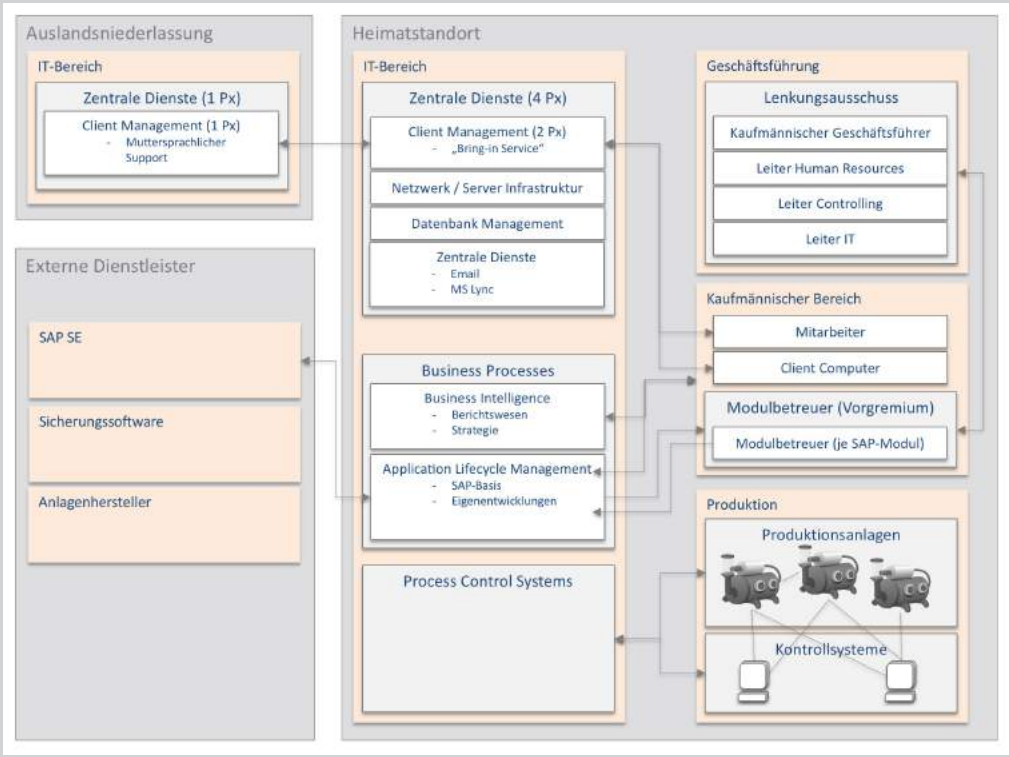
- Was ist das Ziel des Projektes?
- Welche Bereiche des Unternehmens werden tangiert?
- Welche bestehenden IT-Sicherheitsmaßnahmen werden beeinflusst?

Kapitel 3.3 Geschäftssicht

Inhalt dieses Kapitels

- Wie ordnet sich das Projekt in die Unternehmensstruktur ein?
- Wie sieht das Zusammenspiel aller Beteiligten rund um das Projekt aus?
- Welche (externen) Partner sind beteiligt?

Beispielgrafik

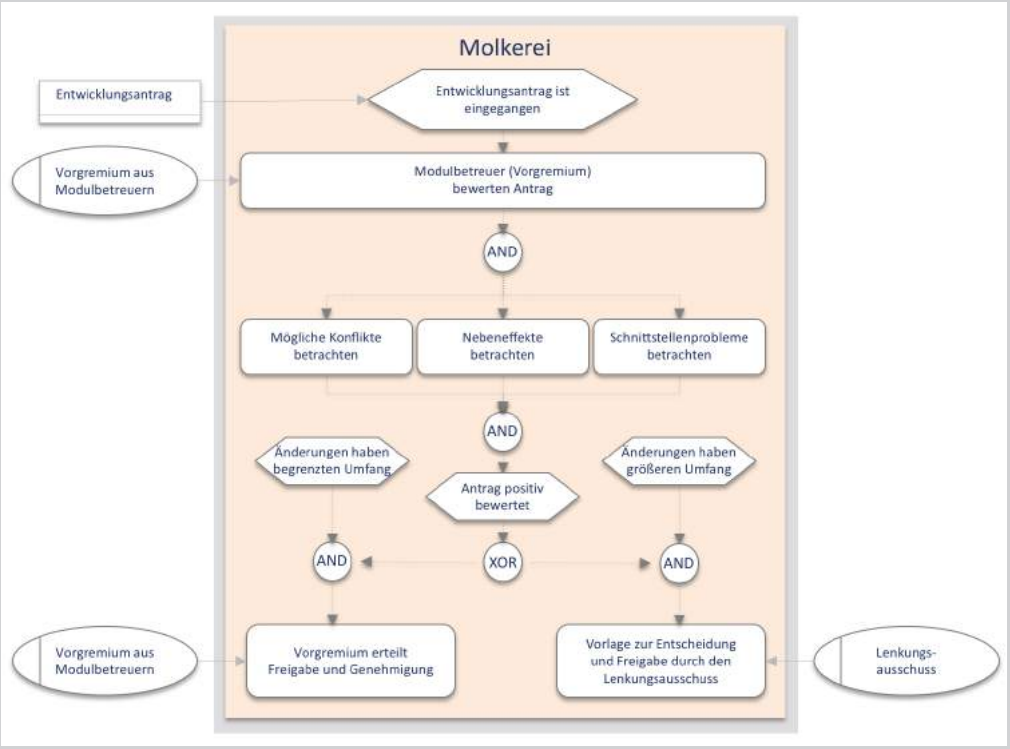


Kapitel 3.4 Prozesssicht

Inhalt dieses Kapitels

- Welcher Prozess wird von dem Projekt abgedeckt?
- Welche anderen Prozesse werden von dem Projekt beeinflusst?
- Gibt es prozessuale Schnittstellen zu anderen Projekten?

Beispielgrafik

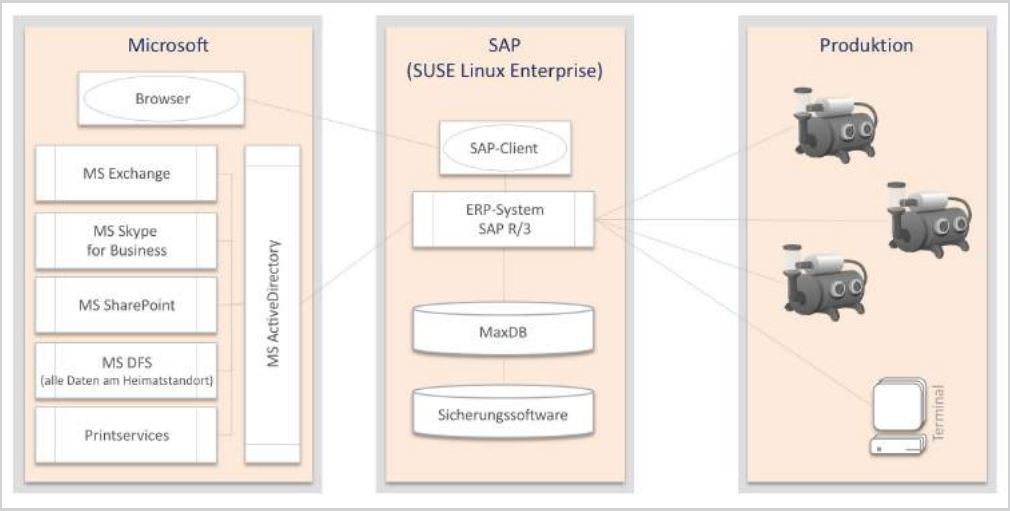


Kapitel 3.5 Anwendungssicht

Inhalt dieses Kapitels

- Welchen Bereich der Anwendungslandschaft des Unternehmens betrifft das Projekt?
- Welche Schnittstellen gibt es nach außen?

Beispielgrafik

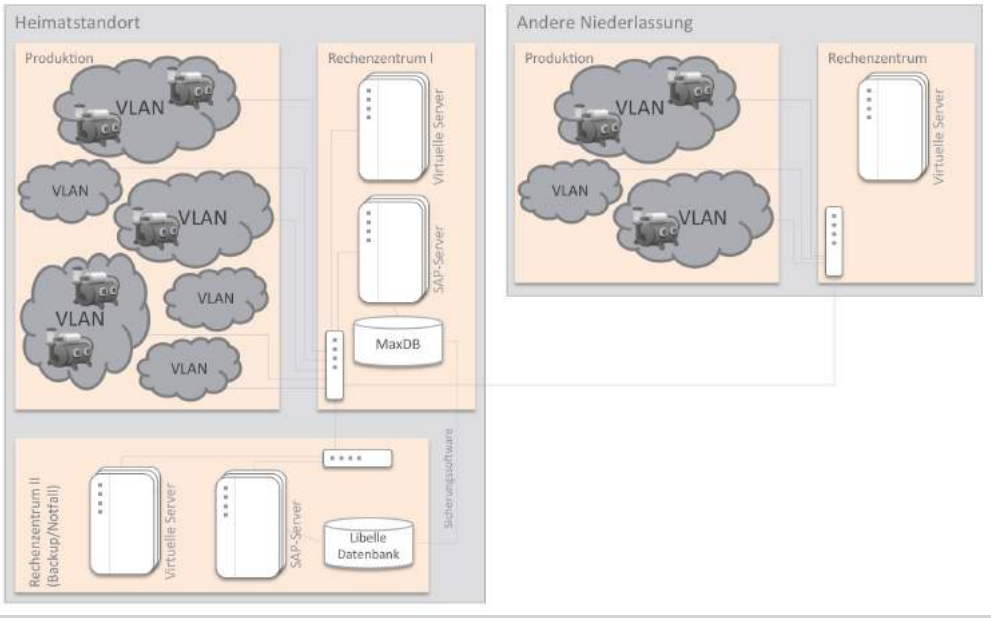


Kapitel 3.6 Technische Sicht

Inhalt dieses Kapitels

- Wie sieht die Verteilung der technischen Komponenten aus?
- Wie sind die verschiedenen Bereiche miteinander vernetzt?
- Wo sind Schnittstellen in oder andere Netze?
- Welche IT-Sicherheitssysteme sind verbaut?

Beispielgrafik



Kapitel 3.7 Umfang und Zeitraum

Inhalt dieses Kapitels

- Wie viel Zeit ist für das Projekt eingeplant?
- Wie viele Personenmonate sind für das Projekt eingeplant?
- Wie hoch sind die Kosten des Projektes?
- Wann erwarten Sie eine Amortisation des Projektes? ROI?

Kapitel 3.8 Vorgehen und Umsetzung

Inhalt dieses Kapitels

- Wie sieht / sah der Projektplan aus?
- Wie wurde das Projektmanagement betrieben?
- Waren Vorbereitungen nötig?
- Wie wurde vorgegangen? (Big Bang / modular / funktional etc.)
- Welche Unternehmensprozesse wurden beeinflusst?
- Wurde die Architektur beeinflusst?
- Wie wurde die Anwendungslandschaft beeinflusst?
- Wurden Schulungen durchgeführt?

Kapitel 3.9 Projektergebnis

Inhalt dieses Kapitels

- Was waren die wesentlichen Ergebnisse des Projektes?
- Gab es Schwierigkeiten bei der Einführung?
- Konnte das Ziel erreicht werden?
- Gibt es Folgeprojekte? (erweiternd / aufbauend etc.)

Kapitel 4 Erfolgsfaktoren

Inhalt dieses Kapitels

- Praxisrelevanz – Haben sich die bisherigen Maßnahmen in der Praxis bewährt?
- Anwenderakzeptanz – Wie wird die IT-Sicherheit im Unternehmen gelebt?
- Lessons Learned – Gibt es spezielle Besonderheiten in dieser Fallstudie?
- Best Practice – Kann die Lösung für andere KRITIS ein Vorbild sein?

17 Fazit und Zukunft

Ulrike Lechner, Universität der Bundeswehr München
Sebastian Dännart, Universität der Bundeswehr München
Andreas Rieb, Universität der Bundeswehr München
Steffi Rudel, Universität der Bundeswehr München

17.1 Fazit aus den CASE|KRITIS-Fallstudien

Neun Fallstudien von erfolgreichen Vorhaben zur IT-Sicherheit und eine vergleichende Analyse dieser neun Fallstudien sind der Kern der Fallstudienserie CASE|KRITIS in diesem Buch. Eine kurze Einführung zu wichtigen Themen der IT-Sicherheit in Kritischen Infrastrukturen und Instrumente für die Praxis zur Durchführung von Analysen im Format einer CASE|KRITIS-Fallstudie sowie Anmerkungen zu strategischen Fragestellungen der Umsetzung von IT-Sicherheit vervollständigen die Fallstudienserie.

In den neun CASE|KRITIS-Fallstudien spielt die IT-Sicherheit die Hauptrolle – die Fallstudien jedoch gehen über die IT-Sicherheit hinaus: Sie vergegenwärtigen die strategische Bedeutung von Sicherheit für Unternehmen in Innovationen und in der Digitalisierung. Ohne Sicherheit sind die modernen Strategien der Digitalisierung nicht denkbar, denn die Gesellschaft wird Innovationen mit Risiken nicht akzeptieren. Das betonen auch die Anmerkungen zu Strategie und Innovationen. IT-Sicherheit ist eines der zentralen Themen der Digitalisierung und so helfen auch die Fallstudien, die in einem Zeitraum entstanden sind, als Unternehmen die Auswirkungen von Cyberangriffen auf Kritische Infrastrukturen erleben konnten, es auch zu Ausfällen in der Versorgung mit Produkten und Dienstleistungen kam und in der vonseiten der Gesetzgebung, der Forschung und vor allem der Kritischen Infrastrukturen große Anstrengungen unternommen wurden, das Niveau der IT-Sicherheit der Kritischen Infrastrukturen schnell zu erhöhen und dafür die notwendigen Konzepte, den rechtlichen Rahmen und Technologien verfügbar zu machen. Diese Fallstudien und die Ergebnisse sind ein Baustein für erfolgreiche Digitalisierungsstrategien.

Fallstudien sind gute Geschichten und im Falle der CASE|KRITIS-Fallstudien gute Geschichten zu erfolgreichen Projekten, in der Praxis bewährten Produkten und gelebten Unternehmenskulturen mit dem gemeinsamen Thema „IT-Sicherheit in Kritischen Infrastrukturen". Die Fallstudien machen als Instrument einer ganzheitlichen Analyse ein erfolgreiches Vorhaben greifbar und machen das sichtbar, was sonst häufig im Verborgenen liegt:

- die Ressourcen ebenso wie die Innovationsfähigkeit, die in der Praxis erforderlich sind, um die Sicherheit Kritischer Infrastrukturen zu gewährleisten, sie immer wieder aktuellen Anforderungen entsprechend zu erhöhen, aber auch um die Anforderungen des IT-Sicherheitsgesetzes zu erfüllen,
- die Ressourcen, die Kosten und vor allem die personellen Aufwände für Implementierung und operativen Betrieb von IT-Sicherheitslösungen,
- den Nutzen von Maßnahmen für die Erhöhung des Niveaus der IT-Sicherheit und darüber hinaus für die Unternehmensstrategie,

- Tipps aus der Praxis von Betreibern Kritischer Infrastrukturen und ihren sicherheitsbewussten Mitarbeitern, die die abstrakten Sicherheitskonzepte für Unternehmen und speziell für kleine und mittlere Unternehmen handhabbar machen,
- dass IT-Sicherheit ein spannendes Thema ist, in dem innovative Technologie ebenso wie Management, Durchsetzungsfähigkeit der Mitarbeiter mit Sicherheitsverantwortung und gute Geschäftsprozesse gleichermaßen gefordert sind,
- das Verantwortungsbewusstsein, mit dem Unternehmen und ihre Mitarbeiter IT-Sicherheit betreiben, die Kreativität und Innovationskraft, die hier sichtbar werden und vor allem die Bereitschaft und der Wille, über das Geforderte hinauszugehen und in Sicherheit zu investieren.

Die Fallstudien sollen Mut machen, das gerade von kleineren und mittleren Unternehmen als abstrakt und schwierig wahrgenommene Thema der IT-Sicherheit mit der notwendigen Entschlossenheit und auch mit der notwendigen Innovationskraft anzugehen. Den Unternehmen, die selbst schon IT-Sicherheitsprojekte erfolgreich realisiert und vielleicht schon einen hohen Stand der IT-Sicherheit erreicht haben, können die CASE|KRITS-Fallstudien, die Analyse und die Templates helfen, ihr Vorgehen und ihre Lösungen zu reflektieren und beides weiter zu verbessern. So weit gehörte das zu der ursprünglichen Idee für diese Fallstudienserie. Prof. Dr. Martin Wirsing, Sprecher des Beirats, hat in Diskussionen zu diesen Fallstudien betont, warum diese Fallstudienserie gerade für Unternehmen relevant ist, die bisher Digitalisierung und IT-Sicherheit nicht als strategische Priorität ansehen – die Unternehmen haben jetzt die Chance, es gleich richtig zu machen.

Mit der Fallstudienserie wollten wir – die Editoren dieses Buches – erfolgreiche IT-Sicherheitslösungen analysieren und vor allem greifbar machen: einerseits für die Praxis und hier vor allem für Unternehmen, die das Niveau ihrer IT-Sicherheit erhöhen wollen, und andererseits für Studierende und Dozierende.

17.2 Ausblick in die Zukunft

Wie kann die Zukunft der IT-Sicherheit aussehen? Die Fallstudien zeigen, dass Unternehmen über die gesetzlichen Anforderungen hinausgehen – Sicherheit nicht nur verwalten, sondern mehr tun, als gesetzlich gefordert ist. IT-Sicherheitsprojekte erbringen Nutzen über die IT-Sicherheit hinaus: Sie vermindern Komplexität, machen Prozesse moderner oder engagieren alle Mitarbeiter in neuen Formen der Zusammenarbeit. Die Fallstudien – zusammen mit den Ergebnissen der beiden Studien Monitor und Monitor 2.0 der IT-Sicherheit für Kritische Infrastrukturen (VeSiKi 2018; VeSiKi 2017) illustrieren, dass die Anforderungen des IT-Sicherheitsgesetzes überwiegend als realistisch eingeschätzt werden. So haben sich in den Fallstudien mehrere Partner für die Sicherheit eher ein Mehr an Regulierung gewünscht, um tatsächlich den Stand der IT-Sicherheit erhöhen zu können. Die zweite Studie Monitor 2.0 hat das bestätigt. Für die Mehrheit der Studienteilnehmer tut die Gesetzgebung zu wenig oder sogar viel zu wenig für die IT-Sicherheit – das betrifft die Mehrheit aller Studienteilnehmer, ebenso wie die Mehrheit der Vertreter von KRITIS-Unternehmen und auch der kleineren

und mittleren Unternehmen. Die meisten Studienteilnehmer halten auch ihr Budget für IT-Sicherheit für nicht ausreichend und planen, es zu erhöhen. Die Mehrheit der Studienteilnehmer fordert darüber hinaus mehr Forschung für die IT-Sicherheit. Die Betreiber Kritischer Infrastrukturen möchten mehr für die Sicherheit tun!

Einen weiteren Ausblick in die Zukunft der IT-Sicherheit in Kritischen Infrastrukturen fasst der ebenfalls im Förderschwerpunkt IT-Sicherheit für Kritische Infrastrukturen ITS|KRITS entstandene „State of the Art: IT-Sicherheit für Kritische Infrastrukturen" (Rudel & Lechner 2018) zusammen. Hier stellen alle 13 Projekte des Förderschwerpunktes in 5 Sektionen

- die Forschungsprojekte selbst mit ihren Inhalten sowie den Projektpartnern vor,
- den Bezug zu den IT-Grundschutzkatalogen und dem IT-Grundschutzkompendium des BSI her,
- die adressierten KRITIS-Sektoren mit ihren Ausprägungen und Besonderheiten dar,
- die Werkzeuge und Methoden der Forschungsprojekte vor und
- die Referenzimplementierung dieser Werkzeuge und Methoden in der Praxis dar und geben einen Ausblick in die Zukunft.

Der State of the Art erweitert damit die vorliegende Fallstudienserie um den Blick „in die Wissenschaft" und zeigt somit mögliche Wege der KRITIS in der Zukunft auf.

Das Thema IT-Sicherheit ist und bleibt also ein wichtiges Thema – geopolitische Entwicklungen ebenso wie ein Trend hin zur Cyberkriminalität werden es notwendig machen, nächste Schritte zu tun – die Anforderungen an die IT-Sicherheit zu erhöhen und neue Technologien bereitzustellen, die es für alle Unternehmen möglich machen, das notwendige und geforderte Niveau der IT-Sicherheit umzusetzen. Eine Gemeinsamkeit weisen hier alle Fallstudien auf: Die Betreiber nehmen ihre Verantwortung ernst und die IT-Sicherheitslösungen in den Fallstudien gehen über das, was gesetzlich gefordert ist, hinaus. Die Betreiber wollen das Möglichste für die IT-Sicherheit tun und das lässt positiv in die Zukunft blicken. Die Kritischen Infrastrukturen in Deutschland sind sicher, das soll so bleiben und – wenn wir diese Fallstudien ansehen – dann wird das auch so bleiben.

17.3 Literaturverzeichnis

Rudel, S.; Lechner, U., 2018. IT-Sicherheit für Kritische Infrastrukturen. State of the Art. Ergebnisse des Förderschwerpunkts IT-Sicherheit für Kritische Infrastrukturen ITS|KRITIS des BMBF. Neubiberg: Universität der Bundeswehr München.

VeSiKi, 2018. Monitor 2.0 IT-Sicherheit Kritischer Infrastrukturen, U. Lechner (Hrsg.). Universität der Bundeswehr München. Verfügbar unter: monitor.itskritis.de [zugegriffen: 7-Juni-2018].

VeSiKi, 2017. Monitor IT-Sicherheit Kritischer Infrastrukturen, U. Lechner (Hrsg). Neubiberg: Universität der Bundeswehr München. Verfügbar unter: monitor.itskritis.de [zugegriffen: 7-Juni-2018].

Kritische Infrastrukturen bilden das Rückgrat unserer Gesellschaft. Fallen sie aus, kaskadieren die Auswirkungen schnell und können katastrophale Folgen haben. Wie andere Unternehmen sind auch Kritische Infrastrukturen weitgehend von Informationstechnik durchdrungen und nicht selten von deren fehlerfreier Funktion abhängig. Es wundert somit nicht, dass auch der Gesetzgeber angemessene Maßnahmen verlangt. Aber welchen speziellen Herausforderungen stehen Kritische Infrastrukturen dabei gegenüber? Und wie kann diesen wirksam und effizient begegnet werden?

Dieses Buch bündelt neun Lösungen aus der Praxis, die Good Practices von Betreibern Kritischer Infrastrukturen, beispielgebende Projekte und Technologien aufzeigen und deren Erfolgsfaktoren mögliche Antworten auf diese Fragen geben.

FACHBEITRÄGE ZU FOLGENDEN THEMEN

- ↗ Gesetzliche Anforderungen an die IT-Sicherheit in Deutschland und Europa
- ↗ Stand der Technik im Bereich der IT-Sicherheit Kritischer Infrastrukturen
- ↗ Umsetzung im Unternehmen: Von der IT-Sicherheit zu Innovation

ITS KRITIS | VeSiKi

Gefördert vom
Bundesministerium für Bildung und Forschung

Logos Verlag Berlin | ISBN 978-3-8325-4727-1