IT-Sicherheit für Kritische Infrastrukturen – State of the Art

Ergebnisse des Förderschwerpunkts IT-Sicherheit für Kritische Infrastrukturen ITS|KRITIS des BMBF

Steffi Rudel, Ulrike Lechner

Impressum

ISBN Print: 978-3-943207-33-0
ISBN Elektronisch: 978-3-943207-34-7

Herausgeberinnen:
Dr. Steffi Rudel, Prof. Dr. Ulrike Lechner

Projekt:
„Vernetze IT-Sicherheit Kritischer Infrastrukturen“
VeSiKi des BMBF, Förderkennzeichen 16KIS0213K

Professur für Wirtschaftsinformatik, Universität der Bundeswehr München

Kontakt:
Professur für Wirtschaftsinformatik
Universität der Bundeswehr München
Werner-Heisenberg-Weg 39
85577 Neubiberg

https://www.unibw.de/wirtschaftsinformatik

1. Auflage, September 2018

Layout:
Nuno de Mendoça, Artes Advertising GmbH
Arnulfstr. 199, 80634 München

Lektorat:
Dr. Heiner Lohmann Lektorat & Textagentur
Coerdestr. 50, 48147 Münster

Druck:
press enter OE+W GmbH
Frankenthaler Str. 20, 81539 München

IT-Sicherheit für Kritische Infrastrukturen – State of the Art

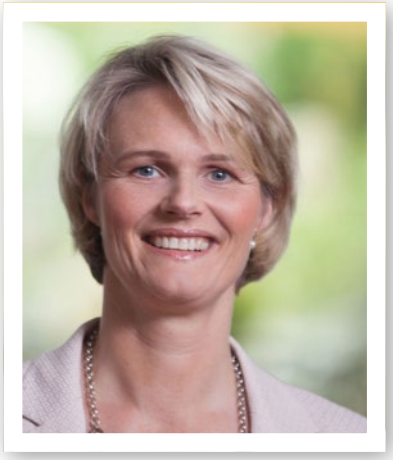
Ergebnisse des Förderschwerpunkts IT-Sicherheit für Kritische Infrastrukturen ITS|KRITIS des BMBF

Steffi Rudel, Ulrike Lechner

Inhaltsverzeichnis

Einleitung		8
Sektion 1	ITS|KRITIS-Projekte und deren Schwerpunkte in der IT-Sicherheit	14
Sektion 2	KRITIS-Bausteine der IT-Sicherheit	34
Sektion 3	Die KRITIS-Sektoren und ihre Spezifika	52
Sektion 4	Der Transfer in die Praxis	80
Sektion 5	Referenzimplementierung und Ausblick	116

Vorwort



Anja Karliczek
Bundesministerin für Bildung und Forschung – MdB

Ob Strom, Wasser oder Informationen: Wenn sie einmal nicht fließen, wie wir es gewohnt sind, kann das gravierende Auswirkungen auf unsere ganze Gesellschaft haben. Um uns mit diesen Gütern zuverlässig zu versorgen, nutzen die Betreiber Kritischer Infrastrukturen inzwischen die neuen digitalen Möglichkeiten. Die dadurch zunehmende Abhängigkeit von moderner Informations- und Kommunikationstechnik birgt jedoch auch Risiken. So erleben wir, dass mit der steigenden Vernetzung auch die Zahl der Cyberangriffe steigt.

Kritische Infrastrukturen sind besonders attraktive Angriffsziele für Kriminelle, Terroristen und ausländische Aggressoren. Der Schutz Kritischer Infrastrukturen vor Cyberangriffen ist ein wichtiges Ziel des Forschungsrahmenprogramms der Bundesregierung zur IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt 2015-2020".

Besonders kleinere Betreiber Kritischer Infrastrukturen, wie kommunale Wasser- oder Energieversorger, stehen vor großen Herausforderungen. Sie in einen intensiven Austausch mit anderen Betreibern, Wissenschaftlern und Forschern zu bringen, zählt zu den Zielen des Forschungsschwerpunktes „IT-Sicherheit für Kritische Infrastrukturen", den das Bundesministerium für Bildung und Forschung mit über 24 Millionen Euro fördert. Wichtig sind Dialog und Transparenz: Nur durch einen regen Erfahrungsaustausch und die Veröffentlichung von Sicherheitsvorfällen können Risiken erfolgreich erkannt und beseitigt sowie neue innovative IT-Sicherheitslösungen erforscht und entwickelt werden.

In insgesamt zwölf Forschungsprojekten haben Hochschulen, Forschungseinrichtungen und Infrastrukturbetreiber aus den Bereichen Energie und Gas, Finanzen und Versicherungen, Wasser, öffentliche Verwaltung und Verkehr gemeinsam neue Ideen entwickelt. Die vielfältigen und praxisnahen Ergebnisse stellt dieses Buch vor. Sie zeigen, wie Kritische Infrastrukturen in Zukunft vernetzt, geschützt und verlässlich funktionieren können – zum Wohle der gesamten Gesellschaft.

Anja Karliczek
Bundesministerin für Bildung und Forschung
Mitglied des Deutschen Bundestages

Geleitwort

Arne Schönbohm
Präsident des BSI

Nichts ist so beständig wie der Wandel. Das gilt insbesondere für den Wandel durch die Digitalisierung. Die Chancen für unseren gesellschaftlichen, wissenschaftlichen und wirtschaftlichen Fortschritt sind immens. Doch neben Chancen gibt es auch Risiken, und die müssen beherrschbar bleiben.

Das BSI als die nationale Cyber-Sicherheitsbehörde gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft. Wir wissen, dass die vergangenen Jahre von IT-Sicherheitsvorfällen geprägt waren wie nie zuvor. Die Vorfälle waren oft schwerwiegend und selten auf Deutschland beschränkt. Es traf unter anderem Krankenhäuser in Großbritannien, Energieversorger in der Ukraine, einen der weltweit größten Logistiker, Banken, Pharmaunternehmen und Stahlproduzenten. Cyberkriminalität, Cyberspionage gegenüber Staat und Wirtschaft und provozierte Ausfälle Kritischer Infrastrukturen sind eine ernstzunehmende Bedrohung unserer Gesellschaft im 21. Jahrhundert.

Wir haben in Deutschland im internationalen Vergleich ein gutes IT-Sicherheitsniveau. Doch auf schon Erreichtem dürfen wir uns nicht ausruhen. Die hohe Dynamik in der Entwicklung der Informationstechnik lässt es nicht zu, dass moderne Wirtschaftsnationen auf dem Gebiet der Digitalisierung und IT-Sicherheit stillstehen. Wir müssen auch künftig unsere rechtlichen, technischen und personellen Möglichkeiten zur Gestaltung der Digitalisierung und zur Gewährleistung weitreichender IT-Sicherheit fortentwickeln. Ein zentraler Bestandteil dieser Entwicklung ist die Forschung. Sie steht bei der Digitalisierung an prominenter Stelle, da ihre Ergebnisse oft den Anfang der Produktentwicklung bilden. Der Förderschwerpunkt „IT-Sicherheit für Kritische Infrastrukturen“ leistet hierzu wertvolle Arbeit. Ich begrüße es ausdrücklich, dass in den Forschungsprojekten des Förderschwerpunkts bereits Betreiber, Hersteller, Verbände und die Politik mitwirken. Ein sichtbares Ergebnis dieser Arbeiten ist der hier vorliegende State of the Art. Dieses Buch und die weiteren Aktivitäten aus dem Förderschwerpunkt bieten zahlreiche Möglichkeiten, die Ergebnisse der Sicherheitsforschung frühzeitig und effektiv in neue Produkte und Dienste zu integrieren. Dies ist ein starker positiver Impuls, um der Cyber-Sicherheit auch zukünftig bei den Kritischen Infrastrukturen einen hohen Stellenwert einzuräumen.

Arne Schönbohm,
Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Liebe Leserinnen und Leser,

die Kritischen Infrastrukturen in Deutschland gehören zu den sichersten der Welt. Das soll so bleiben – insbesondere auch angesichts des Themenfelds der IT-Sicherheit Kritischer Infrastrukturen.

Die Betreiber Kritischer Infrastrukturen nehmen ihre Verantwortung ernst. Denn die zunehmende Durchdringung aller Lebens- und Arbeitsbereiche durch Informations- und Kommunikationstechnologien bestimmt maßgeblich den technologischen Fortschritt und die Innovationsfähigkeit. Weite Bereiche des gesellschaftlichen und wirtschaftlichen Lebens hängen von robusten und resilienten Informations- und Kommunikationstechnologien ab. Der Schutz Kritischer Infrastrukturen vor Cyberangriffen ist für die selbstbestimmte und sichere Zivilgesellschaft lebensnotwendig.

Ulrike Lechner
Universität der Bundeswehr München

Das vorliegende Buch fasst die Forschungsergebnisse des Förderprogramms „IT-Sicherheit für Kritische Infrastrukturen“ (ITS|KRITIS) des Bundesministeriums für Bildung und Forschung (BMBF) zusammen:

- Betreibern Kritischer Infrastrukturen und IT-Sicherheitsverantwortlichen gibt es einen Überblick über die Forschungsergebnisse und damit über die nächste Generation von IT-Sicherheitstechnologien.
- Technologieanbietern zeigt es neue Konzepte der IT-Sicherheit und Kooperationsmöglichkeiten im Themenfeld der IT-Sicherheit Kritischer Infrastrukturen auf.
- Forschenden gibt es einen Überblick über den State of the Art der IT-Sicherheit Kritischer Infrastrukturen.
- Der Öffentlichkeit vermittelt das Buch einen Eindruck von dem Themenfeld der IT-Sicherheit, den spezifischen Anforderungen und den Herausforderungen und was durch die Forschung der Verbundprojekte und die Förderung durch das BMBF erreicht werden konnte.

Steffi Rudel
Universität der Bundeswehr München

Wir – die Herausgeberinnen dieses Buches und die Forscherinnen und Forscher des Projekts VeSiKi – möchten mit diesem Buch einen Beitrag zur IT-Sicherheit der Kritischen Infrastrukturen in Deutschland leisten. Wir möchten uns an dieser Stelle für die Förderung beim Bundesministerium für Bildung und Forschung bedanken. Wir danken dem Beirat für die wichtigen Impulse. Wir danken allen Betreibern Kritischer Infrastrukturen, allen Technologieanbietern und allen Forschungspartnern in den Forschungsprojekten, dass sie zu dem kooperativen Forschungsprozess beigetragen haben und damit diesen State of the Art möglich machten.

Ulrike Lechner und **Steffi Rudel,**
Begleitforschung VeSiKi

Einleitung

Die fortschreitende Digitalisierung in Gesellschaft und Arbeitswelt birgt zahlreiche Potenziale für die wirtschaftliche Entwicklung und die Verbesserung der Lebensbedingungen in der modernen Welt, bringt aber auch eine Reihe neuer Herausforderungen mit sich. Je stärker sich Menschen und Organisationen in ihrem Alltag auf Informationstechnik (IT) verlassen, desto mehr rückt die Frage der Sicherheit dieser Technik in den Fokus. Dabei geht es sowohl um ein fehlerfreies Funktionieren als auch um den Schutz dieser Technologien vor gezielten Angriffen. Besonders bedeutsam sind diese Themen in Bezug auf die IT-Sicherheit in Kritischen Infrastrukturen (KRITIS), die Organisationen oder Einrichtungen mit großer Bedeutung für das staatliche Gemeinwesen darstellen. Ihr Ausfall würde nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen mit sich bringen – daher sind Kritische Infrastrukturen besonders schützenswert.

Industrielle Kontroll- und Steuerungsanlagen und Industrienetze sowie die Versorgung der Bevölkerung mit Produkten und Dienstleistungen sind die zentralen Themen der IT-Sicherheit für Kritische Infrastrukturen. Produktionsanlagen sind genau wie betriebliche Anwendungssysteme Risiken ausgesetzt: Verlust von Daten ebenso wie Ausfall einer Produktion, schadhafte Produkte oder Minderungen der Servicequalität können Folge einer Kompromittierung der Informationstechnik sein.

Die IT-Sicherheit Kritischer Infrastrukturen lässt sich durch technische Maßnahmen alleine nicht sicherstellen. Vielmehr bedarf es einer ganzheitlichen Betrachtung der Faktoren Technik – Organisation – Mensch.

So stellen neue technische Trends, wie die Nutzung mobiler Geräte, die zunehmende Vernetzung der IT-Systeme oder Cloud-Lösungen die IT-Sicherheit Kritischer Infrastrukturen vor neue Herausforderungen. Organisatorisch geht es um wirtschaftliche und strategische Fragestellungen des Risikomanagements, der Gestaltung der Geschäftsmodelle sowie das Wechselspiel zwischen IT-Sicherheit einerseits und den operativen Anforderungen andererseits. Der Mensch spielt die zentrale Rolle im Hinblick auf das Bewusstsein für IT-Sicherheit und die Akzeptanz von IT-Sicherheitsrichtlinien und Technologien. Last but not least sind nicht alleine Robustheit, sondern auch Resilienz sowie Fragen des Krisenmanagements oder des Business-Continuity-Managements relevant.

Im Rahmen der Hightech-Strategie der Bundesregierung und des Bundesministeriums für Bildung und Forschung (BMBF) begann im Jahr 2014 die Forschung im Förderschwerpunkt „IT-Sicherheit für Kritische Infrastrukturen“ (ITS|KRITIS), um im kooperativen Forschungsprozess Beiträge zur IT-Sicherheit der Kritischen Infrastrukturen zu erarbeiten. Es forschten die folgenden Verbundprojekte für die IT-Sicherheit der Kritischen Infrastrukturen in Deutschland, deren herausragende Forschungsergebnisse im vorliegenden State of the Art gebündelt sind: AQUA-IT-Lab, Cyber-Safe, INDI, ITS.APT, MoSaIK, PREVENT, PortSec, RiskViz, SecMaaS, SICIA, SIDATE, SURF und VeSiKi.

Die Sektoren der Kritischen Infrastrukturen

Das Bundesministerium des Innern (BMI) gibt in der Nationalen Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) eine Definition für KRITIS vor. Demnach sind Kritische Infrastrukturen „Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“ [1]

Die folgende Abbildung 1 zeigt die KRITIS-Sektoren nach der Definition des BMI.

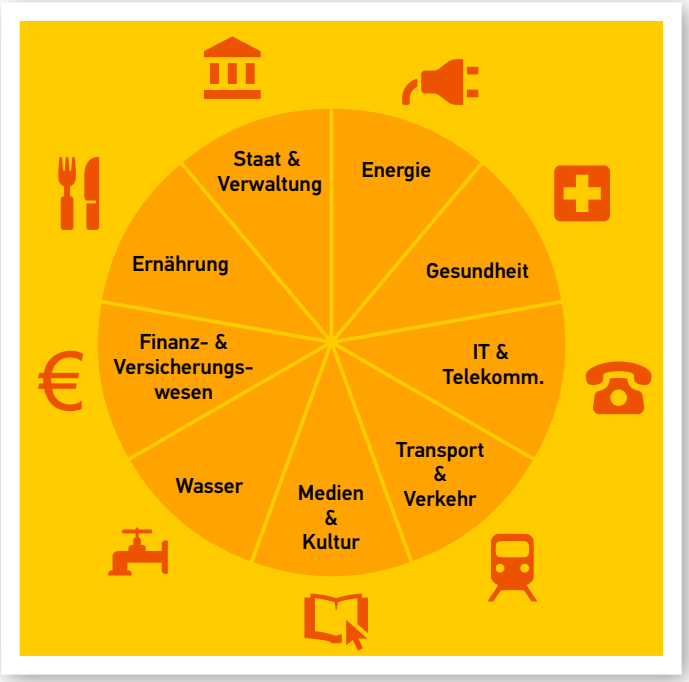


Abb. 1: Sektoren der Kritischen Infrastrukturen

Der Kontext der Forschung

Die Aktivitäten der Forschungsprojekte im Förderschwerpunkt „IT-Sicherheit für Kritische Infrastrukturen“ (ITS|KRITIS) war über die Laufzeit eingebettet in einen dynamischen Kontext. Das Thema selbst hat während der Laufzeit dieses Forschungsprogramms nichts an Aktualität eingebüßt, sondern an Relevanz gewonnen: 73 % der Befragten in der Umfrage „Monitor IT-Sicherheit Kritischer Infrastrukturen“ [2] gaben an, dass ihr Unternehmen Ziel von Angriffen war, und 71 % der Befragten konnten gezielte Attacken gegen ihre Organisation feststellen.

Richtung und Rahmenbedingungen des Förderschwerpunkts ITS|KRITIS wurden von der Hightech-Strategie der Bundesregierung und ihrer Ausgestaltung durch das BMBF vorgegeben. Das Förderprogramm wurde im Jahr 2013 ausgeschrieben und nach einem kompetitiven Auswahlprozess konnten erste Projekte im Jahr 2014 starten; im Jahr 2018 werden die Forschungsprojekte ihre Forschung abschließen. Die folgende Abbildung 2 illustriert den zeitlichen Kontext des Förderschwerpunkts.

Vonseiten der Gesetzgebung wurden während der Laufzeit des Forschungsprogramms zentrale Gesetze verabschiedet. Zum 17. Juli 2015 trat das Gesetz zur Erhöhung der IT-Sicherheit (IT-Sicherheitsgesetz) in Kraft, das zusammen mit der KRITIS-Verordnung festlegt, welche Organisationen als Kritische Infrastrukturen angesehen werden, dass diese Organisationen ein IT-Sicherheitsmanagement haben müssen und welche Informationspflichten bei IT-Sicherheitsvorfällen gelten. Im Sommer 2017 wurde für den Sektor Wasser/Abwasser der erste Branchenstandard durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) akzeptiert.

Die Forschung im Förderschwerpunkt leistet einen Beitrag dazu, dass die Betreiber Kritischer Infrastrukturen die gesetzlichen Anforderungen umsetzen können: In der Umfrage „Monitor IT-Sicherheit Kritischer Infrastrukturen“ [2] wurden IT-Sicherheitsverantwortliche gefragt, ob Bedarf an den IT-Sicherheitsthemen der Forschungsprojekte besteht. Die Antwort war sehr klar ja – über die Themen der Forschungsprojekte haben die Unternehmen nachgedacht, aber es fehlen die Technologien für die Umsetzung von IT-Sicherheitsmaßnahmen. Die Resultate der Forschung werden bei den Betreibern Kritischer Infrastrukturen gebraucht!

> Die Aktivitäten in Forschung und Gesetzgebung sind abgestimmt auf den Bedarf der Betreiber Kritischer Infrastrukturen.

Das Thema der IT-Sicherheit Kritischer Infrastrukturen hat an Relevanz und Brisanz gewonnen – durch die Veränderung der geopolitischen Situation wie auch der IT-Sicherheitslage. Zum Zeitpunkt der Ausschreibung des Forschungsprogramms war im Wesentlichen nur Stuxnet über den engeren Kreis von IT-Sicherheitsexperten hinaus als Schadsoftware bekannt, die sich dediziert

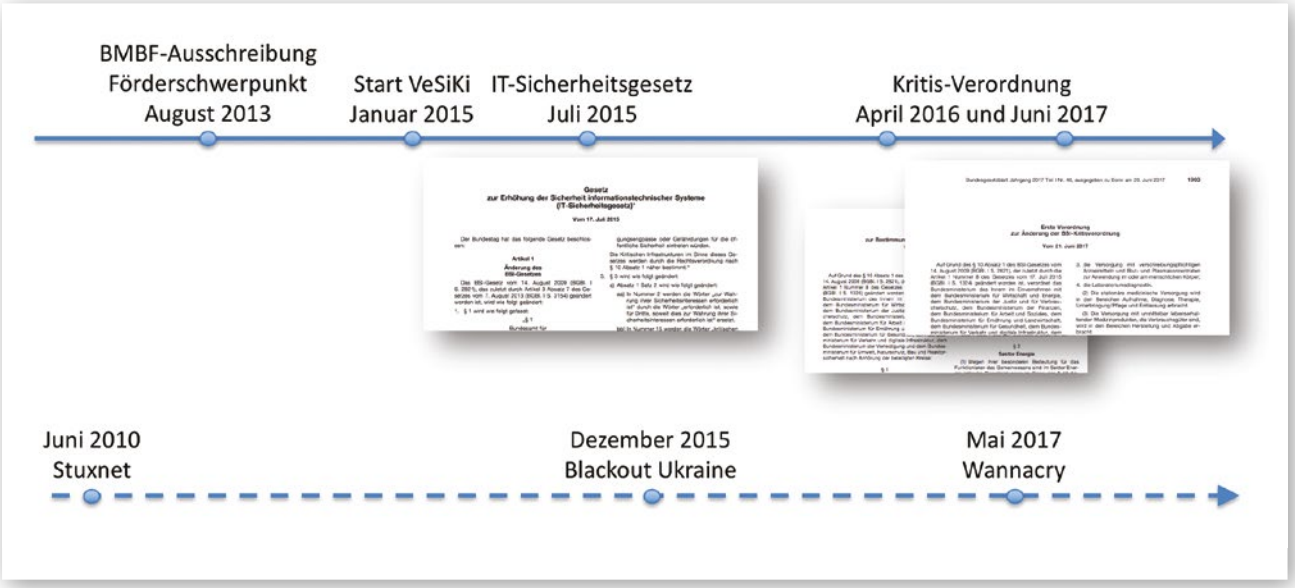


Abb. 2: Der Kontext der Forschung von ITS|KRITIS

gegen Kritische Infrastrukturen und industrielle Kontroll- und Steuerungsanlagen richtet. Prominente Beispiele für IT-Sicherheitsvorfälle bei Kritischen Infrastrukturen sind die Blackouts in der Ukraine von 2015, die Blockierung der Rundfunkanstalt TV5-Monde im Jahr 2015, die Ransomware Locky im Jahr 2016 sowie Wannacry im Mai 2017. Mit der Diskussion über Fake News, Manipulationsmöglichkeiten von demokratischen Wahlen und terroristische Bedrohungen der Zivilgesellschaft rückten während der Laufzeit dieses Forschungsprogramms neue Themen der IT-Sicherheit von Kritischen Infrastrukturen in den Blickpunkt der Öffentlichkeit.

Die Aktivitäten in Forschung und Gesetzgebung sind abgestimmt auf den Bedarf der Betreiber Kritischer Infrastrukturen, verbunden mit der Notwendigkeit, den Stand der IT-Sicherheit bei Kritischen Infrastrukturen feststellen und verbessern zu können. Auch das illustrieren die Zahlen aus der Umfrage „Monitor IT-Sicherheit Kritischer Infrastrukturen“ [2]: Das IT-Sicherheitsgesetz hat Auswirkungen auf die IT-Sicherheit bei Kritischen Infrastrukturen – das bestätigen die befragten IT-Sicherheitsverantwortlichen mehrheitlich. Der Bedarf an Forschungsresultaten, an neuen, einfach umzusetzenden IT-Sicherheitskonzepten besteht. Viele Unternehmen denken über neue IT-Sicherheitsmaßnahmen nach, ihnen fehlen aber überwiegend die Technologien, so wie sie hier entwickelt werden. Dieses Buch fasst die Ergebnisse der geförderten Forschung zusammen, um sie der Öffentlichkeit zugänglich zu machen. Hierbei haben alle Forschungsprojekte zu einem kooperativen Forschungsprozess beigetragen.

Der kooperative Forschungsprozess

Der vorliegende State of the Art der IT-Sicherheit für Kritische Infrastrukturen wurde im kooperativen Prozess mit den Forschungsprojekten des Förderschwerpunkts ITS|KRITIS mit ca. 80 Forschungspartnern, also Betreibern Kritischer Infrastrukturen, Technologieanbietern und Forschungsinstitutionen, erstellt. Das Begleitforschungsprojekt „Vernetzte IT-Sicherheit Kritischer Infrastrukturen“ (VeSiKi) hat diesen kooperativen Prozess koordiniert: Diese Aktivität im kooperativen Forschungsprozess war den Projekten seit 2015 angekündigt worden. Im Herbst 2016 wurde ein dreistufiger Prozess definiert. In Runde 1 wurden ein Call for Ideas an die Mitglieder von ITS|KRITIS versandt und die Ideen zu Zielsetzung, Struktur und Inhalten in Telefonkonferenzen und bilateralen Gesprächen gemeinsam verfeinert.

In Runde 2 wurden die Beiträge bis Mitte Mai 2017 eingereicht, einem Review unterzogen und in einer revidierten Version in Runde 3 bis Ende September 2017 durch die Verbundprojekte eingereicht. Struktur und Aufbau des State of the Art wurden mit dem Vertreter des Bundesamtes für Sicherheit in der Informationstechnik (BSI) abgestimmt und ausgewählte Bereiche einer Revision unterzogen, um die Brücke zu den IT-Grundschutz-Katalogen und dem IT-Grundschutz-Kompendium herzustellen und neue Entwicklungen bei den Branchenstandards der IT-Sicherheit sicherzustellen. Inhalte und Struktur dieses Buches wurden bei einem Review-Workshop im Rahmen des Kongresses „IT-Sicherheit Kritischer Infrastrukturen“ im Oktober 2017 in Berlin den Verbundprojekten und der Öffentlichkeit präsentiert. Die Anregungen aus diesem Review-Workshop und das Meinungsbild zur Art der Veröffentlichung, zu Titel und Layout wurden durch das Projekt VeSiKi bei der Finalisierung und dem Layout eingearbeitet.

Quellen

[1] Bundesministerium des Innern (BMI) (2009): Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie).

[2] Lechner, U. (Hrsg.) (2017): Monitor IT-Sicherheit Kritischer Infrastrukturen. Neubiberg, Universität der Bundeswehr München.

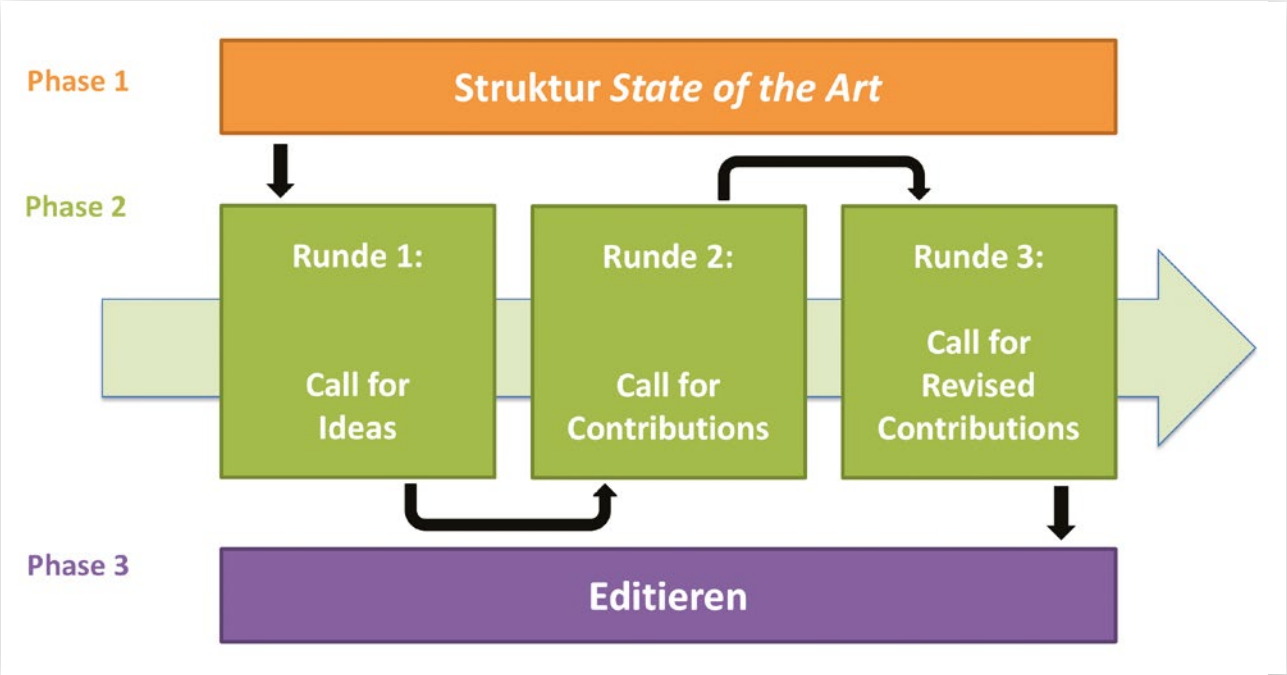


Abb. 3: Prozess der Erstellung des vorliegenden State of the Art

Die Begleitforschung „Vernetzte IT-Sicherheit Kritischer Infrastrukturen“

Das vorliegende Buch entstand im Kontext der Begleitforschung „Vernetzte IT-Sicherheit Kritischer Infrastrukturen“ (VeSiKi).

Das Begleitforschungsprojekt VeSiKi vernetzt zum einen die Verbundprojekte im Förderschwerpunkt und unterstützt so den kooperativen Forschungsprozess. Zum anderen unterstützt VeSiKi die Außendarstellung des Förderschwerpunkts und die Sichtbarkeit der Aktivitäten und Ergebnisse in der Öffentlichkeit und damit den Transfer in die Praxis. Eine Übersicht über die Aktivitäten von VeSiKi gibt die folgende Abbildung 4.

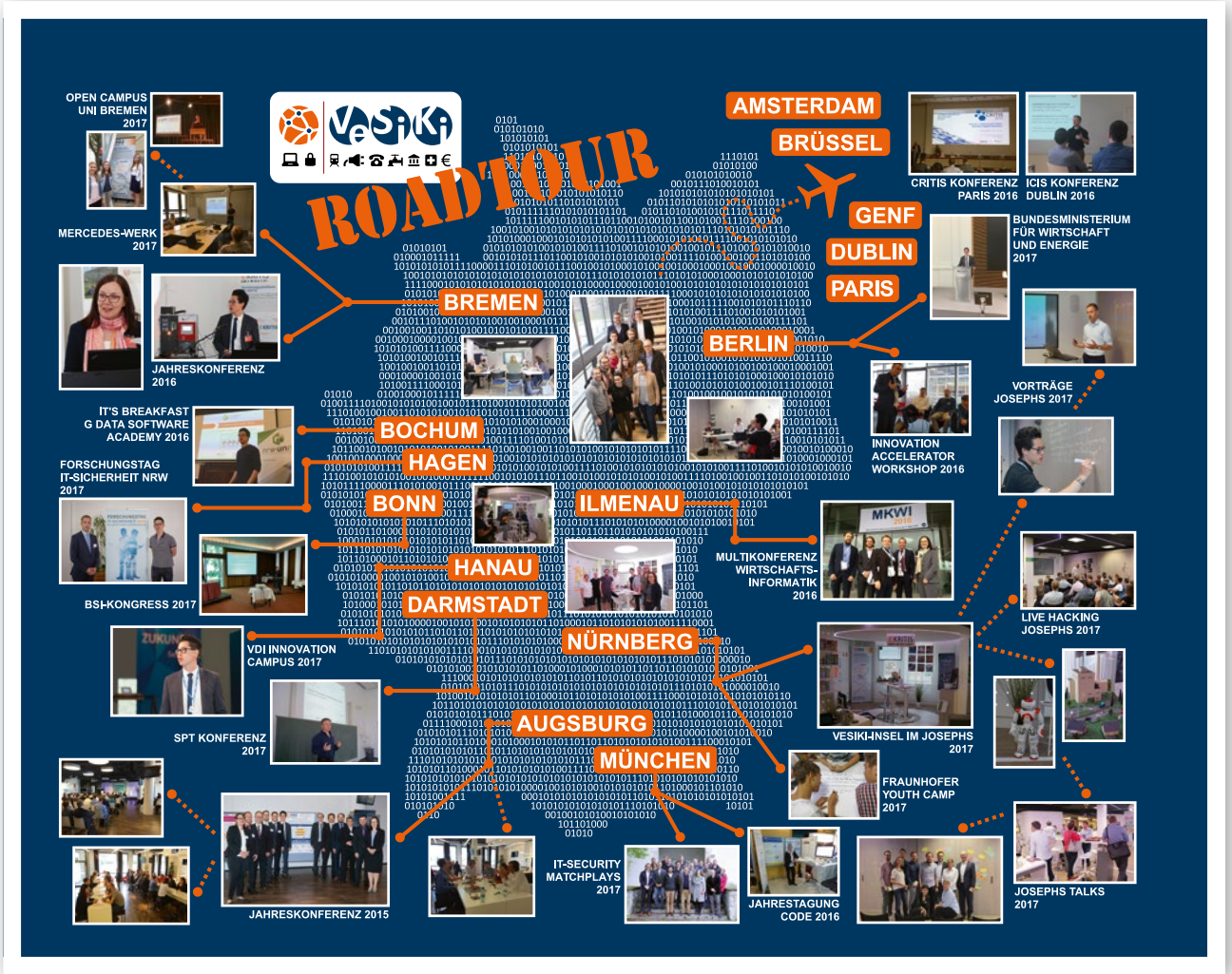


Abb. 4: Aktivitäten der Begleitforschung VeSiKi im ITS|KRITIS-Förderschwerpunkt

Um den Aufgaben der Begleitforschung gerecht zu werden, arbeiten in VeSiKi vier Institutionen Hand in Hand:

Konsortialführer von VeSiKi ist der Lehrstuhl für Wirtschaftsinformatik der Universität der Bundeswehr München (kurz: UniBw).

Als Konsortialführer koordiniert die UniBw die Arbeiten im Projekt VeSiKi. Hierzu zählen beispielsweise die Organisation jährlicher Konferenzen im Förderschwerpunkt ITS|KRITIS, die Vorbereitung, Durchführung und Veröffentlichung der Umfragen zur IT-Sicherheit in Kritischen Infrastrukturen „Monitor" und „Monitor 2.0", die Erstellung der Fallstudiensammlung sowie die Koordinierung des vorliegenden State of the Art.

> Beiträge zu den genannten Themen finden sich in den Sektionen 1, 4 und 5 im vorliegenden Buch wieder.

Von der Friedrich-Alexander-Universität Erlangen-Nürnberg (kurz: FAU) ist der Lehrstuhl für Wirtschaftsinformatik, insbes. Innovation und Wertschöpfung, an VeSiKi beteiligt.

Die FAU deckt in VeSiKi insbesondere den Teilaspekt „Open Innovation für IT-Sicherheit Kritischer Infrastrukturen" ab. Dazu werden beispielsweise die Online-Plattform itskritis.de zur Verfügung gestellt sowie partizipative Gestaltungsprozesse, wie die Themeninsel ITS|KRITIS, im offenen Innovationslabor JOSEPHS® organisiert. Die FAU bietet außerdem Workshops zur wissenschaftlichen Vernetzung und zur gemeinsamen Verwertung der Forschungsergebnisse aus den Projekten an.

> Beiträge zu den genannten Themen finden sich in den Sektionen 1 und 4 im vorliegenden Buch wieder.

Die Universität Bremen ist mit dem Institut für Informations-, Gesundheits- und Medizinrecht (kurz: IGMR) in VeSiKi vertreten.

Die Universität Bremen führt über VeSiKi die IT-Sicherheitsrechtliche Begleitung für den Förderschwerpunkt ITS|KRITIS durch. Dazu werden die aktuellen Entwicklungen in diesem Bereich beobachtet und analysiert und an die Verbundprojekte im Förderschwerpunkt ITS|KRITIS weitergegeben. Daneben wurden beispielsweise Workshops und Vortragsreihen durchgeführt. Ebenso wurde zusammen mit dem VDE | DKE der IT-Security-Navigator als Praxishilfe bei der Umsetzung von Informationssicherheit erarbeitet der www.itsecuritynavigator.de zur Verfügung steht.

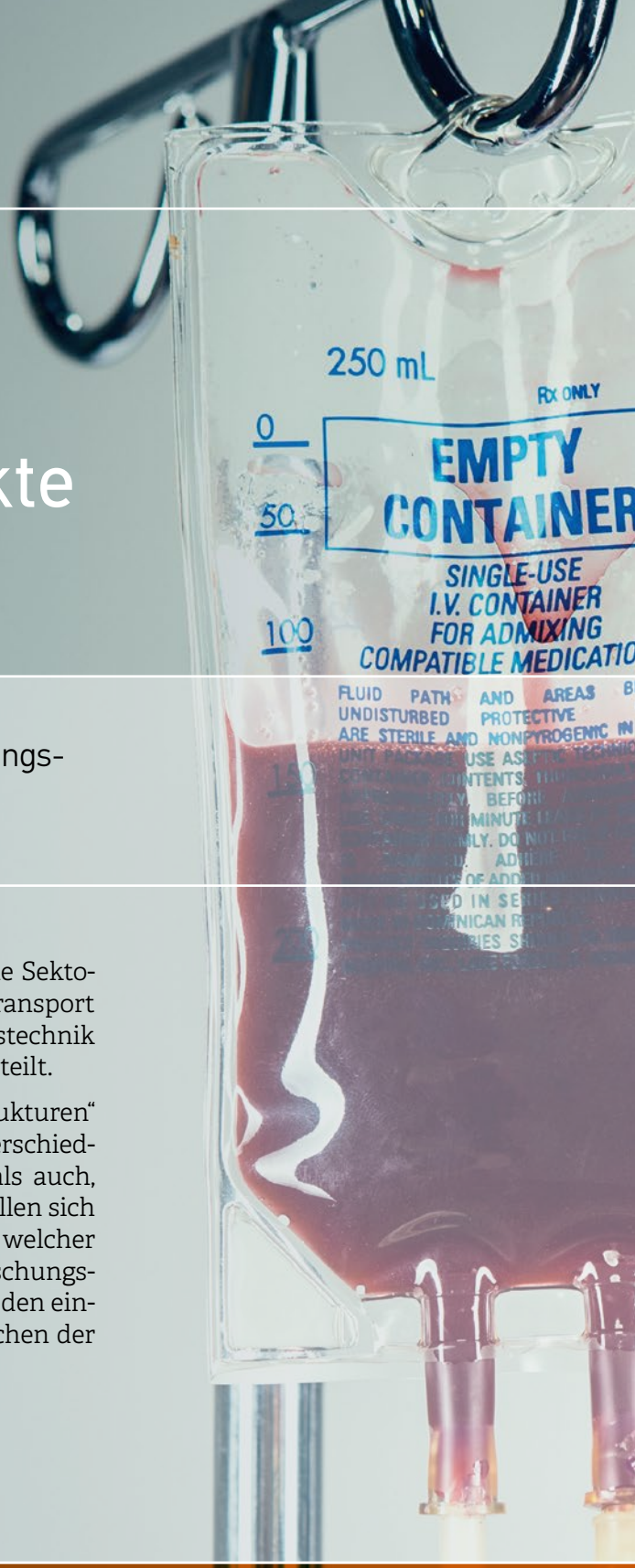
> Beiträge zu den genannten Themen finden sich in den Sektionen 1, 3 und 4 im vorliegenden Buch wieder.

Abgerundet wird VeSiKi vom Fachbereich Standardisierung und Innovation des VDE | DKE in Frankfurt (kurz: VDE | DKE).

Der VDE | DKE bringt über VeSiKi den Aspekt Normung und Standardisierung in den Förderschwerpunkt ITS|KRITIS ein. Dazu wurde beispielsweise die Fachgruppe „Normung und Standardisierung" ins Leben gerufen, der regelmäßig Workshops mit den Verbundprojekten im Förderschwerpunkt ITS|KRITIS durchführt. Die Ergebnisse der Arbeit werden in einem Whitepaper über die Plattform itskrits.de zur Verfügung gestellt. Ebenso wurde zusammen mit der Universität Bremen der IT-Security-Navigator als Praxishilfe bei der Umsetzung von Informationssicherheit erarbeitet und unter www.itsecuritynavigator.de sowie über die Plattform itskritis.de zur Verfügung gestellt.

> Beiträge zu den genannten Themen finden sich in den Sektionen 1 und 4 im vorliegenden Buch wieder.

Sektion 1
ITS|KRITIS-Projekte und deren Schwerpunkte in der IT-Sicherheit



In dieser Sektion wird ein Überblick über die Forschungsprojekte gegeben.

Die Kritischen Infrastrukturen in Deutschland werden in die Sektoren Energie, Gesundheit, Staat und Verwaltung, Ernährung, Transport und Verkehr, Finanz- und Versicherungswesen, Informationstechnik und Kommunikation, Medien und Kultur sowie Wasser eingeteilt.

Der Förderschwerpunkt „IT-Sicherheit für Kritische Infrastrukturen" ITS|KRITIS beinhaltete Forschungsprojekte mit ganz unterschiedlichem Fokus – sowohl, was die KRITIS-Sektoren betrifft, als auch, was die Inhalte der Forschung betrifft. In dieser Sektion 1 stellen sich die einzelnen Forschungsprojekte kurz vor und beschreiben, welcher KRITIS-Sektor adressiert wurde und welche Inhalte das Forschungsprojekt jeweils bearbeitete. Ebenso sind die Projektpartner in den einzelnen Forschungsprojekten sowie die BMBF-Förderkennzeichen der Projekte vermerkt.

Review:

Manfred Hofmeier, Matthias Raß

Sektion 1
Inhaltsverzeichnis

Aqua-IT-Lab	IT-Sicherheit für kleine und mittlere Wasserversorger	16
Cyber-Safe	Schutz von Verkehrs- und Tunnelleitzentralen vor Cyberangriffen	17
INDI	Intelligente Intrusion-Detection-Systeme für Industrienetze	19
ITS.APT	IT-Security-Awareness messbar machen	20
MoSaIK	Modellbasierte Sicherheitsanalyse von IKT-basierten Kritischen Infrastrukturen	21
PortSec	Systematisches und umfassendes Risikomanagement für Hafentelematiksysteme	22
PREVENT	Ein integriertes Framework zum präventiven Krisen- und Risiko-Management	24
RiskViz	Risikolagebild der industriellen IT-Sicherheit in Deutschland	25
SecMaaS	Security Management as a Service	26
SICIA	IT-Sicherheit in kritischen Netzen messen und systematisch verbessern	27
SIDATE	Sichere Informationsnetze bei kleinen und mittleren Energieversorgern	29
SURF	Systemic Security for Critical Infrastructures	30
VeSiKi	Das Begleitforschungsprojekt Vernetzte IT-Sicherheit Kritischer Infrastrukturen	32

Aqua-IT-Lab – IT-Sicherheit für kleine und mittlere Wasserversorger

Christof Thim

Forschungsprojekt:
Aqua-IT-Lab

Sektor Wasserversorgung: Verteilt und kleinteilig

Das Projekt Aqua-IT-Lab adressiert IT-Sicherheit im Sektor Wasserversorgung. Durch die Kleinteiligkeit und regionale Verankerung der Infrastruktur existieren hier viele kleine und mittlere Versorger. Anders als bei großen Versorgern, welche häufig Skaleneffekte bei der Investition in IT-Sicherheit nutzen können, stehen hier eher weniger Ressourcen zur Verfügung. Entsprechend ist der Umfang gängiger ISMS-Ansätze und Assessment-Verfahren nicht angemessen. Daher entwickelt das Projekt zwei Artefakte: Ein Schnelltest, der gängige Rahmenwerke kondensiert und zeiteffizient in Handlungsempfehlungen umsetzt, dient zur Selbstbewertung und zur Priorisierung von IT-Sicherheitsvorhaben. Eine Infrastruktursimulation ermöglicht die Durchführung von Security Assessments, z. B. Penetrationstests, ohne die Versorgung zu gefährden.

Schnelltest

Auf Basis der ISO2700x-Reihe, der IEC62443 sowie weiterer branchenspezifischer Sicherheitsstandards ermöglicht der Schnelltest eine Bewertung des Reifegrades der IT-Sicherheit in elf Dimensionen. Mit insgesamt 50 Fragen werden die größten Lücken in der IT-Sicherheit identifiziert und automatisiert Vorschläge zu deren Behandlung gegeben. Die Priorisierung der Handlungsempfehlung sorgt dafür, dass sie in handhabbaren Projekten mit flexiblem Ressourcenaufwand umgesetzt werden können.

Die Themenbereiche umfassen dabei nicht nur klassische Themen der Sicherheit der Office-IT, sondern greifen auch die Besonderheiten der Operational Technology auf. Der Umgang mit der Sicherheit der Steuerungstechnik im gesamten Komponentenlebenszyklus ist das Kernstück zum Erhalt der Versorgungssicherheit. Zur Verfeinerung der Schnelltestergebnisse wurde daher die Business-Impact-Analyse auf den Wasserversorgungsprozess angepasst, um Komponenten zu identifizieren, welche eines priorisierten Schutzes bedürfen. Der Schnelltest ergänzt somit den Branchenstandard des Wassersektors (W1060).

Testlabor

Mit dem Testlabor adressiert das Verbundprojekt eine weitere Herausforderung kleiner und mittlerer Versorger. Ihre Steuerungsinfrastruktur entwickelt sich sukzessive: Neue Technologien werden nach und nach integriert. Ein tiefgreifendes Assessment der IT-Sicherheit auf den Übertragungswegen und im Steuerungscode ist entweder nur oberflächlich oder unter der Gefährdung der Versorgung möglich.

Das Labor ermöglicht es den Versorgern nun, die kritischen Komponenten ihrer Infrastruktur oder Infrastrukturteile in einer gesicherten Umgebung zu testen. Hierfür werden Industriekomponenten (Firewalls, SPS, VPN, Vernetzung) und -systeme (SCADA, Leitsystem) mit den realen Konfigurationen eingerichtet. Nachrangige Systeme, wie z. B. einfache Input-Output-Steuerungen oder verteilte Sensoren werden simuliert.

Diese Umgebung kann je nach Umfang der Testfälle z. B. für Penetrationstests oder Code-Reviews genutzt werden, um verborgene Schwachstellen zu identifizieren und Hinweise zu deren Behebung zu geben.

Förderkennzeichen:
16KIS0202K , 16KIS0203 bis 16KIS0206

- Universität Potsdam
- HiSolutions AG
- Pretherm GmbH
- Stadtwerke Brandenburg/Havel GmbH
- Wasser- und Abwasserzweckverband Calau

Cyber-Safe – Schutz von Verkehrs- und Tunnelleitzentralen vor Cyberangriffen

Thorsten Holz, Ingo Kaundinya, Selcuk Nisancioglu, Anne Lehan

Forschungsprojekt:
Cyber-Safe

Hintergrund

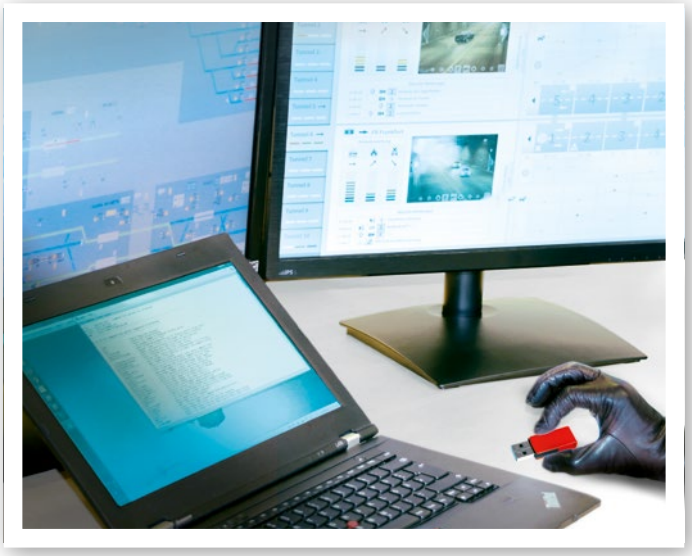
Verkehrs- und Tunnelleitzentralen übernehmen wichtige Funktionen für die Gewährleistung der Verfügbarkeit und Sicherheit des Straßenverkehrsnetzes. In ihnen werden Überwachungs- und Steuerungsmöglichkeiten gebündelt. Da diese Funktionen durch IT-Systeme gesteuert werden, wird der Schutz vor Cyberangriffen zu einer wachsenden Herausforderung. Das Forschungsprojekt Cyber-Safe verfolgt daher das Ziel, Leitzentralenbetreiber in die Lage zu versetzen, Gefährdungen durch Cyberangriffe besser als bisher zu erkennen und systematisch geeignete Schutzmaßnahmen zu ergreifen.

Motivation

Mobilität und Verkehr sind Grundlagen einer modernen Gesellschaft und wirtschaftlicher Prosperität. Eine zentrale Voraussetzung ist daher die Gewährleistung der Verfügbarkeit des Verkehrsnetzes. Eine wichtige Aufgabe übernehmen in diesem Zusammenhang Tunnelleitzentralen, die die Überwachung und Steuerung des Verkehrs in Tunneln ermöglichen, um im Ereignisfall Maßnahmen zur Gewährleistung der Sicherheit der Tunnelnutzer einleiten zu können. Da diese Leitzentralen zunehmend mit IT-Systemen ausgestattet werden, gewinnt ihr Schutz vor Cyber-Angriffen in wachsendem Maße an Bedeutung. Die Schadsoftware BlackEnergy der Sandworm-Gruppe sabotierte im Jahre 2015 Energieversorger in der Ukraine, in dessen Folge mindestens 225.000 Einwohner von einem mehrstündigen Ausfall der Stromversorgung betroffen waren. Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde diese Schadsoftware im Wesentlichen gegen Organisationen aus den Sektoren Energie sowie Transport und Verkehr eingesetzt und sollte nicht nur Betreiber, sondern auch indirekt die Bevölkerung treffen [1].

Eine im Rahmen des Forschungsprojektes Cyber-Safe durchgeführte Recherche zu bisher erfolgten Cyberangriffen auf Verkehrsinfrastrukturen zeigt ebenfalls die Notwendigkeit zu handeln: Im Jahre 2015 musste der bei Haifa (Israel) gelegene und durch das Carmel Gebirge führende ca. neun Kilometer lange Carmel Tunnel infolge eines gezielten Hacker-Angriffs für die Dauer von acht Stunden gesperrt werden, was zu schwerwiegenden Verkehrsbeeinträchtigungen führte [2]. Auch ist vor dem Hintergrund der Entwicklungen im Bereich der intelligenten Verkehrsinfrastrukturen davon auszugehen, dass diese zukünftig immer enger in den Fokus von Cyberangreifern rücken werden. Darüber hinaus wurden mit der ersten Verordnung zur Änderung der BSI-Kritisverordnung [3] die Schwellenwerte für den Sektor Transport und Verkehr festgelegt. Demnach gelten grundsätzlich Anlagen wie Verkehrssteuerungs- und Leitsystem für das Netz der Bundesautobahnen als kritisch und sind entsprechend zu schützen.

> Handlungshilfen zur Identifizierung von Gefahren durch Cyber-Angriffe und zur Ergreifung geeigneter Schutzmaßnahmen für Verkehrs- und Tunnelleitsysteme



Ziel

Ziel des Projektes Cyber-Safe ist es daher, Handlungshilfen zu entwickeln, die die Betreiber von Verkehrs- und Tunnelleitzentralen in die Lage versetzen, mögliche Gefährdungen durch Cyberangriffe zielgerichteter als bislang zu erkennen und geeignete Schutzmaßnahmen zu ergreifen. Hierzu wurden im Rahmen einer Bestandsanalyse bereits umgesetzte Maßnahmen auf ihre Effektivität und Wirksamkeit hin überprüft und gleichzeitig bestehende Defizite identifiziert. Ergänzt wurde diese Analyse durch einen Penetrationstest, der im Zuge einer detaillierten Tiefenanalyse Einblicke in die IT-Systeme lieferte.

Umsetzung

Um die unmittelbare Umsetzbarkeit der zu entwickelnden Handlungshilfen zu erreichen, wurden zwei Workshops mit Betreibern, Ausstattern und Planern von Leitzentralen durchgeführt. Hierbei wurden der Bedarf sowie die Anforderungen an Handlungshilfen zur Bewertung der aktuell vorhandenen IT-Sicherheit und Steigerung der Widerstandsfähigkeit gegen Cyber-Angriffe ermittelt [4]. Diese wertvollen Erkenntnisse bzgl. des Nutzerbedarfs wurden in drei zielgruppenorientierte Handlungshilfen überführt und stehen mit Abschluss des Projektes Betreibern, Ausstattern sowie Planern von Leitzentralen für die direkte Nutzung in der Praxis zur Verfügung.

Quellen

[1] Die Lage der IT-Sicherheit in Deutschland 2016, Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, 2016, S. 40.

[2] The Associated Press: Hallmark of a New Era' // Haifa Tunnel Paralyzed by Cyberattack, Expert Reveals. In: Haaretz (Archives). Stand 27.Oktober 2013. http://www.haaretz.com/israel-news/1.554729 (abgerufen am 14.06.2017).

[3] Erste Verordnung zur Änderung der BSI-Kritisverordnung in der Fassung von der Bekanntmachung vom 29. Juni 2017 (BGBl., S. 1921).

[4] Thienert, C., Nisancioglu, S.: Workshop zur Cyber-Sicherheit von Tunnel- und Verkehrsleitzentralen, Tunnel Magazin Heft 3 2016, S. 54 f., Bauverlag Gütersloh.

Förderkennzeichen:
16KISO168K, 16KISO169 bis 16KISO172

- BASt - Bundesanstalt für Straßenwesen
- DÜRR Group GmbH
- Ruhr-Universität Bochum
- Straßen.NRW
- STUVA e. V.

INDI – Intelligente Intrusion-Detection-Systeme für Industrienetze

Konrad Rieck, Christian Wressnegger, Hartmut König, Andreas Paul, Franka Schuster, Heiko Kanisch, Christoph Moder

Forschungsprojekt:
INDI

Thema und Motivation

Die Sicherheit von Kritischen Infrastrukturen in Deutschland wird zunehmend durch Cyberangriffe gefährdet. Insbesondere gezielte Angriffe und sogenannte "Advanced Persistent Threats" stellen eine enorme Bedrohung für IT-Systeme in Kritischen Infrastrukturen dar. Hinter diesen Angriffen stehen meist größere Organisationen bis hin zu Regierungen, die über umfangreiche Ressourcen für die Entwicklung von Schadcodes verfügen. Ein zuverlässiger Schutz der entsprechenden IT-Systeme ist äußerst aufwändig. Kritische Infrastrukturen zeichnen sich durch eine hochgradig heterogene IT aus, die sich sowohl aus standardisierten Komponenten als auch aus proprietären Speziallösungen zusammensetzt. Die Erkennung von Verwundbarkeiten und Angriffen in einer solchen Umgebung stellt die Betreiber vor eine Reihe von Herausforderungen, die sich nicht mit klassischen Konzepten der IT-Sicherheit lösen lassen.

Während auf der Betriebsebene vorrangig klassische IT-Systeme verwendet werden, kommt beim Übergang von der Steuerungsebene zur Feldebene zunehmend proprietäre IT zum Einsatz, was sich aus Netzsicht in einer wachsenden Anzahl von seltenen und unbekannten Protokollen äußert. Bisherige Ansätze der IT-Sicherheit decken hier nur einen Bruchteil der auftretenden Technologie ab. Deshalb können Angriffe in tieferen Schichten mit aktuellen Mitteln nicht erkannt werden. Ein zuverlässiger Schutz der IT-Systeme in Kritischen Infrastrukturen und eine Erkennung von Angriffen werden nur durch die Schaffung von neuartiger Sicherheitstechnologie möglich, die gezielt die Probleme und Herausforderungen von Industrienetzen adressiert.

Zielsetzung

Das Projekt INDI hat den intelligenten Schutz von Industrienetzen in Kritischen Infrastrukturen zum Ziel. Projektinhalt ist die Entwicklung neuartiger Methoden zur automatischen Erkennung und Eindämmung von Cyberangriffen in heterogenen Industrienetzen mit Echtzeitanforderungen. Der Anspruch der Verbundpartner ist es dabei, durch einen hohen Grad an Selbstjustierung eine alltagstaugliche, kosteneffiziente, benutzerfreundliche und an die Komplexität der Infrastruktur gut skalierbare Sicherheitslösung zu schaffen, die unabhängig von den konkreten industriellen Prozessen der Industrienetze eingesetzt werden kann.

Im Vorhaben werden Sicherheitstechniken entwickelt, die erstmals eine robuste Erkennung von Angriffen in komplexen Industrienetzen mit zum Teil unbekannten Protokollen ermöglichen. Hierzu wird in einer Phase der Selbstjustierung der Netzverkehr von Industrieanlagen mit Techniken des maschinellen Lernens analysiert, um Regeln und Modelle für den Normalbetrieb abzuleiten und unbekannte Protokolle zu beobachten und nachzubilden.

Förderkennzeichen:
16KIS0154K, 16KIS0155 bis 16KIS0157

- Brandenburgische Technische Universität Cottbus-Senftenberg
- Technische Universität Braunschweig
- genua mbH
- LEAG Lausitz Energie Kraftwerke AG

ITS.APT – IT-Security- Awareness messbar machen

Arnold Sykosch

Forschungsprojekt:
ITS.APT

Motivation

Angriffe auf IT-Infrastrukturen werden immer häufiger, da sie mit vergleichsweise geringem Aufwand über das Internet möglich sind. Zudem kann die Identität eines Angreifers über dieses Medium im Vergleich zu einem physischen Angriff leichter verschleiert werden. Sicherheitsexperten spekulieren, ob und in welchem Maße das Sicherheitsbewusstsein von IT-Benutzern den Ausgang sicherheitsrelevanter Vorfälle beeinflussen kann. Zur Messung der Beteiligung von Benutzern liegen jedoch nur wenige empirische Daten vor, unter anderem, weil die Datenerhebung mit hohen Kosten verbunden ist und datenschutz- und personalrechtlich problematisch sein kann.

Eine Bewertung der IT-Sicherheit bei Betreibern Kritischer Infrastrukturen wird üblicherweise durch klassisches „Penetration Testing“ durchgeführt. Bei diesem Vorgang wird die IT-Infrastruktur eines Unternehmens auf Verwundbarkeiten überprüft. Anhand der gewonnenen Ergebnisse wird eine Bewertung vorgenommen. Dabei ist das Testfeld jedoch lediglich auf die technische Infrastruktur beschränkt und lässt den Faktor Mensch bei der IT-Sicherheitsbewertung unberücksichtigt.

Ziele und Vorgehen

Das Verbundprojekt IT-Security Awareness Penetration Testing (ITS.APT) adressiert diese Schwierigkeiten mit dem Ziel, klassisches Penetration-Testing auf die Benutzer der IT-Infrastruktur zu erweitern.

Im Rahmen des Projekts werden Methoden erarbeitet, mit denen denen das IT-Sicherheitsbewusstsein von Benutzern gemessen werden kann. Traditionelle wissenschaftliche Messwerkzeuge zur Erfassung von Anteilen des Bewusstseins von Individuen haben sich mehrfach als impraktikabel erwiesen.

Innovationen und Perspektiven

Im Rahmen dieses Projekts wird erstmals eine umfassende Lösung entwickelt, die tiefere Einblicke in das IT-Sicherheitsbewusstsein von Benutzern gewährt als bisher möglich.

Die angestrebte Innovation umfasst ein Werkzeug zur kosteneffizienten Messung des kollektiven IT-Sicherheitsbewusstseins ganzer Unternehmen und bietet damit neue Erkenntnisse für alle betroffenen Forschungsbereiche: Jura, Datenschutz, Psychologie und Informatik. Auch das IT-Risikomanagement von Unternehmen kann so verfeinert werden. Zudem werden neue Ansätze zur Erhöhung von IT-Sicherheitsbewusstsein geschaffen und exemplarisch im Rahmen des Projekts umgesetzt.

Die Evaluation findet in einem der größten europäischen Zentren für medizinische Versorgung, dem Universitätsklinikum Schleswig-Holstein, statt. In dieser Umgebung sind die Auswirkungen sicherheitsrelevanter Vorfälle besonders gravierend und die Anforderungen an den Datenschutz besonders hoch.

Förderkennzeichen:
16KIS0207K, 16KIS0208 bis 16KIS0212

- Rheinische Friedrich-Wilhelms-Universität Bonn
- Universität Duisburg-Essen
- Universitätsklinikum Schleswig-Holstein
- Enno Rey Netzwerke GmbH
- Westfälische Wilhelms-Universität Münster
- Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

MoSaIK – Modellbasierte Sicherheitsanalyse von IKT-basierten Kritischen Infrastrukturen

Jörn Eichler

Forschungsprojekt:
MoSaIK

Der Forschungsschwerpunkt ist die Entwicklung einer Methode sowie von Werkzeugen zu ihrer Anwendung für die effiziente Risikoanalyse und Bewertung des Sicherheitsniveaus Kritischer Infrastrukturen insbesondere für kleinere Betreiber. Der dabei verfolgte systemische Gesamtansatz adressiert die Aspekte Technik, Organisation und nicht zuletzt den Faktor Mensch.

Relevanz des Verbundprojektes / Grundlagen

Weite Teile des gesellschaftlichen Lebens sind von funktionierenden Infrastrukturen abhängig, welche die grundlegende Versorgung sichern sowie den Erhalt der öffentlichen Sicherheit zentral unterstützen. Wie auch in anderen Lebensbereichen sind diese Kritischen Infrastrukturen zunehmend mit Informations- und Kommunikationstechnologie (IKT) durchdrungen. Insbesondere Kritische Infrastrukturen in der Hand von Städten und Gemeinden sowie kommunalen Versorgern bilden eine wichtige Grundlage des öffentlichen Lebens. Sie bleiben jedoch aus finanziellen und organisatorischen Gründen hinsichtlich ihres Schutzniveaus oftmals deutlich hinter industriellen Infrastrukturen oder solchen mit bundesweiter Bedeutung zurück.

Forschungsfragen

Im Kern der Forschung steht im MoSaIK-Projekt die Frage, ob und wie gut modellgetriebene und modellbasierte Ansätze aus dem System- und Software-Engineering zur effizienten Unterstützung der Risikoanalyse und Sicherheitsbewertung im Kontext Kritischer Infrastrukturen genutzt werden können. Das Vorhaben will untersuchen, ob werkzeuggestützte, auf die Fachanwender zugeschnittene Risikoanalysen und Sicherheitsbewertungen die Bestimmung des Sicherheitsniveaus erleichtern. Als besonderes Augenmerk stehen die Unterstützung unterschiedlicher Granularitätsebenen und die inkrementelle Entwicklung im Fokus.

Ziele

Das Ziel von MoSaIK ist die Entwicklung einer auf kleinere Betreiber fokussierten Methode für die effiziente Risikoanalyse Kritischer Infrastrukturen und die Bewertung ihres Sicherheitsniveaus. Im Rahmen des Projektes werden zudem unter Verwendung modellgetriebener Ansätze aus dem Software-Engineering Werkzeuge zur Anwendung der Methode entwickelt. Die Qualität der Bewertungen wird durch Nutzbarmachung betreiberunabhängigen Know-hows deutlich verbessert bzw. Bewertungen erst ermöglicht. Die systematische Verwendung von Struktur- und Sensordaten erleichtert die kontinuierliche Neubewertung des Sicherheitsniveaus auch bei Änderungen in der Infrastruktur.

Vorgehen

Zunächst wurden die Herausforderungen und Bedürfnisse der Betreiber Kritischer Infrastrukturen an die Vorgehensweisen erhoben. Bei je einem KRITIS-Betreiber wurde eine Methode basierend auf dem IT-Grundschutz bzw. Angriffsbäumen (Attack Trees) durchgeführt und die Erfahrungen dokumentiert.

Durch diese Erfahrungen wird eine neue modellbasierte Risikobeurteilungsmethode erforscht. Die Komplexität der Modellierung wird dabei vorwiegend vom Aufbau der Infrastruktur und der späteren Nutzbarkeit durch die KMUs geprägt. Die Methode entsteht mit dem Blick nach innen auf die etablierten Vorgehensweisen und Technologien in den Unternehmen, wodurch die Bedürfnisse und Herausforderungen von KRITIS-Betreibern berücksichtigt werden. Der Einsatz von Werkzeugen und die Erhebung von Messdaten mittels Sensoren sollen die Betreiber bei der Durchführung der Methode unterstützen und den Aufwand für die Risikobeurteilung verringern sowie die Sicherheitsbewertung auf tatsächliche Daten stützen.

Förderkennzeichen:
16KIS0173K, 16KIS0174 bis 16KIS0176

- Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC
- m-privacy GmbH
- Stadt Gera
- Stadtwerk Haßfurt GmbH

PortSec – Systematisches und umfassendes Risikomanagement für Hafentelematiksysteme

Nils Meyer-Larsen, Rainer Müller, Karsten Sohr, Annabelle Vöge

Forschungsprojekt:
PortSec

Die Seehäfen sind für die deutsche Volkswirtschaft von zentraler Bedeutung. Für den reibungslosen Ablauf beim Ladungsumschlag in Seehäfen werden sogenannte. Hafentelematiksysteme oder Port Community Systems (PCS) eingesetzt. Sie sind zentrale Datendrehscheiben und verbinden die am Seeverkehr beteiligten Unternehmen und Behörden, wie z. B. Reeder, Speditionen, Terminals, die Bahn und den Zoll. Als Teil der Kritischen Infrastruktur in Transport und Verkehr können Ausfälle oder Störungen zu massiven Problemen des Hafenbetriebs führen, im Extremfall sogar zum Stillstand. IT-Angriffe auf Hafentelematiksysteme können sogar je nach Dauer zu Versorgungsengpässen der nachgelagerten Industrien bzw. der Bevölkerung führen.

Datenmanipulationen, z. B. bei einem mit Gefahrgut beladenen Container, könnten bei einer Lagerung ohne die gesetzlich verlangten Trennvorschriften in der Nähe anderer Gefahrgutcontainer unter bestimmten Umständen zu chemischen Reaktionen der Gefahrstoffe und damit zu Bränden oder zu Explosionen führen. Vertrauliche Daten könnten über gezielt zu diesem Zweck angelegte manipulierte Nutzerkonten abgegriffen werden, um auf dieser Basis kriminelle Handlungen, z. B. Drogenschmuggel, vorzubereiten.

PortSec erforscht die Entwicklung eines systematischen und umfassenden IT-Risikomanagements in der Hafentelematik auf Basis der Software-Architektur unter Einbeziehung rechtlicher und wirtschaftlicher Sicherheitsanforderungen. Der softwarezentrierte Ansatz fokussiert auf die Prävention von Angriffen und nicht primär auf eine Angriffserkennung und -abwehr.

Bedrohungsanalyse

Im Rahmen der Bedrohungsanalyse wird ein Gefährdungskatalog erstellt, um mögliche IT-Angriffe auf Hafentelematiksysteme zu beschreiben. Hierzu werden zunächst die domänenspezifischen Geschäftsprozesse im Umfeld der Hafenkommunikation analysiert und die Sicherheitsanforderungen der Prozesse und der verarbeiteten Daten in der Hafentelematik aufgenommen.

In der Analyse sollen mögliche Schwachpunkte identifiziert werden, wobei primär Schnittstellen mit Kommunikation über das Internet untersucht werden. Außerdem werden die verwendeten Systeme hinsichtlich der Schutzfaktoren Verfügbarkeit, Vertraulichkeit und Integrität untersucht.

Auf Basis der Geschäftsprozesse und möglicher Schwachstellen werden relevante Angriffsszenarien definiert und die damit verbundenen volkswirtschaftlichen und betriebswirtschaftlichen Risiken hinsichtlich möglicher Schäden evaluiert. Hierzu wird jedes einzelne Szenario hinsichtlich der Eintrittswahrscheinlichkeit, Verwundbarkeit und Konsequenzen bewertet, um die Auswirkungen und Schäden möglicher Angriffe auf den Hafentelematiksystembetreiber, die Hafenwirtschaft sowie nachgelagerte Logistikprozesse zu evaluieren. Außerdem werden die Auswirkungen von Angriffen auf die Volkswirtschaft untersucht. Um das Bild der Bedrohungsszenarien zu vervollständigen, werden bisherige ähnliche Angriffe in die Betrachtung mit einbezogen.

Einen weiteren Schwerpunkt stellt die Entwicklung eines Verfahrens dar, mit dessen Hilfe Domänenwissen möglichst automatisiert in die gemeinsam zu entwickelnde formalisierte Wissensdatenbank überführt werden kann. Das eingegebene Wissen kann so später für die Prüfprozesse eingesetzt werden. Zunächst wird ein entsprechendes Konzept entwickelt und später in ein implementiertes Verfahren umgesetzt. Schließlich wird das Domänenwissen bezüglich der Gefahren und der daraus resultierenden Risiken in die Wissensdatenbank überführt.

Automatisierte Prüfung der Software

Eine umfassende Betrachtung der IT-Sicherheitsrisiken von Software muss auch grundlegende Sicherheitsprobleme, wie sie in der umgesetzten Software-Architektur bestehen könnten (z. B. fehlende Verschlüsselung, fehlerhafte Berechtigungsprüfung und ungeschützte Einstiegspunkte), identifizieren. Insbesondere muss die architekturelle Risikoanalyse mit der konkreten Implementierung der Software verbunden werden und nicht nur auf oft zu abstrakten oder ohnehin unvollständigen Architekturbeschreibungen stattfinden. Da eine manuelle architekturelle Analyse häufig sehr aufwändig ist und ein umfangreiches Expertenwissen erfordert, sollte dieser Schritt durch Tools unterstützt werden. Daher wird im PortSec-Projekt ein softwarezentrierter Ansatz verfolgt, bei dem IT-Sicherheitsrisiken auf Basis der

implementierten Software-Architektur möglichst automatisiert abgeleitet werden.

Die Abbildung 1 zeigt die einzelnen Schritte des geplanten Ansatzes. Zunächst wird mithilfe von Programmanalysen die implementierte Softwarearchitektur automatisiert aus dem Quellcode des Hafentelematiksystems extrahiert. Die Softwarearchitektur erlaubt es, grundsätzliche Sicherheitsrisiken der Software in Bezug auf mögliche Cyberangriffe zu identifizieren, insbesondere bzgl. der Autorisierung (wie z. B. unsichere Mandantentrennung, fehlerhaftes Rollenmodell, unsichere/fehlende Verwendung von Authentisierungsinformationen bei der Autorisierung). Die wiedergewonnene Softwarearchitektur wird dann um Beschreibungen des Netzes ergänzt, in dem das System betrieben wird.

Die Netzinfrastruktur wird dabei automatisiert erfasst. Insgesamt ergibt sich aus Softwarearchitektur und Informationen über die Netzinfrastruktur eine umfassende Systemarchitektur, die dann Gegenstand der Sicherheitsbetrachtungen ist.

Förderkennzeichen:
16KIS0582K, 16KIS0583 bis 16KIS0585

- Institut für Seeverkehrswirtschaft und Logistik (ISL)
- dbh Logistics IT AG
- datenschutz cert GmbH
- Universität Bremen

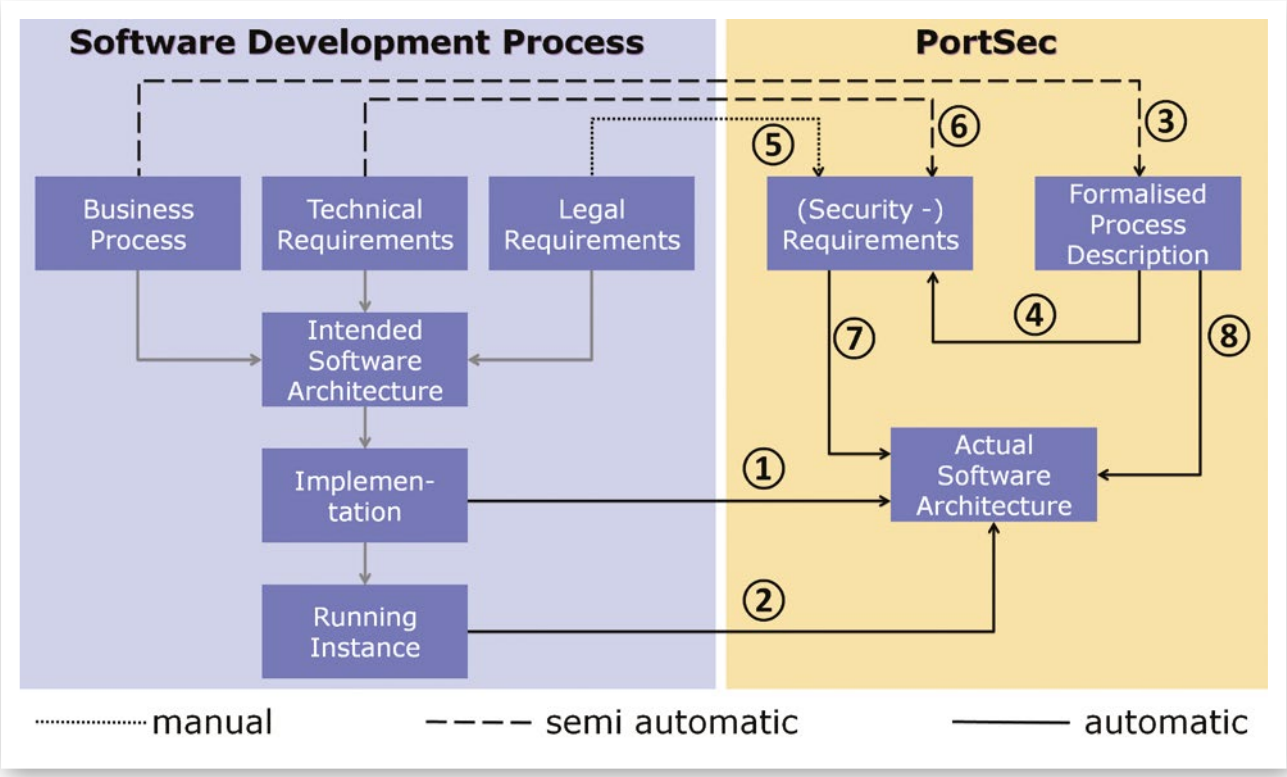


Abb. 1: Konzept zur automatisierten Software-Prüfung

PREVENT – Ein integriertes Framework zum präventiven Krisen- und Risiko-Management

Torsten Bollen

Forschungsprojekt:
PREVENT

Moderne Gesellschaften sind in hohem Maße abhängig von hochintegrierten IT-Systemen und anderen technischen Infrastrukturen, die grundlegende Dienste für das soziale und ökonomische Zusammenleben bereitstellen. Solche Systeme, seien es Kommunikationsnetze, Netze für die intelligente Stromversorgung oder Rechenzentren, integrieren Prozesse und Dienstleistungen über Firmengrenzen hinweg und basieren auf Komponenten verschiedenster Hersteller. Wenn sensible Daten verwaltet oder wichtige Abläufe gesteuert werden und Störungen, Fehlfunktionen oder Ausfälle schwerwiegende sowie weitreichende Folgen hätten, handelt es sich um Kritische Infrastrukturen. Derartige Systeme sind über eine Vielzahl organisatorischer und technischer Schnittstellen in ihre Umgebung integriert und bieten allein schon deshalb eine Vielzahl möglicher Angriffsvektoren, über welche etwa die Verfügbarkeit der Infrastruktur beeinträchtigt werden kann oder sensible Daten gestohlen bzw. manipuliert werden können. Der aktuelle Trend in Richtung Virtualisierung sowie die Tendenz, wichtige Dienste nicht mehr selber betreiben zu wollen, sondern an zentrale Betreiber zu übergeben (Outsourcing) bzw. in die Cloud zu verlegen (Cloudsourcing), stellen – gerade im Hinblick auf Themen wie IT-Sicherheit und Datenschutz sowie deren entsprechende Einbettung in rechtlich-regulatorische Rahmenbedingungen – eine Reihe neuer Herausforderungen dar, die sich speziell an die Betreiber solcher Kritischen Infrastrukturen richten. So muss z. B. besonders in kritischen Prozessen eine Organisation nicht nur sicherstellen, dass sie Daten kontrolliert bei einem Dienstleister bzw. in der Cloud verarbeiten lassen kann, sondern auch, dass sie selber in der Lage ist, dies sicher zu tun, es zu kontrollieren und zu bemessen sowie ihre Sicherheitsinteressen gegenüber dem Dienstleister bzw. Cloud-Anbieter durchzusetzen.

Der zentrale Gegenstand von PREVENT ist das IT-Sicherheits-, Risiko- und Compliance-Management für Rechenzentren systemrelevanter Banken. Solche Rechenzentren sind kritisch, weil sie der Umschlagplatz für große Geldmengen sind. Ihr korrektes Funktionieren und ihre Verfügbarkeit sind zentral für den nationalen und internationalen Zahlungsverkehr und damit für die Geschäftsfähigkeit eines Landes. Darüber hinaus ist der sichere und vertrauliche Umgang mit Finanzdaten die Grundlage für das Vertrauen der Kunden in die elektronische Finanzinfrastruktur und damit die entscheidende Geschäftsgrundlage einer Bank bzw. Grundlage für das Funktionieren elektronischer Handels- und Bezahlmodelle überhaupt.

Geld, insbesondere viel Geld, weckt auf der anderen Seite Begehrlichkeiten. Das Rechenzentrum einer Bank ist nicht nur interessant für einfache Hacker, sondern im Besonderen interessant für den Zugriff durch organisierte Kriminalität, Geheimdienste und politisch motivierten Terrorismus. Zusätzlich dazu sind in den letzten Jahren die Schäden durch Insider-Angriffe und interne, nichtlegitimierte Datenzugriffe immens gestiegen.

Ein effektives IT-Sicherheits-, Risiko- und Compliance-Management gehört zu den fünf wichtigsten Sicherheitsinitiativen zur Absicherung von IT-gestützten Prozessen im Finanzwesen. Es ist die notwendige Basis, um im Betrieb sicherheitsrelevante Entscheidungen fundiert und angemessen treffen zu können. Derzeit verfügbare Ansätze für ein IT-Sicherheits-, Risiko- und Compliance-Management sind in der Regel heterogen, scheitern häufig an der Komplexität hochintegrierter IT-Systeme und ihren vernetzten Abhängigkeiten und sind zu träge, um eine konkrete Entscheidungshilfe in einer akuten Krisensituation bieten zu können. Genau an dieser Stelle setzen wir mit unserem Forschungsvorhaben an und bieten mit der konzeptionellen und technischen Entwicklung eines Integrierten Frameworks zum präventiven Krisen- und Risikomanagement für Rechenzentren systemrelevanter Banken eine Lösung an, die den Anforderungen nach der Konvergenz von technischen IT-Sicherheitslösungen, Risikomanagement und Compliance-Management gerecht wird und durch die Bereitstellung von Echtzeitdaten und speziell für den Finanzsektor zugeschnittenen Sicherheitsindikatoren ein Instrument für kritische Entscheidungen sowohl im Normalbetrieb wie auch in Krisensituationen zur Verfügung stellt.

Förderkennzeichen:
16KIS0182K, 16KIS0183 bis 16KIS0185

- Wincor Nixdorf International GmbH
- Fraunhofer-Institut für offene Kommunikationssysteme FOKUS
- xiv-consult GmbH
- Unicredit Bank AG

RiskViz – Risikolagebild der industriellen IT-Sicherheit in Deutschland

Constance Baban, Jan-Ole Malchow, Matthias Niedermaier

Forschungsprojekt:
RiskViz

Cyberangriffe auf Kritische Infrastrukturen (KRITIS) werden für Unternehmen und öffentliche Einrichtungen und somit auch für die Bevölkerung zunehmend bedrohlicher. Gleichzeitig sind industrielle Kontrollsysteme (ICS), welche auch in Kritischen Infrastrukturen zum Einsatz kommen, teilweise oft unabsichtlich über das Internet erreichbar. Die Ursache hierfür kann zum Beispiel eine fehlerhafte Konfiguration oder schlicht die Forderung nach einer effizienten Fernwartung ohne angemessene Betrachtung der IT-Sicherheit sein. Aktuelle und vergangene Sicherheitsvorfälle zeigen wiederholt auf, dass die mit dem Internet verbundene IT-Umgebung als Einfallstor für Netzwerkeinbrüche, Datendiebstähle und Denial-of-Service-Attacken in die industrielle Umgebung von beispielsweise Energieversorgern und anderen Kritischen Infrastrukturen dienen kann. Gleichzeitig haben Bund, Länder und Kommunen, in denen Kritische Infrastrukturen angesiedelt sind, keine geeignete Möglichkeit, das Ausmaß der Bedrohung zu erfassen und dadurch für die Betreiber transparent zu machen. Zudem sind Kritische Infrastrukturen gegen Schäden durch IT-Sicherheitslücken nur schwierig zu versichern, da hier die potenziellen Schäden sehr groß und die Risiken nur schwer zu berechnen sind.

Im Rahmen des IT-Sicherheitsforschungsprogramms fördert das Bundesministerium für Bildung und Forschung (BMBF) deshalb das Projekt „RiskViz – Risikolagebild der industriellen IT-Sicherheit in Deutschland“ (Förderkennzeichen: 16KIS0251K). Das Konsortium besteht aus Forschungseinrichtungen sowie Unternehmen aus der Industrie. Aufseiten der Forschung und Wissenschaft sind die Hochschule Augsburg, die Freie Universität Berlin sowie das Brandenburgische Institut für Gesellschaft und Sicherheit vertreten. Als praxisnahe und industrielle Partner sind das Technologie Centrum Westbayern, die LEW Verteilnetz GmbH, die genua GmbH, die Koramis GmbH sowie die Munich RE AG Teil des Konsortiums.

Das RiskViz-Konsortium entwickelt Methoden und Instrumente, um mangelhaft geschützte Steuerungssysteme zu identifizieren. Dies muss zudem auf eine rechtskonforme Weise geschehen. Dafür wurde in dem Vorhaben zunächst eine Suchmaschine entwickelt, die ICS findet und Informationen zu ihnen und ihrer Bedrohungslage sammelt, ohne dabei ihren Betrieb zu stören. Ziel des Verbundvorhabens ist es, durch gezielte Informationsbeschaffung die Cybersicherheit der deutschen Wirtschaft und insbesondere Kritischer Infrastrukturen zu verbessern.

Die Suchmaschine ist sowohl im Internet als auch intern in Unternehmensnetzwerken einsetzbar. Des Weiteren sind Werkzeuge entstanden, um die gesammelten Informationen algorithmisch und visuell zu bewerten und hieraus resultierende Erkenntnisse hinsichtlich des IT-Sicherheits-Schutzbedarfs effektiv zu kommunizieren. Die Ergebnisse der RiskViz-Suchmaschine werden hierfür mit weiteren Daten verknüpft. Zu diesen Daten gehören Schwachstellendaten sowie Wirtschafts- und Branchendaten, die im Vorhaben auf ihre Relevanz für die IT-Sicherheit hin untersucht werden. Ein Ziel der Analysen ist es, gefährdete ICSs entsprechenden Betreibern (Kommunen oder Unternehmen) zuzuordnen, damit diese Betreiber gewarnt werden und ihr eigenes Netzwerk schützen können. Zudem helfen die Projektergebnisse Versicherungen bei der Einschätzung des Schadenpotenzials von Cyberrisiken. Da mittels der RiskViz-Suchmaschine sensible Daten erhoben werden, wurden Datenschutzanforderungen berücksichtigt und im Rahmen des Vorhabens zudem Zugriffsberechtigungen geklärt.

Zu den im Vorhaben RiskViz angestrebten Innovationen zählt zunächst eine neuartige Suchmaschine zum Aufspüren von ICSs und zur Bewertung von Risiken, die aus ihrer Erreichbarkeit im Internet resultieren. Dabei wird sichergestellt, dass die Suche nach Sicherheitsrisiken keinerlei Schäden an den untersuchten Anlagen verursacht.

Dieses Forschungsprojekt wird vom Bundesministerium für Bildung und Forschung über die VDI/VDE Innovation + Technik GmbH gefördert.

Förderkennzeichen:
16KIS0251K, 16KIS0252 bis 16KIS0258

- Hochschule Augsburg
- Brandenburgisches Institut für Gesellschaft und Sicherheit
- Freie Universität Berlin
- Munich RE AG
- genua GmbH
- KORAMIS GmbH
- Technologie Centrum Westbayern
- LEW Verteilnetz GmbH

SecMaaS – Security Management as a Service

Daniel Augustin, Markus Hoffmann

Forschungsprojekt:
SecMaaS

Motivation

Das Projekt SecMaaS (Security Management as a Service) wird von der Hochschule Darmstadt, der Bundesdruckerei GmbH, der KommWis GmbH sowie den Bürgerämtern in Siegburg und Saarbrücken durchgeführt.

Das Ziel ist die Erforschung und Entwicklung einer cloudbasierten Lösung, die Mitarbeiterinnen und Mitarbeiter (vor allem Informationssicherheitsbeauftrage und IT-Administratoren) kommunaler Behörden zielgerichtet und anwenderorientiert bei der Etablierung eines Informationssicherheitsmanagements unterstützt.

Viele Aufgaben, die von kommunalen Bürgerämtern übernommen werden, wie zum Beispiel das Pass-, Personal- und Meldewesen, sind durch bundesgesetzliche Regelungen vorgeschrieben, viele andere durch Landesgesetze, die sich daher in ihren Abläufen in der Regel nicht allzu stark voneinander unterscheiden. Gleiches gilt für die von diesen Behörden umzusetzenden Sicherheitsziele.

Vorgehen

Aufgrund der ähnlichen Aufgabenbereiche und des Einsatzes standardisierter IT-Komponenten sind zudem die in den kommunalen Behörden eingesetzten IT-Infrastrukturen sehr ähnlich. In unseren Untersuchungen konnten wir im Wesentlichen drei verschiedene Infrastrukturen beobachten:

1) Behörden, die die IT-Infrastruktur allein betreiben,

2) Behörden, die ihre IT-Infrastruktur von sogenannten kommunalen Rechenzentren betreiben lassen, und

3) Behörden, die Teile der IT-Infrastruktur selbst betreiben und andere Teile an kommunale Rechenzentren ausgelagert haben.

Damit können aber auch die ersten Schritte zur Erarbeitung eines IT-Sicherheitskonzepts (IT-Strukturanalyse, Schutzbedarfsanalyse [der Daten, IT-Komponenten, Netze, Räumlichkeiten], Gefährdungs- und Risikoanalyse) analog für verschiedene kommunale Bürgerämter durchgeführt werden. Bei der Auswahl geeigneter Schutzmaßnahmen muss dann auf die konkreten Bedürfnisse einzelner Behörden eingegangen werden.

SecMaaS ermittelt die verschiedenen IT-Infrastrukturen durch Befragungen und Beobachtungen, erarbeitet allgemeine Sicherheitskonzepte für die verschiedenen IT-Infrastrukturen und stellt, darauf aufbauend, technische Hilfsmittel zur Konkretisierung und Umsetzung von Sicherheitsmaßnahmen bereit und adressiert damit zuallererst die beiden Aspekte: Mensch und Organisation.

Ziele

Das Projekt hat zum Ziel, die Mitarbeiter in Behörden bei der Umsetzung eines Informationssicherheitskonzeptes durch eine cloudbasierte Plattform organisatorisch zu unterstützen und zu leiten. Diese Unterstützung führt zu einer besseren Umsetzung von Schutzkonzepten. Der Cloud-Dienst erinnert an organisatorische Maßnahmen und stellt so die Wirksamkeit des Sicherheitskonzeptes sicher.

Förderkennzeichen:
16KISO162K, 16KISO163 bis 16KISO166

- Bundesdruckerei GmbH
- KommWIS – Gesellschaft für Kommunikation und Wissenstransfer mbH
- Landeshauptstadt Saarbrücken
- Kreisstadt Siegburg
- Hochschule Darmstadt

SICIA – IT-Sicherheit in kritischen Netzen messen und systematisch verbessern

Franka Schuster, Andreas Paul, Hartmut König

Forschungsprojekt:
SICIA

Ausgangslage

Wie in vielen anderen Bereichen kommen auch in Kraftwerken und Energieversorgungsnetzen zunehmend Technologien und Komponenten aus der klassischen IT zum Einsatz. Für die Führung der Kraftwerke und Verteilnetzprozesse werden unterschiedliche Leitsysteme und prozessnahe Rechnersysteme (PRS) bestehend aus jeweils mehreren hundert Komponenten eingesetzt, die über lokale und Weitverkehrsnetze unter Einsatz bewährter Technologien (wie des Ethernet-Standards) bis auf die untersten Automatisierungsebenen vernetzt sind. Daher sind diese Netze mittlerweile ebenfalls anfällig für klassische IT-Gefährdungen und geraten zunehmend in den Fokus sicherheitsrelevanter Betrachtungen. Spätestens Angriffe wie Stuxnet [1], Flame [2] und Duqu [3] machten auf bisher unbekannte Möglichkeiten der Sabotage aufmerksam, die zu einem Totalausfall ganzer Infrastrukturen, z. B. der Energieversorgung, führen können. Zwar existiert bereits eine Reihe von externen und internen Richtlinien hinsichtlich der IT-Sicherheit in technischen Anlagen im Energiebereich [4, 5, 6]. Sie fassen entweder generelle Maßnahmen zur Gewährleistung der IT-Sicherheit zusammen oder zeigen die Ableitung von Schutzmaßnahmen für eine gegebene Infrastruktur nur in abstrakter Form auf. Eine gezielte Erhöhung der IT-Sicherheit einer konkreten Infrastruktur sowie die Einhaltung des Mitte 2015 in Kraft getretenen IT-Sicherheitsgesetzes [7] erfordern jedoch die Messung des Ist-Zustands sowie eine systematische Ableitung und Dokumentation von Verbesserungsmaßnahmen. Ein konkretes Vorgehen, wie diese drei Anforderungen umsetzbar sind, existiert jedoch nicht.

Zielsetzung

Ziel des Verbundprojekts SICIA ist die Entwicklung eines solchen Bewertungsprozesses für Kritische Infrastrukturen der Energieversorgung, der die Implementierung und regelmäßige Durchführung von Schritten kontinuierlicher Sicherheitsprozesse, wie Informationssicherheitsmanagementsystemen (ISMS), unterstützt [8]. Im Gegensatz zu existierenden Bewertungsverfahren wird auf die Betrachtung von Vermögenswerten sowie für Kritische Infrastrukturen schwer bestimmbarer (und oftmals willkürlich festgelegter) Bedrohungen zunächst verzichtet. Stattdessen wird für jede Infrastrukturkomponente (einzelnes technisches Gerät) ein belastbarer Sicherheitsindikator ermittelt, der sich auf verlässliche technische und organisatorische Kriterien, wie die Konfiguration von Systemkomponenten, ihre Vernetzung mit anderen Komponenten sowie ihre Verfügbarkeitsanforderungen stützt. Messgrundlage sind technische Kriterien der DIN ISO/IEC 27002 [9], DIN ISO/IEC TR 27019 [5] und des ICS-Security-Kompendiums des BSI [10].

> Bewertungsprozess für KRITIS der Energieversorgung durch die Ermittlung von Sicherheitsindikatoren diverser Systemkomponenten

Die berechneten Indikatoren können sukzessive zu Sicherheitsindikatoren von Systemen oder anderen Funktionseinheiten für die Betrachtung auf beliebiger Ebene verdichtet werden. Auf diese Weise wird (1) der Sicherheitsgrad von Funktionseinheiten auf der jeweiligen Betrachtungsebene greifbar, (2) sicherere von unsichereren Systembestandteilen durch Vergleich der Indikatoren unterscheidbar und (3) eine fundierte Messgrundlage für eine aufbauende, eher qualitative Risikoanalyse mit Bedrohungspotential und Schadensausmaß bereitgestellt. Die softwarebasierte Erfassung und Bewertung erlaubt zudem die automatische Ableitung infrage kommender Verbesserungsmaßnahmen und die Simulation des potenziellen Effekts ihrer Umsetzung auf die IT-Sicherheit der jeweiligen Infrastruktur. Der Bewertungsprozess und das Gesamtverfahren werden anhand exemplarischer Infrastrukturen der Verbundpartner der LEAG Lausitz Energie Kraftwerke AG (vormals Vattenfall Europe Generation AG), der RWE AG und deren Tochterunternehmen innogy SE konzipiert, die durch große Heterogenität in der Struktur, in der eingesetzten Technik und deren Zulieferern gekennzeichnet sind. So wird die Entwicklung eines Verfahrens bestehend aus möglichst breit einsetzbaren Teilmethoden und Software-Werkzeugen sichergestellt.

Förderkennzeichen:
16KIS0158K, 16KIS0159 bis 16KIS0161

- Brandenburgische Technische Universität Cottbus-Senftenberg
- LEAG Lausitz Energie Kraftwerke AG
- RWE AG
- innogy SE

Quellen

[1] Symantec Security Response: W32.Stuxnet Dossier, 2011.

[2] Symantec Security Response. W32.Flamer: Microsoft Windows Update Man-in-the-Middle, 2012.

[3] Chien, E.; Murchu, L. O.; Falliere, N.: W32.Duqu: The Precursor to the Next Stuxnet. In: Proceedings of the 5th USENIX conference on Large-Scale Exploits and Emergent Threats, LEET'12. USENIX Association, Berkeley, USA, 2012.

[4] DIN ISO/IEC TR 27019: Informationstechnik – Sicherheitsverfahren – Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002.

[5] VGB PowerTech: IT-Sicherheit für Erzeugungsanlagen (VGB-S-175), 2014.

[6] VDI/VDE 2182: Informationssicherheit in der industriellen Automatisierung, 2011.

[7] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), Bundesgesetzblatt 2015 Teil I Nr. 31, 24.07.2015.

[8] Schuster, Franka; Paul, Andreas; König, Hartmut: Messung der technischen IT-Sicherheit in Energieversorgungsanlagen zur Erfüllung des IT-Sicherheitsgesetzes. In: VGB PowerTech Journal 3/2017. VGB Powertech e. V.

[9] DIN ISO/IEC 27002: Informationstechnik – IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management.

[10] Bundesamt für Sicherheit in der Informationstechnik: ICS-Security-Kompendium, 2013.

SIDATE – Sichere Informationsnetze bei kleinen und mittleren Energieversorgern

Julian Dax, Daniel Hamburg, Sebastian Pape, Volkmar Pipek, Kai Rannenberg, Christopher Schmitz, André Sekulla, Frank Terhaag

Forschungsprojekt:
SIDATE

Motivation

Eine reibungslos und sicher funktionierende Energieinfrastruktur ist für fast alle Lebensbereiche der heutigen Gesellschaft grundlegend. Der Schutz dieser Infrastrukturen liegt dementsprechend im Interesse der Allgemeinheit. Um den Anforderungen an eine sichere und nachhaltige Energieversorgung im Rahmen der Energiewende gerecht zu werden, wird auch im Energiesektor immer mehr Informations- und Kommunikationstechnik (IKT) eingesetzt. Durch die Entwicklung neuer Ansätze zur Steigerung von Effektivität und Effizienz unterliegt diese ständigen Veränderungen. Die Abwehr von Angriffen auf diese Kritischen Infrastrukturen ist darum eine ständig wachsende Herausforderung. Die meist privatwirtschaftlichen Betreiber stehen dabei vor einer schwierigen Aufgabe: Sie müssen sowohl den Schutz als auch die Wirtschaftlichkeit ihrer Infrastrukturen sicherstellen. Speziell kleine Betreiber mit kleinen IKT-Abteilungen, die dann oft auch eher kleine IT-Sicherheitsabteilungen mit sich bringen, sind hier besonders herausgefordert. Ziel des Projektes ist es, hier Lösungsansätze aufzuzeigen.

Ziele und Vorgehen

Im Forschungsprojekt SIDATE werden Werkzeuge und Konzepte entwickelt, die eine bessere Einschätzung des vorhandenen Sicherheitsniveaus ermöglichen und damit gleichzeitig helfen, die Sicherheit der Infrastrukturen kleiner und mittlerer Betreiberfirmen zu verbessern. Dabei liegt ein besonderes Augenmerk auf der Praxistauglichkeit der Werkzeuge und Konzepte, die auch für Betreiber mit wirtschaftlichen, organisatorischen und personellen Besonderheiten anwendbar sein sollen. Erarbeitet werden unter anderem Metriken zur Erfassung des Sicherheitsniveaus, eine Beschreibungssprache zur Abbildung der grundlegenden Elemente und Abhängigkeiten der Infrastruktur sowie eine Wissensdatenbank und eine Kooperationsplattform zur Unterstützung organisationsinterner sowie überorganisationaler Kollaborations- und Austauschprozesse. Um eine möglichst große Anwenderfreundlichkeit, auch für Anwender mit verschiedenen Anwendungs- und Kompetenzprofilen, zu erreichen, werden dabei verschiedene Stakeholder und speziell kleine und mittlere Betreiber sowie Hersteller von Fernwirksystemen in den Prozess mit eingebunden.

Innovationen und Perspektiven

Neu an diesem Ansatz ist – neben der Fokussierung auf kleine und mittlere Unternehmen – dass Selbsteinschätzungen eine entscheidende Rolle spielen. Mit dem Werkzeugkasten sollen Betreiber deutlich schneller und zuverlässiger feststellen können, ob alle gesetzlichen Auflagen und Richtlinien zur Absicherung der kritischen Versorgungsinfrastrukturen erfüllt sind. Ob die Umsetzung auch effektiv und wirtschaftlich erfolgt, lässt sich mithilfe von Best- bzw. Good-Practice-Sammlungen beantworten.

Förderkennzeichen:
16KIS0239K, 16KIS0240 bis 16KIS0243

- Universität Siegen
- Goethe-Universität Frankfurt am Main
- TÜV Rheinland i-sec GmbH
- regio iT gesellschaft für informationstechnologie mbH
- Arbeitsgemeinschaft für sparsame Energie- und Wasserverwendung im VKU

SURF – Systemic Security for Critical Infrastructures

Team SURF

Forschungsprojekt:
SURF

Eine funktionierende Energie- und Wasserversorgung, aber auch ein sicherer ÖPNV und ein verlässlicher Flughafenbetrieb sind für unsere Wirtschaft und unsere Gesellschaft von besonderer Bedeutung – sie zählen zu den sogenannten Kritischen Infrastrukturen. Eine ausreichende IT-Sicherheit, und hier insbesondere die Netzwerksicherheit, sind in diesen Bereichen unverzichtbar, um Manipulationen und Ausspähversuche durch Cyberangriffe festzustellen und abzuwehren.

Die heute verfügbaren Lösungen für IT-Sicherheit sind für diese kritischen Systeme unzureichend. Oft werden internetbasierte Kommunikationsinfrastrukturen genutzt, die besonders viele Optionen für Angriffe bieten. Die typische Vorgehensweise beim Betrieb von IT-Systemen, mit Updates Lücken zu schließen und Fehler zu beheben, ist bei produktionsnahen Systemen – wie sie z. B. in Kraftwerken anzutreffen sind – nicht möglich. Erschwerend kommt hinzu, dass Betriebsmittel in Kritischen Infrastrukturen – und dazu zählen auch eingebettete Systeme – deutlich längere Nutzungszeiten aufweisen. Der Austausch dieser Geräte ist aufwendig, Anpassungen sind kaum möglich und Sicherheitsfunktionen können häufig nicht nachträglich ergänzt werden.

Ziele und Vorgehen von SURF

Das Verbundprojekt SURF (Systemic Security for Critical Infrastructures; Entwicklung einer ganzheitlichen Lösung zur Verbesserung der Schutzsysteme für Kritische Infrastrukturen) widmet sich der grundlegenden Verbesserung der Schutzsysteme für Kritische Infrastrukturen. Dabei stehen neben der IT-Sicherheit auch Aspekte wie Alltagstauglichkeit, Bedienbarkeit und Kosten-effizienz im Vordergrund. Dies will das Konsortium mit einem ganzheitlichen Ansatz umfassend berücksichtigen. Neuartige Sicherheitskonzepte müssen zudem bestehende Altsysteme einbet-ten, ohne deren Funktionalität einzuschränken und ohne existierende Zertifizierungen bezüglich der funktionalen Sicherheit abzuschwächen. Um diese Ziele zu erreichen, ist eine Reihe von Entwicklungen notwendig: Diese reichen von der Härtung von Netzkomponenten, der Absiche-rung der Geräte mit speziellen Sicherheitschips, einem neuartigen hardware-basierten Integri-tätsschutz der IT-Systeme und der zuverlässigen und vollständigen Erfassung von Netzinforma-tionen bis hin zur Auswertung und Visualisierung der Informationen hinsichtlich Anomalien sowie der Risikobewertung von Zuständen.

Ergebnisse von SURF

Infineon baute im Rahmen des SURF-Projekts verschiedene Demonstratoren auf Basis der TPM-Plattform (Trusted Platform Module) auf. Verschiedene Anwendungsfälle wurden entwickelt und getestet und auf Messen und bei anderen öffentlichen Gelegenheiten präsentiert.

Von Airbus Group Innovations wurde eine umfangreiche Prüfung von realistischen Angriffsszenarien inkl. einer detaillierten Risikoanalyse innerhalb des Kabinennetzes realisiert. Zusätzlich wurden diverse Messungen in einem Kabinen-Mock-up durchgeführt.

Das Fraunhofer SIT entwickelte eine Reihe von Technologien und Vorgehensweisen zur Absicherung der Integrität von Geräten in Kritischen Infrastrukturen. Ein besonderer Fokus lag dabei auf der Entwicklung von TPM-1.2-, TPM-2.0- und TSS-2.0-basierten Lösungen. Es wurden zwei Protokolle – TUDA 1 und TUDA 2 – entwickelt, die Integritätsinformationen von Geräten in einem kontinuierlichen Monitoring zur Verfügung stellen können. Diese Protokolle werden in der IETF weiterentwickelt und zur Standardisierung vorgeschlagen. Eine prototypische Umsetzung wurde gemeinsam mit den Partnern Infineon und Hirschmann durchgeführt und damit gezeigt, dass ein praxistaugliches Gerät mit diesen Technologien ausgestattet werden kann. Außerdem wurde gemeinsam mit der Technischen Hochschule Deggendorf ein Konzept für Vorschaltboxen weiterentwickelt, um eine Retrofitting-Lösung für solche Geräte bereitstellen zu können, die keine TPMs integriert haben. Der Software-Stack zur Nutzung von TPM 2.0 wurde weiterentwickelt und mehrere Evaluationspattformen für TPM-basierte Lösungen wurden auf Basis eines Banana-Pi-Routers, Raspberry-Pi- und NUC-Rechners umgesetzt.

Hirschmann entwickelte eine Klassifizierung verschiedener Level der Gerätesicherheit. Weiterhin unterstützte Hirschmann die Entwicklung eines Verfahrens zur zeitbasierten unidirektionalen Attestierung (TUDA) von Geräten in enger Zusammenarbeit mit dem Fraunhofer

SIT. Mit den Partnern SIT und Infineon setzte Hirschmann eine prototypische Implementierung eines durch ein TPM abgesicherten Netzwerkgerätes sowie TUDA auf Basis einer industriellen Firewall von Hirschmann sowie dem Netzwerkmanagement-Tool Industrial HiVision um. Auf Basis dieses Prototyps wurde gemeinsam mit dem SIT ein Demonstrator entwickelt, der die Funktionsweise von TUDA veranschaulicht.

Die Technische Hochschule Deggendorf (THD) entwickelte im Projekt SURF passive Ansätze zur Erkennung von Anomalien innerhalb von Netzwerken, die die Netzwerke nicht negativ beeinträchtigen. Hierbei entstanden die Prototypen für eine Messsonde und für ein Vorschaltgerät, die zusammen Pakete über das Netzwerk vor Ort interpretieren und Warnungen generieren, die später bei einer Korrelationsstelle zusammengefasst und in einen Kontext gebracht werden können. In der Kooperation mit den Projektpartnern wurden die Prototypen an die Anforderungen Kritischer Infrastrukturen angepasst und die in den Prototypen generierten Informationen den akademischen Partnern für eine Korrelation zur Verfügung gestellt.

Im Projekt SURF entwickelte die TUM ein umfassendes Incident-Handling-System. Dieses basiert auf dem Blackboard Pattern und verwendet daher eine zentrale Informationsverteilungskomponente. Zusätzlich wurden folgende Module entwickelt: ein anomaliebasiertes Intrusion-Detection-System zur Protokollanalyse, ein Reaktionsidentifizierungsmodul, ein Reaktionsauswahlmodul inklusive Metriken zur situativen Bewertung und ein Reaktionsausführungsmodul. Zusätzlich wurde ein Tool zur grafischen Analyse des Netzverkehrs entwickelt sowie ein Verfahren zur Berechnung der Ausfallsicherheit unter Berücksichtigung von Redundanz.

Der Flughafen München definierte im Rahmen des Projektes einen praxisrelevanten Use Case im Umfeld der Gebäudeautomation auf Basis des Protokolls BACNet/IP. In Zusammenarbeit mit den Projektpartnern wurden verschiedene Untersuchungen des Protokolls und des Netzwerk-Verkehrs durchgeführt, um daraus geeignete Schutzmaßnahmen zu entwickeln. Es wurde ein auf Funktionalität und Sicherheit hin optimiertes Netzwerkdesign für die Gebäudeautomation entwickelt und zusammen mit Projektpartnern erprobt. Während dieses Proof of Concept wurden weitere Sicherheitstechnologien, welche im Rahmen des Projektes entwickelt wurden, unter realen Bedingungen validiert.

Ausgewählte Veröffentlichungen

- Wachs, M.; Herold, N.; Posselt, S. A.; Dold F.; Carle G. (2016): GPLMT: A Lightweight Experimentation and Testbed Management Framework, in: Karagiannis, T.; Dimitropoulos X. (eds.): Passive and Active Measurement. PAM 2016. Lecture Notes in Computer Science, vol. 9631. Cham: Springer.

- Herold, N.; Posselt, S. A.; Hanka, O.; Carle, G. (2016): Anomaly detection for SOME/IP using complex event processing, in: NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium. Istanbul, 2016, pp. 1221-1226. doi: 10.1109/NOMS.2016.7502991.

- Herold, N.; Kinkelin, H.; Carle, G. (2016): Collaborative Incident Handling Based on the Blackboard-Pattern, in: WISCS ,16 Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, pp. 25-34.

- Herold, N.; Wachs, M.; Posselt, S. A.; Carle, G. (2017): An Optimal Metric-Aware Response Selection Strategy for Intrusion Response Systems, in: Cuppens, F.; Wang, L.; Cuppens-Boulahia, N.; Tawbi, N.; Garcia-Alfaro, J. (eds.): Foundations and Practice of Security. FPS 2016. LNCS, vol. 10128. Cham: Springer.

Förderkennzeichen:
16KIS140K, 16KIS0041, 16KIS0042, 16KIS0044-16KIS0046, 16KIS0305

- Infineon Technologies AG
- Hirschmann Automation & Control GmbH
- Technische Hochschule Deggendorf
- Fraunhofer-Institut für Sichere Informationstechnologie SIT
- Technische Universität München
- Airbus Group Innovations
- Flughafen München GmbH

VeSiKi – Das Begleitforschungsprojekt Vernetzte IT-Sicherheit Kritischer Infrastrukturen

B. Buchner, S. Dännart, T. Diefenbach, A. Fritzsche, A. Harner, M. Hofmeier, M. Jalowski, D.-K. Kipker, U. Lechner, K. Möslein, S. Müller, M. Raß, A. Rieb, S. Rudel

Forschungsprojekt:
VeSIKi

VeSiKi ist das wissenschaftliche Begleitforschungsprojekt des Förderschwerpunktes IT-Sicherheit für Kritische Infrastrukturen (ITS|KRITIS).

Kooperativer Forschungsprozess im Förderschwerpunkt

VeSiKi beschäftigt sich mit neuen, sektorenübergreifenden Ansätzen zur Beurteilung der IT-Sicherheit Kritischer Infrastrukturen und erarbeitet Verbesserungsvorschläge für bestehende technische sowie etablierte Prozesse. Des Weiteren unterstützt VeSiKi den kooperativen Forschungsprozess der Verbundprojekte, koordiniert die Zusammenarbeit, unterstützt die Außendarstellung des Förderschwerpunkts und die Sichtbarkeit der Aktivitäten und Ergebnisse in der Öffentlichkeit sowie den Transfer in die Praxis.

Im Begleitforschungsprojekt VeSiKi arbeiten Forscher des Lehrstuhls für Wirtschaftsinformatik der Universität der Bundeswehr München, des Lehrstuhls für Wirtschaftsinformatik, insb. Innovation und Wertschöpfung, der Friedrich-Alexander-Universität Erlangen-Nürnberg, dem Institut für Informations-, Gesundheits- und Medizinrecht (IGMR) an der Universität Bremen sowie der Fachbereich Standardisierung und Innovation des DKE|VDE in Frankfurt zusammen.

Um seinen Aufgaben bei der Begleitung der Verbundprojekte gerecht zu werden, bedient sich VeSiKi verschiedener Werkzeuge und Maßnahmen. So wird die Vernetzung der Verbundprojekte beispielsweise durch Open-Innovation-Ansätze, die Plattform itskritis.de sowie die Förderung gemeinsamer wissenschaftlicher Veröffentlichungen unterstützt. Des Weiteren werden jedes Jahr für den Förderschwerpunkt Jahreskonferenzen und weitere Workshops ausgerichtet, die den kooperativen Forschungsprozess unterstützen.

Eigene Forschungsbeiträge

Darüber hinaus leistet VeSiKi eigene, die Arbeiten der anderen Verbünde flankierende Forschungsbeiträge. So wurde beispielsweise im Herbst 2016 der Monitor ITS|KRITIS, eine Studie zur Lage der IT-Sicherheit in Kritischen Infrastrukturen, durchgeführt. Dabei wurden IT-Sicherheitsverantwortliche zum Stand der IT-Sicherheit befragt und in der Auswertung Vergleiche zwischen KRITIS und Nicht-KRITIS gezogen. Die Ergebnisse dieser Studie wurden im Frühjahr 2017 veröffentlicht [1]. Die Folgestudie Monitor 2.0 wurde von Herbst 2017 bis Frühjahr 2018 durchgeführt und wird Mitte 2018 veröffentlicht [6].

Ein weiterer Forschungsschwerpunkt von VeSiKi ist Open Innovation [2] [3]. Im Fokus stehen dabei vor allem die Herausforderungen und Potenziale offener und kollaborativer Innovations- bzw. Forschungs- und Entwicklungsprozesse. Ein Beispiel hierfür ist die Einbeziehung von Besuchern in einem offenen Innovationslabor in Nürnberg. Diese können vor Ort aktiv ihre Ideen, Lösungsvorschläge und Ansichten zu Fragestellungen aus den Forschungsprojekten einbringen.

Im Rahmen von VeSiKi wurden weiterhin die IT-Security-Matchplays als eine spielerische Methode entwickelt, IT-Fachpersonal für das Thema IT-Sicherheit zu sensibilisieren. Eine Variante ist „Operation Digitale Schlange“, die auf der IT-Infrastruktur eines Krankenhauses basiert. „Operation Digitale Schlange“ wurde im Mai 2017 sowie im März 2018 mit Vertretern aus KRITIS sowie aus den Verbundprojekten gespielt. Ausführlicher werden die IT-Security-Matchplays in den Beiträgen [4] und [5] vorgestellt.

> Vernetzung und Unterstützung aller ITS|KRITIS Verbundprojekte durch die Etablierung eines kooperativen Forschungsprozesses

Um Betreibern Good Practices der IT-Sicherheit in KRITIS an die Hand zu geben, wurden von VeSiKi in Zusammenarbeit mit den Verbundprojekten Fallstudien erstellt und u. a. auf der Vernetzungsplattform itskritis.de sowie als Buch [7] veröffentlicht. Die Fallstudien beleuchten jeweils eine konkrete Lösung praxisorientiert aus verschiedenen Perspektiven. Bislang entstanden unter anderem Fallstudien zum Thema sichere Fernwartung, Lagebilder in Banken, zur Ransomware in Krankenhäusern sowie zur IT-Sicherheit in einer Kommune.

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

Darüber hinaus werden den Mitgliedern des Förderschwerpunktes sowie der interessierten Öffentlichkeit durch das IGMR verschiedene Informationsangebote zur aktuellen IT-Sicherheitsgesetzgebung in Deutschland und Europa zur Verfügung gestellt.

Förderkennzeichen:
16KIS0213K, 16KIS0214 bis 16KIS0216

- Universität der Bundeswehr München
- Friedrich-Alexander-Universität Erlangen-Nürnberg
- DKE/VDE
- Universität Bremen

Quellen

[1] Lechner, U. (Hrsg.): Monitor IT-Sicherheit Kritischer Infrastrukturen, Neubiberg, Universität der Bundeswehr München, 2017.

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

[3] Reichwald, R.; Piller, F.: Interaktive Wertschöpfung: Open Innovation, Individualisierung und neue Formen der Arbeitsteilung. Wiesbaden, 2009.

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

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

[6] Lechner, U. (Hrsg.): Monitor 2.0 IT-Sicherheit Kritischer Infrastrukturen, Neubiberg, Universität der Bundeswehr München, 2018.

[7] Lechner, U., Dännart, S., Rieb, A., Rudel, S. (Hrsg.): CASE KRITIS: Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen. Logos-Verlag, 2018.

Sektion 2
KRITIS-Bausteine der IT-Sicherheit

In dieser Sektion wird der Bezug zum IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) aufgezeigt.

In dem Förderschwerpunkt ITS|KRITIS wurden innovative Konzepte und Technologien zur Informationssicherheit erforscht. Die innovativen Ansätze der Informationssicherheit des Förderschwerpunkts IT-Sicherheit für Kritische Infrastrukturen sind in dieser Sektion aufgeführt – abstrahiert von den Sektoren Kritischer Infrastrukturen, die den Kontext für die Forschung lieferten.

Die Referenzwerke für diesen Abschnitt sind das IT-Grundschutz-Kompendium, das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegeben wird, und die IT-Grundschutz-Kataloge.

Während der Erstellung des vorliegenden State of the Art hat das BSI mit dem IT-Grundschutz-Kompendium einen neuen Ansatz zur Strukturierung des Themenfelds IT-Sicherheit entwickelt und so schlägt dieser Abschnitt hier die Brücke zwischen Bausteinen der IT-Sicherheit Kritischer Infrastrukturen zum Format des IT-Grundschutz-Kompendiums.

Review:

Manfred Hofmeier, Andreas Rieb und Ulrike Lechner

Sektion 2
Inhaltsverzeichnis

Das ITS|KRITIS-Kompendium der IT-Sicherheit für Kritische Infrastrukturen 36

- *Überlegungen des Verbundprojekts SICIA zum Sektor „Energie“* 38
- *Die Überlegungen von AQUA-IT-Lab zum Sektor „Wasser“* 39

Bausteine der IT-Sicherheit Kritischer Infrastrukturen 40

- Innovative Bausteine und Maßnahmen der IT-Sicherheit Kritischer Infrastrukturen 40
  - INDI: Bausteine der Schwachstellensuche und Angriffserkennung für Industrienetze 40
  - RiskViz: Bausteine Cyberversicherung und cyber-physische Systeme 40
  - RiskViz: Bausteine für eingebettete Systeme sowie innere und äußere Suche 41
  - RiskViz: Liste der Gefährdungen 41
  - PREVENT: Bausteine Rechenzentren und Kommunikationsnetzwerk 43
- Innovative Methoden der IT-Sicherheit für Kritische Infrastrukturen 45
  - AQUA-IT-Lab: Dynamische Maßnahmenkataloge 45
  - Cyber-Safe: Rollenspezifische Handlungshilfen 48
  - PortSec: Spezifischer Gefährdungskatalog 50
  - SICIA: Messung des Umsetzungsgrades aller gängigen Funktionen, Verfahren und Maßnahmen zur Erhöhung von IT-Sicherheit 50
  - SIDATE: Gefährdungen und Sicherheitsmaßnahmen 51

Das ITS|KRITIS-Kompendium der IT-Sicherheit für Kritische Infrastrukturen

Das IT-Grundschutz-Kompendium des Bundesamts für Sicherheit in der Informationstechnik legt Anforderungen an IT-Sicherheitsmaßnahmen fest. Die folgende Liste enthält Anforderungen an IT-Sicherheitstechnologien für Kritische Infrastrukturen – die folgenden Kapitel haben ihren Fokus auf den Technologien und Lösungen.

AQUA-IT-Lab

Für einen Sektor mit erhöhtem Schutzbedarf, spezifischen Industriestrukturen und spezifischen kritischen Geschäftsprozessen sollte es ein Verfahren geben, auf der Basis eines standardisierten und interaktiven Fragebogens einen auf die individuelle Organisation zugeschnittenen und effizienten Maßnahmenkatalog zu definieren.

CYBER SAFE

Für Technologien Kritischer Infrastrukturen und vor allem für die Leitzentralen sollte es ein ganzheitliches Konzept zur Bewertung des Sicherheitsniveaus und ein Risikomanagement für Organisationsstrukturen, den Faktor Mensch, technologische Maßnahmen, die Vernetzung und den Aspekt der Dynamik geben.

Für industrielle Technologien und industrielle Netzwerke sollte es ein Verfahren geben, das Verhalten der Komponenten zu analysieren, Kompromittierungen zu entdecken und Cyberangriffe einzudämmen. Das beinhaltet Sensoren zur Datengewinnung und intelligente Verfahren der Analyse der Kommunikation von Komponenten.

ITS APT

Für Kritische Infrastrukturen sollte es ein effizientes Testverfahren geben, das Sicherheitsbewusstsein der Mitarbeiter zu erhöhen und das Sicherheitsniveau als Teil des Risikomanagements einer Organisation zu testen.

MOSAIK

Für Kritische Infrastrukturen sollte es ein modellbasiertes Verfahren mit Werkzeugunterstützung geben, ausgehend von der Architektur und Sensordaten das Level der IT-Sicherheit kontinuierlich zu bestimmen.

PortSec

Für Softwaresysteme sollte es ein standardisiertes und zertifizierbares Risikomanagementverfahren auf der Basis von automatisierten Tests geben.

PREVENT

Für einen Geschäftsprozess sollte ein Risikomanagementverfahren definiert sein. In diesem Risikomanagement sind die Erfassung der Daten, die Auswertung der Daten und die zielgruppengerechte Darstellung der Analyseresultate gebündelt.

RISKVIZ

Für industrielle Informationstechnologien sollte es ein Verfahren der Suche geben, mit dem sichtbare Komponenten identifiziert werden, für die anhand von Metriken die Risiken bestimmt und das Ergebnis mit Geoinformationen in einem Risikolagebild visualisiert werden kann.

SecMaaS
SECURITY MANAGEMENT AS A SERVICE

Das Identitätsmanagement unterliegt besonderem Schutzbedarf. Für das Identitätsmanagement sollte es ein User-Centric-Security-Verfahren geben, mit dem ohne vertiefte Kenntnisse der Informationssicherheit geeignete Maßnahmen identifiziert werden können und die Umsetzung in einem IT-Sicherheitsmanagementsystem unterstützt wird.

Für Technologien Kritischer Infrastrukturen sollte es ein Verfahren geben, um aus den technischen Parametern der Komponenten und der Architektur die tatsächliche Sicherheit abzuleiten.

Für einen Sektor sollte es ein Verfahren geben, speziell die kleinen und mittleren Betreiber in die Weiterentwicklung des State of the Art in IT-Sicherheit einzubinden, und es sollte ein Kennzahlensystem (eine Metrik) geben, mit der Betreiber ihr Sicherheitsniveau effizient selbst einschätzen können, und eine Sammlung von in der Praxis bewährten Maßnahmen, um das Schutzniveau effizient anheben zu können.

Für eine Kritische Infrastruktur sollten Systemstörungen erfasst werden und modellbasiert Reaktionsmöglichkeiten vorgeschlagen und priorisiert werden, um im Störungsfall effektiv reagieren zu können und die Servicequalität wiederherstellen zu können.

Für die internen und externen Mitarbeiter mit erhöhten Anforderungen an Kenntnisse in der Informationssicherheit sollten aktivierende Trainings durchgeführt werden, die es erlauben, aktuelle IT-Sicherheitsthemen im Kontext der Organisation zu bewerten. Diese Trainings sollten Spaß machen und die Teilnehmer aktiveren.

Überlegungen des Verbundprojekts SICIA zum Sektor „Energie“

Autoren: SICIA-Projekt

Ein Schwerpunkt im Verbundprojekt SICIA ist die Messung des Umsetzungsgrades von Maßnahmen, die die IT-Sicherheit von technischen Komponenten in kritischen Netzen sicherstellen bzw. erhöhen, wobei die Anwender im Konsortium Unternehmen aus der Energieerzeugung (LEAG Lausitz Energie Kraftwerke AG und RWE AG) und -verteilung (innogy SE) sind. Um die Akzeptanz des im Projekt entwickelten Verfahrens für weitere potentielle Anwender zu erhöhen, war es das Ziel, dieses an mindestens einer anerkannten Vorgabe (Norm oder anderen Richtlinie) auszurichten. Neben dem IT-Grundschutz des BSI gibt es eine Fülle weiterer Richtlinien, -normen und Leitfäden zur IT-Sicherheit [1-6]. Alle ähneln sich inhaltlich stark und variieren hauptsächlich in Struktur, Abstraktionsgrad und dem adressierten Anwendungsbereich. Am Anfang des Projekts war deshalb die Frage zu beantworten, aus welchen der zahlreichen existierenden Regularien messbare Kriterien abgeleitet werden sollten.

Das Verbundprojekt SICIA hat die DIN ISO/IEC 27002 [5], DIN ISO/IEC TR 27019 [6] und das ICS-Security-Kompendium [2] des BSI als Basis für ihre Bewertung gewählt, denn im Vergleich zum IT-Grundschutz des BSI gilt:

- *Die deutschen Normen DIN ISO/IEC 27002, DIN ISO/IEC TR 27019 sind Übersetzungen internationaler Normen, sodass deren Inhalt international anerkannten Vorgaben entspricht. Für Betreiber von Infrastrukturen, die Teile eines internationalen Energienetzes sind, ist für eine durchgehende und konsistente Absicherung dieses Netzes nur die Orientierung an einem gemeinsamen, internationalen Sicherheitsstandard zielführend.*
- *Für Energienetzbetreiber ist in dem an sie gerichteten IT-Sicherheitskatalog [7] die Implementierung von Informationssicherheitsmanagementsystemen (ISMS) gemäß DIN ISO/IEC 27001 [8] bereits de facto vorgeschrieben [9] und DIN ISO/IEC 27002 und DIN ISO/IEC TR 27019 stellen darauf direkt abgestimmte international anerkannte Leitfäden mit allgemeinen bzw. mit für Energieversorgungsunternehmen spezifischen Kriterien dar. Zwar existiert auch ein Schema zur „Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz“ [10], hier liegen jedoch die Nachteile in der nur nationalen Bedeutung des IT-Grundschutz des BSI sowie der im Vergleich zu den beiden internationalen Leitfäden enorme Umfang der nicht einmal Energiesektor-spezifischen IT-Grundschutz-Kriterien.*
- *Für kritische Energieerzeugungsanlagen wird diese defacto-Vorschrift zur Umsetzung von ISMS gemäß ISO/IEC 27001 ebenfalls erwartet, ein Entwurf des Katalogs für Energieerzeuger ist seit Januar 2018 einsehbar. Auch hier sind statt dem IT-Grundschutz neben dem VGB-Standard „IT-Sicherheit für Erzeugungsanlagen“ [3] die Normen DIN ISO/IEC 27002 und ISO/IEC 27019 genannt.*
- *Das ICS-Security-Kompendium des BSI liefert, da an industrielle Steuerungssysteme gerichtet, gezieltere Kriterien für die Netze der Energieversorgung als der an Standard-IT ausgerichtete IT-Grundschutz des BSI. Sie ergänzen die allgemeinen und Energiesektor-spezifischen Kriterien der DIN ISO/IEC 27002 und DIN ISO/IEC TR 27019 zur Schaffung von IT-Sicherheit um weitere Kriterien für industrielle Steuerungssysteme.*

Zusammenfassend ist der IT-Grundschutz des BSI quasi ein weiteres, paralleles Werk an Kriterien (Bausteinen) und Maßnahmen plus Gefährdungen, wobei diese nur nationale Bedeutung haben. Für Energieversorger, die mittlerweile in meist internationale Firmengeflechte eingebunden sind, ist eine Orientierung an rein deutschen Vorgaben zur Gestaltung firmenweiter Prozesse ungeeignet. Keiner der im Projekt SICIA mitwirkenden Betreiber orientiert sich bei der Absicherung seiner kritischen Netze am IT-Grundschutz des BSI. Im Gegenteil, der IT-Grundschutz wird mit seinen tausenden Kriterien als schlicht nicht praktikabel angesehen.

[1] *VDI/VDE 2182: Informationssicherheit in der industriellen Automatisierung, Januar 2011.*

[2] *Bundesamt für Sicherheit in der Informationstechnik: ICS-Security-Kompendium, 2013.*

[3] *VGB PowerTech: IT-Sicherheit für Erzeugungsanlagen (VGB-S-175), 2014.*

[4] *BDEW Bundesverband der Energie und Wasserwirtschaft: Anforderungen an sichere Steuerungs- und Telekommunikationssysteme, Stand 3/2015.*

[5] *DIN ISO/IEC 27002: Informationstechnik – IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management.*

[6] *DIN ISO/IEC TR 27019: Informationstechnik – Sicherheitsverfahren – Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002.*

[7] *IT-Sicherheitskatalog gemäß §11 Absatz 1a Energiewirtschaftsgesetz, Stand 8/2015.*

[8] *DIN ISO/IEC 27001: Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits- Managementsysteme – Anforderungen.*

[9] *Franka Schuster, Andreas Paul, Hartmut König: Messung der technischen IT-Sicherheit in Energieversorgungsanlagen zur Erfüllung des IT-Sicherheitsgesetzes. In: VGB PowerTech Journal 3/2017. VGB Powertech e.V.*

[10] *Bundesamt für Sicherheit in der Informationstechnik: Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz. Zertifizierungsschema, Version 1.2, 2014.*

Die Überlegungen von AQUA-IT-Lab zum Sektor „Wasser“

Autoren: David Fuhr, Christof Thim

Statische Maßnahmenkataloge – Eine der Besonderheiten der IT-Grundschutzmethodik ist es, dass in den Bausteinen für bestimmte Zielobjekte neben den Standardgefährdungen für diese Assets feste Maßnahmen aufgeführt sind. Diese Maßnahmen sind umzusetzen, um eine Basisabsicherung zu erreichen. Es bleibt lediglich zu überprüfen, welche Maßnahmen bereits umgesetzt sind („Basis-Sicherheitscheck“, BSC) und welche ggf. überflüssig sind bzw. an konkrete lokale Gegebenheiten angepasst werden müssen. Der große Vorteil dieses Vorgehens ist, dass bei „normalem“ Schutzbedarf die aufwändige Risikoanalyse eingespart werden kann. Letztere ist lediglich in einem der folgenden drei Fälle durchzuführen:

- *höherer Schutzbedarf (hoch oder sehr hoch),*
- *ungewöhnliche Einsatzszenarien oder*
- *kein passender Baustein in den Grundschutz-Katalogen vorhanden.*

Die Besonderheiten des Wassersektors. Im Wassersektor kommen vier Effekte zusammen, die den Nutzen der eigentlichen Grundschutzvorgehensweise nach BSI-Standard 100-2 infrage stellen:

1. Kritische Infrastruktur – (sehr) hoher Schutzbedarf:
Da es sich beim Wassersektor in allen Staaten um eine Kritische Infrastruktur handelt, liegt zumindest für die Technik zur Steuerung der Prozesse fast immer hoher, häufig sogar sehr hoher Schutzbedarf vor. Die Basisabsicherung des IT-Grundschutzes genügt dadurch grundsätzlich nicht.

2. Wassersektor – andere Einsatzszenarien:
Da der IT-Grundschutz für die öffentliche Verwaltung entwickelt und von da aus nach und nach für klassische private Unternehmen geöffnet wurde, betrachtet er vor allem Einsatzszenarien der Office-IT, von Rechenzentren, Bürogebäuden und Arbeitsplätzen. Die entscheidenden IT-Prozesse der Wasserversorgung und Wasserentsorgung hingegen werden in Warten, Klärwerken, Pumpstationen und anderen Außenstellen betrieben, worauf die Maßnahmenbündel nicht ausgelegt sind.

3. Automatisierungstechnik – keine passenden Bausteine:
Dazu kommt, dass für die wichtigsten Komponenten der Automatisierungstechnik – SPSen, Prozessleitsysteme, Feldbus- und Fernwirktechnik sowie Programmiergeräte – keine Bausteine vorhanden sind. Zwar hat das BSI Ende 2016 einen Baustein IND.1 „ICS-Betrieb“ für komponentenübergreifende, konzeptionelle und architektonische Sicherheitsanforderungen für ICS-Anlagen als Community Draft veröffentlicht und weitere sind in Arbeit (SPS, HMI, Fernwirksystem, Leitwarte); diese stehen jedoch Stand heute noch nicht zur Verfügung, sodass auf weiten Strecken manuelle Analyse notwendig ist.

4. Ressourcenmangel – keine Wirtschaftlichkeitserwägungen:
Die genannten Probleme werden dadurch verschärft, dass kleine (aber auch mittlere) Betreiber von Wasserinfrastrukturen in der Regel weder über ausreichend eigene Kompetenzen noch Ressourcen verfügen, um die Risikoanalyse vorzunehmen.

Bausteine der IT-Sicherheit Kritischer Infrastrukturen

Die Grundschutzkataloge des Bundesamts für Sicherheit in der Informationstechnologie stellen den De-facto-Standard der Informationssicherheit dar und werden als Referenzwerk der IT-Sicherheit genutzt. Kritische Infrastrukturen können notwendige Sicherheitsmaßnahmen mit den Grundschutzkatalogen identifizieren und umsetzen. Die Grundschutzkataloge gliedern sich in Bausteine, Gefährdungskataloge und Maßnahmenkataloge und werden um die IT-Grundschutz-Vorgehensweise ergänzt.

Der Förderschwerpunkt geht mit seinen innovativen Technologien über den Stand der Technik in den IT-Grundschutz-Katalogen hinaus. In den Katalogen sind die Gefährdungen und Schwachstellen – auch von industriellen Steuerungssystemen – aufgeführt. Die Projekte tragen innovative Bausteine der IT-Sicherheit zu diesem Referenzwerk bei – als Forschungsergebnisse werden sie die Sicherheit Kritischer Infrastrukturen verbessern.

Die Innovationen aus dem Förderschwerpunkt verfeinern den Stand der IT-Sicherheit Kritischer Infrastrukturen um:

- innovative Bausteine,
- innovative Methoden und Verfahren.

Diese Überlegungen, Bausteine, Methoden und Verfahren zeigen auch den Forschungsbedarf an neuen Ansätzen für Kritische Infrastrukturen in der Informationssicherheit auf – und dass ITS|KRITIS hier methodisch und inhaltlich Neuland betreten hat.

Innovative Bausteine und Maßnahmen der IT-Sicherheit Kritischer Infrastrukturen

Der erste Abschnitt thematisiert Bausteine und Maßnahmen – zwei Themengebiete, die hier synergetisch betrachtet werden und aufzeigen, dass die Komplexität der Technologie Kritischer Infrastrukturen auf geeignetem Abstraktionsniveau analysiert werden muss.

INDI: Bausteine der Schwachstellensuche und Angriffserkennung für Industrienetze

Autoren: Konrad Rieck, Christian Wressnegger, Hartmut König, Andreas Paul, Franka Schuster, Heiko Kanisch, Christoph Moder

Das Vorhaben INDI entwickelt Technologie zur Schwachstellensuche und Angriffserkennung für Industrienetze. Diese Technologie schafft die Grundlage für neue Sicherheitsprodukte, die verschiedene Maßnahmen des BSI-Grundschutzes umsetzen können, zum Beispiel werden differenziert:

M 5.71	Intrusion-Detection- und Intrusion-Response -Systeme
M 5.150	Durchführung von Penetrationstests
M 2.302	Sicherheitsgateways und Hochverfügbarkeit

RiskViz: Bausteine Cyberversicherungen und cyber-physische Systeme

Autor: Jan-Ole Malchow

Im IT-Grundschutz fehlt der Aspekt der Cyberversicherung bisher vollständig. Dies ist dem Umstand zuzuschreiben, dass Cyberversicherungen in Deutschland bisher quasi nicht existent waren. Mit Veröffentlichung der Musterbedingungen durch den GDV ist hier jedoch eine wichtige Hürde genommen worden.

Baustein cyber-physische Systeme

Beschreibung:
Der Begriff cyber-physisches System bezeichnet informatische, softwaretechnische Komponenten, welche physische Welt und Dateninfrastruktur miteinander verbinden. Ziel ist es jeweils, physische Prozesse zu kontrollieren und regulieren. Dies kann z. B. direkt durch Sensoren und Aktuatoren geschehen, jedoch auch indirekt durch Anzeigen. Ein häufiger Fall sind industrielle Kontrollsysteme zur Steuerung von Produktionsprozessen. Die hier eingesetzten Komponenten enthalten komplexe Steuerungsbefehle zur Steuerung der Produktion und bilden somit das Rückgrat der Automatisierung in der Produktion. Alle im Baustein B 3.407 beschriebenen Anforderungen gelten hier analog.

Gefährdungslage:
In der Beschreibung des Bausteins wird jedoch Gefährdungslagen, welche durch die Vernetzung entstehen, bisher nicht hinreichend Rechnung getragen. Diese spielt jedoch eine wichtige Rolle und die Bedeutung wird im Rahmen der Strategie für Produktion 4.0 stetig zunehmen. Cyber-physische Systeme müssten also zusätzlich zum Beispiel nach dem Baustein „B 3.101 Allgemeiner Server“ zugeordnet werden.

Die praktischen Probleme beim Schutz von cyber-physischen Systemen deuten darauf hin, dass diese Doppelrolle schwer zu erfassen ist. Daher integrieren wir Gefährdungslagen aus Vernetzung hier direkt in den erweiterten Baustein. Die folgende Liste der Gefährdungslagen ist

nicht vollständig, sondern umfasst nur diejenigen, welche durch das Projekt RiskViz mit innerer und äußerer Suche adressiert werden.

Maßnahme Cyberversicherung

Das Projekt RiskViz schlägt eine Maßnahme „Cyberversicherung " für den IT-Grundschutz vor. Die Anbindung an den technischen Teil des RiskViz-Projekts mit innerer und äußerer Suche liegt dabei in den Aspekten Assessment und Überwachung.

Dementsprechend werden keine konkreten Empfehlungen für Versicherungen gegeben, sondern nur diese Anknüpfungspunkte im Rahmen von Maßnahmen gemäß einem IT-Grundschutz-Baustein gezeigt.

RiskViz: Bausteine für eingebettete Systeme sowie innere und äußere Suche

Autor: Jan-Ole Malchow

RiskViz befasst sich mit der Erfassung des Ist-Zustands einer Systemkonfiguration sowie deren Auswertung zum Beispiel in Form von Lagebildern. Die beiden neuen Maßnahmen gelten jeweils sowohl für die äußere als auch für die innere Suche.

B 3.407 Eingebettetes System

Der relevante Kernbaustein des IT-Grundschutz-Katalogs, welcher von RiskViz adressiert wird, ist der Baustein „B 3.407 Eingebettetes System", denn die bei RiskViz im Fokus stehenden cyber-physischen Systeme fallen unter diese Kategorie.

Maßnahme äußere Suche

1. Planung und Konzeption
- Erfassung relevanter IP-Adressen
- Erfassung relevanter Protokolle
- Festlegung des Soll-Zustands
- Festlegung zu versichernder Schäden

2. Umsetzung
- Regelmäßige Scans
- Vergleich Soll-Zustand Ist-Zustand
- Abschluss Cyber-Versicherung

3. Betrieb
- Dokumentation der Scan-Ergebnisse
- Anpassung zu scannender IP-Adressen bei Veränderung
- Anpassung relevanter Protokolle bei Veränderung
- Anpassung Soll-Zustand bei Veränderung des Systems

4. Notfallvorsorge
- Verhaltensregeln bei Differenz zwischenschen Soll-Zustand und Ist-Zustand
- Verhaltensregeln bei Ausfall des Scans
- Meldung des Schadens an die Versicherung

Maßnahme innere Suche

1. Planung und Konzeption
a. Erfassung relevanter Protokolle
b. Festlegung des Soll-Zustands
c. Festlegung zu versichernder Schäden

2. Umsetzung
a. Regelmäßige Scans
b. Vergleich Soll-Zustand Ist-Zustand
c. Abschluss Cyber-Versicherung

3. Betrieb
a. Dokumentation der Scan-Ergebnisse
b. Anpassung relevanter Protokolle bei Veränderung
c. Anpassung Soll-Zustand bei Veränderung des Systems

4. Notfallvorsorge
a. Verhaltensregeln bei Differenz zwischen Soll-Zustand und Ist-Zustand
b. Verhaltensregeln bei Ausfall des Scans
c. Meldung des Schadens an die Versicherung

RiskViz: Liste der Gefährdungen

Autor: Jan-Ole Malchow

Diese Maßnahmen der inneren und äußeren Suche adressieren unmittelbar folgende Gefährdungen des IT-Grundschutz-Katalogs:

Organisatorische Mängel

G 2.4 Unzureichende Kontrolle der Sicherheitsmaßnahmen
G 2.7 Unerlaubte Ausübung von Rechten
G 2.9 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
G 2.27 Fehlende oder unzureichende Dokumentation
G 2.45 Konzeptionelle Schwächen des Netzes
G 2.59 Betreiben von nicht angemeldeten Komponenten
G 2.60 Fehlende oder unzureichende Strategie für das Netz- und Systemmanagement
G 2.206 Unzureichende Sicherheitsanforderungen bei der Entwicklung von eingebetteten Systemen
G 2.207 Ungesicherte Ein- und Ausgabe-Schnittstellen bei eingebetteten Systemen

G 2.208 Unzureichende physische Absicherung der elektronischen Komponenten bei eingebetteten Systemen

Menschliche Fehlhandlungen

G 3.2 Fahrlässige Zerstörung von Gerät oder Daten
G 3.3 Nichtbeachtung von Sicherheitsmaßnahmen
G 3.8 Fehlerhafte Nutzung von IT-Systemen
G 3.9 Fehlerhafte Administration von IT-Systemen
G 3.28 Ungeeignete Konfiguration der aktiven Netzkomponenten
G 3.29 Fehlende oder ungeeignete Segmentierung
G 3.34 Ungeeignete Konfiguration des Managementsystems
G 3.35 Server im laufenden Betrieb ausschalten

Technisches Versagen

G 4.10 Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
G 4.22 Software-Schwachstellen oder -Fehler
G 4.38 Ausfall von Komponenten eines Netz- und Systemmanagementsystems
G 4.43 Undokumentierte Funktionen
G 4.100 Hardwareausfall und Hardwarefehler bei eingebetteten Systemen

Vorsätzliche Handlungen

G 5.2 Manipulation an Informationen oder Software
G 5.8 Manipulation von Leitungen
G 5.9 Unberechtigte IT-Nutzung
G 5.16 Gefährdung bei Wartungs-/Administrierungsarbeiten
G 5.20 Missbrauch von Administratorrechten
G 5.23 Schadprogramme
G 5.66 Unberechtigter Anschluss von IT-Systemen an ein Netz
G 5.67 Unberechtigte Ausführung von Netzmanagement-Funktionen
G 5.86 Manipulation von Managementparametern
G 5.201 Einspielen (Flashen) von manipulierten Software-Updates/-Upgrades bei eingebetteten Systemen
G 5.203 Physikalischer Eingriff in ein eingebettetes System

PREVENT: Bausteine Rechenzentren und Kommunikationsnetzwerk

Autor: Torsten Bollen

Banken-IT ist stark proprietär, aber es gibt vereinheitlichende Merkmale, wie beispielsweise die redundante Auslegung von Bankenrechenzentren, die – wenn auch kein Alleinstellungsmerkmal – durchaus bankenspezifisch sind. Die Ergebnisse des Projekts PREVENT sind auf Rechenzentren mit erhöhten Sicherheitsanforderungen generell anwendbar.

Das Projekt PREVENT schlägt zwei Bausteine vor: Rechenzentren und Kommunikationsstrukturen.

PREVENT-Baustein Rechenzentrum

Eine Architekturskizze eines nach TÜV-Richtlinien umgesetzten RZ kann hier auf einem hohen Abstraktionsniveau wie folgt aussehen.

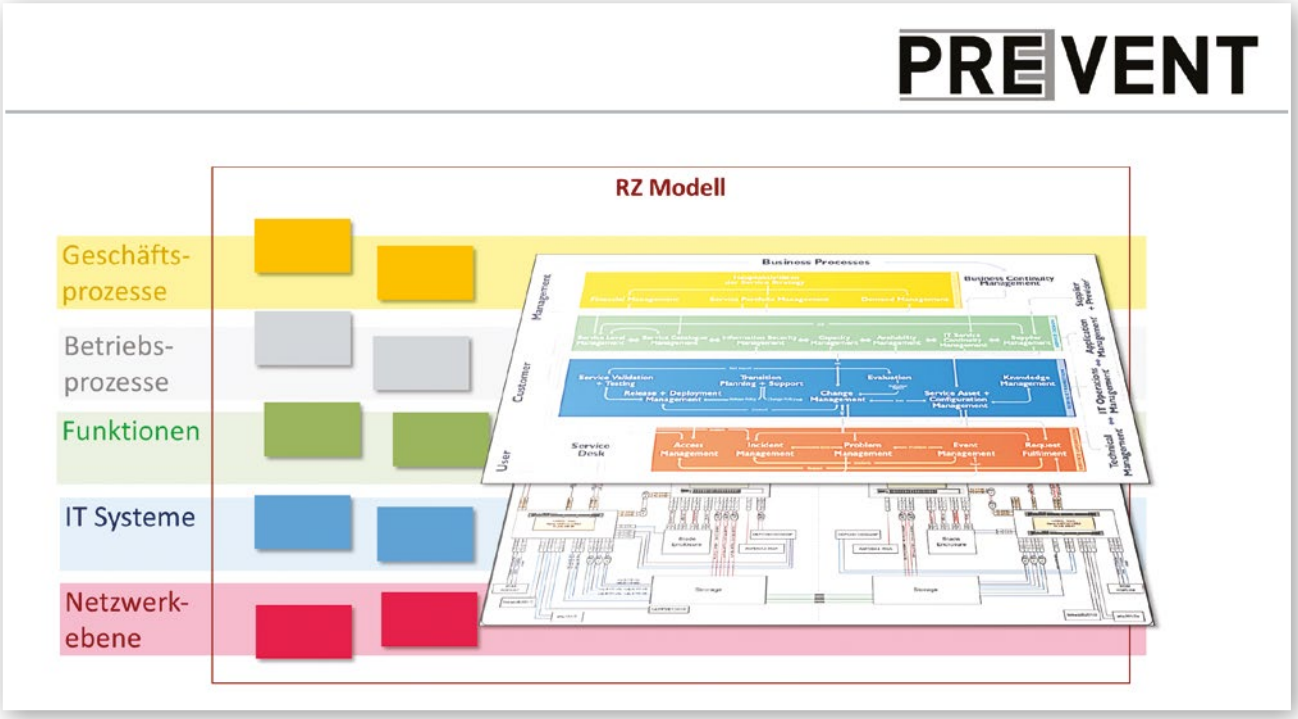


Abb. 1: Komplexität der Kommunikationsebenen in Rechenzentren

PREVENT-Baustein Kommunikationsstruktur

PREVENT entwickelt ein Verfahren zum Risikomanagement und schlägt vor, die gesamte Kommunikationsstruktur als Baustein zu betrachten – für den es das von PREVENT entwickelte Verfahren des Risikomanagements von Geschäftsprozessen gibt.

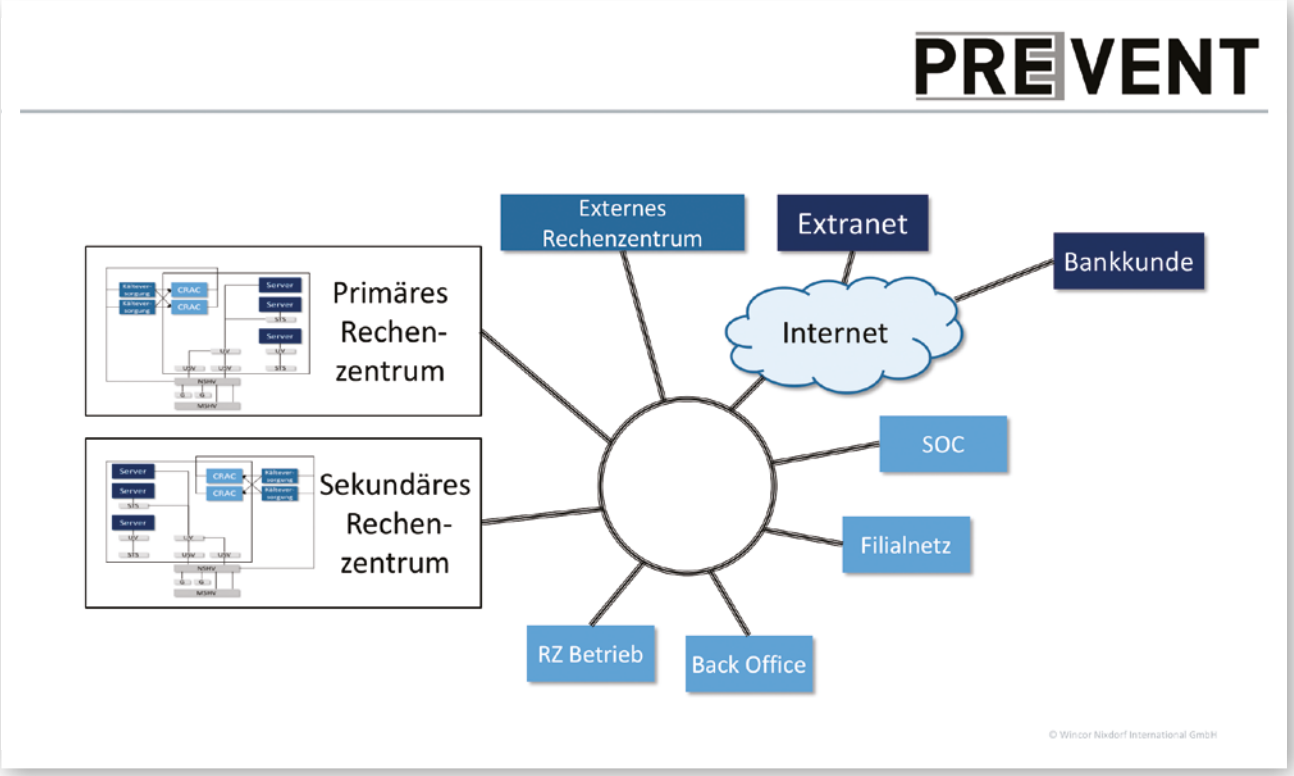


Abb. 2: Kommunikationsstruktur

Innovative Methoden der IT-Sicherheit für Kritische Infrastrukturen

Innovative Methoden, mit der Komplexität des Themas IT-Sicherheit Kritischer Infrastrukturen umzugehen, haben sich als ein Schwerpunkt von ITS|KRITS herauskristallisiert. Zu innovativen Methoden und Verfahren für die IT-Sicherheit von Kritischen Infrastrukturen haben mehrere Projekte Vorschläge entwickelt, die sie für den vorliegenden State of the Art vorschlagen:

- Dynamische Maßnahmenkataloge des Projekts Aqua-IT-Lab
- Rollenspezifische Handlungshilfen des Projekts Cyber-Safe
- Spezifische Gefährdungskataloge des Projekts PortSec
- Ermittlung des Sicherheitslevels – vorrangig anhand konkreter Komponenten- und Netzkonfigurationen des Projektes SICIA
- Ermittlungen des Sicherheitslevels – integrierte Betrachtung von Gefährdungen und Sicherheits maßnahmen des Projekts SIDATE

AQUA-IT-Lab: Dynamische Maßnahmenkataloge

Autoren: David Fuhr, Christof Thim

Das Verbundprojekt Aqua-IT-Lab adressiert das Grundproblem – Ressourcenknappheit gerade bei kleinen und mittleren Betreibern Kritischer Infrastrukturen – und macht daraus eine Chance – Kräfte werden durch den dynamischen Maßnahmenkatalog effizient eingesetzt.

Die Methode ist aufwandsarm – es ist für die Betreiber Kritischer Infrastrukturen keine Aufwandsanalyse notwendig. Aqua-IT-Lab hat es sich zum Ziel gesetzt, dass kleine Betreiber um die Risikoanalyse herumkommen. Dies konnte auf zwei Wegen erfolgen: Erstens musste ähnlich wie im Grundschutz die Bedrohungsanalyse allgemein a priori vorgenommen werden – denn die Voraussetzungen, wie Akteure, zeitliche Entwicklung der Bedrohungslage, grobe Typen von Prozessen, Anlagen und Technik – sind bei kleinen Betreibern ähnlich. Zweitens waren für die typischen Prozesse und Installationen allgemeine Maßnahmen nach Stand der Technik für den passenden Schutzbedarf – hoch bis sehr hoch – zu entwickeln. Beides konnte geleistet werden durch die Analyse diverser einschlägiger Bedrohungs- und Maßnahmenkataloge, Standards und Richtlinien sowie durch die in Aqua-IT-Lab entwickelten Self-Assessments. Kernstück der Methode ist die automatische Erzeugung von Maßnahmen. Um in der Ressourcenschonung noch einen Schritt weiterzugehen, haben wir uns entschlossen, auch den Schritt der Umsetzungsüberprüfung der Maßnahmen (BSC, siehe oben) zu integrieren und halbautomatisch ausführen zu lassen. Zu dem Zweck wurde das Self-Assessment um die automatische Generierung von Handlungsempfehlungen, also High-Level-Maßnahmen, erweitert. Dem zugrunde liegt ein umfangreicher Maßnahmenkatalog, der jedoch nie in Gänze ausgegeben wird, um einen Abschreckungseffekt und Demotivation zu vermeiden, sondern immer gemäß der aktuell geltenden Selbsteinschätzung über 11 Themenfelder die ressourcenoptimal jeweils schutzmaximierenden/risikominimierenden nächsten Maßnahmen berechnet.

Input: Self-Assessment

Der erste Schritt ist ein Self-Assessment. Die folgenden Themenfelder werden im Self-Assessment nach Umsetzungs- („nicht umgesetzt“ bis „trifft voll zu und wurde überprüft“) sowie Dokumentationsgrad („nicht dokumentiert“ bis „vollständig dokumentiert und regelmäßig aktualisiert“) eigenständig bewertet:

Abb. 3: Themenfelder des Self-Assessment

Das Resultat des Self-Assessment ist eine Abschätzung des Reifegrads der existierenden Maßnahmen mit einer Abschätzung des Restaufwands und der Minima des Reifegrads. Diese dienen der Erkennung der größten Risiken (vgl. Abb. 4).

Abb. 4: Auswertung des Reifegrads mit Reifegrad und Minima

Auswertung - Reifegrad

Thema	Praxis - Minimum	Praxis - Reifegrad	Doku - Minimum	Doku - Reifegrad
1 - Organisation	0%	49%	33%	62%
2 - Dokumentation und Zonen	40%	60%	33%	67%
3 - Datenübertragung	20%	33%	33%	44%
4 - Berechtigungsmanagement	40%	55%	33%	58%
5 - Outsourcing & Fernadministr.	40%	56%	33%	60%
6 - Schadsoftware & Schwachstellen	40%	56%	33%	47%
7 - Wechseldatenträger & mobil	20%	50%	33%	50%
8 - Komponentenlebenszyklus	20%	51%	33%	48%
9 - IT-Störungsmanagement	40%	55%	33%	42%
10 - Notfallplanung	20%	50%	33%	67%
11 - Audit	60%	67%	67%	67%
Gesamtergebnis	0%	53%	33%	56%

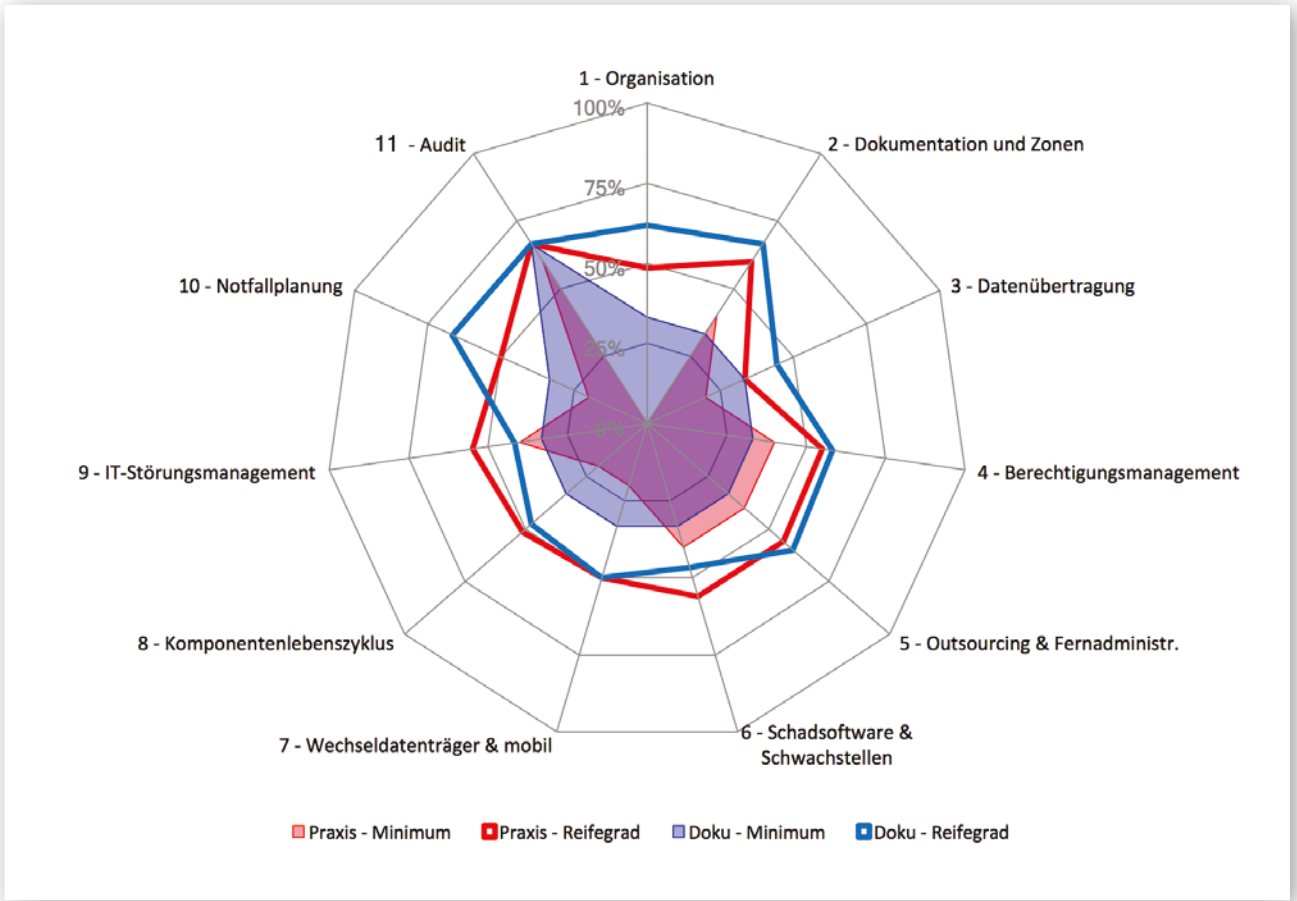
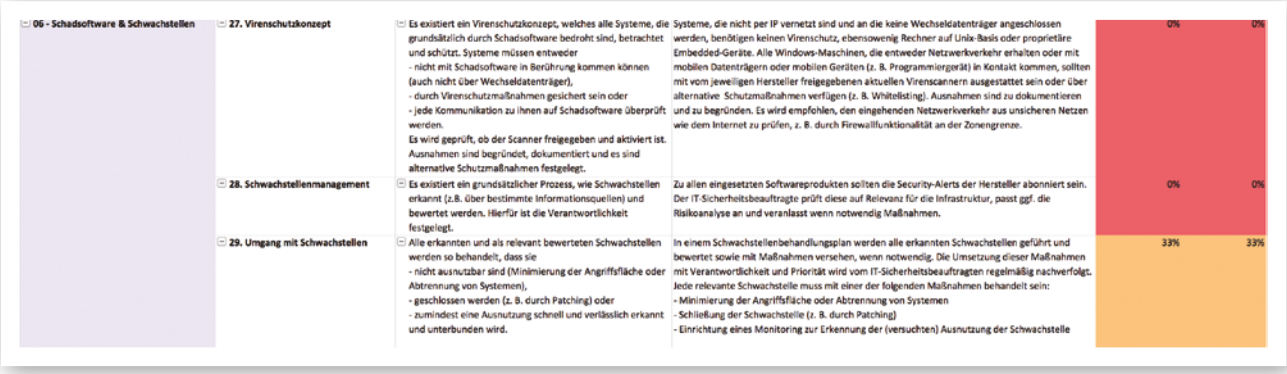


Abb. 5: Darstellung der Ergebnisse des Self-Assessments

Output: generierte Handlungsempfehlungen

Aus den Ergebnissen des Self-Assessment generiert das System automatisch eine Liste von Handlungsempfehlungen, die in ihrer Priorisierung (Reihenfolge) den optimalen Pfad abbilden, um ressourcensparend den Security-Reifegrad der Themen mit den größten Risiken sukzessive anzuheben.



06 - Schadsoftware & Schwachstellen	27. Virenschutzkonzept	Es existiert ein Virenschutzkonzept, welches alle Systeme, die grundsätzlich durch Schadsoftware bedroht sind, betrachtet und schützt. Systeme müssen entweder - nicht mit Schadsoftware in Berührung kommen können (auch nicht über Wechseldatenträger), - durch Virenschutzmaßnahmen gesichert sein oder - jede Kommunikation zu ihnen auf Schadsoftware überprüft werden. Es wird geprüft, ob der Scanner freigegeben und aktiviert ist. Ausnahmen sind begründet, dokumentiert und es sind alternative Schutzmaßnahmen festgelegt.	Systeme, die nicht per IP vernetzt sind und an die keine Wechseldatenträger angeschlossen werden, benötigen keinen Virenschutz, ebensowenig Rechner auf Unix-Basis oder proprietäre Embedded-Geräte. Alle Windows-Maschinen, die entweder Netzwerkverkehr erhalten oder mit mobilen Datenträgern oder mobilen Geräten (z. B. Programmiergerät) in Kontakt kommen, sollten mit vom jeweiligen Hersteller freigegebenen aktuellen Virenscannern ausgestattet sein oder über alternative Schutzmaßnahmen verfügen (z. B. Whitelisting). Ausnahmen sind zu dokumentieren und zu begründen. Es wird empfohlen, den eingehenden Netzwerkverkehr aus unsicheren Netzen wie dem Internet zu prüfen, z. B. durch Firewallfunktionalität an der Zonengrenze.	0%	0%
	28. Schwachstellenmanagement	Es existiert ein grundsätzlicher Prozess, wie Schwachstellen erkannt (z.B. über bestimmte Informationsquellen) und bewertet werden. Hierfür ist die Verantwortlichkeit festgelegt.	Zu allen eingesetzten Softwareprodukten sollten die Security-Alerts der Hersteller abonniert sein. Der IT-Sicherheitsbeauftragte prüft diese auf Relevanz für die Infrastruktur, passt ggf. die Risikoanalyse an und veranlasst wenn notwendig Maßnahmen.	0%	0%
	29. Umgang mit Schwachstellen	Alle erkannten und als relevant bewerteten Schwachstellen werden so behandelt, dass sie - nicht ausnutzbar sind (Minimierung der Angriffsfläche oder Abtrennung von Systemen), - geschlossen werden (z. B. durch Patching) oder - zumindest eine Ausnutzung schnell und verlässlich erkannt und unterbunden wird.	In einem Schwachstellenbehandlungsplan werden alle erkannten Schwachstellen geführt und bewertet sowie mit Maßnahmen versehen, wenn notwendig. Die Umsetzung dieser Maßnahmen mit Verantwortlichkeit und Priorität wird vom IT-Sicherheitsbeauftragten regelmäßig nachverfolgt. Jede relevante Schwachstelle muss mit einer der folgenden Maßnahmen behandelt sein: - Minimierung der Angriffsfläche oder Abtrennung von Systemen - Schließung der Schwachstelle (z. B. durch Patching) - Einrichtung eines Monitoring zur Erkennung der (versuchten) Ausnutzung der Schwachstelle	33%	33%

Abb. 6: Generierte Handlungsempfehlungen (Auszug)

Für den Betreiber Kritischer Infrastrukturen, der diese Methode wählt, bleiben im Wesentlichen folgende Aufgaben:

1. Verifizierung der Priorisierung mit der Leitungsebene
2. Planung der Umsetzung und Ressourcen über die Zeit
3. Konkretisierung der Handlungsempfehlungen für die eigenen Rahmenbedingungen
4. Umsetzung der geplanten Maßnahmen

Insbesondere bei letzterem Punkt kann das Vorgehensmodell nur unterstützen. Bei den Punkten 2 und 3 sollte in der Regel die Hilfe eines Beraters für eine effiziente Umsetzung hinzugezogen werden.

Cyber-Safe: Rollenspezifische Handlungshilfen

Autoren: Selcuk Nisancioglu, Kai Jacobsen, Benjamin Kollenda, Christian Thienert, Christoph Klaproth, Kalliopi Anastassiadou

Im Zuge der Grundlagenanalyse und Workshops mit Betreibern der Leitzentralen konnten wertvolle Erkenntnisse bzgl. des Bedarfs und der Nutzeranforderungen an die zu entwickelnden Handlungshilfen gesammelt werden. Diese Handlungshilfen, die aus drei Software-Tools und einem Leitfaden bestehen, sollen Betreiber von Leitzentralen in die Lage versetzen, Hinweise auf Schwachstellen in ihrem IT-System und ihren Organisationsstrukturen zu erkennen. In diesem Zusammenhang sind bei der Entwicklung zwei wesentliche Randbedingungen zu beachten gewesen. Zum einen dürfen die Empfehlungen keine Widersprüche zu existierenden Regelwerken, v. a. zum BSI-Grundschutz-Katalog und der ISO-27000-Reihe enthalten. Zum anderen handelt es sich bei praktisch allen Verkehrs- und Tunnelleitzentralen um Einrichtungen öffentlicher Verantwortungsträger, die öffentliche Mittel nur sparsam und zielgerichtet verwenden dürfen. Inhaltlich und in der Detailtiefe wurden die Handlungshilfen auf insgesamt drei unterschiedliche Zielgruppen zugeschnitten, die nachfolgend dargestellt werden:

Übergeordnete Managementebene (Checkliste)

Die übergeordnete Managementebene stellt die erforderlichen finanziellen und personellen Ressourcen zur Verfügung. In der Regel handelt es sich dabei um keine IT-Experten. Sie sind sowohl bei der Bewertung der vorhandenen IT-Sicherheit als auch bei der Entscheidung über die Umsetzung von Maßnahmen auf die Unterstützung der IT-Verantwortlichen angewiesen. Für diese Ebene wurde daher die Handlungshilfe „Checkliste“ (Abbildung 7), eine kompakte browser-basierte Software, zur Verfügung gestellt, die die Umsetzung wichtiger übergeordneter Themen überprüft. Dabei handelt es sich um insgesamt 20 Fragen zu bereits ergriffenen Maßnahmen.

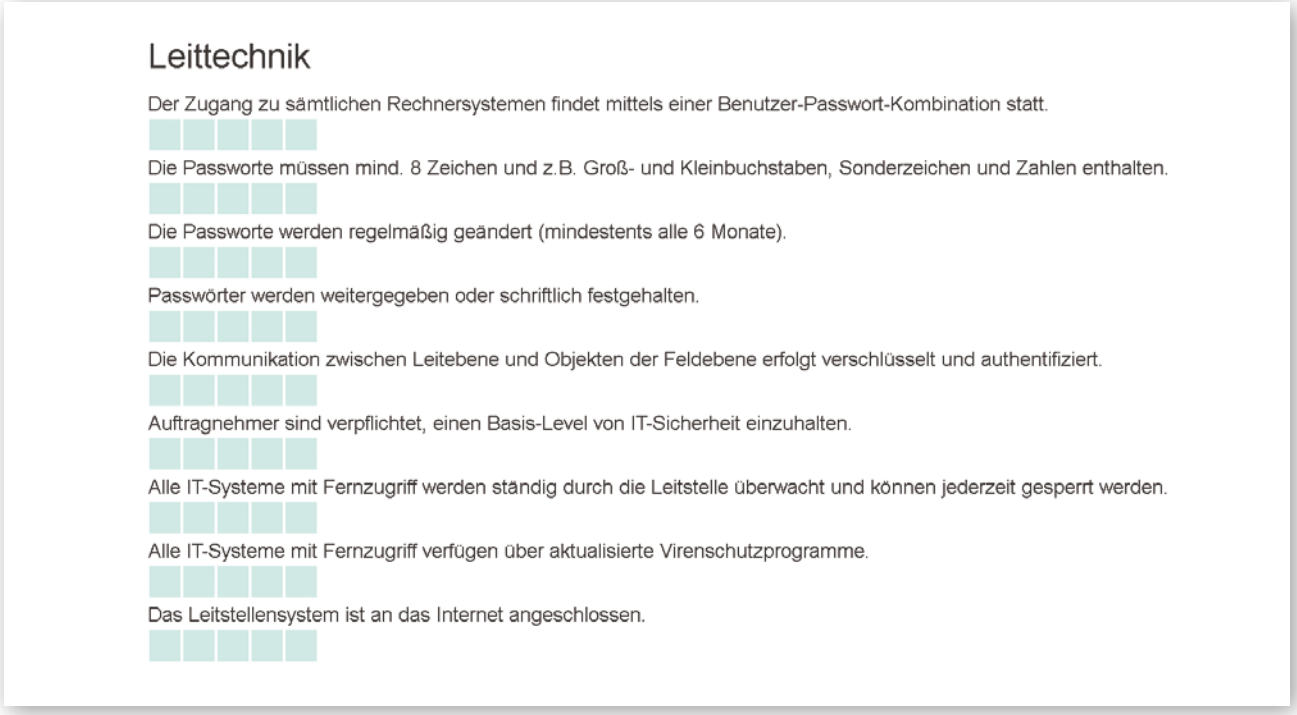


Abb. 7: Bedienoberfläche der Handlungshilfe „Checkliste“ (Ausschnitt)

Mittlere Managementebene (Leitfaden und Bewertungssoftware)

Die mittlere Managementebene ist überwiegend mit konkreten organisatorischen und personellen Aspekten befasst. Fachwissen über die IT der Leitzentrale ist in umfangreichem Maße vorhanden, jedoch oft nicht genug zu sämtlichen Aspekten der IT-Sicherheit. Für diese Zielgruppe werden ein Leitfaden und eine Bewertungssoftware (Abbildung 8) zur Verfügung gestellt; diese überprüfen das Vorhandensein unterschiedlicher Maßnahmen aus den Bereichen Technik, Organisation und Personal für die entsprechend den Richtlinien für die Ausstattung und den Betrieb von Straßentunneln (RABT) [1] gegliederten Ebenen von Leitstellenkomponenten (Leit-, Automatisierungs- und Feldebene). Eine besondere Herausforderung bei der Entwicklung hierbei war, eine übergreifende Bewertung im Rahmen eines Gesamtsicherheitsniveaus zur Verfügung zu stellen.

Quelle

[1] Richtlinien für die Ausstattung und den Betrieb von Straßentunneln (RABT 2016), Forschungsgesellschaft für Straßen- und Verkehrswesen (FGSV), Köln, Entwurf 2016

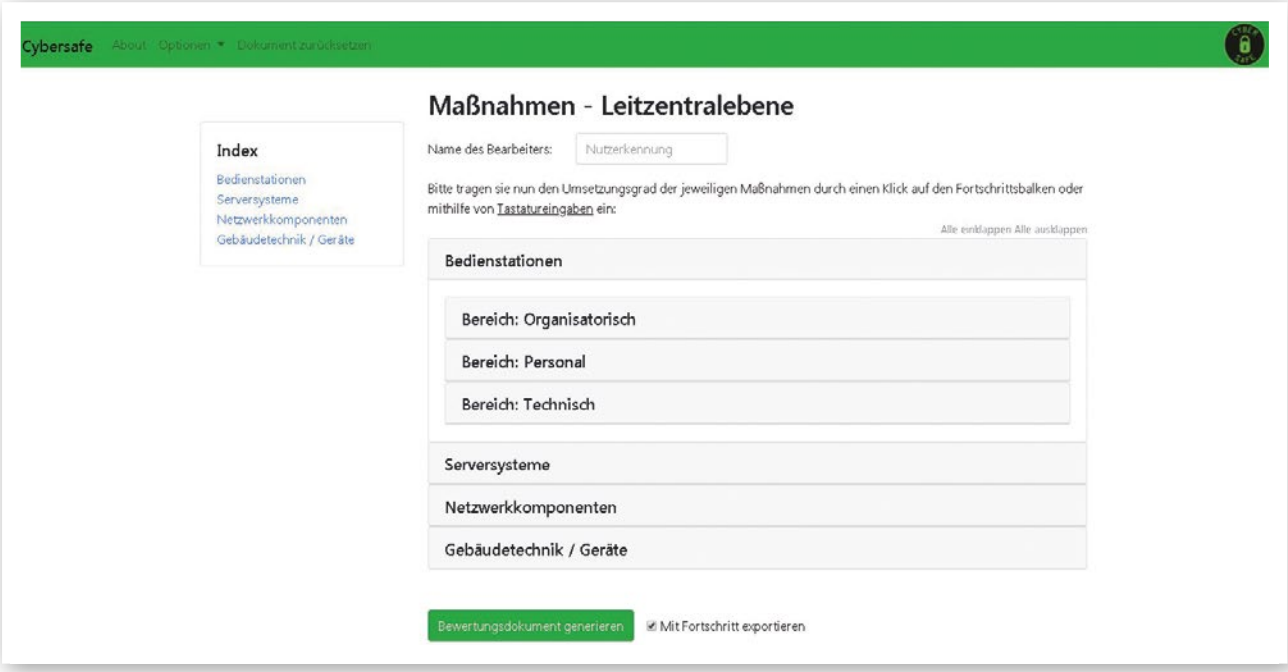


Abb. 8: Bedienoberfläche Bewertungssoftware für die mittlere Managementebene

Diese Handlungshilfe identifiziert nicht automatisch Schwachstellen, kann aber iterativ dazu verwendet werden, das Sicherheitsniveau unter Einbeziehung zusätzlicher umsetzbarer Maßnahmen zu bewerten und damit zweckmäßige Maßnahmen zu identifizieren. Begleitet wird diese Handlungshilfe von einem Leitfaden, der den aktuellen Stand von Maßnahmen zur Verbesserung der IT-Sicherheit in Verkehrs- und Tunnelleitzentralen zusammenfasst und die Nutzung aller Software-Tools nachvollziehbar erläutert.

IT-Verantwortliche (Tiefenanalysesoftware)

IT-Verantwortliche verfügen sowohl über detailliertes Fachwissen bzgl. der IT-Struktur als auch über Kenntnisse der zu berücksichtigenden organisatorischen und personellen Aspekte. Für diese Ebene wird daher eine Analysesoftware entwickelt, auf deren Grundlage eine Tiefenanalyse der vorhandenen IT-Struktur erfolgen kann. Dabei wird ein modellhaftes Abbild geschaffen, welches gefährdete Komponenten und Verbindungen aufzeigt. Insofern ist es eine Ergänzung der oben beschriebenen Handlungshilfe für die mittlere Managementebene und gleichzeitig auch Planungshilfe für Ausstatter und Planer.

Für die umfängliche sicherheitstechnische Untersuchung und Beurteilung eines vernetzten, aus vielen Komponenten bestehenden IT-Systems ist es notwendig, detaillierte Informationen der vorhandenen Hard- und Software sowie ihrer Vernetzungsstruktur zu erfassen. Für die Bewältigung dieser komplexen Aufgabe bietet sich eine Unterstützung durch eine Software geradezu an. Die einzelnen Komponenten, wie etwa Server, PC-Arbeitsplätze und Drucker, aber auch externe Schnittstellen, können durch den Benutzer mittels Drag-and-drop innerhalb eines vordefinierten Arbeitsbereiches auf einer grafischen Bedienoberfläche platziert werden. Mittels zu ziehender Verbindungslinien zwischen den einzelnen Komponenten kann die Struktur der Netzwerkverbindungen abgebildet und erfasst werden. Die einzelnen Komponenten verfügen über variable Attribute, die durch den Anwender gesetzt werden können. Ebenso ist es möglich, bereits umgesetzte Maßnahmen einzelnen Komponenten zuzuweisen. Auf fehlende oder unvollständige Eingaben wird der Anwender durch entsprechende Fehlermeldungen hingewiesen. Die eingegebenen Daten werden zur Vermeidung missbräuchlicher Verwendung mit einem Sitzungspasswort verschlüsselt gespeichert. Nach Abschluss dieses Erfassungsprozesses erfolgt die Analyse des IT-Systems. Hierbei werden potenzielle Bedrohungen ermittelt, bereits umgesetzte Maßnahmen bewertet, das aktuelle Sicherheitsniveau bestimmt und geeignete Sicherheitsmaßnahmen auf Grundlage des im Rahmen des Projektes entwickelten Maßnahmenkataloges empfohlen.

PortSec: Spezifischer Gefährdungskatalog

Autoren: Nils Meyer-Larsen, Rainer Müller, Karsten Sohr, Annabelle Vöge

PortSec verwendet eine eigene Methode, den Stand der IT-Sicherheit zu erkennen und diese zu verbessern. Zentrales Element der Analyse ist die Entwicklung eines Gefährdungskataloges, insbesondere die Ermittlung von Gefährdungen, die spezifisch für ein Hafentelematiksystem sind. Hierbei wird maßgeblich auf eine Analyse der relevanten Geschäftsprozesse zurückgegriffen. Ein zweites zentrales Element ist eine Literaturrecherche nach den bisherigen Vorfällen von IT-Angriffen auf Hafentelematiksysteme, um die Vorgehensweise der Täter zu analysieren. Die Gefährdungsliste wird um Einträge aus der Liste der elementaren Gefährdungen gemäß BSI erweitert.

Der Gefährdungskatalog, den PortSec entwickelt, beinhaltet:

1. Beschreibung der Gefährdung
2. Relevanz für welches Zielobjekt (Wert)
3. Motivation
4. Typisierung des Angreifers

SICIA: Messung des Umsetzungsgrades aller gängigen Funktionen, Verfahren und Maßnahmen zur Erhöhung von IT-Sicherheit

Autoren: Franka Schuster, Hartmut König

Im Verbundprojekt SICIA werden Methoden und Software-Werkzeuge zur systematischen Messung und Bewertung der IT-Sicherheit in kritischen Netzen entwickelt. Die Messung und Bewertung der IT-Sicherheit stützt sich dabei auf Kriterien der Normen DIN ISO/IEC 27002, DIN ISO/IEC TR 27019 und des ICS-Security-Kompendiums des BSI. Da in diesen Regularien alle gängigen Funktionen, Verfahren und Maßnahmen zur Erhöhung von IT-Sicherheit (u. a. Verschlüsselung, Zugriffskontrolle, Existenz interner Sicherheitsrichtlinien, physischer Schutz der IT-Systeme) thematisiert werden, wie sie ebenfalls im IT-Grundschutz des BSI abgehandelt werden, betreffen die rund 350 Messkriterien des Bewertungsprozesses von SICIA gleichzeitig die überwiegende Mehrzahl der Kriterien aus allen Bausteinen des IT-Grundschutzes des BSI.

SIDATE: Gefährdungen und Sicherheitsmaßnahmen

Autoren: Daniel Hamburg, Thorsten Niephaus, Wolfgang Noll, Sebastian Pape, Christopher Schmitz, Kai Rannenberg

SIDATE entwickelt ein Framework zur ganzheitlichen Bewertung der Informationssicherheit von Energieversorgern. Im Sinne eines gesamtheitlichen Ansatzes werden alle fünf Bausteine des BSI-Grundschutz-Katalogs gleichermaßen adressiert. Die Methode von SIDATE zielt darauf ab, die Angriffe strukturiert zu erfassen, um dann bzgl. der Angriffe gezielte Sicherheitsmaßnahmen zu definieren, die das IT-Sicherheitsniveau erhöhen.

Gefährdungen

Für die Bewertung des Sicherheitsniveaus werden bereits existierende Gefährdungskataloge für Energieversorger zugrunde gelegt, insb. die Ergebnisse einer Studie der National Electric Sector Cybersecurity Organization Resource (NESCOR) [1], welche vom US-Energieministerium gefördert wird. Darin werden Gefährdungen für die Informationssicherheit von Energieversorgern identifiziert und hinsichtlich ihres Risikos bewertet. Ergänzend dazu werden viele der Gefährdungen in einer weiteren NESCOR-Publikation [2] als Angriffsbäume dargestellt. Solche strukturierten Darstellungen von Angriffen können z. B. der (teil-)automatisierten Bewertung von Gefährdungen dienen. Im SIDATE-Projekt werden diese existierenden Kataloge auf Basis von Security Audits um zusätzliche Angriffsbäume angereichert.

Sicherheitsmaßnahmen

Weiterhin werden in den NESCOR-Publikationen [1][2] die identifizierten Gefährdungen den möglichen Sicherheitsmaßnahmen zugeordnet. Das gilt ebenfalls für die im SIDATE-Projekt ergänzten Gefährdungen. Solche Zuordnungen vereinfachen Analysen, inwieweit implementierte Sicherheitsmaßnahmen reale Gefährdungen tatsächlich abdecken.

Quellen

[1] National Electric Sector Cybersecurity Organzation Resource (NESCOR), “Electric sector failure scenarios and impact analyses”, Tech. Rep., 2013.

[2] National Electric Sector Cybersecurity Organization Resource (NESCOR), “Analysis of selected electric sector high risk failure scenarios”, Tech. Rep., 2013.

Sektion 3
Die KRITIS-Sektoren und ihre Spezifika

In dieser Sektion werden die Besonderheiten der KRITIS-Sektoren beschrieben.

Die Kritischen Infrastrukturen in Deutschland werden in die Sektoren Energie, Gesundheit, Staat und Verwaltung, Ernährung, Transport und Verkehr, Finanz- und Versicherungswesen, Informationstechnik und Kommunikation, Medien und Kultur sowie Wasser eingeteilt.

Der Förderschwerpunkt „IT-Sicherheit für Kritische Infrastrukturen“ ITS|KRITIS beinhaltete Forschungsprojekte aus verschiedenen Sektoren der Kritischen Infrastrukturen. In dieser Sektion 3 werden die Besonderheiten der jeweiligen KRITIS-Sektoren, in denen das Forschungsprojekt angesiedelt ist, beschrieben. Dabei wird beispielsweise auf die Infrastruktur, Regelwerke, Gesetzliche Grundlagen, Vorschriften sowie Normen und Standard der jeweiligen KRITIS-Sektoren eingegangen.

Review:

Sven Müller, Thomas Diefenbach

Sektion 3
Inhaltsverzeichnis

Aqua-IT-Lab	Trinkwasser – Besonderheiten einer traditionell hochgeschützten Infrastruktur	54
Cyber-Safe	Tunnel- und Verkehrsleitzentralen	56
INDI	Prozessnahe Kommunikation als besondere Herausforderung	57
ITS.APT	IT-Security-Risiken im Sektor Gesundheitsversorgung	58
MoSaIK	Angesprochene Sektoren und Branchen	61
PortSec	Hafentelematik – Zentraler Hub für die Hafenwirtschaft	63
PREVENT	Compliance und Risikomanagement – Anforderungen an Finanzinstitute in der EU	64
RiskViz	Risikolagebild der industriellen IT-Sicherheit am Beispiel des Energiesektors	65
SICIA	Informationstechnik in der Energieversorgung – Besonderheiten und Regularien	67
SIDATE	Stand der IT-Sicherheit bei deutschen Stadtwerken	69
VeSiKi	IT-Sicherheitsrecht	75
VeSiKi	Datenschutz und Compliance	77

Trinkwasser – Besonderheiten einer traditionell hochgeschützten Infrastruktur

Edgar Korte

Forschungsprojekt:
Aqua-IT-Lab

Trinkwasser – die Basis-Infrastruktur

Sauberes Trinkwasser ist traditionell eine entscheidende Voraussetzung für menschliche Zivilisation. Mit dem Beginn der Industrialisierung wurde der Schutz einer qualitativ und quantitativ hochwertigen Wasserversorgung auf eine technologisch hochwertige Grundlage gestellt.

Der Schutz des Trinkwassers wird zum einen über die Trinkwasserverordnung geregelt, die in wesentlichen Teilen EU-Recht folgt. Sie soll die Verbraucher vor Gefahren schützen, die sich aus der Verunreinigung von Trinkwasser ergeben. In der Verordnung werden an einer Vielzahl von Stellen Prozesse beschrieben, die der Datenübermittlung, Kommunikation und der Steuerung technischer Prozesse dienen und damit alle IT-relevant sind. Es ist Aufgabe der IT-Verantwortlichen diese Prozesse bei ihrer Schutzkonzeptplanung besonders zu berücksichtigen.

Als deutsche Besonderheit ist der DVGW e. V. anzusehen, der mit seinem Regelwerk den Stand der Technik definiert. Insbesondere mit der DVGW – DIN EN 15975-2 - vormals W1001 - wurde die Rolle des Trinkwassers als KRITIS schon früh realisiert. Ausgangspunkt der W1001 ist eine Gefährdungsanalyse, in der die Gefährdung der verschiedenen Prozesse des Versorgers entlang der Gewinnungs-, Aufbereitungs-, Förderungs-, Speicherungs-, Transport- und Verteilungskette des Versorgers untersucht wird. Dabei werden die Auswirkungen unterschiedlicher Gefährdungen (z. B. unterteilt in Naturkatastrophen, menschliches oder technisches Versagen und schwere Kriminalität und Terrorismus) auf die einzelnen Prozesse untersucht und bewertet. Die Analyse kulminiert in einer Risikoabschätzung, in der Eintrittswahrscheinlichkeit und Schadensausmaß der verschiedenen Gefährdungen z.B. in einer 3X3 Matrix erfasst werden. Das im Projekt entwickelte Self-Assessment-Tool lässt sich mit dieser Risikomatrix verknüpfen. Nur so kann ein einheitliches Schutzkonzept erarbeitet werden, in dem auch eine optimale Zuteilung der für Sicherheit vorhandenen Ressourcen möglich ist. Die IT-Risikoanalyse ist demnach eine Teilbetrachtung der gesamten Risikosituation des Unternehmens.

In vergleichbarer Weise ist eine einheitliche IT-Maßnahmenplanung in das Krisenfall-Management des Versorgers zu integrieren. In der hier relevanten DIN EN 15975-1 (ursprünglich W1002) des DVGW kommt beispielsweise der Einberufung, Zusammensetzung und Arbeitsweise eines Krisenstabes besondere Bedeutung zu. Diese Komponente spielt in den üblichen IT-Schutzkonzepten keine vergleichbare Rolle. Das im Forschungsprojekt entwickelte Tool berücksichtigt in dem Bereich „Notfallplanung“ diese Anforderung.

Der Schutz der relevanten Gebäude ist ein Teil der Maßnahmenplanung, der sich traditionell auch in den Zonenkonzepten von IT-Sicherheitsanalysen wiederfindet. Das Self-Assessment-Tool enthält ebenfalls eine solche Anforderung. Im Regelwerk des DVGW wird dieser Schutz in der W1050 („Objektschutz von Wasserversorgungsanlagen“) geregelt. Dort wird Bezug genommen auf die Einteilung von Objekten in Widerstandsklassen nach DIN EN 1627. Leitstellen sind demnach nach den Anforderungen der höchsten Widerstandklasse 4 zu schützen. Es ist Aufgabe des Versorgers, die Anforderungen des IT-Zonenkonzeptes mit denen des Objektschutzes nach W1050 in Übereinstimmung zu bringen.

> Ergänzung der Trinkwasser Sicherheitsarchitektur um eine als lex specialis fungierende IT-Sicherheitskomponente

Das Tool berücksichtigt auch die W1000, die grundsätzlich die „Anforderungen an die Qualifikation und die Organisation von Trinkwasserversorgern“ beschreibt. Dort wird zum Beispiel gefordert, dass in einer Aufbauorganisation Zuständigkeiten, Verantwortlichkeiten und Befugnisse „in transparenter und überschneidungsfreier Form schriftlich“ festzulegen sind. Das beinhaltet natürlich auch die mit allen Unternehmensbereichen eng vernetzte IT-Organisation.

Die Ablauforganisation sollte so geregelt sein, dass „Schnittstellen, die durch innerbetrieblich abgegrenzte Aufgabenfelder, bei Kooperationen mehrerer Trinkwasserversorger oder durch Einschaltung von Dienstleistern entstehen“, widerspruchsfrei zu regeln sind. Auch hier bestehen für die IT besonders vielfältige Anforderungen.

Trinkwasserversorger benötigen weiterhin eine „Technische Führungskraft“, die „über die erforderlichen Befugnisse verfügt, um in sicherheitsrelevanten und insbesondere hygienischen Angelegenheiten verantwortlich handeln zu können“. Damit liegen auch die Entscheidungen über die IT-Sicherheit in ihren Händen, was bei Qualifikations- und Schulungsmaßnahmen zu berücksichtigen ist.

IT-Sicherheit als neues Element in der Sicherheitsarchitektur

Mit dem IT-Sicherheitsgesetz ist ein neuer Schutzbedarf vom Gesetzgeber formuliert worden, den es in die Sicherheitsarchitektur der Wasserwirtschaft zu integrieren gilt. Dies geschieht durch die Einführung eines Branchenstandards, dessen wesentlichen Elemente die neue W1060 („IT-Sicherheit – Branchenstandard Wasser/Abwasser“) und ein IT-Sicherheitsleitfaden sind. Als lex specialis hat sie Vorrang vor den genannten bestehenden technischen Regelungen. Insbesondere die in der DIN EN 15975-1 festgelegten Regeln zum Krisenmanagement bleiben jedoch weiter gültig.

Tunnel- und Verkehrsleitzentralen

Kai Jacobsen, Selcuk Nisancioglu

Forschungsprojekt:
Cyber-Safe

Die Überwachungs- sowie Steuerungsmöglichkeiten mehrerer Straßentunnel, Streckenbeeinflussungsanlagen bzw. Lichtsignalanlagen werden in Tunnel- bzw. Verkehrsleitzentralen gebündelt. Im Vordergrund steht dabei zunächst die Regelung der Abläufe im Normalbetrieb. Im Falle eines besonderen Ereignisses, bspw. einer Betriebsstörung oder eines Notfalls, übernehmen Leitzentralen die Leitfunktion für die Einsatz- und Rettungsdienste und gewährleisten somit den Schutz und die Rettung der betroffenen Verkehrsteilnehmer sowie der Verkehrsinfrastruktur. Mit Inkrafttreten der ersten Verordnung zur Änderung der BSI-Kritisverordnung [1] wurden die Schwellenwerte für den Sektor Transport und Verkehr festgelegt. Grundsätzlich sind Anlagen wie Verkehrssteuerungs- und Leitsystem für das Netz der Bundesautobahnen als kritisch bewertet worden und müssen daher entsprechend geschützt werden. Die große Herausforderung für die Erhöhung der IT-Sicherheit von Verkehrs- und Tunnelleitzentralen vor Cyberangriffen liegt insbesondere in der Komplexität der gewachsenen Systeme und dem mittlerweile hohen Technisierungsgrad.

Aufgrund des stetig steigenden Verkehrsaufkommens und der damit ebenso steigenden Anzahl von zu überwachenden Tunneln und Verkehrswegen, steigen auch der Einsatz und die Komplexität von Überwachungs-, Informations- und Kommunikationstechnologien, was wiederum zu einer Steigerung potenzieller Angriffspunkte für Cyberangriffe führt. Insbesondere die Auswirkungen von Angriffen auf Tunnelleitzentralen können aufgrund der besonderen baulichen Situation der Tunnel gravierend sein. Tunnelbauwerke bilden eine Art Nadelöhr im Straßennetz und erfordern daher eine möglichst hohe Verfügbarkeit.

Auch ein Ausfall bzw. eine Fehlfunktion der IT-Systeme von Verkehrsleitzentralen kann erhebliche Auswirkungen auf Verkehrsablauf und Sicherheit haben. Kommt es beispielsweise zu einem Ausfall des zentralen übergeordneten Steuerrechners von Lichtsignalanlagen, kann dies bis zu einem Totalausfall aller angeschlossenen Lichtsignalanlagen führen, was zu gestörten Verkehrsabläufen, Staus und einer Häufung von Unfällen führen kann. Die Vermeidung des Ausfalls von Verkehrs- und Tunnelleitzentralen und der Schutz vor Fremdeinwirkung sind daher von hoher Relevanz.

Quelle

[1] Erste Verordnung zur Änderung der BSI-Kritisverordnung in der Fassung von der Bekanntmachung vom 29. Juni 2017 (BGBl. S. 1921).

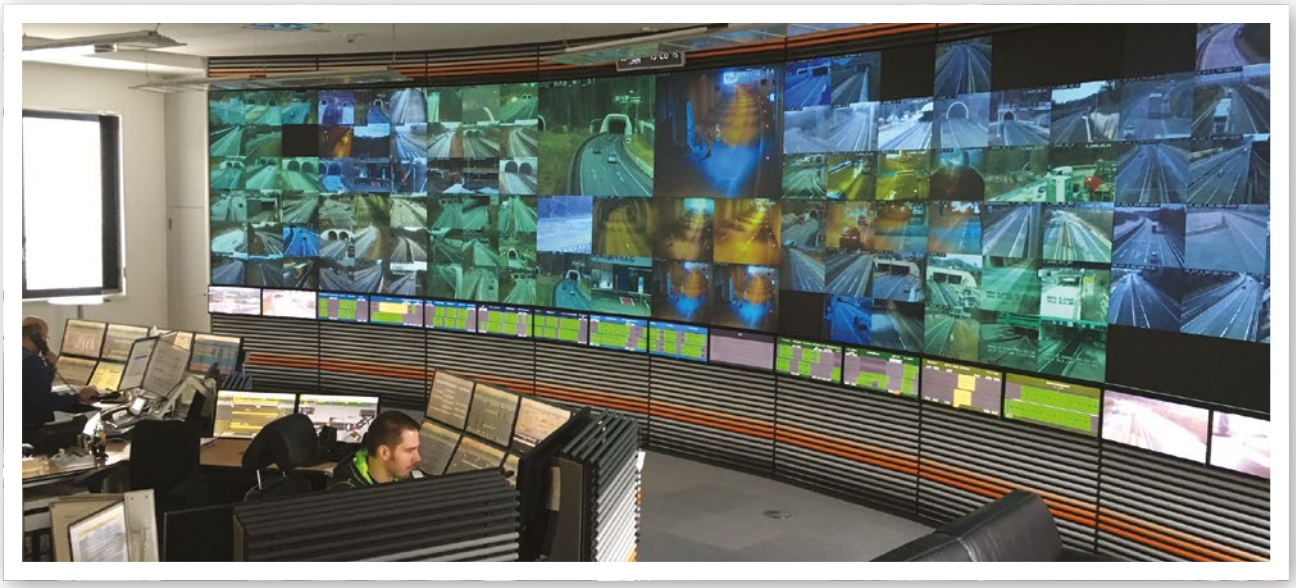


Abb. 1: Tunnelleitzentrale (Foto: DÜRR Group GmbH)

Prozessnahe Kommunikation als besondere Herausforderung

Konrad Rieck, Christian Wressnegger, Hartmut König, Andreas Paul,
Franka Schuster, Heiko Kanisch, Christoph Moder

Forschungsprojekt:
INDI

Grundsätzlich können Kritische Infrastrukturen in zwei Gruppen von Bereichen differenziert werden:

- Bereiche, die keine industriellen Prozesse involvieren, wie die Telekommunikation und das Finanzwesen, und
- Bereiche, die zur Erfüllung ihrer Funktion auf die Nutzung physischer Systeme angewiesen sind, wie die Energie- und Wasserversorgung.

Während der Schutz der erstgenannten Bereiche oftmals durch bewährte Methoden der IT-Sicherheit erhöht werden kann, müssen sicherheitstechnische Lösungen für Industrienetze den fließenden Übergang zu physischen Systemen gewährleisten. Industrienetze sind Kommunikationsnetze, die prozessnahe IT-Systeme mit Sensoren und Aktuatoren zur physischen Welt steuern. Die Schwierigkeit liegt hierbei nicht nur in der Berücksichtigung der anders gelagerten Technologien physischer Systeme, sondern vor allem auch in der zu einer Vielzahl von technischen Vorschriften konformen Integration neuer Sicherheitsmechanismen.

Abbildung 1 stellt beispielhaft die im Kontext der Supervisory Control and Data Acquisition (SCADA) häufig anzutreffende Automatisierungspyramide für Industrienetze dar. Während auf der Betriebsebene vorrangig klassische IT-Systeme verwendet werden, kommt beim Übergang von der Steuerungsebene zur Feldebene zunehmend proprietäre IT zum Einsatz, was sich aus Netzsicht in einer wachsenden Anzahl von seltenen und unbekannten Protokollen äußert."

In Kraftwerken zur Energieerzeugung sind hohe Anforderungen zur Echtzeitverarbeitung und zu garantierten Antwort- beziehungsweise Aktualisierungszeiten gestellt sowie spezielle Rahmenbedingungen gegeben. Dazu zählen: industrielle Kommunikationsprotokolle mit geringen Latenzzeiten, lange Revisions- und Wartungsintervalle der Steuerungsnetze, Funktionen zum Schutz von Leib und Leben von Personen sowie die Systemverfügbarkeit als höchstes Schutzziel für Bedienung, Beobachtung, Steuerung und Regelung der technologischen Prozesse. Durch die Beteiligung von Betreibern und die enge Kooperation mit Herstellern solcher Anlagen entwickelt das Vorhaben INDI eine Sicherheitslösung, die erstmalig alle genannten Rahmenbedingungen in Konzeption und Implementierung berücksichtigen kann. Es ergibt sich somit erstmals die Möglichkeit, Industrienetze sowohl innerhalb der Kraftwerke als auch in der Energieverteilung vor Angriffen zu schützen. Mit Blick auf den wachsenden Bedarf an Smart-Grid-Technologie kann so ein entscheidender Schritt zum Schutz der zukünftigen Energieversorgung erzielt werden.

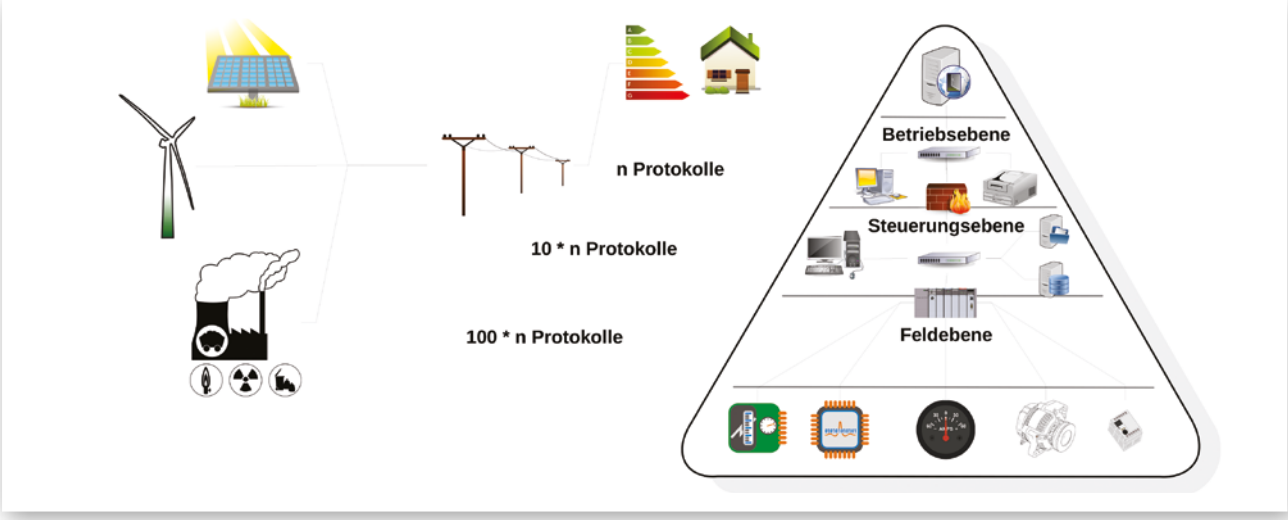


Abb. 1: Automatisierungspyramide: Netze und Protokolle in Industrienetzen

IT-Security-Risiken im Sektor Gesundheitsversorgung

Armin Will

Forschungsprojekt:
ITS.APT

IT in der klinischen Gesundheitsversorgung

Unternehmen der Gesundheitsbranche sind zur Erfüllung ihrer Kernaufgaben auf eine umfangreiche IT-Organisation und –Infrastruktur angewiesen. Industrie 4.0, eigentlich die industriellen Produktion fokussierend, durchdringt auch die Gesundheitsbranche und verändert vorhandene Prozesse und generiert neue Arbeitsabläufe. Neben Patientendaten, Untersuchungs- und Therapiedaten werden Behandlungspfade und Workflows digital abgebildet. In ausgewählten klinischen und administrativen Bereichen ist Prozesssteuerung bereits seit längerem Standard (Laborstraßen, OP-Besteck Sterilisation, Essensversorgung u. a.). Kommissionierungsautomaten bereiten die Medikation jedes einzelnen Patienten tagesaktuell und vollautomatisch auf. Die Einsatzplanung von Personal, das Management der Materialflüsse, die Belegung der Operations- und Untersuchungseinheiten erfolgen mittels digitaler Tools. Diese elektronischen Werkzeuge sind zunehmend untereinander vernetzt. Über mobile Endgeräte erfasste Vitalparameter werden über Schnittstellen in der zentralen, elektronischen Krankenakte dokumentiert. Die mobil erfassten Materialverbräuche finden Eingang in die Krankenakte und lösen parallel

> Sensibilisierung des Krankenhauspersonals bezgl. der Cyber-Bedrohungslage mit Hilfe von interaktiven E-Learning-Angeboten

in der Materialverwaltung die Verbuchung und bei Bedarf automatisiert die Nachbestellung bei Hersteller bzw. Lieferant aus. Mit der Online-Buchung einer Untersuchung oder Operation werden relevante Patienteninformationen, wie z. B. Allergien, Risikofaktoren, wesentliche Medikationen etc., übermittelt. Untersucher und Behandler stehen die Informationen der elektronischen Krankenakte unmittelbar am Behandlungssystem zur Verfügung. Diese transparente Bereitstellung der notwendigen klinischen Daten direkt am Ort des Geschehens sichert einen konsistenten Informationsstand für alle Beteiligten. Der optimierte Behandlungsworkflow kommt in erster Linie der Verbesserung der Behandlung des Einzelnen, aber auch den beteiligten Mitarbeitern zugute. Unnötige Aktensuche, fehlende Informationen reduzieren den administrativen Aufwand und helfen den Mitarbeitern, sich auf den Patienten zu konzentrieren.

Neben krankenhausinterner Vernetzung kommt in steigendem Maße der elektronische Datenaustausch mit Kostenträgern, Lieferanten, Herstellern, anderen Partnern der Gesundheitsversorgung (Ärzte, Krankenhäuser, Pflegeeinrichtungen etc.) und nicht zuletzt auch mit dem Patienten selber hinzu. Zur bereits obligatorischen Onlinepräsenz für die Außendarstellung des Krankenhauses gesellen sich Portale für Patienten, Ärzte und andere Partner. Über diese erfolgt einerseits Datenaustausch (Arztbriefe, Befunde etc.) zwischen den an einer Behandlung beteiligten Partnern, andererseits werden Behandlungspfade (ambulant – stationär – Rehabilitation) enger miteinander verzahnt, somit der Behandlungsprozess für den Patienten optimiert. Der Kontakt mit Lieferanten und Herstellern erfolgt zusehends über Internet (Mail, Online-Bestellungen etc.). Service- und Wartung erfolgen per Fernzugriff auf die betreffenden Systeme und Geräte direkt in der Krankenhaus-IT-Landschaft.

Die eingesetzten IT-Systeme sind sowohl innerhalb als auch außerhalb des Krankenhauses vielfältig vernetzt. Interne und externe Kommunikation und Datenverarbeitung sind dabei vielfältigen Regelungen, Normen und Standards unterworfen bzw. fußen darauf. Eine grobe Übersicht liefert die Abbildung 1.

Risiken des IT-Betriebs

Der Ausfall oder die Störung wesentlicher Komponenten der skizzierten Infrastruktur können erhebliche Auswirkungen – für Patienten evtl. sogar letale Komplikationen – zur Folge haben. Es ist somit unerlässlich, ja zwingend, die IT-Infrastruktur eines Krankenhauses vor Störungen und Ausfall so gut wie möglich zu schützen. Zu den altbekannten Risiken durch Stromausfall, Hardwaredefekte etc. gesellen sich in immer größerem Maße Cyberrisiken, die durch die IT-Systeme selbst (mangelndes Patch- und Release-Management), die Vernetzung (Fernwartung übers Internet, Viren- und Phishing-Mails etc.) und den Datenaustausch (z. B. Datenträger mit Patientendaten) entstehen.

Maßnahmen

Zwar lassen sich die genannten „Schnittstellen“ in die Krankenhaus-IT mittels technischer Maßnahmen gegen Cyberrisiken absichern, aber diese Absicherung ist nur so gut, wie die handelnden Personen sich der Gefahren bewusst sind und verantwortlich agieren. Das vermeintlich schwächste Glied in der Abwehrkette ist der Anwender. Mails von Patienten, Krankenkassen, Lieferanten und Herstellern können potenziell mit Malware oder „gefährlichen“ Links versehen oder gefakt sein. Der Anwender muss entsprechend sensibilisiert sein und angemessen reagieren. Auch wenn „dringend“ die mitgebrachten Befunde vom USB-Stick eingelesen werden müssen, darf der – hoffentlich etablierte – sichere Übertragungsweg über einen „Schleusenrechner“ nicht umgangen werden. Auch wenn die Einladung zu dem hochinteressanten und begehrten Kongress verlockend ist, sollte der angesprochene Anwender zunächst den „unauffälligen“ Link in der Mail nicht einfach anklicken, sondern sich von der „Echtheit“ überzeugen. Selbstverständlich erfolgen heute Bewerbungen auch per E-Mail, dennoch sollte der Sachbearbeiter die angehängten Dateien erst dann auf seinem PC öffnen, wenn bereits eine Viren- und Malwareprüfung der Anhänge erfolgt ist und zudem auf dem PC keine unberechtigten Makros oder ausführbaren Dateien erlaubt sind. Auch der notwendige Remotezugriff zu Wartungs- und Pflegearbeiten auf Systeme darf nur unter gesicherten Verfahren erfolgen. Grundsätzlich sollten sich die betroffenen Systeme nicht aktuell im klinischen Intranet befinden und idealerweise werden die Aktivitäten des Remotezugangs beobachtet. Nach Abschluss der Arbeiten müssen die gesicherten Verbindungen getrennt und die temporär geöffneten Ports wieder verschlossen werden.

Ein Krankenhaus sollte fehlender Awareness seiner Mitarbeiter durch gezielte Informations- und Schulungsmaßnahmen entgegentreten. Neben gezielten Informationen zu aktuellen Bedrohungslagen (siehe Ransomware-Wellen Locky und WannaCry) gehören hierzu auch wiederholte Hinweise zum richtigen Umgang mit Mails, dem Internet, mitgebrachten Datenträgern etc. Awareness-Schulungen sollten fester Bestandteil des innerbetrieblichen Schulungsprogramms oder mindestens Teil der Initialschulung für neue Mitarbeiter sein. Idealerweise stehen den Mitarbeitern im Intranet neben Informationen zur Bedrohungslage und Hinweisen zur Reduzierung von Cyberrisiken interaktive Online-Schulungsmöglichkeiten zur Verfügung.

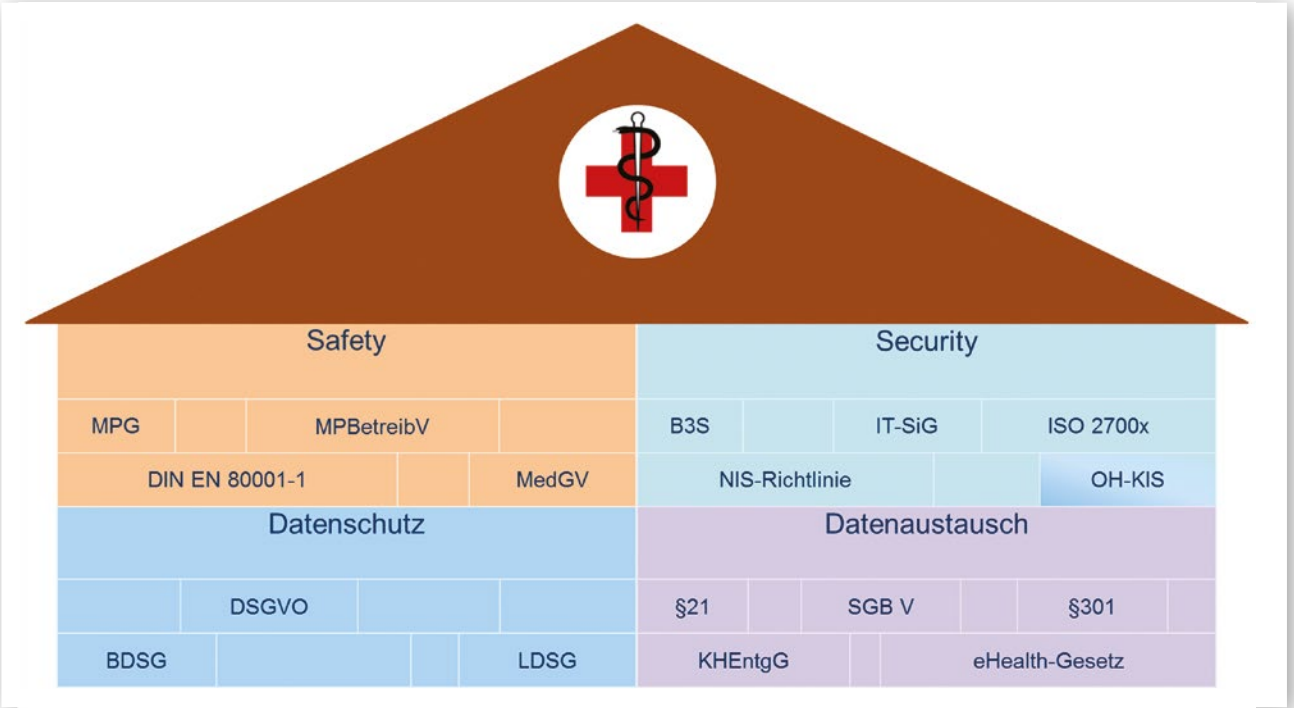


Abb. 1: Wesentliche Regelungen, Normen und Standards im Krankenhausbetrieb, die IT-Sicherheit tangierend

Verwendete Abkürzungen

NIS	Netz- und Informationssicherheit
IT-SiG	IT-Sicherheitsgesetz
DSGVO	Datenschutz-Grundverordnung
BDSG	Bundesdatenschutzgesetz
LDSG	Landesdatenschutzgesetz
KHEntgG	Krankenhausentgeltgesetz
eHealth-Gesetz	Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen
SGB V	Sozialgesetzbuch Fünftes Buch
MPG	Medizinproduktegesetz
MedGV	Medizingeräteverordnung
MPBetreibV	Verordnung über das Errichten, Betreiben und Anwenden von Medizinprodukten

MoSaIK: Angesprochene Sektoren und Branchen

Patrick Leibbrand, Holger Maczkowsky

Forschungsprojekt:
MoSaIK

Sektoren und Branchen

Das Verbundprojekt „Modellbasierte Sicherheitsanalyse IKT-basierter Kritischer Infrastrukturen“ (MoSaIK) überspannt insgesamt drei unterschiedliche Sektoren entsprechend der aktuell überarbeiteten und auf Bundesebene gültigen Einteilung Kritischer Infrastrukturen in neun Sektoren und 29 Branchen. Es nimmt konkret Bezug auf die Sektoren Staat und Verwaltung, Energie sowie Informationstechnik und Telekommunikation.

Insbesondere der letztgenannte Sektor kann als eine Art Querschnittdisziplin aufgefasst werden, welcher die beiden anderen angesprochenen, jedoch auch alle übrigen definitionsgemäßen Sektoren technisch und organisatorisch verknüpft. Diese Verknüpfung ist nicht etwa nur akademischer Natur, sondern spiegelt sich in vielfältigen Interdependenzen der Sektoren wider und entspricht der täglichen Praxis beim Aufbau und dem operativen Betrieb Kritischer Infrastrukturen.

Unter diesem Aspekt ist es geradezu notwendig, die Bedürfnisse und Implikationen für die betrachteten Infrastrukturen der Anwendungspartner von MoSaIK unter Forschungs- und Entwicklungsaspekten integriert zu betrachten, um schließlich die angestrebte Modellbildung zur verallgemeinerten Sicherheitsanalyse Kritischer Infrastrukturen zu forcieren.

> Gewinnung valider Messdaten ohne Störung des laufenden Produktivbetriebes involvierter Sektoren als Grundlage der IT-Sicherheit

Derlei Sicherheitsanalysen sind die Voraussetzung für die Gewinnung valider Daten als Grundlage für Sicherheitsmaßnahmen, die im neuen IT-Sicherheitsgesetz aus dem Jahr 2015 verankert wurden. Diese Rechtsgrundlage trägt der besonderen, gesellschaftsübergreifenden Bedeutung Kritischer Infrastrukturen vor dem Hintergrund einer umfänglichen Durchdringung mit Informations- und Kommunikationstechnik Rechnung. Insbesondere für den Sektor „Energie“ ist darüber hinaus das Energiewirtschaftsgesetz (EnWG) maßgeblich, das unter anderem einen dedizierten Sicherheitskatalog mit Umsetzungsverpflichtung zur Abwehr von informationstechnischen Bedrohungen für IT-Systeme von Energieversorgungseinrichtungen festschreibt.

Staat und Verwaltung

Im Sektor Staat und Verwaltung richtet sich MoSaIK an die Branche Notfall-/Rettungswesen einschließlich Katastrophenschutz, in der Behörden und Organisationen an sich bereits eine Kritische Infrastruktur darstellen. Nicht zuletzt der hohe Detaillierungsgrad heutiger Organisationen der Notfallrettung macht diese anfällig für äußere Störungen, zusätzlich zu deren Belastung bei eigener Betroffenheit durch Schadenlagen unterschiedlicher Ausprägung und unterschiedlichen Umfangs. Ohne weitreichenden Einsatz von Informationstechnik und Telekommunikation ist die praktische Arbeit im Notfall- und Rettungswesen nicht leistbar. Technik, die einerseits die Umsetzung von Schutzmaßnahmen erst ermöglicht, eröffnet andererseits auch immer Einfallstore insbesondere für anthropogene Gefahren.

Energie

Im Sektor Energie richtet sich MoSaIK vorwiegend an die Branche Elektrizität, obgleich die betreffenden Anwendungspartner auch mit den übrigen Branchen aus dem Sektor Energie in engem Bezug stehen. Dies erscheint mit Blick auf eine sachgerechte Begrenzung der Projektkomplexität angebracht, bringt jedoch auch vor dem Hintergrund der Übertragbarkeit der Ergebnisse auf angrenzende Branchen keine Nachteile im Hinblick auf die Modellierung von Sicherheitsanalysen für Kritische Infrastrukturen aus dem Sektor Energie im Allgemeinen.

Informationstechnik und Telekommunikation

Im Sektor Telekommunikation und Informationstechnik spielt im Verbundprojekt MoSaIK vorwiegend die Branche Informationstechnik eine Rolle, wobei auch Telekommunikation für die Funktion der Kritischen Infrastrukturen der Anwendungspartner von großer Bedeutung ist. Wie bereits angesprochen beschreibt dieser Sektor eine Querschnittfunktion und durchzieht die beiden erstgenannten, grundsätzlich jedoch auch alle weiteren definitionsgemäßen KRITIS-Sektoren in der Praxis

sowohl technisch als auch organisatorisch. Aus diesem Grund setzen zentrale Prozesse zur Messdatenerhebung unmittelbar an informationstechnischen Komponenten der untersuchten Kritischen Infrastrukturen der Anwendungspartner an. Dies ermöglicht eine vergleichsweise einfache Gewinnung aussagekräftiger Daten, ohne zu stark in den laufenden Produktivbetrieb einzugreifen oder letztlich deutlich schwieriger handhabbare Organisationsdaten zu akkumulieren.

Abb. 1: Definitionsgemäße KRITIS-Sektorenansicht mit ITK als Querschnittsektor. Jedem Sektor gehören mehrere Branchen an. Im Projekt MoSaIK wurden die außen dargestellten Branchen „Notfall- / Rettungswesen" (zum Sektor „Staat und Verwaltung" gehörig) sowie „Elektrizität" (den Sektor „Energie" betreffend) exemplarisch betrachtet.

Hafentelematik – Zentraler Hub für die Hafenwirtschaft

Nils Meyer-Larsen, Rainer Müller, Karsten Sohr, Annabelle Vöge

Forschungsprojekt:
PortSec

Mehr als 90 Prozent der weltweit gehandelten Güter werden auf dem Seeweg transportiert – gerade für den „Exportweltmeister" Deutschland sind die Häfen daher eine zentrale Voraussetzung für den wirtschaftlichen Erfolg. Ein Ausfall der Hafeninfrastrukturen würde jedoch nicht nur finanzielle Folgen haben, sondern könnte auch zu Versorgungsengpässen bei der Bevölkerung führen. Nicht zuletzt können auch gravierende Sicherheitsrisiken entstehen, wenn Gefahrgüter nicht sachgemäß umgeschlagen und überwacht werden. Einen möglichen Angriffspunkt bilden dabei die Informations- und Kommunikationstechnologien: In modernen Häfen wird der gesamte Umschlag mittlerweile elektronisch gesteuert und der Datenaustausch zwischen einer Vielzahl von Beteiligten zentral organisiert. Eine zentrale Rolle nehmen hier Hafentelematiksysteme ein. Sie verfügen funktionsbedingt über eine Vielzahl von Schnittstellen zu vielen verschiedenen Partnern: Zoll, Terminal-Betreiber, Reeder, Lkw-Operateure, Bahn-Operateure, Binnenschiff-Operateure, Speditionen und weitere Behörden und Unternehmen. Die Schnittstellen sind technisch heterogen: EDIFACT, XML, RPC, SOAP, aber auch E-Mail.

Um spezifische Sicherheitsanforderungen für Hafentelematiksysteme zu berücksichtigen, werden die Geschäftsprozesse und entsprechende rechtliche und betriebswirtschaftliche Anforderungen formal repräsentiert. Hierdurch kann ein Sicherheitsevaluator eventuell bestehende Situationen aufdecken, in denen unerlaubte Zugriffe auf Geschäftsprozesse möglich sind und organisationsinterne Kontrollregeln umgangen werden (wie z. B. die Aufgabentrennung bzw. das Vieraugen-Prinzip). Dieser Schritt trägt dazu bei, dass die Sicherheitsanforderungen mit den gesetzlichen und organisatorischen Vorgaben übereinstimmen, die für den Betrieb und die Nutzung von Hafentelematiksystemen gelten. Die zu prüfenden Sicherheitsanforderungen werden dabei aus den formalen Beschreibungen der Geschäftsprozesse, gesetzlichen/wirtschaftlichen Anforderungen sowie technischen Anforderungen abgeleitet.

Im nächsten Schritt wird die tatsächlich implementierte Software- bzw. Systemarchitektur gegen die ermittelten Sicherheitsanforderungen und die formal repräsentierten Prozessbeschreibungen geprüft. Dieser Schritt führt dazu, dass für die Hafentelematik spezifische Risiken ermittelt werden können, etwa ob ein Mitarbeiter aufgrund von zu umfassenden Zugriffsrechten unkontrolliert die Deklaration von Gefahrgutcontainern ändern könnte. Gleichzeitig werden eventuell bestehende allgemeinere technische Sicherheitsrisiken identifiziert, wie z. B. unsichere Verwendung von Software-Frameworks oder fehlerhafte Verschlüsselung.

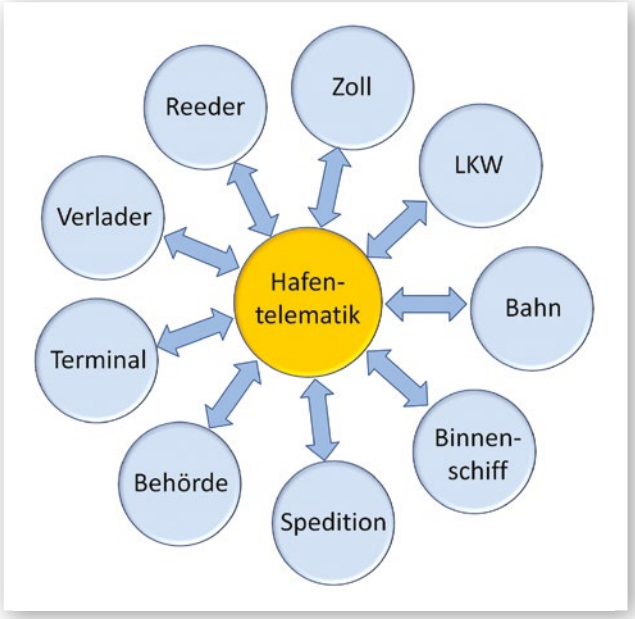


Abb. 1: Hafentelematik und Kommunikationspartner

Compliance und Risikomanagement – Anforderungen an Finanzinstitute in der EU

Torsten Bollen

Forschungsprojekt:
PREVENT

Finanzdienstleister, insbesondere Banken, sind stark reguliert durch EU- und Bundesgesetze, Bankenaufsicht, nationale und internationale Standards und Gremien. Es gibt eine Reihe von Gesetzen, Standards und Regularien, die hier in Kurzform mit ihrer jeweiligen Kernaussage genannt und skizziert werden können.

Diese zunehmend stärker werdenden regulativen Anforderungen werden für die Banken im Umfeld der Compliance sichtbar. Ein wesentlicher Teil der Regularien stellt unmittelbare Anforderungen an das operative Risikomanagement in der Bank mit Schwerpunkt auf den Risiken im IT-Betrieb.

Compliance – Normen und Gesetze, die in Banken-RZ unter anderem bereits Anwendung finden:

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

Teil des PREVENT-Ansatzes ist es, die sich aus den Geschäftsprozessen ergebenden Compliance Anforderungen durch IT-Verfahren so abzubilden, dass das Management der Bank in seinen Entscheidungen unterstützt wird.

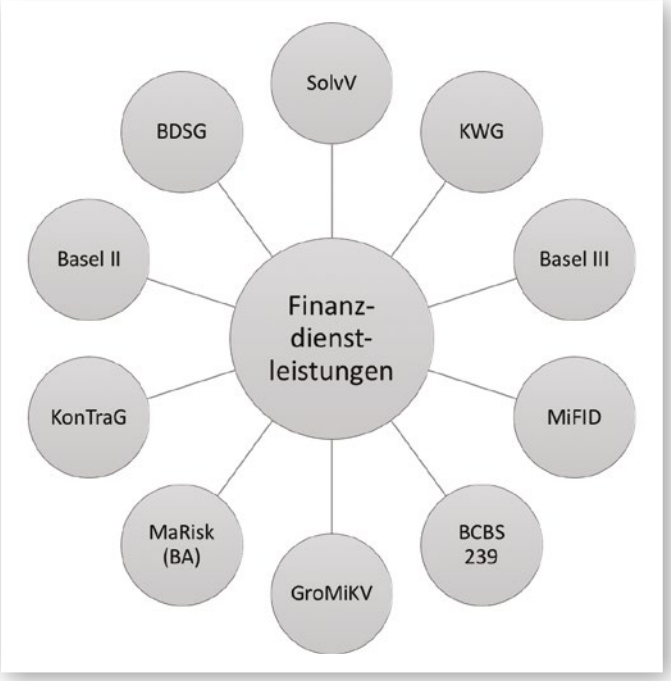


Abb. 1: Beispiele von Gesetzen und Regularien für Finanzdienstleister

Risikolagebild der industriellen IT-Sicherheit am Beispiel des Energiesektors

Wigand Weber

Forschungsprojekt:
RiskViz

IT-Sicherheitslagebild am Beispiel Energiesektor

Dem Sektor Energie mit seinen Branchen Elektrizität, Mineralöl und Gas kommt eine zentrale Rolle im gesamtem KRITIS-Umfeld zu. Ein Ausfall der Versorgung mit Energie hätte auch für alle anderen Sektoren große Auswirkungen.

Konventionelle Kraftwerke, wie Atom-, Kohle- und Gaskraftwerke, setzen sehr viele Steuerungskomponenten ein, die untereinander vernetzt sind. Diese Netze sind im Allgemeinen nach außen abgeschottet. Ein Betrieb ist ohne Verbindung zum Internet möglich. Es bestehen jedoch immer wieder temporäre Verbindungen nach außen. Über diese Verbindungen können externe Dienstleister über das Internet Wartung und Support durchführen oder es werden statistische Daten oder Messdaten an andere Standorte übermittelt. Der Trend zum externen Zugriff auf alle Daten über das Internet hat jedoch in den letzten Jahren stark zugenommen. Diese Schnittstellen stellen eine erhebliche Angriffsfläche dar.

Wasser-, Solar- und Geothermiekraftwerke sowie Windkraftanlagen und Umspannwerke werden oft dezentral und unbemannt betrieben. Daher müssen ihre Mess- und Steuerungsdaten an zentrale Leitstellen übermittelt werden. Hier werden die Daten oft mithilfe von unsicheren Fernwirkprotokollen über das Internet übermittelt. Ein nicht zu unterschätzendes Problem stellen zudem die vielen privaten Solarenergie-Einspeiser und Blockheizkraftwerke dar. Auch hier müssen Steuerungs- und Messdaten über öffentlich verfügbare Datenverbindungen in die Zentralen der Energieversorger übermittelt werden. Die Betreiber dieser privaten Anlagen besitzen jedoch meist nicht das nötige IT-sicherheitstechnische Grundwissen, um ihre Anlagen gegen Angriffe von außen zu schützen. Ein gezielter und gleichzeitiger Angriff auf eine größere Anzahl solcher Kleinanlagen könnte die gesamte Energieversorgung aus dem Gleichgewicht bringen.

Der Trend zu Industrie 4.0 hält auch in den Energiesektor Einzug. Immer mehr Industrie- und Steuerungskomponenten kommunizieren selbständig und autonom über das Internet miteinander oder auch mit ihrem Hersteller oder Lieferanten.

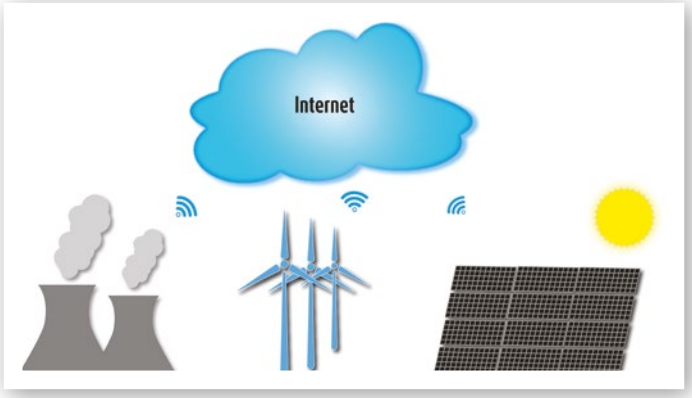


Abb. 1: Vernetzung im Zeitalter von Industrie 4.0

Mit der im Verbundprojekt entwickelten Suchmaschine können diese direkt an das Internet angeschlossenen Komponenten aufgespürt und lokalisiert werden. Ferner können sie anhand ihrer Eigenschaften, wie z. B. der genutzten Kommunikationsprotokolle, Modellreihe, Hersteller usw. sicherheitstechnisch bewertet werden.

Vorschriften und Normen

Durch das IT-Sicherheitsgesetz von 2016 werden u. a. Betreiber Kritischer Infrastrukturen, wie hier die Energieversorger, verpflichtet, Prozesse zu entwickeln, um die Versorgungssicherheit mit elektrischer Energie zu gewährleisten und diese im Schadensfall schnell wiederherzustellen. Sicherheitsrelevante Vorfälle müssen gemeldet werden. Die Betreiber müssen den Nachweis erbringen, dass ihr Sicherheitsmanagement dem neuesten Stand der Technik entspricht.

Diese Anforderungen können z. B. durch die Einführung eines „Managementsystems für Informationssicherheit“ (ISMS) erfüllt werden. Ein ISMS legt fest, mit welchen Instrumenten und Methoden das Management die auf Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenkt (plant, einsetzt, durchführt, überwacht und verbessert).

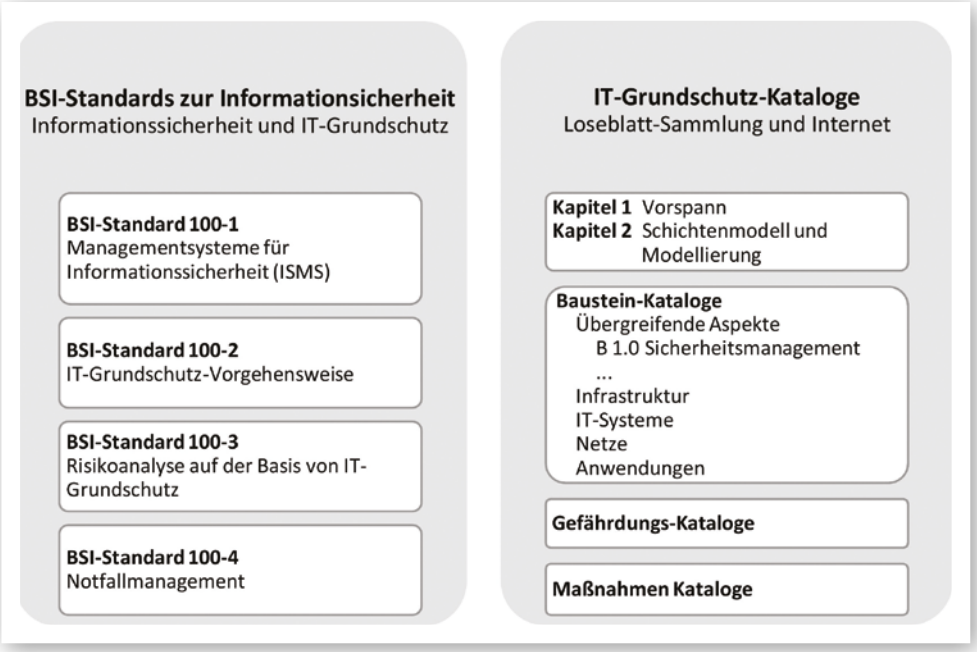


Abb. 2: Bestandteile eines Managementsystems für Informationssicherheit (ISMS) (Quelle: BSI-Standard 100-1)

Eine zentrale Bedeutung kommt hier den Normen ISO/IEC 27001/27002 und 27019 zu. In diesen Normen werden die Anforderungen an ein ISMS und dessen Einführung und Etablierung im Unternehmen beschrieben. Weiterhin werden darin die Einführung und Durchführung von Risikoanalysen und eines Risikomanagements gefordert. Die Norm ISO/IEC 27019 wurde speziell für den Energiesektor entwickelt. Durch die Zertifizierung von Unternehmen nach diesen Normen können die Unternehmen die Vorgaben des IT Sicherheitsgesetzes einhalten.

Mit den Grundschutz-Standards des BSI (Bundesamt für Sicherheit in der Informationstechnik) wird eine andere Herangehensweise bei der Einführung eines ISMS beschrieben. Hier werden Bottom-up IT-sicherheitsrelevante Vorgaben für IT-Komponenten gemacht, um so ein Sicherheitslagebild zu erstellen. Zur Vereinheitlichung wurden Anleihen an die Normen ISO/IEC 2700x gemacht. So ist nun z. B. der BSI-Standard 100-1 vollständig kompatibel zur Norm 27001.

Der gezielte Einsatz der im Verbundprojekt entwickelten Suchmaschine kann in ein ISMS eingebunden werden, um initial die mit dem Internet verbundenen Komponenten eines Betreibers aufzuspüren und sicherheitstechnisch zu bewerten, und danach die evtl. getroffenen Maßnahmen abzusichern. Durch die regelmäßige Nutzung kann eine Verbesserung oder Verschlechterung des Sicherheitsniveaus dokumentiert werden (siehe auch Sektion 2.)

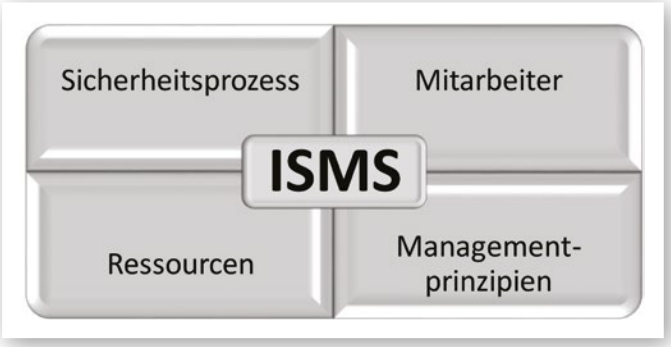


Abb. 3: BSI-Standards zur Informationssicherheit (Quelle: BSI-Standard 100-1)

Informationstechnik in der Energieversorgung – Besonderheiten und Regularien

Heiko Kanisch, Franka Schuster, Hartmut König

Forschungsprojekt:
SICIA

Charakteristik der IT in der Energieversorgung

Moderne, dem Stand der Technik entsprechende digitale Prozessleitsysteme zur Steuerung und Überwachung von Kraftwerken und Energieversorgungsnetzen nutzen verstärkt Technologien, Hard- und Softwarekomponenten und Netzprotokolle, wie sie in der klassischen Informationstechnik zum Einsatz kommen oder häufig den Anforderungen dieser Industriebranche entsprechend entwickelt wurden und werden. Beispiele sind Intel-basierte Client- und Serversysteme mit Standard-Betriebssystemen wie Windows, Anwendungen wie relationale Datenbank-Managementsysteme und Kommunikation über Ethernet-basierte und IP-Netze. Im Bereich der Prozessleittechnik kommen diese Standardprodukte insbesondere auf Ebene der Prozessführung (Bedienen und Beobachten, Mensch-Maschine-Schnittstelle), der Planungs- und Engineering-Werkzeuge und der technologischen Expertensysteme zur Anlagenanalyse und -optimierung zum Einsatz. Hervorzuheben ist dabei die große Heterogenität der eingesetzten Systeme in den Kraftwerken und Verteilnetzen.

Anforderungen an die IT in der Energieversorgung

Leitsysteme dienen primär nicht der Informations- und Datenverarbeitung, sondern steuern, regeln und überwachen vielfältige und komplexe technologische Prozesse. Dazu wird eine Vielzahl von aktuellen Messwerten und Signalen aus dem technologischen Prozess (Feldsensorik) verwendet und es wird über Stelleingriffe (Feldaktuatorik) auf die Anlage und den Prozess unmittelbar eingewirkt. Besonderes Kennzeichen ist hierbei die Echtzeit-Anforderung für die gesamte Signalkette (Erfassung, Übertragung, Verarbeitung, Rückwirkung und Visualisierung), die unmittelbar aus der Dynamik der physikalischen und chemischen Naturgesetzmäßigkeiten folgt. Unzulässige Abweichungen können unter Umständen zur Abschaltung der Anlage und zur Überführung in den sicheren Prozesszustand (Not-Aus) führen. Ein weiteres

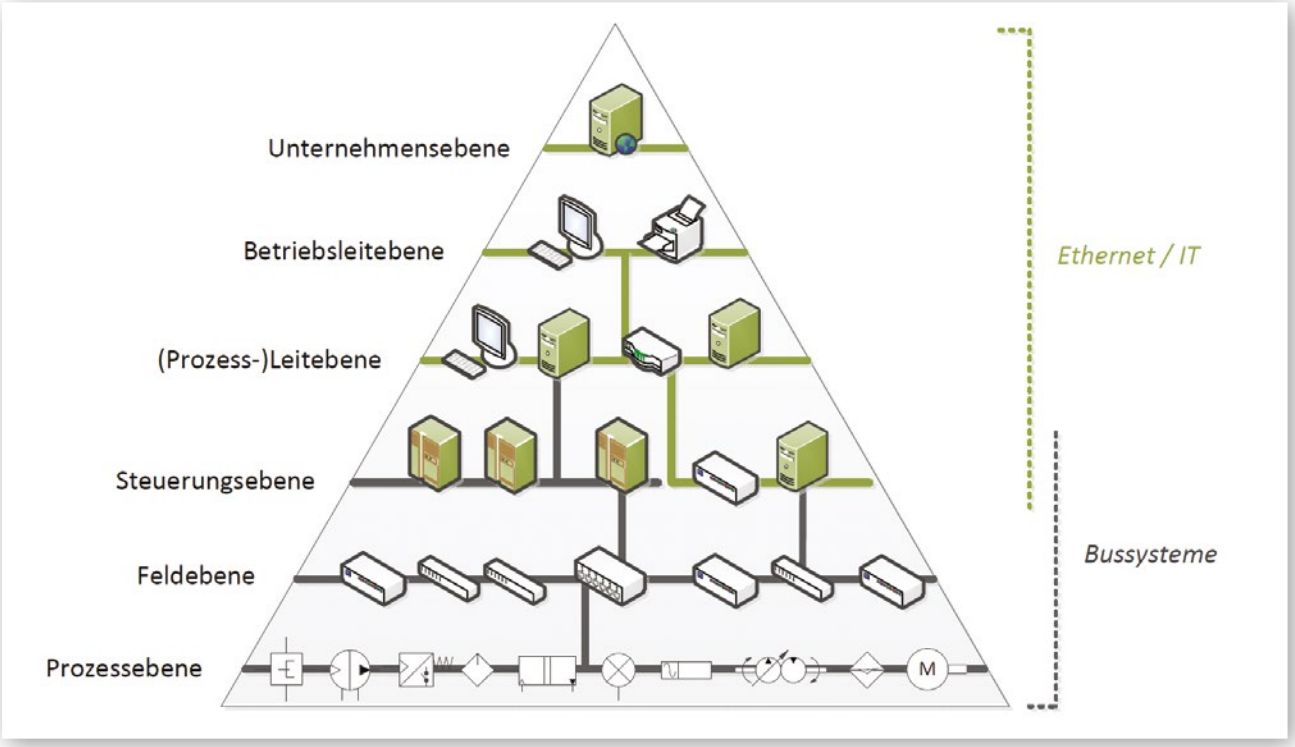


Abb. 1: Klassische Kommunikationstechnik (Ethernet) bis auf Steuerungsebene

wesentliches Merkmal ist die überwiegend geforderte „24 Stunden, 365 Tage"-Betriebsführung der Anlagen. Daraus folgt die Anforderung an eine sehr hohe Verfügbarkeit des Leitsystems. Planmäßige und umfangreiche Wartungen können in der Regel nur in Revisionsstillständen mit Intervallen von zwei bis vier Jahren durchgeführt werden. Ein monatliches „Wartungsfenster" in den Nachtstunden oder am Wochenende – wie in der Büro-IT üblich – ist bei der derzeitigen Betriebsweise nur bedingt anwendbar.

Abb. 2: Eingesetzte IT in der Prozessleittechnik (www.siemens.com/presse)

Nationale Regularien

Zwar gab es vor 2015 bereits branchenspezifische Standards, wie die VGB-S-175 [1] oder das BDEW-Whitepaper [2], die eine systematische Bewertung und Erhöhung der IT-Sicherheit verlangen. In 2015 sind mit dem IT-Sicherheitsgesetz [3] und dem IT-Sicherheitskatalog für Energienetze [4] jedoch die zwei bisher entscheidenden Regelungen zur IT-Sicherheit in der Energieversorgung in Kraft getreten. Nach den Netzbetreibern muss nun laut IT-Sicherheitsgesetz Artikel 3 Abs. 1b auch jeder Betreiber einer Erzeugungsanlage, die laut BSI-Kritisverordnung [5] Kritische Infrastruktur und an ein Energieversorgungsnetz angeschlossen ist, zukünftig einen angemessenen Schutz gegen Bedrohungen für IT-Systeme, die für einen sicheren Betrieb notwendig sind, gewährleisten. Wie für Energienetze soll es einen IT-Sicherheitskatalog der Bundesnetzagentur mit Anforderungen an Erzeugungsanlagen geben.

Der IT-Sicherheitskatalog, der für Energienetze bereits veröffentlicht ist, gilt ab 31.01.2018. Ein Termin für die Veröffentlichung des IT-Sicherheitskatalogs für Erzeugungsanlagen steht bisher nicht fest (Stand 9/2017). Vermutlich wird dieser inhaltlich weitgehend identisch mit dem für die Netzbetreiber sein.

Quellen

[1] VGB PowerTech: IT-Sicherheit für Erzeugungsanlagen (VGB-S-175), 2014.

[2] BDEW Bundesverband der Energie und Wasserwirtschaft: Anforderungen an sichere Steuerungs- und Telekommunikationssysteme, Stand 3/2015.

[3] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), Bundesgesetzblatt 2015 Teil I Nr. 31, 24.07.2015.

[4] IT-Sicherheitskatalog gemäß §11 Absatz 1a Energiewirtschaftsgesetz, Stand 8/2015.

[5] Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung, BSI-KritisV), Bundesgesetzblatt 2016 Teil I Nr. 20, 02.05.2016.

Stand der IT-Sicherheit bei deutschen Stadtwerken

Julian Dax, Benedikt Ley, Sebastian Pape, Volkmar Pipek, Kai Rannenberg, Christopher Schmitz, André Sekulla

Forschungsprojekt:
SIDATE

Stand der IT-Sicherheit bei deutschen Stromnetzbetreibern

Im Projekt SIDATE wurde eine Umfrage zum Stand der IT-Sicherheit bei deutschen Stromnetzbetreibern durchgeführt. Dazu wurden alle 881 im August 2016 bei der Bundesnetzagentur gelisteten Betreiber angeschrieben. Im Umfragezeitraum vom 1. September 2016 bis 15. Oktober 2016 antworteten von diesen 61 (6,9%) Betreiber. Der Fragebogen fokussiert auf die Umsetzung der rechtlichen Anforderungen und die Implementierung eines Managementsystems für Informationssicherheit (ISMS). Weiterhin wurden aber auch Fragen zu Leitsystem, Netzaufbau, Prozessen und organisationalen Strukturen und zur Büro-IT gestellt. Nachfolgend werden einige ausgewählte Ergebnisse der Umfrage präsentiert. Die vollständige Umfrage ist als technischer Bericht verfügbar [1].

Übersicht der teilnehmenden Stromnetzbetreiber

Zunächst wurde die Größe abhängig von den Zählpunkten der befragten Stromnetzbetreiber ermittelt. Anhand der Ergebnisse, wie in Abbildung 1 dargestellt ist, wurden vier etwa gleich große Gruppierungen festgelegt (kleine (bis 15.000 Zählpunkte), mittlere (15.001 bis 30.000 Zählpunkte), große (30.001 bis 100.000 Zählpunkte) und sehr große (ab 100.000 Zählpunkten) Stromnetzbetreiber).

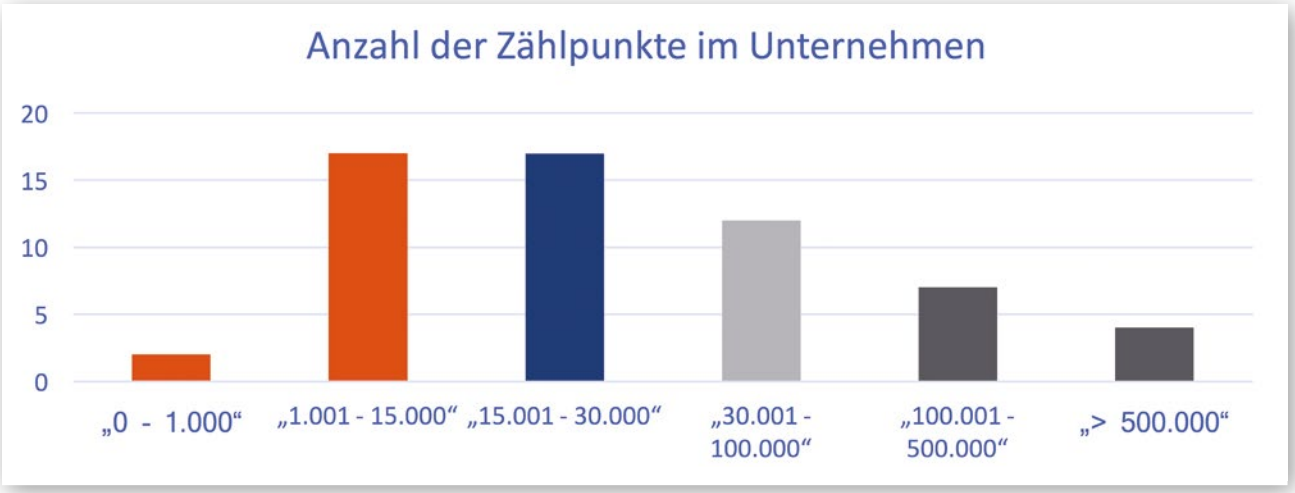


Abb. 1: Anzahl der Zählpunkte im Unternehmen

IT-Sicherheit als Dienstleistung

Aus zwei weiteren Fragen (Abbildung 2) wird deutlich, dass der Großteil der Netzbetreiber auf externes Informationssicherheits-Know-how zurückgreift, insbesondere bei der Einführung eines ISMS (ohne Abbildung, siehe technischer Bericht [1]).

Auch für die Durchführung von Sicherheitsaudits (Abbildung 3) werden externe Dienstleister herangezogen. Diese sollen Schwachstellenscans oder Penetrationstests für die Systeme zur Steuerung der Netzleittechnik durchführen. Wobei etwa die Hälfte der Befragten angibt keine Sicherheitsaudits durchzuführen.

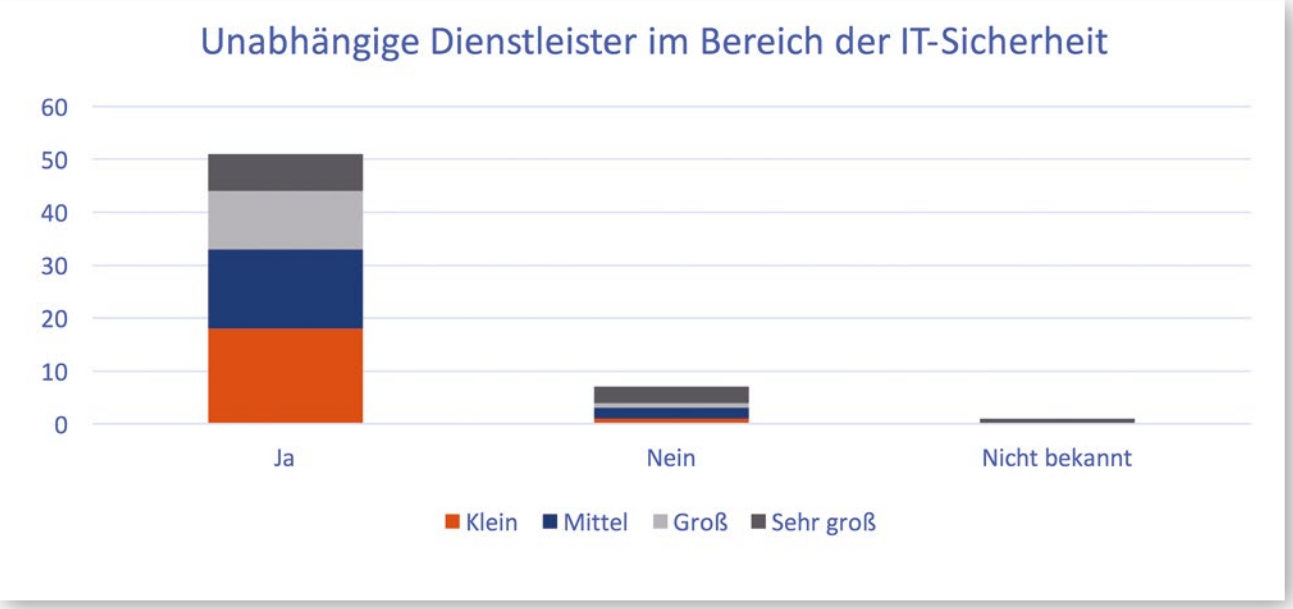


Abb. 2: Unabhängige Dienstleister im Bereich der IT-Sicherheit

IT-Sicherheitsmanagement

Anhand der aufgeführten Umfrageergebnisse wird ersichtlich, daß ein Großteil der Stromnetzbetreiber ihre IT-Sicherheit an externe Dienstleister ausgelagert haben. Dies kann für eine kurzfristige Lösung, die Einführung des ISMS, sinnvoll sein. Auf längere Sicht gesehen sollten sich die Mitarbeiter des Betreibers dennoch vermehrt um IT-Sicherheit kümmern denn sie ist notwendig und wird immer wichtiger. An dieser Stelle soll das SIDATE Portal anknüpfen und als Wissensaustauschplattform zur Verbreitung von Erfahrungen in Bezug auf IT-Sicherheit und entsprechende Maßnahmen beitragen.

Sicherheitsaudits und -leitlinien

Fast die Hälfte der befragten Stromnetzbetreiber führt keine regelmäßigen Sicherheitsaudits durch (siehe Abbildung 3). Die Stromnetzbetreiber, die Audits durchführen, greifen überwiegend entweder nur oder auch auf externe Dienstleister zurück, was den unter IT-Sicherheit als Dienstleistung beschriebenen Eindruck verstärkt. Ebenso verfügt fast die Hälfte der befragten Stromnetzbetreiber über keine Sicherheitsleitlinien (siehe Abbildung 4), die auch in regelmäßigen Zeitabständen überprüft und gegebenenfalls angepasst werden (ohne Abbildung, siehe technischer Bericht [1]).

Bei beiden Punkten ist der Trend zu sehen, daß der Anteil von Stromnetzbetreibern, die Sicherheitsaudits durchführen bzw. Leitlinien haben von klein zu mittleren zu (sehr) großen Betreibern zunimmt.

ISMS-Einführung

Zur Zeit der Befragung haben die meisten Stromnetzbetreiber mit der Einführung eines Managementsystems für Informationssicherheit (ISMS) begonnen (siehe Abbildung 5). Im 2. Halbjahr 2017 planen über 85% die Einführung abgeschlossen zu haben. Abbildung 6 gibt einen detaillierten Einblick in den Stand der Einführung von ISMS bei den Betreibern. Hier wird z.B. deutlich das 36 der befragten Unternehmen mit der Erstellung der geforderten Dokumentationen begonnen haben und 24 bereits die Phase der Zielsetzung und des Scopings, d.h. der Frage welche Unternehmensbereiche vom ISMS abgedeckt werden sollen, beendet haben. Mit den Vorbereitungen auf das Zertifizierungsaudit hatten hingegen noch die wenigsten Energieversorger begonnen. Als Hauptgründe für die Einführung eines ISMS wurden rechtliche Anforderungen und die gestiegene Bedrohungslage genannt (ohne Abbildung, siehe technischer Bericht [1]). Erwartungen an die Einführung des ISMS waren konsequenterweise dann auch die Erfüllung rechtlicher Anforderungen sowie die Verbesserung der Informationssicherheit im Unternehmen (ohne Abbildung, siehe technischer Bericht [1]).

Risikoanalysen

Einer der komplexeren Teile des ISMS sind Risikoanalysen, bei denen das Risiko möglicher Sicherheitsvorfälle bewertet wird. Leider war etwas der Hälfte der Befragten nicht bekannt wie häufig Risikoanalysen im Unternehmen durchgeführt werden (siehe Abbildung 7). Positiv stimmt aber, dass bei der verbleibenden Hälfte die Mehrzahl Risikoanalysen mindestens einmal im Jahr durchführt.

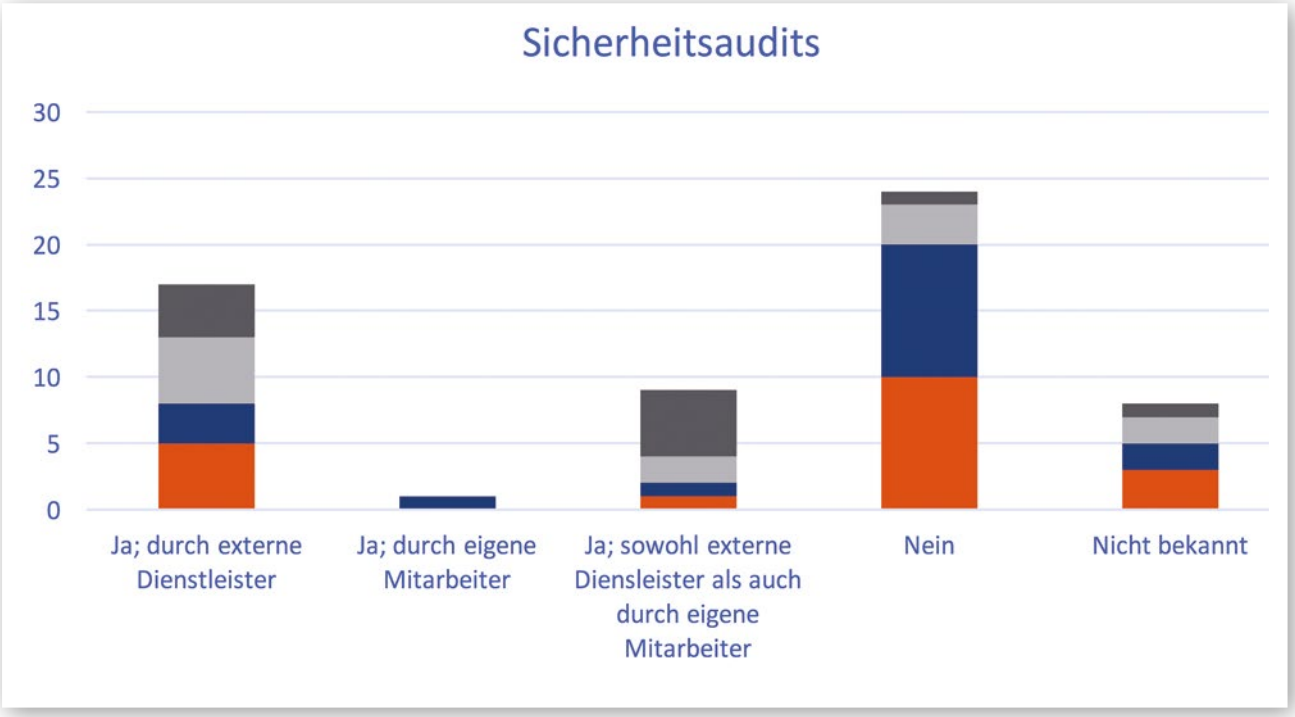


Abb. 3: Sicherheitsaudits

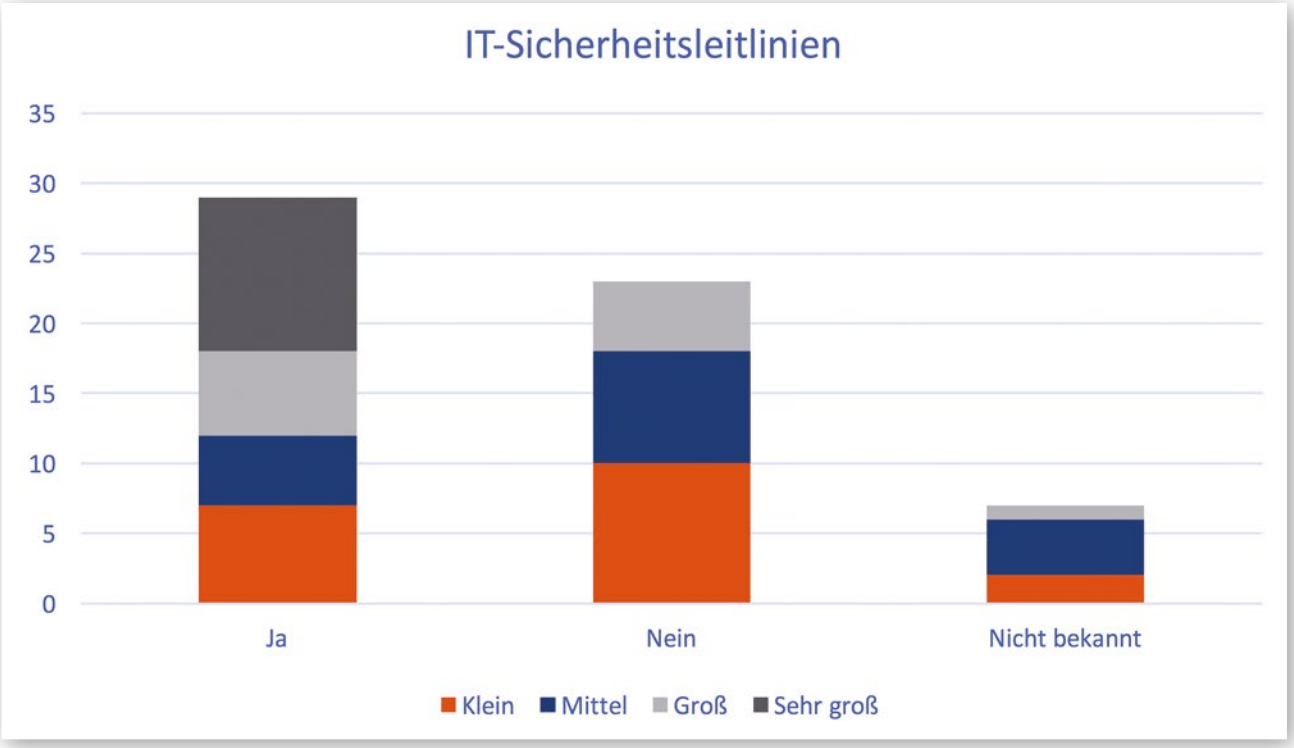


Abb. 4: IT-Sicherheitsleitlinien

Quelle

[1] Dax, J.; Ley, B.; Pape, S.; Pipek, V.; Rannenberg, K.; Schmitz, C: und Sekulla, A.: Stand zur IT-Sicherheit deutscher Stromnetzbetreiber: technischer Bericht, Universität Siegen, 2017. URL: http://dokumentix.ub.uni-siegen.de/opus/volltexte/2017/1185/.

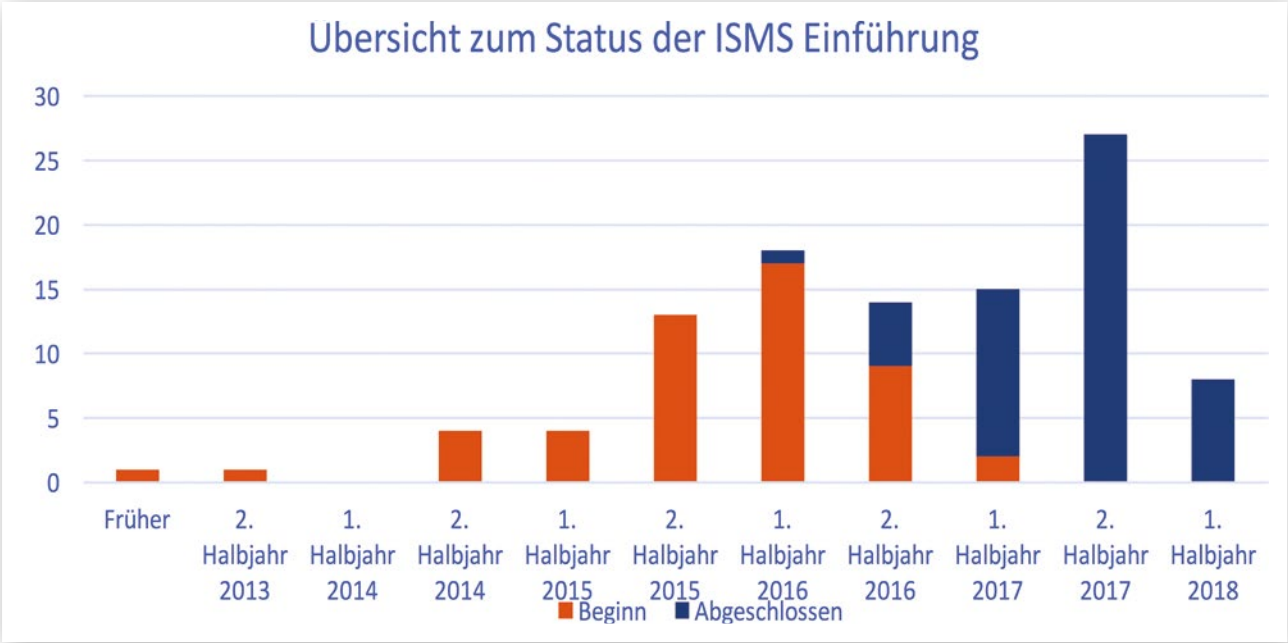


Abb. 5: Übersicht zum Status der ISMS Einführung

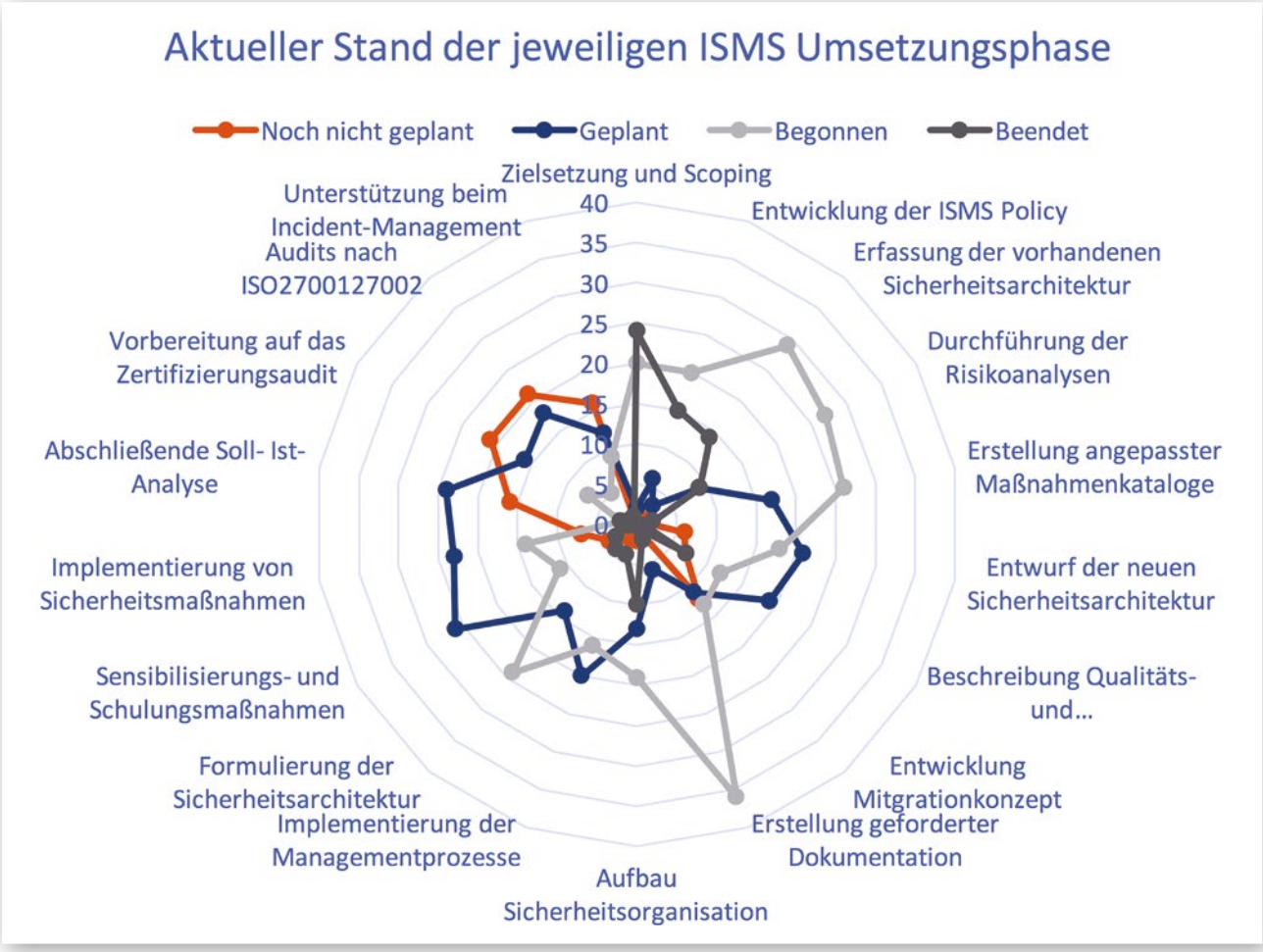


Abb. 6: Aktueller Stand der jeweiligen ISMS Umsetzungsphase

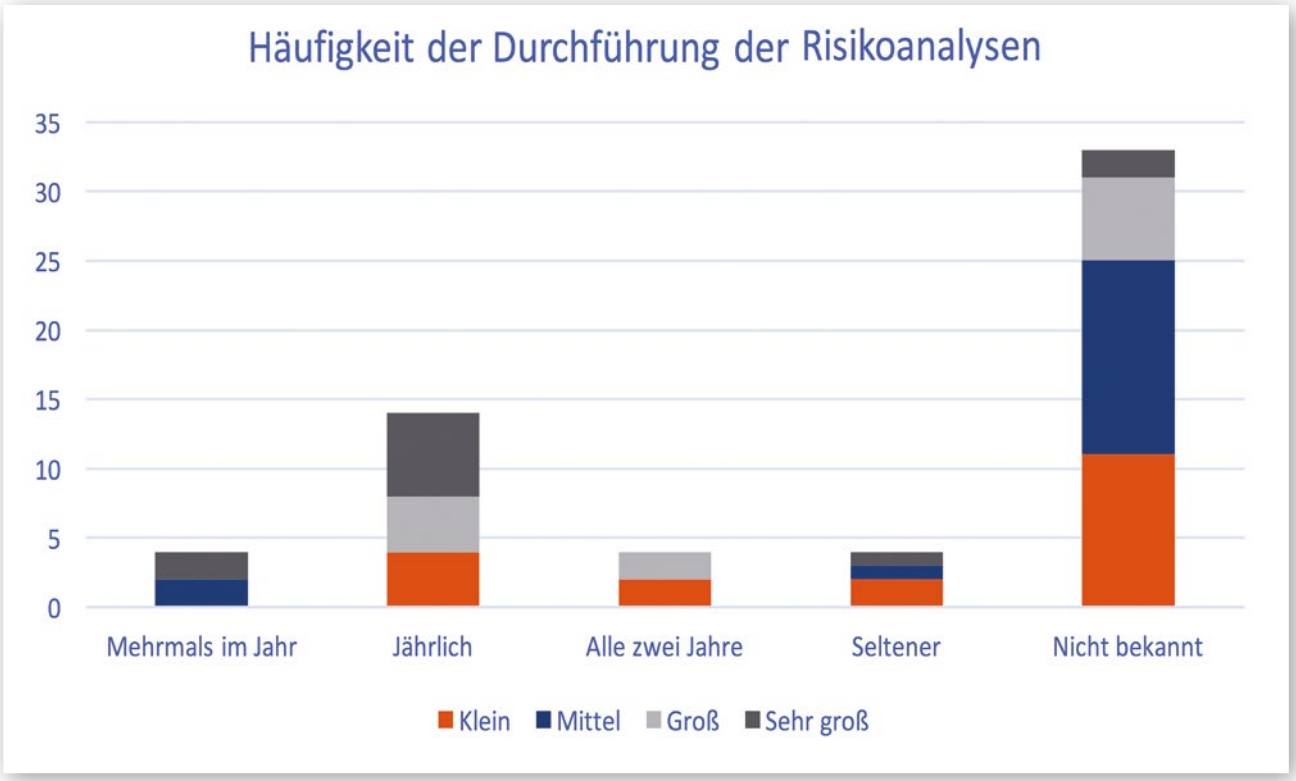


Abb. 7: Häufigkeit derDurchführung der Risikoanalysen

IT-Sicherheitsrecht

Dennis-Kenji Kipker

Forschungsprojekt:
VeSiKi

Das Institut für Informations-, Gesundheits- und Medizinrecht (IGMR) an der Universität Bremen bildet die rechtswissenschaftliche Forschung im Förderschwerpunkt „ITS|KRITIS" ab. Neben der individuellen juristischen Begleitung der jeweiligen Verbundprojekte steht die Analyse der Rechtsetzungsakte im Bereich der Cybersecurity auf deutscher und europäischer Ebene im Mittelpunkt, daneben werden transnationale Bezüge zu weiteren Rechtsordnungen hergestellt. Erklärtes Forschungsziel des IGMR ist es, nicht nur das bestehende IT-Sicherheitsrecht darzustellen und eine anwendernahe und praxisgerechte Aufbereitung der Regulierung von Cybersecurity zu geben – beispielsweise in der Form von Workshops, Seminaren und Vorträgen – sondern ebenso das geltende Recht fortzuschreiben, indem dem Gesetzgeber und weiteren relevanten Stakeholdern aus Wirtschaft und Wissenschaft Impulse zu aktuellen Rechtsetzungsthemen zur Verfügung gestellt werden. Im Rahmen

Literatursammlung zur deutschen und internationalen IT-Sicherheitsgesetzgebung seit 2015

seiner Tätigkeit für das Begleitforschungsprojekt „VeSiKi" hat das Institut deshalb verschiedene Beiträge veröffentlicht, wobei nahezu der gesamte deutsche und europäische Gesetzgebungsprozess im Bereich der IT-Security seit dem Jahr 2015 abgebildet wird. Eine Auswahl der Veröffentlichungen findet sich, in chronologischer Auflistung, an dieser Stelle:

- Kipker: Stellungnahme zum Entwurf des People 's Republic of China Cybersecurity Law, MMR-Aktuell 2015, 370972 (Aufsatz)
- Kipker: Das IT-Sicherheitsgesetz (IT-SiG): Wesentliche Gesetzesänderungen und neue rechtliche Rahmenbedingungen, BMBF-Begleitforschung VeSiKi, November 2015 (Working Paper)
- Kipker: Der Referentenentwurf des BMI zur BSI-Kritisverordnung (BSI-KritisV) vom 13.01.2016, MMR-Aktuell 2016, 375759 (Aufsatz)
- Buchner/Kipker: Datenschutzrelevante Themen in der IT: Das neue IT-Sicherheitsgesetz, in: Praxishandbuch Datenschutz im Gesundheitswesen, D/7, AOK-Verlag 2016 (Buchbeitrag)
- Kipker/Harth/Jacumeit: IT-Sicherheit in Deutschland und Europa. Kritische Infrastrukturen. Neuer nationaler und europäischer Rechtsrahmen, DIN-Mitteilungen 4/2016, 4 (Aufsatz)
- Kipker: Der neue Anforderungskatalog der Bundesnetzagentur nach § 113f TKG – Zur Datensicherheit der TK-Diensteanbieter für die Vorratsdatenspeicherung, MMR-Aktuell 2016, 378702 (Aufsatz)
- Kipker: Die NIS-RL der EU im Vergleich zum IT-SiG – Deutschland ist für den neuen europäischen Cybersecurity-Raum gut gerüstet, ZD-Aktuell 2016, 05261 (Aufsatz)
- Kipker: Datenschutzrelevante Themen in der Informationstechnologie (IT): Normen und Standards im Gesundheitswesen, in: Praxishandbuch Datenschutz im Gesundheitswesen, D/8, AOK-Verlag 2016 (Buchbeitrag)
- Kipker/Pfeil: IT-Sicherheitsgesetz in Theorie und Praxis. Was Betreiber (wirklich) beachten müssen. Eine interdisziplinäre Fallstudie, DuD 2016, 810 ff. (Aufsatz)
- Kipker: The EU NIS Directive compared to the German IT Security Act – Germany is well positioned for the new European Cybersecurity Space, ZD-Aktuell 2016, 05363 (Aufsatz)
- Kipker: Der BMI-Referentenentwurf zur Umsetzung der EU NIS-RL: Wenig Überraschendes für die Betreiber von Kritischen Infrastrukturen, Neues für die Anbieter digitaler Dienste, MMR 2017, 143 (Aufsatz)
- Kipker: Umsetzungsgesetz zur NIS-RL mit nur geringen Anpassungen gegenüber der bisherigen Rechtslage beschlossen, MMR-Aktuell 2017, 389121 (Aufsatz)
- Kipker: Das neue chinesische Cybersecurity Law – ein ganzheitlicher Ansatz zur Regulierung von Informationssicherheit, MMR 2017, 455 (Aufsatz)

- Kipker: Datenschutzrelevante Themen in der IT: EU NIS-RL und nationales Umsetzungsgesetz, in: Praxishandbuch Datenschutz im Gesundheitswesen, D/7.6, AOK-Verlag 2017 (Buchbeitrag)
- Kipker: Der 2. Korb der BSI-Kritisverordnung tritt in Kraft, MMR-Aktuell 2017, 393037 (Aufsatz)
- Kipker/Harner/Müller: Der Mensch an der Schnittstelle zur Technik – Praxishilfe in der Umsetzung von Datensicherheit durch den IT-Security Navigator, in: Deutsche Stiftung für Recht und Informatik (DSRI), Tagungsband zur 18. Herbstakademie 2017, S. 651 ff. (Buchbeitrag)
- Kipker: Massiver Ausbau der EU-Cybersicherheitskapazitäten – Jahresansprache 2017 des EU-Kommissionspräsidenten Juncker und Veröffentlichung der neuen europäischen Cyber-Sicherheitsstrategie, MMR-Aktuell 2017, 394677 (Aufsatz)
- Kipker/Stelter: Trotz „Brexit": Britische Regierung plant langfristige Umsetzung der EU NIS-Richtlinie, MMR-Aktuell 2017, 394832 (Aufsatz)
- Kipker: Neuer Verordnungsentwurf für ein einheitliches europäisches IT-Sicherheitsnetzwerk, MMR-Aktuell 2017, 395945 (Aufsatz)
- Kipker: IT-Sicherheit, in: Der NEUE Datenschutz im Gesundheitswesen, Kap. E, AOK-Verlag 2018 (Buchbeitrag)
- Kipker: Anmerkung zum Entwurf einer Verordnung des Europäischen Parlaments und des Rates über einen Rahmen für den freien Verkehr nicht personenbezogener Daten in der Europäischen Union, DuD 2018, 252 im Erscheinen (Aufsatz)
- Kipker/Harner/Müller: Der Mensch an der Schnittstelle zur Technik – Praxishilfe in der Umsetzung von Datensicherheit durch den IT-Security Navigator, InTeR 2018, 24 im Erscheinen (Aufsatz)
- Kipker/Harner/Müller: Der Mensch an der Schnittstelle zur Technik – Praxishilfe in der Umsetzung von Datensicherheit durch den IT-Security Navigator, PinG 2018, im Erscheinen (Aufsatz)
- Kipker: Legal Challenges for IT Security in Clinical Data Processing, Tagungsband GenoPerspektiv-Symposium, Mohr Siebeck 2018, im Erscheinen (Buchbeitrag)
- Kipker: IT-Sicherheit und Datenschutz in China, Dokumentation zum Datenschutz, Nomos-Verlag 2018, im Erscheinen (Loseblatt)
- Kipker (Hrsg.): Praxishandbuch Cybersecurity-Recht, Beck-Verlag 2018, im Erscheinen (Buch)

Mit dem Erscheinen des zweiten Korbes der BSI-KritisV sowie der Umsetzung der EU-NIS-RL in das deutsche Recht ist der nationale wie europäische Gesetzgebungsprozess im Bereich der Cybersicherheit vorerst abgeschlossen und die Implementierung der vorgeschriebenen Maßnahmen durch Betreiber und Behörden steht im Mittelpunkt. Im Laufe der kommenden Jahre wird jedoch – gegebenenfalls auch in Anpassung an den technologischen Fortschritt – mit einer erneuten Überarbeitung bzw. Novellierung der IT-Sicherheits-Gesetzgebung zu rechnen sein, so zum Beispiel mit dem aktuell vorliegenden Entwurf der EU Cybersecurity-Verordnung. Die Universität Bremen wird diesen Umsetzungs- und Evaluationsprozess auch nach Ende der Projektlaufzeit des BMBF-Förderschwerpunktes weiter begleiten, dies insbesondere durch den IT-Security-Navigator, der in Kooperation mit VDE/DKE entsteht.

Datenschutz und Compliance

Dennis-Kenji Kipker

Forschungsprojekt:
VeSiKi

Ein funktionierendes Compliance-Management ist eine zwingende Voraussetzung zur Realisierung angemessener Maßnahmen der IT-Security. IT-Security-Compliance beschäftigt sich deshalb mit der Einhaltung derjenigen Vorgaben, die sich speziell mit der IT-Sicherheit befassen. Zu benennen sind hier unterschiedlichste Erkenntnisquellen, die von IT-Sicherheitsbeauftragten je nach Unternehmenstypus zu beachten sind: allgemeine gesetzliche Vorschriften, wie das durch das IT-SiG novellierte BSIG; branchenspezifische gesetzliche Vorschriften zum Beispiel für Banken, Versicherungen, Industrie, die Informations- und Kommunikationstechnologie, Logistik und für die öffentliche Verwaltung; technische Normen und Standards; unternehmensinterne Vorgaben, vertragliche Bestimmungen wie Geheimhaltungsverpflichtungen und Vertraulichkeitsvereinbarungen und nicht zuletzt auch die Anforderungen des so genannten „Soft Laws", worunter der Deutsche Corporate Governance Kodex (DCGK) fällt. Soweit ein IT-Sicherheitsmanagement implementiert wird, sind jedoch nicht nur allein die Quellen der IT-Security-Compliance zu beachten, sondern ebenso die zwingenden datenschutzrechtlichen Vorgaben, soweit es für Zwecke der IT-Sicherheit zu einer Verarbeitung von personenbezogenen Daten kommt.

Schnittmengen von Datenschutz und IT-Sicherheit

In diesem Rahmen zuständig ist der Datenschutzbeauftragte, der im Regelfall in einer intensiven Kooperation mit dem IT-Sicherheitsbeauftragten steht. Dabei weisen die IT-Sicherheit und der Datenschutz in vielerlei Hinsicht Schnittmengen auf. So sind zentrale Schutzziele der IT-Security, wie die Authentizität, Integrität und Vertraulichkeit von Daten, die einerseits für die Betriebssicherheit von Anlagen und Systemen zwingend sind, andererseits auch zentrale Schutzzwecke des Datenschutzrechts. So gesehen bildet die IT-Sicherheit eine Grundvoraussetzung, um in datenverarbeitenden Unternehmen das gesetzliche geforderte Datenschutzniveau einzuhalten, welches durch das BDSG und durch die EU DS-GVO abgebildet wird.

Zweckbindung als Lösung

Trotzdem stehen IT-Sicherheit und Datenschutz aber auch in einem Zielkonflikt: Zum Zwecke der IT-Sicherheit ergriffene Schutzmaßnahmen bringen es in vielen Fällen mit sich, dass auch personenbezogene Daten verarbeitet werden. Ein zentrales Beispiel in diesem Zusammenhang ist die durch das IT-SiG von 2015 getroffene Regelung des § 100 TKG, die es Telekommunikationsdiensteanbietern ermöglicht, die Bestandsdaten und die Verkehrsdaten der Teilnehmer und Nutzer zu erheben und zu verwenden, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. Diese gesetzlich eingeräumte Befugnis zur Verarbeitung von personenbezogenen Daten wurde im Gesetzgebungsverfahren auch als „kleine Vorratsdatenspeicherung" kritisiert, da hier im Vergleich zur klassischen Vorratsdatenspeicherung zu Zwecken der Gefahrenabwehr und der Strafverfolgung ebenso die Verkehrsdaten durch die Anbieter entsprechender Dienste zu speichern sind (siehe §§ 113a, 113b TKG). Um dem tatsächlich bestehenden Risiko vorzubeugen, dass es unter dem Deckmantel der IT-Sicherheit zu einer Aufweichung der Grenzen zulässiger Datenverarbeitungsvorgänge kommt, ist die Verarbeitung personenbezogener Daten für Cybersecurity-Maßnahmen einer strengen Zweckbindung zu unterwerfen. Dies wird durch § 8b Abs. 7 BSIG gesetzlich herausgestellt: Soweit im Rahmen des Meldeverfahrens der Kritischen Infrastrukturen personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ist eine darüber hinausgehende Verarbeitung und Nutzung zu anderen Zwecken unzulässig. Im Übrigen gelten die Vorschriften des BDSG.

Bedarf für spezielle Datenschutzregelungen im Bereich der IT-Sicherheit

Nicht berücksichtigt hingegen hat der Gesetzgeber des IT-SiG die rechtspolitischen Forderungen nach einer ausdrücklichen Normierung weiterer datenschutzrechtlicher Vorgaben bei der Datenverarbeitung zu Zwecken der IT-Sicherheit. Insbesondere finden sich keine konkretisierten Anforderungen im Hinblick auf die Datensparsamkeit, die vor allem auch durch Anonymisierung, Pseudonymisierung, Löschen und Abschotten zu gewährleisten ist. Ähnliche datenschutzrechtliche Defizite in den geltenden gesetzlichen Vorschriften zur IT-Sicherheit werden auch in der europäischen NIS-RL von 2016 deutlich: Hier findet sich in Art. 2 lediglich ein allgemeiner Verweis auf die EU-Datenschutzrichtlinie 95/46/EG, die ab dem 25. Mai 2018 durch die EU DS-GVO ersetzt wird. Wünschenswert ist hier die Schaffung von Spezialregelungen für die Verarbeitung personenbezogener Daten zu Zwecken der IT-Sicherheit, um den hierin liegenden Besonderheiten und Herausforderungen angemessen Rechnung zu tragen.

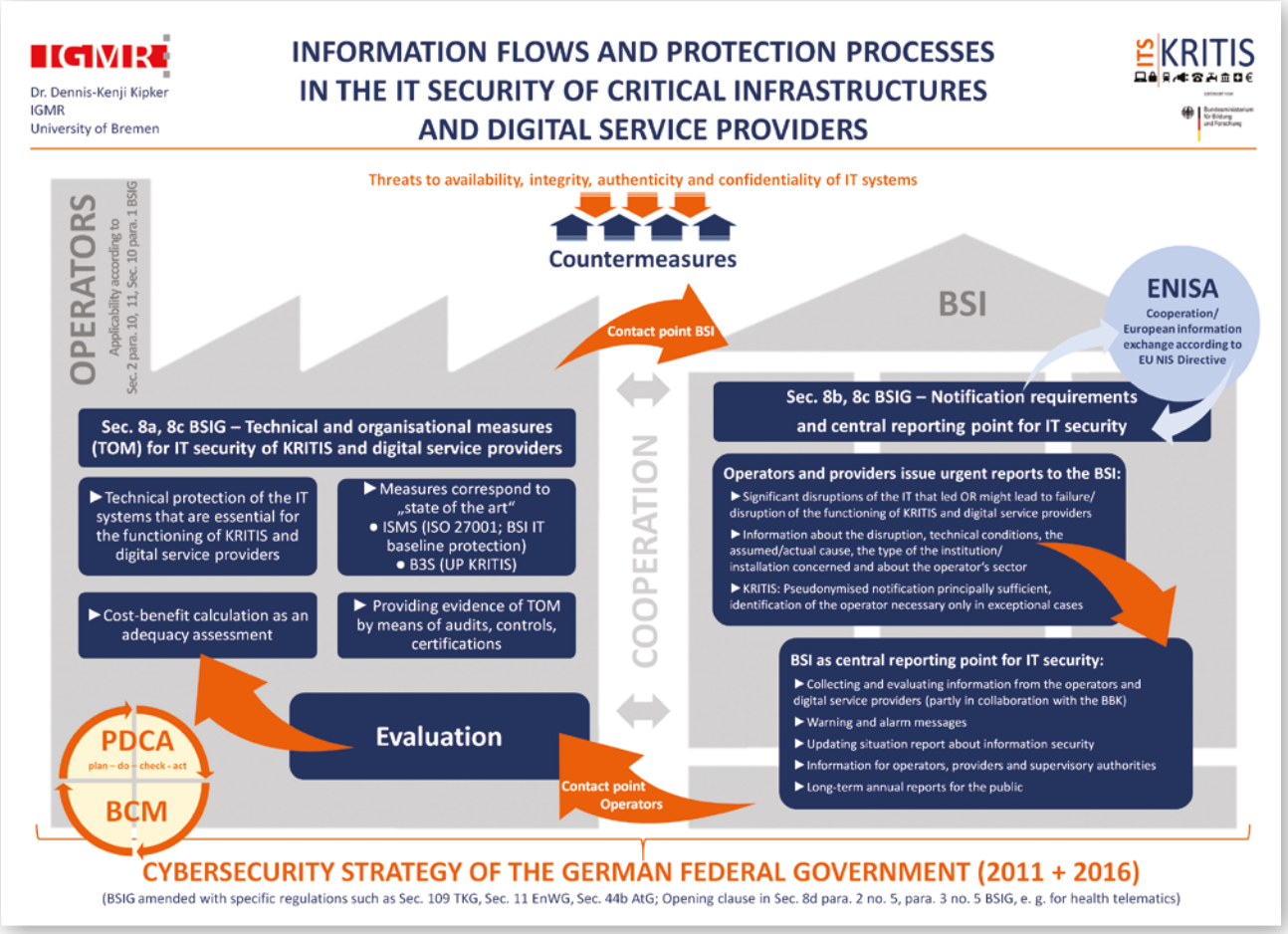


Abb. 1: Gesetzlich geregelte Informationsflüsse im Bereich der IT-Sicherheit Kritischer Infrastrukturen sowie von Anbietern digitaler Dienste

Sektion 4
Der Transfer in die Praxis

In dieser Sektion werden die entwickelten Werkzeuge und Maßnahmen beschrieben.

Aus der Arbeit der Forschungsprojekte im Förderschwerpunkt „IT-Sicherheit für Kritische Infrastrukturen“ ITS|KRITIS entstanden vielfältige Werkzeuge und Maßnahmen für die Praxis. In dieser Sektion 4 werden diese vorgestellt und beschrieben. Eine beispielhafte Referenzimplementierung wird in der folgenden Sektion 5 erläutert.

Review:

Dennis-Kenji Kipker, Sven Müller

Sektion 4
Inhaltsverzeichnis

Aqua-IT-Lab	Ressourceneffiziente Evolution der IT-Sicherheit im Wassersektor	82
Cyber-Safe	Cyber-Safe: Ausblick	84
INDI	Werkzeuge und Veröffentlichungen	85
ITS.APT	Muster-Betriebs-/Dienstvereinbarung zur Implementierung der ITS.APT-Lösung	86
ITS.APT	Muster-Verfahrensverzeichnis	87
MoSaIK	Weiterverwendbare Ergebnisse	89
PortSec	Transfer in die Praxis – Sicherheitsregeln und automatisierte Prüfungen	91
PREVENT	Methodik von PREVENT	92
RiskViz	Informationsfluss nach der Datenerhebung einer internetweiten Suche	94
SecMaaS	Cloudservices für das Informationssicherheitsmanagement	96
SICIA	Das SICIA-Verfahren: Messung & Bewertung der IT-Sicherheit – mit oder ohne ISMS	98
VeSiKi	Fallstudien – Lösungen verständlich und strukturiert präsentieren	100
VeSiKi	Bedarf an Werkzeugen und Verfahren für die IT-Sicherheit	103
VeSiKi	Praxishilfe in der Umsetzung von Informationssicherheit durch den IT-Security-Navigator	105
VeSiKi	IT-Security-Awareness für Fachpersonal mit dem IT-Security-Matchplay „Operation Digitale Schlange“	107
VeSiKi	Einblicke in die Vielfalt von Verwertungsmaßnahmen des Förderschwerpunkts ITS|KRITIS	109
SIDATE & VeSiKi	Juristische Bewertung eines Social-Engineering-Abwehr-Trainings	112

Ressourceneffiziente Evolution der IT-Sicherheit im Wassersektor

Christof Thim

Forschungsprojekt:
Aqua-IT-Lab

Iterative Erhöhung der IT-Sicherheit bei kleinen und mittleren Wasserversorgern

Das Spannungsfeld zwischen den Zielen Kosteneffizienz und Versorgungssicherheit führt bei kleinen und mittleren Versorgern dazu, dass sie mit stark begrenzten finanziellen und personellen Mitteln die IT-Sicherheit aufrechterhalten müssen. Die oben vorgestellten Beiträge des Projektes Aqua-IT-Lab können in einem Entwicklungsprozess angewandt werden und die IT-Sicherheit sukzessiv erhöhen. Dem Vorgehen liegt der Gedanke eines kontinuierlichen Verbesserungsprozesses zugrunde, welcher aus den Schritten Selbstbewertung, Analyse sowie Maßnahmenauswahl und -umsetzung besteht.

Selbstbewertung

Der IT-Sicherheitsschnelltest (Self-Assessment) ist nicht nur für die einmalige Bewertung des Standes der IT-Sicherheit und deren Systematisierung ausgelegt. Vielmehr bietet die periodische Wiederholung der Bewertung dem IT-Verantwortlichen die Möglichkeit, den Reifegrad zu überwachen und weiterzuentwickeln. Eine jährliche Selbstbewertung ist damit der Ausgangspunkt für die Reflektion und Planung der nächsten Maßnahmen. Hierdurch setzt ein Lernprozess ein, welcher den IT-Betrieb sukzessiv systematisiert und in die Nähe der Anforderungen aus dem Branchenstandard und der ISO2700x rückt.

Zudem wird die Selbstbewertung als Managementwerkzeug der Verbands- oder Geschäftsführung genutzt, um die IT-Aufgaben zu steuern und zu priorisieren. Die Schwerpunktsetzung in den Bewertungsdimensionen lässt das Budget priorisiert verteilen.

Der Schnelltest erzeugt weiterhin Vorschläge für Maßnahmen, welche im nächsten Schritt umgesetzt werden sollen. Die voreingestellte Priorisierung sorgt dafür, dass sich die Gesamtreife des Versorgers schnell erhöhen kann.

Sowohl bei der Bewertung als auch bei der Priorisierung kann der IT-Verantwortliche eng mit Dienstleistern und Beratern zusammenarbeiten und zusätzliches Wissen zur Erhöhung der IT-Sicherheit kombinieren.

Analyse

Der Selbstbewertung folgt eine tiefergehende Analyse, welche zur Konkretisierung der Handlungsempfehlungen führt. Sie bezieht sich primär auf technische Maßnahmen. Zunächst werden in einer auf den Wasserversorgungsprozess angepassten Business-Impact-Analyse die kritischen Elemente identifiziert. Davon ausgehend können entweder organisatorische Maßnahmen wie z.B. das Vorhalten zusätzlicher Ressourcen zur Behebung des Notfalls, z. B. Fallback-Komponenten, oder zusätzliches Personal zur zeitweisen manuellen Steuerung der Versorgung konkretisiert werden. Oder es werden konkrete

> IT-Sicherheitsschnelltest zur Selbstbewertung und Ableitung von Handlungsempfehlungen auf dem Weg zur Implementierung eines ISMS

Angriffsvektoren untersucht, welche die Versorgung gefährden. Hierfür kann das Testlabor genutzt werden. Es werden dabei sowohl die konkreten Auswirkungen eines erfolgreichen Angriffs simuliert als auch technische Maßnahmen miteinander verglichen. Unterschiedliche Architekturen oder Code-Revisionen im Labor werden hierbei einem standardisierten Angriffsmuster unterzogen.

Maßnahmenauswahl

Sowohl aus dem Schnelltest als auch aus der tiefergreifenden Analyse ergibt sich eine Reihe von Maßnahmen. Es werden häufig nicht alle umgesetzt, daher ist es notwendig, systematisch einzelne Maßnahmen auszuwählen. Eine Zielstellung ist dabei die schnelle Erhöhung des Sicherheitsniveaus mithilfe des Schnelltests. Hierbei wird auf Maßnahmen zurückgegriffen, welche den Reifegrad des Versorgers in kurzer Zeit erhöhen. Es wird keiner ISMS-Systematik gefolgt, sondern nur die schwächsten Punkte des IT-Sicherheitskonzeptes werden sukzessiv abgearbeitet. Die zweite Zielstellung besteht in der Einführung eines ISMS. Hierfür sind Schritte notwendig, welche dem Versorger nicht ad hoc ein höheres Sicherheitsniveau versprechen, die weitere Entwicklung jedoch

effizienter gestalten. Der Schnelltest stellt beide Varianten der Auswahl zur Verfügung.

Der Versorger muss auswählen, ob er kurzfristig Schwachstellen beseitigen oder mittel- und langfristig ein höheres Maß an Systematisierung in seiner IT erreichen will. Häufig ist die Auswahl eine Frage der verfügbaren Ressourcen. Dem Nutzen der Maßnahmen müssen daher ihre Kosten gegenübergestellt werden. Sie dienen zum einen zur Priorisierung, zum anderen führt eine Wirtschaftlichkeitsbetrachtung gegenüber der Verbands- und Geschäftsführung zu einer klareren Argumentation. Aus dem Projekt wurde ein Bewertungsvorgehen entwickelt, welches dem IT-Verantwortlichen eine schnelle Kalkulationsmöglichkeit bietet und somit die IT-Sicherheitsaufwände argumentativ untermauert.

Maßnahmenumsetzung

Den Abschluss des Verbesserungszyklus bildet die Umsetzung der Maßnahmen. Diese können technischer, organisatorischer oder personaler Natur sein. Viele technische Maßnahmen lassen sich aus den vorangegangenen Detailanalysen ableiten. So kann die weitere Segmentierung des Netzes oder die Überarbeitung der SPS-Codebasis eine technische Folge sein. Entsprechende Umsetzungshinweise können durch die Überprüfung im Testlabor gewonnen werden.

Weiterhin können auf organisatorischer Ebene verschiedene Best-Practices umgesetzt werden. Diese betreffen z. B. den Zugangsschutz, die Auswahl von Lieferanten und Dienstleistern sowie die Lebenszyklen der verwendeten Komponenten. Die organisatorischen Maßnahmen können in weiten Teilen aus dem Schnelltest abgeleitet werden. Hier stehen auch Vorlagen und ausformulierte Best-Practices zur Verfügung.

Die personalen Maßnahmen sorgen dafür, dass die Mitarbeiter zur IT-Sicherheit befähigt werden. Hierzu sind individuelle und organisatorische Entwicklungspläne zu entwerfen. Neben wiederkehrenden Belehrungen zur IT-Nutzung im Rahmen von Betriebsvereinbarungen ist auch die Schulung der Fähigkeit der Mitarbeiter zur Erkennung von IT-Risiken und der Umgang mit Bedrohung zu berücksichtigen. Im Zuge einer Sensibilisierung kann z. B. der Umgang mit E-Mails und externen Speichermedien sowie organisationsfremdem Personal thematisiert werden und somit Schwachstellen, die über Social Engineering ausgenutzt werden können, geschlossen werden.

Auch das eigentliche IT-Personal sollte in Bezug auf IT-Sicherheit eine weitere Qualifikation aufbauen. Hierfür ist die Einrichtung eines eigenen Budgets sinnvoll, welches für Schulungen, Zertifikate oder Trainings mit externen Dienstleistern genutzt werden kann. Insbesondere die Beobachtung eines Penetrationstests im Labor kann dem IT-Personal notwendiges Wissen zur Erkennung, Eindämmung und zum Schutz gegen Angriffe vermitteln.

Wenngleich das Vorgehen im kontinuierlichen Entwicklungsprozess keine vollkommene Neuentwicklung darstellt, ist die Übertragung auf den Wassersektor und das Augenmerk auf Ressourceneffizienz und Machbarkeit für die Professionalisierung der IT-Sicherheit in diesem Bereich hilfreich. Somit wird die Sicherheit der IT-Infrastruktur zur Versorgung nachhaltig geschützt.

Cyber-Safe: Ausblick

Jürgen Krieger, Selcuk Nisancioglu

Forschungsprojekt:
Cyber-Safe

Wie bereits zuvor beschrieben, sind mit Inkrafttreten der ersten Verordnung zur Änderung der BSI-Kritisverordnung [1] Anlagen wie Verkehrssteuerungs- und Leitsystem (Betriebstechnik sowie Telekommunikationsnetze) für das Netz der Bundesautobahnen als kritisch bewertet worden. Im kommunalen Bereich liegt der Schwellenwert bei 500.000 Einwohnern der versorgten Stadt. Vor diesem Hintergrund gewinnen die Ergebnisse des Projektes an weiterer Bedeutung, denn sie sind gleichbedeutend von großer Relevanz für die Betreiber dieser Straßenverkehrsinfrastruktur sowie für die Sicherheit der Verkehrsteilnehmer. Die bisherigen Ergebnisse des Projektes zeigen deutlich, dass die Empfehlung eines Mindestschutzniveaus für Tunnelleitzentralen notwendig ist. Planer, Ausstatter und Betreiber von Tunnelleitzentralen verfügen aktuell nur begrenzt über die notwendigen Kenntnisse, um geeignete Schutzmaßnahmen auch bereits in der Planungsphase zu berücksichtigen und ihnen die notwendige Bedeutung beizumessen. Im Zuge der Experteninterviews und Workshops konnte bereits die nötige Sensibilisierung erreicht werden, und das Interesse der Gesprächspartner lässt den Schluss zu, dass die Handlungshilfen ihren Weg in die tägliche Praxis finden werden. Die aktuelle Gesetzeslage infolge der Änderung der BSI-Kritisverordnung wird aller Wahrscheinlichkeit nach diesen Prozess noch beschleunigen. Der große Vorteil der Handlungshilfen ist, dass sie auf Grundlage der Vorgaben des BSI entwickelt und auf die besonderen Randbedingungen von Leitzentralen angepasst und konkretisiert wurden. Die Handlungshilfen werden mit Abschluss des Forschungsprojekts veröffentlicht und allen interessierten Betreibern, Ausstattern und Planern unentgeltlich zur Verfügung stehen.

Abb.1: Cyber-Safe Handlungshilfe Leitfaden

Quelle

[1] Erste Verordnung zur Änderung der BSI-Kritisverordnung in der Fassung von der Bekanntmachung vom 29. Juni 2017 (BGBl., S. 1921).

Werkzeuge und Veröffentlichungen

Konrad Rieck, Christian Wressnegger, Hartmut König, Andreas Paul,
Franka Schuster, Heiko Kanisch, Christoph Moder

Forschungsprojekt:
INDI

Das Vorhaben leistet einen zentralen Beitrag zum Schutz von Kritischen Infrastrukturen: Nur durch eine effektive Erkennung von Angriffen in Industrienetzen wird es langfristig möglich, gezielte Cyberangriffe und Sabotageversuche abzuwehren. Neben der Untersuchung grundsätzlicher Ansätze zur Anomalieerkennung in Industrienetzen wird durch die Unterstützung typischer Protokolle in der Anlagenautomatisierung sowie der Energieverteilung eine direkte Verwertung der Ergebnisse des Vorhabens in der Praxis möglich. Konkret wurden und werden Werkzeuge und Methoden für den praktischen Einsatz aus folgenden Teilbereichen entwickelt.

Topologieexploration

Es wurde ein Werkzeug entwickelt, das es ermöglicht, aus passiv aufgezeichneten Netzdaten automatisiert die Netztopologie abzuleiten. Vorbereitend wurde hierzu Datenverkehr an ausgewählten Betreiberstandorten aufgezeichnet und hinsichtlich enthaltener Informationen über die Kommunikation im Netz analysiert.

Publikationen:

- „Network Topology Exploration for Industrial Networks“, INISCOM 2016.

Selbstlernende Schwachstellenanalyse

Es wurden Methoden zur Schwachstellenanalyse in Industrienetzen entwickelt. Hierzu wird automatisiert und intelligent in den Implementierungen von bekannten als auch unbekannten Protokollen nach Schwachstellen gesucht. Nachrichtenformate und -sequenzen werden aus aufgezeichnetem Verkehr abgeleitet und anschließend durch Fuzzing zur Erkennung von Verwundbarkeiten eingesetzt.

Publikationen:

- „Pulsar: Stateful Black-Box Fuzzing of Proprietary Network Protocols“, SECURECOMM 2015.
- „Twice the Bits, Twice the Trouble: Vulnerabilities Induced by Migrating to 64-Bit Platforms“, CCS 2016.
- „64-bit Migration Vulnerabilities“, IT 2017.

Protokollspezifische Anomalieerkennung

Ziel der protokollspezifischen Anomalieerkennung ist das Erkennen von Abweichungen gegenüber typischen Protokollabläufen auf Basis der Protokollspezifikationen sowie weiterführend einer Regression auf den übermittelten Messwerten. Die zu diesem Zweck mittels maschinellen Lernens generierten Modelle sollen daran anschließend in für den Betreiber verständliche Regeln überführt werden.

Publikationen:

- “Potentials of Using One-class SVM for Detecting Protocol-Specific Anomalies in Industrial Networks”, CICS 2015.

Protokollunabhängige Anomalieerkennung

Um Angriffe in unbekannten Protokollen zu identifizieren, wurde eine protokollunabhängige Anomalieerkennung entwickelt. Hierzu werden die relevanten Nachrichtenfelder und Protokollzustände automatisch in der Kommunikation von unbekannten Protokollen identifiziert und in diesen anomale Muster aufgespürt.

Publikationen:

- „Harry: A Tool for Measuring String Similarity“, JMLR 2016.
- „ZOE: Content-based Anomaly Detection for Industrial Control Systems“, DSN 2018.

Muster-Betriebs-/Dienstvereinbarung zur Implementierung der ITS.APT-Lösung

Tim Hey, Robert Ortner

Forschungsprojekt:
ITS.APT

Zweck der Betriebs-/Dienstvereinbarung

Das Verbundprojekt ITS.APT stellt ein Muster einer Betriebs-/Dienstvereinbarung als Werkzeug für den Transfer in die Praxis bereit. Mithilfe einer solchen Vereinbarung kann eine rechtliche Grundlage geschaffen werden, um das IT-Sicherheitsbewusstsein der Beschäftigten testen zu dürfen. Sie ist ein Instrument der betrieblichen Mitbestimmung und enthält Bestimmungen mit unmittelbarer Auswirkung auf das Arbeitsverhältnis. Geschlossen wird sie zwischen dem Arbeitgeber und der jeweiligen Mitarbeitervertretung, die dementsprechend früh in die Ausarbeitung miteinbezogen werden sollte.

Im Rahmen der Testdurchführung kommt der Vereinbarung sowohl in arbeitsrechtlicher Hinsicht als auch in datenschutzrechtlicher Hinsicht Bedeutung zu.

In arbeitsrechtlicher Hinsicht dient sie dazu, die Rechte der Mitarbeitervertretung zu wahren. Diese hat diverse Informations- und Mitbestimmungsrechte. Beispielsweise ist sie im Rahmen ihrer Informationsrechte über die einzelnen Projektphasen umfassend zu unterrichten. Die Unterrichtung muss nicht zwingend schriftlich erfolgen. Um die Mitbestimmungsrechte zu wahren, würde ebenfalls eine formlose Absprache ausreichen. Allerdings ist eine schriftliche Fixierung der Absprachen in Form einer Betriebs-/Dienstvereinbarung rechtssicherer.

Gleichzeitig dient die Vereinbarung als datenschutzrechtliche Erlaubnisnorm. Um das Allgemeine Persönlichkeitsrecht der Beschäftigten zu wahren, stellt das BDSG/die DSGVO bzw. die entsprechende landesrechtliche Regelung hohe Anforderungen an den Umgang mit personenbezogenen Daten von Arbeitnehmern. Die Betriebs-/Dienstvereinbarung kann eine Erlaubnisnorm im Sinne dieser Vorschriften für den Umgang mit den Daten der Beschäftigten darstellen. Inhaltlich ist es jedoch nicht möglich von zwingendem Gesetzesrecht und grundgesetzlichen Wertungen abzuweichen. Daher kann auch das Datenschutzniveau durch die Betriebs-/Dienstvereinbarung nicht unter das gesetzlich bestimmte Schutzniveau gesenkt werden.

Inhaltliche Anforderungen an die Betriebs-/Dienstvereinbarung

Die Betriebs-/Dienstvereinbarung sollte inhaltlich klar formuliert sein und alle wesentlichen Phasen der Testdurchführung erfassen. Neben dem Test an sich muss daher auch eine eventuelle Schulung sowie die Datenerhebung und deren Auswertung geregelt werden. Folgende Punkte sind dabei schwerpunktmäßig zu beachten:

Zunächst sind die Bewertungskriterien ausdrücklich zu benennen, anhand derer bestimmt werden soll, ob das Verhalten der Testperson für einen potenziellen Angreifer förderlich oder hinderlich wäre.

Des Weiteren empfiehlt es sich, allgemeine Grundsätze der Datenverarbeitung sowie des Persönlichkeitsschutzes aufzustellen. In dem Zusammenhang ist darauf einzugehen, welche Daten erhoben bzw. nicht erhoben werden. Insbesondere sollte darauf hingewiesen werden, dass die Gestaltung des Testszenarios keine Rückschlüsse auf private Belange oder Interessen der Testpersonen zulässt und die Ergebnisse der Tests nicht zur Leistungs- oder Verhaltenskontrolle genutzt werden. Das BDSG sieht zudem vor, dass personenbezogene Daten nicht anlasslos erhoben und verarbeitet werden dürfen. Dementsprechend ist der Zweck der Datenverarbeitung anzugeben, der vorliegend in der Durchführung der Tests liegt.

Im Weiteren sollte möglichst detailliert geregelt werden, welche Daten auf welche Art und Weise erfasst werden. Beispielsweise ist anzugeben, welche konkreten Informationen, wie Name oder Alter des Getesteten, erhoben werden und ob diese Daten kumuliert werden. Zudem muss geregelt werden, ob und unter welchen Umständen die Daten pseudonymisiert oder anonymisiert werden. Außerdem ist in der Vereinbarung festzulegen, durch wen die Daten verarbeitet werden, welche technischen Sicherheitsvorkehrungen getroffen werden und wie lange die Daten gespeichert werden. Schließlich ist auf die Rechte der Betroffenen, der Mitarbeitervertretung sowie des Datenschutzbeauftragten einzugehen.

Um alle Anforderungen zu erfüllen, stellt der Verbundpartner ITS.APT ein Muster einer Betriebs-/Dienstvereinbarung als Orientierungshilfe für die Umsetzung der ITS.APT-Lösung in der Praxis zur Verfügung.

Muster-Verfahrensverzeichnis

Felix Bieker

Forschungsprojekt:
ITS.APT

Das Verbundprojekt ITS.APT stellt ein Muster für ein Verfahrensverzeichnis als Werkzeug für den Transfer in die Praxis bereit. Ein solches ist gemäß § 7 Landesdatenschutzgesetz Schleswig-Holstein für jedes von einer verantwortlichen Stelle betriebene automatische Verfahren erforderlich. Weiterhin sieht Artikel 30 der im Mai 2018 in Kraft tretenden EU-Datenschutz-Grundverordnung, die in Deutschland unmittelbar anwendbar sein wird, ein solches Verzeichnis von Verarbeitungstätigkeiten vor.

Zweck des Muster-Verfahrensverzeichnisses

Die Verpflichtung, ein solches Verfahrensverzeichnis zu führen, trifft sämtliche verantwortlichen Stellen, die Daten verarbeiten. Es ist von der verantwortlichen Stelle selbst zu erstellen und dient der Herstellung von Transparenz gegenüber den Betroffenen sowie zur besseren Überwachbarkeit der Datenverarbeitung, auch durch die zuständige Datenschutzaufsichtsbehörde. Da das Verzeichnis auch der Information der Betroffenen dient, sollte es möglichst zugänglich und verständlich formuliert sein.

Weiterhin ist das Verzeichnis eine wichtige Grundlage für eine Datenschutz-Folgenabschätzung gemäß Artikel 35 Datenschutz-Grundverordnung, die für Verarbeitungstätigkeiten, die ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben, verpflichtend durchzuführen ist.

Auch für die Durchführung eines Tests des IT-Sicherheitsbewusstseins unterstützt sie die verantwortliche Stelle bei deren Durchführung, da durch ein solches Verzeichnis sichergestellt wird, dass die Datenflüsse und Verantwortlichkeiten innerhalb der Organisation festgelegt, Ansprechpartner verfügbar und die datenschutzrechtlichen Anforderungen umgesetzt sind.

Gemäß § 7 Abs. 3 Landesdatenschutzgesetz Schleswig-Holstein führt der Datenschutzbeauftrage, soweit ein solcher bestellt ist, das Verzeichnis. Dies ist in der Datenschutz-Grundverordnung nicht explizit vorgesehen, aufgrund der beratenden Tätigkeit des Datenschutzbeauftragten sollte dieser aber in jedem Falle frühzeitig in die Erstellung einbezogen werden.

Inhaltliche Anforderungen an das Verfahrensverzeichnis

Das Verfahrensverzeichnis enthält folgende Angaben:

- den Namen und die Kontaktdaten der verantwortlichen Stelle sowie des Datenschutzbeauftragten, soweit ein solcher bestellt ist;
- eine Beschreibung der Zwecke und Rechtsgrundlagen der Datenverarbeitung. Dabei sollten der Sinn der Durchführung des Tests und der Ablauf beschrieben werden. Als Rechtsgrundlage sollte auf eine Betriebs-/Dienstvereinbarung zurückgegriffen werden, auf die an dieser Stelle verwiesen werden kann;
- den Kreis der Betroffenen oder Betroffenengruppen. Dabei handelt es sich um die vorausgewählten Teilnehmer/-innen des Tests, wie sie bereits in der Dienstvereinbarung festgelegt sind. Es sollten die ungefähre Anzahl der Betroffenen sowie die einzelnen Bereiche/Dezernate/Abteilungen benannt werden;
- die Kategorien personenbezogener Daten. Dabei ist zwischen den einzelnen Phasen des Tests, wie etwa dem Versand der Phishing-Mails, den Schulungen und der späteren Evaluation zu unterscheiden. Es sollte zudem vermerkt werden, wenn besondere Kategorien von Daten im Sinne von Artikel 9 Datenschutz-Grundverordnung verarbeitet werden;
- die Löschungs- und Aufbewahrungsfristen. Diese ergeben sich aus der Dienstvereinbarung. Die Daten sollten spätestens nach Abschluss der Tests und Evaluation gelöscht werden;
- die Empfänger von Daten, sowohl innerhalb der verantwortlichen Stelle, als auch außerhalb. Dabei sollten die Datenflüsse genau dargestellt werden und die Verantwortlichkeiten klar definiert sein;
- die Empfänger von Daten in einem Drittland oder eine internationale Organisation, soweit eine solche Übertragung vorgesehen ist. Dieses wird in den meisten Fällen nicht notwendig sein und sollte daher, mit Rücksicht auf die Risiken eines solchen Transfers, nicht umgesetzt werden;

- eine Beschreibung der technischen und organisatorischen Maßnahmen, um die Sicherheit der Verarbeitung gemäß Artikel 32 Datenschutz-Grundverordnung sicherzustellen. Dabei empfiehlt sich eine Aufgliederung der einzelnen Maßnahmen nach den Schutzzielen des Standard-Datenschutz-Modells der Aufsichtsbehörden von Bund und Ländern. Danach sind die Maßnahmen zu unterteilen nach Verfügbarkeit (Wie wird gewährleistet, dass Verfahren und Daten zeitgerecht zur Verfügung stehen?), Vertraulichkeit (Wie wird gewährleistet, dass nur befugte Personen auf Daten und Verfahren zugreifen?), Integrität (Wie wird gewährleistet, dass Daten unversehrt, vollständig, zurechenbar und aktuell bleiben?), Transparenz (Wie wird gewährleistet, dass die automatisierte Verarbeitung von Daten mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden kann), Intervenierbarkeit (Wie kann die Daten verarbeitende Stelle nachweisen, dass sie den Betrieb ihrer informationstechnischen Systeme steuernd beherrscht und dass Betroffene die ihnen zustehenden Rechte ausüben können?) und Nicht-Verkettbarkeit (Wie wird sichergestellt, dass Daten nur zu dem ausgewiesenen Zweck automatisiert erhoben, verarbeitet und genutzt werden). Dabei ist auch zu beurteilen, ob das Schutzniveau angemessen ist und insbesondere die Risiken berücksichtigt, die mit der Verarbeitung verbunden sind, wie etwa durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

Weiterverwendbare Ergebnisse

Patrick Leibbrand, Holger Maczkowsky, Kristian Beilke,
Alexander Nieding

Forschungsprojekt:
MoSaIK

MoSaIK – Transfer in die Praxis

Bereits während der Durchführung des Forschungsvorhabens erfolgte ein kontinuierlicher Praxisbezug durch Erhebung und Verarbeitung von Echtdaten der Anwendungspartner. Diese wurden aus laufenden Produktivsystemen bezogen, spezielle Testsysteme kamen nicht zum Einsatz. Die Messdaten beeinflussten und präzisierten schließlich die Ergebnisse des parallel entwickelten Modellierungswerkzeugs, wodurch die zugrunde liegenden Modelle gleichfalls einen direkten Bezug zum Wirkbetrieb Kritischer Infrastrukturen erlangten.

Beitrag der Anwendungspartner

Wesentliche Arbeiten im Lauf des Verbundprojekts erfolgten unmittelbar in der produktiv genutzten Kritischen Infrastruktur der Anwendungspartner. Dies betraf insbesondere die Sensorplatzierung und die Messdatenakquise zur Kenngrößengewinnung. Hierdurch ergab sich praktisch zwangsläufig maximale Praxisrelevanz der akquirierten Daten und der damit optimierten Modelle.

Anwendungspartner Stadt Gera

Die Zentrale Leitstelle verfügt als definitionsgemäß ständig besetzte Stelle über fünf identisch ausgestattete Disponentenarbeitsplätze. Umfangreiche Leitstellentechnik und eine komplexe Telekommunikationsanlage konzentrieren die Kritische IT-Infrastruktur auf einen vergleichsweise kleinen Bereich, der des besonderen Schutzes beispielsweise gegenüber Angriffen aus dem Internet bedarf. Durch Abbildung des Internetzugangs über den Webbrowser durch Einschleifung hochgradig gesicherter Security-Appliances-Web können fundierte Daten über den Angriffsdruck aus dem offenen Internet auf eine der „Achillesfersen" der Kritischen Infrastruktur zur Laufzeit gesammelt werden.

Anwendungspartner Stadtwerk Haßfurt GmbH

Die Stadtwerk Haßfurt GmbH liefert als kommunaler Versorger Strom, Erdgas und Trinkwasser für die Bürger der Stadt Haßfurt und ihrer Stadtteile. Das Versorgungsgebiet ist mit rund 17.000 Haushalten deutlich kleiner als der Zuständigkeitsbereich der Zentralen Leitstelle der Stadt Gera. Jedoch sind die Komponenten der Kritischen Infrastruktur in diesem Fall über die gesamte Fläche verteilt und nicht allein in der Leitstelle konzentriert.

Bedingt durch die weitverzweigte IT-Infrastruktur und die darüber möglichen, vielfältigen Einflussmöglichkeiten auf Infrastrukturen der Sektoren Energie sowie Informationstechnik und Telekommunikation liegt in diesem Fall ein potenziell attraktives Ziel für Angreifer vor. Auch in diesem Fall wurde der Internetzugang durch Einschleifung der Security Appliance Web gesichert und zugleich detaillierte Daten zu Angriffsdruck, Angriffsvektoren und -mechanismen gesammelt.

Beiträge des Entwicklungspartners und des Forschungspartners

Entwicklungspartner im Verbundprojekt MoSaIK die m-privacy GmbH mit Sitz in Berlin. Das Unternehmen entwickelt vornehmlich IT-Sicherheitsprodukte zum Schutz Kritischer Infrastrukturen vor Angriffen aus dem Internet, die innovative Präventivansätze verfolgen und daher ohne konventionelle Filtertechniken oder statistische Verfahren auskommen.

Die wissenschaftlich fundierten Eigenentwicklungen folgen fortlaufend den neuesten, praxisgetriebenen Erkenntnissen der IT-Sicherheitsforschung.

Bereits zu Projektbeginn konnten zahlreiche Erkenntnisse an die Anwendungspartner zurückgespiegelt werden, die sich gut verallgemeinern ließen. Die der Strukturanalyse initial folgende, manuelle Risikoanalyse wurde einerseits nach den bewährten Vorgehensweisen des Bundesamts für Sicherheit in der Informationstechnik (BSI) durchgeführt (Anwendungspartner: Stadt Gera). Andererseits erfolgte eine Risikoanalyse nach dem grundlegend anderen Ansatz der Attack Tree Analysis, die im Gegensatz zu den BSI-Grundschutz-Katalogen die Sichtweise des Angreifers repräsentiert und die sicherheitstechnische Gesamtsicht auf die zu schützende Kritische Infrastruktur um einen entscheidenden, jedoch seltener eingenommenen Blickwinkel erweitert (Anwendungspartner: Stadtwerk Haßfurt GmbH). Hier wurde deutlich, dass insbesondere die Verbindung einer Kritischen Infrastruktur zum Internet per se einen erheblichen Angriffsvektor darstellt.

An dieser Stelle wurde die Ausleitung aussagekräftiger Messdaten über die Security Appliance Web vorgenommen. Unter Sicherheitsaspekten trennt das System die Kritische Infrastruktur vom Internet in einer Art und Weise, die Angriffe über den Browser unabhängig vom Modus Operandi nach menschlichem Ermessen ausschließt. Bereits zu diesem Zeitpunkt zeigte sich ein hoher Praxisnutzen nicht nur unter Forschungsaspekten, sondern insbesondere mit Blick auf den laufenden Produktivbetrieb der Anwendungspartner.

Die Auswertung der gewonnenen Sensordaten erfolgte hernach unter anderem mit einem speziell optimierten Software-Werkzeug unter den Vorgaben der Modellierung des Forschungspartners Fraunhofer AISEC. Die resultierende Bewertung des Sicherheitsniveaus der betrachteten Kritischen Infrastrukturen der beiden Anwendungspartner wurde über geeignete Schnittstellen in das ursprüngliche Modell rückgekoppelt, um dieses anhand der Praxisdaten kontinuierlich zu verfeinern.

Perspektivisch ist denkbar, eine akkumulierte, praxisgestützte Gesamtkompetenz in der Beurteilung des Sicherheitsniveaus Kritischer Infrastrukturen in Abhängigkeit von bestimmten Betriebsparametern in Form eines universellen Werkzeugs an Betreiber Kritischer Infrastrukturen zurückfließen zu lassen.

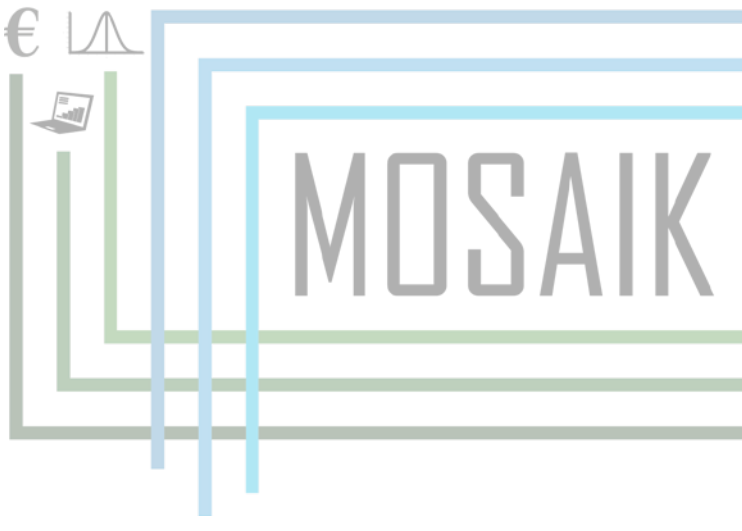
Risikoanalysemethode

Die im Verbundprojekt entwickelten Werkzeuge für die effiziente Risikoanalyse und Bewertung des Sicherheitsniveaus Kritischer Infrastrukturen basieren auf einer Risikoanalysemethode, welche die Aktualität und Qualität der Bewertung des Sicherheitsniveaus im Vergleich zum derzeitigen Stand deutlich verbessert.

Ein wesentliches Ziel bei der Entwicklung der Methode war die Flexibilität zur Anwendung auf unterschiedliche Untersuchungsgegenstände in verschiedensten Umgebungen. Der Aufwand für die Risikobeurteilung sollte an heterogene Anforderungen anpassbar sein und sich nach der Höhe der identifizierten Risiken richten. Die Risikoanalysemethode musste daher die Möglichkeit bieten, den Aufwand für gering priorisierte Bedrohungen und Schutzziele niedriger als für hoch priorisierte zu gestalten.

Die Zusammenarbeit mehrerer Analysten sowie sich ändernde Bedrohungen erforderten. nachvollziehbare und reproduzierbare Ergebnisse Diese wurden durch eine Trennung zwischen der Struktur der Methode und den Anleitungen zu den einzelnen Arbeitsschritten erreicht. Die grundsätzlichen Aktivitäten und zugehörigen Ergebnisse bildeten den Kern der Risikoanalyse, der über verschiedene Projekte gleich blieb. Die Anleitungen erhielten explizite Informationen, wie die einzelnen Schritte auszuführen waren und wie Entscheidungen protokolliert werden. Diese konnten auf spezielle Untersuchungsgegenstände angepasst werden. Schließlich wurde durch das Bereitstellen von Katalogen von Bedrohungen, Maßnahmen und Bewertungskriterien eine Grundlage für die Vergleichbarkeit unterschiedlicher Analysen gegeben.

Die Methode besteht aus vier Aktivitäten (Untersuchungsgegenstand erfassen, Schutzbedarfsfeststellung, Bedrohungsanalyse und Risikobewertung). Die zwei wesentlichen Ergebnisse sind die Beschreibung des Untersuchungsgegenstandes und die Risikobewertung. Jede der Aktivitäten wird mit den benötigten Eingangsarbeitsprodukten, den erzeugten Arbeitsprodukten und den zugehörigen Aufgaben beschrieben. Die Aufgaben beschreiben nicht das „Wie“, sondern „was“ erreicht werden soll. Anwender können für das „Wie“ entsprechende Anleitungen wählen, die systematische Abläufe für den gegebenen Kontext enthalten. Die Arbeitsergebnisse entstehen durch das Ausführen der Aufgaben. Schließlich enthalten die Anleitungen auch Richtlinien, Vorlagen und Kataloge, welche den Aktivitäten und Arbeitsergebnissen zugeordnet sind.



Transfer in die Praxis – Sicherheitsregeln und automatisierte Prüfungen

Nils Meyer-Larsen, Rainer Müller, Karsten Sohr, Annabelle Vöge

Forschungsprojekt:
PortSec

Erstellung des Gefährdungskataloges

Für die Erstellung eines branchenspezifischen. Gefährdungskataloges wird in PortSec eine Methodik entwickelt, die folgende Schritte umfasst: (i) Literaturrecherche in der wissenschaftlichen Literatur und Veröffentlichungen aus dem Bereich Maritime Logistik bezüglich bisheriger Cyberangriffe auf Hafentelematiksysteme und der entsprechenden Vorgehensweise der Täter, (ii) Geschäftsprozess-Analyse von Hafentelematiksystemen, (iii) Brainstorming-Workshops bezüglich möglicher Risikoszenarien, (iv) Analyse der System- und Netzstrukturen von Hafentelematiksystemen und (v) Analyse der Verwundbarkeiten der unterschiedlichen Software-Komponenten von Hafentelematiksystemen, u. a. Analyse und Dokumentation von Systemkomponenten, Schnittstellen sowie Schutz-, Authentifizierungs- und Verschlüsselungsmechanismen.

Entwicklung eines Analyse-Werkzeuges für die Systemarchitektur

Das Technologie-Zentrum Informatik und Informationstechnik (TZI) der Universität Bremen verfügt über umfassendes Know-how bei der automatisierten Prüfung von Software auf mögliche Schwachstellen. „Es wäre sehr zeitaufwändig und teuer, jede Zeile eines Programms einzeln durchzusehen und von einem Analysten prüfen zu lassen“, erklärt Dr. Karsten Sohr, der am TZI das Thema Informationssicherheit koordiniert. „Wir entwickeln daher Systeme, die den Bauplan der Software untersuchen und dort vor allem die Kommunikationsschnittstellen nach außen aufzeigen. Diese Zugänge müssen ausreichend gesichert sein.“ Im Bereich der Hafentelematik wird jedoch nicht nur der Programmcode auf diese Weise durchleuchtet, sondern auch die Netzinfrastruktur mit berücksichtigt, sodass die Software-Analyse mit der Sicherheit des Rechnernetzes verbunden wird. Durch beide Schritte erhält ein Sicherheitsauditor also ein Gesamtbild von der aktuell implementierten IT-Sicherheitsarchitektur des Hafentelematiksystems, sodass eine umfassende Einschätzung der IT-Risiken möglich wird.

Schwachstellen auf Knopfdruck finden

Im Rahmen von PortSec wird ein Werkzeug entwickelt, das aus dem Programmcode mithilfe statischer und dynamischer Programmanalysen Teile der Sicherheitsarchitektur z. B. in Form von Datenflussdiagrammen extrahiert. Diese extrahierte Software-Architektur kann dann um Informationen über die Netzinfrastruktur angereichert werden, in der das Hafentelematiksystem betrieben wird. Hierdurch erhält man eine Gesamtsystemarchitektur, die gegen Sicherheitsregeln, die sich in einer Wissensdatenbank befinden, geprüft wird. Typische Sicherheitsregeln betreffen die (rollenbasierte) Zugriffskontrolle. Diese umfasst beispielsweise die Bedingung, dass eine Zollfreigabe ausschließlich durch den Zoll erfolgen darf. Weiterhin ist die Mandantenfähigkeit sicherzustellen, bei der jeder Teilnehmer der Hafentelematik eben nur auf seine Daten und nicht auf die eines anderen Beteiligten zugreifen darf. Auch Fragen der Kopplung von Authentisierungsinformationen mit Autorisierungsentscheidungen sind hier von Bedeutung. Weitere Sicherheitsregeln betreffen die geeignete Verschlüsselung der Kommunikation der einzelnen Partner der Hafentelematik untereinander.

Die Ergebnisse der automatischen Untersuchung werden anschließend von Experten begutachtet, um aufgeworfene Fragen zu klären und Handlungsempfehlungen abzuleiten. Übernommen wird diese Rolle von der datenschutz cert GmbH, einer Prüf- und Zertifizierungsgesellschaft mit Fokus auf Datenschutz und IT-Sicherheit. „Wir haben bereits andere Projekte erfolgreich mit dem TZI durchgeführt und daraus neue Dienstleistungen entwickelt, die vom Markt nachgefragt werden“, berichtet Jan Schirrmacher. Akuten Handlungsbedarf bei Häfen sieht er aufgrund des IT-Sicherheitsgesetzes, das die Bundesregierung verabschiedet hat. Betreiber von sogenannten „Kritischen Infrastrukturen“ müssen in Zukunft sicherstellen, dass sie nach dem aktuellen Stand der Technik geschützt sind. Die datenschutz cert GmbH will die Ergebnisse des PortSec-Projekts nutzen, um entsprechende Zertifizierungen für Hafentelematiksysteme anzubieten.

Methodik von PREVENT

Torsten Bollen

Forschungsprojekt:
PREVENT

Es wird der Ansatz verfolgt, Verhaltensregeln und Risikomanagement mit Echtzeitmessungen, Sicherheitstests und Simulationen von Bedrohungsszenarien zu verbinden. Die Kombination dieser unterschiedlichen Instrumente in einer neuartigen Software garantiert eine verbesserte Absicherung von Rechenzentren. Hierbei zeigt sich u. a., dass „Big-Data"-Analyse ein geeigneter Weg sein kann, unterschiedliche Bedrohungsszenarien gezielt zu verhindern.

Durch geplante Simulationen werden neue Ansätze zur Beurteilung des Sicherheitsniveaus verfolgt. Des Weiteren wird basierend auf den erarbeiteten Ansätzen die Sicherheit der bestehenden IT-Sicherheitslösung für kritische Bankeninfrastruktur weiter verbessert.

In Ermangelung eines generischen Bankenmodells wird im Rahmen von PREVENT exemplarisch für verschiedene Kommunikationsebenen innerhalb eines Bankenrechenzentrums ein Modell erstellt und bestehende Standards werden erweitert. Dieses Vorgehen ermöglicht es, abstrakte Informationen über das Modell in verwertbare Daten zu transferieren, die als Eingabewerte für einen SW-gestützten Demonstrator dienen.

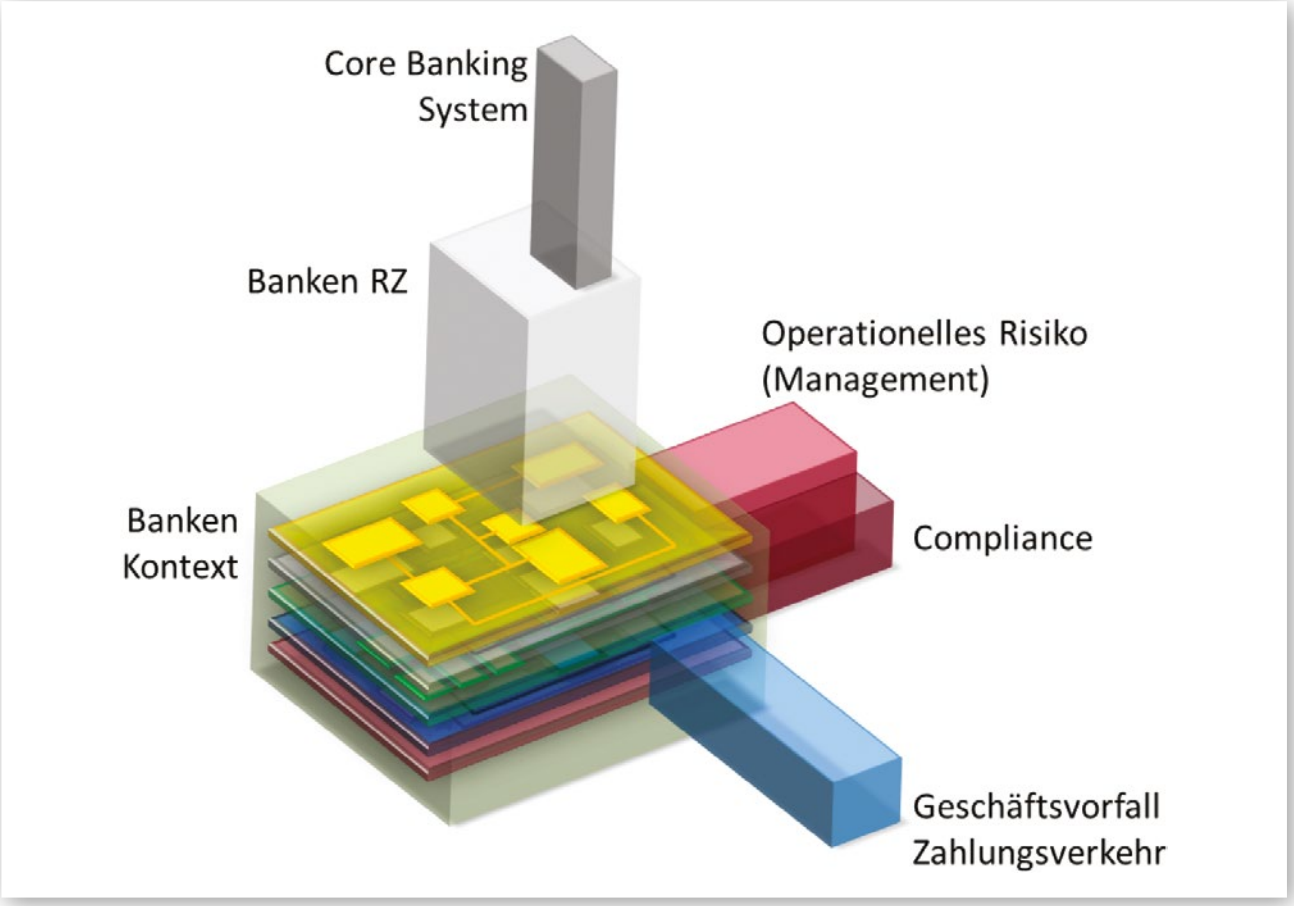


Abb. 1: Modell Business-Prozess (allgemein)

Dieses stark vereinfachte Bild veranschaulicht die an die Banken-IT gestellten Anforderungen zur Abbildung der Geschäftsprozesse. Zur Realisierung der an das PREVENT-Framework gestellten Anforderungen sind weitere Komponenten, Verfahren und Tools erforderlich.

Den prinzipiellen Aufbau von PREVENT zeigt die Abbildung 2.

Gut zu erkennen ist, dass in PREVENT-Simulationen (z. B. aus dem RACOAT) Monitoring-Daten, Businessprozess-Modelle und Compliance-Anforderungen in einem Tool ausgewertet werden. Das sich hieraus ergebende Gesamtbild wird in verschiedenen Ansichten aggregiert, um die Nutzer (z. B. Administratoren, Compliance Officer, Management) bestmöglich bei ihren Entscheidungen zu unterstützen.

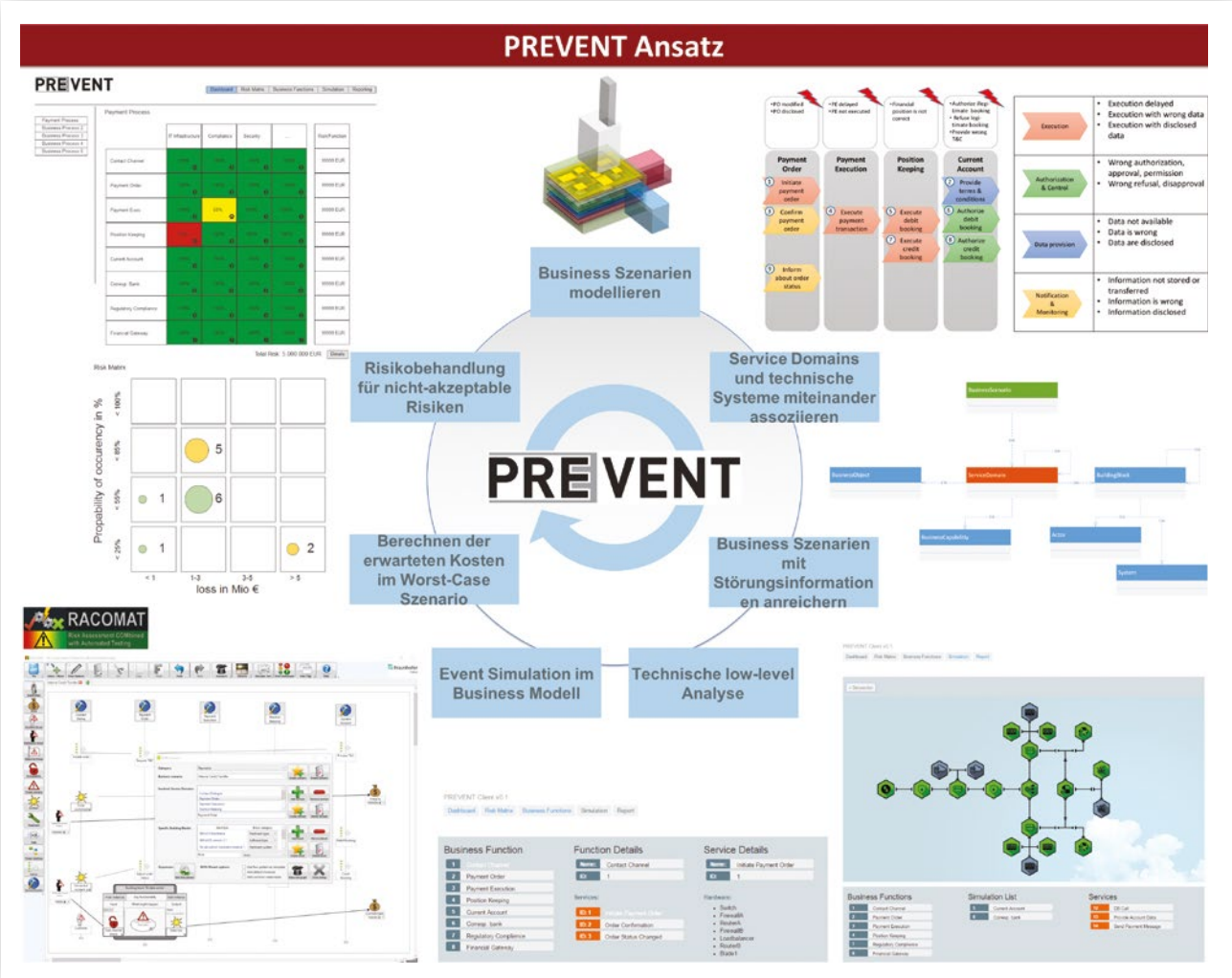


Abb. 2: PREVENT-Lösungsansatz

Informationsfluss nach der Datenerhebung einer internetweiten Suche

Jan-Ole Malchow, Constance Baban

Forschungsprojekt:
RiskViz

Datenerhebung der Äußeren Suche

Das Verbundprojekt stellt eine verteilte Suchmaschine als Werkzeug für den Transfer in die Praxis bereit. Mithilfe der Suchmaschine ist es möglich, das Internet nach industriellen Kontrollsystemen (ICS) und anderen IT-Systemen zu durchsuchen. Die Besonderheit ist, dass nicht nur IP-Adressen als Suchbegriffe in die Suchmaschine eingegeben werden können, sondern auch geografische Gebiete, die mithilfe eines Frontends freihändig selektiert oder durch die Eingabe von Postleitzahlen ausgewählt werden können.

Die erhobenen Daten werden anschließend weiterverarbeitet. Für eine sinnvolle Anwendung wird ein Nutzermanagement implementiert, um hierdurch automatisierte Risiko-Lagebilder und deren Auswertung den richtigen Verantwortlichen bereitstellen zu können. Des Weiteren werden Data-Science-Modelle für Versicherungen entwickelt beziehungsweise die passenden Schnittstellen dafür bereitgestellt.

Informationsflussmodelle

Im Rahmen von RiskViz wurden mehrere Informationsflussmodelle entwickelt, die gewährleisten sollen, dass die durch die Suchmaschine gewonnenen Erkenntnisse über Verwundbarkeiten zügig und rechtskonform an die Betreiber verwundbarer Systeme und/oder zuständige öffentliche Institutionen weitergeleitet werden oder von diesen selbst direkt über einen konkreten Suchauftrag in Erfahrung gebracht werden können. Für diese Entwicklung wurde der Dialog mit potenziellen Anwendern gesucht, um zu ermitteln, welche Interessen und Nutzungsmöglichkeiten dahingehend bestehen, wie nach Auffassung der Bedarfsträger ein sinnvoller, das heißt nützlicher, Informationsfluss der aufgedeckten Verwundbarkeiten auszugestalten wäre.

Als Ausgangspunkt wurden daher für die Identifikation von möglichen Informationsflussstrategien und -wegen zwei Workshops mit interessierten Endanwendern durchgeführt, um gemeinsam mit dem RiskViz-Konsortium den Umgang mit den zu ermittelnden Daten über Verwundbarkeiten (d. h. Verbleib, Verwendung sowie Distribution) von ICS zu ermitteln. Die Workshops mit Verbands- und Unternehmensvertretern im März 2016 und mit Vertretern von Behörden und Organisationen mit Sicherheitsaufgaben (BOS) im Mai 2016 ermöglichten es, erste Nutzungsmöglichkeiten für Bedarfsträger zu konkretisieren. Im Rahmen der beiden Workshops wurden folgende Fragen diskutiert:

- **Machbarkeit und Bedürfnisse:** Welche Daten werden gesammelt und welche Informationen werden zurückgesendet? Welche Daten können/sollten nicht gesammelt und weitergegeben werden?
- Wie können Prozesse der **Gestaltung des Informationsflusses** aussehen? Welche externen Akteure sollten eingebunden werden?
- **Datenerhebung:** Wer beauftragt die Scans? Wer führt die Scans durch?
- **Datenzugriff:** Wer darf die Daten einsehen? Besteht Interesse an anonymisierten bzw. aggregierten Daten?
- Welche **Informationsflussstrategie** ist für die im RiskViz-Projekt ermittelten Informationen von Verwundbarkeiten in KRITIS-ICS wünschenswert und sinnvoll?

Final wurden innerhalb von RiskViz drei Informationsflussmodelle identifiziert:

Informationsflussmodell		Staatsmodell	Unternehmensmodell	Forschungsmodell
ROLLEN		AKTEURE		
1	Technische Durchführung	Staat	Unternehmen	Universität
		Dienstleister		
2	Frontend	Staat	Unternehmen	Forscher an der Universität
			(Versicherung)	
			(Verband)	
3	Auftraggeber	Staat	Unternehmen	Forscher an der Universität
		Unternehmen	(Versicherung)	
		Forschung	(Verband)	
			Eigentümer oder Nicht-Eigentümer der IP-Adressen	
4	Dritte	Unternehmen	BSI (bei KRITIS)	CERT-Verbund
		Forschung	Forschung	DFN CERT
		Verbände	Verbände	Öffentlichkeit
		CERTs	Öffentlichkeit	
		Öffentlichkeit		

Tabelle 1: Informationsflussmodell, Rollen und Akteure; Quelle: BIGS

Da durch die RiskViz-Suchmaschine möglicherweise sensible Daten erhoben werden, mussten für diese drei Informationsflussmodelle zunächst die mit den jeweiligen Modellen verbundenen Rollen und Akteure geklärt werden, um dann in einem weiteren Schritt die mit den erhobenen Daten allgemein einhergehenden rechtlichen Fragen zum Datenumgang sowie final die hiermit verbundenen Fragen modellspezifisch zu skizzieren.

Diese Informationsflussmodelle umfassen jeweils die vier Rollen (technische Durchführung, Frontend, Auftraggeber, Dritte), die in den Modellen jeweils von unterschiedlichen Akteuren – zum Teil mit Überschneidungen – realisiert werden können. Die Modelle umfassen zudem jeweils das Maximum an technisch Möglichem sowie das Minimum an technisch Verfügbarem in Bezug auf die erhobenen Daten, um einen optimalen Ablauf des Scanprozesses und der Datendistribution zu ermöglichen sowie darüber hinaus die damit einhergehenden rechtlichen Fragen zu Datenumgang und -verwertung.

Cloudservices für das Informationssicherheits-management

Daniel Augustin, Markus Hoffmann

Forschungsprojekt:
SecMaaS

SecMaaS
SECURITY MANAGEMENT AS A SERVICE

SecMaaS legt den Fokus auf Bürgerämter und bindet deren Sachbearbeiter sowie IT-Administratoren und Informationssicherheitsbeauftragte in alle Phasen des Projekts ein.

Von der Forschung bis zur Umsetzung

Zunächst bildeten qualifizierte Interviews durch die Experten der Hochschule Darmstadt in den Behörden die Grundlage der zu erarbeitenden Projektziele. Dann wurden die aus Beobachtungen gewonnenen Erkenntnisse und daraus abgeleiteten Vorgehensmodelle mit den Anwendern diskutiert. Schließlich ermöglicht ein agiler Entwicklungsprozess bei der technischen Umsetzung die Bereitstellung von Teillösungen in kurzen zeitlichen Abständen, die hinsichtlich ihrer Nutzbarkeit und Akzeptanz evaluiert werden.

Diese praxisnahe und anwenderorientierte Vorgehensweise innerhalb des Forschungsprojekts bietet einen geeigneten Leitfaden für die Erweiterung der Plattform auf andere Kritische Infrastrukturen.

Grundlage Forschung

Die durchgeführten Interviews und die dabei gemachten Beobachtungen lieferten als Ergebnis, dass sich die Sicherheitsziele der Behörden in vielen Teilen stark ähneln. Gleiches gilt für mögliche Maßnahmen zur Umsetzung der Sicherheitsziele. Aus diesem Umstand entstand der Gedanke, das IT-Sicherheitskonzept generisch und zentral zu erstellen. Diese Herangehensweise erlaubt die qualifizierte und effiziente Erstellung des IT-Sicherheitskonzeptes. Es hat sich gezeigt, dass bei seiner Erarbeitung viel Vorwissen vorhanden sein muss, um ein qualifiziertes Konzept zu erstellen. In vielen Behörden übernimmt ein Mitarbeiter neben seiner normalen Tätigkeit zusätzlich auch die Aufgaben des Informationssicherheitsbeauftragten. Dadurch ist der Umfang der von ihr/ihm durchgeführten Aufgaben stark begrenzt. Die Erstellung und Umsetzung eines qualifizierten IT-Sicherheitskonzepts kommt dabei meistens zu kurz oder absorbiert einen Großteil der Arbeitskraft. Durch den Einsatz eines Informationssicherheitsmanagement-Tools werden viele Aufgaben durch den Service abgenommen. Die dadurch gewonnene Zeit des Informationssicherheitsbeauftragten kann dazu genutzt werden, um das Konzept umzusetzen und im laufenden Betrieb aufrechtzuerhalten.

Entwicklung eines Cloudservices für das Informationssicherheitsmangement

Um das zentrale, generische Sicherheitskonzept für verschiedene Behörden nutzbar zu machen, wird ein cloudbasierter Service entwickelt. Der Service stellt für verschiedene Ausprägungen von Behörden vorkonfigurierte Sicherheitskonzepte zur Verfügung. Diese können dann durch die Benutzer des Dienstes an die speziellen Gegebenheiten der Behörde adaptiert werden. Nach dem Festlegen der Grundkonfiguration werden die daraus resultierenden Maßnahmen angepasst und den Benutzern des Services angezeigt.

Jede Maßnahme hat konkrete Anweisungen zur Umsetzung. Dieses Vorgehen soll den Anwender auch ohne spezielle Kenntnisse in die Lage versetzen, die anstehenden Maßnahmen qualifiziert umzusetzen. Dies garantiert die Aufrechterhaltung des zugrundeliegenden Konzepts.

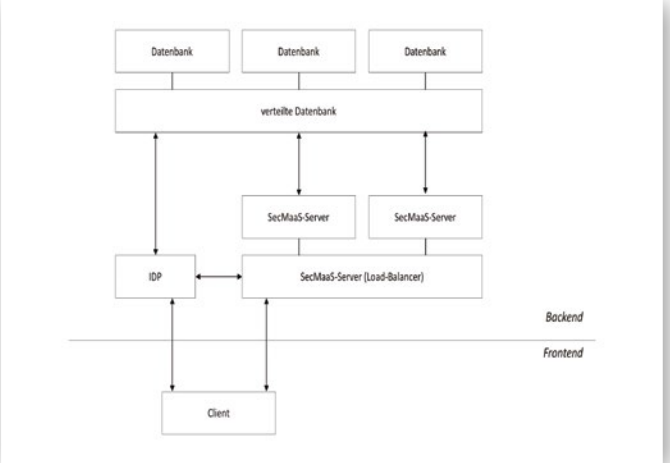


Abb. 1: Systemarchitektur des Services

Der Service besteht aus einem Frontend, welches zum Konfigurieren des Systems und Informieren der Benutzer genutzt wird. Ein weiterer Bestandteil des Dienstes ist ein Backend-Server mit angebundener Datenbank und Identitäts-Provider. Der Backend-Server beinhaltet die Geschäftslogik und kümmert sich um den Informationsaustausch zwischen dem Frontend und der Datenbank. Durch den ID-Provider können verschiedene Authentifizierungsmechanismen eingesetzt werden. In der aktuellen Planung soll zur Authentifizierung die Verwendung von FIDO-Sticks sowie individuellen Zugangsdaten (Username/Passwort-Kombination) umgesetzt werden. Durch den Einsatz eines modularen IdP können aber noch sehr viel mehr Methoden zum Einsatz kommen - angedacht ist die spätere Unterstützung der Online-Ausweisfunktion des Personalausweises. Die Datenbank dient der Datenspeicherung und ist, nach dem aktuellen Stand der Technik, in eine sichere Zone verschoben worden.

Zusätzlich gibt es noch einen Administrationsbereich, in dem die vorkonfigurierten Ausprägungen erstellt werden können. Dieser Bereich kann nicht nur dazu genutzt werden, um bestehende Konfigurationen zu optimieren, sondern ermöglicht auch die Ausweitung des Services von Behörden auf weitere Anwendungsfälle, wie z. B. KMUs oder kleine Energieversorger.

Das SICIA-Verfahren: Messung & Bewertung der IT-Sicherheit – mit oder ohne ISMS

Franka Schuster, Stefan Mehner

Forschungsprojekt:
SICIA

Der wachsenden Bedrohung Kritischer Infrastrukturen ist mit der Einführung des IT-Sicherheitsgesetzes [1] Rechnung getragen worden. Die im Gesetz enthaltene Pflicht zum Nachweis der aktuellen IT-Sicherheit alle zwei Jahre (mindestens) in Form von Sicherheitsaudits, Prüfungen oder Zertifizierungen sowie der IT-Sicherheitskatalog der Bundesnetzagentur [2] zwingen Betreiber zukünftig zur regelmäßigen Messung und Darlegung ihres aktuellen IT-Schutzes. Die dafür notwendige Implementierung eines angemessenen Sicherheitsprozesses, wie eines Informationssicherheitsmanagementsystems (ISMS), stellt Betreiber von Erzeugungsanlagen und Netzen vor eine große Herausforderung, denn es gilt, zahlreiche Anforderungen bei der Implementierung zu erfüllen, ohne dass konkrete Methoden zur Umsetzung verfügbar sind. Daher werden genau solche Methoden und Werkzeuge benötigt, die Betreiber kleiner und großer Anlagen gleichermaßen darin unterstützen, solch einen angemessenen Sicherheitsprozess zu implementieren und mit dessen Hilfe die gesetzliche Nachweispflicht zu erfüllen.

Methoden und Werkzeuge für die vier Hauptschritte von ISMS

Im Verbundprojekt SICIA werden dazu Methoden und Werkzeuge entwickelt, die Betreiber unterstützen, ein für sie passendes ISMS zu implementieren. Dazu werden für aufwendige Schritte, die im Rahmen eines kontinuierlichen Sicherheitsprozesses regelmäßig durchgeführt werden müssen, unterstützende Methoden sowie Software-Werkzeuge zu deren Automatisierung entwickelt. Zu diesen Schritten gehören gemäß der Norm DIN ISO/IEC 27000 [3]:

1. Identifikation von Informationswerten mit relevanten Sicherheitsanforderungen
2. Bestimmung von Informationssicherheitsrisiken
3. Auswahl und Umsetzung geeigneter Maßnahmen, um unakzeptable Risiken zu handhaben
4. Überwachung, Pflege und Verbesserung der Wirksamkeit verfügbarer Maßnahmen.

Die im Projekt SICIA entwickelten Methoden und Werkzeuge sind jedoch auch unabhängig von der Existenz eines ISMS einsetzbar. Sie bauen schrittweise aufeinander auf und bilden zusammen ein Verfahren zur systematischen Messung und Bewertung der IT-Sicherheit in kritischen Netzen jeder Größe. Die vier grundlegenden Schritte zur praktischen Durchführung des SICIA-Verfahrens mit den dazugehörigen Aktivitäten sind in Abbildung 1 dargestellt.

Im ersten Schritt werden die initialen Informationen

Abb. 1: Die vier Schritte des SICIA-Verfahrens

zur Infrastruktur zusammen mit dem Betreiber erhoben, die zur Vorbereitung der in Schritt 2 genutzten Methoden notwendig sind. Mithilfe von Netzplänen und Komponentenlisten werden Netzzugangspunkte für das Mitschneiden von Netzverkehr identifiziert und Skripte für die Analyse relevanter Komponenten in der Infrastruktur vorbereitet. Im zweiten Schritt werden die entwickelten automatischen und manuellen Methoden zur Erfassung sicherheitskritischer Parameter in der Infrastruktur angewendet. Die erfassten Informationen werden im Nachhinein im dritten Schritt mithilfe der Referenzimplementierung „offline" zusammengeführt, analysiert und aufbereitet. Im letzten Schritt wird das Ergebnis der Sicherheitsbewertung, die IT-Sicherheit der Anlage, mithilfe grafischer Mittel dem Betreiber zugleich differenziert und kompakt präsentiert. Neben der Veranschaulichung der Ergebnisse werden anhand der konkreten Mess- und Bewertungsergebnisse eine direkte und automatische Ableitung von Verbesserungsmaßnahmen und eine Simulation und der Vergleich verschiedener potentzieller Maßnahmenkombinationen möglich und durch die Referenzimplementierung softwarebasiert unterstützt. Zudem können die im Zuge der Bewertung ermittelten Sicherheitsindikatoren in bestehende Verfahren des Betreibers zur Risikoanalyse integriert werden.

Die Durchführung der Schritte 2 bis 4 des SICIA-Verfahrens wird durch Software unterstützt. Sie stellt Algorithmen bereit, um die zu den Teilschritten gehörenden Aktivitäten zu automatisieren und die Fülle sicherheitsrelevanter Informationen zusammenzutragen, zu verwalten und aufzubereiten. Dazu zählen die nicht-intrusive netz- und/oder hostbasierte Messung von Komponenten- und Netzkonfigurationen, die automatische Bewertung dieser Messung anhand IT-Sicherheitskriterien und Verwundbarkeitsdatenbanken sowie die interaktive Darstellung der IT-Sicherheit in Form von „Landkarten" auf Komponenten-, System- und Standortebene sowie die Simulation von Verbesserungsmaßnahmen mit ihrem potentziellen Effekt auf die IT-Sicherheit dieser Infrastrukturebenen. Das Verfahren ist unmittelbar anwendbar auf kritische Netze beliebiger Größe.

Quellen

[1] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), Bundesgesetzblatt 2015 Teil I Nr. 31, 24.07.2015.

[2] IT-Sicherheitskatalog gemäß §11 Absatz 1a Energiewirtschaftsgesetz, Stand 8/2015.

[3] DIN ISO/IEC 27000: Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Überblick und Terminologie.

Fallstudien – Lösungen verständlich und strukturiert präsentieren

Sebastian Dännart

Forschungsprojekt:
VeSiKi

Geschichten erzählen – Methode „Fallstudie“

Gerade in den komplexen Strukturen der IT-Sicherheit, in denen neben der Technik und den organisatorischen Rahmenbedingungen immer auch der Mensch eine elementare Rolle spielt, lassen sich Zusammenhänge oft nur unscharf erkennen und noch schwieriger darstellen.

Die Wissenschaft kennt für diese Aufgabe eine Methode: die Fallstudie. Sie ermöglicht es, komplexe, schwer abgrenzbare Phänomene in ihrem natürlichen Kontext erforschen zu können. Es gelingt so, auf qualitativer Basis, meist auf Grundlage von Experteninterviews und Beobachtungen, strukturierte Berichte zu erstellen, die gleichzeitig beliebig tiefe Detailgrade und gute Lesbarkeit ermöglichen.

Mithilfe einer Fallstudie können so komplexe Lösungen strukturiert aufbereitet und einem breiten Publikum zur Verfügung gestellt werden. Dabei dient die Fallstudie im Sinne von Good oder Best Practices als Beispiel für andere Unternehmen, darüber hinaus kann sie auch zur Demons- tration und Problemanalyse in der Lehre genutzt werden.

Die Methode Fallstudie bietet also sowohl eine Möglichkeit, Wissen aus der Praxis zu gewinnen, als auch des Transfers von Wissen in die Praxis hinein.

Spezielle Anpassung für ITS|KRITIS

Für den Förderschwerpunkt ITS|KRITIS sollen diese Möglichkeiten genutzt werden, indem Projektergebnisse und bereits in der Nutzung befindliche IT-Sicherheitskonzepte in ihrer vorgesehenen Umgebung dargestellt werden und so einen Blick auf Good und Best Practices erlauben sowie eine Plattform zum Transfer vorhandenen Wissens über die IT-Sicherheit für Kritische Infrastrukturen in die Praxis zu ermöglichen.

Da es sich hierbei um einen kollaborativen Forschungsansatz zwischen den Betreibern Kritischer Infrastrukturen oder Technologiepartnern und dem durchführenden Forscher handelt, entwickelte das Begleitforschungsprojekt VeSiKi Vorgehensweisen und Vorlagen zur Erstellung der Fallstudien. Darüber hinaus ermöglichen einheitliche Templates für die Struktur der einzelnen Fallstudien eine Vergleichbarkeit und eine fallstudien- und sektorübergreifende Analyse. Je nach Schwerpunkt werden Vorlagen für eine unternehmensbezogene und eine projektbezogene Fallstudie zur Verfügung gestellt. Dabei fokussiert die unternehmensbezogene Fallstudie auf das IT-Sicherheitskonzept eines Unternehmens oder einzelne Teilbereiche der Umsetzung. Demgegenüber beschäftigt sich die projektbezogene Fallstudie immer mit einem konkreten Projekt mit IT-Sicherheitsbezug, welches bereits erfolgreich umgesetzt wurde.

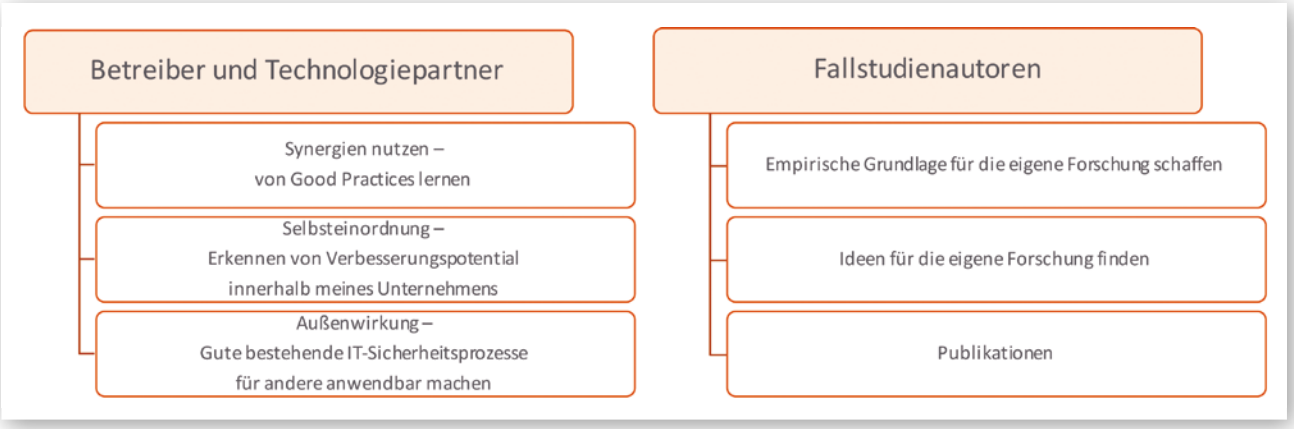


Abb. 1: Nutzen aus der Erstellung einer Fallstudie für die Beteiligten

Unternehmensbezogene Fallstudie	Projektbezogene Fallstudie
1. Unternehmen 1.1 Unternehmensprofil 1.2 Strategische Ausrichtung 1.3 Ansprechpartner im Unternehmen **2. Kritische Infrastruktur** 2.1 Einordnung als KRITIS 2.2 Risikoanalyse **3. IT-Sicherheit** 3.1 IT-Infrastruktur 3.1.1 Geschäftssicht 3.1.2 Prozesssicht 3.1.3 Anwendungssicht 3.1.4 Technische Sicht 3.2 Normen, Standards und Gesetze 3.3 Stand der IT-Sicherheit	**1. Unternehmen** 1.1 Unternehmensprofil 1.2 Strategische Ausrichtung 1.3 Ansprechpartner im Unternehmen 1.4 IT-Sicherheit im Unternehmen **2. Kritische Infrastruktur** 2.1 Einordnung als KRITIS 2.2 Risikoanalyse **3. Projekt** 3.1 Beschreibung 3.1.1 Projektstart 3.2 Projektziel 3.3 Geschäftssicht 3.4 Prozesssicht 3.5 Anwendungssicht 3.6 Technische Sicht 3.7 Umfang und Zeitraum 3.8 Vorgehen und Umsetzung 3.9 Projektergebnis **4. Erfolgsfaktoren**

Tabelle 1: Struktureller Vorschlag für Fallstudien

Beide Strukturen haben gemein, dass zum einen eine grundlegende Beschreibung und Einordnung der KRITIS stattfindet und des Weiteren vier verschiedene Sichten auf das Unternehmen oder das Projekt modelliert und beschrieben werden.

- **Geschäftssicht**
  Beteiligte Geschäftspartner und ihre Rollen, Geschäftskonzepte, Verträge, strategische und operative Ziele
- **Prozesssicht**
  Detaillierungen zu den Geschäftsprozessen, Prozessübergänge zwischen den Beteiligten, Bewertung der Prozessqualität
- **Anwendungssicht**
  Übersicht über die beteiligten Informationssysteme, Verteilung der Funktionen, Lokalisierung der Datenhaltung, Integrationsebenen
- **Technische Sicht**
  Beteiligte Systemkomponenten, Netzwerke, Datenübertragung

Mögliche Transferleistungen

Das Ergebnis einer Fallstudie kann nun verschiedener Art sein. Es kann zum Beispiel lediglich die Umsetzung eines Konzeptes oder einer technischen Anwendung dargestellt werden, darüber hinaus ist es denkbar, strategische Ausrichtungen eines Unternehmens bezüglich des Schutzes von Informationen zu analysieren oder die komplexen Compliance-Auflagen einer Organisation zu beschreiben. Das Ziel und der Fokus einer Fallstudie sind höchst individuell und frei gestaltbar.

In vergangenen Fallstudien haben wir unter anderem die mitarbeiterzentrierte IT-Sicherheitsphilosophie eines familiengeführten Lebensmittelproduzenten untersucht und dabei festgestellt, dass Traditionsbewusstsein und State-of-the-Art-IT-Sicherheit sich hervorragend ergänzen. Neben innovativen Informationssicherungsmechanismen konnten wir hier ebenfalls zuverlässige Maßnahmen zum Schutz der Produktionsanlagen beobachten und in der Fallstudie darstellen. In einer anderen Fallstudie war es uns möglich, Einblicke in das IT-Sicherheitsmanagement eines Krankenhausverbundes zu bekommen sowie den Druck, den das Aufkommen von Ransomware mit dem Ziel Krankenhaus erzeugt, am praktischen Beispiel zu erleben und unter Berücksichtigung der getroffenen Maßnahmen zu analysieren. Hier verschaffte das negative Beispiel anderer die nötige Argumentationsgrundlage und diente als Treiber für innovatives und konsequentes IT-Sicherheitsmanagement. Gerade in den beiden genannten Beispielen ist Compliance von enorm großer Bedeutung und ist für die IT-Sicherheit Kritischer Infrastrukturen beispielgebend. Vor allem auch zur Unterstützung kleiner und mittlerer Unternehmen können Fallstudien als initiale Ideen zur Umsetzung eigener IT-Sicherheitsprojekte genutzt werden

Veröffentlichung der Fallstudien

Im Sommer 2018 werden die Fallstudien in einem Buch erscheinen [1]. Neben einer Reihe Fallstudien zur IT-Sicherheit Kritischer Infrastrukturen, wird das Buch eine CrossCase-Analyse enthalten, welche Fallstudien-übergreifende Aussagen und Erkenntnisse identifiziert. Darüberhinaus setzen Experten die Ergebnisse in Relation zu ihren Erfahrungen.

Quelle

[1] Lechner, U., Dännart, S., Rieb, A., Rudel, S. (Hrsg.): CASE KRITIS: Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen. Logos-Verlag, 2018.

Bedarf an Werkzeugen und Verfahren für die IT-Sicherheit

Manfred Hofmeier, Tamara Gurschler, Sebastian Dännart

Forschungsprojekt:
VeSiKi

Die Umfrage „Monitor IT-Sicherheit Kritischer Infrastrukturen“ des Projekts VeSiKi will den aktuellen Stand der IT-Sicherheit für Kritische Infrastrukturen vor allem aus der Sicht der Betreiber abbilden. Themen der Umfrage sind die Bedrohungslage, Selbsteinschätzung der Bedrohungslage, Cybersecurity-Fähigkeiten, Stand der IT-Sicherheitsmaßnahmen, Budgets für Sicherheit, Einfluss des IT-Sicherheitsgesetzes auf Kritische Infrastrukturen und Innovationsfähigkeit. Einen Themenschwerpunkt im Monitor stellt der Bedarf Kritischer Infrastrukturen an Konzepten, Verfahren und Technologien der IT-Sicherheit dar.

Für diese Studie wurden vom Juni 2016 bis Oktober 2017 IT-Sicherheitsverantwortliche in Deutschland befragt.

Die Ergebnisse der Umfrage haben gezeigt, dass ein Bedarf an neuen Konzepten, Verfahren und Technologien vorhanden ist. Es wurde mit Fragen der Verbundprojekte des Förderschwerpunkts ITS|KRITIS nach dem Stand bei Kritischen Infrastrukturen und dem Bedarf an neuen IT-Sicherheitsprodukten und Dienstleistungen gefragt (Abbildung 1). Der Bedarf an solchen Technologien ist hoch und viele der Befragten würden solche Technologien kurz- und mittelfristig einsetzen. Die Projekte im Förderschwerpunkt erforschen also Konzepte, Verfahren und Technologien, die bei den Betreibern benötigt werden und auch eingesetzt würden.

Publikationen:

- Lechner, U. (Hrsg.): Monitor IT-Sicherheit Kritischer Infrastrukturen, Neubiberg, Universität der Bundeswehr München, 2017
- Gurschler, T., Dännart, S., Lechner, U.: Monitor IT-Sicherheit Kritischer Infrastrukturen. In: Schartner, P., Baumann, A. (Hrsg.): DACH Security 2017. Tagungsband zur Konferenz 5.-6.9.2017 in München. Syssec: Frechen 2017, S. 170-180.
- Lechner, U. (Hrsg.): Monitor 2.0 IT-Sicherheit Kritischer Infrastrukturen, Neubiberg, Universität der Bundeswehr München, 2018.

Abb. 1: Bedarf an Werkzeugen und Verfahren im Monitor

Praxishilfe in der Umsetzung von Informationssicherheit durch den IT-Security-Navigator

Dennis-Kenji Kipker, Andreas Harner, Sven Müller

Forschungsprojekt:
VeSiKi

Letztlich ist es der Mensch, der IT-Security realisieren muss. Diese Kernidee bildet die Grundlage der Schaffung des IT-Security-Navigators, der im Rahmen des BMBF-Förderschwerpunkts „ITS|KRITIS" am Institut für Informations-, Gesundheits- und Medizinrecht (IGMR) an der Universität Bremen sowie von VDE/DKE in Frankfurt am Main entwickelt wurde.

Die aktuellen Vorgaben zeitgemäßer IT-Sicherheit werden vorwiegend aus technischen Normen und Standards sowie aus gesetzlichen Regelungen abgeleitet, die von technischen und juristischen Experten entworfen werden und durch entsprechende Beratungsunternehmen sowie Inhouse-Consulting-Maßnahmen für das einzelne Unternehmen konkretisiert werden können. Was jedoch, wenn ein Unternehmen weder über eigenen technischen noch juristischen Sachverstand verfügt, gleichwohl aber verpflichtet ist, angemessene IT-Security umzusetzen, sei es aufgrund neuer gesetzlicher Verpflichtungen, wie beispielsweise aus dem IT-Sicherheitsgesetz und der EU NIS-RL, oder aber, um mögliche Haftungsrisiken zu vermeiden, sollten kritische Systeme ausfallen und Dritte geschädigt werden? Im Regelfall sind gerade solche KMUs, die nicht unmittelbar auf fachspezifischen Sachverstand zurückgreifen können, auf sich allein gestellt, wenn es um die Realisierung der neuen Anforderungen an die IT-Sicherheit im Unternehmen geht.

Abhilfe schaffen soll hier der IT-Security-Navigator von VDE/DKE und der Universität Bremen. In interdisziplinärer Zusammenarbeit sind zunächst sämtliche Rechtsvorschriften sowohl im Europa-, Bundes- und Landesrecht, die für die IT-Sicherheit eine Relevanz besitzen, für alle Sektoren Kritischer Infrastrukturen ermittelt worden. Zur Verbesserung der Anwenderfreundlichkeit hat eine geeignete Aufbereitung der Vorschriften, sortiert nach Kategorien und Rechtsetzungsinstanz, daneben aber auch nach Anwenderrelevanz, stattgefunden. Für jede Kategorie von Rechtsvorschriften wurden darüber hinaus einschlägige Publikationen und die Rechtsprechung erfasst. Zur leichteren Anwendbarkeit wurden sämtliche Gesetze online verlinkt, und relevante Einzelparagraphen werden separat nach Relevanz sortiert aufgeführt, sodass ein schneller und gezielter Abruf möglich ist. Diese so geschaffene, mehrere Hundert Gesetze umfassende Sammlung von Rechtsvorschriften erfährt eine laufende Aktualisierung und ist online frei und kostenlos unter der URL www.itsecuritynavigator.de zur Nutzung verfügbar. Die Online-Maske enthält zudem verschiedene Filter, sodass eine einfache Verwendung möglich ist.

Um Juristen und technischen Anwendern nicht nur einen schnellen und einfachen Überblick über die für sie relevanten Gesetze verschaffen zu können, sondern die Gesetze und die in vielen von ihnen enthaltenen unbestimmten Rechtsbegriffe zu konkretisieren, werden in einem zweiten Schritt der wissenschaftlichen Forschung gezielt sämtliche in den Rechtsvorschriften enthaltenen unbestimmten Rechtsbegriffe, wie beispielsweise der „Stand der Technik", ermittelt und katalogisiert. Darauf basierend erfolgt im Anschluss die Konkretisierung der unbestimmten Rechtsbegriffe mit Technikbezug für sämtliche Sektoren Kritischer Infrastrukturen in Zusammenarbeit mit verschiedenen Normungsgremien

> Datenbank bestehend aus den relevanten Rechtsvorschriften und technischen Normen zur IT-Sicherheit

von VDE/DKE. In einer Symbiose aus Recht und Technik werden hier die Schnittstellen zwischen den Normen und Spezifikationen und den entsprechenden unbestimmten Rechtsbegriffen ermittelt, das heißt, es wird für jede Generalklausel in jeder relevanten Rechtsvorschrift geprüft, welche Normen und Spezifikationen zur Ausfüllung selbiger herangezogen werden können. Nach Abschluss dieses Abgleichs ist es möglich, einen Großteil der Rechtsvorschriften und Normen/Spezifikationen aus den bestehenden Datenbanken zusammenzuführen und dem Anwender zugänglich zu machen.

Durch die damit geleistete Forschungsarbeit können sämtliche Rechtsvorschriften zur IT-Sicherheit erstmals nicht nur vollumfassend und einfach systematisiert dargestellt werden, sondern es kann mithilfe der unmittelbar stattfindenden Konkretisierung durch einschlägige technische Normen und Spezifikationen dem Anwender eine sofortige und zuverlässige Erst-Entscheidungshilfe zur Verfügung gestellt werden, wie er für ihn möglicherweise verpflichtende IT-Security-Maßnahmen auf angemessene Weise technisch implementieren kann. Der Na-

vigator wird laufend mit neuen Features ausgestattet, wie beispielsweise zusätzlichen Such- und Filteroptionen, der Anzeige weiterer Informationen zu den Normen und Spezifikationen auf Anforderung des Nutzers und einer grafischen Darstellung der Ergebnisse (beispielsweise zur Aktivität in Gremien/Domänen als Tortendiagramm und als Heat Map; Statistiken zur Zahl der Referenzierungen in Gesetzen und Standards). Da die Praxistauglichkeit der Plattform im Vordergrund steht, erhält auch der Anwender die Möglichkeit zur Mitwirkung, indem er selbst neue Gesetze sowie Normen und Spezifikationen vorschlagen kann, die nach einer Prüfung in die Datenbank implementiert und dort vernetzt werden.

Der IT-Security-Navigator schafft somit die Voraussetzungen für eine Cybersecurity im Dienste des Menschen – und dies nicht nur in der Zielsetzung, sondern bereits in der Implementierung, indem jeder potenzielle Anwender an die Hand genommen und es ihm erleichtert wird, notwendige IT-Sicherheitsmaßnahmen für jetzt wie auch für die Zukunft normenkonform zu ergreifen.

Abb. 1: IT-Security-Navigator – www.itsecuritynavigator.de

IT-Security-Awareness für Fachpersonal mit dem IT-Security-Matchplay “Operation Digitale Schlange“

Andreas Rieb, Ulrike Lechner

Forschungsprojekt:
VeSiKi

„Operation Digitale Schlange“ ist eine IT-Sicherheitsschulung, die als ein Serious Game konzipiert und im Rahmen des Forschungsprojektes „Vernetzte IT-Sicherheit Kritischer Infrastrukturen” (VeSiKi) als Teil der IT-Security-Matchplay-Serie entwickelt und validiert wird. Die IT-Security-Matchplays basieren auf dem Format des Wargamings und integrieren Elemente der IT-Risiko- und IT-Bedrohungsanalyse. Ziel ist es, IT-Sicherheitsverantwortliche und IT-Sicherheitsprofessionals im Umgang mit Advanced Persistent Threats (APTs) zu schulen, wie sie typisch sind für KRITIS.

Neben „Operation Digitale Schlange“ gibt es zwei weitere IT-Security-Matchplays: „Operation Digitale Eule“ sowie „Operation Digitales Chamäleon“, welche jeweils andere IT-Infrastrukturen mit KRITIS-Bezug realisieren. In Summe wurden die IT-Security-Matchplays in drei Ländern mit mehreren hundert Teilnehmern aus den Bereichen CERTs, Landeskriminalämtern, Krankenhäusern, Energiewesen, Logistik und Transport, Finanzwesen und vielen anderen Sektoren und Branchen Kritischer Infrastrukturen erfolgreich gespielt.

Das Spielkonzept

In den IT-Security-Matchplays treten zwei Teams – Rot vs. Blau – gegeneinander an. Auf Basis einer fiktiven IT-Infrastruktur entwickeln die Teams in Spielmissionen Angriffe bzw. Verteidigungsmaßnahmen. Die IT-Infrastruktur wiederum repräsentiert in „Operation Digitale Schlange“ ein Krankenhaus, welches die spezifischen Gegebenheiten wie bspw. smarte Operationssysteme, mobile Endgeräte für die tägliche Visite, veraltete Betriebssysteme u. a. beinhaltet.

„Operation Digitale Schlange“ verwendet konventionelle, nicht-digitale Spielmaterialien. Dazu gehören u. a. ein Spielbrett, auf dem der Netzplan mit IT-Infrastrukturkomponenten abgebildet ist. Mit Karten wird markiert, welches Asset der IT-Infrastruktur angegriffen bzw. verteidigt wird. Auf Post-its werden Ideen zu Angriffsvektoren oder Schutzmaßnahmen notiert. Das Spielmaterial beinhaltet (pro Team) Karten, die die Rollen beschreiben, einen Satz Spielregeln sowie Stifte für Notizen auf dem Spielbrett. Spielleibchen in den Farben Rot, Blau oder Weiß markieren die Teamzugehörigkeit.

Der Spielablauf

Zu Beginn der Spielphase wird die Rahmenlage durch die Spielleitung präsentiert. Team Rot wird vorgegeben, dass der Angriff entsprechend der gewählten Spielerrolle eine Wirkung entfalten muss, die es notwendig macht, das BSI entsprechend den Meldepflichten – so wie sie im IT-Sicherheitsgesetz festgelegt sind – zu informieren.

Die Teams werden im Briefing ermuntert kreativ zu sein. Somit sind der Phantasie im Spiel nur wenig Grenzen gesetzt – es limitieren Spielzeit und Plausibilität.

Team Rot nimmt die Sicht des gewählten Threat Actors ein und soll einen Angriffspfad entwickeln, der für diese Angreiferrolle hinsichtlich Absichten, Ressourcen und Methoden typisch ist. Dieser Angriffspfad besteht aus voneinander abhängigen und ggf. alternativen Angriffsvektoren.

Abb. 1: Team Blau bei der Erarbeitung eines IT-Sicherheitskonzepts

Das blaue Team (siehe Abbildung 1) verfolgt das Ziel, die bevorstehenden Cyberangriffe erfolgreich abzuwehren.

Team Blau entwickelt ein IT-Sicherheitskonzept sowie Schutzmaßnahmen zu den Faktoren Organisation,

Technik und Mensch. Die Regeln des Spiels legen fest, dass die IT-Sicherheitsstrategie von Team Blau jedoch nicht zulasten der Verfügbarkeit und Nutzerfreundlichkeit der IT der KRITIS gehen darf. Die Regeln geben ebenfalls vor, dass die Mitarbeiter (der KRITIS) die Internetanbindung auch für Internetdienste wie Facebook nutzen. Ferner dürfen Netzverbindungen und Fernwartungszugänge nicht aus Gründen der IT-Sicherheit gekappt werden. Solche und andere der Realität entsprechenden Prämissen verhindern, dass Team Blau die „sicherste" Lösung – das dauerhafte Trennen sämtlicher Internetverbindungen – wählt. Team Blau ist so gefordert, kreative Lösungen zu entwickeln, um die Angriffe von Team Rot zu antizipieren und abzuwehren.

Die Siegerermittlung

Für die Bewertung der Spielergebnisse ist es wichtig, den Sieger transparent und nachvollziehbar zu ermitteln. Hier nimmt der Spielleiter (repräsentiert durch Team Weiß) eine zentrale Rolle ein. In „Operation Digitale Schlange" wird der Sieger systematisch und schrittweise ermittelt. Der Spielleiter baut einen Angriffsbaum auf, der auf den Spielergebnissen des roten Teams basiert, und bewertet diesen mittels drei Prüfkriterien: (technische) Machbarkeit (1), Plausibilität (2) und Erfolg im Hinblick auf etwaige entgegenstehende Schutzmaßnahmen, die von Team Blau festgelegt wurden (3). Sofern Team Rot mehrere alternative Angriffsvektoren innerhalb des Angriffspfades entwickelt hat, werden diese ebenfalls bewertet.

So geht der Spielleiter schrittweise durch den Angriffspfad mit den Angriffsvektoren, bis evtl. das Ziel (z. B. Offenlegung der Daten) erreicht ist und der Gewinner ermittelt werden kann.

Das Debriefing

Das im Anschluss stattfindende Debriefing gibt den Teilnehmern die Möglichkeit, ihre persönlichen Erkenntnisse zu reflektieren, und gibt Anregungen, das im Spiel Erfahrene in den Arbeitsalltag zu übernehmen.

Ergebnisse

Basierend auf den Ergebnissen des Debriefings konnten wissenschaftlich verschiedene Effekte mithilfe der IT-Security-Matchplays nachgewiesen werden. So konnte bspw. eine Steigerung der IT-Security-Awareness der Spielteilnehmer hinsichtlich der Kategorien Wissen, Wahrnehmung und Verhalten nachgewiesen werden. Zweitens wurde mit dem IT-Security-Matchplay „Operation Digitales Chamäleon" ein neuer Angriffsvektor identifiziert. Ferner tragen die IT-Security-Matchplays zum psychologischen Verständnis von Tätern im Bereich Cybercrime bei, welches wiederum Grundlage für die Entwicklung wirkungsvoller Präventions- und Schutzmaßnahmen in der Praxis ist.

Publikationen:

- Rieb, A. & Lechner, U., 2016. Operation Digital Chameleon – Towards an Open Cybersecurity Method. In Proceedings of the 12th International Symposium on Open Collaboration (OpenSym 2016). Berlin, S. 1–10.
- Rieb A., Lechner U. (2017) Towards a Cybersecurity Game: Operation Digital Chameleon. In: Havarneanu G., Setola R., Nassopoulos H., Wolthusen S. (eds) Critical Information Infrastructures Security. CRITIS 2016. Lecture Notes in Computer Science, vol 10242. Springer.
- Rieb, A., Hofmann, M., Laux, A., Rudel, S. & Lechner, U., 2017. Wie IT-Security Matchplays als Awarenessmaßnahme die IT-Sicherheit verbessern können. In J. M. Leimeister & W. Brenner, hrsg. Towards Thought Leadership in Digital Transformation: 13. Internationale Tagung Wirtschaftsinformatik. St. Gallen, S. 867–881.
- Rieb, A., Gurschler, T. & Lechner, U., 2017. A Gamified Approach to Explore Techniques of Neutralization of Threat Actors in Cybercrime. In E. Schweighofer u. a., hrsg. GDPR & ePrivacy – APF 2017 - Proceedings of the 5th ENISA Annual Privacy Forum. Wien: Springer International Publishing AG & Österreichische Computer Gesellschaft, S. 111–127.

Einblicke in die Vielfalt von Verwertungsmaßnahmen des Förderschwerpunkts ITS|KRITIS

Albrecht Fritzsche, Matthias Raß, Max Jalowski

Forschungsprojekt:
VeSiKi

Die folgenden Aktivitäten verbinden zwei unterschiedliche Strategien zur Verwertung des Wissens, das im Projekt VeSiKi und dem gesamten Förderschwerpunkt ITS|KRITIS gewonnen wurde. Es handelt sich dabei zum einen um die aktive Vermittlung von Wissen in klar strukturierten Veranstaltungs- und Veröffentlichungsformaten und zum anderen um die weitere Bereitstellung von Wissen an geeigneten Stellen, um es verschiedenen Interessengruppen zu ermöglichen, dieses Wissen nach eigenem Bedarf abzufragen.

Aktive Wissensvermittlung über Vorträge, Workshops und Publikationen

Aktive Wissensvermittlung fand zunächst durch verschiedene Vorträge, Workshops und Publikationen zu IT-Sicherheit in anwendungsorientierten Medien statt. Für die breite Öffentlichkeit wurden zum Beispiel Vorträge und Workshops im offenen Innovationslabor JOSEPHS angeboten, das durch seine Lage in der Nürnberger Innenstadt einfach für alle Bürgerinnen und Bürger zugänglich ist. Themen der Workshops waren IT-Sicherheitsstrategien, Gefahrenwahrnehmung und Live Hacking Events genauso wie Rechtsfragen und Themen der Standardisierung, wie sie im Projekt VeSiKi behandelt wurden. Weitere Workshops wurden für spezielle Zielgruppen angeboten, wie etwa die Wissenschaftler und Praktiker in den einzelnen Projekten des Förderschwerpunkts oder die Sicherheitswirtschaft bei einschlägigen Konferenzen wie der CIPRE in Den Haag. Publikationen in Fachmedien wie dem Mittelstandswiki oder den Auslagen des zugehörigen Fachverlags bei der CeBIT ebenso wie ein Fernsehbericht des Bayerischen Rundfunks runden das Bild ab.

Abb. 1: Medien

Ein zweiter Fokus bei der aktiven Wissensvermittlung lag auf dem Thema Zusammenarbeit und Wissensaustausch zwischen Experten, das von der Friedrich-Alexander-Universität Erlangen-Nürnberg im Projekt VeSiKi umfangreich bearbeitet wurde. Hierzu wurden gemeinsame Strategieworkshops mit aktuellen und zukünftigen Führungskräften angeboten (sogenannte High Potential Workshops). Weitere Workshops befassten sich mit der Frage der Identifikation der Stakeholder im Bereich IT-Sicherheit und der zielgerichteten Ansprache dieser Gruppen zur Weitergabe von Wissen und der Anbahnung zukünftiger gemeinsamer Aktivitäten. Zu den Teilnehmern gehörten Experten aus dem gesamten Förderschwerpunkt sowie angrenzenden Bereichen. Aufgrund der großen Nachfrage fand ein weiterer Workshop zum Thema Bildung und Management professioneller Netzwerke statt, der zahlreiche praktische Übungselemente mit einschloss.

Befriedigung weiteren Bedarfs an Information und Austausch

Die Möglichkeit zum bedarfsorientierten Abruf von Wissen und dem bilateralen Austausch von Experten über spezielle Themen wurde durch die ITS|KRITIS-Vernetzungsplattform geschaffen. Die Plattform enthält nicht nur Informationen über die Projekte des Förderschwerpunkts und die darin gewonnenen Erkenntnisse. Es werden darüber hinaus auch andere nützliche Informationen über die Plattform verfügbar gemacht, etwa zur Expertenfindung oder zu Recht, Normung und Standardisierung.. Die Internetplattform kann jederzeit über das World Wide Web erreicht werden und enthält neben dem öffentlichen Teil, der für alle zugänglich ist, auch einen geschlossenen Teil, für den die Freischaltung gesonderter Nutzerprofile mit entsprechendem Passwortschutz erfolgen muss. Somit dient die Plattform sowohl der Ver-

Abb. 2: Forschungsinsel im offenen Innovationslabor JOSEPHS

breitung von Informationen in der Bevölkerung als auch der Vernetzung von Experten im Feld.

Besondere Aufmerksamkeit erhielt das Innovationslabor JOSEPHS als Ort für intensive fachliche Interaktion zu speziellen Themen der IT-Sicherheit Kritischer Infrastrukturen. Besucher des Labors konnten über einen Zeitraum von drei Monaten täglich zu üblichen Ladenöffnungszeiten an der Interaktion teilnehmen. Hier gab es keine Beschränkungen – vielmehr stand das offene Labor allen interessierten Bürgerinnen und Bürgern über den gesamten Zeitraum hinweg zur Verfügung und konnte nach deren Vorlieben genutzt werden. Die Interaktionsfläche im JOSEPHS enthielt dabei Objekte aus mehreren Projekten des Förderschwerpunkts, die im offenen Labor auf ihre Eignung in der Praxis getestet und anhand der Beiträge der Besucher weiterentwickelt und auf einen höheren Reifegrad gebracht werden konnten. Darüber hinaus trug die Forschungsinsel auch zur generellen Sensibilisierung der Bevölkerung im Themenbereich IT-Sicherheit Kritischer Infrastrukturen bei. Besucher konnten etwa in einer Simulation selbst versuchen, in das Datennetz eines Infrastrukturbetreibers einzudringen. Ferner wurden sie dazu ermutigt, selbst über Schutzbedarfe und Sicherheitslücken nachzudenken und Rückmeldung dazu abzugeben. Rund um die Nutzung des offenen Innovationslabors und in der weiteren Bearbeitung von Fallstudien mit einzelnen Infrastrukturbetreibern schuf das Projektteam darüber hinaus weitere Anlässe zum intensiven Austausch über die Projektarbeiten und die erzielten Ergebnisse mit Experten für Kritische Infrastrukturen aus den beteiligten Unternehmen. Diese trugen ebenfalls dazu bei, die Projektergebnisse über die Grenzen des Förderschwerpunkts hinweg in den entsprechenden Fachkreisen bekannt zu machen und dauerhaft in der aktuellen Forschungs- und Entwicklungslandschaft zu verankern.

Zu vermerken ist in der Zusammenfassung der Ergebnisse insbesondere, dass die genannten Aktivitäten auch merkbar zur Bildung einer „Community“ von Forschern im Themengebiet beigetragen haben. Dies ist im Hinblick auf die weitere Verwertung der Ergebnisse insofern von entscheidender Bedeutung, als dadurch grundlegende Strukturen geschaffen wurden, um den Wissensfluss über das Projekt hinaus mittel- und langfristig zu unterstützen. Damit wurde eine Voraussetzung für die nachhaltige Aufnahme der Projektergebnisse in Wissenschaft und Anwendung geschaffen.

Juristische Bewertung eines Social-Engineering-Abwehr-Trainings

D.-K. Kipker, S. Pape, S. Wojak, K. Beckers

Forschungsprojekte:
SIDATE & VeSiKi

Social Engineering

Bei Social Engineering (SE) wird durch Beeinflussungen der Opfer versucht, ein bestimmtes Verhalten hervorzurufen und auszunutzen, um sensible Informationen zu beschaffen. Laut dem aktuellen Datensatz des Data Breach Investigations Report [1] enthalten 43 % aller Datendiebstähle einen SE-Angriff. Dabei ist der SE-Angriff oft der erste Schritt eines größeren Angriffs, bei dem der Angreifer die dort gewonnen Informationen für weitere Angriffe verwendet.

Trainingsmaßnahmen zur Social-Engineering-Abwehr

Zurzeit haben Firmen hauptsächlich zwei Strategien, um SE-Angriffe abzuwehren: Einerseits können sie Penetration-Tester beauftragen, die als „gutartige Hacker" die Mitarbeiter angreifen und dabei Schwachstellen finden sollen. Leider ist dieser Ansatz nicht ganz unproblematisch. Experimente haben gezeigt, dass dieser Ansatz auch dazu führen kann, dass Angestellte demotiviert werden, wenn sie mit den Ergebnissen des Tests konfrontiert werden. Außerdem kann ein derartiger Test in das Persönlichkeitsrecht der Mitarbeiter eingreifen, sodass es zahlreiche arbeitsrechtliche Anforderungen an SE Penetration-Tests gibt [2, 3]. Andererseits können Firmen Schulungen und Security-Awareness-Trainings durchführen, in denen die Mitarbeiter auf Socia-Engineering-Bedrohungen hingewiesen werden. Oft sind diese Schulungen verpflichtend, haben aber keinen lang anhaltenden Effekt [4].

Eine dritte Möglichkeit sind Serious Games, d. h. Spiele, die neben Unterhaltung auch ein ernsthaftes Ziel verfolgen. Diese können zum Beispiel für Awareness-Trainings eingesetzt werden, um Mitarbeiter auf mögliche IT-Sicherheitsbedrohungen aufmerksam zu machen.

HATCH

Eines der beschriebenen Serious Games ist HATCH (siehe Abbildung 1), das das Verständnis der Arbeitnehmer von SE verbessert [5]. Durch das Spiel kann außerdem eine Liste möglicher SE-Bedrohungen erstellt werden, die zur Verbesserung der Sicherheit dienen kann [6]. Je nach Ziel wird mit einem ausgedachten (virtuellen) Szenario oder einem (realistischen) Szenario, das das reale Arbeitsumfeld abbildet, gespielt.

Virtuelle Szenarien

Beim Einsatz von HATCH zu Schulungs- und Awarenesszwecken kommen virtuelle Szenarien zum Einsatz. Diese bestehen aus einem Plan einer Abteilung oder Firma (siehe Abbildung 2 links) und für jede der im Plan dargestellten Mitarbeiter existiert eine Persona-Karte, die die grundlegenden Eigenschaften des Mitarbeiters skizziert (siehe Abbildung 2 rechts). Aufgabe der Spieler ist es nun, sich einen auf Basis der gezogenen Karten möglichst plausiblen Angriff auszudenken, der die Eigenheiten der im Spiel vorhandenen Mitarbeiter ausnutzt. Der gefundene Angriff wird dann von den Mitspielern auf Plausibilität bewertet.

Abb. 1: HATCH im Einsatz auf dem ITS-KRITIS Workshop

Abb. 2: Ein Spielplan von HATCH (links) und eine Persona-Karte (rechts)

Realistische Szenarien

Der grundlegende Spielablauf von HATCH mit einem realistischen Szenario ist derselbe wie mit einem virtuellen Szenario. Allerdings kommen hier keine virtuellen Personen zum Einsatz, stattdessen wird ein Plan der realen Arbeitsumgebung erstellt und die Spieler denken sich Angriffe auf ihre Kollegen aus. Dabei verwenden sie das bereits vorhandene Wissen über Arbeitsabläufe, Kompetenzen und Vorlieben der Kollegen. Als Ergebnis entsteht deswegen eine Liste mit möglichen SE-Bedrohungen, die dann dazu dienen kann, Arbeitsabläufe und Sicherheitsrichtlinien zu verbessern. Der Vorteil gegenüber einer Bedrohungsanalyse von Experten besteht darin, dass die Mitarbeiter einer Abteilung oder eines Unternehmens die realen Arbeitsabläufe bestens kennen, so dass es leichter ist, sie in SE zu schulen, als Experten alle Arbeitsabläufe studieren zu lassen.

Juristische Bewertung von HATCH

Allgemein ist anerkannt, dass die Geschäftsleitung eine rechtliche Verpflichtung besitzt, Maßnahmen der IT-Sicherheit als Bestandteil der unternehmenseigenen Compliance zu unterhalten und zu betreiben – hierzu gehört auch die Schulung von Mitarbeitern im Hinblick auf Social Engineering-Angriffe. Abgeleitet werden kann die IT-sicherheitsrechtliche Compliance-Verpflichtung dabei aus den unterschiedlichsten Rechtsvorschriften und in Abhängigkeit von der jeweiligen Branche, ganz allgemein aus § 43 Abs. 1 GmbHG und § 93 Abs. 1 AktG. Wo auf der einen Seite unternehmerische Verpflichtungen zur Realisierung eines angemessenen IT-Sicherheitsniveaus bestehen, stellt sich auf der anderen Seite die Frage, ob und wie der Arbeitnehmer damit verbundene Maßnahmen dulden und gegebenenfalls auch an diesen mitwirken muss. Der Konflikt zwischen Freiheit und Sicherheit aktualisiert sich hier in der Form arbeitsrechtlicher und auch datenschutzrechtlicher Fragestellungen sowie für die unternehmerische Compliance und Corporate Governance. Speziell für ein SE-Spiel wie HATCH, das eine aktive Teilnahme des einzelnen Mitarbeiters voraussetzt, eröffnen sich deshalb verschiedene juristische Problemfelder. Zu unterscheiden ist dabei zwischen dem realistischen und dem virtuellen Spielszenario.

Realistische Szenarien

Im realistischen Szenario von HATCH spielen sich die im Unternehmen beteiligten Akteure selbst. Eine besondere rechtliche Relevanz ergibt sich für diesen Fall daraus, dass die simulierten SE-Angriffe auf reale Personen und deren Charaktereigenschaften abzielen. Für die Frage der rechtlichen Zumutbarkeit für den einzelnen Arbeitnehmer ist dabei dessen aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG folgendes Allgemeines Persönlichkeitsrecht (APR) zu berücksichtigen. Einfluss auf das Arbeitsrecht findet das APR unter anderem als arbeitsvertragliche Nebenpflicht des Arbeitgebers gem. § 241 Abs. 2 BGB. Für den Arbeitgeber streiten demgegenüber, ebenfalls auf der mittelbaren Drittwirkung der Grundrechte im Privatrechtsverhältnis beruhend, die aus Art. 12 GG folgende Berufsfreiheit und der damit verbundene Schutz von unternehmerischen Interessen. Grundsätzlich gilt, dass der Arbeitgeber im Rahmen seiner mittelbar aus dem APR folgenden Verpflichtungen den Arbeitnehmer vor rechtswidrigen Eingriffen in seine Persönlichkeitsrechte zu schützen hat [7]. Hierzu gehört auch der Schutz vor potenziell bloßstellenden Maßnahmen, die sich negativ auf die Beschäftigten auswirken können [8]. Speziell für ein SE-Spiel in einem realistischen Szenario bestehen hier Risiken, indem sich Mitarbeiter bloßgestellt oder in ihrer betrieblichen Wertschätzung herabgesetzt fühlen, indem durch ein Erleben des Spiels als realistische Situation persönliche Grenzen überschritten werden und gruppendynamisch nicht vorhersehbare Spielverläufe eintreten. Fraglich ist, ob demgegenüber und im konkreten Fall die betrieblichen Interessen an der Durchführung des Spiels überwiegen und damit die Befolgung der IT-sicherheitsrechtlichen Compliancepflicht als gegenüber dem Arbeitnehmerschutz höherrangig einzustufen ist. Hierbei gilt der Grundsatz, dass in besonders sicherheitsrelevanten Sektoren und Branchen Lücken in der Unternehmenssicherheit durchaus ein hohes Gewicht im Rahmen der Interessenabwägung besitzen [9]. Daraus lässt sich, in Abwägung der Arbeitgeber- gegen die Arbeitnehmerinteressen, für den Regelfall folgern, dass sich die mit HATCH verbundene, unter wahrscheinlichen Umständen erfolgende fiktive Schaffung eines potenziell arbeitnehmerschädigenden Umfelds, in welchem die reale Persönlichkeit des Arbeitnehmers mit für Social-Engineering relevanten Schwachpunkten exponiert wird, in nicht in besonderem Maße exponierten Betrieben nur schwerlich mit dem potenziell erhöhten Lernerfolg einer Sensibilisierungsmaßnahme zur Förderung der IT-Sicherheit wird rechtfertigen lassen. Anders wäre dies bei Kritischen Infrastrukturen mit einem hohen Angriffsrisiko bzw. bei Unternehmen, die bereits häufig Opfer von Social Engineering-Vorfällen gewesen sind und für die sich eine ähnliche Gefährdungslage auch für die Zukunft abzeichnet: Hier könnte der erhöhte Bedarf an Sensibilisierungsmaßnahmen als Sachzusammenhang mit dem Schutz der Arbeitnehmer und von deren Arbeitsplätzen eine Durchführbarkeit der Maßnahme vor allem auch im Interesse des Mitarbeiters begründen. Eine unter Umständen anders gelagerte rechtliche Würdigung kann sich auch für die Fälle einer Bedrohungsanalyse ergeben, indem die hier durchzuführende Methodik zwingend voraussetzt, dass sämtliche für die IT-Sicherheit relevanten Schwachstellen in einem Unternehmen ermittelt werden, worin deshalb zwangsläufig auch der Faktor Mensch einzubeziehen ist.

> Die IT-sicherheitsrechtliche Compliancepflicht des Arbeitgebers steht in Konflikt mit dem Schutz des APR der Arbeitnehmer

Virtuelle Szenarien

Im virtuellen Szenario von HATCH werden die SE-Angriffe anhand fiktiver Charaktere und der damit verbundenen erdachten Rollenzuweisungen gespielt. Auch hier hat, wie schon für das realistische Szenario, eine rechtliche Abwägung zwischen den Persönlichkeitsinteressen des Arbeitnehmers und den betrieblichen und wirtschaftlichen Interessen des Arbeitgebers zu erfolgen. Ein Stigmatisierungsrisiko für den einzelnen Mitarbeiter besteht hier insoweit, als durch technische oder inhaltliche Wissenslücken in Bezug auf Social-Engineering-Bedrohungen persönliche Defizite gegenüber dem Arbeitgeber offenbart werden. Dem kann jedoch durch vor dem Spiel durchgeführte Schulungsmaßnahmen zur SE-Prävention entgegengewirkt werden. Klar formulierte Kommunikations- und Spielregeln tragen ferner dazu bei, dass Situationen potenzieller Anfeindung, Schikane

oder Diskriminierung während des Spielverlaufes schon im Vorfeld effektiv begegnet werden kann. Nicht zuletzt ist aufgrund der Wahl von fiktiven Charakteren auch das Maß einer Persönlichkeitsbeeinträchtigung deutlich geringer, indem innere Strukturen und Eigenschaften des Arbeitnehmers grundsätzlich nicht Spielgegenstand sind [10]. Ebenso bietet HATCH im fiktiven Szenario eine Möglichkeit, die Persönlichkeitsentwicklung der Arbeitnehmer im Rahmen der Pflichtausübung von § 75 Abs. 2 BetrVG zu fördern und zu unterstützen. Wie im realistischen Szenario auch ermöglicht das Spiel dem Arbeitgeber, durch eine verbesserte Awareness seiner Mitarbeiter den Betrieb vor Angriffen durch Social Engineering zu schützen. Im Ergebnis überwiegen deshalb im virtuellen Spielbetrieb die Arbeitgeberinteressen grundsätzlich diejenigen des Arbeitnehmers, sodass der Einsatz von HATCH eine denkbare Alternative zu den klassischen Schulungsmaßnahmen in diesem Bereich darstellt.

Quellen

[1] Verizon (2017, Mai). Data Breach Investigations Report, 10th Edition. Abgerufen am 24. Mai, 2017, 2017. http://www.verizonenterprise.com/verizon- insights-lab/dbir/2017/.

[2] Kuhn, Jörn; Willemsen, Alexander: Arbeitsrechtliche Aspekte von Social Engineering Audits. In: DER BETRIEB, Heft 02 vom 15.01.2016, S. 111-117. https://www.wiso-net.de/document/MCDB__DBDBDB1167400.

[3] Zimmer, Mark; Helle, Alicia: Tests mit Tücke – Arbeitsrechtliche Anforderungen an Social Engineering Tests. In: Betriebs-Berater, 21/2016 vom 23.05.2016, S. 1269.

[4] Stahl, Stan: Beyond information security awareness training: It's time to change the culture. In: Information Security Management Handbook, Sixth Edition, edited by Hal Tipton and Micki Krause, Auerbach, 2006. https://citadel-information.com/wp-content/uploads/2010/12/Beyond-Awareness-Training-Its-Time-to-Change-the-Culture-Stahl-0504.pdf.

[5] Beckers, Kristian; Pape, Sebastian; Fries, Veronika: HATCH: Hack And Trick Capricious Humans – A Serious Game on Social Engineering. In Proceedings of the 2016 British HCI Conference, Bournemouth, United Kingdom, Juli 2016.

[6] Beckers, Kristian; Pape, Sebastian: A Serious Game for Eliciting Social Engineering Security Requirements. In Proceedings of the 24th IEEE International Conference on Requirements Engineering, IEEE Computer Society, RE ,16, September 2016.

[7] GK-BetrVG/Kreutz, Bd. 2, 10. Aufl. 2014, § 75 BetrVG, S. 99, Rn. 106.

[8] Kuhn/Willemsen, DB 2016, S. 112.

[9] Ricken, RdA 2001, S. 52.

[10] Vgl. Kittner et al., Arbeitsrecht 2015, S. 1206, Rn. 61.

Sektion 5
Referenzimplementierung und Ausblick

In dieser Sektion wird die Implementierung der Werkzeuge und Maßnahmen in der Praxis vorgestellt und ein Ausblick in die Zukunft gegeben.

Aus der Arbeit der Forschungsprojekte im Förderschwerpunkt „IT-Sicherheit für Kritische Infrastrukturen“ ITS|KRITIS entstanden vielfältige Werkzeuge und Maßnahmen für die Praxis. In der vorangegangenen Sektion 4 wurden diese vorgestellt und beschrieben. In dieser Sektion 5 wird nun die beispielhafte Referenzimplementierung dieser Werkzeuge und Maßnahmen aufgezeigt. Darüber hinaus wird ein Ausblick in die Zukunft gegeben.

Review:

Steffi Rudel, Max Jalowski

Sektion 5
Inhaltsverzeichnis

Aqua-IT-Lab	Das hybride Labor als Testumgebung für IT-Sicherheit	118
Cyber-Safe	Cyber-Safe: Refernzimplementierung	121
INDI	Implementierung und Umsetzung	122
ITS.APT	Das ITS.APE-Framework	125
MoSaIK	Abschirmung und selbstlernende Organisation für mehr Sicherheit in KRITIS	129
PortSec	Praktische Umsetzung – Auditierungs- und Zertifizierungskonzept für Hafentelematiksysteme	132
PREVENT & VeSiKi	Die Managementlösung PREVENT in der Banken-IT	133
RiskViz	RiskViz als Werkzeug zur Erfassung und Erhöhung der IT-Sicherheit Kritischer Infrastrukturen	135
SICIA	Anwendung des SICIA-Verfahrens in der Praxis – am Beispiel eines ISMS	139
SIDATE	Das SIDATE-Portal im Einsatz	145

Das hybride Labor als Testumgebung für IT-Sicherheit

David Kotarski, Stephan Arndt, Christof Thim

Forschungsprojekt:
Aqua-IT-Lab

IT-Sicherheitsassessments im Hybridtestlabor

Kleine und mittlere Versorger scheuen häufig das Testen der IT-Sicherheit an laufenden Systemen wie z. B. bei Penetrationstests oder Sicherheitsassessments vor Ort. Zu hoch sind die Risiken von Seiteneffekten und ungeplanten Ausfällen der Versorgungsinfrastruktur. Dem begegnet der Gedanke des hybriden Testlabors, welches die kritischen Komponenten der Versorgungsinfrastruktur abbildet und risikolos mit festgelegter Zielrichtung analysierbar macht.

Laborarchitektur

Das Labor besteht aus vier Komponententypen, welche in Abbildung 1 dargestellt sind. Zunächst werden Kopf-SPS, also industrielle Steuerungseinheiten, physisch vorgehalten. Sie dienen dazu, zeitkritische Steuerungscodeanteile auszuführen. In Versorgungssystemen spielen diese Kopf-SPS zumeist eine aktiv steuernde Rolle und sind somit ein besonders schützenswerter Bestandteil der IT-Infrastruktur.

Neben den Hardwarekomponenten werden periphere Komponenten, wie passive Pumpensteuerungen, Sensorik etc., über simulierte SPS abgebildet. Diese Steuerungssimulation ist analog zum realen Versorgungssystem über entsprechende Protokolle an die Hardwarekomponenten angebunden.

Weiterhin können zur Überwachung und Steuerung reale Leit- und Monitoring-Systeminstanzen verwendet werden, um z. B. die Übernahme des Prozessleitsystems abzubilden.

Zur Steuerung der Simulation wird ein Command-and-Control-Server verwendet, mit dem die simulierten Slaves durch einen Nutzer manipuliert werden können. So ist es beispielsweise möglich, die Auswirkungen eines durch Angreifer manipulierten oder blockierten Datenverkehrs zwischen Kopf-SPS und dezentraler Peripherie zu simulieren, indem entsprechende Einstellungen über den Command-and-Control-Server vorgenommen werden.

Auch eine Simulation von weiteren Versorgungseffekten, wie beispielsweise der Wasserdruck in Rohrnetzen, soll durch Anbindung einer Softwaresimulation an die Logging-Datenbank in das Szenario integriert werden. Ziel ist die Aufdeckung von Effekten, wie geplatzte Leitungen durch unzulässige Druckverhältnisse, die bei Manipulation des Steuerungs-Datenverkehrs vielleicht auftauchen könnten.

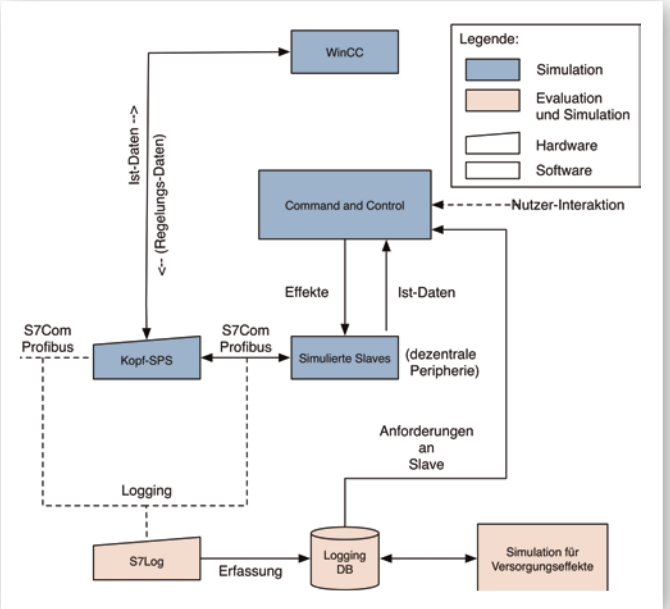


Abb.1: Grundarchitektur des hybriden Testlabors

Für die Nachvollziehbarkeit der Versuche und zur späteren Auswertung ist es vorgesehen, jegliche Kommunikation zwischen SPS-Komponenten und Simulation über einen Logging-Dienst aufzuzeichnen, und in einer Datenbank abzuspeichern. Das Logging soll hierbei durch eine weitere, dedizierte SPS übernommen werden, um den Programmablauf der Simulation nicht für das Aufzeichnen von Logging-Daten verändern zu müssen.

Der Laboraufbau kann je nach Untersuchungsziel variiert werden. Hier werden zwei mögliche Szenarien beschrieben, welche im Projekt Aqua-IT-Lab behandelt wurden.

Szenario 1: Angriff auf die standortübergreifende Kommunikation

Im ersten Szenario wird eine standortübergreifende Kommunikation nachgebaut und auf typische Angriffsvektoren, wie beispielsweise das unbefugte Eindringen in die Infrastruktur, geprüft. Abbildung 2 verdeutlicht das zu untersuchende Szenario. Es wurde von einem unserer Forschungspartner übernommen, um einen realitätsgetreuen Aufbau zu garantieren.

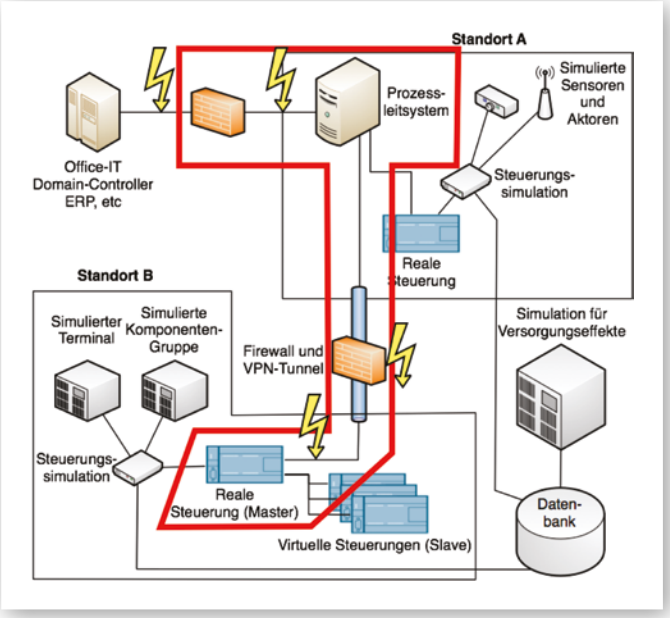


Abb. 2: Laboraufbau Szenario 1

Die zwei Standorte, die hier dargestellt werden, sind ein Prozessleitsystem (Standort A), mit dem eine Leitwarte simuliert wird, sowie ein Standort mit einer SPS, die eine zu überwachende Anlage in der Infrastruktur abbildet (Standort B). Beide Standorte sind mittels VPN-Gateways miteinander verbunden und kommunizieren damit verschlüsselt im öffentlichen Teil miteinander. Der Pentest-PC stellt den Angreifer da, er ist mit mehreren Netzwerkkarten an verschiedenen Zugangspunkten verbunden, sodass mehrere Arten von Angreifern zeitgleich ohne Änderung der Konfiguration simuliert werden können.

Der erste untersuchte Angriff erfolgt von außerhalb des Unternehmens. Hierbei ist das Ziel des Angreifers, von außen in den verschlüsselten VPN-Verkehr einzudringen oder Lücken in der Konfiguration der beiden Firewalls aufzuspüren. Dabei wird die identische Hardware wie beim Untersuchungsgegenstand eingesetzt. Die Konfiguration dieser Hardware ist ebenfalls ein Abbild des Produktivsystems. Somit können alle erzielten Erkenntnisse auf das zu überprüfende System überführt werden.

Der zweite simulierte Angreifer geht von einer Kompromittierung der internen Verbindung aus und stellt somit eine interne Bedrohung dar. Dabei werden die ebenfalls nachgestellten Systeme (Prozessleittechnik und SPS) jeweils auf Schwachstellen untersucht. Auf beiden Systemen läuft die identische Konfiguration wie auf dem Produktivsystem von einem Forschungspartner, damit die Übertragung der Erkenntnisse gesichert bleibt.

Szenario 2: Resilienz des Versorgungssystems

Im zweiten Szenario steht die Untersuchung der Effekte, die ein interner Angreifer auf eine Infrastruktur im Bereich der Wasserversorgung haben kann, im Fokus. Im Gegensatz zum ersten Szenario liegt der Fokus daher nicht auf der Sicherheit von Lösungen zur Abschirmung des internen Netzes vor externen Angriffen oder den Zugriffskontrollen, die für interne Prozessleit- oder SPS-Systeme vorhanden sind, sondern es soll eine Untersuchung stattfinden, welche Auswirkungen verschiedene Arten von Angriffen auf die Gesamtinfrastruktur haben.

Der Versuchsaufbau besteht zu diesem Zweck aus der Nachbildung verschiedener Sektionen realer Wasserwerke. Im Mittelpunkt der Architektur steht die Kopf-SPS, auf der die Steuerungslogik für den zu untersuchenden Teilabschnitt liegt, sowie die Peripherie, die von dieser SPS gesteuert wird (Abbildung 3).

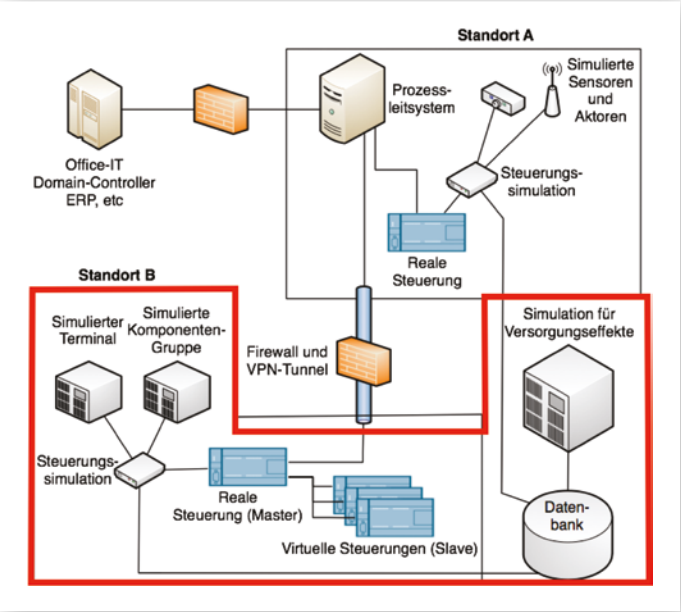


Abb. 3: Laboraufbau Szenario 2

Da aus Kostengründen die nachzubildenden Sektionen nicht komplett als Hardware bereitgestellt werden können, werden die peripheren Komponenten des Wasserwerkes durch eine Softwarelösung simuliert. Diese Systeme werden häufig über reine Slave-Sensoren oder -aktoren implementiert, welche keine oder nur sehr rudimentäre Steuerungslogik enthalten. Sie hängen von den Steuerungsbefehlen der Kopfsysteme ab, also den Steuerungen, auf denen die eigentliche Steuerungslogik ausgeführt wird. Diese sind in Hardware vorhanden, um eine möglichst detailgetreue Simulation der nachgebildeten Sektionen garantieren zu können und auch hardwarespezifische Latenzen berücksichtigen zu können. In diesem Aufbau werden die originalen Steuerungsprogramme für die Simulation und die Hardwarekomponenten verwendet.

Der Sicherheitstest bezieht sich nun auf den Zugriff auf die SPS und die Überprüfung der Robustheit des verwendeten Codes. Dabei wird davon ausgegangen, dass der Angreifer bereits den Sicherheitsperimeter überschritten hat und sich im gleichen Netz wie die SPS befindet.

Anders als in Szenario 1 kommt hierbei die gesamte Laborinfrastruktur zum Einsatz. Nicht nur die Möglichkeit des Zugriffs und der Manipulation, sondern die Wirkung kompromittierter Anlagen im Versorgungssystem wird untersucht. Die Kopfstationen bilden den Schwerpunkt der Überprüfung. Gelingt es dem Angreifer, dort einzudringen oder die Steuerungssignale zu manipulieren, sind die Auswirkungen auf den simulierten Steuerungen und später die Effekte in der Versorgungssimulation direkt zu beobachten. So können der Umfang und die Ausdehnung des Versorgungsausfalls besser abgeschätzt werden. Dies erleichtert die Planung reaktiver Maßnahmen und sensibilisiert für Investitionen in Prävention. Das mitlaufende Logging zeigt im Nachgang die Lücken auf und ermöglicht eine Detailanalyse des Angriffs. Hieraus können sowohl Versorger als auch Penetrationstester Muster der Angriffe erlernen. Der IT-Verantwortliche ist damit in der Lage, auffälliges Verhalten der Anlage schneller zu erkennen und früh Gegenmaßnahmen einzuleiten.

Wie in den Szenarien gezeigt werden konnte, eignet sich der hybride Ansatz, um ohne große Risiken in einem begrenzten Testumfang Sicherheitsassessments durchzuführen. Er bildet somit für Versorger einen Ansatzpunkt zur Vertiefung der Analysen aus dem Schnelltest. Weiterhin können IT-Sicherheitsunternehmen mithilfe des Labors radikaler testen und auch Ausfälle einzelner Komponenten und Regelkreise provozieren. Die hierdurch erzielten Effekte erhöhen die Sensibilität der Versorger bei der Absicherung ihrer Steuerungs-IT.

Für die weitere Forschung bildet die Infrastruktur die Möglichkeit, Seiteneffekte von Angriffen genauer zu betrachten und über einen längeren Zeitabschnitt die Wirkung im Versorgungssystem zu untersuchen. Auch die Nutzung als HoneyPot zur Analyse externer Angreifer und zur Identifikation ihrer Angriffsmuster ist denkbar.

Cyber-Safe: Referenzimplementierung

Anke Nölting, Selcuk Nisancioglu

Forschungsprojekt:
Cyber-Safe

Insgesamt stehen den Anwendern Handlungshilfen in drei Stufen mit steigendem Detailierungsgrad zur Bewertung und Verbesserung der IT-Sicherheit einer Leitzentrale zur Verfügung, wobei die einzelnen Stufen definierte Zielgruppen innerhalb der Organisationsstruktur einer Leitzentrale ansprechen. Die Stufe 1 wurde für die übergeordnete Managementebene in Form einer einfachen Checkliste entwickelt und soll die Entscheidungsträger im Wesentlichen für das Thema der IT-Sicherheit von Tunnel- und Verkehrsleitzentralen sensibilisieren und eine erste Bewertung der vorhandenen IT-Sicherheit ermöglichen. Dabei besteht die Checkliste aus kurzen und einfach zu beantwortenden Fragen rund um das Thema IT-Sicherheit. Sofern ein weiterer Handlungsbedarf besteht, wird dem Nutzer im Ergebnis der Checkliste empfohlen, die Stufe 2 anzuwenden und das entsprechende Personal einzubinden. Diese zweite detaillierte Stufe wendet sich an die mittlere Managementebene und besteht aus dem Cyber-Safe-Leitfaden, der den aktuellen Stand der „Best Practice" zur IT-Sicherheit in Leitzentralen zusammenfassend darstellt, und einer Bewertungssoftware, die es dem Benutzer ermöglicht, detaillierte Verbesserungsmaßnahmen in den Bereichen Personal, Organisation und Technik zu identifizieren. Mit der Stufe 3 steht dem Nutzer eine weitere Software zur Verfügung, die es ihm erlaubt, seine gesamte IT-Architektur im Rahmen einer Tiefenanalyse zu bewerten. Diese Tiefenanalysesoftware ist eine Hilfe von „Experten für Experten" und sollte nur von IT-Verantwortlichen oder ähnlich qualifiziertem Personal genutzt werden. Gleichzeitig kann es als Planungshilfe von Ausstattern und Planern herangezogen werden.

Idealerweise sollten die Handlungshilfen in ein ISMS (Managementsystem für Informationssicherheit) integriert werden, das systematisch die Anpassung und Verbesserung der IT-Sicherheit in definierten Zyklen gewährleistet.

Im Rahmen des Forschungsprojektes Cyber-Safe werden die entwickelten Handlungshilfen exemplarisch in einer Tunnelleitzentrale sowie einem Tunnel angewendet. Die aus der Bewertung resultierenden Härtungsmaßnahmen werden anschließend vom Tunnelbetreiber und dem Tunnelausstatter umgesetzt. In einem weiteren gezielten Penetrationstest wird dann die Wirksamkeit der empfohlenen Härtungsmaßnahmen überprüft um abschließend die Handlungshilfen zu optimieren.

Abb. 1: Demonstrations-Tunnel (Foto: Straßen.NRW)

Implementierung und Umsetzung

Konrad Rieck, Christian Wressnegger, Hartmut König,
Andreas Paul, Franka Schuster, Heiko Kanisch, Christoph Moder

Forschungsprojekt:
INDI

Die Implementierung der angestrebten Sicherheitstechnologie kann durch vier Bausteine beschrieben werden: (A) eine Topologieexploration zur Erfassung eines Industrienetzes; (B) eine selbstlernende Schwachstellenanalyse zur Beurteilung von Verwundbarkeiten und (C) eine protokollabhängige sowie (D) eine protokollunabhängige Anomalieerkennung zum Aufspüren von Angriffen.

A. Topologieexploration

Der erste Baustein der Implementierung ist ein Werkzeug zur automatisierten Exploration der Netztopologie aus passiv aufgezeichneten Netzdaten. Dieses Werkzeug kann einzeln für sich zur Erfassung eines Industrienetzes aber auch in Kombination mit den anderen Bausteinen operieren.

Verkehrsanalyse
Als Voraussetzung für diese automatische Topologieexploration sowie die protokollspezifische Anomalieerkennung wird Industrieverkehr an entscheidenden Netzknotenpunkten im Betrieb mitgeschnitten und einer umfangreichen Verkehrsanalyse (Topologie und Kommunikationsbeziehungen) unterzogen. Zugleich stellt der hier erfasste Netzverkehr Trainingsdaten für die selbstlernenden Verfahren zur Anomalieerkennung bereit.

Werkzeug zur automatisierten Topologieexploration
Basierend auf den erhobenen Daten und den daraus erlangten Erkenntnissen über Industrieverkehr entstehen Techniken zur Ableitung von Topologie und Kommunikationscharakteristika, die unter anderem unbekannte Geräte und ungewollte Kommunikationsbeziehungen aufzeigen können. Alle Verfahren werden in ein Werkzeug gebündelt, das einen Baustein der Sicherheitslösung (SCADA-Gateway) darstellt.

B. Selbstlernende Schwachstellenanalyse

Ziel des zweiten Bausteins ist es, eine Schwachstellenanalyse für Industrienetze bereitzustellen. Die entwickelten Methoden suchen selbstlernend in den Implementierungen von bekannten als auch unbekannten Protokollen nach Schwachstellen. Hierzu müssen Modelle von Nachrichtenformaten und Nachrichtensequenzen aus aufgezeichnetem Verkehr abgeleitet werden, um darauf aufbauend mit Fuzzing Verwundbarkeiten zu erkennen.

Modellierung von unbekannten Protokollen
Dieser Ansatz nutzt moderne Konzepte der Protokollanalyse, die auf Techniken des maschinellen Lernens basieren. Ausgehend von beobachtetem Netzverkehr wird das Format von Nachrichten und der Zustandsautomat der Protokolle approximiert. Hierfür wurden im Vorhaben existierende Ansätze, wie z. B. PRISMA, für den Einsatz in Industrienetzen angepasst und erweitert.

Replay und Fuzzing von Nachrichtenformaten
Basierend auf den zuvor erstellten Modellen können dann Techniken zur aktiven Schwachstellensuche (Fuzzing) eingesetzt werden. Diese Techniken ermöglichen es, das Format von Nachrichten systematisch zu manipulieren, z. B. durch das Einfügen von langen Feldern oder ungewöhnlichen Bytefolgen. Die manipulierten Nachrichten werden dann in die Kommunikation zu einem Zielsystem eingeschleust und erlauben es, Schwachstellen in den Protokollparsern der Systeme automatisch aufzuspüren.

Mithilfe der erstellten Modelle können dann auch Techniken zur Schwachstellensuche im Zustandsautomat von unbekannten Protokollen angewendet werden. Hierbei wird nicht der Inhalt von Nachrichten manipuliert, sondern deren sequentielle Reihenfolge, z. B. durch das Vertauschen von Nachrichten. Die manipulierten Nachrichtensequenzen werden in die Kommunikation zu einem Zielsystem eingeschleust und können Fehler in der Implementierung der Protokolle aufdecken.

Generierung von Mustern für Schwachstellen
Grundsätzlich sollten Sicherheitsschwachstellen möglichst rasch behoben werden. Da dies in Industrieanlagen durch sehr hohe Laufzeitanforderungen nicht immer möglich ist, können aus den gefundenen Schwachstellen Muster für die Erkennung entsprechender Angriffe abgeleitet werden. Diese Muster können in ein Intrusion-Detection-System geladen werden und somit schon vor der eigentlichen Korrektur einen Schutz der gefundenen Schwachstellen ermöglichen.

C. Protokollspezifische Anomalieerkennung

Ziel des dritten Bausteins - der protokollspezifischen Anomalieerkennung - ist das Erkennen von Abweichungen gegenüber typischen Protokollabläufen auf Basis der

Protokollspezifikationen sowie von Prozessanomalien durch Regression auf übermittelten Messwerten. Die zu diesem Zweck mittels maschinellen Lernens generierten Modelle werden in für den Betreiber verständliche Regeln überführt, die einen Eingriff in das Lernverhalten ermöglichen, um Fehlalarme zu minimieren. Zusätzlich können anhand der gelernten Modelle Regeln für die Konfiguration der Systeme (z. B. Firewalls) des Betreibers abgeleitet werden.

Analyse von Protokollspezifikationen
Für eine detaillierte, protokollspezifische Analyse ist es nötig, Netzpakete zu dekodieren, um so Nachrichten von standardisierten Protokollen für die anschließende Analyse aufzubereiten. Für diese Dekodierung ist umfangreiches Wissen über den Aufbau der Netzpakete erforderlich, das durch Analyse der Spezifikation des jeweiligen Protokolls erlangt werden muss. Im Rahmen dieser Protokollanalyse können zudem typische Protokollabläufe studiert werden, sodass protokollspezifische Angriffsmöglichkeiten frühzeitig identifiziert werden können.

Protokollspezifische Präprozessoren
Mithilfe des erlangten Protokollwissens können Dekodierer eingesetzt werden, die in Netzpaketen enthaltene Daten extrahieren und in geeigneter Form den Algorithmen der anschließenden Anomalieerkennung zur Verfügung stellen. Für jedes unterstützte Industrieprotokoll wird ein gesonderter Dekodierer bereitgestellt, sodass je nach Bedarf für die Analyse in dem jeweiligen Netzsegment die passende Sicherheitslösung aktiviert werden kann. Jeder Dekodierer sollte hierbei in der Lage sein, Industriekommunikation in Echtzeit zu analysieren.

Maschinelles Lernen auf Protokollfragmenten
Durch den Einsatz von Techniken des maschinellen Lernens und der von den entwickelten Dekodierern bereitgestellten Netzdaten wird eine selbstlernende Anomalieerkennung möglich. Zu lösende Kernprobleme sind hier die Bestimmung einer für die Lernalgorithmen optimalen Abbildung der Netzdaten auf Vektoren sowie die Entwicklung einer nachgelagerten Bewertung der Ergebnisse der gelernten Anomalieerkennung. Es entstehen Erkennungstechniken, die sowohl ungewöhnliche Kommunikation (u. a. protokollspezifische Man-in-the-Middle-Angriffe und Denial-of-Service-Angriffe, andere ungewöhnliche Nachrichtensequenzen) sowie Prozessanomalien (u. a. ungewöhnlicher Messwertverlauf, Grenzwertüberschreitung) identifizieren.

Entwicklung von Regeln zur Konfiguration des Normalverhaltens
Aus den gelernten Modellen der Anomalieerkennung können dann Regeln abgeleitet werden. Diese sollen dem Betreiber einen Zugang zu den gelernten Modellen der Anomalieerkennung geben, indem sie die Modelle in kompakter Weise darstellen und so ein Verständnis der gelernten Kommunikationsmuster ermöglichen. Zugleich dienen diese Regeln dem Betreiber zur Konfiguration der Sicherheitslösung selbst sowie zur Verbesserung der Konfiguration anderer Komponenten des Betreibers wie vorhandene Firewalls und Router.

D. Protokollunabhängige Anomalieerkennung

Um Angriffe in unbekannten Protokollen zu identifizieren, besteht der vierte Baustein aus einer protokollunabhängigen Anomalieerkennung. Hierzu sind Methoden konzipiert worden, die relevante Protokollfelder und -zustände automatisch in der Kommunikation von unbekannten Protokollen identifizieren und anomale Muster in diesen aufspüren. Die gelernten Modelle werden ebenfalls als Grundlage für Regeln und die Konfiguration angeschlossener Systeme genutzt.

Extraktion und Filterung von relevanten Nachrichtenfeldern
Um ungewöhnliche Aktivitäten in einem Industrienetz zu finden, ist es nötig, Nachrichten von proprietären Protokollen zu parsen und soweit möglich semantisch aufzubereiten. Hierzu wurden Techniken zur syntaktischen und semantischen Analyse von Feldern in Nachrichten entwickelt. Diese Techniken bauen auf Konzepten zur automatischen Protokollanalyse auf, um den Inhalt von Nachrichten unbekannter Protokolle so gut wie möglich syntaktisch und semantisch aufzuschlüsseln.

Extraktion und Filterung von relevanten Protokollzuständen
Im zweiten Schritt werden dann Techniken zur Ableitung und Filterung von Protokollzuständen eingesetzt. Hierfür werden probabilistische Modelle über einzelne Nachrichten gelernt, die es erlauben zu ermitteln mit welcher Wahrscheinlichkeit ein Nachrichtentyp von

einem anderen Nachrichtentyp gefolgt wird. Diese Modelle greifen existierende Ansätze zur zustandsabhängigen Protokollanalyse auf und erweitern diese für den Einsatz in Industrienetzen.

Zustandsabhängige Anomalieerkennung für unbekannte Protokolle
Durch eine detaillierte Sicht auf unbekannte Protokolle (Felder und Zustände) wird es möglich, ungewöhnliche Kommunikation und somit neuartige Cyberangriffe aufzuspüren. Hierfür werden die gelernten Nachrichtenfelder und Protokollzustände mit Methoden zur Anomalieerkennung kombiniert. Es können so Erkennungstechniken entstehen, die sowohl ungewöhnliche Felder (z. B. hohe Werte oder lange Zeichenketten) als auch ungewöhnliche Nachrichtensequenzen (z. B. häufig wiederholte Nachrichten) identifizieren.

Ableitung von Regeln zur Konfiguration des Normalverhaltens
Um dem Betreiber einen Zugang zu den gelernten Modellen der Anomalieerkennung zu geben, werden zusätzlich Regeln aus den Modellen abgeleitet. Diese Regeln sollen das Modell in kompakter Weise darstellen und so ein Verständnis der gelernten Kommunikationsmuster ermöglichen. Es können so auch Regeln für unbekannte Nachrichtenformate und -sequenzen entstehen.

Das ITS.APE-Framework

Arnold Sykosch

Forschungsprojekt:
ITS.APT

Im Rahmen des Projekts ITS.APT wurde ein Framework zur Messung von IT-Security-Awareness entwickelt, das ITS.APE-Framework (ITS.APE: IT-Security Awareness Penetration Testing Environement). Dieses Framework wird im Folgenden vorgestellt.

IT-Security-Awareness-Messmethoden

Nach dem aktuellen Stand der Wissenschaft wird die IT-Security-Awareness als handlungsrelevanter Faktor der Entscheidungsfindung angesehen. Derartige Entscheidungen werden zumeist in bestimmten Situationen durch Individuen getroffen. Somit ergeben sich weitere handlungsrelevante Faktoren, welche die Entscheidungsfindung beeinflussen. Diese Faktoren reichen von situativ bestimmten Faktoren, wie Motivation oder aktueller Konzentrationsfähigkeit, bis hin zu Charaktereigenschaften der Entscheidenden, wie genereller Risikobereitschaft, Selbstsicherheit, Neugier und vielen mehr.

Aus dem Forschungsbereich der situativen Awareness auf Basis der Arbeiten von Mika Endsley sind bereits verschiedene Messmethoden bekannt und nach ihren Eigenschaften klassifiziert worden. Zunächst lassen sich diese Methoden in direkte und indirekte Methoden gruppieren. Direkte Messmethoden setzen einen interaktiven Kommunikationskanal mit dem Probanden voraus. Dieser wird durch den Versuchsleiter unter Laborbedingungen in eine kontrollierte Simulation einer Situation versetzt und dann während der Entscheidungsfindung interviewt. Dies passiert entweder inline in der Situation, indem der Versuchsleiter beispielsweise einen Schreibtischnachbarn verkörpert, der Fragen zu der Situation stellt, oder outline, indem die Simulation angehalten wird und dem Probanden entsprechende Fragen gestellt werden. Ein derartiger Aufbau ist jedoch für die Belegschaft eines gesamten Unternehmens wegen der hohen Kosten nicht zu realisieren.

Indirekte Messmethoden ergeben sich entweder durch die Selbsteinschätzung eines Probanden oder durch eine schlussfolgernde Messung. An der Messmethode mit Indirektion durch Selbsteinschätzung (Fragebögen) wurde schon viel Kritik geübt und die Existenz einer Verzerrung der Ergebnisse auch experimentell belegt. Die einzig praktikable Vorgehensweise ist die schlussfolgernde Messung.

Hier ergeben sich wieder zwei Untergruppen: Gesamtleistungsmessung und individuelle Resonanzmessung. Die Gesamtleistungsmessung vergleicht Indikatoren, die das Gesamtbild widerspiegeln, etwa „Wie viele sicherheitsrelevante Vorfälle sind im Zeitraum X aufgetreten?“, „Wie viele sicherheitsrelevante Vorfälle wurden von Nutzern berichtet?“ oder „Wie oft glaubte ein Nutzer, ein sicherheitsrelevanter Vorfall läge vor, obwohl dies nicht der Fall war?“.

Die Gesamtleistungsmessung gewährt jedoch nur wenig Möglichkeit zur Einsicht in die Zusammenhänge zwischen den Faktoren. Individuelle Resonanzmessung bietet hier eine Alternative. Bei dieser Messmethode wird ein Proband in eine Situation versetzt, in der eine sicherheitsrelevante Entscheidung getroffen werden muss. Das Ergebnis dieses Prozesses ist die ergriffene Handlungsoption, diese kann nun bewertet werden.

IT-Security-Awareness-Messung mithilfe von Artefakten

Für die korrekte Interpretation der durch den Probanden ergriffenen Handlungsoption ist das Wissen um die entscheidungsrelevanten Elemente der Situation, in der die Entscheidung getroffen wurde, unabdingbar. Da eine Situation, die ein Computernutzer in seinem Alltag durchlebt, nicht vollständig zu erfassen und die Kontrolle über die entscheidungsrelevanten Elemente der Situation unabdingbar ist, gilt es, diese in die Situation einzubringen.

Abbildung 1 zeigt schematisch die Situation eines Nutzers bei der Bedienung eines Computers. Der Nutzer verfolgt mit dem Haupthandlungsstrang ein Ziel. Dabei durchläuft der Nutzer eine Reihe von aufeinanderfolgenden undineinanderübergehenden Situationen. In diesen befinden sich verschiedene Elemente. Einige davon haben einen Sicherheitsbezug. Dieser kann sich natürlich ergeben, wie etwa eine Passwortabfrage beim Zugriff auf eine geschützte E-Mail oder aber künstlich in die Situation eingebracht werden, z. B. eine Passwort-Abfrage auf einer sogenannten „Landing-Page“.

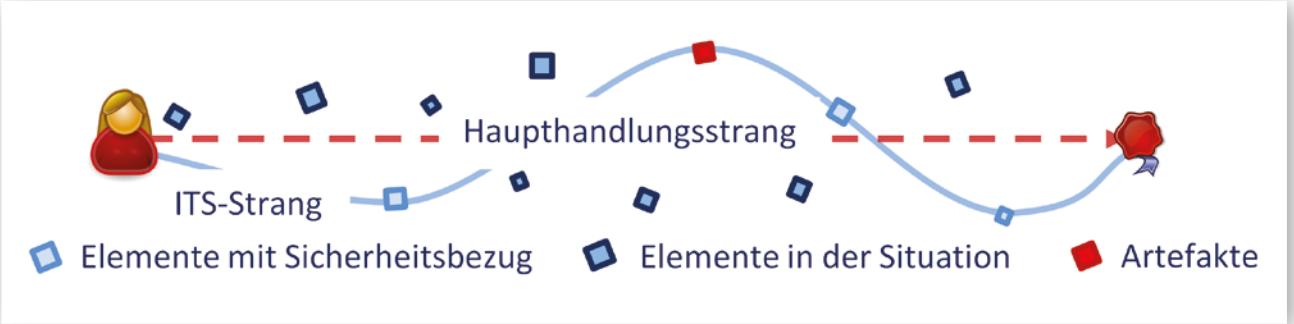


Abb. 1: Schematische Darstellung der verschiedenen Elementtypen in den, durch einen Nutzer durchlaufenen, Situationen

Sind diese Artefakte kontrolliert in die Situation eingebracht und wurde die ergriffene Handlungsoption erfasst, lässt sich noch nicht direkt ein Rückschluss auf die IT-Security-Awareness des Nutzers ziehen. Hier ist der Einfluss der anderen entscheidungsrelevanten Faktoren zu groß. Es gilt nun, den Einfluss beherrschbar zu machen. Für die entscheidungs-beeinflussenden Charaktereigenschaften lässt sich ein Fragebogen entwerfen, der diese erfassbar macht. Die Ergebnisse eines derartigen Fragebogens müssen dann mit der Bewertung der Handlung korreliert werden. Zur Beherrschung situativer Einflüsse ohne die Möglichkeit, die Situation selbst zu kontrollieren, steht die Mehrfachausführung, angelehnt an die Effektgrößeneinschätzung einer Meta-Analyse, zur Verfügung. Dieses Vorgehen hat zur Folge, dass situative Einflüsse und die Qualitätsmerkmale der Artefakte (wie deren Sichtbarkeit) nicht signifikant in das Ergebnis einfließen. Genau hier setzt das ITS.APE-Framework ein.

IT-Security-Awareness-Messung mit dem ITS.APE-Framework

Das ITS.APE-Framework automatisiert die zur IT-Security-Awareness-Messung benötigten Vorgänge. Es ist in der Lage, auf Basis von sogenannten Rezepten Artefakte auszubringen und ergriffene Handlungsoptionen datenschutzkonform aufzuzeichnen.

Anwendbarkeit

Die Messung von IT-Security-Awareness mit dem ITS.APE-Framework ist nur dann sinnvoll, wenn die IT-Infrastruktur durch Administratoren betreut wird. Das Framework ist für den Einsatz innerhalb eines Unternehmensnetzes entworfen und benötigt entsprechende Infrastruktur. Insbesondere muss es möglich sein, zu jeder

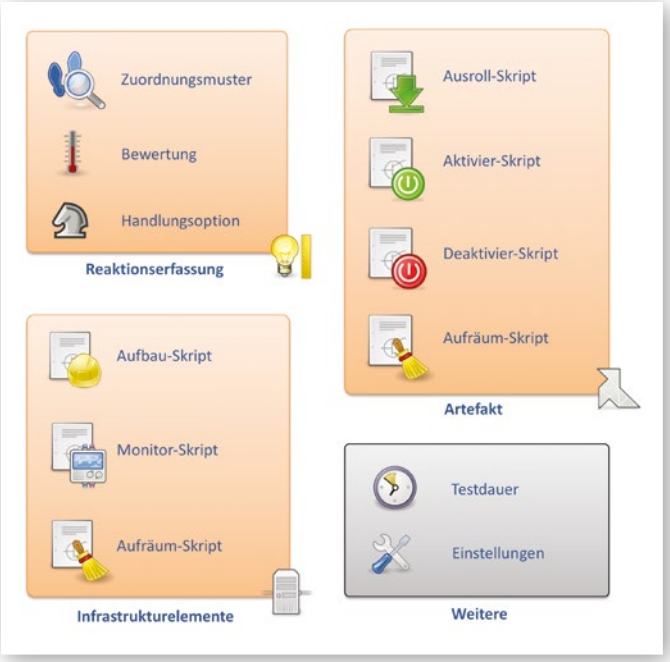


Abb. 2: Schematische Darstellung der Komponenten eines Rezepts

Zeit festzustellen, an welchem Gerät welche Person arbeitet (User-Tracking). Dies setzt personalisierte Nutzerkonten oder individuell nutzbare Computerarbeitsplätze voraus. Weiter geht das Framework davon aus, dass alle zu testenden Personen dieselbe Infrastruktur nutzen.

Das Framework selbst ist eine Applikation, die auf einem Host in der Infrastruktur installiert wird. Zur Inbetriebnahme werden drei Dinge benötigt:

1. eine Datei, in der die Teilnehmer beschrieben sind,
2. eine Schnittstelle für das User-Tracking (als ladbares Plug-in),
3. eine Batterie von Rezepten.

Die Rezepte entscheiden, was genau passieren soll. Mit ihrer Hilfe können personalisierte Artefakte erzeugt und ausgebracht werden. Das Framework stellt den Rezepten die nötige Umgebung zur Verfügung.

Rezepte

Rezepte sind eine geordnete Sammlung von Skripten und Parametern. Sie sind der spezifische Teil, der das generische Framework in konkreten Teststellungen komplettiert. Abbildung 2 verdeutlicht schematisch die Komponenten eines Rezepts.

Die Ausführung eines Rezepts wird durch das Framework terminiert. Die Durchführungs-dauer (in der Abbildung mit „Testdauer“ gekennzeichnet) wird jedoch durch das Rezept vorgegeben. Ebenso ist es dem Versuchsleiter erlaubt, Einstellungen vorzunehmen (z. B. den Absender einer E-Mail zu ändern oder den Namen einer Datei zu bestimmen, sofern dies durch das Rezept unterstützt wird.

Wird die Durchführung eines Testdurchlaufs vorbereitet, so werden zunächst die erforderlichen Infrastrukturelemente aufgebaut. Hier können Webserver für Landing-Pages aufgebaut werden oder Man-in-the-Middle-Proxies aufgesetzt werden. Das Monitor-Skript wird durch das Framework in regelmäßigen Abständen ausgeführt, um die Bereitschaft der Infrastrukturelemente zu prüfen und den Versuchsleiter bei einem Fehler zu informieren. Dieser kann dann manuell in den Vorgang eingreifen. Die Aufräum-Skripte dienen dem Abbau der Infrastruktur bei Testende.

Sind die Infrastrukturelemente aufgebaut und betriebsbereit, so können sie (falls benötigt) durch die Ausroll-Skripte mit Artefakten bestückt werden. Ist dies ge-

schehen, so wird der Test durch das Framework aktiviert. Hierzu wird das Aktivier-Skript ausgeführt. Ab diesem Zeitpunkt ist es dem Nutzer möglich, das Artefakt wahrzunehmen. Am Ende der Testdauer wird der Test durch das Deaktivier-Skript wieder deaktiviert. Diese Skripte ermöglichen auch das Pausieren der Tests in kritischen Situationen. Das kann nötig werden, wenn alle Ressourcen des Unternehmens ohne Störungen benötigt werden, z. B. in einem Krankenhaus, wenn aufgrund eines Unfalls ein stark erhöhtes Aufkommen von Patienten zu bewältigen ist.

Für die Dokumentation der Nutzerreaktionen sind die Elemente der Reaktionserfassung verantwortlich. Der Nutzer hinterlässt bei der Interaktion mit Elementen in der Situation Spuren in Form von Protokolleinträgen. Dies kann durch einen Anruf beim Helpdesk geschehen oder durch einen Klick auf den Link einer präparierten E-Mail. Diese Logs müssen entweder kontinuierlich während des Tests oder aber im Nachgang in das Framework eingespielt werden. Mithilfe der Zuordnungsmuster werden diese Spuren dann Probanden und entsprechenden Testzeiträumen zugeordnet. Lässt sich eine Spur nicht zuordnen, so wird der Eintrag gelöscht, lässt sie sich zuordnen, so werden die entsprechende Handlungsoption sowie deren Bewertung erfasst. Diese Erfassung komplettiert den Testdurchlauf.

Auswertung

Auswertungen werden anhand der festgestellten, durch den Teilnehmer ergriffenen Handlungsoptionen bestimmt. Um diese mithilfe eines Zahlenwertes vergleichbar zu machen, werden die einzelnen Handlungsoptionen mit einem Punktewert belegt. Dieser entsteht zunächst durch die Einschätzung eines Experten, sollte aber im Laufe der Zeit durch einen kontinuierlichen Prozess angepasst werden. Die Tatsache, dass die ergriffene Handlungsoption sowie ihre Bewertung aufgezeichnet werden, garantiert die Vergleichbarkeit der Ergebnisse auch über größere Zeiträume hinweg.

Das Framework erlaubt dabei per Design ausschließlich pseudonymisierte oder anonymisierte Ergebnisberichte. Idealerweise werden ausschließlich nach Teilnehmergruppe oder Artefakt gruppierte Berichte genutzt. Soll jedoch etwa gezielt nach Individuum geschult werden, so müssen die Ergebnisse mit der Identität der Teilnehmer korrelierbar sein. In diesem Fall ist ein pseudonymisierter Bericht zu nutzen. Das Pseudonym jedes Teilnehmers ist dann in der Datei der Teilnehmergruppe kodiert. Die Auflösung des Pseudonyms ist ausschließlich für den Besitzer der Liste möglich. Wird die Liste nach der Testdurchführung gelöscht, so wird den Pseudonymen damit die Möglichkeit der Aufdeckbarkeit entzogen (sofern keine weitere Kopie existiert).

Fazit

Mit dem ITS.APE-Framework kann in entsprechend vorbereiteten Computernetzwerken von Unternehmen, die individuelle IT-Security-Awareness der Mitarbeiter systematisiert ermittelt werden. Dabei kommen sichere Verfahren zur Pseudonymisierung und Anonymisierung zum Einsatz, sodass die Persönlichkeitsrechte der Probanden gewahrt werden – eine Grundvoraussetzung, um die in jedem Fall notwendige Zustimmung der Personalvertretung für die Durchführung von Mitarbeiterbeobachtungen zu erzielen.

Das modulare Konzept des Frameworks und die Verwendung von flexibel anzupassenden Rezepten für unterschiedlichste Artefakte machen ITS.APE in nahezu jeder IT-Umgebung einsetzbar. Sowohl für Betreiber von Kritischen Infrastrukturen (KRITIS) als auch für jedes andere Unternehmen, dessen Betriebsfähigkeit auf einer funktionierenden IT-Infrastruktur basiert, stellt das ITS.APE-Framework eine Möglichkeit zur Verfügung, die etablierten PEN-Tests der Infrastruktur auf die eigenen Mitarbeiter zu erweitern und damit ein vollständiges Bild des betrieblichen IT-Security-Status zu ermitteln. Auf Basis der gewonnen Ergebnisse lassen sich Mitarbeiter gezielt zu Risiken schulen und damit die Resilienz ganzheitlich erhöhen.

Abschirmung und selbstlernende Organisation für mehr Sicherheit in KRITIS

Patrick Leibbrand, Holger Maczkowsky, Kristian Beilke

Forschungsprojekt:
MoSaIK

Synergieeffekte für maximale Sicherheit in KRITIS

Das entwickelte Werkzeug zur modellbasierten Sicherheitsanalyse und der sichere Sensorträger innerhalb der Kritischen Infrastruktur (Security Appliance Web) ergänzen einander in der Anwendungspraxis ideal, können jedoch auch unabhängig voneinander eingesetzt und anwendungsübergreifend in Kritischen Infrastrukturen diverser Ausprägung implementiert werden. Während das Modellierungswerkzeug für unterschiedlichste Kritische Infrastrukturen die Ermittlung des Sicherheitslevels unter frei definierbaren Randbedingungen erlaubt und sofortige Rückschlüsse im Fall einer Veränderung dieser Parameter zulässt, sorgt der sichere Sensorträger für einen kontinuierlichen Zustrom vom Realdaten aus dem Produktivbetrieb Kritischer Infrastrukturen. Diese Daten verbessern die dem Werkzeug zugrundeliegenden Modelle fortlaufend, sodass Aussagen mit immer weiter gesteigerter Richtigkeit und Präzision zu erwarten sind. Zugleich bleiben die Kritischen Infrastrukturen selbst bezüglich ihrer informationstechnischen Anbindung an das offene Internet jederzeit vor Angriffen über das zentrale Einfallstor des Webbrowsers zuverlässig geschützt – auch wenn konventionelle Schutzmechanismen bei neuartigen Angriffsmustern versagen.

Den Aufbau einer adäquaten Datenhaltung vorausgesetzt, können Betreiber von KRITIS sektor- und standortübergreifend wechselseitig von Erfahrungen und Erkenntnissen in Bezug auf bekannte und neuartige Bedrohungen profitieren. Der Datentransfer könnte zukünftig überdies automatisiert erfolgen, wodurch große Flexibilität bei kurzen Reaktionszeiten und vergleichsweise geringem manuellem Aufwand erreichbar wäre.

Werkzeugbeschreibung

Das Werkzeug zur Unterstützung der Risikoanalyse verwendet professionelle Open-Source-Rahmenwerke als technische Plattform. Die Grundlage bildet JetBrains Meta Programming System (MPS). MPS ist eine Entwicklungs- und Laufzeitumgebung für domänenspezifische Sprachen (Domain Specific Languages, DSL). Alle Elemente einer Sicherheitsanalyse werden im Werkzeug in speziell entwickelten DSLs erfasst und bearbeitet. Dabei kommen für die unterschiedlichen Aspekte einer Analyse, wie z. B. Systemarchitektur oder Funktionshierarchie, verschiedene DSLs zum Einsatz, die flexibel ausgetauscht, erweitert und um weitere DSLs ergänzt werden können. Die Modelleditoren arbeiten projizierend, d. h., unterschiedliche Syntaxen werden kombiniert in einer vereinheitlichten Sicht bearbeitet, z. B. als Tabellen, Formulare, Text und Grafiken. Dies ermöglicht sehr hohe Freiheitsgrade in der Anpassung des Werkzeugs, ohne dass der Endnutzer dadurch beeinträchtigt wird. Konkret ist es möglich, dokumentierte Schutzziele, Bedrohungen, Schutzmaßnahmen und Risiken neben einer textuellen auch in einer tabellarischen Syntax darzustellen.

Anwendungsszenario des Werkzeuges

Der Sicherheitsspezialist erstellt mithilfe des Werkzeuges in Absprache mit den Fachverantwortlichen eines Kritischen-Infrastruktur-Betreibers eine Risikoanalyse. Im Dialog werden Anpassung an die konkreten Gegebenheiten und die Umgebung in der Modellierung erfasst sowie eine Überprüfung der Schadensklassen und -kriterien durchgeführt. Dem schließt sich eine Anpassung der Funktionen an. Diesen wird wiederum ein konkretes Schadenspotentzial zugeordnet, welches die Fachverantwortlichen realistisch einschätzen können, da mit dem Verletzen von Schutzzielen von Funktionen klare Vorstellungen über den potentziellen Schaden verbunden sind. Die Übertragung dieser Schäden auf die tatsächlichen IT-Komponenten und Daten wird entsprechend der Methode vom Werkzeug berechnet. Der Sicherheitsspezialist ordnet die relevanten Bedrohungen den Komponenten und Daten zu und bestimmt den benötigten Angriffsaufwand, den er durch sein Fachwissen beurteilen kann. Daran schließt sich die Analyse der Risiken an. Somit ergibt sich eine erste Bewertung der vorhandenen Risiken für den Betreiber. Bereits vorhandene, aber auch geplante Maßnahmen werden in das Modell integriert. Dadurch lassen sich die Risiken mit und ohne Maßnahmen darstellen und ihre Wirksamkeit kann einfach visualisiert werden. Somit ergibt sich eine Lageeinschätzung, aufgrund derer weitere Maßnahmen beurteilt werden können. Das Ergebnis wird beispielsweise wie in Abbildung 1 dargestellt.

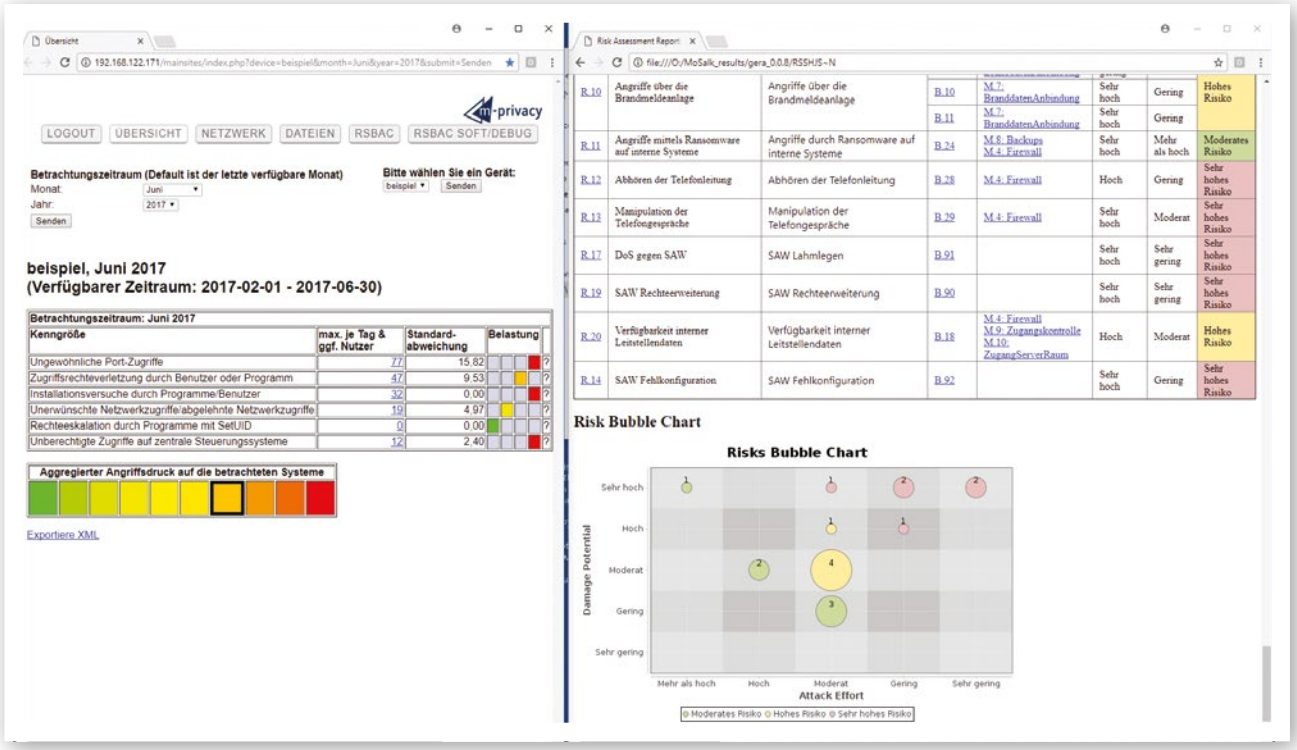


Abb. 1: Kenngrößen vom Sensorträger sowie Risikodarstellung als Export aus dem Werkzeug

Das so entstandene Modell der Risikoanalyse wird dann um Sensordaten erweitert. Diese bieten die Möglichkeit, durch laufende Aktualisierungen Änderungen in der Bedrohungslage direkt in das Modell einfließen zu lassen. Damit können Risiken, die sich in ihrer Bewertung verändern, festgestellt werden. Somit ist auch eine zeitnahe Reaktion durch weitere Maßnahmen umsetzbar.

Modellierungswerkzeug: Weiterentwicklung und Praxiseinsatz

Ziel des zu entwickelnden Werkzeugs ist es, eine modellbasierte Sicherheitsanalyse Kritischer Infrastrukturen entsprechend definierbarer Parameter zu liefern. Es könnte zukünftig quasi zur Simulation des Sicherheitsverhaltens Kritischer Infrastrukturen unter variablen Betriebszuständen und Bedrohungsszenarien dienen. Dies kann im Fall der Neukonzeption einer KRITIS entscheidende Hinweise auf verbleibende Sicherheitslücken liefern, die noch vor Fertigstellung der betreffenden Anlagen bereits im Systemdesign behoben werden könnten. Weiterhin könnte ein solches Werkzeug zur Optimierung bestehender KRITIS dienen, wobei auch unter betriebswirtschaftlichen Gesichtspunkten Maßnahmen im Hinblick auf technisch-organisatorische Wirksamkeit und Kosteneffizienz systematisch evaluiert werden könnten.

Nicht zuletzt unterliegen Kritische Infrastrukturen einem steten Wandel infolge technischer Fortschritte und veränderter Anforderungen. Eine Veränderung kann jedoch Einfluss auf das Sicherheitsniveau der Infrastruktur nehmen, dies gilt insbesondere für den Sektor Informationstechnik und Telekommunikation als Querschnittbereich. Es ist ohnehin davon auszugehen, dass sich die Sicherheit Kritischer Infrastrukturen zukünftig maßgeblich über die Sicherheit ihrer IT-Systeme und -Netzwerke definieren wird, während anthropogene Gefahren durch physisch-manuelle Einflussnahme an Bedeutung verlieren dürften.

Vor diesem Hintergrund erlangt die Option eines kontinuierlichen, werkzeugbasierten Monitorings des Sicherheitsniveaus Kritischer Infrastrukturen besondere Praxisrelevanz.

Eine Besonderheit der modellbasierten Analyse liegt im Fall des Verbundprojekts MoSaIK in der Verfeinerung der zugrunde liegenden Modelle durch in der Betriebspraxis erhobene Realdaten. Über längere Zeiträume betrachtet entstünde in einer späteren Implementierung so ein sehr großer Kompetenzfundus, der vielfältig nutzbar ist. Modellbasierte Werkzeuge mit fortlaufend aktualisiertem, datenbasiertem Hintergrund hätten gegenüber manuellen Analysen den Vorteil, umfassendes Praxiswissen lückenlos zu verdichten und damit Sicherheitsexperten optimal zu unterstützen.

Security Appliance Web: Routineeinsatz mit Mehrfachnutzen

Die zur sicheren Messdatengewinnung eingesetzte Komponente in Form der Security Appliance Web könnte in Zukunft zur Routineausstattung der IT-Umgebung einer jeden Kritischen Infrastruktur gehören. Sie schirmt deren interne Netzwerke weitgehend vom Internet ab und sorgt dennoch für Nutzbarkeit des Internets auch in Bereichen mit hohem Schutzbedarf – beispielsweise infolge enger und nicht in jedem Fall entflechtbarer Kopplung von Verwaltungs- und Steuersystemen. Entsprechende Implementierung vorausgesetzt, verhält sich die Security Appliance Web dabei weitgehend transparent und beeinflusst weder technische noch organisatorische Prozesse des Produktivbetriebs in nennenswertem Umfang. Zugleich ermöglicht die Security Appliance Web als sicherer Sensorträger die Implementierung bewährter und neuartiger Sensoren zur Datengewinnung hinsichtlich Angriffsdruck und Angriffswegen.

Zukünftig könnte die Datenaggregation in standardisierten Formaten und in zentralen Datenbanken erfolgen. Auf diese Weise stünden die betreffenden Daten für sämtliche Betreiber Kritischer Infrastrukturen unterschiedlicher Sektoren zum Abruf bereit.

Vor Ort installierte Modellierungswerkzeuge könnten darauf zurückgreifen und damit quasi in Echtzeit praktische Erfahrungen aus Kritischen Infrastrukturen anderer Sektoren, anderer Branchen und anderer Standorte in die eigenen Sicherheitsbetrachtungen integrieren.

Über den sicheren Sensorträger Security Appliance Web erfolgt ein zuverlässiger Schutz Kritischer Infrastrukturen vor akuten Bedrohungen aus dem Internet. Zusammen mit dem modellgetriebenen Analysewerkzeug und einer zentralen Datenhaltung ließe sich das Sicherheitsmanagement Kritischer Infrastrukturen um eine Art selbstlernenden Kompetenzpool ergänzen. Betreiber Kritischer Infrastrukturen könnten ihre Anlagen und Systeme a priori sicher konzipieren, diese fortlaufend sicherheitstechnisch optimieren und im Fall besonderer Bedrohungen zeitnah und synchron reagieren.

Praktische Umsetzung - Auditierungs- und Zertifizierungskonzept für Hafentelematiksysteme

Nils Meyer-Larsen, Rainer Müller, Karsten Sohr, Annabelle Vöge

Forschungsprojekt:
PortSec

Die Software-Security ist ein wichtiges Thema, wie die Vielzahl von aktuellen, zum Teil in der Presse diskutierten Vorfällen belegt. Vor allem sicherheitskritische Spezialanwendungen und ihre Schnittstellen zu Standard- oder Altsoftware müssen systematisch abgesichert werden. Hafentelematiksysteme sind durch die Vielzahl der verbundenen Systeme und interagierenden Partner exponiert, was diese Systeme grundsätzlich besonders gefährdet. Die regelmäßige sicherheitstechnische Überprüfung aller Systemkomponenten bedeutet einen hohen Aufwand für deren Betreiber.

Daher ist die dbh Logistics IT AG ebenfalls zentral am Verbundprojekt beteiligt – sie entwickelt und betreibt unter anderem die Hafentelematik- und Port-Community-Systeme für die Bremischen Häfen (Bremen und Bremerhaven) sowie den Jade-Weser-Port in Wilhelmshaven. Das Unternehmen ist bereits nach dem IT-Qualitätsstandard ISO 27001 zertifiziert, möchte aber noch einen Schritt weitergehen, denn eine aktive Suche nach Schwachstellen in der Software ist noch kein geforderter Bestandteil der internationalen Norm. Im Rahmen des Projekts will die dbh dieses Thema angehen und dabei untersuchen, wie werkzeugunterstützte Risikoanalysen von Software in das ISO-27001-Rahmenwerk eingebunden werden können.

PortSec trägt dazu bei, Sicherheitslösungen zu entwickeln, die eine Automatisierung entsprechender Überprüfungen ermöglicht. Hierdurch wird der Aufwand für regelmäßige sicherheitstechnische Überprüfungen der Systemkomponenten von Hafentelematiksystemen deutlich optimiert, sodass die Systeme mit geringerem Aufwand noch häufiger und gründlicher überprüft werden können.

Nach Projektende werden die im PortSec-Projekt als Demonstratoren erarbeiteten Sicherheitswerkzeuge nach entsprechender Weiterentwicklung einsatzfähig sein und für die praktische Anwendung zur Verfügung stehen. Weiterhin wird der PortSec-Ansatz hinsichtlich seiner Übertragbarkeit auf andere Technologien (z. B. Programmiersprachen) und Branchen (z. B. andere Bereiche der Logistik) geprüft.

Branchenspezifischer Sicherheitsstandard

Das seit Juli 2015 gültige Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) ist die konsequente Weiterentwicklung des Bestrebens der Bundesregierung, die IT-Systeme und digitalen Infrastrukturen Deutschlands zu den sichersten weltweit zu machen. Insbesondere im Bereich der Kritischen Infrastrukturen hätte ein Ausfall oder eine Beeinträchtigung der Versorgungsdienstleistungen dramatische Folgen für Wirtschaft, Staat und Gesellschaft in Deutschland. Die Verfügbarkeit und Sicherheit der IT-Systeme spielt somit, speziell im Bereich der Kritischen Infrastrukturen, eine wichtige und zentrale Rolle.

Das IT-Sicherheitsgesetz ermöglicht Betreibern Kritischer Infrastrukturen und deren Branchenverbänden, gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) branchenspezifische Sicherheitsstandards zu definieren. Aufbauend auf den Ergebnissen aus PortSec wird ein branchenspezifischer Sicherheitsstandard für Hafentelematiksysteme (maritimer Transport und Verkehr) entwickelt, der dem IT-Sicherheitsgesetz genügt. Wesentlich hierbei ist die Kompatibilität mit ergänzenden Standards. Geplant ist die Entwicklung von normativen Kontrollen, die – ähnlich wie der Annex A der ISO/IEC 27019 – als Ergänzung zu einer bestehenden ISO/IEC-27001-Zertifizierung Berücksichtigung finden. Der Sicherheitsstandard wird mit dem BSI sowie relevanten Branchenverbänden abgestimmt. Er besteht aus einem Auditierungsschema, welches unter anderem Prüfumfang, -tiefe und -methoden definiert, sowie einen Zertifizierungsschema, welches die Prozesse für einen mehrstufigen Zertifizierungsprozess vorgibt und den Lebenszyklus von Zertifikaten, Auditoren und Prüfstellen definiert. Dies ist besonders wichtig, da das IT-Sicherheitsgesetz für alle Betreiber von Kritischen Infrastrukturen einen Nachweis über die Erfüllung aller Anforderungen fordert und dabei explizit die Möglichkeit von Sicherheitsaudits und Zertifizierungen vorsieht.

Im Rahmen von PortSec wird ein Auditierungs- und Zertifizierungskonzept entwickelt werden, das alle vorangegangenen PortSec-Ergebnisse berücksichtigt und dabei für alle Betreiber von Kritischen Infrastrukturen im Bereich des maritimen Transports und Verkehrs Anwendung finden kann.

Die Managementlösung PREVENT in der Banken-IT

Torsten Bollen, Steffi Rudel

Forschungsprojekte:
PREVENT & VeSiKi

Die Managementlösung PREVENT als umfassendes Framework wird in Zukunft über Dash-Boards verschiedenste Informationen zur Verfügung stellen. So wird jeder Nutzer die für seine Tätigkeiten angepasste Sicht auf die PREVENT-Datenbasis erhalten. Vorstellbar sind aktuell Ansichten für:

- Administratoren
- IT-Sicherheit
- Compliance Officer
- Management

In einem späteren Schritt soll PREVENT Handlungsempfehlungen geben, um Entscheidungen präziser und schneller zu treffen.

Wegen der Komplexität der Daten und der sich daraus ergebenden Fragestellungen erarbeitet das PREVENT-Konsortium einen Demonstrator. Auf Basis von Testdaten und eigens erarbeiteten Testfällen wird die Leistungsfähigkeit der Managementlösung PREVENT gezeigt. Aus der Demonstrator-Umgebung werden für eine spätere Detailplanung bei Kunden (Banken) ebenfalls Erkenntnisse gesammelt.

Das Framework richtet sich nicht ausschließlich an Finanzdienstleister. Vielmehr kann PREVENT überall dort eingesetzt werden, wo ein sicherer IT-Betrieb zwingend erforderlich ist (KRITIS-Umfeld).

Fallstudie IT-Sicherheit für Geschäftsprozesse im Finanzsektor

Zusammen mit dem Begleitforschungsprojekt VeSiKi wurde eine Fallstudie erstellt, welche die Managementlösung PREVENT vorstellt [1]. Dabei wird anhand eines Szenarios die Implementierung der Managementlösung PREVENT in einem fiktiven Unternehmen (FutureBank unter Beteiligung des FutureRZ als Dienstleister) beschrieben.

Die Fallstudie fokussiert sich auf den Prozess des Zahlungsverkehrs, konkret wird als Referenzprozess eine Überweisung innerhalb Deutschlands herausgegriffen, welcher einen typischen Geschäftsprozess darstellt. Die folgende Abbildung 1 zeigt zunächst das Zusammenspiel der Akteure und der Prozesse in der Fallstudie.

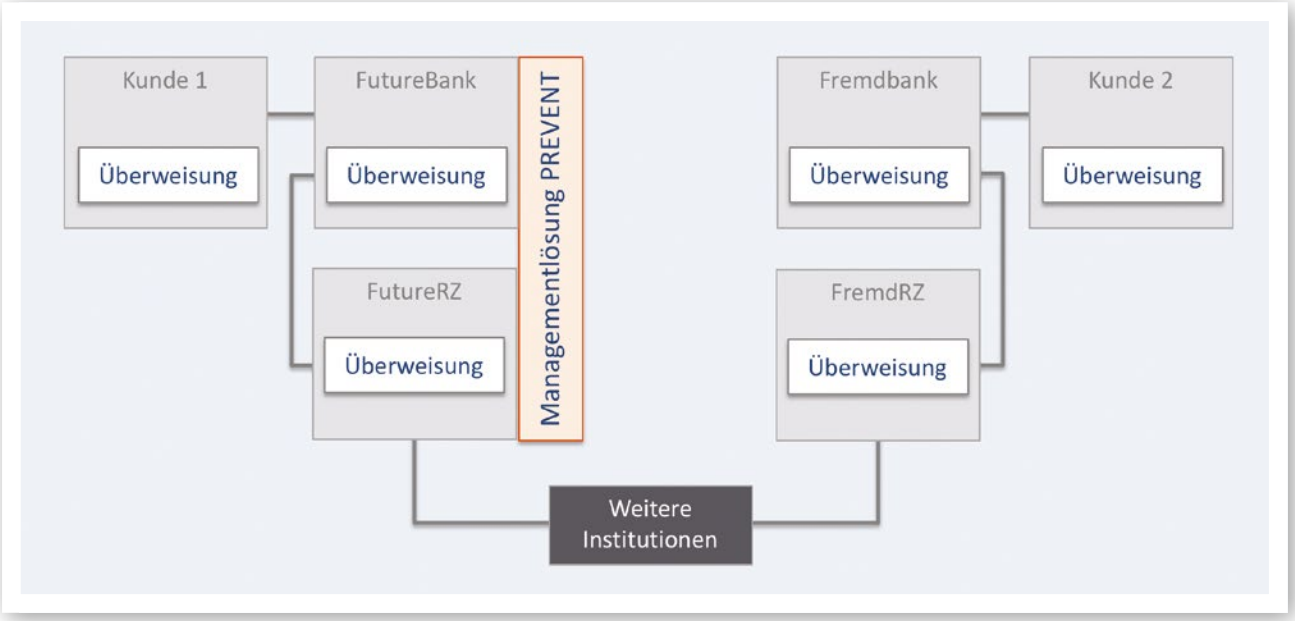


Abb. 1: Zusammenspiel der Akteure und der Prozesse in der Fallstudie

Die Fallstudie betrachtet, wie sich der Ausfall eines Switches (=Netzwerkebene) auf den Überweisungsprozess (=Geschäftsprozess) auswirken könnte. Die folgende Abbildung 2 illustriert, wie dies bis hin zum Ausfall des Geschäftsprozesses „Überweisung" führen könnte.

Für eine PREVENT-Installation beim Kunden bedeutet dies die Notwendigkeit einer engen Zusammenarbeit, nur so können die komplexen Anforderungen zielführend in PREVENT abgebildet werden.

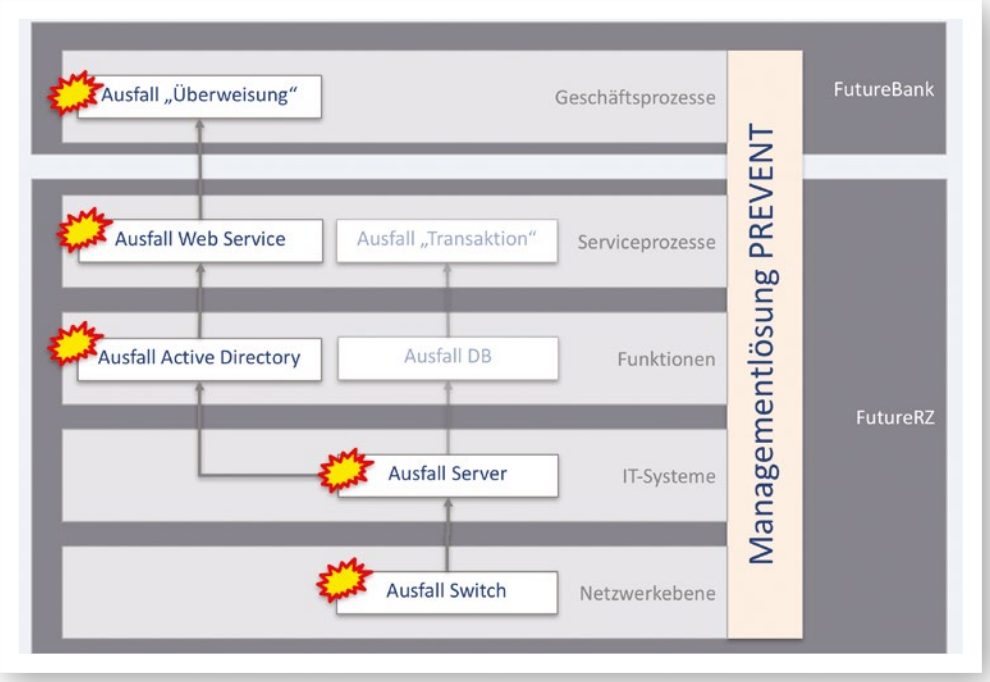


Abb. 2: Auswirkung eines Ausfalles des Switches über die verschiedenen Ebenen

Für weitere Details sei an dieser Stelle auf die Fallstudie verwiesen, welche im Rahmen des Förderschwerpunktes „IT-Sicherheit für Kritische Infrastrukturen" in 2018 veröffentlicht wird [1].

Implementierung beim Kunden

Der beschriebene Ansatz verbindet Verhaltensregeln und Risikomanagement mit Echtzeitmessungen, Sicherheitstests und Simulationen von Bedrohungsszenarien. Die Kombination dieser unterschiedlichen Instrumente in einem neuartigen Framework garantiert u. a. eine verbesserte Absicherung von Rechenzentren. Hieraus ergeben sich Vorteile für die nachgelagerten Business-Prozesse der Kunden. So hat sich beispielsweise gezeigt, dass PREVENT dabei hilft, Bedrohungsszenarien im Vorfeld zu erkennen.

Damit ist klar, dass PREVENT keine „Plug and Play"-Lösung ist. Die Realisierung muss als Gemeinschaftsprojekt verstanden und gelebt werden.

Zusammenfassung

Die ersten Projektergebnisse des PREVENT-Konsortiums zeigen, dass die Managementlösung PREVENT helfen wird, die Sicherheit in den Geschäftsprozessen der Banken deutlich zu erhöhen. Gleichzeit hilft PREVENT, die hohen Anforderungen durch Gesetze, Regularien und Compliance zu erfüllen.

Quelle:

[1] Rudel, S., Bollen, T.: IT-Sicherheit für Geschäftsprozesse im Finanzsektor – die Managementlösung PREVENT. In: Lechner, U., Dännart, S., Rieb, A., Rudel, S. (Hrsg.): CASE KRITIS: Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen. Logos-Verlag, 2018, S. 123-135.

RiskViz als Werkzeug zur Erfassung und Erhöhung der IT-Sicherheit Kritischer Infrastrukturen

Matthias Niedermaier, Christoph Moder, Jan-Ole Malchow

Forschungsprojekt:
RiskViz

Äußere Suche

Ein Teil des RiskViz-Forschungsprojekts besteht aus der Bereitstellung einer extern verteilten Suchmaschine. Diese ermöglicht es, nach spezifischen Ports und Protokollen zu suchen und damit industrielle Kontrollsysteme (ICS) zu finden und analysieren. Die Besonderheit besteht darin, dass nicht nur IP-Adressen als Suchbegriffe in die Suchmaschine eingegeben werden können, sondern auch geografische Gebiete, die mithilfe eines Frontends freihändig selektiert oder durch die Eingabe von Postleitzahlen ausgewählt werden können.

Nach einem erfolgreichen Scan werden die Daten mit Informationen über den Besitzer/Eigentümer der IP, der Geokoordinate (Ort), möglichen Schwachstellen/Exploits sowie Wirtschaftsdaten angereichert und anschließend auf einer Karte dargestellt. Diese Darstellung ermöglicht es, umgehend ein Risikolagebild für ganze Regionen oder Länder zu erhalten. Regelmäßige Scans ermöglichen den Aufbau einer Datenbank, die Versicherern Informationen über mögliche Gefährdungen von Firmen zum aktuellen oder einem vergangenen Zeitpunkt nennen können. Dies könnte zum Beispiel ähnlich wie bei der Schufa funktionieren, nur dass Cyberversicherungen anstatt der finanziellen Bonität die „Cyber-Security-Bonität" abfragen würden.

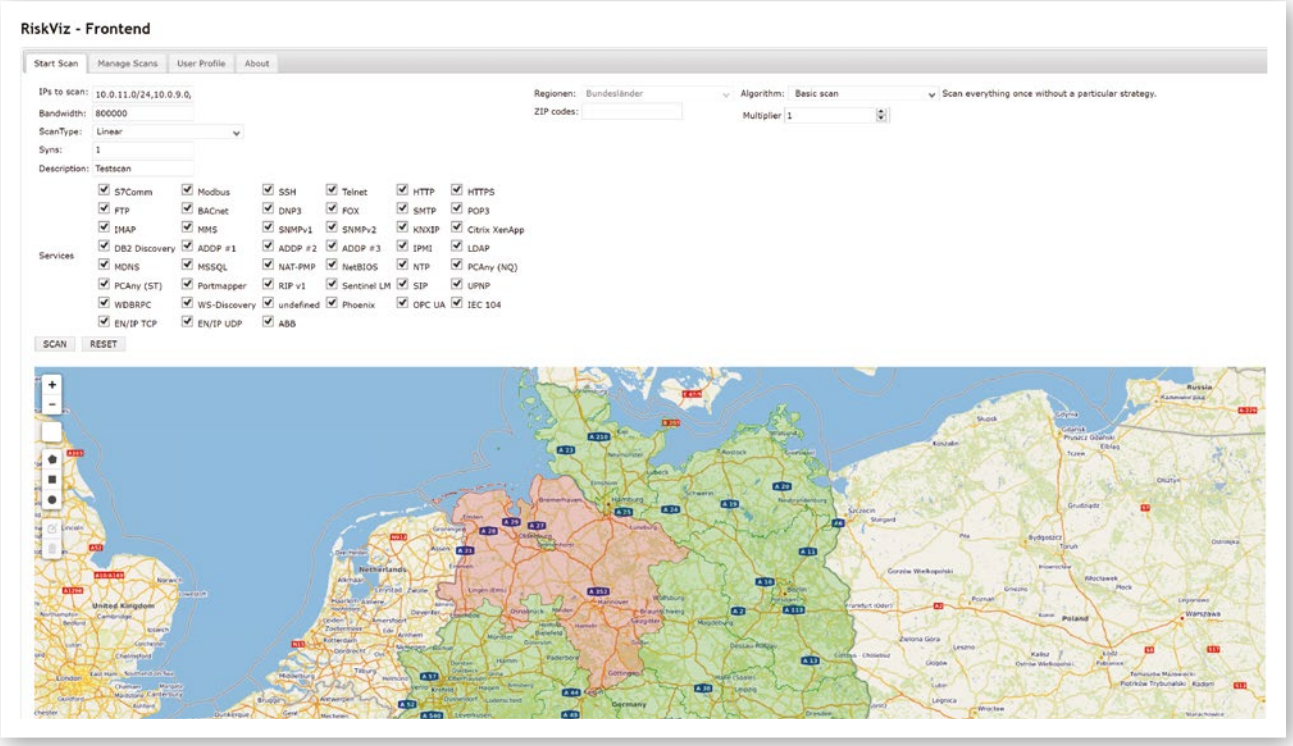


Abb. 1: RiskViz-Frontend: Suchmaske

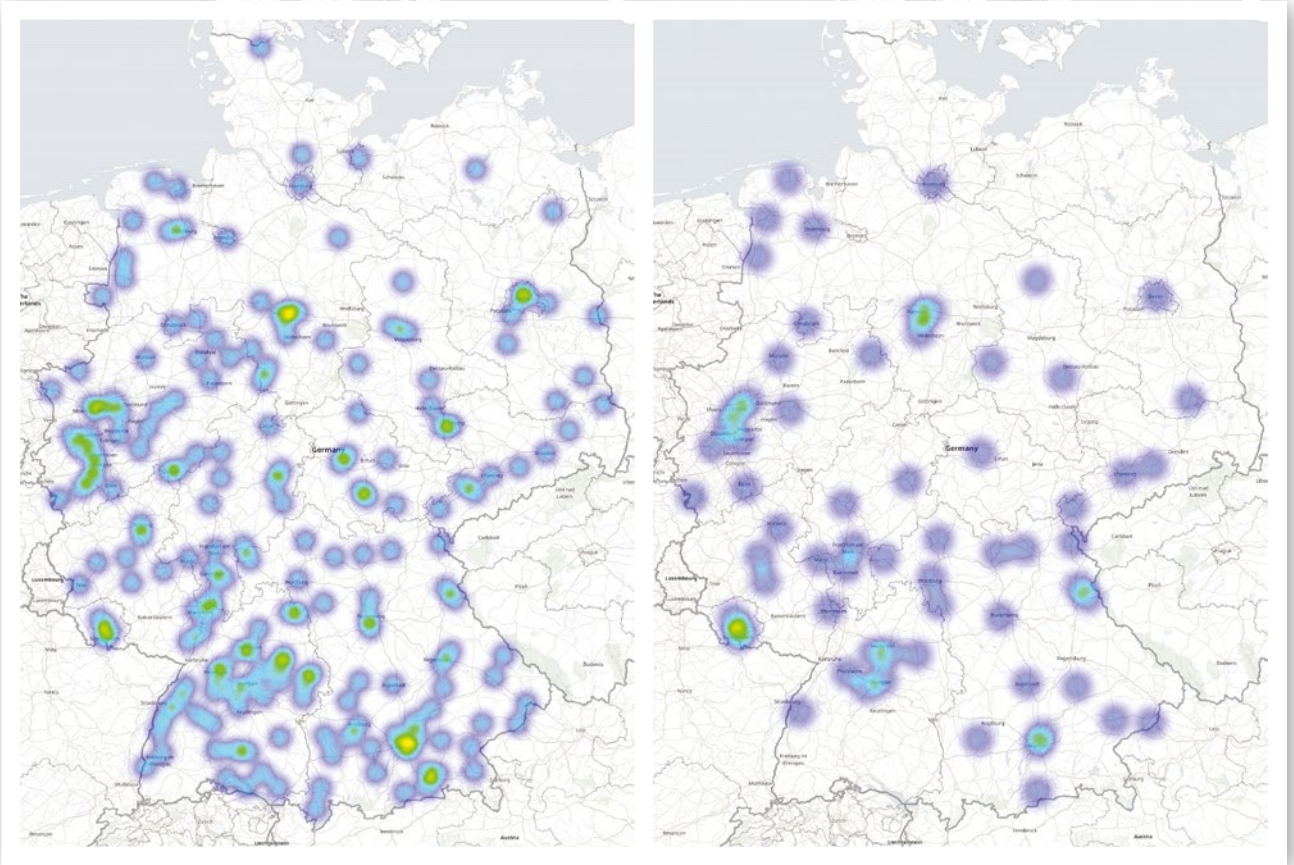


Abb. 2: RiskViz-Frontend: Heatmap der Suchergebnisse (Links: gefundene Geräte/rechts: Geräte mit Schwachstellen)

Abbildung 2 zeigt das Suchergebnis gefundener industrieller Steuerungen (links) sowie die Steuerungen, welche bekannte Schwachstellen aufweisen (rechts). Hierdurch ist anschaulich dargestellt, welche Bedrohungslage aktuell in Deutschland vorliegt.

Innere Suche

Die Suche nach Schwachstellen in industriellen Steuerungen kann nicht nur aus dem Internet, sondern auch direkt aus dem Anlagennetz heraus durchgeführt werden. Dies liefert ein deutlich detaillierteres Bild vom Sicherheitszustand einer Anlage und gibt somit den Betreibern die Möglichkeit, in regelmäßigen Abständen automatisierte Audits ihres Netzwerks durchzuführen.

Konkret wird dabei ein Netz-Sensor in jedes zu überwachende Netzwerksegment integriert, der folgende Aufgaben erledigt:

- Auflistung aller aktiven Netzwerkteilnehmer, inkl. Fingerprinting
- Überprüfung der Software-Versionen der einzelnen Netzwerkgeräte
- Erstellung von Snapshots für den Vergleich von Netzwerkzuständen unterschiedlicher Zeitpunkte
- Logging der Steuerbefehle

Die gesammelten Daten werden verschlüsselt an eine zentrale Stelle übermittelt, wo sie ausgewertet und übersichtlich dargestellt werden. Insbesondere wird überprüft, ob Software-Updates für einzelne Geräte verfügbar sind, ob sich in aktuellen Exploit-Datenbanken Schwachstellen bzw. Exploits für die verwendeten Hardware- und Software-Versionen findet oder ob ein unerwartetes Verhalten im Netzwerk registriert wurde. In diesen Fällen wird sofort eine Warnung an den Betreiber gesendet. Somit erfüllt die Innere Suche einerseits im Schadensfall eine forensische Funktion und kann andererseits im Normalbetrieb z. B. gegenüber einer Versicherung Belege dafür liefern, dass die Anlage nach dem Stand der Technik abgesichert wurde.

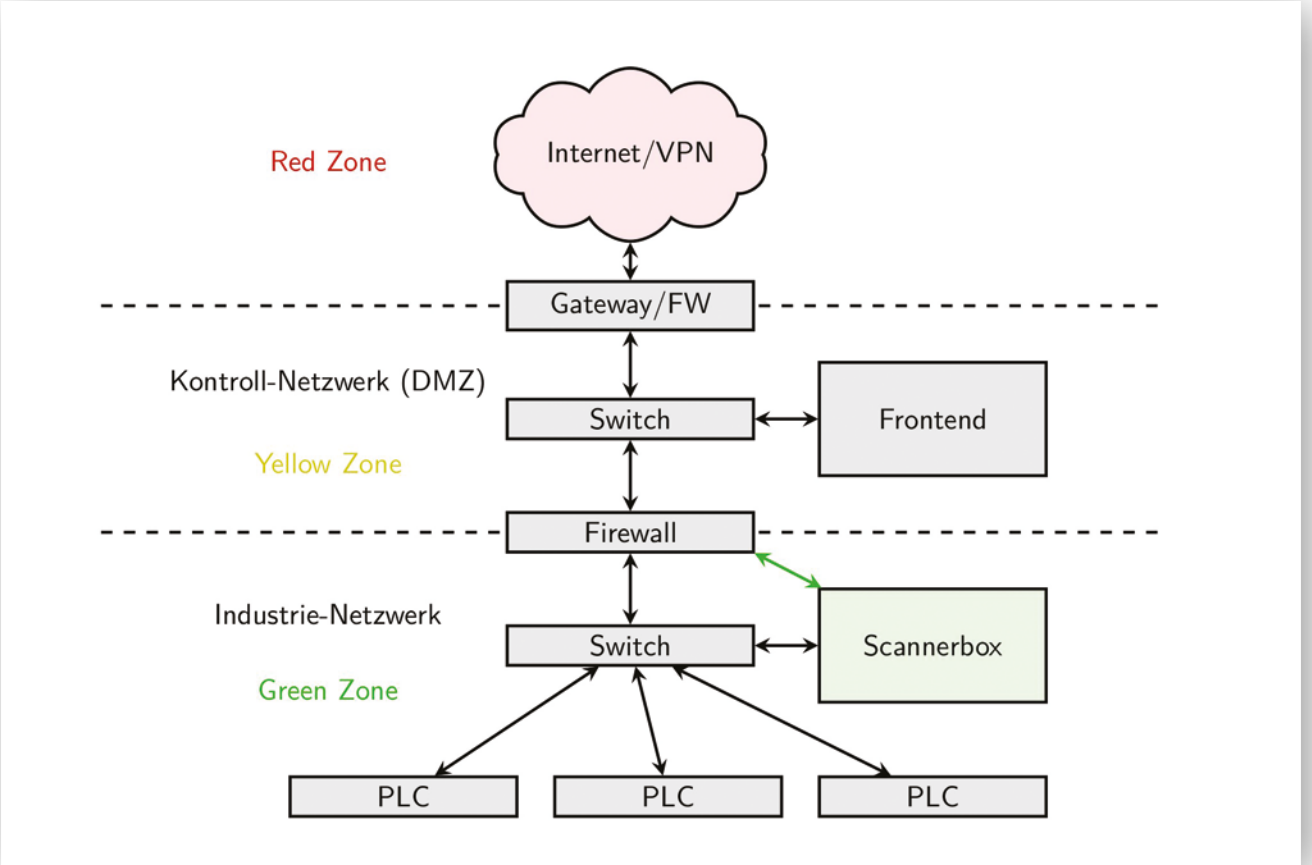


Abb. 3: RiskViz, Interne Scanner, Integration

Da sich die Suchknoten im Anlagennetz befinden, aber auch eine Anbindung nach außen haben, ist eine gute Absicherung unabdingbar. Dazu wurde die Innere Suche stark modularisiert und verwendet einen hochsicheren L4-Microkernel als Plattform. Dieser ermöglicht die strikte Separation der Module und die explizite Freigabe erlaubter Kommunikationsbeziehungen zwischen ihnen. Somit werden potenziell fehlerhafte Softwarebestandteile isoliert und verbotene Informationsflüsse unterbunden. Es gibt weder einen direkten Zugriff von der zentralen Stelle auf das Anlagennetz noch einen Single Point of Failure, bei dessen Ausfall ein derartiger Zugriff möglich wäre.

Anwendungsbeispiel 1: Nutzung der RiskViz-Suchmaschine im Kontinuitätsmanagement einer Firma

In diesem Fall wird die Suche (Innere und Äußere Suche) auf der IP-Range der Firmen-IT durchgeführt. Zunächst liefert das Ergebnis der Suchmaschine ein Lagebild der eventuell. gefährdeten Infrastruktur der Firma. Das Ergebnis muss daraufhin bewertet und eventuell gefundene Schwachstellen beseitigt werden. Einige Probleme werden jedoch oft bestehen bleiben, wie beispielsweise Wartungsverbindungen oder andere Risiken, die nicht zeitnah beseitigt werden können. Klassische Risikoanalysen berechnen lediglich Risiken aus Momentaufnahmen. Das Kontinuitätsmanagement berechnet hingegen zuerst einen monetären Schaden, der aus einem Vorfall entstehen kann. Dies kann bis hin zur Nicht-Einhaltung von Lieferverträgen gehen. Daraus definiert es angemessene Maßnahmen, die greifen, falls eine Schwachstelle zum Problem wird. Es plant Kapazitäten für den Problemfall ein, seien es menschliche Ressourcen, Material oder Budgets, und es definiert auch Notfallpläne. Außerdem nutzt es die Suchmaschine als einen Sensor, denn Änderungen in der IT-Infrastruktur bedingen unter Umständen auch Änderungen im Krisenmanagement einer Firma. Die Ergebnisse der Suchmaschinen dienen dann ebenfalls zur Dokumentation der Nachvollziehbarkeit des ganzen Prozesses des Kontinuitätsmanagements.

Anwendungsbeispiel 2: Risikolagebild des TR-069-Protokolls mithilfe der Äußeren Suche

Am 27. November 2016 kam es deutschlandweit zu Ausfällen der Internetversorgung im Netz der Deutschen Telekom. Ursächlich hierfür war ein sogenanntes Botnetz, welches versuchte über einen Wartungsport (TR-069) an DSL-Routern die Kontrolle über diese zu erlangen. Auf den Routern der Deutschen Telekom war zu diesem Zeitpunkt das Protokoll fehlerhaft implementiert, wodurch die Router vorerst nicht von den Hackern übernommen wurden, sondern es zu Abstürzen und Fehlverhalten kam.

Snapshot-Vergleich erreichbarer Geräte über TR-069-Protokoll vor (links) und nach (rechts) dem Angriff am 27. November 2016 auf Basis der mit RiskViz möglichen Äußeren Suche.

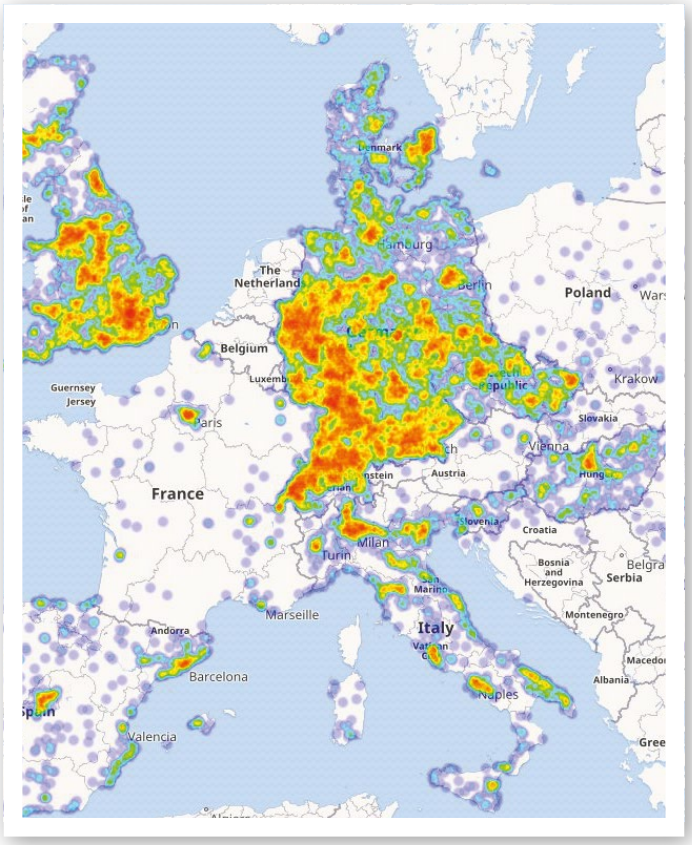


Abb. 4: TR-069 vor dem Angriff

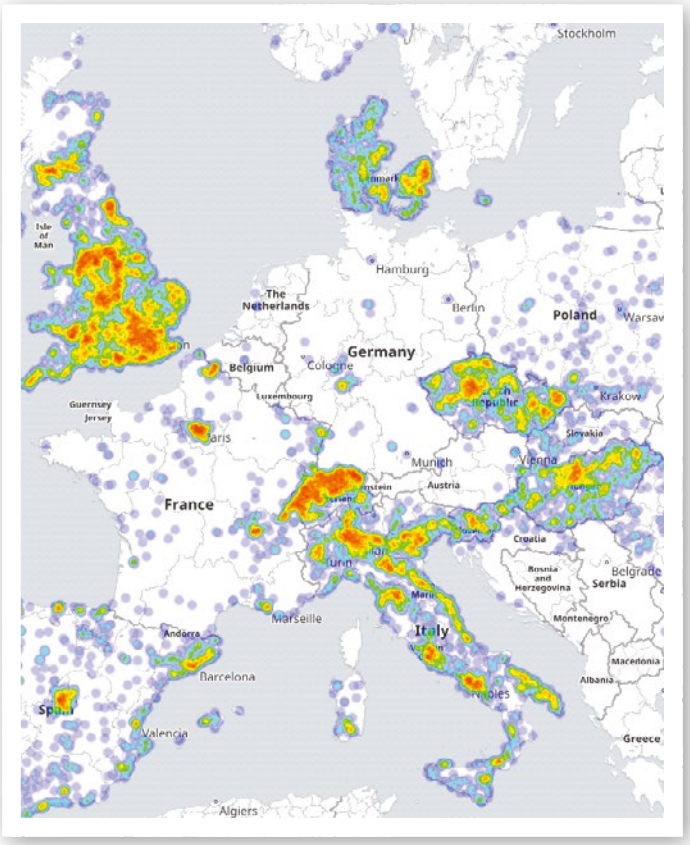


Abb. 5: TR-069 nach dem Angriff

Anwendung des SICIA-Verfahrens in der Praxis – am Beispiel eines ISMS

Franka Schuster, Andreas Paul, Hartmut König

Forschungsprojekt:
SICIA

Wie in Sektion 4 beschrieben, sind die im Verbundprojekt SICIA entwickelten Methoden und Software-Werkzeuge so konzipiert, dass sie entweder die notwendigen Schritte eines Informationssicherheitsmanagementsystems (ISMS) unterstützen (vgl. Abbildung 1) oder ohne das Vorhandensein eines ISMS aufeinander aufbauend ein Verfahren zur systematischen Messung und Bewertung der IT-Sicherheit in kritischen Netzen bilden. Im Folgenden wird die Verknüpfung der Methoden und Software-Werkzeuge mit den Schritten eines ISMS erläutert, woraus jedoch ebenfalls die sukzessive Anwendung der Methoden und Werkzeuge ohne ISMS erkennbar wird.

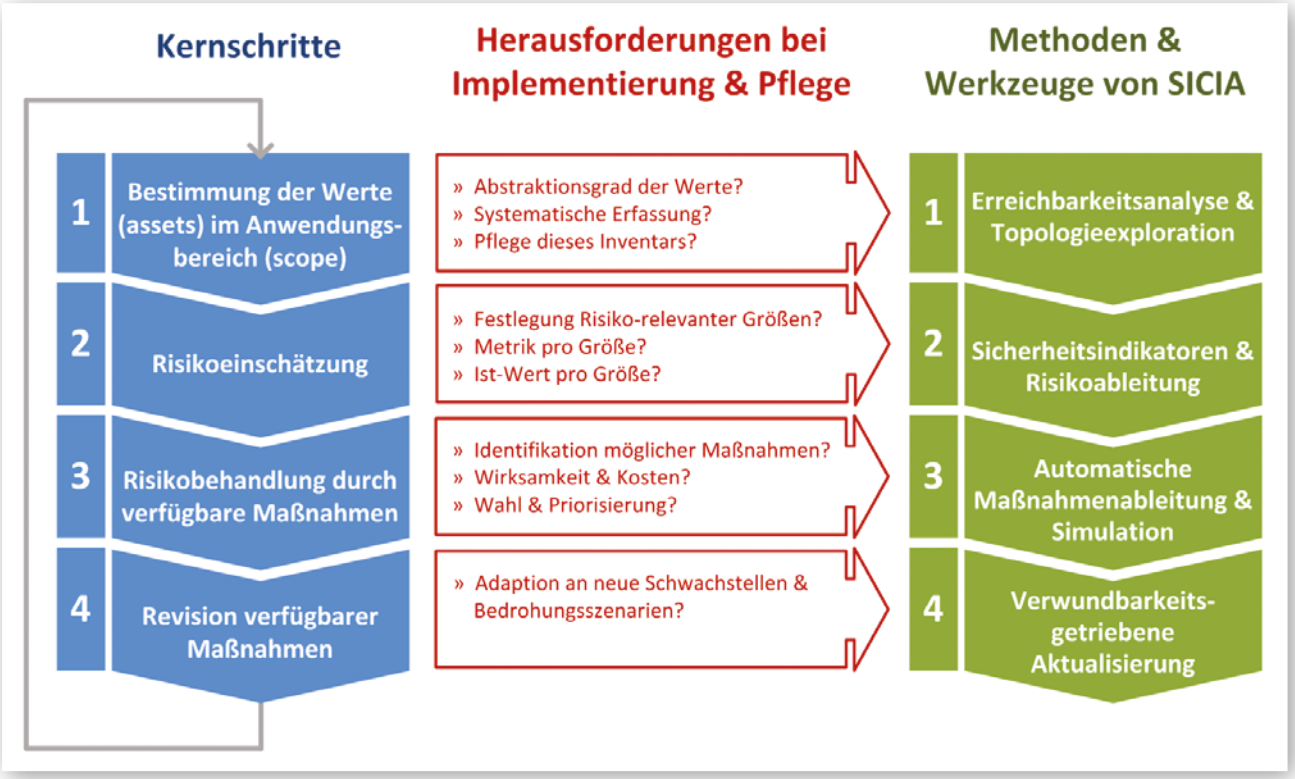


Abb. 1: Methoden und Werkzeuge für die vier ISMS-Schritte

ISMS-Schritt 1: Wertebestimmung im Anwendungsbereich durch Erreichbarkeitsanalyse

Zunächst muss der Bereich, für den die IT-Sicherheit ermittelt und erhöht werden soll, eindeutig durch den Betreiber der Infrastruktur festgelegt und abgegrenzt werden. Ist dieser Anwendungsbereich für das ISMS festgelegt, kann die Erfassung von Komponenten und Systemen durch eine so genannte Erreichbarkeitsanalyse in den zugehörigen Netzsegmenten erfolgen. Dafür wurde in SICIA ein manuelles und automatisiertes Vorgehen entwickelt. Bei der automatisierten Variante wird der Netzverkehr von jedem relevanten Netzsegment für eine gewisse Dauer passiv erfasst und in diesem sichtbare Komponenten und Kommunikationspartner extrahiert. Das Ergebnis wird der vorhandenen Netzdokumentation gegenübergestellt, um einerseits die erfassten Daten zu ergänzen und gleichzeitig eventuelle Abweichungen zwischen dokumentierter und tatsächlicher Netzkonfiguration festzustellen. Ergebnis ist ein Erreichbarkeitsgraph, der im relevanten Bereich alle im Netzverkehr sichtbaren Komponenten mit physischer Vernetzung zu anderen Komponenten enthält (siehe Abbildung 2).

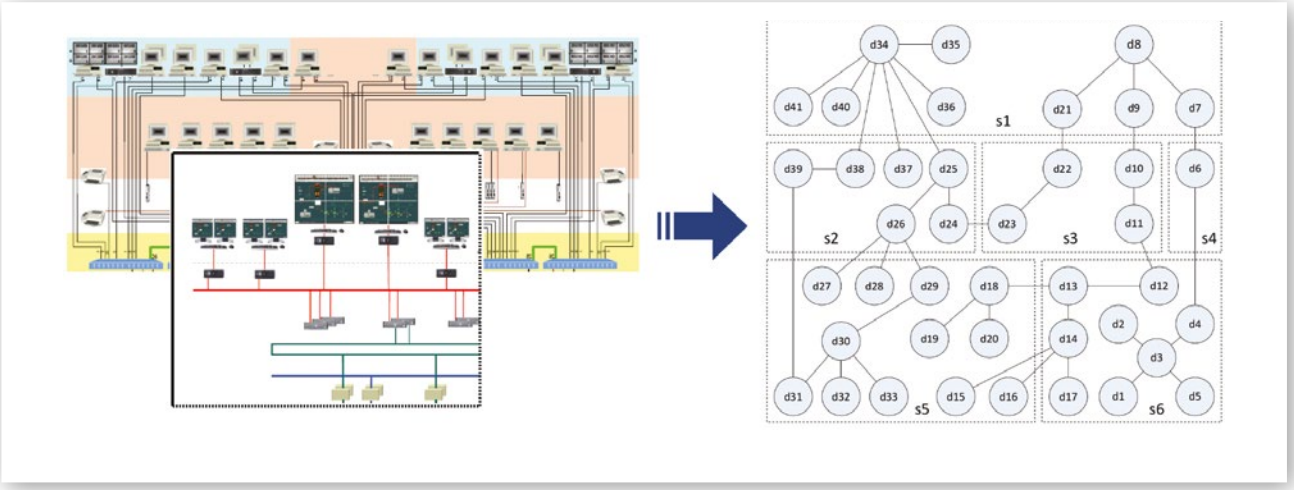


Abb. 2: Ableitung des Erreichbarkeitsgraphen

ISMS-Schritt 2: Sicherheitsbewertung und Risikoeinschätzung mittels Sicherheitsindikatoren

Der zweite Hauptschritt ist die Risikoeinschätzung. Ihr Ziel ist eine systematische Identifikation und Bewertung von Informationssicherheitsrisiken im festgelegten Anwendungsbereich. Ein Informationssicherheitsrisiko wird, wie in Abbildung 3 dargestellt, aus dem Ausmaß eines Schadens und der Wahrscheinlichkeit seines Eintretens ermittelt (vgl. DIN ISO/IEC 27005 [1]). Der Betreiber muss festlegen, auf welcher Betrachtungsebene die Risikoeinschätzung erfolgen soll. Für den, von den Regelungen für die Energieversorgung, geforderten Anwendungsbereich bieten sich Teilsysteme oder Betriebsprozesse an. Zumindest die Bestimmung eines Teils der während der Risikoeinschätzung zu erhebenden Basisgrößen kann durch automatisierbare Methoden unterstützt werden. Schwachstellen und der Grad bereits umgesetzter Sicherheitsmaßnahmen für ein System oder einen Prozess lassen sich aus den Eigenschaften involvierter technischer Komponenten direkt ableiten und auch quantifizieren.

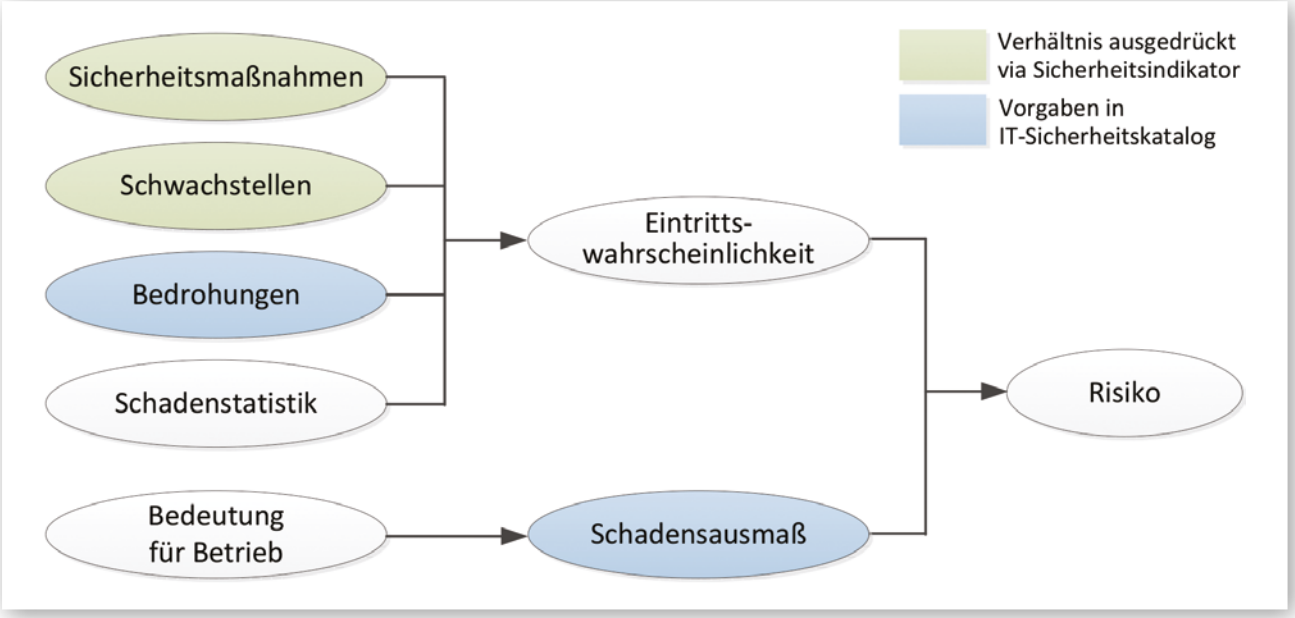


Abb. 3: Größen der Risikoeinschätzung

Dafür werden im Projekt SICIA Methoden mit Softwareunterstützung zur möglichst automatisierten Bewertung des Sicherheitsgrads von Komponenten und Systemen oder Prozessen entwickelt. Zunächst wird die technische Konfiguration von IT-Komponenten erfasst und sicherheitsrelevante Eigenschaften werden auf Zahlenwerte abgebildet. Eventuell auch verknüpft mit organisatorischen Eigenschaften der Komponenten ergeben diese Zahlenwerte den so genannten Sicherheitsindikator der Komponente. Er bildet die IT-Sicherheit der Komponente auf einen Zahlenwert zwischen null und eins ab und drückt aus, zu welchem Grad mögliche Sicherheitsmaßnahmen bei der Komponente umgesetzt sind. Diese Sicherheitsmaßnahmen sind systematisch aus dem Inhalt der Normen DIN ISO/IEC 27002 [2] und DIN ISO/IEC TR 27019 [3] sowie dem ICS-Security-Kompendium des BSI [4] extrahiert. Zudem werden für die Bewertung der Sicherheit von Betriebssystemen und Anwendungen aktuelle Verwundbarkeiten aus internationalen Verwundbarkeitsdatenbanken hinzugezogen. Demzufolge kann mithilfe dieser Messmethode der Betreiber der jeweiligen Infrastruktur für jede IT-Komponente seines technischen Anwendungsbereichs feststellen, ob und zu welchem Maße bei dieser bereits allgemein anerkannte, beziehungsweise verlangte Sicherheitsmaßnahmen umgesetzt sind.

Das Ausdrücken der IT-Sicherheit einer Komponente als prozentualer Wert, ist für eine isolierte Betrachtung nicht geeignet. Es ist jedoch ein starkes Mittel, um in einer komplexen Infrastruktur eine Vergleichsmöglichkeit über eine hohe Anzahl von Komponenten zu schaffen und farblich unterstützt IT-Sicherheit zu visualisieren. Für den Betreiber kann wie in Abbildung 4 eine „Landkarte der IT-Sicherheit“ erzeugt werden, die gleichzeitig eine vollumfängliche sowie differenzierte Betrachtung seiner Anlage ermöglicht. So können auf einen Blick unsichere Komponenten (rot) von teilweise sicheren (gelb) und sehr sicheren Komponenten (grün) unterschieden werden.

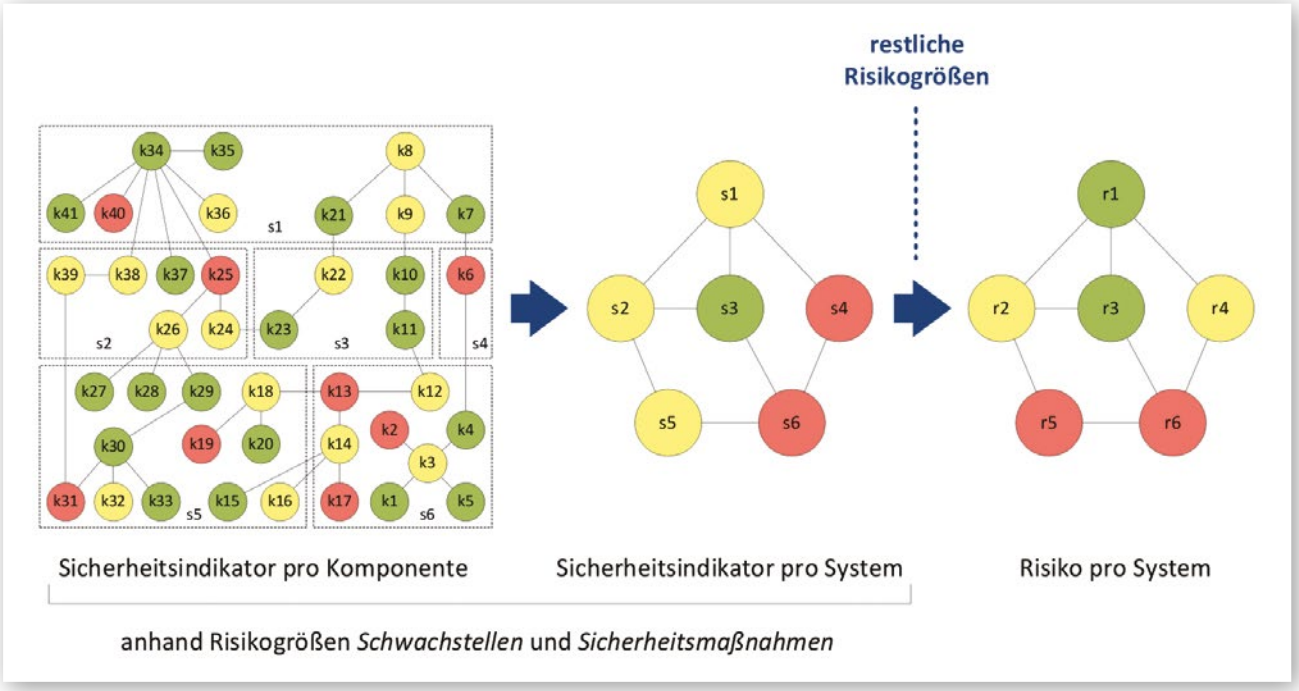


Abb. 4: Von Sicherheitsindikatoren zum Risiko

ISMS-Schritt 3: Risikobehandlung mithilfe Maßnahmenableitung und -simulation

Anhand (1) der Bewertung des Verhältnisses von Schwachstellen zu umgesetzten Sicherheitsmaßnahmen für Komponenten in Form der Komponenten-Sicherheitsindikatoren, (2) der daraus abgeleiteten Sicherheitsindikatoren für Systeme oder Prozesse sowie (3) des pro System oder Prozess aus dem zugehörigen Sicherheitsindikator und den restlichen Größen der Risikoeinschätzung ermittelten Risikos pro System oder Prozess (vgl. Abbildung 4), kann eine gezielte Risikobehandlung erfolgen.

Der in der Risikoeinschätzung ermittelte Erreichbarkeitsgraph mit Risiken der Systeme beschreibt die Risiken beziehungsweise den Sicherheitszustand des Anwendungsbereichs des ISMS vor der gezielten Risikobehandlung. Da bei der Risikoeinschätzung das quantifizierte Schadensausmaß sowie festgelegte Bedrohungen und Schadenstatistiken als Einflussgröße für die Eintrittswahrscheinlichkeit (vgl. Abbildung 3) weitestgehend fixe Größen bei der Ermittlung des Risikos für Systeme oder Prozesse sind, kann eine Verminderung des Risikos praktisch nur durch Umsetzung weiterer Sicherheitsmaßnahmen erfolgen. Da die Informationen über Komponenten und Systeme oder Prozesse, die für die Ermittlung der Sicherheitsindikatoren verwendet wurden, softwarebasiert abgelegt sind, kann diese Datenbasis im Schritt der Risikobehandlung für die automatische Identifizierung möglicher Verbesserungsmaßnahmen genutzt werden. Da auch die Berechnungsmethodik der Sicherheitsindikatoren softwarebasiert vorliegt, kann mit ihrer Hilfe der Effekt möglicher Verbesserungsmaßnahmen simuliert werden (vgl. Abbildung 5).

Wird nach abgeschlossener Risikobehandlung ein aktueller Graph mit umgesetzten Maßnahmen im Anwendungsbereich erzeugt, können beide Graphen durch Gegenüberstellung als grafische Dokumentation der ermittelten Risiken und deren gezielter Behandlung dienen. So können, wie im IT-Sicherheitsgesetz Artikel 3 gefordert, die Einhaltung der kommenden durch den IT-Sicherheitskatalog für Erzeugungsanlagen festgelegten Maßnahmen (mit erwartetem Bezug zu ISMS nach ISO/IEC 27001) dokumentiert und deren positiver Effekt auf die Risiken im System nachgewiesen werden. Neben diesem grafischen Nachweis auf Ebene der Risikoeinschätzung (Systeme oder Prozesse), kann der Betreiber für einen detaillierteren Nachweis auf die Erreichbarkeitsgraphen mit den ermittelten Komponenten-Sicherheitsindikatoren (vgl. Abbildung 5) vor und nach der Risikobehandlung zurückgreifen.

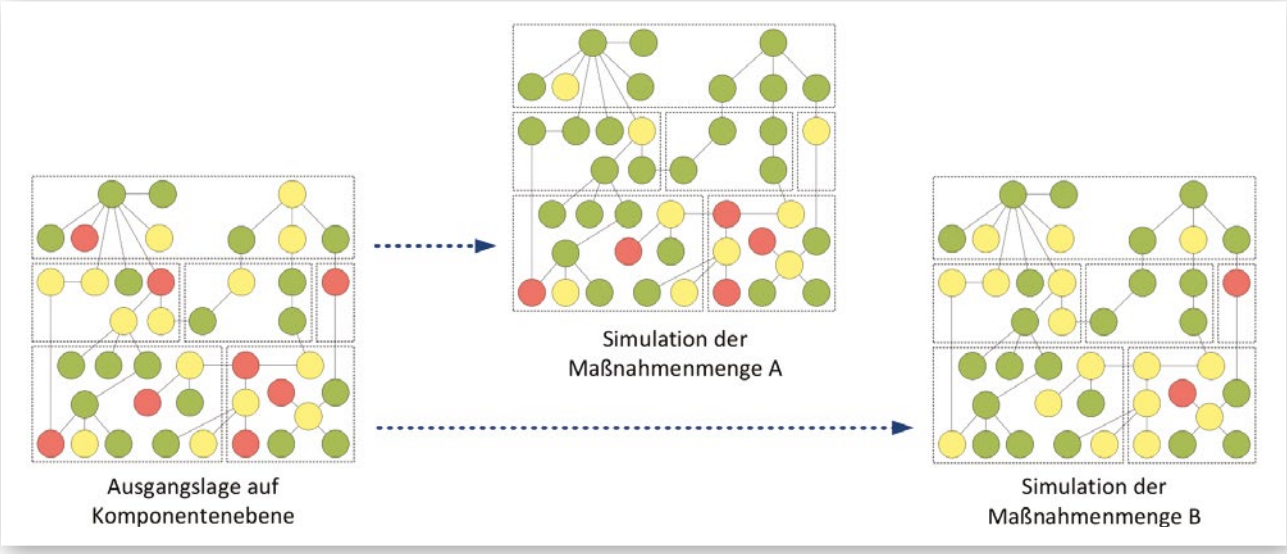


Abb. 5: Simulation verschiedener Maßnahmen(-mengen)

ISMS-Schritt 4: Revision von Maßnahmen

Jede IT-Sicherheitsanalyse steht und fällt mit ihrer Aktualität. Entscheidend bei dem beschriebenen Verfahren ist die Aktualität der Messkriterien. Während sich der Inhalt der zugrunde gelegten Regularien nach einer Konsolidierungsphase nur langsam und relativ geringfügig verändern wird, werden ständig neue Verwundbarkeiten für Betriebssysteme und Anwendungen bekannt werden. Daher ist der Bewertungsprozess so implementiert, dass er stets aktuell bekannte Verwundbarkeiten, die in internationalen Datenbanken zusammengetragen werden, in die Bewertung einbezieht. Auf diese Weise fließen immer alle derzeit bekannten Schwachstellen und der Umsetzungsgrad von Maßnahmen gegen ihre Ausnutzung in die Analyse mit ein.

Quellen

[1] DIN ISO/IEC 27005: Informationstechnik – IT-Sicherheitsverfahren - Informationssicherheits-Risikomanagement.

[2] DIN ISO/IEC 27002: Informationstechnik – IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management.

[3] DIN ISO/IEC TR 27019: Informationstechnik – Sicherheitsverfahren – Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002 .

[4] Bundesamt für Sicherheit in der Informationstechnik: ICS-Security-Kompendium, 2013.

Das SIDATE-Portal im Einsatz

Julian Dax, Sebastian Pape, Volkmar Pipek, Kai Rannenberg,
Christopher Schmitz, André Sekulla, Frank Terhaag

Forschungsprojekt:
SIDATE

Ein Ergebnis des Projektes SIDATE ist das SIDATE-Portal: eine interaktive und interorganisationale Wissensdatenbank und Austauschplattform, die es Betreibern ermöglicht, Erfahrungen untereinander auszutauschen und Gebrauch von vorhandenem Wissen zu machen (siehe Abbildung 1). Das SIDATE-Portal ist an IT-Mitarbeiter von Energienetzbetreibern gerichtet. Es enthält einen Katalog von auf Energienetzbetreiber ausgerichteten IT-Sicherheitsmaßnahmen, eine Fragen- und Antworten-Komponente, eine interaktive Selbstbewertungsfunktion und eine Dokumentensammlung zum Thema IT-Sicherheit bei Energienetzbetreibern.

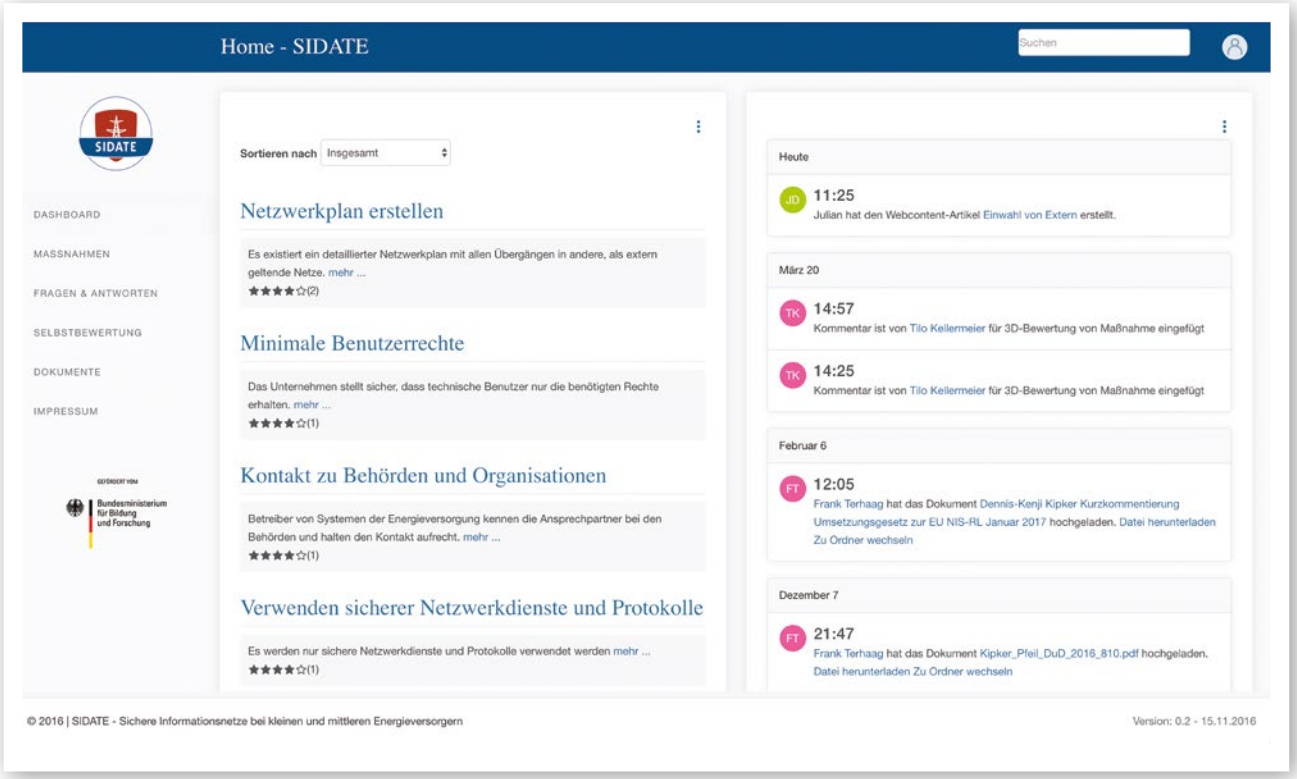


Abb. 1: Dashboard des SIDATE-Portals

Das Portal inkl. IT-Sicherheitsmaßnahmen

Das SIDATE-Portal gibt den Mitarbeitern von Energienetzbetreibern die Möglichkeit, sich unternehmensübergreifend austauschen zu können. Dadurch wird eine nachhaltige Verbesserung der IT-Sicherheit bei den beteiligten Unternehmen erreicht. Im SIDATE-Portal können unterschiedliche IT-Sicherheitsmaßnahmen bewertet und kommentiert werden. So tauschen Portalnutzer ihre Erfahrungen mit diesen Maßnahmen untereinander aus und erlauben es anderen Betreibern, sich vor Einführung einer Maßnahme über mögliche Probleme (z. B. die Verschlechterung der Benutzbarkeit) praxisorientiert zu informieren. Auf diese Weise entstand auf der Plattform eine Sammlung von Best Practices und Nutzer werden bei der Auswahl und Umsetzung von Sicherheitsmaßnahmen unterstützt. Abbildung 2 zeigt den Bereich des Portals, der sich mit den IT-Sicherheitsmaßnahmen beschäftigt.

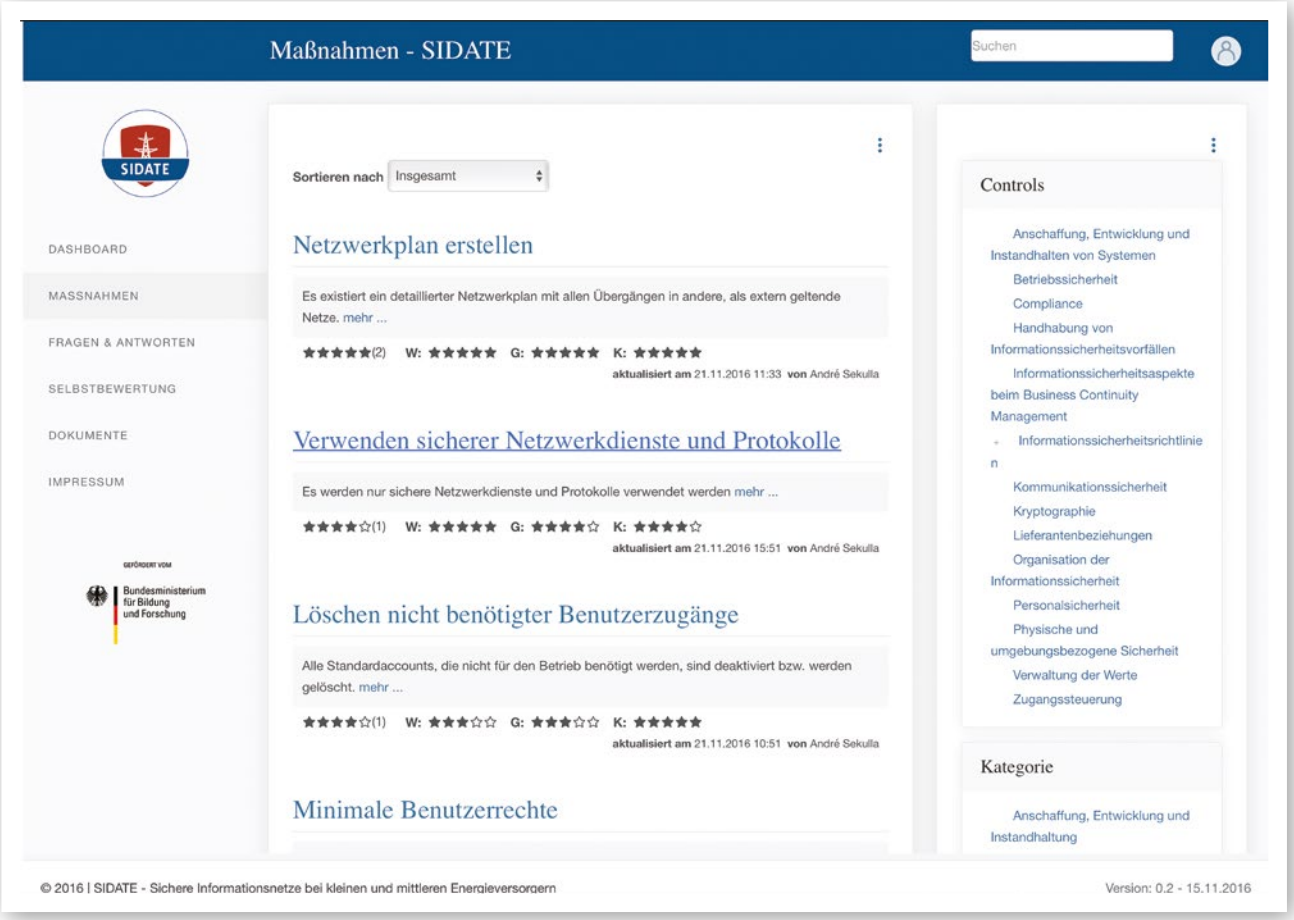


Abb. 2: IT-Sicherheitsmaßnahmen-Katalog im SIDATE-Portal

Bereich für Fragen und Antworten

In einem weiteren Bereich, dem Modul für Fragen und Antworten, stellen die Nutzer eigene Fragen an die Community oder steigen in eine zugehörige Diskussion ein. Hier werden auch Fragen zu den bereits erwähnten IT-Sicherheitsmaßnahmen gestellt. Die beiden Bereiche „Fragen und Antworten“ und „IT-Sicherheitsmaßnahmen“ sind untereinander verlinkt, sodass jeder Nutzer schnell zu einer Maßnahme eine Frage stellen kann oder umgekehrt zu der diskutierten Maßnahme gelangen kann, um detaillierte Informationen einzuholen. Abbildung 3 zeigt auch die Kennzeichnung der Fragen durch mehrere Schlagwörter, um es den Benutzern zu erleichtern, thematisch ähnliche Fragen zu finden.

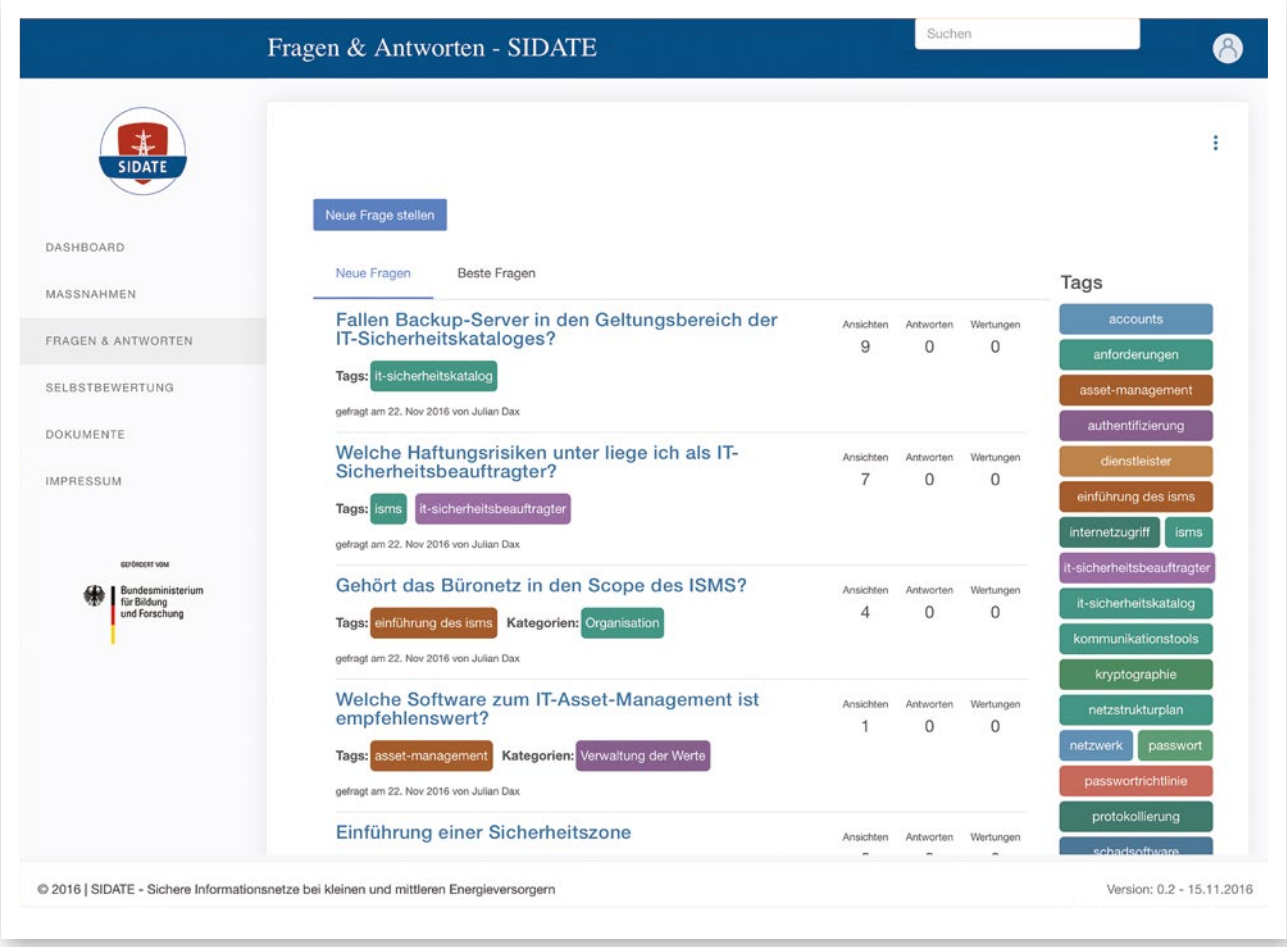


Abb. 3: Modul für Fragen und Antworten im SIDATE-Portal

Selbstbewertungsmodul

Zusätzlich besteht die Möglichkeit, das eigene Unternehmen einer Selbstbewertung zu unterziehen. In diesem Abschnitt des Portals beantworten Nutzer eine Anzahl von Fragen in Bezug auf die IT-Sicherheit im Unternehmen. Als Feedback erhalten sie dann eine Auswertung zur Sicherheit der Kritischen Infrastruktur (siehe Abbildung 4).

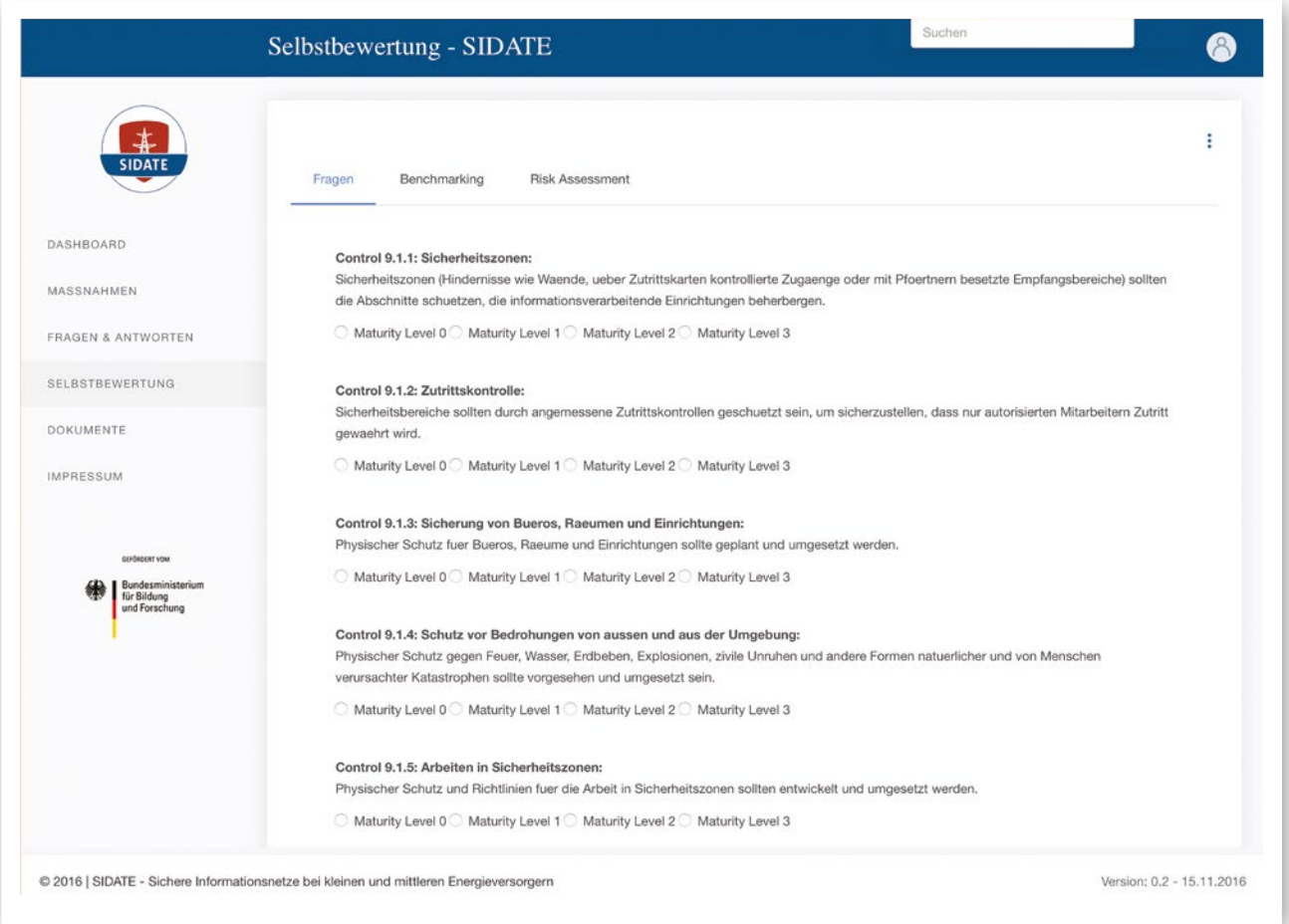


Abb. 4: Selbstbewertungsmodul des SIDATE-Portals

Dokumentensektion

Neben den genannten Modulen des SIDATE-Portals gibt es noch einen Bereich für Dokumente, wie in Abbildung 5 gezeigt. Dort kann der Nutzer Dateien für die Community hochladen bzw. hochgeladene Dateien Anderer herunterladen. Die Dokumentensektion enthält unter anderem Checklisten und Formulare, die bei der Einführung eines ISMS hilfreich sind. Auch hier ist es möglich, die Inhalte zu kommentieren und eine Diskussion zu dem jeweiligen Kontext zu starten.

Zukünftige Arbeiten

Ziel zukünftiger Arbeiten ist es, die Benutzbarkeit des Portals weiter zu erhöhen. Eine Möglichkeit dazu bietet das Selbstbewertungsmodul. So soll einerseits die Eingabe verschiedener Fragen im Stile sozialer Netzwerke in Einzelfragen aufgebrochen und auf verschiedenen anderen Unterseiten erscheinen. Andererseits soll die Auswertungsfunktion des Selbstbewertungsmoduls noch besser mit lückenhaften Eingaben umgehen können. In diesem Zusammenhang soll den Nutzern die Möglichkeit geboten werden, ihre Selbsteinschätzung auf unterschiedlichen Ebenen vorzunehmen, wie beispielsweise Reifegrade einzelner Controls oder Control-Gruppen oder die Angabe, ob einzelne Sicherheitsmaßnahmen im Unternehmen durchgeführt werden.

Ein weiteres Ziel liegt in der Umsetzung und Einbindung eines Feedbacktools. Mithilfe des Tools soll die Auswirkung von eingeführten Sicherheitsmaßnahmen auf die Nutzbarkeit in Form von Benutzerfeedback gesammelt, ausgewertet und in dem SIDATE-Portal hinzugefügt werden.

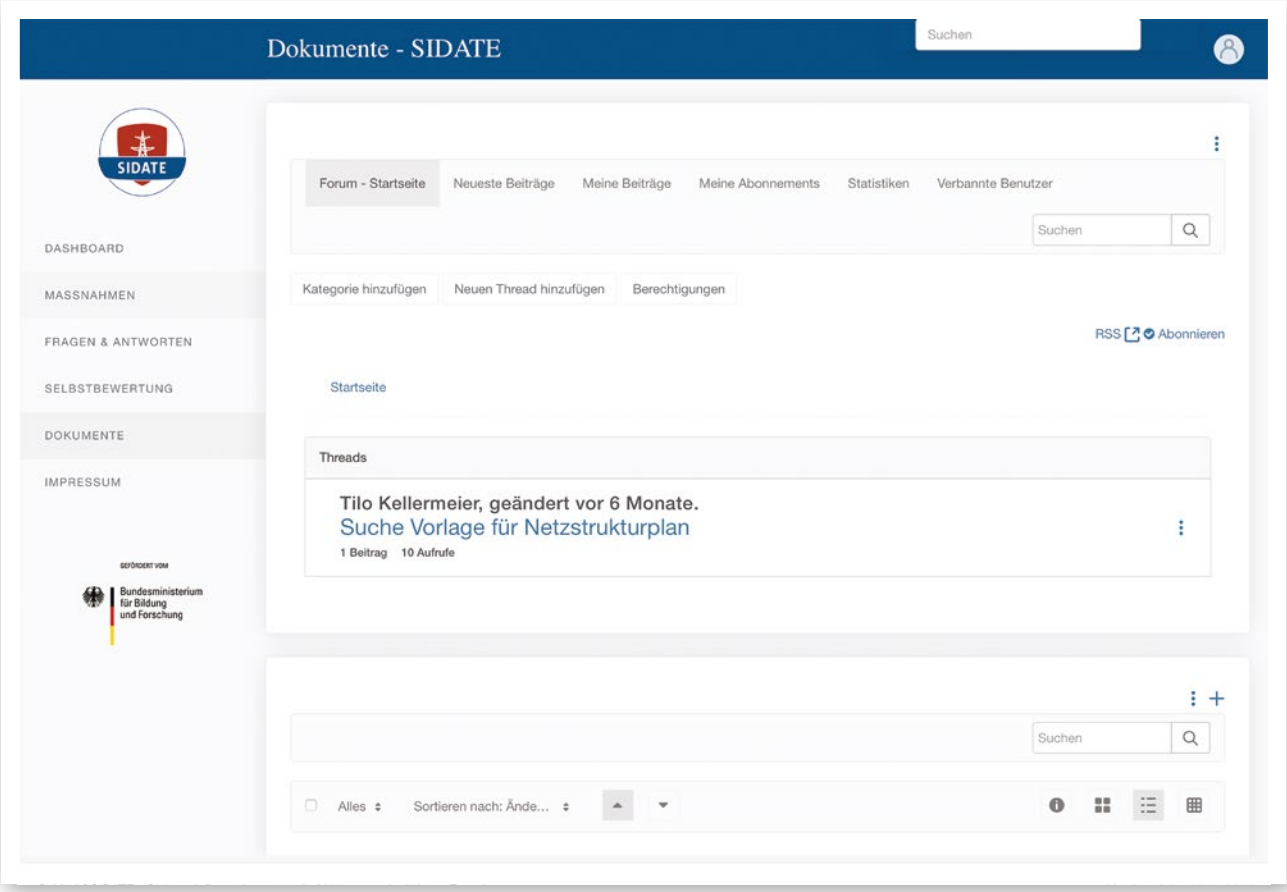
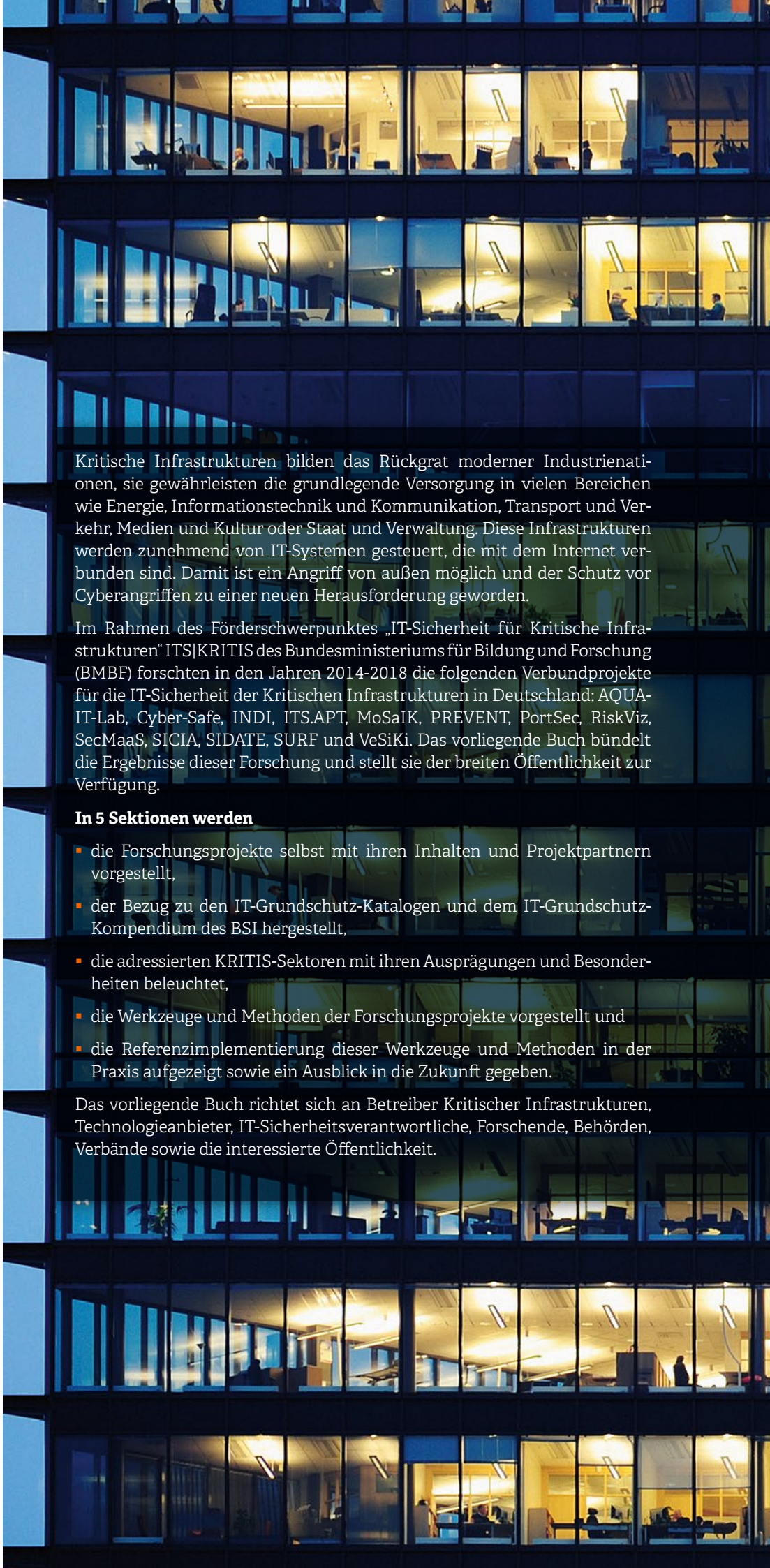


Abb. 5: Dokumentensektion des SIDATE-Portals



Kritische Infrastrukturen bilden das Rückgrat moderner Industrienationen, sie gewährleisten die grundlegende Versorgung in vielen Bereichen wie Energie, Informationstechnik und Kommunikation, Transport und Verkehr, Medien und Kultur oder Staat und Verwaltung. Diese Infrastrukturen werden zunehmend von IT-Systemen gesteuert, die mit dem Internet verbunden sind. Damit ist ein Angriff von außen möglich und der Schutz vor Cyberangriffen zu einer neuen Herausforderung geworden.

Im Rahmen des Förderschwerpunktes „IT-Sicherheit für Kritische Infrastrukturen" ITS|KRITIS des Bundesministeriums für Bildung und Forschung (BMBF) forschten in den Jahren 2014-2018 die folgenden Verbundprojekte für die IT-Sicherheit der Kritischen Infrastrukturen in Deutschland: AQUA-IT-Lab, Cyber-Safe, INDI, ITS.APT, MoSaIK, PREVENT, PortSec, RiskViz, SecMaaS, SICIA, SIDATE, SURF und VeSiKi. Das vorliegende Buch bündelt die Ergebnisse dieser Forschung und stellt sie der breiten Öffentlichkeit zur Verfügung.

In 5 Sektionen werden

- die Forschungsprojekte selbst mit ihren Inhalten und Projektpartnern vorgestellt,
- der Bezug zu den IT-Grundschutz-Katalogen und dem IT-Grundschutz-Kompendium des BSI hergestellt,
- die adressierten KRITIS-Sektoren mit ihren Ausprägungen und Besonderheiten beleuchtet,
- die Werkzeuge und Methoden der Forschungsprojekte vorgestellt und
- die Referenzimplementierung dieser Werkzeuge und Methoden in der Praxis aufgezeigt sowie ein Ausblick in die Zukunft gegeben.

Das vorliegende Buch richtet sich an Betreiber Kritischer Infrastrukturen, Technologieanbieter, IT-Sicherheitsverantwortliche, Forschende, Behörden, Verbände sowie die interessierte Öffentlichkeit.

ITS|KRITIS

VeSiKi

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung