HMD Praxis der Wirtschaftsinformatik
https://doi.org/10.1365/s40702-023-01014-7

SPEKTRUM

Referenzarchitektur Cybersicherheit im Föderalsystem Deutschlands

Thomas Rehbohm · Kurt Sandkuhl

Eingegangen: 11. April 2023 / Angenommen: 5. September 2023

Zusammenfassung Cybersicherheitsarchitekturen sind im Föderalsystem Deutschlands elementarer Bestandteil der digitalen Daseinsvorsorge für Gesellschaft, Wirtschaft und Verwaltung. In Deutschland stehen neben dem Bund alle Länder vor vergleichbaren Herausforderungen, die Akteure ihrer Region dergestalt in eine Architektur einzubinden, dass eine gegenüber Cybersicherheitsbedrohungen resiliente IKT-Infrastruktur entsteht. Sofern die Länder eine harmonisierte Architektur implementiert haben, kann die Gesamtarchitektur im Binnenverhältnis der Länder in kooperativer und komplementärer Zusammenarbeit mit dem Bund und für Europa aufwachsen. Das Ziel der hier vorgestellten Forschungsarbeit ist es, die Verzahnung der systemrelevanten Akteure der regionalen und föderalen Cybersicherheit zu unterstützen und zu vereinfachen. Konkret werden dazu sowohl die inter-organisationalen Prozesse und davon betroffenen Rollen und Organisationseinheiten bei Land, Kommune und Unternehmen der Privatwirtschaft als auch gemeinsam nutzbare Komponenten einer Cybersicherheitsorganisation betrachtet und in Form einer Unternehmensarchitektur dokumentiert, die zu einer Referenzarchitektur weiterentwickelt werden soll. Die Modellierung der Referenzarchitektur in der Modellierungssprache ArchiMate wird in Auszügen vorgestellt.

Schlüsselwörter Unternehmensarchitektur · Cybersicherheit · Föderale Sicherheitsarchitektur · Referenzmodell

✉ Thomas Rehbohm · Kurt Sandkuhl
Institut für Informatik, Universität Rostock, A.-Einstein-Str. 22, 18051 Rostock, Deutschland
E-Mail: thomas.rehbohm@uni-rostock.de

Kurt Sandkuhl
Universität Jönköping, Gjuterigatan 5, 55111 Jönköping, Schweden

Published online: 10 November 2023

Reference Architecture Cybersecurity in the Federal System of Germany

Abstract This article discusses cybersecurity architectures in the context of Germany's federal system. The architecture presented are to become a fundamental component of the German and at the same time digital services of general interest for society, the economy and the administration.

At the time when the hybrid threat situation and the supply of fossil fuels are a matter of constant debate in politics and the media, all of the German federal states face compareable challenges. The European Union, Germany and Germanys constituent the federal states have had to recognise how very fragile social and societal cohesion is. Bottlenecks, as they have become increasingly likely in electricity and gas supply, are transferable to ICT infrastructures.

The aim of the cybersecurity architecture described here is to enable cybersecurity actors at the national and federal level to network more closely to strengthen resilience against threats. The architecture set out here will be further refined in an iterative evaluative manner and represents a federal solution to the challenges of the asymmetric threat landscape. Apart from a possible and future legal change in the distribution of competences in Germany, this research paper considers cybersecurity in the context of a distributed and federal structure.

Keywords Enterprise architecture · Cybersecurity · Federated security architecture · Reference model

1 Einleitung

Die neuerlichen Cyberangriffe in verschiedenen Bundesländern und auf Bundes- und Landesbehörden (Heller 2021) unterstreichen die wachsende Bedeutung eines systematischen Managements der Cybersecurity. Die Komplexität dieses Themas mit so unterschiedlichen Aspekten wie Netzwerksicherheit, Informationssicherheit, Softwaresicherheit oder Emergency Response erfordert koordinierte Maßnahmen auf allen Ebenen der Verwaltung und der Betreiber systemrelevanter Infrastrukturen, um Bedrohungen zu minimieren und Ausfälle zu vermeiden. Für die Gesellschaft ist die Frage nach der Verfügbarkeit von elementaren Verbrauchsgütern und Infrastrukturen so wichtig und aktuell, wie schon seit Jahrzehnten nicht mehr. Der wirtschaftliche und soziale Zusammenhalt ist mittlerweile in einem hohen Maß von Informationstechnik abhängig. Cybersicherheit stellt folglich das Bindeglied zwischen der Informationssicherheit verschiedener staatlicher und privater Organisationen dar.

In der Cybersicherheitsarchitektur – als Teilmenge der Gesamtsicherheit – Deutschlands kommt den Ländern des Föderalstaates eine exponierte Rolle bei der Digitalen Daseinsvorsorge – und den in ihren Regionen betriebenen Informationstechnik- Infrastrukturen zu (Wenzelburger 2020, S. 382). Kommunen, deren Bevölkerung und Wirtschaftsunternehmen sind grundsätzlich in der Verantwortung der Länder. Die Kommunen sind prinzipiell mit einem hohen Grad an verfassungskonformer Selbständigkeit ausgestattet. Gleichzeitig sind Kooperationsnormen

angesichts der Herausforderungen unterentwickelt, was zu Verfassungsänderungen und Kompetenzverlagerungen zum Bund mündete (von Beyme 2017, S. 387).

In Deutschland ist die Verlagerung von Kompetenzen auch im Cybersicherheitsbereich zugunsten des Bundes in Diskussion[1]. Weiterhin ist mit dem Vorschlag der Europäischen Union und des Rates eine neue Richtlinie für Netz- und Informationssicherheit in der Union verabschiedet worden (European Union 2022), die in nationales Recht innerhalb von 21 Monaten umgesetzt werden muss und erheblichen Einfluss auf die föderale Ausgestaltung der Cybersicherheitsarchitektur nimmt.

Das Ziel der hier vorgestellten Forschungsarbeit ist es, einen Beitrag zur weiteren Verzahnung der systemrelevanten Akteure der regionalen und föderalen Cybersicherheit zu leisten. Dazu werden die notwendigen Abläufe zwischen den betroffenen Organisationseinheiten bei Land, Kommune und Unternehmen der Privatwirtschaft betrachtet und inter-organisationale Prozesse sowie gemeinsam nutzbare Komponenten einer Cybersicherheitsorganisation vorgeschlagen. Ein Beispiel ist, wie der sichere, technische und vertrauliche Austausch von Angriffsverktoren zwischen diesen Akteuren erfolgen kann.

Als Mittel für die Darstellung der vorgeschlagenen Cybersiucherheitsorganisation wird ein Unternehmensarchitekturmodell gewählt. Unternehmensarchitekturen betrachten typischerweise unterschiedliche Ebenen einer Organisation, wie die Geschäfts-, Informations- und Technologiearchitektur. Da bei der Verzahnung von Land, Kommunen und Unternehmen zur Erzielung einer verbesserten Cyberarchitektur alle Ebene erforderlich sind, bietet sich die Verwendung eines Unternehmensarchitekturansatzes an. Gegenstand der Modellierung muss dabei nicht die komplette Cybersicherheitsarchitektur aller Beteiligten sein, sondern der Fokus kann auf der bisher fehlenden Verzahnung liegen, was konkret die betroffenen Schnittstellenbereiche auf Prozess-, Organisations-, Informations- und Technolgieebene sind. Die Entwicklung der Architektur erfolgt beispielhaft für die Freie und Hansestadt Bremen (FHB) mit ihren Kommunen und KRITIS-Unternehmen. Das Ziel ist dabei die Schaffung einer Referenzarchitektur im Sinne eines auf die Bundesländer übertragbaren Ansatzes.

2 Grundlagen und bisherige Arbeiten

2.1 Notwendigkeit und Bedarf an Cybersicherheitsforschung in föderalem Umfeld

Um die Sicherheit von Technologie zu gewährleisten, ist eine effektive Koordination von Instrumenten von entscheidender Bedeutung. Ein wichtiger Aspekt der Resilienz eines Landes bzw. seiner Metropolregion, ist die vertrauensvolle Zusammenarbeit zwischen den wesentlichen Akteuren, die für das Gemeinwohl verantwortlich sind. Eine solche Kooperation ermöglicht es, Bedrohungen schneller zu erkennen und effektiver zu bekämpfen. Cybersicherheitsbedrohungen sind dynamisch und bedürfen

[1] Pressekonferenz der Bundesinnenministerin im Juli 2022 zur Cybersicherheitsagenda der Bundesregierung.

einer zeitnahen Reaktion bei den Angegriffenen sowie deren Initiative. Eine Bewusstseinsbildung für die Cybersicherheitsgefahren in vernetzter Technologie muss hierfür in den Unternehmen und im Regierungshandeln Einzug halten, um Cybersicherheit in einer sich ständig verändernden digitalen Welt zu gewährleisten. Folglich sollen die Technologie und der Technologieeinsatz selbst verbessert werden.

Die aktuelle Forschung zeigt, dass im Umfeld der föderalen Strukturen nur wenige einschlägige Arbeiten entstanden sind, die sich der Herausforderungen von Cybersicherheits-Resilienz in föderalen Strukturen widmen. Mehrheitlich befassen sich europäische Beiträge mit dem Binnenmarktrecht, dem Wettbewerbsrecht und im Kontext von strukturellen und demografischen Wandel, mit den Sozial-, Versorgungs- und Gesundheitssystemen. Dienstleistungen im allgemeinen Interesse oder „services of general interest" (SGI), im Zusammenhang von Cybersicherheitsstrukturen sind noch unterrepräsentiert. Es wurden in der strukturierten Literaturrecherche relevante Veröffentlichungen aus den Vereinigten Staaten, europäische Beiträge und der Forschungsstand in Deutschland erhoben. Die Literaturrecherchen sind Teil der unter 2.3 benannten Vorfeldstudien.

2.2 Unternehmensarchitekturen

Das Gebiet des Unternehmensarchitekturmanagements (UA) (Lankhorst 2017), (Nurmi et al. 2019) hat sich seit mehr als einem Jahrzehnt als eine Disziplin sowohl in der Forschung als auch für die praktische Unterstützung entscheidungsunterstützender Funktionen und Modelle in Unternehmen und Organisationen entwickelt (Simon et al. 2014). Ziel der Unternehmensarchitektur ist es, wichtige Zusammenhänge und Querbeziehungen zwischen betrieblichen bzw. organisatorischen und informationstechnischen Aspekten zu modellieren, abzustimmen und zu verstehen, um so die Voraussetzung für einen gut angepassten und strategisch ausgerichteten Entscheidungsrahmen sowohl für Veränderungen in Organisationen, bspw. bei der Anpassung von Geschäftsmodellen oder der Einführung technologischer Innovationen, zu schaffen (Niemi und Pekkola 2017).

Unternehmensarchitekturmanagement (UAM), wie es heute durch verschiedene Standards wie ArchiMate (Group 2017) und TOGAF (*The TOGAF Standard* 2018) definiert ist, verwendet unterschiedlicher Sichten und Perspektiven für die Dokumentation, Planung und Visualisierung zentraler Bestandteile einer Organisation bzw. eines Unternehmens (Simon et al. 2014). Die Geschäftsarchitektur bildet die zentralen Ziele der Unternehmensstrategie, Geschäftsprozesse, Organisationsstrukturen und Governance-Strukturen des Unternehmens ab. Die Informationsarchitektur besteht meistens aus zwei Ebenen: Datenarchitektur und Anwendungsarchitektur. Weiterhin werden auch die Beziehungen zwischen Anwendungen und Geschäftsprozessen sowie zwischen Daten und Anwendungen erfasst. Die Technologiearchitektur erfasst die physischen IT-Komponenten, deren Zusammenhänge und geographische Verteilung.

Das UAM bildet insgesamt einen Managementansatz, der ein kohärentes Ganzes von Richtlinien, Architekturprinzipien und Governance-Regelungen festlegt, pflegt und verwendet. Ein effektiver Architekturmanagement-Ansatz für Cybersicherheitsarchitekturen sollte zusätzlich die Digitalisierung von Produkten und Dienstleistun-

gen unterstützen (Urbach und Ahlemann 2019) und sowohl ganzheitlich als auch leicht anpassbar sein.

2.3 Vorfeldstudien

Im Vorfeld der in diesem Beitrag dargestellten Ergebnisse wurden verschiedene Studien durchgeführt, die zur Analyse des Problems beitragen sowie zur Entwicklung und ersten Evaluation des Unternehmensarchitekturmodells führten. Insbesondere wurde erarbeitet, welche Aufgaben und Herausforderungen bestehen, um öffentliche, private bzw. zivilgesellschaftliche Akteure der Daseinsvorsorge interagieren zu lassen (Neu 2009, S. 42). Zusammengefasst hat sich der Bedarf an einem integrierten Ansatz in Form einer Unternehmensarchitektur ergeben, die Empfehlungscharakter haben sollte und somit als eine Referenzarchitektur bzw. ein Referenzmodell entwickelt werden soll. Insgesamt wurden vier Studien als Grundlage für diesen Artikel durchgeführt

1. Studie bei den Ländersicherheitsbeauftragten zu den Herausforderungen des Cyber- und Informationssicherheitsmanagements in föderalen Strukturen (Rehbohm et al. 2019): Die mit den CISOs der Länder durchgeführte Studie zu politischen, strategischen, technischen und rechtlichen Herausforderungen in der Cybersicherheit hat gezeigt, dass weder durch den Bund definierte, noch in den Ländern, eine vergleichbare oder belastbare Vorgehensweise zur Lösung des Problems vorliegen. Zusammenfassend konnte bestätigt werden, dass der Bedarf, an spezifischeren Instrumenten zur Koordinierung der Landesebenen, existiert. Organisationsbezogene Informationssicherheitsmanagementansätze greifen zu kurz und adressieren nicht die regionale Daseinsvorsorge. Insbesondere kann unterstellt werden, dass ein Referenzmodell – basierend auf einem Unternehmensarchitekturmodell – eine mögliche Lösung des Problems darstellen kann.
2. Integriertes Sicherheitsmanagement des öffentlichen und privaten Sektors für kritische Infrastrukturen – Problemanalyse (Rehbohm et al. 2021) Die Studie mit den Unternehmen der regionalen Daseinsvorsorgen in der FHB konnte durchgeführt werden, weil diese die bundegesetzlichen Schwellenwerte nach der Definition der BSI Kritisverordnung übertrafen und Zugang zu diesen Unternehmen bestand. Die befragten Unternehmen hatten keine vergleichbaren Ansätze oder Architekturen in der Organisation etabliert, die Cybersicherheitsrisiken angemessen adressierten. Insbesondere hatten die kleinen Unternehmen keine Sicherheitsstrategie oder relevante Managementsysteme bzw. auch noch kein Verständnis für die eigene Tätigkeit als Daseinsvorsorgeträger. Technische und organisatorische Maßnahmen waren zum Teil nicht zielführend. Auch hat die FHB keine Strukturen zur Förderung der Zusammenarbeit der relevanten Akteure im Sinne des Gemeinwohls geschaffen. Gleichzeitig existieren keine rechtlichen Bindungsvorgaben im Sinne von gesetzlichen Regelungen.
3. Empirische Studie in deutschen Kommunen zu Sicherheitsmanagement, Cybersicherheit und Daseinsvorsorge: (Rehbohm et al. 2022): Angelehnt an die Studie bei den Landesinformationssicherheitsbeauftragten, sollte diese Umfrage die politischen, organisatorischen, strategischen und juristischen Perspektiven qualifizie-

ren. In der Gesamtschau ließ sich beweisen, Informationssicherheitsmanagementprozesse sind im Allgemeinen unterentwickelt. Auch wenn Empfehlungen seitens des zuständigen Landes oder von den Deutschen Spitzenorganisationen existieren, werden diese überwiegend nicht befolgt, umgesetzt, ihre Umsetzung nicht unabhängig kontrolliert und die Systeme nicht nachhaltig etabliert. Dabei existiert mit *CISIS12* ein Vorgehensmodell, das es grundsätzlich jeder Organisation ermöglicht, externe und interne Anforderungen an ein Informationssicherheitsmanagement systematisiert, effektiv und effizient einzuführen (Moses und Rehbohm 2022, S. 61). Kleinere Kommunen sind dabei durchweg schlechter aufgestellt als größere Organisationen. Erstaunlicherweise wird die eigene Dienstleistungserbringung im kommunalen Umfeld nicht als kritische Dienstleistung bewertet, gleichwohl wird eingeräumt, für solche Dienstleistungen Verantwortlichkeiten zu besitzen. In diesem Kontext wurde auch geprüft, ob eine Bereitschaft zur technischen Kooperation mit größeren Organisationen oder Kommunalverbünden besteht. Diese Bereitschaft ist jedoch eher auf politischer kommunaler Leitungsebene nachweisbar.

4. Grundforderungen von Informations- und Cybersicherheit in Ländern, Studie zu den rechtlichen Rahmenbedingungen im föderalen Kontext (Rehbohm und Kalmbach 2021): In der Rechtsstudie wurde erhoben, ob Regelungsdefizite in den Ländern und abseits der Gesetzgebung der europäischen Union und Deutschland bestehen. Die vorliegende Arbeit basiert auf Erkenntnissen von Interview- und Umfragestudien in den Ländern und den zuständigen Ministerien. Dabei wurde erarbeitet, dass es eine rechtsstaatliche Aufgabe ist, die IKT-Infrastrukturen der öffentlichen Gewalt, hier der Länder und der Kommunen, gegen Angriffe abzusichern. Gleichzeitig sind aber auch privatwirtschaftliche Bereiche von dieser staatlichen Verantwortung betroffen. Die Gewährleistungsverantwortung des Staates gegenüber der Bevölkerung ist hier relevant (kollektives Rechtsgut).
5. Das Gefahrenabwehrrecht liegt bei den Ländern, folglich muss das einschlägige Bundesrecht komplementär um Inhalte im Landerechts ergänzt werden. Der Anspruch auf Daseinsvorsorge und das Funktionieren der IKT-Systeme ist rechtlich zu sichern. Sinnlogisch sind Anbieter von Dienstleistungen oder Waren, welche elementar wichtig für große Teile der Bevölkerung sind, also Träger der Daseinsfürsorge als maßgebliche Akteure per Gesetz und nötigenfalls per Verwaltungsakt zu identifizieren und in die Pflicht zu nehmen.

3 Forschungsansatz

Das Ziel der hier vorgestellten Forschungsarbeiten ist, die Integration einer Cybersicherheitsstrategie in Cybersicherheitsarchitekturansätzen aufzuzeigen und zu einem Referenzmodell weiterzuentwickeln.

Forschungsmethodisch wird zur Erreichung dieses Ziels ein konstruktionsorientierter Forschungsansatz (Frank 2009) eingesetzt, wie er besonders in der Wirtschaftsinformatik weit verbreitet ist. Der Unternehmensarchitektur wird dabei nicht als Selbstzweck betrachtet, sondern dezidiert als Mittel zur Erreichung organisatorischer Zielsetzungen verstanden. Der konstruktionsorientierte bzw. gestaltungsorien-

tierte (Österle et al. 2010) Forschungsansatz wird im internationalen Umfeld auch als „Design Science (Hevner et al. 2004), (Peffers et al. 2007)“ bezeichnet.

Während konstruktionsorientierte Forschung den Gesamtansatz darstellt, wird bei der Durchführung der Forschungsarbeiten eine Vielzahl von Einzelmethoden eingesetzt, die im Wesentlichen zur Begründung der Forschungsresultate erforderlich sind. Da Begründung von Forschungsergebnissen etwa durch einen formalen Beweis oder durch eine empirisch bestätigte Theorie aufgrund der Natur der Fragestellung oder fehlender Daten häufig nicht möglich ist, sind in der Regel alle Annahmen, die dem Entwurf einer Konstruktion zugrunde liegen, explizit machen. Dazu gehören Annahmen, die Anforderungen, Entwurfsentscheidungen wie auch die Evaluation des „Artefakts“ (in unserem Fall: der Referenzarchitektur) betreffen (Frank 2008).

Konstruktionsorientierte Forschung beinhaltet in der Regel drei miteinander integrierte Forschungszyklen, die auch für die Entwicklung der Referenzarchitektur gelten:

- Der Relevanzzyklus verankert die Entwurfsentscheidungen und Merkmale der Referenzarchitektur in Anforderungen des betreffenden Handlungskontextes, also der Verbindung zwischen Land, Kommune und relevanten Wirtschaftsunternehmen. Dies erfolgte durch die in Abschn. 2 beschriebenen Vorfeldstudien.
- Der Rigorositätszyklus setzt die Forschungsresultate in Verbindung zum Stand des Wissens im jeweiligen Fachgebiet, was über Literaturanalysen erfolgen kann. Auch dies in den Publikationen zu den Vorfeldstudien erfolgt.
- Die Entwurfs-/Evaluationszyklus dient der eigentlichen Konstruktion der Referenzarchitektur auf Grundlage der Ergebnisse aus dem Relevanzzyklus und unter Berücksichtigung der Resultate des Rigorositätszyklus. In der Regel wechseln sich hier Entwurf- und Validierungsschritte bzw. Verbesserungs- und Validierungsschritte ab. Die Abschn. 4 und 5 beschreiben einen solchen Zyklus.

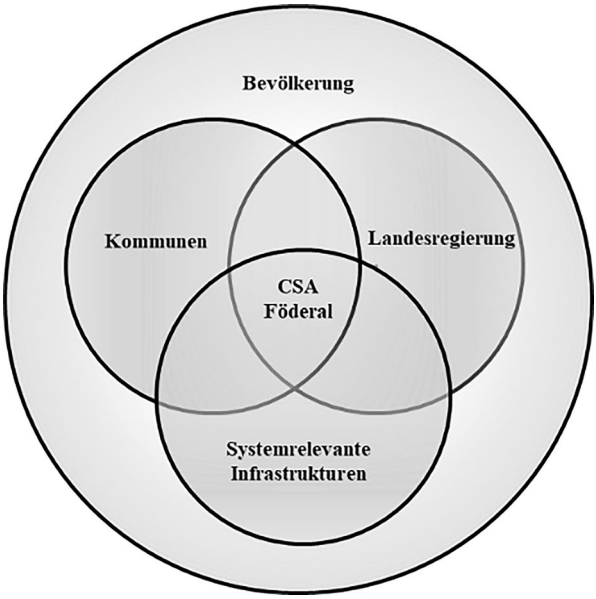
Die zentrale Forschungsfrage für diesen Beitrag ist: Kann die vorgestellte Referenzarchitektur für Länder Deutschlands einen wesentlichen Beitrag zur Nationalen Cybersicherheitsarchitektur leisten? Die zur Beantwortung dieser Forschungsfrage und die angewandte Forschungsmethode ist eine Kombination aus Literaturrecherche, konzeptionell-deduktiver Arbeit und Evaluation. Die Referenzarchitektur wurde mit der Modellierungssprache ArchiMate dokumentiert.

4 Anforderungen und Lösungsansatz der Referenzarchitektur

4.1 Anforderungen an eine föderale Architektur

Eine wirksame föderale Cybersicherheitsarchitektur soll strukturelle Rahmenbedingungen, technische Interaktionen und Rechtssicherheit schaffen, die eine gleichberechtigte Teilhabe aller Akteure ermöglicht. Zum Schutz der Bevölkerung in der jeweiligen Region ist es notwendig, Akteure in den Kommunen eines Landes oder Metropolregion unter regulierender Aufsicht eines Landes mit den systemrelevanten Unternehmen zu vernetzen (vgl. Abb. 1). Systemrelevante Unternehmen sind die Summe aus kritischen Infrastrukturen nach Definition und Regulierung des Bundes,

Abb. 1 Akteure



Infrastrukturen nach Regulierung der EU und wesentliche und wichtige Einrichtungen, die durch das jeweilige Land zu identifizieren sind. Staatliche Akteure der Landesverwaltung müssen rechtliche, technische und organisatorische Rahmenbedingungen schaffen, die eine Kollaboration zulassen und nötigenfalls erzwingen.

Die Architektur muss es zulassen, Forschungs- und Entwicklungseinrichtungen in einem Teilhabeprozess einzubinden. Diese Aufgabe kann durch organisatorische Regelungen der Landesverwaltung erfolgen. Die Weiterentwicklung der Architektur muss aktuelle Entwicklungen der Cybersicherheitsforschung berücksichtigen. Auch ist die Architektur darauf auszurichten, dass Digitale Kompetenzen aufgebaut und erhalten werden. Themen, wie die Aus und Fortbildung, Awareness, Fachkräfteaquirierung Fachkräftebindung und Arbeitgebermarkenbildung können das Handlungsfeld Forschung und Entwicklung flankieren.

Auf Seiten der öffentlichen Verwaltung sind neben externen Kooperationen weitere Anforderungen an die Architektur zu berücksichtigen, z. B. Adressierung von Polizei und Verfassungsschutz.

4.2 Lösungsansatz

Die erstellte Architektur soll zeigen, dass ein übergreifendes Informationssicherheitsmanagement zwischen den Ländern zum einen und zum Bund zum anderen entstehen soll. Das Bild soll (Abb. 2) illustrieren, welche Akteure, mit Aufgaben und verbundenen Methode zu adressieren sind. Der im ersten Ring beschriebene Teil der Cybersicherheitsarchitektur (CSA) Föderal muss die Akteure der Verwaltung (Herpig und Rupp 2022, S. 173) um Wirtschaft und Gesellschaft erweitern und derart integrieren, dass ein kooperativer Baustein in der deutschen Gesamtarchitektur

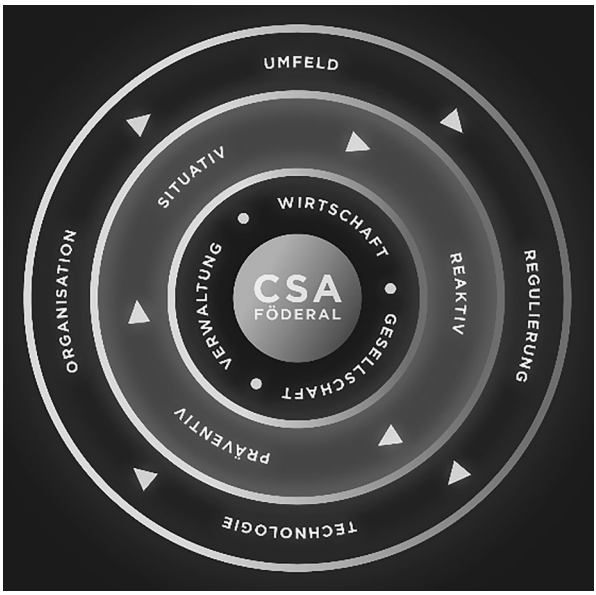


Abb. 2 Cybersicherheitsarchitektur Land

entsteht und die Cybersicherheitsstrategie Deutschlands ergänzt (Bundesministerium des Innern, für Bau und Heimat 2021, S. 21).

Auf Seiten der Verwaltung werden hierfür die Ebenen der deutschen Verwaltungsgliederung adressiert, auf Seiten der Wirtschaft werden die kritischen Infrastrukturen nach Definition des Bundes (Kritis) sowie die Wirtschaftsunternehmen der Daseinsvorsorge der Region (Subkritis) in den Fokus genommen.

Eingebunden werden alle zu identifizierenden Stellen der Architektur für die im Einzelnen subsummierten präventiven, situativen und reaktiven Aufgaben, welche ergänzend durch regulatorische Maßnahmen umrahmt werden. Das bedeutet im Einzelnen, dass nach Abstufung der Unternehmen in „wesentlich“ oder „wichtig“ für die Daseinsvorsorge insbesondere Kontrollen, Berichtspflichten und Informationsaustausch zu berücksichtigen sind (European Union 2022, S. 39).

5 Unternehmensarchitektur

5.1 Strategische und Motivatorische Betrachtung der CSA Land

Das strategische Ziel eines übergreifenden Cybersicherheitsmanagements in einem Land wird von intrinsischen und extrinsischen Motivationen befördert. Intrinsische Motive liegen dabei in der Wirtschaftlichkeit, Nachhaltigkeit und Widerstandsfähigkeit der angestrebten Lösung. Extrinsische Motive liegen in der Rechtskonformität bzw. Comliance und in der Reputation, also der Glaubwürdigkeit der Organisation und das in dieses gesetzte Vertrauen. Aufgrund der zahlreichen parlamentarischen und medialen Anfragen in den Ländern, stehen die Landesregierungen unter enormen Erfolgsdruck. Sowohl die eigenen IT-Infrastrukturen der öffentlichen Ver-

waltung, als auch die Wirtschaftsunternehmen der Daseinsvorsorgen sind Ziel von politischen Anfragen.

In Abb. 3 wird veranschaulicht, welche Fähigkeiten das Land mindestens vorhalten soll, um die strategischen Ziele erreichen zu können. Die drei elementaren Aufgabenbereiche sind zuvorderst den Themenfeldern IT-Servicemanagement, IT-Securitymanagement und Threat-Intelligence-Management zuzuordnen. Für ausge-

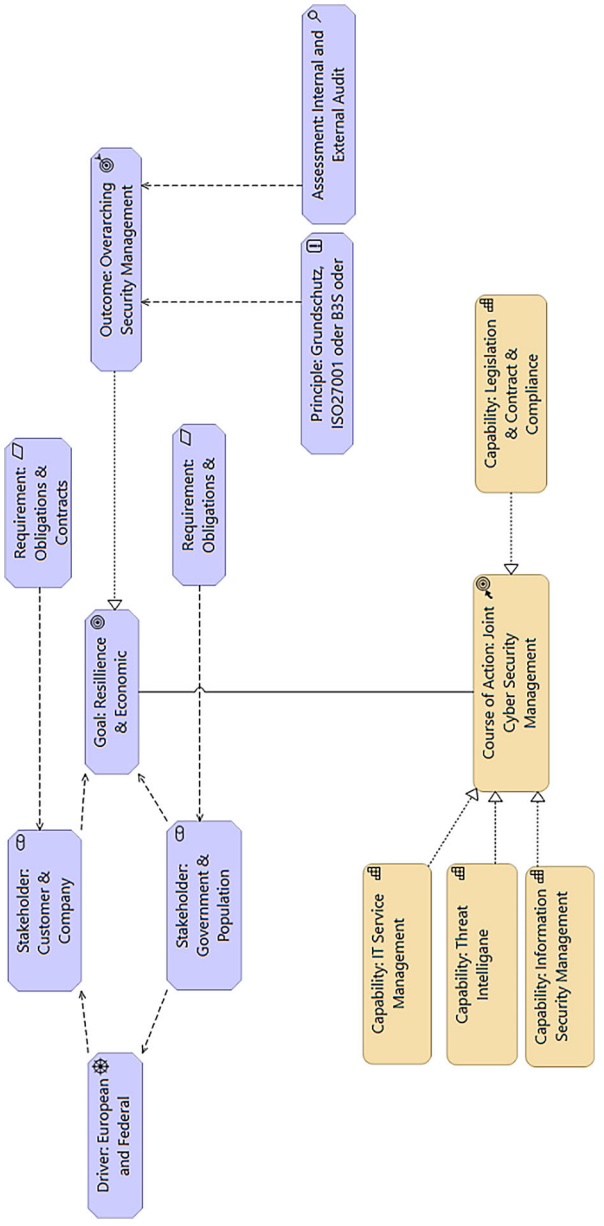


Abb. 3 CSA Land Strategie

wählte Sektoren der kritischen Infrastrukturen gelten Mindestanforderungen, die der Beherrschung von Cybersicherheitsrisiken dienen. Die Einhaltung der NIS-2-Richtlinie wird durch nationale Behörden überwacht und bei Nichteinhaltung auch sanktioniert werden können.

Neben den verpflichtenden Regelungen aus der Richtlinie existieren weitere Handlungsfelder der föderalen Cybersicherheitsarchitektur, wie insbesondere die Förderung von digitalen Kompetenzen, die Aus- und Fortbildung, die Awarenessbildung und Bekämpfung des Fachkräftemangels, welche in den Bereich von organisatorischen Regelungen fallen und die Beschäftigten in Wirtschaft, Verwaltung und Gesellschaft adressieren. Zudem wird in der Architektur berücksichtigt, dass die einem Land zustehende Fähigkeit einer gesetzgebenden Unterstützung dieser Managementbereiche gegeben ist.

Mindestanforderungen an die Architektur, die unter *Präventiv* subsummiert werden, sind als Business, Application und Technology modelliert. Hierbei handelt es sich um Applikationen die zu *Exchange & Advisory* gezählt werden. Weitere Teile der Architektur CSA-Land sind den Abschnitten *Situativ* und *Reaktiv* zuzuordnen und definieren Business Architekturen.

5.2 Erörterung der Business-/Application Ebenen

Für eine föderale Architektur sollen in diesem Abschnitt Anwendungen aus der Prävention und jeweils eine Anwendung aus den Bereichen Situativ und Reaktiv erläutert werden. In der Präventionsarbeit bieten sich zahlreiche Möglichkeiten der Interaktion mit den Akteuren, wie zum Beispiel Employer Recruitment, Training & Awareness, Research & Development oder auch Exercise an. Dies sind ausbaubare Elemente einer Landes-Architektur.

5.2.1 WIS

Ein wesentlicher Baustein der Prävention sind sogenannte Warn- und Information Services (WIS). Diese müssen inhaltlich auf die Organisation zugeschnitten sein und dürfen den Adressaten in Quantität nicht überfordern. Auch müssen die Informationen in der Organisation verarbeitet werden können, das heißt, entsprechende Ressourcen müssen zur Verfügung stehen.

Grundsätzlich werden solche Business Services von den Computer Emergency Response Teams (CERT) angeboten. Hier besteht die Möglichkeit an einem Landes CERT teilzuhaben, welches die verfügbaren Informationen sammelt ggf. erstellt und bereitstellt. Akteure der Daseinsvorsorge sind ausschließlich beim Land, teilweise auch beim Bund bekannt und werden über die Webanwendung zur Registrierung aufgefordert. Hierfür werden bestehende Möglichkeiten der öffentlichen Verwaltung zu Identifizierung solcher Unternehmen insbesondere die Beziehungen zu Branchenverbänden und Kammern genutzt, um unabhängig von der Relevanz für die Daseinsvorsorge jedes Unternehmen der Region teilhaben zu lassen. Gewünschte Informationen werden von der jeweiligen Organisation selbst zusammengestellt, abonniert und ausgewertet. Dabei handelt es sich insbesondere um Informationen von bekannten Schwachstellen in Hard- und Softwareprodukten sowie bekannten

Sicherheitslücken bzw. Angriffsmustern. Die in der Plattform integrierten Informationen zu Sicherheitslücken werden aus angebundenen „Common Vulnerabilities and Exposures“ Datenbanken gewonnen. Schwachstellen in Hard- und Software werden regelmäßig bei kommerziellen Anbietern eingekauft, integriert und zur Verfügung gestellt.

5.2.2 MISP

Ein weiterer Business Service ist modelliert und beruht auf der *„Malware Information Sharing Platform“*. Dieser Service wird in den Ländern regelmäßig beim Security Operation Center (SOC) betrieben werden. Die hier über eine Partnerschnittstelle zur Verfügung gestellten Informationen sind anders als im WIS nicht frei verfügbar, sondern teilweise vertraulich, im Sinne von Verschlusssachen nach den jeweiligen gesetzlichen Rahmenbedingungen. Die Prävention schließt aktuelle Ereignisse der Detektion ein (Indicator of Attacks). Der Datenaustausch folgt einer festgelegten Taxonomie (Mokaddem et al. 2019). Wie die Abb. 4 illustrieren soll, wird der Prozess von externen Ereignissen initiiert. Solche Ereignisse werden unter anderem über Sicherheitsvorfälle und forensischer Aufarbeitung erzeugt bzw. wird aus aktuellen Ergebnissen von Detektoren gespeist. Die Weitergabe von ermittelten Ergebnissen aus Sicherheitsvorfällen, Ereignissen aus „Threat Intelligence“ oder Intrusion Detection Systems (IDS)/Security Information and Event Management (SIEM) erfordern in jeder teilnehmenden Organisation Expertise. Diese Expertise muss ggf. aufgebaut und ausgebaut werden. Das Land reichert die auf der Plattform verfügbaren Informationen zudem noch um Erkenntnisse des Bundes an. Solche „Indicator of Compromises“ (IoC) können nur unter bestimmten vertraulichen Bedingungen bereitgestellt werden. Die Plattform kann bidirektional genutzt werden, insofern wird beim Land eine Datenqualitätskontrolle der gelieferten IoCs erfolgen müssen. Für die Teilnehmenden aus der Wirtschaft muss ein Vertragskonstrukt gewählt werden, dass die Vertraulichkeit aller Informationen sicherstellt. Auch kann die Integrität des Datenaustausches über kryptografische Maßnahmen verbessert werden (van de Kamp u. a. 2016, S. 3). Des Weiteren werden die Akteure der Wirtschaft untereinander nicht identifiziert, da sie auf der Plattform pseudonymisiert werden müssen.

5.2.3 SR

In der Architektur sind weitere Themen aus Sicht eines Landes zu bedienen. Zum einen handelt es sich dabei um die Erfassung eines Lagebildes Cybersicherheit für das jeweilige Land. Dies kann nur in Zusammenarbeit der Sicherheitsmanagements und der Organisationen der allgemeinen öffentlichen Sicherheit erfolgen, insbesondere des Katastrophenschutzes. Es handelt sich hierbei um einen Business Prozess, der bislang nicht technisch abgebildet ist.

Das Land muss einen Prozess vorhalten, der geeignet ist, Informationen der beteiligten Akteure regelmäßig und verstetigt entgegenzunehmen, weiterzuverarbeiten und an die nächst höheren Instanzen zu melden (e.g. European Union Agency for Cybersecurity).

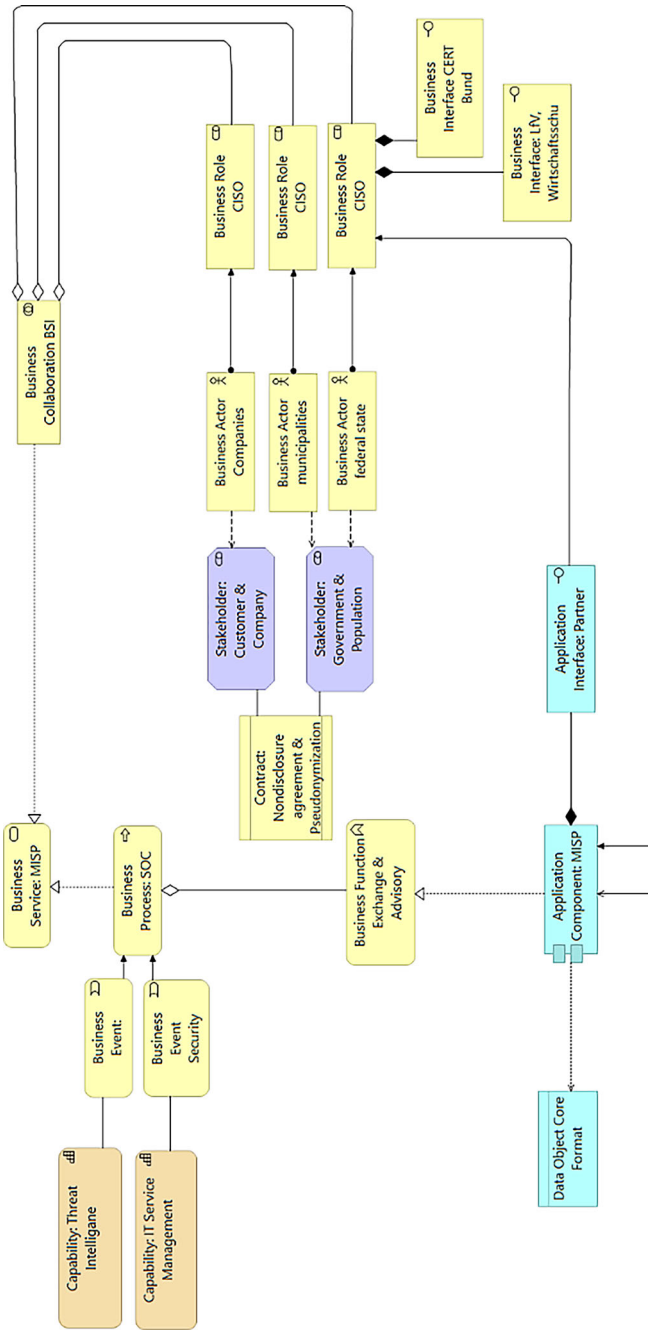


Abb. 4 Malware Information Sharing Platform

5.2.4 MIRT

Der zwingend nötige Prozess des Mobile Incident Response greift erst, nachdem eine in der CSA-Land involvierte Organisation Opfer eines Cybersicherheitsangriffes wurde. Es sind in diesem Fall die Beteiligten der öffentlichen Sicherheit zu involvieren. Je nach Typ des Angriffs kann das die Polizei, eine Schwerpunktstaatsanwaltschaft oder der Wirtschaftsschutz sein. Im Vorfeld sind jedoch aktive Maßnahmen des Einsatzes von Hilfskräften zu steuern. Im Grunde muss hierdurch verhindert werden, dass durch unterlassene Hilfe des Landes die Situation für die Organisation oder die abhängigen Dienstleister eskaliert. Ein Security Breach eines involvierten Akteurs übt einen zwingenden Druck auf das Land aus. Die Business Rolle CISO eines Landes ist verantwortlich für die Akquirierung von Kräften des BSI, Kräften des möglichen Partnerlandes oder auch von spezialisierten Unternehmen. Hierfür sind neben rechtlich schon definierten Szenarien zwischen dem Bund und den Ländern auch die vertraglichen Möglichkeiten mit externen Dienstleistern auszuschöpfen.

5.3 Rechtliche Betrachtung

Eine Länder-Allianz für Cybersicherheit kann nur unter bestimmten Voraussetzungen, insbesondere unter der Abwägung von gesetzlichen bzw. gesetzgeberischen Möglichkeiten oder vertraglichen Regelungen entstehen.

Die durchgeführten Studien haben jedoch gezeigt, dass eine Zusammenarbeit verschiedener Organisationen der Wirtschaft von Misstrauen geprägt ist. Erschwerend kommt hinzu, dass Unternehmen, die im Mitbewerb stehen, nicht willens sind, Informationen mit den Wettbewerbern ohne externe Verpflichtungen auszutauschen. Der Erstautor dieses Beitrags hat hierfür im Rahmen seiner hauptamtlichen Tätigkeit als CISO der FHB, zusammen mit dem Co-Autor der Rechtsstudie, ein IT-Sicherheitsgesetz für die FHB entworfen. Mit dem Gesetz werden die Akteure zur Kooperation verpflichtet und müssen dem Land zudem Kontrollrechte einräumen. Die mit der NIS-2-Richtlinie veröffentlichten Rechte und Pflichten der Mitgliedsstaaten greifen genau diese Regulierungsmöglichkeiten auf.

Solange nicht absehbar ist, dass ein für diesen Zweck hilfreiches Gesetz verabschiedet wird, bleibt für die Entfaltung einer kooperativen Beziehung aller Akteure ausschließlich die Vertragsgestaltung.

6 Evaluierung der Architektur

6.1 Evaluation der Anforderungen an die Architektur

Die hier vorgestellte Architektur erhebt nicht den Anspruch auf eine vollständige Abdeckung aller heute bekannten technischen und organisatorischen Anforderungen. Vielmehr wird hier und im Forschungsfeld Cybersicherheit in föderalen Strukturen auf die wesentlich zu gestaltenden informationstechnischen Systeme abgestellt. Dort,

wo zeitkritische Informationen unverzüglich den Partnern der CSA zur Verfügung gestellt werden müssen, greift die vorgestellte Architektur zuvorderst.

Weitere Anforderungen an die Architektur sind überwiegend einer rein organisatorischen und rechtlichen Art. Hier kann die Architektur grundsätzlich erweitert werden, im Rahmen der Evaluation und Iteration.

6.2 Evaluationsstrategie

Die Evaluationsstrategie sieht vor, dass die entstandene Architektur zusammen mit Kommunen und den Ländern in Episoden verifiziert werden soll. Dies geschieht schrittweise, so dass eine Allgemeingültigkeit der vorgestellten Referenzarchitektur hergestellt werden kann.

Im ersten Evaluationsschritt wurde ein strukturiertes Experteninterview im Zeitraum August 2022 mit den Informationssicherheitsbeauftragten (CISOs) der Länder und sofern notwendig mit den zuständigen Vertretern weiterer Ministerien durchgeführt. Es wurden drei thematische Gebiete in der Kooperation und der komplementären Zusammenarbeit zwischen den Akteuren erörtert. Die Interviews wurden mittels qualitativer Inhaltsanalyse ausgewertet (Mayring 2008, S. 128–35). Entlang von definierten Fragen wurde festgestellt, ob Kritis-Unternehmen durch den Bund beim Land gemeldet und welche durch das Land selbst identifiziert wurden. Weiterhin sollte festgestellt werden, ob und wie die Länder mit den systemrelevanten Unternehmen zusammenarbeiten. Es bestand grundsätzlich keine Architektur, die eine Zusammenarbeit vergleichbar macht oder eine Allgemeingültigkeit in Anspruch nehmen kann. Die Länder kooperieren derzeit entweder nicht, wenige nur mit staatlichen Beteiligungen an Unternehmen und zudem nur auf freiwilliger Basis. In vereinzelten Fällen bestand die Möglichkeit einer Kooperation (Wissenstransfer) im Land, die von Kommunen und Unternehmen in Anspruch genommen werden können. Die hier vorgestellte Architektur wurde als zuführend bewertet. Die CISOs der Länder sahen den Etablierung eines ISMS als sehr wichtig an. Die Verpflichtung zu einer Zertifizierung war unterdurchschnittlich ausgeprägt. Alle Länder haben auf ministerieller Ebene ein zentrales Informationssicherheitsmanagement eingeführt. Eine Zertifizierung von einzelnen Ressorts besteht allerdings nicht, bzw. ist nur bei einzelnen Ressorts im Planungsstatus (4 von 186 Ministerien). Zentrale Rechenzentrumsdienstleister der ministeriellen Verwaltung sind regelmäßig zertifiziert. Vereinzelt sind auch zentrale Netzwerkinfrastrukturen (wie ein Landesnetz) zertifiziert.

Die Zahl von Unternehmen in kritischen Infrastrukturen, welche durch den Bund identifiziert wurden, liegt in den Ländern zwischen einem einstelligen und einem kleinen dreistelligen Bereich. Unabhängig von einer etwaigen öffentlichen Beteiligung an entsprechenden Unternehmen, liegt die Anzahl subkritischer Infrastrukturen nach Ersterhebung in zwei Ländern um den Faktor 20 bis 100 höher als die kritischen Infrastrukturen (gemäß Bund). Nur ein Land gab an, dass sie aktiv die Interdependenzen systemrelevanter Infrastrukturen analysieren wollen.

Grundsätzlich sind die Länder von einer harmonisierbaren Architektur, die als Minimalanforderung zu verstehen ist, überzeugt. Andererseits sind derzeit auch Länder unter den Befragten, die das Themenfeld der systemrelevanten Infrastrukturen

vollständig dem Bund überlassen wollen und keine eigenen Anstrengungen unternehmen, die Resilienz gegen Cybersicherheitsgefahren in ihrer Region zu erhöhen.

7 Schlussfolgerungen und zukünftige Arbeit

Die in diesem Beitrag vorgelegte Architektur ist nach ersten Iterationsschritten Teil einer möglichen Cybersicherheitsstrategie der FHB. In dieser Arbeit wurde eine erste Referenzarchitektur anhand der strategischen Anforderungen konkretisiert, die auch in der FHB relevant sein wird.

Erste Evaluierungsergebnisse liegen aus der Befragung der Länder vor und werden in der Fortschreibung der Architektur berücksichtigt. Idealerweise werden Prozesse erarbeitet, die es einem Land ermöglichen soll, voneinander abhängige Betreiber subkritischer Infrastrukturen, egal welcher Größe, zu identifizieren.

Die vorliegende Arbeit und die Architektur ist Teil weiterer Evaluationsepisoden in Kommunen und bei Vertretern der Länderarbeitsgruppe Cybersicherheit der Innenministerkonferenz. Die Einarbeitung der Ergebnisse stellt den finalen Evaluierungsschritt dar und soll die Gesamtarchitektur verbessern.

Funding Open Access funding enabled and organized by Projekt DEAL.

Literatur

von Beyme K (2017) Der Föderalismus. In: von Beyme K (Hrsg) Das politische System der Bundesrepublik Deutschland: Eine Einführung. Springer, Wiesbaden, S 377–417 https://doi.org/10.1007/978-3-658-14499-9_9

Bundesministerium des Innern, für Bau und Heimat (2021) Cybersicherheitsstrategie für Deutschland 2021, S 142

European Union (2022) EUR-Lex—32022L2555—EN—EUR-Lex. https://eur-lex.europa.eu/eli/dir/2022/2555/oj. Zugegriffen: 4. Mai 2023

Frank U (2008) Konstruktionsorientierter Forschungsansatz. In: Kurbel K, Becker J, Gronau N, Sinz E, Suhl L (Hrsg) Enzyklopädie der Wirtschaftsinformatik : Online-Lexikon. Oldenbourg, München (http://www.oldenbourg.de:8080/wi-enzyklopaedie/lexikon/uebergreifendes/Forschung-in-WI/Konstruktionsorientierter-Forschungsansatz.)

Frank U (2009) Die Konstruktion möglicher Welten als Chance und Herausforderung der Wirtschaftsinformatik. In: Becker J, Krcmar H, Niehaves B (Hrsg) Wissenschaftstheorie und gestaltungsorientierte

Wirtschaftsinformatik. Physica, Heidelberg, S 167–180 https://doi.org/10.1007/978-3-7908-2336-3_8
Heller G (2021) Immer mehr Cyberangriffe: IT-Sicherheitsbehörde BSI schlägt Alarm – Professionalität steigt. Passau. Neue Presse
Herpig S, Rupp C (2022) Deutschlands staatliche Cybersicherheits-architektur, S 221
Hevner, March, Park, Ram (2004) Design science in information systems research. MIS Q 28(1):75. https://doi.org/10.2307/25148625
van de Kamp T, Peter A, Everts MH, Jonker W (2016) Private sharing of IOCs and sightings. In: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security. ACM, Vienna, S 35–38 https://doi.org/10.1145/2994539.2994544
Lankhorst M (2017) Enterprise architecture at work: modelling, communication and analysis, 4. Aufl. The enterprise engineering series. Springer, Berlin, Heidelberg https://doi.org/10.1007/978-3-662-53933-0
Mayring P (2008) Qualitative Inhaltsanalyse: Grundlagen und Techniken, 10. Aufl. Beltz, Weinheim, Basel (Dr. nach Typoskr)
Mokaddem S, Wagener G, Dulaunoy A, Iklody A (2019) Taxonomy driven indicator scoring in MISP threat intelligence platforms. ArXiv 03914:1902
Moses F, Rehbohm T (2022) CISIS12. CISIS12, Nr. 1: 11
Neu C (Hrsg) (2009) Daseinsvorsorge: eine gesellschaftswissenschaftliche Annäherung, 1. Aufl. VS, Wiesbaden
Niemi E, Pekkola S (2017) Using enterprise architecture artefacts in an organisation. Enterp Inf Syst 11(3):313–338. https://doi.org/10.1080/17517575.2015.1048831
Nurmi J, Pulkkinen M, Seppänen V, Penttinen K (2019) Systems approaches in the enterprise architecture field of research: a systematic literature review. In: Aveiro D, Guizzardi G, Guerreiro S, Guédria W (Hrsg) Advances in enterprise engineering XII. Lecture notes in business information processing, Bd. 334. Springer, Cham, S 18–38 https://doi.org/10.1007/978-3-030-06097-8_2
Österle H, Becker J, Frank U et al (2010) Memorandum zur gestaltungsorientierten Wirtschaftsinformatik. Schmalenbach Z Betriebswirtsch Forsch 62(6):664–669
Peffers K, Tuunanen T, Rothenberger MA, Chatterjee S (2007) A design science research methodology for information systems research. J Manag Inf Syst 24(3):45–77. https://doi.org/10.2753/MIS0742-1222240302
Rehbohm T, Kalmbach P (2021) MMR-Aktuell 2021, 438461 – beck-online, Grundforderungen von Informations- und Cybersicherheit in Ländern. https://beck-online.beck.de/?vpath=bibdata/zeits/MMRAktuell/2021/438461.htm. Zugegriffen: 8. September 2022
Rehbohm T, Sandkuhl K, Kemmerich T (2019) On challenges of cyber and information security management. In: Federal structures—The example of German public administration, S 13
Rehbohm T, Sandkuhl K, Cap CH, Kemmerich T (2021) Integrated security management of public and private sector for critical infrastructures—Problem investigation. In: Abramowicz W, Auer S, Stróżyna M (Hrsg) Business information systems workshops. Lecture notes in business information processing. Springer, Cham, S 291–303 https://doi.org/10.1007/978-3-031-04216-4_26
Rehbohm T, Kemmerich R, Cap CH, Sandkuhl K (2022) Sicherheitsmanagement, Cybersicherheit und Daseinsvorsorge: Empirische Studie in deutschen Kommunen. Datenschutz Datensicherheit DuD 46(7):448–454. https://doi.org/10.1007/s11623-022-1637-0
Simon D, Fischbach K, Schoder D (2014) Enterprise architecture management and its role in corporate strategic management. Inf Syst E-Bus Manage 12(1):5–42. https://doi.org/10.1007/s10257-013-0213-4
The Open Group (2017) ArchiMate® 3.0.1 specification. Van Haren, Zaltbommel
The TOGAF Standard (2018) Version 9.2. Van Haren, Zaltbommel
Urbach N, Ahlemann F (2019) Transformable IT landscapes: IT architectures are standardized, modular, flexible, ubiquitous, elastic, cost-effective, and secure. In: Urbach N, Ahlemann F (Hrsg) IT management in the digital age. Management for professionals. Springer, Cham, S 93–99 https://doi.org/10.1007/978-3-319-96187-3_10
Wenzelburger G (2020) Einheit und Vielfalt im Sicherheitsföderalismus. In: Knüpling F, Kölling M, Kropp S, Scheller H (Hrsg) Reformbaustelle Bundesstaat. Springer, Wiesbaden, S 381–405 https://doi.org/10.1007/978-3-658-31237-4_22