HMD Praxis der Wirtschaftsinformatik (2023) 60:494–509
https://doi.org/10.1365/s40702-023-00944-6

SCHWERPUNKT

Cyber-Sicherheit für kritische Energieinfrastrukturen – Handlungsempfehlungen zur Umsetzung einer Zero-Trust-Architektur

Christoph Buck · Torsten Eymann · Dennis Jelito · Vincent Schlatt · André Schweizer · Jacqueline Strobel · Florian Weiß

Eingegangen: 28. Juni 2022 / Angenommen: 16. Januar 2023 / Online publiziert: 9. Februar 2023

Zusammenfassung Kritische Infrastrukturen – wie diejenigen der Sektoren Wasser, Energie und Ernährung – bilden die Grundlage einer funktionierenden, modernen Gesellschaft. Eine Kompromittierung dieser Infrastrukturen kann zu weitreichenden Störungen und Gefahren für Leib und Leben führen. Der Schutz sowie die Sicherstellung des Betriebs kritischer Infrastrukturen sind deshalb von entscheidender Bedeutung. Während in der Vergangenheit hauptsächlich der physische Schutz vor Angriffen im Mittelpunkt stand, entstehen durch die zunehmende Digitalisierung kritischer Infrastrukturen zusätzliche Angriffspunkte und Risiken. Im Gegensatz zu herkömmlichen Ansätzen zur Absicherung kritischer Energieinfrastrukturen kann eine Absicherung mithilfe einer Zero-Trust-Architektur die mit diesen Entwicklungen einhergehenden Anforderungen erfüllen.

Aufgrund der verhältnismäßig geringen Verbreitung von Zero-Trust-Architekturen im kritischen Energieinfrastruktursektor existiert bisher allerdings nur unzureichend praxisrelevante Literatur zur Entwicklung und Implementierung einer solchen Architektur. Diese Arbeit stellt daher sowohl die Erfahrungen aus einem laufenden Entwicklungs- und Implementierungsprojekt als auch die hiervon abgeleiteten technischen und organisationalen Handlungsempfehlungen im Rahmen eines Action-Design-Forschungsansatzes vor und trägt dadurch zur Schließung dieser Forschungslücke bei.

Autoren (in alphabetischer Reihenfolge).

Christoph Buck · Torsten Eymann · Dennis Jelito · Vincent Schlatt · Jacqueline Strobel · ✉ Florian Weiß
Universität Bayreuth, Bayreuth, Bayern, Deutschland
E-Mail: Florian.Weiss@uni-bayreuth.de

André Schweizer
TRUSTEQ GmbH, München, Bayern, Deutschland

Schlüsselwörter Cyber-Sicherheit · Zero-Trust-Architektur · Kritische Infrastruktur · Netzwerkarchitektur · Action-design Forschung

Cyber security for critical energy infrastructures – recommended actions for the implementation of a Zero-Trust-Architecture

Abstract Critical infrastructures—such as water, energy, and food supply—provide the foundation for a functioning modern society. Any compromise of these infrastructures could result in widespread disruption and pose a threat to life and health. Protecting and ensuring the operational continuity of critical infrastructures is therefore decisive. While the focus in the past was primarily on protection against physical attacks, the increasing use of digital technologies in critical energy infrastructures is creating additional potential points of attack. In contrast to conventional approaches protecting critical energy infrastructures, Zero-Trust-Architectures are able to meet the requirements resulting from these developments.

Due to the comparatively low level of adoption of Zero-Trust-Architectures in critical energy infrastructure sectors, only limited practice-related literature exists until today on the development and implementation of such architectures. Therefore, this paper presents the experiences gained from an ongoing development and implementation project in the form of an action-design research approach, thereby contributing to filling this research gap.

Keywords Cyber-Security · Zero-Trust-Architecture · Critical infrastructure · Network architecture · Action-design research

1 Ein zukunftsfähiges Konzept für die Cyber-Sicherheit kritischer Energieinfrastrukturen

Kritische Infrastrukturen bilden die Grundlage einer funktionierenden, modernen Gesellschaft. Typische Beispiele für kritische Infrastrukturen sind etwa Wasser, Energie und Ernährung (Blokus-Roszkowska und Dziula 2016). Eine Kompromittierung dieser Infrastrukturen kann zu verheerenden Auswirkungen wie weitreichenden Störungen und Gefahren für Leib und Leben führen (Aradau 2010). Der Schutz sowie die Sicherstellung des Betriebs kritischer Infrastrukturen ist deshalb von besonders hoher Relevanz. Zu den wichtigsten Schutzzielen im Kontext kritischer Infrastrukturen neben den klassischen Sicherheitszielen (Verfügbarkeit, Integrität und Vertraulichkeit) gehören Kontinuität und Resilienz, wodurch sowohl die Minimierung von Einschränkungen als auch eine schnellstmögliche Wiederherstellung der Funktionalität im Falle eines Ausfalls umgesetzt sein sollen (Blokus-Roszkowska und Dziula 2016). Während in der Vergangenheit hauptsächlich der physische Schutz vor Angriffen im Mittelpunkt stand, entstehen durch die zunehmende Digitalisierung kritischer Infrastrukturen neue Risiken und Angriffsszenarien (McCreight 2022; Yusta et al. 2011). U. a. durch die zunehmende Dezentralisierung von Infrastrukturen – besonders im Energiesektor-, sind digitale Technologien zu zentralen Bausteinen des kritischen Infrastrukturbetriebs geworden. So hat im Zuge der räumlichen Dezen-

tralisierung die Bedeutung von Fernzugriffen im Kontext mobilen Arbeitens oder die Vielzahl zu integrierender, vernetzter Geräte unterschiedlicher Organisationszugehörigkeiten stark zugenommen (Ackerman 2017; Gheorghe und Schlapfer 2006). Ein Resultat dieser Entwicklungen sind komplexere Netzwerkarchitekturen, in der signifikant mehr Systeme und Akteure miteinander interagieren und infolgedessen mehr Angriffspunkte entstehen (Moubayed et al. 2019; Chen et al. 2019). Typische Angriffsszenarien auf kritische Energieinfrastrukturen sind hierbei u. a. Angriffe auf Software-Lieferketten sowie die Verbreitung von Schadcode über reguläre Update-Mechanismen (Bundesamt für Sicherheit in der Informationstechnik 2022).

Herkömmliche (Netzwerk-) Sicherheitsarchitekturen zum Schutz kritischer Infrastrukturen sind diesen Gegebenheiten nicht ausreichend gewachsen (Compastié et al. 2016). Die meisten der entsprechend zugrunde liegenden Konzepte beruhen noch auf einer Trennung zwischen internen und externen Netzwerken, wie Buck et al. (2021) erläutern. Alle Benutzer:innen, Geräte und Dienste innerhalb dieser geschützten Netzwerke werden ohne weitere Prüfung als vertrauenswürdig eingestuft, während externe Benutzer:innen, Geräte und Dienste als nicht vertrauenswürdig gelten (Chen et al. 2019). Problematisch ist allerdings, dass heutige Netzwerkarchitekturen keine homogenen Systeme mehr sind, bei denen alle Applikationen im eigenen Rechenzentrum gehostet werden und Zugriffe primär von intern erfolgen. Vielmehr haben sich komplexe Strukturen entwickelt, welche sich u. a. aus On-Premises-Lösungen, externen Cloud-Services und IoT-Geräten zusammensetzen (Moubayed et al. 2019). Daher befinden sich viele Applikationen und Geräte heute nicht mehr ausschließlich in geschlossenen Netzwerken und Zugriffe erfolgen von überall. Infolgedessen können Angreifer Sicherheitsschwachstellen oder ungesicherte Geräte ausnutzen, um sich Zugang zu einem internen Netzwerk zu verschaffen und ungehindert im „sicheren“ Netzwerk zu operieren (Mcginthy und Michaels 2019; Moubayed et al. 2019). Zudem können auch böswillige „Insider:innen“ eine Bedrohung darstellen (Mehraj und Banday 2020; Pan und Yang 2018). Sowohl in der Wissenschaft als auch in der Praxis hat sich daher ein Konsens herausgebildet, wonach kein Netzwerk – ob intern oder extern – als generell vertrauenswürdig eingestuft werden sollte (Mehraj und Banday 2020; Zaheer et al. 2019).

Das Zero-Trust-Paradigma ist durch die Problematik des generell vorausgesetzten Vertrauens menschlicher oder maschineller Entitäten motiviert. Anstatt jegliche Art von als intern klassifizierten Zugriffen ohne weitere Prüfung zu erlauben, erfordert eine Zero-Trust-Architektur (ZTA) stets eine passende Autorisierung sowie Authentifizierung vor der Freigabe (D'Silva und Ambawade 2021). Selbst „interne“ Entitäten müssen ihre Vertrauenswürdigkeit demnach zunächst beweisen, anstatt dass diese – wie in traditionellen Architekturen – vorausgesetzt wird (Buck et al. 2021; Chen et al. 2019). Trotz erkennbarer Vorteile ist es ZTAs allerdings noch nicht gelungen, die bestehenden Lösungen flächendeckend zu ersetzen, weshalb bisher wenig praktische Erfahrung mit dem neuen Paradigma gesammelt werden konnte (He et al. 2022). Auch eine strukturierte Literaturrecherche von Buck et al. (2021) hat gezeigt, dass die bisherige Forschung insbesondere die Domäne der kritischen Infrastruktur nur unzureichend adressiert und entsprechende Einblicke in die Einführung von ZTAs erfordert.

Zur Anreicherung der bestehenden ersten Erfahrungen zu ZTAs im Bereich kritischer Infrastrukturen berichtet diese Arbeit aus einem Projekt über die prototypischen Entwicklungen sowie Implementierungen von ZTAs in drei Anwendungsfällen, welche nach dem Action Design Research (ADR) Prinzip nach Sein et al. (2011) durchführt wurden. Basierend auf den Erkenntnissen des laufenden Projekts wurden Handlungsempfehlungen abgeleitet, welche insbesondere die technischen und organisationalen Aufgabenbereiche der Einführung entsprechender Systeme adressieren. Neben der Erweiterung der Wissensbasis innerhalb der Wirtschaftsinformatik, hat diese Arbeit zum Ziel interessierten Praktiker:innen fundierte Erkenntnisse bereitzustellen, um bestehende Unsicherheiten durch einen Mangel an praktischen Erfahrungsberichten zu senken.

In den nächsten Abschnitten folgen neben einer Einführung in ZTAs, eine Vorstellung der betrachteten Anwendungsfälle sowie die Präsentation gewonnener Erkenntnisse, ehe im Anschluss die abgeleiteten Handlungsempfehlungen erläutert werden und eine Zusammenfassung sowie ein Ausblick diese Arbeit schließen.

2 Grundlagen von Zero-Trust-Architekturen in kritischen Energieinfrastrukturen

Eine zukunftsträchtige Absicherung kritischer Infrastrukturen bedarf eines ganzheitlichen und integrierten Ansatzes zum Schutz von Industrieanlagen (Isom 2019). Umzusetzen sind hierbei u. a. eine individuelle und feingranulare Absicherung von Applikationen und Geräten, die Analyse von Nutzerverhalten inkl. Kontextfaktoren (z. B. Ort und Zeitpunkt von Zugriffen) sowie eine Echtzeitüberprüfung des Datentransfers (Alcaraz und Zeadally 2015; Gadze et al. 2007). ZTAs werden in diesem Zusammenhang als passende Lösungen diskutiert (Ahmed et al. 2020). Gemäß des Zero-Trust-Ansatzes kann Nutzenden der Zugang zu einem Dienst in vollem Umfang oder zu bestimmten Funktionen bzw. Daten nur nach einer erfolgreichen Authentifizierung sowie im Falle von passenden Berechtigungen gewährt werden (Rose et al. 2020). Nutzende können in diesem Fall sowohl menschliche als auch maschinelle Entitäten umfassen (Rose et al. 2020). Die Überprüfung von Berechtigungen können hierbei neben den jeweiligen Zugriffsrechten weitere Faktoren und Informationsquellen wie die verwendeten Geräte oder Standortzeiten berücksichtigen (Omar und Abdelaziz 2020).

In Anwendungsfällen, die eine Echtzeitkommunikation erfordern, wie u. a. im kritischen Energieinfrastruktursektor häufig gegeben, kann eine Vielzahl an Authentifizierungen und Autorisierungsprüfungen jedoch zu höheren Zugriffszeiten führen, die eine Echtzeitkommunikation verhindern (Richardson und Goel 2022). Um eine effiziente Kommunikation in Echtzeit dennoch gewährleisten zu können, kann die zeitaufwendigere Authentifizierung – bspw. mittels Multifaktorauthentifizierung (MFA) – für einzelne Sitzungen einmalig durchgeführt und im Anschluss nur noch die Autorisierungen für Zugriffe geprüft werden. Ein vergleichbares Vorgehen ist etwa bei etablierten Standards wie TLS analog umgesetzt (Bhargavan et al. 2014; Eckert 2018).

Insgesamt handelt es sich bei ZTA nicht um eine fest definierte, technische Lösung, sondern um ein Lösungsparadigma, welches spezielle Prinzipien und Komponenten beinhaltet, die im Folgenden genauer vorgestellt werden (Rose et al. 2020). Zudem grenzt sich ZTA von bestehenden Instrumenten zur Sicherstellung von Netzwerksicherheit wie Firewalls, Virtual Private Networks (VPN) oder Identity und Access Management (IAM) insofern ab, als dass es sich bei Letzteren um Technologien und Ansätze handelt, die Teil von Netzwerkarchitekturen wie ZTAs sein können. Eine ZTA stellt also ein umfangreiches Sicherheitskonzept dar, das neben Cyber-Sicherheitstechnologien zusätzliche Aspekte wie u. a. die Systemumgebung, die Infrastruktur, Asset Management, oder Monitoring berücksichtigt (Mehraj und Banday 2020; Rose et al. 2020).

Obwohl sich bis heute eher generische ZTA-Standards herausgebildet haben, beinhalten alle hieraus entwickelten Lösungen mindestens folgende Komponenten: Policy Engine (PE), Policy Administrator (PA) und Policy Enforcement Points (PEPs). Während die PE über Zugriffserlaubnisse oder -verweigerungen anhand von konfigurierten Regeln entscheidet, nehmen PAs eingehende Zugriffsanfragen an und leiten diese an die PE weiter. Sofern der Zugriff genehmigt wurde, stellt der PA eine Verbindung zwischen der anfragenden Entität und der Ressource über PEPs her. PEPs setzen die Anweisungen der PE um und lassen nur von der PE genehmigte Zugriffe zu. Ein hiermit verbundenes wichtiges Prinzip von ZTAs lautet „vertraue niemals, kontrolliere immer“ und wird dadurch umgesetzt, dass es in ZTAs für Zugriffe auf Ressourcen keinen anderen Weg als über eine Anfrage über PAs gibt (Rose et al. 2020).

Die Entscheidungsgrundlage der PE stellen hierbei bspw. anwendungs- sowie domänenspezifische Regeln dar, die auf Nutzer:innen(-gruppen) mit entsprechenden Eigenschaften angewendet werden. Zudem können diese Regeln statisch (z. B. org. Zugehörigkeit eines Akteurs) oder dynamisch (z. B. Verhalten eines Akteurs) definiert sein (Pan und Yang 2018). Häufig verwendete Kriterien sind hierbei Informationen wie bspw. organisationsinterne Rolle, Standort, Zeitpunkt des Zugriffs, usw. (Rose et al. 2020). Bspw. könnten Funktionen wie die Notfalldeaktivierung von wichtigen Systemen auf eine bestimmte Gruppe und nur auf Arbeitszeiten eingegrenzt werden oder einige Wartungsfunktionen nur abrufbar sein, wenn sich Nutzende im unmittelbaren Umfeld der jeweiligen Maschine befinden. Bei der Definition dieser Regeln ist in ZTA zudem das Least Privilege-Prinzip zu berücksichtigen, nach dem Berechtigungen nur für individuell erforderliche Ressourcen erteilt werden dürfen (Eidle et al. 2017). Es ist daher essenziell, Zugriffsrichtlinien für alle Akteure passend zu definieren und deren Aktualität fortlaufend sicherzustellen (Rose et al. 2020). PAs sind in ZTAs für das Herstellen sowie für die Verwaltung von sicheren Verbindungen zwischen PE und PEPs verantwortlich (Rose et al. 2020). Der Schutz der PE als zentralen Ausfallpunkt ist also dadurch sichergestellt, dass Zugriffe niemals direkt, sondern jegliche Art von Kommunikation über den PA läuft (Rose et al. 2020).

3 Vorstellung der Anwendungsfälle und Umsetzung auf Basis von Action Design Research

Die Entwicklung einer ZTA für kritische Energieinfrastrukturen erfolgt in dieser Arbeit im Rahmen eines interdisziplinären Forschungsprojekts. Konkret wird an der Erforschung, Entwicklung, Prototypisierung und Evaluierung einer solchen Architektur für drei verschiedene Anwendungsfälle, die sich hinsichtlich der jeweiligen technischen Systeme, Akteurskonstellationen und der betrachteten Marktsegmente unterscheiden, gearbeitet. Näher zeichnen sich die betrachteten Systeme der Anwendungsfälle durch variierende Größen (u. a. Anzahl der Maschinen und Leistung) sowie verschiedene Grade von Dezentralität und Mobilität aus. Durch die unterhalb beschriebene Diversität der gewählten Anwendungsfälle kann eine Vielzahl an potenziellen Anforderungen und Herausforderungen berücksichtigt werden.

Der erste Anwendungsfall charakterisiert sich durch den Einsatz eines Steuerungs- und Monitoring-Gerätes in einem räumlich entfernten Kraftwerk sowie durch die Überführung der gesamten Einheit in eine ZTA. Ermöglicht werden soll die Weiterleitung von Steuerungsbefehlen an die Kraftwerksanlage sowie der Empfang aktueller Betriebsdaten aus dem laufenden Prozess zur Auswertung.

Im zweiten Anwendungsfall wird auf Basis einer ZTA die Anbindung eines Kraftwerks mit Kraft-Wärme-Kopplung (KWK) an einen Cloud-Service und die dortige Integration von Echtzeitdaten wie Strommarktpreisen und Wetterinformationen zur Optimierung des Anlagenfahrplans untersucht. Die Besonderheit dieses Anwendungsfalls ist neben der Vielzahl an potenziell zusätzlich zu steuernden Anlagen die Kombination mehrerer innovativer Technologien und Ansätze.

Im Rahmen des dritten Anwendungsfalls wird ein grundlegendes Problem mobiler Heizkraftwerke gelöst. Typische Einsatzzwecke dieser Systeme sind bspw. der Ersatz von ausgefallenen Wohnbeheizungen oder die Notversorgung von Krankenhäusern. Durch die Integration einer Fernsteuerungseinheit mithilfe einer ZTA wird eine dynamische Regelung des Betriebs ermöglicht und somit signifikante Effizienzsteigerungen realisiert, ohne zugleich den Bedarf an Personalaufwand zu erhöhen.

Trotz der Diversität und Unterschiede der Anwendungsfälle, sind die zentralen Ziele identisch: eine generelle Verbesserung der Cyber-Sicherheit sowie Effizienzsteigerungen des Infrastrukturbetriebs durch die sichere Nutzung digitaler Technologien – insbesondere in Bezug auf die Steuerung von Anlagen sowie die Verwaltung und Nutzbarkeit von gesammelten Daten.

Das Projekt wurde nach dem Vorbild des ADR nach Sein et al. (2011) konzipiert. Diese Methodik eignet sich besonders aufgrund der integrierten Betrachtungsweise des Entwicklungs- und Bewertungsprozesses für interdisziplinäre Projekte, in denen Akteure aus der Wissenschaft und Praxis zusammenarbeiten (Redlich et al. 2020). Konkret beinhaltet ADR vier Phasen:

1. Problemdefinition
2. Iterative Durchführung von Entwicklungs-, Interventions- und Evaluationsschritten
3. Reflexion und gewonnene Erkenntnisse

4. Formalisierung des Gelernten und Verallgemeinerung der generierten Lösungen zur Übertragung auf ähnliche Problemstellungen

Da sich das Projekt zum Zeitpunkt der Erstellung des Artikels in Phase 3 des ADR nach Sein et al. (2011) befindet, wird nachfolgend der Prozess sowie die vorläufigen Ergebnisse entlang der ersten drei Phasen vorgestellt.

3.1 Phase 1: Problemdefinition

Die Problemformulierung des Projekts beruht sowohl auf Praxiserfahrungen als auch auf bestehenden theoretischen Erkenntnissen. Hierzu wurden zunächst einige Workshops und Interviews mit den Beteiligten des Projekts durchgeführt, um die Praxisperspektive zu berücksichtigen (Myers und Newman 2007). So wurden innerhalb von Workshops die Anforderungen an die zu entwickelnde Architektur in einem iterativen Charakter erarbeitet. In Kombination mit diesen Ergebnissen, einer Erfassung des Ist-Zustandes und einer Umfeldanalyse der Systeme konnten schließlich Sollkonzepte entwickelt werden, die als Grundlage für die Entwicklung einer adäquaten Architektur dienten. Diese Zielbilder enthielten sowohl technische (z. B. geringe Latenz sowie hohe Fehlertoleranz und Resilienz) als auch nutzerakzeptanzbezogene Anforderungen (z. B. geringe Einschränkungen des operativen Betriebs). Darüber hinaus wurden Angriffsvektoren identifiziert, deren Mitigation in der Entwicklung der Zielarchitektur berücksichtigt werden sollte (z. B. sollten die Schnittstellen der integrierten Systeme nicht unkontrolliert abrufbar sein). Die theoretischen Grundlagen der Anforderungen sowie bestehende Herausforderungen von ZTA wurden in Buck et al. (2021) in Form einer multivokalen Literaturanalyse aufgearbeitet, um den gegenwärtigen Stand der Literatur zu inkludieren (Kitchenham und Charters 2007). Die wichtigsten Anforderungen waren hierbei ein modularer Charakter der zu entwickelnden Lösungen, die Integration geeigneter Mitigationsmaßnahmen für identifizierte Angriffsvektoren und die Kompatibilität der Lösungen mit bestehenden Standards im Kontext von ZTA.

3.2 Phase 2: Iterative Entwicklung, Intervention und Evaluation

Hinter dem Forschungsvorhaben steht ein interdisziplinäres Konsortium, welches neben den Betreibern und Dienstleistern im Kontext kritischer Infrastrukturen wie die SWW Wunsiedel GmbH und mobitherm GmbH auch die Forschungs- und Entwicklungskompetenzen der Universität Bayreuth sowie der TRUSTEQ GmbH und die Forschungstransferkompetenz der VK Energie GmbH vereint.

Abb. 1 stellt das generische Schema zur Entwicklung, Intervention und Evaluation von Artefakten mit einem Technologiefokus angewandt im Kontext des vorliegenden Forschungsprojektes dar. Die Universität Bayreuth, die TRUSTEQ und die VK Energie haben eine Alpha-Version des Artefakts entwickelt, die als Grundlage für die Umsetzung in den Anwendungsfällen diente. Daraufhin wurde diese Alpha-Version zusammen mit der Mobitherm und der SWW Wunsiedel in den Anwendungsfällen implementiert, zu einer Beta-Version kontinuierlich weiterentwickelt und hinterher hinsichtlich der Nutzerakzeptanz und des gegebenen Sicherheitsniveaus evaluiert.

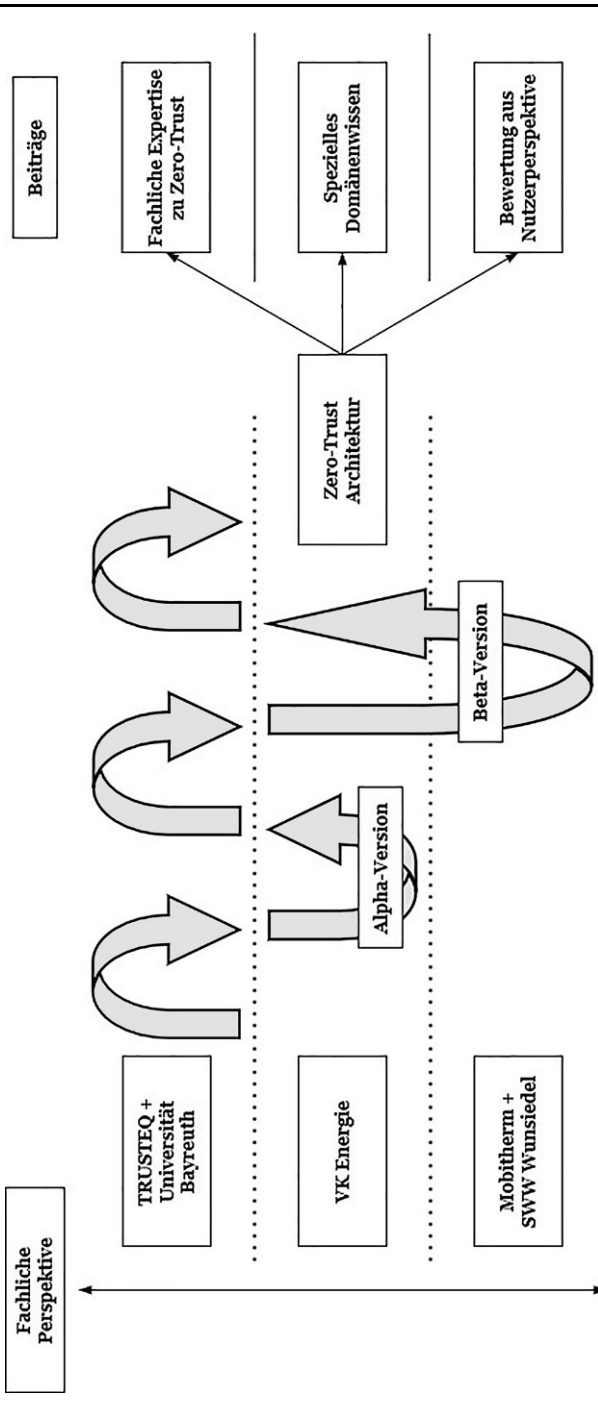

Abb. 1 Rollen der Projektbeteiligten während Phase 2 des ADR-Prozesses nach Sein et al. (2011)

Zum Einsatz kamen hierbei etablierte Methoden wie der UTAUT Fragebogen (Smith et al. 2011) oder eine mehrstufige sicherheitstechnische Überprüfung auf Basis des OSSTMM3 Frameworks (Institute for Security and Open Methodologies 2010). Jede Organisation lieferte innerhalb des Prozesses wertvolle Beiträge: die TRUSTEQ sowie die Universität Bayreuth brachten die fachliche Expertise zu ZTAs ein, die VK Energie lieferte spezielles Domänenwissen und mobitherm und die SWW Wunsiedel fokussierten sich auf die Bewertung der Lösung aus der Nutzerperspektive, die ebenfalls in das initiale Soll-Konzept einflossen.

Die nachfolgend vorgestellte Architektur stellt die erarbeitete Beta-Version des technischen Artefakts dar. Weil sich die Anforderungen und Voraussetzungen in der Praxis zwischen Anwendungsfällen grundlegend unterscheiden können, beinhaltet das Artefakt das technische Gerüst (inkl. aller Komponenten, Zusammenhänge und Funktionalitäten) der Architektur, das für den konkreten Einsatz fallspezifisch ausgestaltet werden muss.

Weil in den betrachteten Anwendungsfällen diverse nicht-internetfähige Systeme entweder individuell oder als Gruppe integriert werden mussten, wurden „Device Agent/Gateway Model“- sowie „Enclave-based“-Implementierungen von ZTA als grundlegende Strukturen für die Zielarchitektur gewählt (Rose et al. 2020). In beiden Variationen werden die PEPs durch Gateways umgesetzt. Der Unterschied zwischen ihnen ist lediglich das Verhältnis von Gateways und den zu integrierenden Ressourcen (z. B. Generatoren), die in der ZTA integriert werden. Laut Rose et al. (2020) sehen Implementierungen nach dem „Device Agent/Gateway Model“ eine eindeutige Zuordnung vor (d. h. ein Gateway pro Ressource), während Gateways in „Enclave-based“-Strukturen mehrere Ressourcen integrieren können (z. B. wenn diese einheitlich agieren oder Daten aggregiert gesammelt werden sollen). Alternativ hierzu könnten lokale Agenten auf den Nutzersystemen im „Resource Portal Model“ durch ein sogenanntes „Gateway Portal“ ersetzt werden. „Gateway Portals“ stellen allerdings eine zentrale Schwachstelle bzw. einen „Flaschenhals“ dar und wurden daher als Alternative verworfen (Rose et al. 2020).

In der Praxis dienen Gateways als Zugriffspunkte für Systeme und Industrieanlagen, wodurch ein direkter Zugriff auf die kritischen Systeme verhindert wird. Zunächst authentifiziert sich der Nutzende oder das IT-System mittels MFA gegenüber dem PA, welcher anschließend die Überprüfung der jeweiligen Berechtigungen bei jedem Zugriff mittels einer Kontaktaufnahme zur PE anstößt. Sofern der Zugriff genehmigt wurde, stellt der PA eine Verbindung zwischen der anfragenden Entität und der Ressource über das Gateway her. Die PE kennt zu jedem Benutzer die zugewiesenen Zugriffsberechtigungen und kann zur einfacheren Integration in ein Organisationsnetzwerk auf einen vorhandenen Identitätsprovider, wie das Active Directory von Microsoft, zurückgreifen. Die PE wird als Cloud-Service gehostet, wohingegen das Gateway die Verbindungsstelle zwischen dem Internet und dem „Local Area Network“ (LAN) der Organisation darstellt. Damit das breite Spektrum an in kritischen Energieinfrastrukturen eingesetzten Anlagen in eine ZTA integriert werden kann, wird zumeist eine individuelle Anbindung der Industrieanlage benötigt. Im Falle der Integration von nicht-internetfähigen Systemen ist zudem die Entwicklung von Schnittstellenlösungen erforderlich. Zu diesem Zweck sind die Gateways der Prototypen in der vorliegenden Zielarchitektur auf Basis von RaspberryPis mit

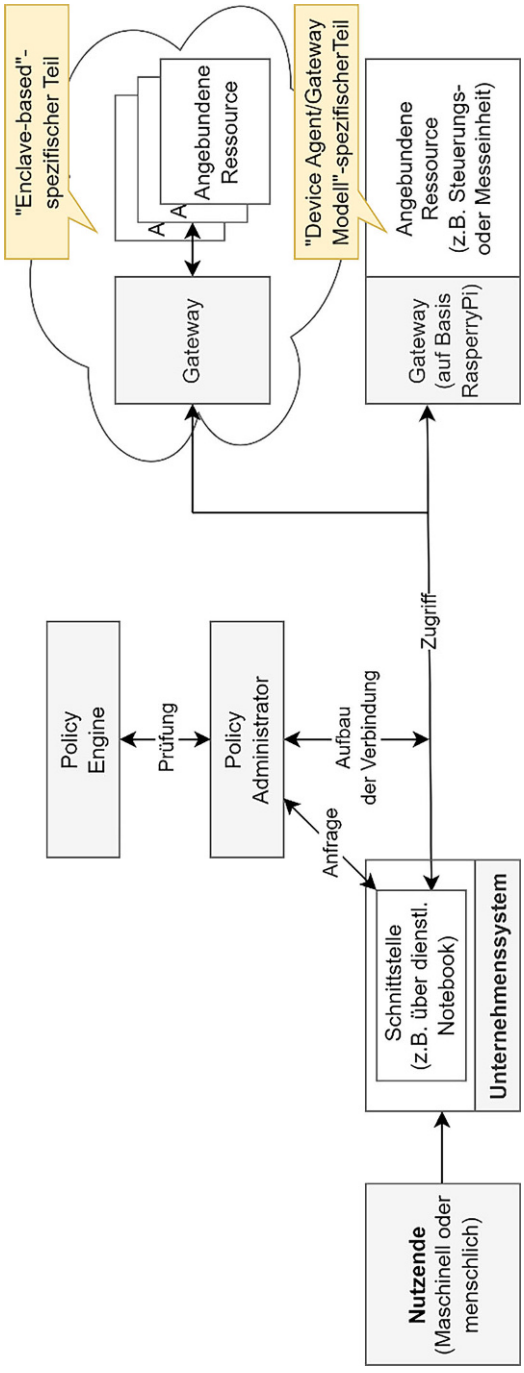

Abb. 2 Architektur zur Anlagensteuerung im Kontext kritischer Infrastrukturen auf Basis von Rose et al. (2020)

Netzwerkmodulen umgesetzt. Abb. 2 zeigt die vereinfachte Struktur der bestimmten Zielarchitektur.

3.3 Phase 3: Reflexion und gewonnene Erkenntnisse

In der dritten Phase von ADR geht es um die Reflexion und die gewonnenen Erkenntnisse entlang der ersten zwei Phasen. Diese Phase verläuft also parallel zur Problemdefinition sowie zum Entwicklungsprozess des Artefaktes, weshalb sich auch die Ergebnisse dieser Phase auf die Gesamtheit des Gelernten während der ersten zwei Phasen bezieht (Sein et al. 2011).

Neben den Lösungen einzelner Herausforderungen hat sich über die bisherige Projektlaufzeit eine zentrale Erkenntnis immer weiter herauskristallisiert, auf die sich im Folgenden konzentriert werden soll: Die Kernproblematik bei der Einführung von ZTAs im kritischen Energieinfrastruktursektor liegt darin, dass durch die vielen verschiedenen technischen Systeme, die integriert werden müssen, die Aufwände zur Anbindung an die Architektur schnell stark steigen können. Unter Umständen skaliert die Entwicklung und Implementierung einer ZTA also schlecht. Es ist daher essenziell, genau zu analysieren, wie groß diese Aufwände sein werden (bzw. ob es begünstigende Faktoren gibt) und zu bestimmen, wie groß der Mehrwert der neuen Netzwerksicherheitsarchitektur sein wird.

Die Autor:innen möchten interessierten Praktiker:innen daher im kommenden Abschnitt vier wichtige Handlungsempfehlungen zur Verfügung stellen, um bei der kosteneffizienten Einführung einer ZTA im kritischen Energieinfrastruktursektor zu unterstützen.

4 Handlungsempfehlungen zur Einführung einer Zero-Trust-Architektur im kritischen Energieinfrastruktursektor

Als Ergebnis der dritten Phase des ADR-basierten Entwicklungsprozesses, wurden vier besonders wirkungsvolle Handlungsempfehlungen für eine kosteneffiziente Einführung einer ZTA im kritischen Energieinfrastruktursektor erarbeitet. Während einige technische Voraussetzungen erfüllt sein sollten, können auch mehrere organisationale Faktoren begünstigend für die Einführung einer ZTA sein. Tab. 1 fasst die einhergehenden Handlungsempfehlungen des Projektteams zusammen, bevor diese nachfolgend detaillierter erläutert werden.

4.1 [TH1] Die Eignung bestehender Systeme prüfen

Nicht jede Hardware und Software ist für den Einsatz in einer ZTA gleichermaßen geeignet. Bestimmte Gegebenheiten erleichtern die Umsetzung des Konzeptes und können somit auch den Aufwand bei der Einführung verringern. Daher sollten die bestehenden IT-Systeme bezüglich ihrer Kompatibilität im Sinne der Modularität und der verwendeten Netzwerkprotokolle geprüft werden. Im Projekt war bspw. die Einführung eines Identitätsproviders für die Festlegung der Zugangsregelung von großer Relevanz. Sofern dieser bereits vorhanden und als ein unabhängiges

Tab. 1 Handlungsempfehlungen zur Einführung einer Zero-Trust-Architektur im kritischen Energieinfrastruktursektor

Technische Handlungsempfehlungen	*Organisationale Handlungsempfehlungen*
[TH1] Die Eignung bestehender Systeme prüfen **1. Modularität** **2. Netzwerkprotokolle**	*[OH1]* Die Anforderungen der Geschäftsprozesse evaluieren **1. Remotezugriffe** **2. Dezentralität von Anwendungen**
[TH2] Die Wiederverwendbarkeit vorhandener Sicherheitselemente kontrollieren **1. Zertifizierungsstelle** **2. Authentifizierungsmechanismen**	*[OH2] Ein holistisches* Realisierungskonzept entwickeln **1. Detaillierte Planung der Umstellung inkl. der Implikationen auf Systeme** **2. Realisierung von Synergieeffekten durch kombinierte Technologieeinführungen**

Modul gestaltet ist, kann die direkte Einbindung in die Gesamtarchitektur erfolgen. Diese Modularität begünstigte die Einführung der ZTA, da bereits auf bestehende Infrastruktur zur Abbildung der Identitäten zurückgegriffen werden konnte.

Damit bestehende Lösungen in eine ZTA überführt werden können, sind zudem einige Protokolle zum Netzwerkzugriff besser für eine Integration geeignet als andere. Tendenziell gilt: je standardisierter ein Protokoll ist, desto einfacher lässt es sich implementieren (besonders verbreitet ist z. B. HTTPS). Im Kontext von kritischen Infrastrukturen kann dies problematisch werden, da proprietäre Protokolle, welche oftmals im Umfeld von Maschinen und vernetzten Anlagen genutzt werden, die Entwicklung von Übersetzungsmodulen erfordern. Dies kann aufwändig und teuer sein. So musste z. B. im Projekt das branchenspezielle Kommunikationsprotokoll BacNet in HTTPS übersetzt werden, um mit dem Gateway interagieren zu können.

4.2 [TH2] Die Wiederverwendbarkeit vorhandener Sicherheitselemente kontrollieren

Vor der Einführung von ZTAs im kritischen Energieinfrastruktursektor sollten bereits vorhandene Cyber-Security-Technologien und -Konzepte erfasst und evaluiert werden. Da eine ZTA durch die Kombination verschiedener Elemente entsteht und in modernen Cyber-Sicherheitsstrukturen ein Teil oftmals bereits vorhanden ist, muss dieser nicht erneut eingeführt werden. Dies betrifft z. B. Zertifizierungsstellen oder Identitätsprovider; während hingegen ZTA-spezifische Elemente (wie PEs) in der Regel nicht bereitstehen. In dem vorliegenden Projekt wurden zwei wesentliche Elemente identifiziert:

1. Einerseits ist eine bereits vorhandene Zertifizierungsstelle inklusive Rechteabbildung der Nutzer:innen von Vorteil, da Rechte durch Zertifikate abgebildet werden. Daher gilt es zu ermitteln, ob eine Public-Key-Infrastruktur (PKI) bereits vorhanden ist, die die jeweiligen Zertifizierungsstellen nutzen können. Im Projekt ist dabei aufgefallen, dass insbesondere bei kleineren Betreibern kritischer Infrastrukturen solche Zertifizierungsstellen häufig nicht vorhanden sind.
2. Da ZTAs zudem auf feingranulare Zugriffskontrollen setzen, sind sichere Authentifizierungsmechanismen unabdingbar. Sind in einem System bereits entsprechend

sichere Authentifizierungsmechanismen, wie bspw. MFA vorhanden, so müssen diese nicht speziell für die Umstellung auf eine ZTA eingeführt werden.

4.3 [OH1] Die Anforderungen der Geschäftsprozesse evaluieren

Neben den technischen Voraussetzungen sollten auch die Geschäftsprozesse einige Eigenschaften aufweisen, damit die Einführung einer ZTA einen Vorteil erzielen kann. Bei ZTAs handelt es sich um Lösungen zur Absicherung von Netzwerkzugriffen. Wenn bei Anwendungsfällen allerdings nur wenig (Fern-) Zugriffe durch tendenziell wenig Entitäten auf die Infrastruktur erfolgen, so ist möglicherweise die Umstellung der Sicherheitsarchitektur nicht zielführend. Konkret bedeutet dies, dass sofern nur wenige, einfach zu überwachende Zugriffe auf eine Anlage stattfinden (bspw. beim räumlich zentralisierten Kraftwerksbetrieb), herkömmliche Mechanismen (z. B. die Abschottung durch Perimeter Firewalls) ihren Zweck ausreichend erfüllen. Da gerade im Umfeld von erneuerbaren Energieinfrastrukturen allerdings oftmals eine hohe Dezentralität, z. B. durch verschiedenste Technologien an unterschiedlichen Standorten vorherrscht, wodurch eine ausreichend komplexe und dezentrale Zugriffslage gegeben ist, kann sich die Einführung einer ZTA häufig lohnen.

4.4 [OH2] Ein holistisches Realisierungskonzept entwickeln

Eine weitere organisationale Maßnahme ist die Erstellung eines holistischen Realisierungskonzepts hin zu einer ZTA. Da möglicherweise Anpassungen der Netzwerkarchitektur notwendig sind, ist eine detaillierte Analyse des Status Quo und eine Kostenaufstellung für einen potenziellen Umstieg unabdingbar. Aufgrund der womöglich tiefgreifenden Änderungen sollte diese Gelegenheit auch dazu genutzt werden, die kombinierte Einführung von anderen Technologien oder von neuen Funktionalitäten zu prüfen. In einem der Anwendungsfälle konnte etwa neben der generellen Optimierung des Sicherheitsniveaus mithilfe der implementierten ZTA (nachgewiesen im Rahmen einer mehrstufigen sicherheitstechnischen Überprüfung) die Funktionalität zur Fernsteuerung von Industrieanlagen ergänzt werden.

Darüber hinaus muss insbesondere bei kritischen Infrastrukturen eine ausreichende Kontinuität der Funktionsweise aller Anlagen sichergestellt werden, weshalb die Implikationen einer Umstellung auf alle betroffenen Systeme erfasst und berücksichtigt werden sollten.

5 Fazit

Der vorliegende Forschungsbeitrag bietet Einblicke in die Einführung einer ZTA im Umfeld kritischer Energieinfrastrukturen. In diesem Kontext wurde eine grundlegende Architektur entwickelt und in drei verschiedenen Anwendungsfällen umgesetzt. Basierend auf einem technischen Artefakt als Ergebnis eines ADR-Entwicklungsprozesses wurden Handlungsempfehlungen für vergleichbare Vorhaben abgeleitet,

die interessierten Praktiker:innen bei der kosteneffizienten Einführung von ZTAs unterstützen sollen. Diese umfassen die Prüfung der Eignung bestehender Systeme, die Kontrolle aktueller Sicherheitselemente auf Wiederverwendbarkeit, die Evaluation der Anforderungen der Geschäftsprozesse sowie die Entwicklung eines holistischen Realisierungskonzepts.

Die vorgestellte Forschung unterliegt Grenzen. Sie basiert u. a. auf einer ersten Version eines ADR-orientierten Vorgehens. Evaluation und Untersuchungen in der Praxis sind insbesondere über einen längeren Zeitraum hinweg durchzuführen, um ein nachhaltiges Verständnis über die Cyber-Sicherheit und verwandte Prozesse zu erlangen. Zum anderen wurden die Perspektiven aller Endnutzer:innen bisher nicht vollständig evaluiert, welche jedoch einen maßgeblichen Effekt auf den Erfolg und die Umsetzung von Cyber-Sicherheitsmaßnamen haben könnten.

Aufgrund dieser Einschränkungen lassen sich weitere Forschungsvorhaben für die Zukunft ableiten. Insbesondere mangelt es aufgrund des jungen Forschungsfelds an längerfristigen Studien. Außerdem wird eine stärkere Einbindung von Endnutzer:innen in die Forschung rund um ZTAs empfohlen und bereits in einschlägiger Literatur als essentieller Bereich deklariert (Kerman et al. 2020). Vor dem Hintergrund steigender Cyber-Sicherheitsrisiken in kritischen Infrastrukturen sind ZTAs vielversprechende Konzepte, deren Entwicklungen es in Zukunft aufmerksam zu beobachten gilt.

Danksagung Dieses Forschungsprojekt wird durch das Bayerische Staatsministerium für Wirtschaft, Landesentwicklung und Energie (StMWi) im Rahmen des Bayerischen Verbundforschungsprogramms (BayVFP) – Förderlinie „Digitalisierung“ gefördert.

Funding Open Access funding enabled and organized by Projekt DEAL.

Literatur

Ackerman P (2017) Industrial cybersecurity; efficiently secure critical infrastructure systems. Packt Publishing, Birmingham

Ahmed I, Nahar T, Urmi SS, Taher KA (2020) Protection of sensitive data in zero trust model. In: Proceedings of the international conference on computing advancements. Association for Computing Machinery, New York, S 1–5

Alcaraz C, Zeadally S (2015) Critical infrastructure protection: requirements and challenges for the 21st century. Int J Crit Infrastructure Prot 8:53–66. https://doi.org/10.1016/j.ijcip.2014.12.002

Aradau C (2010) Security that matters: critical infrastructure and objects of protection. Secur Dialogue 41:491–514. https://doi.org/10.1177/0967010610382687
Bhargavan K, Fournet C, Kohlweiss M, Pironti A, Strub P-Y, Zanella-Béguelin S (2014) Proving the TLS handshake secure (as it is). In: Garay JA, Gennaro R (Hrsg) Advances in cryptology—CRYPTO 2014. 34th annual cryptology conference. Springer, Berlin, Heidelberg, S 235–255
Blokus-Roszkowska A, Dziula P (2016) An approach to identification of critical infrastructure systems. AIP Conf Proc 1738:1–4. https://doi.org/10.1063/1.4952223
BSI (2022) Die Lage der IT-Sicherheit in Deutschland 2022. Bundesamt für Sicherheit in der Informationstechnik, Bonn
Buck C, Olenberger C, Schweizer A, Völter F, Eymann T (2021) Never trust, always verify: a multivocal literature review on current knowledge and research gaps of zero-trust. Comput Secur 110:1–26. https://doi.org/10.1016/j.cose.2021.102436
Chen Y, Hu H, Cheng G (2019) Design and implementation of a novel enterprise network defense system by maneuvering multi-dimensional network properties. Front Inf Technol Electron Eng 20:238–252. https://doi.org/10.1631/FITEE.1800516
Compastié M, Badonnel R, Festor O, He R, Kassi-Lahlou M (2016) A software-defined security strategy for supporting autonomic security enforcement in distributed cloud. In: 8th IEEE international conference on cloud computing technology and science CloudCom 2016, Luxembourg City, Luxembourg, 12–15 December 2016 IEEE, Piscataway, S 464–467
D'Silva D, Ambawade DD (2021) Building a zero trust architecture using kubernetes. In: 6th international conference for convergence in technology Pune, India, Apr. 02-04, 2021 IEEE, Piscataway, S 1–8
Eckert C (2018) IT-Sicherheit; Konzepte – Verfahren – Protokolle. De Gruyter Oldenbourg, Berlin, Boston
Eidle D, Ni SY, DeCusatis C, Sager A (2017) Autonomic security for zero trust networks. In: Chakrabarti S, Saha HN (Hrsg) 8th annual ubiquitous computing, electronics and mobile communication conference. IEEE, Piscataway, S 288–293
Gadze J, Pissinou N, Makki K (2007) Wireless networked—based sensing for protection and decentralized control of critical infrastructures. In: 2007 IEEE international conference on networking, sensing, and control London, United Kingdom, 15–17 April 2007 IEEE, Piscataway, S 644–649
Gheorghe AV, Schlapfer M (2006) Ubiquity of digitalization and risks of interdependent critical infrastructures. In: International conference on systems, man and cybernetics. IEEE, Piscataway, S 580–584
He Y, Huang D, Chen L, Ni Y, Ma X (2022) A survey on zero trust architecture: challenges and future trends. Wirel Commun Mob Comput 2022:1–13. https://doi.org/10.1155/2022/6476274
ISECOM (2010) OSSTMM 3—the open source security testing methodology manual; contemporary security testing and analysis
Isom PK (2019) IT modernisation in the energy sector: preventing cyberthreats to critical infrastructure. Cyber Secur 3:208–219
Kerman A, Borchert O, Rose S (2020) Implementing a zero trust architecture; project description. National Cybersecurity Center of Excellence, National Institute of Standards and Technology, Rockville, Gaithersburg
Kitchenham B, Charters SM (2007) Guidelines for performing systematic literature reviews in software engineering; version 2.3. Keele Univesity, University of Durham, Keele, Durham
McCreight R (2022) Space based platforms and critical infrastructure vulnerability. In: Nichols RK, Carter CM, Hood JP, Jackson MJ, Joseph S, Larson H, Lonstein WD, Mai R, McCreight R, Mumm HC, Oetken M, Pritchard MJ, Ryan JJ, Sincavage SM, Slofer W (Hrsg) Space systems: emerging technologies and operations. New Prairie Press, Los Angeles
Mcginthy JM, Michaels AJ (2019) Secure industrial Internet of things critical infrastructure node design. Ieee Internet Things J 6:8021–8037. https://doi.org/10.1109/JIOT.2019.2903242
Mehraj S, Banday MT (2020) Establishing a zero trust strategy in cloud computing environment. In: 2020 international conference on computer communication and Informatics. IEEE, Piscataway, S 1–6
Moubayed A, Refaey A, Shami A (2019) Software-defined perimeter (SDP): state of the art secure solution for modern networks. IEEE Netw 33:226–233. https://doi.org/10.1109/MNET.2019.1800324
Myers MD, Newman M (2007) The qualitative interview in IS research: examining the craft. Inf Organ 17:2–26. https://doi.org/10.1016/j.infoandorg.2006.11.001
Omar RR, Abdelaziz TM (2020) A comparative study of network access control and software-defined perimeter. In: Uskenbayeva R (Hrsg) Proceedings of the 6th international conference on engineering & MIS 2020. Association for Computing Machinery, New York, S 1–5
Pan J, Yang Z (2018) Cybersecurity challenges and opportunities in the new "edge computing + IoT" world. In: Ahn G-J, Gu G, Hu H, Shin S (Hrsg) Proceedings of the 2018 ACM international work-

shop on security in software defined networks & network function virtualization. Association for Computing Machinery, New York, S 29–32

Redlich B, Becker F, Lattemann C, Robra-Bissantz S (2020) Wie Action Design Research und Design Thinking ein Innovationsprojekt zum Erfolg führen. In: Gronau N, heine M, Poustcchi K, Krasnova H (Hrsg) 15th International Conference on Wirtschaftsinformatik. GITO, Berlin, S 1616–1631

Richardson B, Goel P (2022) Enhancing zero trust security with data | NVIDIA technical blog. https://developer.nvidia.com/blog/enhancing-zero-trust-security-with-data/. Zugegriffen: 12. Dez. 2022

Rose S, Borchert O, Mitchell S, Connelly S (2020) NIST SP 800-207; zero trust architecture. National Institute of Standards and Technology, Gaithersburg

Sein MK, Henfridsson O, Purao S, Rossi M, Lindgren R (2011) Action design research. MISQ 35:37–56. https://doi.org/10.2307/23043488

Smith HJ, Dinev T, Xu H (2011) Information privacy research: an interdisciplinary review. MISQ 35:989–1015. https://doi.org/10.2307/41409970

Yusta JM, Correa GJ, Lacal-Arántegui R (2011) Methodologies and applications for critical infrastructure protection: state-of-the-art. Energy Policy 39:6100–6119. https://doi.org/10.1016/j.enpol.2011.07.010

Zaheer Z, Chang H, Mukherjee S, van der Merwe J (2019) EZTrust: network-independent zero-trust perimeterization for microservices. In: Proceedings of the 2019 ACM symposium on SDN research. Association for Computing Machinery, New York, S 49–61