Deutsches Zentrum für
Schienenverkehrsforschung beim

Eisenbahn-Bundesamt

Berichte
des Deutschen Zentrums
für Schienenverkehrsforschung

Bericht 37 (2023)

# Studie „Security und geplanter Technologieeinsatz“


Berichte des Deutschen Zentrums
für Schienenverkehrsforschung, Bericht 37 (2023)
Projektnummer 2021-17-S-1202

# Studie „Security und geplanter Technologieeinsatz“

von

Michael Nord, Bernd Leppla,
Industrieanlagen-Betriebsgesellschaft mbH, 85521 Ottobrunn

Prof. Dr. Dietmar P. F. Möller,
Institut für Mathematik, TU Clausthal, 38678 Clausthal-Zellerfeld

Patrik Krause,
3DSE Management Consultants GmbH, 80335 München

Nikolai Lenski,
Fraunhofer AISEC, 14199 Berlin

Peter Czerkewski,
Institut für Bahntechnik GmbH, 10587 Berlin

im Auftrag des Deutschen Zentrums für Schienenverkehrsforschung beim Eisenbahn-Bundesamt

# Impressum

HERAUSGEBER
Deutsches Zentrum für Schienenverkehrsforschung beim Eisenbahn-Bundesamt

August-Bebel-Straße 10
01219 Dresden

www.dzsf.bund.de

DURCHFÜHRUNG DER STUDIE
Industrieanlagen- Betriebsgesellschaft MBH
Einsteinstraße 20
85521 Ottobrunn

Technische Universität Clausthal
Institut für Mathematik
Adolph-Roemer-Straße 2a
38678 Clausthal-Zellerfeld

3DSE Management Consultants GmbH
Seidlstraße 18 a
80335 München

Fraunhofer AISEC
Breite Straße 12
14199 Berlin

IFB Institut für Bahntechnik GmbH
Carnotstraße 6
10587 Berlin

ABSCHLUSS DER STUDIE
April 2022

REDAKTION
DZSF
Dr. Lukas Iffländer, Dr. Kristin Mühl, Forschungsbereich Sicherheit

BILDNACHWEIS
IABG GmbH

PUBLIKATION ALS PDF
https://www.dzsf.bund.de/Forschungsergebnisse/Forschungsberichte

ISSN 2629-7973

doi: 10.48755/dzsf.230004.01

Dresden, Februar 2023

# Inhaltsverzeichnis

# Kurzbeschreibung

Cybersecurity und neue Technologien sind in den heutigen Industriesektoren Kernelemente der digitalen Transformation. Sie haben enorme Auswirkungen auf industrielle Steuerungssysteme und -prozesse und sind Grundlage für fortschrittliches, effizientes und effektives Wirtschaften. Allerdings werden durch sie auch schwerwiegende Sicherheitsprobleme hervorgerufen. Diese sind durch den massiven Einsatz sowohl digitaler als auch neuer Technologien und deren Vernetzung über das Internet im Rahmen der digitalen Transformation verstärkt worden. Hierdurch können Sicherheitslücken entstehen, die aus Sicherheitsverletzungen durch Cyberangriffe resultieren. Damit steht der Begriff „Cybersecurity“ für die Notwendigkeit eines Schutzes vor Cyberangriffen.

Vor diesem Hintergrund wurde die Studie „Security und geplanter Technologieeinsatz“ mit Bezug auf den Eisenbahnsektor durchgeführt. Im Bericht der European Network and Information Security Agency (ENISA) mit dem Titel „Railway Cybersecurity“ [1] wird hierzu klar konstatiert: „Bisher scheint der Eisenbahnsektor kein direktes Ziel für Cyberangriffe gewesen zu sein“. Jedoch haben sich Cyberangriffe und Vorfälle in den vergangenen Jahren verstärkt, wovon auch der Eisenbahnsektor als sicherheitskritische Branche betroffen war. Dies hat seine Ursache im allgegenwärtigen, hohen Angriffspotenzial auf die industriellen, öffentlichen und privaten Sektoren, welches aus dem mit der digitalen Transformation verbundenen Wandel sowie seinen Auswirkungen auf die Cybersecurity und den Einsatz neuer Technologien entsteht.

Die Studie „Security und geplanter Technologieeinsatz“ untersucht den Ist-Zustand zur Cybersecurity und den geplanten Technologieeinsatz im Eisenbahnsektor auf der Grundlage einer Onlinebefragung und darauf aufbauender Interviews. Mit diesem Ansatz sollen Inkonsistenzen, die sich gegebenenfalls aus der Onlinebefragung ergeben haben, durch die Interviews untersucht und ausgeräumt werden. Die aus der Onlinebefragung gewonnenen Daten werden mit dem NIST-Reifegradmodell [2] ausgewertet, welches hinsichtlich mehrerer Kenngrößen, wie Mitarbeiteranzahl, Wissensstand zum abgefragten Thema oder dem vorhandenen Potenzial neue Technologien einzuführen, gegliedert ist. Als weitere Bewertungsmethode wurde die SWOT-Analyse (Strengths, Weaknesses, Opportunities, Threats) genutzt, die bezogen auf Stärken, Schwächen, Möglichkeiten und Gefahren vertiefende Erkenntnisse im Rahmen der Interviews zur Cybersecurity und zum Einsatz neuer Technologien im Eisenbahnsektor ermöglicht.

Die Ergebnisse zeigen, dass der größte Teil des Sektors beim Thema Cybersecurity noch kein Basisschutzniveau erreicht hat. Besonders negativ fällt der Untersektor der Eisenbahninfrastrukturunternehmen auf. Beim Einsatz neuer Technologien bestehen noch starkes Innovationspotenzial und mangelndes Verständnis für viele Technologien. Unternehmensgröße und die Zugehörigkeit zu einzelnen Untersektoren wurden als relevante Einflussgrößen identifiziert. Als Fazit daraus wurden mehrere Handlungsempfehlungen abgeleitet, mit deren Umsetzung Politik und Verbände den Sektor unterstützen können. Dazu zählen beispielsweise themenbezogene, akkreditierte Ansprechpartner, zielorientierte Zertifikatsprogramme und weitere Maßnahmen.

# Abstract

Cybersecurity and new technologies are key elements of today's digital transformation of the industrial sectors. New technologies have an enormous impact on industrial control systems as well as processes and are the basis for advanced, efficient, and effective management. However, they also create serious security issues. These have only intensified due to the massive use of both digital and new technologies and their networking via the Internet as part of the digital transformation. As a result, security vulnerabilities can arise from security breaches caused by cyberattacks. Thus, the term "cybersecurity" stands for the need for protection against cyberattacks.

Against this background, the study "Security and Planned Technology Adoption" was conducted with a focus on the railroad sector. The report of the European Network and Information Security Agency (ENISA) entitled "Railway Cybersecurity" [1] clearly states: "So far, the railroad sector does not seem to constitute a direct target for cyberattacks. However, cyberattacks and incidents intensified in recent years, which also affected the railroad sector as a safety-critical industry. This effect is due to the ubiquitous, high attack Potenzial on the industrial, public, and private sectors resulting from the changes associated with digital transformation and their impact on cybersecurity and the adoption of new technologies.

The study "Security and Planned Technology Adoption" examines the current state of cybersecurity and the planned adoption of technology in the rail sector based on an online survey and interviews that build on it. This approach is intended to investigate and resolve inconsistencies that may arise from the online survey through the interviews. We evaluated the data obtained from the online survey using the NIST maturity model [2], which incorporates several parameters such as the number of employees, the knowledge level regarding the surveyed topic, and the existing Potenzial for introducing new technologies. As a further evaluation method, we used the SWOT analysis (Strengths, Weaknesses, Opportunities, Threats), which provides in-depth insights in relation to strengths, weaknesses, opportunities and threats in the context of the interviews on cybersecurity and the use of new technologies in the railroad sector.

The results show that most of the sector has not yet reached a basic level of protection when it comes to cybersecurity. The subsector of railroad infrastructure operators stands out in a particularly adverse manner. Strong Potenzial for innovation and a lack of understanding of many technologies still exists when it comes to the adoption of new technologies. Company size and affiliation with individual subsectors are relevant influencing factors. As a conclusion, we derived several recommendations for actions that policymakers and associations can implement to support the sector. These include, for example, topic-related, accredited contact persons, target-oriented certificate programs and other measures.

# Abkürzungsverzeichnis

| Abkürzung | Bedeutung |
|---|---|
| AEG | Allgemeines Eisenbahngesetz |
| AG | Aktiengesellschaft |
| AP | Arbeitspaket |
| AVG | Albtal-Verkehrs-Gesellschaft mbH |
| BeNEX | „Bene Nexus“ (lateinisch für Gute Verbindung), ein Hamburger EVU |
| BGBl | Bundesgesetzblatt |
| BOB | Bayerische Oberlandbahn GmbH |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| BSI-KritisV | BSI-Kritisverordnung |
| CEO | Chief Executive Officer |
| CIO | Chief Information Officer |
| CRRC | China Railway Rolling Stock Corporation Limited |
| CSF | Cybersecurity-Framework |
| csv | comma-separated values - Dateinamenserweiterung |
| DB | Deutsche Bahn |
| DDoS | Distributed-Denial-of-Service |
| DE | Detect |
| DoS | Denial-of-Service |
| DRE | Deutsche Regionaleisenbahn GmbH |
| DSGVO | Datenschutz-Grundverordnung |
| DZSF | Deutsches Zentrum für Schienenverkehrsforschung |
| EBA | Eisenbahn-Bundesamt |
| ECM | entity in charge of maintenance (Instandhaltungsverantwortliche Stelle) |
| EG | Europäische Gemeinschaft |
| EIU | Eisenbahninfrastrukturunternehmen |
| ENISA | European Union Agency for Cybersecurity |
| EVB | Eisenbahnen und Verkehrsbetriebe Elbe-Weser GmbH |
| EVU | Eisenbahnverkehrsunternehmen |
| FaaS | Function-as-a-Service |
| GAVD | Go-Ahead Verkehrsgesellschaft Deutschland GmbH |
| GmbH | Gesellschaft mit beschränkter Haftung |
| HTML | Hypertext Markup Language |
| HVLE | Havelländische Eisenbahn AG |
| IaaS | Infrastructure-as-a-Service |
| ID | Identity |
| IFB | Institut für Bahntechnik GmbH |
| IIC | Industrial Internet Consortium |
| IoT | Internet der Dinge (Internet of Things) |

| Abkürzung | Bedeutung |
|---|---|
| IT | Informationstechnologie |
| ITSG | Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) |
| KI | Künstliche Intelligenz |
| KRITIS | Kritische Infrastrukturen |
| KVP | kontinuierlicher Verbesserungsprozess |
| LTE | Long Term Evolution |
| ML | Machine Learning |
| NaaS | Network-as-a-Service |
| NE | Nichtbundeseigene Eisenbahn(en) |
| NEB | Niederbarnimer Eisenbahn AG |
| NFV | Networks Function Virtualization |
| NIST | National Institute of Standards and Technologies |
| NWB | NordWestBahn GmbH |
| ODEG | Ostdeutsche Eisenbahn GmbH |
| ÖPNV | Öffentlicher Personennahverkehr |
| OT | Betriebstechnik |
| OTT | Over the Top |
| PaaS | Platform-as-a-Service |
| PR | Protect |
| RC | Recover |
| RDC | Railroad Development Corporation |
| Ril | Richtlinie |
| RS | Respond |
| SaaS | Software-as-a-Service |
| SBB | Schweizerische Bundesbahnen AG |
| SDN | Software-defined Network |
| SE | Societas Europaea (Rechtsform für Aktiengesellschaften in der Europäischen Union) |
| SMLC | Smart Manufacturing Leadership Coalition |
| SNCF | Société nationale des chemins de fer français |
| SWOT | Akronym, das aus den Anfangsbuchstaben der folgenden englischen Begriffe gebildet wird: Strenghts, Weaknesses, Opportunities und Threats. |
| TXL | TX Logistik AG |
| VDB | Verband der Bahnindustrie in Deutschland |
| VDV | Verband Deutscher Verkehrsunternehmen |
| VIS | Verkehrs Industrie Systeme GmbH |
| WEG | Württembergische Eisenbahn-Gesellschaft mbH |
| WSN | Wireless Sensor Networks |

# 1 Einleitung

Die durch die fortschreitende Digitalisierung ausgelöste digitale Transformation bestimmt mittlerweile alle Bereiche des industriellen, öffentlichen und privaten Handelns. Hiervon betroffen sind industrielle Prozesse, ausgehend von der Produktentwicklung über die Produktion und die Unternehmensführung bis zum Betrieb und der Bereitstellung von Produkten und Dienstleistungen für den Kunden. Neben nachhaltigeren Prozessen erfordert die digitale Transformation den Aufbau einer Infrastruktur zur effizienten Nutzung der sich schnell entwickelnden digitalen Technologien. Den Vorteilen steht allerdings das Risiko potenzieller Cyberangriffe auf die digitale Infrastruktur der industriellen, öffentlichen und privaten Sektoren gegenüber. Damit wird Cybersecurity systemrelevant.

Der Begriff Cybersecurity ist umfassend zu sehen, weshalb er in einer Vielzahl von Kontexten Anwendung findet und durch mehrere Ausprägungen charakterisiert ist. Hierzu gehören Anwendungssicherheit (Application Security), Betriebssicherheit (Operational Security), Computersicherheit (Computer Security), Datensicherheit (Data Security), Informationssicherheit (Information Security) und Netzwerksicherheit (Network Security) [3].

Im Axa Deutschland Future Risks Report 2021 [4] gaben 66 % der befragten Cybersecurity-Verantwortlichen deutscher Unternehmen an, dass das Risiko, Cyberattacken ausgesetzt zu sein, in den kommenden fünf bis zehn Jahren deutlich ansteigen wird. Bezogen auf den Eisenbahnsektor heißt es dazu im ENISA-Report Railway Cybersecurity: „Bisher scheint der Eisenbahnsektor kein direktes Ziel für Cyberangriffe gewesen zu sein“ [1]. Allerdings ist auch hier eine tendenziell steigende Anfälligkeit zu verzeichnen. Po-Chi Haung [5] gibt in diesem Zusammenhang die zunehmende IT-Anwendung im Bahnsektor als markanten Grund an, was als wichtiger Hinweis auf die potenzielle Anfälligkeit des Eisenbahnsektors gewertet werden kann. Der ENISA-Report Railway Cybersecurity listet für die Umsetzung umfassender Cybersecurity-Konzepte für die Unternehmen im Eisenbahnsektor folgende Schwächen auf:

- Geringes Bewusstsein für Cybersecurity,
- Probleme, die Sicherheit und insbesondere Cybersecurity-Risiken richtig einzuschätzen,
- Probleme, die Cybersecurity mit der Wettbewerbsfähigkeit und der betrieblichen Effizienz in Einklang zu bringen,
- Abhängigkeit der Lieferketten von der Cybersecurity,
- Digitale Transformation im Eisenbahnsektor erfordert höhere Cybersecurity-Awareness,
- Komplexität der Vorschriften zur Cybersecurity.

Vor diesem Hintergrund sollte mit der Studie „Security und geplanter Technologieeinsatz“ der Ist-Zustand über die Cybersecurity-Awareness im Schienenverkehrssektor (Eisenbahn und Öffentlicher Personennahverkehr) in Deutschland erhoben werden. Im Fokus der Studie steht neben dem Einsatz eines Modells zur Evaluierung des Reifegrads von Cybersecurity-Maßnahmen auch der Einsatz neuer Technologien, um zukünftige Herausforderungen im Kontext Cybersecurity und damit möglicher Angriffsvektoren frühzeitig zu erkennen. Dafür wurde ein Gesamtkonzept mit drei Arbeitspaketen aufgestellt und umgesetzt, welches in Abbildung 1 dargestellt ist.

Wie aus Abbildung 1 ersichtlich, werden zunächst die Ziele der Studie adressiert: die Ermittlung des Status quo für den Reifegrad der Cybersecurity sowie der Stand bei der Einführung neuer Technologien. Darauf aufbauend werden die erforderlichen Ausführungsschritte der Studie umgesetzt. Hierbei handelt es sich um die Ausarbeitung der Fragen und die durchzuführenden Interviews für die Befragung der teilnehmenden Unternehmen des Eisenbahnsektors. Nach der Durchführung folgen die Auswertung und die Bewertung der Ergebnisse. Die Ergebnisse der Studie werden im Forschungsbericht zusammengefasst. Im Rahmen der Studie werden damit innerhalb von drei Arbeitspaketen belastbare Daten zur Ist-Situation für

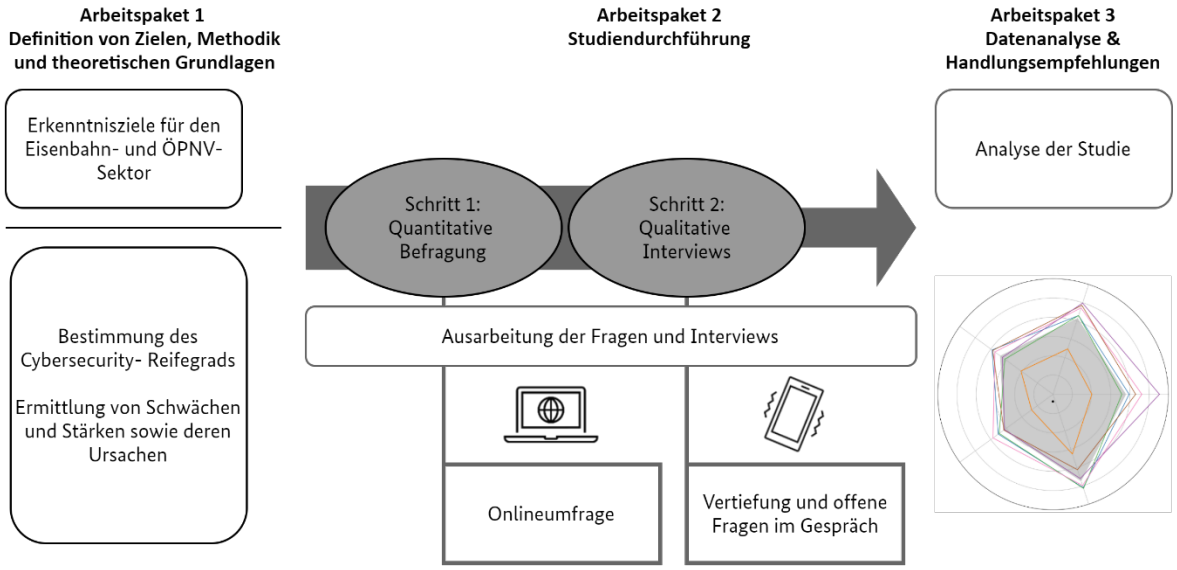


Abbildung 1: Konzeptueller Aufbau der Studie „Security und geplanter Technologieeinsatz“

die Themenfelder Cybersecurity und neue Technologien erhoben. Mit deren Auswertung können Hinweise zur Erreichung höherer Reifegrade oder der Verbreitung bestimmter Technologien abgeleitet werden.

Das Arbeitspaket 1 (AP1) umfasst die Definition der Ziele, der Methodik und der theoretischen Grundlagen. In diesem Zusammenhang wurden der Stand der Wissenschaft zu den Themen Cybersecurity und neue Technologien identifiziert und die relevanten Forschungsfragen abgeleitet. Bezüglich der neuen Technologien wurden zwölf Technologien gemeinsam mit dem Auftraggeber ausgewählt. Für die methodischen Grundlagen wurden einerseits die Bestimmung eines Reifegradmodells zur Cybersecurity sowie andererseits die Durchführung einer SWOT-Analyse zur Gegenüberstellung der internen Faktoren (Stärken und Schwächen) und der externen Faktoren (Chancen und Risiken) genutzt. Die dafür erforderlichen Daten wurden im Rahmen der Ausarbeitung eines Interviewleitfadens erhoben. Für eine umfassende Stichprobe waren die zu befragenden Unternehmen aus dem Sektor Bahn zu identifizieren und diese nach gemeinsam mit dem Auftraggeber definierten Kriterien in vordefinierte Untersektoren (Eisenbahnverkehrsunternehmen (EVU), Eisenbahninfrastrukturunternehmen (EIU), Verkehrsverbünde und ÖPNV-Unternehmen, Fahrzeughersteller und Fahrzeuginstandhalter, Infrastrukturhersteller, Energieversorger und Sonstige) zu kategorisieren. Zu diesem Arbeitspaket gehörte auch die Planung und Organisation der Befragung.

Das Arbeitspaket 2 (AP2) umfasste die Durchführung der Studie. Diese wurde in zwei Schritten vollzogen, der initialen Onlinebefragung und den darauf aufbauenden Interviews. Beide Formate dienten zur Identifizierung und Beschreibung der Ist-Situation der Themenbereiche Cybersecurity und neue Technologien im Eisenbahnsektor. Die methodische Evaluierung der erhaltenen Daten erfolgte mittels Reifegradmodell und der SWOT-Analyse. Mit dem Reifegradmodell ist basierend auf einer Reifegradskala eine systematische bewertende Analyse des Entwicklungs- oder Umsetzungsstandes der Cybersecurity sowie der neuen Technologien möglich. Die SWOT-Analyse erlaubt es, ein ganzheitliches Bild des Ist-Zustands des Sektors im Kontext Cybersecurity und neue Technologien darzustellen. Mithilfe der Onlinebefragung und anschließenden Telefon-Interviews können dabei schnell und einfach der Ist-Zustand in Bezug auf die Ausprägungsmerkmale der Cybersecurity und der neuen Technologien bestimmt und darauf aufbauend das gegebenenfalls erforderliche Verbesserungspotenzial ermittelt werden.

Das Arbeitspaket 3 (AP3) umfasst die Datenanalyse und darauf aufbauende, essenzielle Handlungsempfehlungen. Hierbei standen die deskriptive und die statistische Auswertung der Befragungsergebnisse aus AP1 und AP2 zum Ist-Zustand bei den Themen Cybersecurity und neue Technologien im methodischen Vordergrund. Damit konnte abgeleitet werden, inwieweit das Thema Cybersecurity im Eisenbahnsektor bislang durchdrungen worden ist und inwieweit das Thema neue Technologien in den Untersektoren im Eisenbahnbereich Einzug gehalten hat oder auf absehbare Zeit halten wird. Auf dieser Grundlage werden richtungsweisende Handlungsempfehlungen abgeleitet, deren Umsetzung eine Verbesserung der Cybersecurity und der Technologieanwendung im Sektor unterstützen kann. Damit trägt die Studie dazu bei, die Themen Cybersecurity und neue Technologien im Eisenbahnsektor in Richtung des anzustrebenden Soll-Zustands ergebnisbezogen zu entwickeln.

# 2 Internationaler Forschungsstand zu Security und geplantem Technologieeinsatz

## 2.1 Cybersecurity

Das rasante Wachstum der technologischen Entwicklungen, insbesondere der Digitalisierung und Vernetzung ist Teil der heutigen vierten industriellen Revolution, die in Deutschland unter dem Begriff Industrie 4.0 bekannt ist [6]. Im Rahmen der Digitalisierung werden etwa wichtige und teilweise sensible Daten eines Unternehmens erfasst, verarbeitet und gespeichert. Dies führt zu grundlegenden Veränderungen der Entwicklungs- und Geschäftsprozesse von Unternehmen, die sowohl zu neuen Produktentwicklungen, neuen Fertigungsprozessen, neuen Services und weiteren technischen Innovationen, als auch zu neuen Geschäftsmodellen einschließlich der damit verbundenen gesellschaftlichen Veränderungen führen können.

Die durch die Digitalisierung hervorgerufenen, mannigfachen Veränderungen haben zum Paradigma der digitalen Transformation geführt. Die digitale Transformation erhält große Aufmerksamkeit, weshalb sich die industriellen Branchen mit diesem Narrativ auseinandersetzen müssen, da sich das jeweilige Geschäftsumfeld grundlegend verändert hat. Das Narrativ der digitalen Transformation besteht darin, anstelle der Replikation bestehender Prozesse in digitaler Form, diese in intelligente Prozesse umzuwandeln, die vernetzt, zugänglich, steuerbar und digital gestaltet sind [6]. Die daraus resultierende Komplexität der Prozesse und Systeme macht sie allerdings auch anfällig für Bedrohungen von innen und außen, was im Aufkommen von Cybersecurity-Problemen durch Cyberangriffe Gestalt annahm. Dieser Umstand kennzeichnet eine negative Auswirkung der digitalen Transformation. Vor diesem Hintergrund wurde Cybersecurity international zu einem zentralen Thema, welches verstärkt in das Bewusstsein und die Verantwortlichkeit der Unternehmensleitungen rückte. Eine internationale Untersuchung aus dem Jahr 2019 von Gartner Research [7] zeigte, dass Chief Executive Officers (CEOs) zunehmend für die Ereignisse im Kontext der Cybersecurity in ihren Unternehmen verantwortlich gemacht werden. CEOs werden dabei in ihren Bemühungen, eine größere Verteidigungsfähigkeit gegenüber Cyberbedrohungen zu erreichen, von ihren Chief Information Officers (CIOs) unterstützt, die sich mit Cyberrisiken befassen. Im Rahmen der Analyse [7] wurden folgende Gründe identifiziert, die beachtet werden sollten, um zur Verbesserung der Cybersecurity beizutragen:

- Unternehmen haben kein hinreichendes Bewusstsein für immanent unbekannte, technische und administrative Cybersecurity-Risiken;
- Unternehmen haben die Trennung zwischen Technik, IT und Vertrieb zur Verbesserung der Cybersecurity nicht aufgehoben;
- Unternehmen investieren Geld in Insellösungen anstelle unternehmensweiter Cybersecurity-Lösungen;
- Cybersecurity-Beauftragte der Unternehmen sind häufig nicht für das ganze technische und administrative Umfeld des Unternehmens zuständig;
- In Unternehmen ist häufig kein integraler Ansatz für die Cybersecurity-Verantwortlichkeit vorhanden, um die technischen und vertrieblichen Belange zusammenzuführen;
- Häufig sind nur unklar formulierte oder gar keine Aussagen zur unternehmensweiten Cybersecurity-Strategie vorhanden;

- Häufig sind keine unternehmensweiten Cybersecurity-Maßnahmen oder Cybersecurity-Akzeptanz vorhanden;
- Eine unternehmensweite Cybersecurity-Governance, um Cybersecurity-Risiken erfolgreich angehen zu können, ist häufig nicht vorhanden.

Die Berücksichtigung der vorstehend genannten Gründe zur Erreichung eines effizienten Cybersecurity-Schutzes ist sowohl für die generelle Cybersecurity-Betrachtung als auch für die spezielle Ableitung der Cybersecurity-Strategie von zentraler Bedeutung. Dies berücksichtigt auch den Sachverhalt, dass weltweit nicht nur das Risiko von Cyberangriffen, sondern vielmehr auch die Cyberangriffe zunehmen, was für die angegriffenen Unternehmen neben hohen Kosten auch große Reputationsverluste nach sich zieht. Mehrheitlich erwartet die deutsche Wirtschaft eine Zunahme der Bedrohungslage durch Cyberangriffe, wie der Branchenverband Bitkom im Rahmen einer Studie durch Bitkom Research festgestellt hat [8]. Betreiber kritischer Infrastrukturen, wie z. B. Energieversorger, kommunale Verwaltungen, industrielle Organisationen, Transportsektor und andere, sind dabei besonders bedroht und benötigen für ihre Cybersecurity ein durchgängiges, integriertes Cybersecurity-Konzept, welches sowohl für die Informationstechnik (IT)- als auch für die Operational Technology (OT)-Infrastruktur implementiert werden muss. Hierbei handelt es sich um einen End-to-End-Lösungsansatz über alle Bereiche, der neben den Prozessen auch qualifizierte Cybersecurity-Fachkräfte umfasst. Neben wachsenden Cybersecurity-Anforderungen an die vorhandene IT- und OT-Infrastruktur, darf die Gewährleistung der Cybersecurity bei der Einführung und Erweiterung durch neue Technologien nicht außer Acht gelassen werden. Die größte Gefahr sehen die Unternehmen dabei durch Cyberangriffe in Form von Ransomware.

Vor diesem Hintergrund ist es für den Schienenverkehrssektor, als Teil der kritischen Infrastruktur, wichtig, sich mit diesem Thema auseinanderzusetzen. Der ENISA-Report Railway Cybersecurity führt hierfür konkrete Maßnahmen an, die auf die Anfälligkeit des Sektors Bezug nehmen [1]. Dabei spielt u. a. die massive Zunahme der Internetanbindung mit ihrer großen Bandbreite im deutschen Schienenverkehr sowie ÖPNV eine wichtige Rolle. Drahtlose Internetverbindungen sind ein attraktives Angebot für Fahrgäste, indem sie ein Ökosystem aus Borddiensten und Echtzeit-Datenfeeds zur Verfügung stellen. Allerdings ist die Privatheit dieser Dienste durch geeignete Cybersecurity-Maßnahmen zu gewährleisten. Neben dieser IT-Sicherheit hat die OT-Sicherheit im Rahmen des softwaregestützten Zugbetriebs eine zentrale Bedeutung im Rahmen einer durchgängigen Cybersecurity-Strategie. Weiterhin erfordert auch die Nutzung von Cloud-Services (z. B. Apple Cloud und Amazon Web Services) ein integratives und durchgängiges Cybersecurity-Konzept. Im Kontext der Cybersecurity-Strategie des Eisenbahnsektors erhält dabei der Return on Investment des eingesetzten Cybersecurity-Budgets eine wichtige Bedeutung. Dieser steht im Zusammenhang mit den umgesetzten Maßnahmen, die auf die Cybersecurity der IT- und OT-Systeme und die internen Netzwerke des Eisenbahnsektors, aber auch auf die Cybersecurity der Ticketsysteme, Online-Fahrgastdienste, Cloud-Services und weitere ausgerichtet sind, um eine cybersichere Infrastruktur zu gewährleisten.

## 2.2 Neue Technologien

Industrie 4.0 stellt ein ambitioniertes Leitbild für die Innovation und technologische Weiterentwicklung der Industrie durch neue Technologien dar [9]. Dieser Wandel findet sich weltweit in entsprechenden Konzepten, die durch spezifische Begriffe gekennzeichnet sind. In den U.S.A. sind die Begriffe Industrial Internet Consortium (IIC) sowie Smart Manufacturing Leadership Coalition (SMLC) gleichbedeutend mit der Plattform Industrie 4.0. In China ist Made in China 2025 ebenfalls gleichbedeutend mit Industrie 4.0. Auch Japan, Korea und andere große Produktionsländer haben gleichbedeutende Aktivitäten in diesem Kontext etabliert [6]. Industrie 4.0 baut dabei neben der Digitalisierung auf neuen Technologien auf. Neue Technologien – im englischen „emerging technologies“ – sind in diesem Zusammenhang Technologien, die allein oder in Kombination mit anderen Technologien signifikante Erweiterungen oder Sprünge in den

TABELLE 1: ZUSAMMENSTELLUNG WESENTLICHER AUFSTREBENDER TECHNOLOGIEN

| Technologie | Möglichkeiten/Fähigkeiten |
|---|---|
| Materialwissenschaft | Materialwissenschaft ist eine Querschnitttechnologie mit hoher wirtschaftlicher Bedeutung, welche neue Materialeigenschaften und -funktionen ermöglicht oder die Eigenschaften bekannter Materialien verbessert. Die Forschung in diesem Bereich ist für Innovationen in der Vielfalt der erforderlichen technologischen Lösungen arrondiert. Hierzu zählen: künstliche Intelligenz aus Glas, die Licht verwendet, um Ikonen zu erkennen und zu unterscheiden [10]; Biomaterialien, die stärker als Stahl und biologisch abbaubar sind; Material, welches Kohlenstoff aus der Atmosphäre absorbieren kann; Silizium X, welches eine Matrix aus Silizium-Nanopartikeln und anderen Nanopartikeln enthält; Materiale und Substanzen für effiziente Batterien. Ein weiteres neues Materialforschungsgebiet konzentriert sich auf zweidimensionales Material, Grafene, eine nur ein Atom dicke Schicht aus kristallinem Kohlenstoff. Die Forschung zu neuen Materialien betrachtet auch Bedürfnisse wie die haptische Interaktion in der Kommunikation, intelligente Lösungen für niederschwelliges Leiten von Entladungen und die Komposition von Material mit minimiertem Energie- und Ressourcenverbrauch bei der Verarbeitung. |
| Nanotechnologie | Nanotechnologie ermöglicht die Erstellung von Objekten im Nano- und Sub-Nano-Maßstab [11]. Die Nanotechnologie ist eine wesentliche Voraussetzung für neuartige Komponenten und Konzepte in der digitalen Elektronik, den Multicore-Halbleiterchips, der Optoelektronik, im Pervasive Computing, in der Informations- und Kommunikationstechnik, in den biologischen Wirkstoffen, den nanoskalierbaren Sensoren und Aktoren [12] sowie neuen Technologien für eine digitale Kreislaufwirtschaft und vielem mehr [13]. Abgesehen davon hat die Nanotechnologie potenzielle Fortschritte in der und Auswirkungen auf die Landwirtschaft, die Umwelt und die menschliche Gesundheit. |
| Smarte (intelligente) Fertigung (Intelligent Manufacturing) | Durch den integralen Einsatz von Big-Data-Technologien, künstlicher Intelligenz, maschinellen Lerntechnologien und anderen entwickelt sich die smarte (intelligente) Fertigung zu einer technologisch anspruchsvollen Entwicklung, welche sich im Zukunftsprojekt Industrie 4.0 manifestiert [14]. Auf diese Weise können kritische Ereignisse in der Produktion vorhergesagt oder vorbeugende Maßnahmen für erwartete Probleme im Produktionsprozess identifiziert und frühzeitig eine Lösung bereitgestellt werden, um gravierende Auswirkungen auf den Produktionsprozess zu vermeiden [6]. Weiterhin kann die Produktentwicklung in Zukunft durch intelligente Technologien interaktiv an die jeweilige Anwendung angepasst werden. Genetisch intelligente Technologien arbeiten mit funktionalen Werkzeugmaschinenkomponenten zusammen, um eine „sensible Maschine“ zu schaffen. Dieser Ansatz verwendet gemessene Maschinendaten und simultane Simulationsprozessdaten [15]. Die Forschung in diesem Bereich konzentriert sich unter anderem auf die intelligente Optimierung der Produktion, die Minimierung des Ressourcen- und Energieverbrauchs durch den Übergang zu einer Kreislaufwirtschaft [16] und auf anderes. |

Anwendungsmöglichkeiten und dem spezifischen Leistungsumfang erreichen [9]. In diesem Zusammenhang ist es charakteristisch, dass der industrielle Sektor, im Zuge der rasanten technologischen Entwicklung, radikalen Innovationen und Veränderungen unterzogen wird [3, 6, 9, 17]. Beispielsweise ist das Internet der Dinge (Internet of Things – IoT) eine Schlüsseltechnologie. Das IoT ermöglicht es, Netzwerke aus Sensoren und Aktoren zu Alltagsgegenständen werden zu lassen, die in digitale Elektronik, Software

und Netzwerkkonnektivität eingebettet sind. Auf diese Weise können Nutzer mit Objekten kommunizieren, sie steuern oder notwendige Informationen abrufen [3, 9]. Die im Rahmen der digitalen Transformation eingesetzten Technologien [3, 16] können in entstehende Technologien, häufig als Zukunftstechnologien bezeichnet, und verfügbare Technologien unterteilt werden. Entstehende oder zukünftige Technologien sind diejenigen Technologien, die über das Bekannte und Anerkannte hinausgehen, wohingegen verfügbare Technologien, häufig als neue Technologien bezeichnet, im Wesentlichen diejenigen Technologien repräsentieren, welche die Treiber der digitalen Transformation darstellen. Einige wesentliche der entstehenden Technologien (Zukunftstechnologien) sind in Tabelle 1 dargestellt.

Das Ziel bei entstehenden Technologien ist es, diese u. a. so zu entwickeln, dass die Herstellbarkeit von Produkten aus ökonomischer, ökologischer und gesellschaftlicher Sicht nachhaltiger wird. Dabei ist neben der Wettbewerbsfähigkeit auch die Energieeffizienz des industriellen Sektors zu berücksichtigen, um die Nachhaltigkeit der Produktionsprozesse zu gewährleisten und so die Wirtschaft per se ressourcen- und energieeffizienter zu gestalten.

Es stehen heute bereits vielfältige neue Technologien zur Verfügung, die ein großes Anwendungsspektrum bedienen. In diesem Zusammenhang sei zunächst auf diejenigen neuen Technologien hingewiesen, welche die technologischen Grundlagen der digitalen Transformation darstellen und sie entscheidend mitbestimmt haben oder noch mitbestimmen. Hierbei handelt es sich um die in Tabelle 2 angegebenen Technologien.

TABELLE 2: WESENTLICHE TECHNOLOGISCHE GRUNDLAGEN FÜR DIE DIGITALE TRANSFORMATION

| **Technologie** | **Eigenschaften** |
|---|---|
| Big Data | Big Data ist ein Begriff, der verwendet wird, um große Mengen an unstrukturierten und halb-strukturierten Datensätzen aus einer Vielzahl von Quellen zu beschreiben. Big Data ist durch ein hohes Datenvolumen, eine hohe Geschwindigkeit und eine große Datenvielfalt gekennzeichnet, um die Eigenschaften von Informationen zu beschreiben. Dies wird durch spezifische Anforderungen an technologische und analytische Methoden erreicht. |
| Blockchain | Eine Blockchain ist eine verteilte, öffentliche Datenbank, die zur Verwaltung von Transaktionen verwendet wird. Der Begriff Kette in Blockchain bezieht sich auf die chronologische Reihenfolge, in der Transaktionen hinzugefügt oder ausgeführt werden. |
| Cloud Computing | Cloud Computing ist eine große und hochgradig skalierbare Bereitstellung von Rechen- und Speicherressourcen, auf die von überall zugegriffen werden kann. Cloud Computing und zentralisierte Datenverarbeitung sind zwei der heute vorherrschenden Architekturparadigmen. |
| Cloud Dienste | Cloud-as-a-Service-Modelle sind über das Internet verfügbar, wobei das Geschäftsmodell festlegt, wie eine Anwendung Wert für ihre Benutzerinnen und Benutzer generieren. Unternehmen können ihre langfristigen IT-Investitionen reduzieren, indem sie Cloud-Services-IT-Ressource einsetzen, die flexibel servicebasiert bereitgestellt werden. |
| Internet der Dinge | Das Internet der Dinge (IoT) ist ein Informationsnetzwerk aus mit dem Internet verbundenen physischen Geräten (Dinge, Objekte, Entitäten), um Daten zu sammeln und auszutauschen. Dies ermöglicht die Interaktion und Kooperation von Dingen, Objekten und Entitäten, um gemeinsame Ziele in der realen und virtuellen Welt zu erreichen. |

Die in Tabelle 2 genannten Technologien können in einem breiten Anwendungsbereich in verschiedenen industriellen Sektoren eingesetzt werden. So ist z. B. das IoT heute in vielfältigen Anwendungen bei der Wertschöpfung vertreten, die von der industriellen Fertigung über das Gesundheitswesen bis zum sogenannten „Smart Home“, dem vernetzten Eigenheim reicht. In einer Studie zum IoT wurden dazu etwa 300 Anwendungsszenarien in verschiedenen Umgebungen untersucht [18]. Trotz aller Vorteile, welche die Anwendung der Technologien für die industriellen Sektoren mit sich bringen, müssen sich die Unternehmen auch erheblichen Herausforderungen stellen. Zu diesen gehören u. a. die Vernetzung verschiedener Fachabteilungen und der Aufbau eines vertieften Wissens und solider Kompetenzen der Mitarbeiterinnen und Mitarbeiter, um bei der Entwicklung und der Anwendung der Technologien erfolgreich zu sein. Hinzu kommt als eine Querschnittsaufgabe die Gewährleistung der Cybersecurity bei der Einführung und/oder Erweiterung des Einsatzes der Technologien im Zusammenhang mit weitreichenden Vernetzungen, was nicht außer Acht gelassen werden darf.

# 3 Forschungsansatz

## 3.1 Forschungsfragen

Der Eisenbahnsektor ist ein breit ausdifferenzierter, komplexer, industrieller Bereich, der sich verstärkt mit den Themen Cybersecurity und neue Technologien auseinandersetzen muss. Daher steht zunächst die Frage, welche der vielfältigen Forschungsthemen a priori zu priorisieren sind. Bezogen auf das Thema der Studie ergeben sich zwei wichtige Forschungsfragen, welche einerseits auf den jeweiligen Ist-Zustand Bezug nehmen und andererseits darauf aufbauend eine Projektion in die Zukunft aufzeigen:

- Welche Teile des Eisenbahnsektors sind bereits, bezugnehmend auf Cybersecurity, gut aufgestellt und wo gibt es Defizite?
- Welche neuen Technologien kommen realistisch in den kommenden Jahren zum Einsatz?

Da Cybersecurity ein zentrales Thema für den Eisenbahnsektor darstellt, ist die vorstehende erste Forschungsfrage weiter auszudifferenzieren. Es ergeben sich die folgenden weiteren Forschungsfragen:

- Warum sind Unternehmen beim Thema Cybersecurity besonders weit fortgeschritten oder zeigen noch Nachholbedarf?
- Welche Wünsche haben die Unternehmen im Bereich Cybersecurity?
- Welchen Förder- und Forschungsbedarf gibt es?
- Lohnt es sich, bahnspezifische Cybersecurity-Forschung zu bestimmten Technologien zu betreiben?

Unter Berücksichtigung einer breiten Ausdifferenzierung und Komplexität des Eisenbahnsektors ist auf ein Problem hinzuweisen, welches Einfluss auf das vorstehend skizzierte Projektziel, die Erarbeitung einer Bewertungsgrundlage, nehmen kann. Dies ist die möglicherweise unzureichende Datengrundlage. Trotz dieser möglichen Einschränkung trägt die Studie zum Aufbau einer Bewertungsgrundlage und daraus resultierender Handlungsempfehlungen bei.

## 3.2 Forschungsgegenstand

Neue Technologien entstehen und existierende Technologien entwickeln sich kontinuierlich und schnell weiter, worauf bereits in Abschnitt 2.2 Bezug genommen wurde. Ein Beispiel hierfür ist das Internet. Ursprünglich für den militärischen Bereich entwickelt, ist es heute praktisch für jeden zugänglich geworden, der über einen Internetanschluss verfügt. Hinter dem Begriff Internet steht heute ein großes Repertoire an unterschiedlichen Technologien. Das Thema Cybersecurity hat durch die uneingeschränkte Vernetzung dieser Technologien an Bedeutung gewonnen. Infolgedessen ist es notwendig, einerseits Cybersecurity prinzipiell zu gewährleisten und andererseits durch Cyberangriffe bedingte Cybersecurity-Risiken zu reduzieren oder ganz auszuschließen. Weiterhin ist zu beachten, dass Cybersecurity-Risiken vielfältige Ausprägungsmerkmale aufweisen und sich verändern. Kritische Infrastrukturen wie der Eisenbahnsektor sind einer ständigen Bedrohung durch Cyberattacken ausgesetzt. In diesem Zusammenhang bezieht sich der Forschungsgegenstand Cybersecurity auf die erfolgreiche Abwehr jedweder Form von Cyberangriffen. Potenzielle Cybersecurity-Bedrohungen können sich entweder auf namentlich bekannte Angriffsformen beiziehen, für die es infolge ihrer Variabilität keine Standardverfahren zu deren Abwehr gibt, oder auf namentlich unbekannte Cyberangriffsformen, für die noch keine Abwehrmechanismen bekannt sind. Bezugnehmend auf die Forschungsergebnisse in [3], die in Tabelle 3 zusammenfassend dargestellt sind, ist der Forschungsgegenstand im Wesentlichen thematisch charakterisiert.

TABELLE 3: RISIKOSTUFEN VON CYBERBEDROHUNGEN UND ZUGEHÖRIGE SECURITYMODELL

| **Risikostufe für Cyberbedrohungen** | **Securitymodell** |
|---|---|
| Bekannte – Bekannte | Informationssicherheit |
| Bekannte – Unbekannte | Cybersecurity |
| Unbekannte – Unbekannte | Cyberresilienz |

Wie aus Tabelle 3 ersichtlich, ist es für die Entwicklung geeigneter Cybersecurity-Modelle wichtig, die Risikostufe für Cyberbedrohungen zu analysieren und darauf aufbauend ein entsprechendes Cybersecurity-Modell zu entwickeln. Dies ist ein komplexer Prozess, der ausführlich in [3] dargestellt ist.

Vor dem Hintergrund der in [3] dargestellten Forschungsmethodik soll die Ist-Situation sowohl der Cybersecurity-Awareness als auch deren potenzielle Umsetzung im Hinblick auf mögliche Cybersecurity-Strategien im deutschen Eisenbahnsektor und ÖPNV erfasst und deren Auswirkungen bewertet werden. Hierfür sind entsprechende Zielgruppen sowohl im Hinblick auf eine Clusterbildung als auch im Hinblick auf Ressourcen, Infrastruktur, Interaktionen und weiteres zu unterteilen (siehe hierzu Kapitel 4). Weiterhin ist die Cybersecurity im Rahmen der Nutzung sozialer Netzwerke zu verbessern. Hybride Angriffe, die sowohl real als auch virtuell auftreten, müssen eindeutig zu erkannt werden können, um sie wirkungsvoll zu bekämpfen. Dies kann beispielsweise durch die regelmäßige Schulung des Personals erreicht werden.

Neben dem Thema Cybersecurity ist auch das Thema „geplanter Technologieeinsatz“ zu untersuchen. Hierbei ist das Hinterfragen des potenziellen Cybersecurity-Risikos wichtig, welches im Zusammenhang mit dem geplanten Technologieeinsatz einen Hinweis auf mögliche Schwachstellen im Rahmen der Cybersecurity-Awareness gibt. Auf dieser Grundlage soll die Ist-Situation neuer Technologien im deutschen Eisenbahnsektor und im ÖPNV untersucht und bewertet werden.

Für den beschriebenen Forschungsgegenstand ist darüber hinaus eine themenbezogene Literaturrecherche erforderlich.

## 3.3 Cybersecurity-Risikolandschaft

Cybersecurity dient der gezielten Abwehr böswilliger Cyberangriffe. Cyberangriffe werden durch die Nutzung der extremen Vernetzungsfähigkeiten digitaler Technologien ermöglicht.

Durch die sich ständig und schnell weiterentwickelnden Cyberbedrohungen durch Cyberangriffe ist von einer ernst zu nehmenden Gefährdung digitaler Systeme und Infrastrukturkomponenten im Eisenbahnsektor auszugehen, was zielgerichtete Cybersecurity-Maßnahmen erforderlich macht. Der traditionelle Ansatz in der Informationssicherheit, wonach man sich auf die kritischen und damit wichtigen Prozesse der Infrastrukturressourcen konzentriert, um diese vor den größten bekannten Sicherheitslücken zu schützen, ist nicht mehr zielführend. Weniger wichtige Systeme oder Komponenten bleiben bei diesem Ansatz vielfach ungeschützt und sind damit mehr oder weniger leicht für Cyberangriffe erreichbar. Ein derartiger statischer Ansatz der Informationssicherheit ist für die sich rasch entwickelnden, neuen digitalen Technologien unzureichend.

Vor diesem Hintergrund sind die traditionellen Ansätze zur Sicherung industrieller, staatlicher und privater Computersysteme oder Netzwerke, Maschinen oder Geräte in Bezug auf den Schwerpunkt Cybersecurity anzupassen, um Cybersecurity-Risiken zu reduzieren. Allerdings sind Cyberangriffe mittlerweile

hochkomplexer Natur. Vielfach werden erfolgreiche Cyberangriffe als Attack-as-a-Service, Malware-as-a-Service oder Fraud-as-a-Service im Darknet angeboten. Hierbei handelt es sich um die Bereitstellung illegaler Aktivitäten durch Cyberkriminelle. Das dahinterstehende Geschäftsmodell stellt ein Angebot im Untergrund (Darknet) zur Verfügung, welches auf eine ständig wachsende Nachfrage reagiert. Der größte Teil dieser Dienste wird in der Untergrundwirtschaft auf der Grundlage eines Abonnements oder einer Pauschalgebühr angeboten, was sie bequem und attraktiv macht, da die Hauptkosten für die Vermittlung mit der Kundschaft geteilt werden. Gleichzeitig liegt der Kundennutzen in einer Reduzierung des Aufwands, selbst entwickeln zu müssen. Folglich nimmt die Bedeutung von Cybersecurity zu.

Cybersecurity-Verantwortliche versuchen daher mittels Schwachstellenanalyse das Cybersecurity-Risiko abzuschätzen. Dabei wird das identifizierte Risiko für Cyberbedrohungen im Rahmen eines Angriffsszenarios modelliert und ein passendes Cybersecurity-Modell zur Abwehr des Cyberangriffs entwickelt [3, 9]. Das Cybersecurity-Risiko eines Computersystems, eines Netzwerks oder einer Infrastrukturressource entspricht damit der Wahrscheinlichkeit einer Cybersecurity-Verletzung durch einen Cyberangriff. In diesem Zusammenhang sind vielfältige Formen von Cyberangriffen für den Eisenbahnsektor von Bedeutung, beispielsweise:

- Botnet-Angriffe: Es wird dabei eine Software verwendet, die speziell entwickelt wurde, um eine große Anzahl von Geräten zu infizieren, die über das Internet verbunden sind.
- Denial-of-Service-Angriffe (DoS-Angriffe): Es handelt sich dabei um Versuche, um z. B. eine Website unzugänglich zu machen, indem der Server mit großen Mengen an gefälschtem Datenverkehr überlastet wird.
- Distributed-Denial-of-Service-Angriffe (DDoS-Angriffe): Eine Überlastung von Servern, Systemen und Netzwerken mit Netzwerkverkehr wird dabei initiiert, um die Ressourcen oder die Bandbreite zu erschöpfen und sie zum Absturz zu bringen. Danach kann die angegriffene Ressource keine legitimen Anfragen mehr bedienen. DDoS-Angriffe werden in vielen Fällen durch zuvor übernommene Botnets durchgeführt.
- Phishing-Angriffe: Dies sind eine Art von Social-Engineering-Cyberangriffen. Der Angriff wird dazu verwendet, Benutzerdaten und kritische Daten und Informationen zu stehlen. Die Angriffsform wird auch verwendet, um im Rahmen eines größeren Angriffs, wie eines Advanced-Persistent-Threat-Vorfalls (APT-Vorfall), in öffentliche oder private Netzwerke einzudringen. In diesem Szenario werden Mitarbeitende kompromittiert, um Zugangskontrollen (Sicherheitsperimeter) zu umgehen, Malware innerhalb einer geschlossenen Umgebung öffentlicher oder privater Organisationen zu verbreiten oder privilegierten Zugriff auf gesicherte Daten zu erhalten.
- Ransomware-Angriffe: Sie verschlüsseln die Daten und Informationen eines Angegriffenen und verlangen die Zahlung eines Lösegelds als Gegenleistung für den Entschlüsselungscode. Selbst wenn Lösegeld gezahlt wird, ist nicht notwendigerweise garantiert, dass die verschlüsselten Daten uneingeschränkt wiederhergestellt werden können. Häufig wird die Verschlüsselung nur vorgegeben, obwohl die Daten in Wirklichkeit gelöscht wurden [19, 20].
- Spam-Angriffe: Hierbei handelt es sich um eine elektronische Version einer Junk-Mail, die unerwünschte Nachrichten (oft unerwünschte Werbung) an eine große Anzahl von Adressaten sendet. Diese Angriffsform ist ein ernsthaftes Sicherheitsproblem, da sie Trojaner, Viren, Würmer, Spyware und gezielte Phishing-Angriffe verbreiten kann.

Wenngleich der Eisenbahnsektor laut ENISA-Report [1] bis heute kein direktes Ziel für Cyberbedrohungen zu sein scheint, haben bereits mehrfach Vorfälle stattgefunden, die auf die Anfälligkeit des Eisenbahnsektors hindeuten. Daher sind neben bisher erfolgten Cyberangriffen auch Angriffsszenarien auf zukünftige Systeme der Leit- und Sicherungstechnik zu erfassen, um diese Systeme gegenüber Cyberangriffen resilienter zu machen [21]. Die durch die digitale Transformation bewirkte rasche Digitalisierung und Vernetzung lässt neben dem IT-Bereich auch im OT-Bereich neue Angriffsvektoren für Cyberangriffe ent-

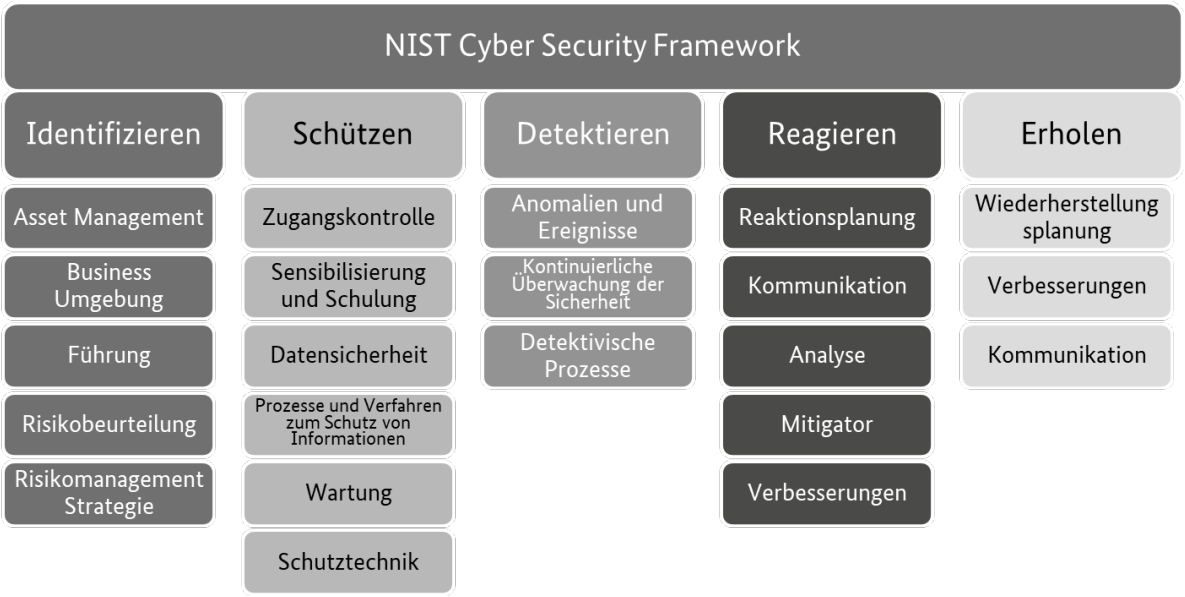


Abbildung 2: Kategorien der fünf NIST-CSF-Kernfunktionen [2]

stehen. Dies erfordert entsprechende Maßnahmen zur Gewährleistung der Cybersecurity, da die ursprünglich in sich geschlossenen OT-Systeme durch die zunehmende Vernetzung Schwachstellen aufweisen, die durch Cyberkriminelle gezielt ausgenutzt werden können.

Zur Durchführung von Cybersecurity-Maßnahmen ist der effiziente und effektive Einsatz von vorhandenen Personalressourcen und zur Verfügung stehender Budgets ein zentrales Thema. Dafür sollten Personal und Budget in Relation zur Unternehmensgröße eingesetzt werden, d. h. zu Kenngrößen wie Umsatz oder Anzahl der Beschäftigten. Diese Themen sind, neben anderen, im Rahmen einer Datenerhebung durch entsprechende Fragen zu erheben und zu bewerten.

Für die Bewertung ist ein standardisiertes Verfahren, z. B. im Rahmen einer Befragung, erforderlich, welches den Reifegrad des betrachteten Unternehmens im Hinblick auf die Umsetzung von organisatorischen, von prozessualen und von technischen Maßnahmen zur Cybersecurity und damit der Resilienz des Unternehmens gegenüber Cyberangriffen abbildet (siehe Abschnitt 5.1). Die entsprechenden Fragen zielen daher u. a. auf eingesetzte oder einzusetzende Schutzkonzepte und Technologien ab.

Hierbei gibt es mehrere Möglichkeiten zur Strukturierung der Fragen. Eine den IT- und OT-Bereich übergreifende, geeignete Struktur ist durch das National Institute of Standards and Technologies (NIST) Cybersecurity-Framework (CSF) gegeben [2]. NIST-CSF ermöglicht es, eine Bestandsaufnahme der aktuellen Aktivitäten zur Cybersecurity aus unternehmensweiter Sicht vorzunehmen, um feststellen zu können, ob die aktuelle Integration von Cybersecurity-Maßnahmen des Risikomanagements gegenüber potenziellen Cyberangriffen ausreichend ist. Dazu weist NIST-CSF die fünf Kernfunktionen Identifizieren (Identify), Schützen (Protect), Erkennen (Detect), Reagieren (Respond) und Wiederherstellen (Recover) aus, wie in Abbildung 2 dargestellt. Im Folgenden werden die englischsprachigen Begriffe weiterverwendet.

Wie aus Abbildung 2 ersichtlich, werden für jede Kernfunktion des NIST-Cybersecurity-Frameworks, Unterkategorien für Cybersecurity-Ergebnisse und Cybersecurity-Kontrollen definiert. Bei der Kernfunktion „Protect“ geht es beispielsweise um die Entwicklung und Implementierung geeigneter Sicherheitsvorkehrungen. Hier sind die zugehörigen Unterkategorien Zutrittskontrolle (Access Control), Bewusstsein und Training (Awareness and Training), Datensicherheit (Data Security), Informationsschutz von Prozessen und Verfahren (Information Protection of Processes & Procedures), Wartung (Maintenance) und

Schutztechnik (Protective Technology). Betrachtet man in diesem Zusammenhang etwa die Unterkategorie Zutrittskontrolle, wird der Zugriff auf Assets und zugehörige Einrichtungen nur für autorisierte Benutzer, Prozesse oder Geräte sowie für autorisierte Aktivitäten und Transaktionen zugelassen. In der Unterkategorie Awareness und Training geht es dagegen um das Training von Mitarbeitenden zur Sensibilisierung für Cybersecurity, damit sie ihre Aufgaben im Rahmen der Cybersecurity unter Berücksichtigung der entsprechenden Richtlinien, Verfahren und Vereinbarungen optimal erfüllen können.

Unter Berücksichtigung der effektiv und effizient durchgeführten Maßnahmen der Unterkategorien zu den Kernfunktionen des NIST-Cybersecurity-Frameworks können die aus potenziell erfolgreichen Cyberangriffen resultierenden Schäden, unter anderem der Verlust kritischer Daten oder der Ruf des Unternehmens nicht nur minimiert, sondern auf ein verschwindend geringes Niveau reduziert werden. Dies kann allerdings nur durch die zur jeweiligen NIST-Kernfunktion zugehörigen Maßnahmen der Unterkategorien erreicht werden. Diese sind zu klassifizieren und kontinuierlich hinsichtlich eines potenziellen Anomalieverhaltens zu bewerten. Letztlich trägt das umfassende und kontinuierliche Monitoring dazu bei, Cybersecurity-Risiken so weit zu reduzieren, dass nur noch ein verschwindend kleines Restrisiko fortbesteht, welches handhabbar ist.

## 3.4 Technologielandschaft

Der Begriff Technologie repräsentiert als Oberbegriff einen systemischen Ansatz, bezogen auf eine Wissensbasis, ein zu lösendes Problem und der sich daraus ergebenden Problemlösungskompetenz. Durch kontinuierliche Forschung und Entwicklung kommt es zu einer Veränderung der aktuell zur Verfügung stehenden Technologien, woraus auch vollkommen neue Technologien entstehen können. Die Veränderungen werden in der Regel vor dem Hintergrund genauer Zielvorgaben verfolgt, um z. B. schneller und qualitativ besser produzieren zu können, Geschäftsprozesse zu vereinfachen oder diese mit größerem Kundennutzen auszustatten. Damit ist der Begriff Technologie mit einem immanenten Ziel verknüpft, das mit der Suche nach einer Veränderung gleichgesetzt werden kann. Diese Veränderung resultiert in der Regel aus deutlichen Unterscheidungsmerkmalen gegenüber der bislang zum Einsatz kommenden, erprobten und anerkannten Technologie.

Zur Abgrenzung gegenüber erprobten und anerkannten Technologien werden die mit neuen Unterscheidungsmerkmalen ausgestatteten Technologien häufig als „neue Technologien“ bezeichnet. Deren Einführung führt zu Veränderungen des betrieblichen Alltags. Dieser Veränderungsprozess wird national, wie international als digitale Transformation bezeichnet [3, 9]. Die digitale Transformation der industriellen Sektoren erfordert ein dezidiertes Wissen der Fach- und Führungskräfte über die neuen Technologien.

Um national und international wettbewerbsfähig zu sein und treibende Kraft des innovativen Fortschritts zu bleiben, müssen die industriellen Sektoren frühzeitig das Veränderungspotenzial der neuen Technologien vorausnehmen. Die digitale Transformation ermöglicht dabei im Gefolge der neuen Technologien viele neue und innovative Funktionen in Produkten, wie eine erhöhte Verfügbarkeit, einen erhöhten Produktnutzen und ein reibungsloses Zusammenspiel innerhalb des betrachteten Gesamtsystems. Diese generischen Eigenschaften sind für den Eisenbahnsektor von zentraler Bedeutung und bilden durch grundlegende Modernisierung und Digitalisierung der Infrastruktur das Fundament für das Zukunftsprojekt eines digitalen Bahnsystems [22]. Die hierfür infrage kommenden neuen Technologien waren in Betracht zu ziehen und wurden im Rahmen eines Brainstorming-Ansatzes identifiziert.

In der nachfolgenden Auflistung wurden der Vollständigkeit halber auch die bereits in Kapitel 2.2 betrachteten Technologien aufgenommen.

- Additive Fertigung: Das ist ein Fertigungsverfahren, bei dem 3D-Objekte auf Basis einer schichtweisen Herstellung erzeugt werden. Die Flexibilität im Entwurf und der Herstellung ermöglicht, mit dieser Technologie schnell neue Produkte auf den Markt zu bringen. On-Demand-Ersatzteildruck ist etwa eine Option.
- Big Data und Analytics: Dies bezeichnet die Verarbeitung großer und komplexer Datensätze, die mit herkömmlichen Verfahren und Werkzeugen aufwendig zu analysieren sind. Die Verfahren, mit denen die Daten gespeichert und analysiert werden, erfordern in der Regel den Einsatz von Analysemethoden der künstlichen Intelligenz und des maschinellen Lernens.
- Blockchain: Eine Blockchain ist ein Informationsverzeichnis, das kryptografisch mittels einer Prüfsumme die in einem dezentralen Netzwerk Teilnehmenden authentifiziert und verwaltet. Die Basis hierbei ist ein kryptografischer Beweis, sodass zwei Parteien ohne Dritte miteinander sicher interagieren können.
- Cloud Computing: Das Cloud Computing stellt sowohl Ressourcen in Form von Infrastruktur und Anwendungen als auch von Dienstleistungen über das Internet zur Verfügung. In diesem Zusammenhang ermöglicht das Cloud Computing auch komplexe und innovative IT-Infrastrukturen relativ kurzfristig in Unternehmen einzubinden.
- Cloud Dienste: Diese repräsentieren Infrastrukturen, Plattformen, Software oder Technologien, die von einem Drittanbieter gehostet und potenziellen Nutzenden über das Internet zur Verfügung gestellt werden. Die Leistungen werden als Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS) und Function-as-a-Service (FaaS) zur Verfügung gestellt.
- Glasfaser: Das ist eine Technologie, mit der Daten und Informationen als Lichtimpulse durch Fasern aus Glas und Kunststoff erfasst und über große Distanzen verlustfrei übertragen werden können.
- Internet der Dinge/Internet of Things (IoT): Das Internet der Dinge besteht aus physischen Einheiten (Dingen), die ursprünglich nicht für die Kommunikation untereinander und mit der Umwelt gedacht waren. Im IoT sind diese Dinge in der Lage, sich selbst zu identifizieren, zu kommunizieren und über ein auf Internettechnologien basierendem Netz zu interagieren. Sie können in Abhängigkeit von externen Auslösern oder lokaler Logik handeln.
- Künstliche Intelligenz (KI): Methode, welche die Fähigkeit von Maschinen beschreibt, ähnlich wie der Mensch zu „denken“. Ein Ziel der angewandten KI ist, dass intelligente Systeme entwickelt werden können, die z. B. Anlagenfehler identifizieren.
- Machine Learning (ML): ML ist ein Computersystem, welches anhand unterschiedlicher Lernverfahren Daten analysiert. Maschinelle Lernverfahren sind: unüberwachtes Lernen (unsupervised learning), überwachtes Lernen (supervised learning) und Verstärkungslernen (reinforcement learning). Diese Technologie wurde in der Studie gemeinsam mit künstlicher Intelligenz abgefragt.
- Networks Function Virtualization (NFV): Dies ist ein Verfahren, mit dem Netzwerkprozesse in virtualisierte Software-Plattformen umgewandelt werden können, die besser skalierbar sind. Diese Technologie wurde in der Studie gemeinsam mit Virtualisierung abgefragt.
- Software-defined Network (SDN): Dies ist eine Netzwerkarchitektur, bei der die Software-Abstraktions-Schicht über die physische Netzwerkinfrastruktur gelegt wird. SDN ermöglicht durch agilere und günstigere Netzwerke die Trennung der Steuerungsebene (control plane) und des eigentlichen Datenverkehrs (data plane). Diese Technologie wurde in der Studie gemeinsam mit Virtualisierung abgefragt.
- Virtualisierung: Die Virtualisierung ermöglicht durch logische Trennung mehrere virtuelle Computer auf einem realen Computer zu realisieren. Dies erlaubt den sicheren Betrieb Dienste unterschiedlicher Nutzer auf einer Hardware, wodurch Kosten gesenkt und eine neue Flexibilität generiert werden kann.

- Drahtlose Sensornetze/Wireless Sensor Network (WSN): WSN ist ein drahtloses Netzwerk, welches eine große Anzahl von Sensorknoten in einer Kommunikations-Infrastruktur verbindet, um Zustände an verschiedenen Standorten zu überwachen. Die Verbindung wird mittels ad-hoc-Routing hergestellt. Die Daten werden mittels eines eingebauten Mikroprozessors verarbeitet.
- 5G: Dies repräsentiert die fünfte Generation mobiler, drahtloser Breitbandtechnologien. Durch die 100-fache Datenübertragung, im Vergleich zu Long Term Evolution (LTE)-Technologie der vierten Generation, kann mit 5G in Echtzeit kommuniziert werden. Die Eigenschaften dieser Technologie sind ein hoher Durchsatz, eine geringe Latenz, die große Zuverlässigkeit und eine erhöhte Skalierbarkeit.

Im Rahmen der Online- und Interview-Befragung wurden einige der vorstehend genannten Technologien aus inhaltlicher Sicht zusammengefasst, wie künstliche Intelligenz und maschinelles Lernen.

Der Einsatz neuer Technologien geht häufig mit zahlreichen Schnittstellen sowie teils auch drahtlosen Kommunikationswegen einher und stellt damit oft neue Herausforderungen an die Cybersecurity. Daher ist es wichtig, das Thema Cybersecurity gleich von Beginn an mitzubetrachten, um Cybersecurity-Maßnahmen zügig umsetzen zu können.

Mit der Fokussierung auf neue Technologien ist auch dem vielfältigen und nebenläufigen Zusammenspiel „alter“ und „neuer“ Technologien Rechnung zu tragen, um in einer integrativen Systemarchitektur ein tragfähiges Fundament für den Eisenbahnsektor der Zukunft zu skizzieren. Dafür ist ein Erfahrungsaustausch zwischen den Mitarbeitenden bezüglich „alte Technologien“ und „neue Technologien“ unabdingbar. Es bietet sich zunächst eine Datenerhebung an, inwieweit die jeweilige neue Technologie bereits eingeführt ist oder vor welchem Hintergrund sie eingeführt werden soll. Im Rahmen eines zweiten Ansatzes ist es interessant, die Art der Bereitstellung bzw. des Betriebs der neuen Technologien im Sinne einer Stärken-Schwächen- und Chance-Risiken-Analyse zu betrachten.

# 4 Zielgruppen in den Sektoren Eisenbahn und ÖPNV

## 4.1 Festlegung der Zielgruppen zwecks Clusterbildung

Um eine detaillierte Betrachtung des Eisenbahnsektors und des Öffentlichen Personennahverkehrs (ÖPNV) in Deutschland zu ermöglichen, wurde eine Segmentierung und Kategorisierung der vom Auftraggeber vorgeschlagenen Sektoren vorgenommen. Diese Untersektoren werden nachfolgend vorgestellt und darin enthaltene Spezifika erläutert. Die Nennung von Unternehmensnamen bedeutet nicht automatisch, dass die entsprechenden Unternehmen an der Umfrage teilgenommen haben – Teilnehmende werden aus Gründen der Anonymisierung nicht genannt. Folgende Untersektoren wurden in dieser Studie betrachtet:

1. Eisenbahnverkehrsunternehmen (EVU),
2. Eisenbahninfrastrukturunternehmen (EIU),
3. Energieversorger,
4. Fahrzeughersteller,
5. Fahrzeuginstandhalter,
6. Infrastrukturhersteller,
7. Verkehrsverbünde und ÖPNV-Unternehmen,
8. Vertriebsplattformen.

## 4.2 Darstellung der Untersektoren

### 4.2.1 Untersektor 1: Eisenbahnverkehrsunternehmen

Die Bahnbetreiber im „System Eisenbahn“ sind die Eisenbahnverkehrsunternehmen, die für die Erbringung von Dienstleistungen für den Transport von Gütern und Fahrgästen auf der Schiene zuständig sind. In diesen Untersektor wurden aus der Liste des Eisenbahn-Bundesamts [23] alle 418 Unternehmen aufgenommen, beispielsweise zählen hierzu:

- DB Fernverkehr AG für den Personenfernverkehr,
- DB Regio AG und Usedomer Bäderbahn GmbH für den Personennahverkehr sowie
- DB Cargo Deutschland AG für den Güterverkehr.

Von den nichtbundeseigenen Eisenbahnen (NE-Bahnen) wurden Personenverkehrsunternehmen/Beteiligungsgesellschaften aufgenommen. Hierzu zählen beispielhaft:

- BeNEX GmbH (z. B. Cantus Verkehrsgesellschaft mbH, Metronom Eisenbahngesellschaft mbH, ODEG Ostdeutsche Eisenbahn GmbH)
- Transdev GmbH (z. B. Bayerische Oberlandbahn GmbH (BOB), NordWestBahn GmbH (NWB), Württembergische Eisenbahn-Gesellschaft mbH (WEG))

- Société nationale des chemins de fer français (SNCF) (z. B. SNCF Voyages Deutschland GmbH, NEB Betriebsgesellschaft mbH, Keolis Deutschland GmbH & Co. KG).

Aufgenommen wurden weiterhin nichtbundeseigene Güterverkehrsunternehmen (evtl. betreiben bereits bei den Personenverkehrsunternehmen aufgeführte Unternehmen ebenfalls Güterverkehr), so z. B.:

- SBB Cargo Deutschland GmbH
- METRANS Rail (Deutschland) GmbH
- Havelländische Eisenbahn AG (HVLE).

### 4.2.2 Untersektor 2: Eisenbahninfrastrukturunternehmen

Die Eisenbahninfrastrukturunternehmen sind für den Aufbau, die Verwaltung und die Instandhaltung der Eisenbahninfrastruktur, der ortsfesten Installation einschließlich Verkehrsmanagements, der Zugsicherung und Signalisierung, aber auch für den Betrieb von Bahnhöfen und Fahrstromversorgung (Anmerkung: Bahnenergieversorger werden innerhalb dieser Studie als eigener Untersektor aufgeführt) verantwortlich [24]. In diesen Untersektor wurden 115 Unternehmen als bundeseigene Unternehmen aufgenommen, z. B.:

- DB Netz AG,
- DB RegioNetz Infrastruktur GmbH,
- DB Station & Service AG

sowie als nichtbundeseigene Unternehmen, z. B.

- Deutsche Regionaleisenbahn GmbH (DRE),
- Albtal-Verkehrs-Gesellschaft mbH (AVG),
- Eisenbahnen und Verkehrsbetriebe Elbe-Weser GmbH (EVB).

### 4.2.3 Untersektor 3: Verkehrsverbünde und ÖPNV-Unternehmen

Diesem Untersektor sind Besteller/Betreiber von Öffentlichem Personennahverkehr (ÖPNV) zugeordnet. Hier kann zwischen Verkehrsverbünden (Tarifgemeinschaften) und ÖPNV-Unternehmen unterschieden werden [26]. In diesen Untersektor wurden 105 Unternehmen aufgenommen. Eine Übersicht findet sich in Abbildung 3 [27].

### 4.2.4 Untersektor 4: Fahrzeughersteller

Unter dem Gesichtspunkt „Hersteller des Endprodukts Fahrzeug im Eisenbahn- und ÖPNV-Sektor in Deutschland“ wurden Schienenfahrzeughersteller betrachtet. Es wurden die Unternehmen aufgenommen, die Elektrolokomotiven, Diesellokomotiven, U-Bahn-, Stadtbahn- und Straßenbahnfahrzeuge sowie Arbeits- und Sonderfahrzeuge produzieren. In die Betrachtung wurden 22 Unternehmen aufgenommen, u. a.:

- Alstom Transport Deutschland GmbH/Bombardier Transportation GmbH,
- Stadler Deutschland GmbH und
- Vossloh Locomotives GmbH (heute CRRC).

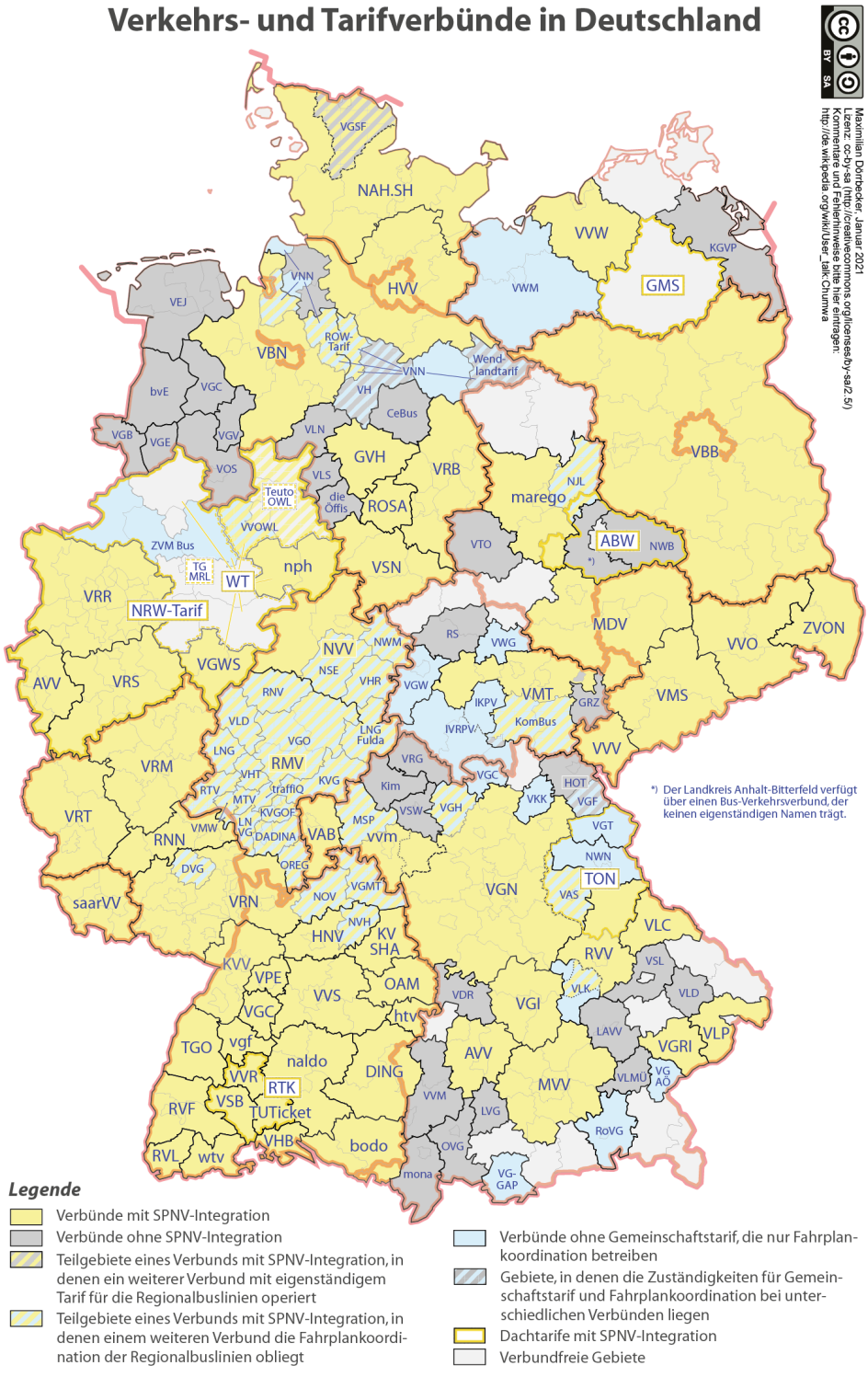


Abbildung 3: Tarif und Verkehrsverbünde in Deutschland [27]

## 4.2.5 Untersektor 5: Fahrzeuginstandhalter

In der Kategorie „Anbieter von Instandhaltung am Fahrzeug in Deutschland“ wurden Instandhaltungswerke identifiziert (Instandhaltungsverantwortliche Stellen – entity in charge of maintenance (ECM) gemäß Ril 2004/49/EG). In die Auswahl der Zielgruppe wurden 15 Unternehmen aufgenommen.

Dazu gehören die 12 Werke/Standorte der bundeseigenen

- DB Fahrzeuginstandhaltung GmbH,

die Dienstleistungen in Wartung und leichter Instandhaltung anbieten.

Ebenso betreiben auch nichtbundeseigene Unternehmen oder deren Tochterunternehmen eigene Werkstätten. Dazu gehören z. B.:

- EuroMaint Rail GmbH
- VIS Verkehrs Industrie Systeme GmbH
- Talgo (Deutschland) GmbH.

Es gibt auch zahlreiche Leasingunternehmen für Schienenfahrzeuge, die die Fahrzeuge von der Herstellerfirma erwerben und den Eisenbahnunternehmen in Miet- oder Leasingmodellen zur Verfügung stellen. Zum Teil haben diese Unternehmen die Instandhaltung ihrer Flotten mitorganisiert, zum Teil vertraglich ihren Mietparteien oder Leasingnehmern übertragen [25].

Außerdem besitzen die Hersteller:

- Alstom (Braunschweig (Projektsteuerung), Salzgitter, Stendal und Waibstadt)
- Siemens (Ersatzteillager in Neu-Isenburg)
- Stadler (Berlin und eigene Division als Service-Gesellschaft aus der Schweiz)

in Deutschland ebenfalls Standorte für die Modernisierung/Instandhaltung von Fahrzeugen, die teils auch Produktionsstandorte (siehe Untersektor 4) sind.

### 4.2.6 Untersektor 6: Infrastrukturhersteller

Als Infrastrukturhersteller wurden hier die Hersteller von Komponenten oder schlüsselfertigen Lösungen für die Eisenbahninfrastruktur aufgenommen. Laut Allgemeinem Eisenbahngesetz (AEG) sind dies Hersteller zum Bau und zur Unterhaltung von Schienenwegen. In die Auswahl der Zielgruppe wurden insgesamt 26 Unternehmen aufgenommen. Aus den Bereichen Gleisbau und Ingenieurbauwerke sind dies z. B.:

- DB Bahnbau Gruppe GmbH
- Spitzke SE.

Aus den Bereichen Betriebsleit- und Sicherheitssysteme sind es z. B.:

- Siemens Mobility GmbH
- Thales Deutschland GmbH
- Scheidt & Bachmann GmbH.

### 4.2.7 Untersektor 7: Energieversorger

In die Auswahl der Zielgruppe wurde der für die vorgenannten Untersektoren maßgebliche Energieversorger aufgenommen. Dies ist der Bahnstromversorger:

- DB Energie GmbH.

TABELLE 4: ANZAHL DER ANGESCHRIEBENEN UNTERNEHMEN IN DEN ENTSPRECHENDEN UNTERSEKTOREN

| Nr. | Untersektoren | Anzahl |
|---|---|---|
| 1 | Eisenbahnverkehrsunternehmen (EVU) | 418 |
| 2 | Eisenbahninfrastrukturunternehmen (EIU) | 115 |
| 3 | Energieversorger | 1 |
| 4 | Fahrzeughersteller | 22 |
| 5 | Fahrzeuginstandhalter | 15 |
| 6 | Infrastrukturhersteller | 26 |
| 7 | Verkehrsverbünde und ÖPNV-Unternehmen | 105 |
| 8 | Vertriebsplattformen | 5 |
| 9 | Andere: Unternehmen, die nicht den oben beschriebenen Untersektoren zugeordnet werden können | 1 |
| | Gesamt | 708 |

Weiterhin können hier Stadtwerke, die als örtliche Stromversorger und gleichzeitig als ÖPNV-Unternehmen (siehe Untersektor 7: Verkehrsverbünde und ÖPNV-Unternehmen) agieren, eingruppiert werden. Diese Eingruppierung wurde im Rahmen der Befragung durch die Befragten selbst vorgenommen.

### 4.2.8 Untersektor 8: Vertriebsplattformen

Bei den Vertriebsplattformen wurden nur Online-Vertriebsplattformen berücksichtigt. Diese sollen für die Fahrgäste die Leistungen im schienengebundenen Personenfernverkehr sowie lokale ÖPNV-Dienstleistungen und Services und nach Möglichkeit die übrigen verfügbaren Mobilitätsangebote multimodal verknüpfen. In die Auswahl der Zielgruppe wurden vier Unternehmen aufgenommen, beispielhaft:

- DB Vertrieb GmbH
- Transdev Vertrieb GmbH
- FAIRTIQ AG.

## 4.3 Zusammenfassung zu den Zielgruppen

Im Rahmen der Studie wurde eine Liste der zu befragenden Unternehmen in den entsprechenden Untersektoren erstellt, die für die Umfrage das System Eisenbahn und ÖPNV in Deutschland repräsentieren. Alle erfassten Unternehmen wurden mit der Bitte um Teilnahme an der Onlinebefragung angeschrieben (vgl. Serienbriefvorlage im Anhang 1). Die vollständige Liste der zu befragenden Unternehmen beinhaltet zum Zeitpunkt der Übergabe an das DZSF insgesamt 708 Datensätze (siehe Tabelle 4 und Abbildung 4).

Dabei fallen unter die Kategorie „Andere“ die Unternehmen, die nicht den oben beschriebenen Untersektoren zugeordnet werden können, wie Beratungsunternehmen im Bahnsektor.

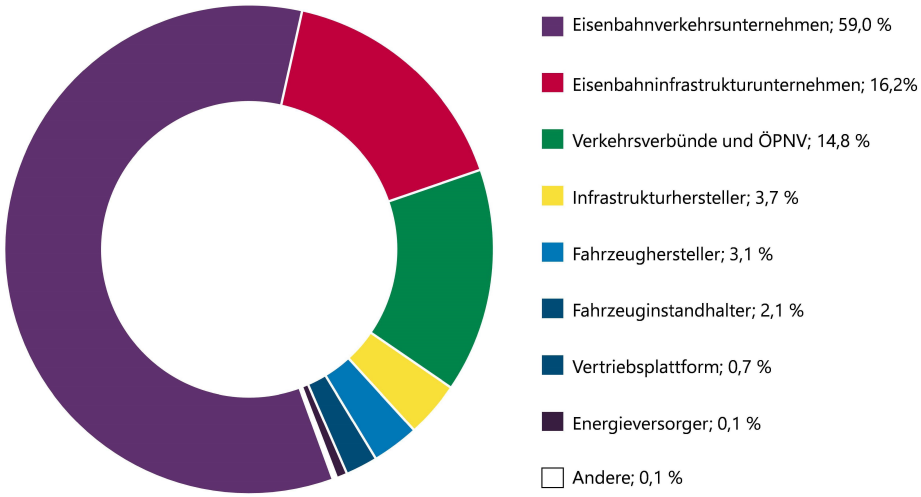


Abbildung 4: Verteilung der angefragten Unternehmen nach Untersektoren

# 5 Methodischer Ansatz

## 5.1 Reifegradmodell

In der vorliegenden Studie wird die Ist-Situation zur Cybersecurity und zu neuen Technologien im Eisenbahnsektor erfasst und bewertet. Zur Bewertung werden die mittels Befragung erhobenen Daten in einem Reifegradmodell abgebildet. Ziel des Reifegradmodells ist es, darzustellen, welche Prozesse oder Planungen noch unzureichend ausgestaltet sind und somit Handlungsbedarf besteht. Das Reifegradmodell erlaubt Zuordnungen, die beispielsweise im Bereich von 0 (niedrigste Bewertungsstufe des Reifegradmodells) bis 5 (höchste Bewertungsstufe des Reifegradmodells) liegen können [28]. Auf dieser Bewertungsgrundlage sind Hinweise auf mögliche Hindernisse für den zielorientierten Einsatz von Cybersecurity-Maßnahmen und den Einsatz neuer Technologien ableitbar. Gleichzeitig geben diese Informationen Hinweise auf ggf. erforderliche Maßnahmen zur Verbesserung der Cybersecurity und zum geplanten Einsatz neuer Technologien. Damit beschreibt das Reifegradmodell einen zielgerichteten kontinuierlichen Verbesserungsprozess zur Erreichung eines angestrebten Soll-Zustands.

Neben spezifisch technisch-orientierten Maßnahmen kann dies auch Entscheidungen zu den Zuständigkeiten und Verantwortlichkeiten zur Durchführung der Maßnahmen betreffen. Dies gilt auch für sich daraus ggf. ergebende Erfordernisse, beispielsweise für ad-hoc Aktivitäten zur Cybersecurity und zu neuen Technologien, die innerhalb des Unternehmens aktuell zu bedenken sind. Damit können die Ergebnisse der Befragung einen möglichen Entwicklungspfad in aufeinander folgenden Rangstufen aufzeigen. Das Reifegradmodell nutzt dafür Dimensionen, denen bei der Bewertung des jeweiligen Objekts Rechnung zu tragen ist. Allerdings berücksichtigt ein Reifegradmodell mehr als lediglich technologische Aspekte [29], was gleichbedeutend mit dem Sachverhalt ist, dass es kein einheitliches Modell zur Bestimmung des Reifegrads gibt.

Im Kontext der Studie kann beispielsweise im Reifegradmodell zum Thema Cybersecurity das aktuelle Erfahrungswissen zu Cyberangriffen auf Grundlage der Kernfunktionen des NIST-Cybersecurity-Frameworks für den Ist-Zustand des jeweils betrachteten Unternehmens abgebildet werden, wie in Abbildung 5 dargestellt. Weitere Dimensionen können auf organisatorische Rahmenbedingungen zum Thema Cybersecurity Bezug nehmen. Hierzu zählen unter anderem Projekte zur Implementierung einer Cybersecurity-Strategie. Die Mitarbeitenden müssen dafür aber das erforderliche Wissen und die notwendige Erfahrung mitbringen. Weiterhin muss aber auch das dafür erforderliche Budget bewilligt sein, um dem Projektumfang umfänglich Rechnung tragen zu können [30, 31].

Um das Reifegradmodell im spezifischen Kontext des jeweiligen Objekts (Cybersecurity, neue Technologien) einsetzen zu können, sind die zugrundeliegenden Dimensionen durch entsprechende Bewertungskriterien zu operationalisieren. Dazu werden im Allgemeinen Bewertungskriterien für die Reifegradstufen zugrunde gelegt, die im folgenden Bereich liegen können: 0 (niedrigste Bewertung: Es existiert keine Cybersecurity-Strategie, es gibt auch keine Planungen hierzu) bis 5 (höchste Bewertung: Neben der implementierten Cybersecurity-Strategie sind zusätzliche Maßnahmen zur kontinuierlichen Verbesserung vorhanden). Die Skala der Bewertungskriterien für die im Allgemeinen verwendeten Reifegradstufen ist in Tabelle 5 zusammengefasst.

TABELLE 5: BEWERTUNGSKRITERIEN FÜR REIFEGRADSTUFEN

| Stufe | Bewertungskriterien zur Cybersecurity und/oder neuen Technologien |
|---|---|
| 0 | Keine Aktivitäten |
| 1 | Planungen sind vorhanden, es gibt jedoch noch keine konkreten Umsetzungen |
| 2 | Teile aus der Maßnahmenplanung sind bereits umgesetzt |
| 3 | Thema ist vollständig umgesetzt und vollständig dokumentiert |
| 4 | Thema wird kontinuierlich auf Stand der Technik und im Hinblick auf Effizienz geprüft |
| 5 | Thema unterliegt einem kontinuierlichen Verbesserungsprozess (KVP) |

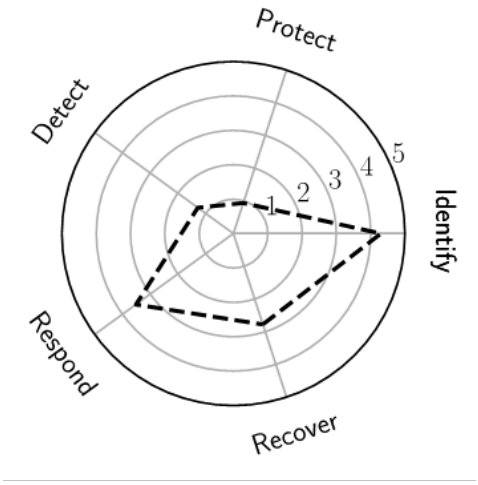


Abbildung 5: Netzdiagramm mit fünf Achsen (Dimensionen) des NIST-Rahmenwerks und sechs Reifegraden für einen beispielhaften Vergleich der Reifegrade verschiedener Unternehmen.

Die in der Tabelle 5 angegebenen Bewertungskriterien lassen sich in einem Netzdiagramm abbilden. Dieses eignet sich besonders zur anschaulichen Darstellung des Ist-Zustands der Studienobjekte Cybersecurity und geplanter Technologieeinsatz. Wie aus Tabelle 5 ersichtlich, bilden die Reifegradstufen den aktuellen Ist-Zustand innerhalb der dimensionalen Zuordnung zum jeweiligen Studienobjekt ab. Mit jeder Reifegradstufe steigt der Reifegrad. Dort, wo ein geringer Reifegrad vorliegt, ist ein größerer Handlungsbedarf erforderlich als bei einem höheren Reifegrad. Vor diesem Hintergrund kann das Reifegradmodell im Grunde genommen als ein Evaluationsmodell zur Darstellung der aktuellen unternehmerischen, technologischen oder wirtschaftlichen Fähigkeiten entlang des Anwendungsbezugs des jeweiligen Objekts betrachtet werden, welches auf dem reflexiven Prozess der Selbsteinschätzung aufbaut. Es ermöglicht implizit auch Handlungsempfehlungen für eine kontinuierliche Weiterentwicklung des Ist-Zustands in Richtung des angestrebten Soll-Zustands, um z. B. die Qualität oder die Innovation für einen betrachteten Prozess zu verbessern. Dafür sind dezidierte a-priori Kenntnisse zur Ist-Situation der betrachteten Organisation unabdingbar. Diese müssen gegebenenfalls an die spezifischen Rahmenbedingungen für das Reifegradmodell angepasst werden.

Abbildung 5 zeigt ein Beispiel für ein Netzdiagramm, welches auf das NIST-Cybersecurity-Framework Bezug nimmt. Das NIST-Cybersecurity-Framework [2] beschreibt fünf Kernfunktionen (vergleiche Abbildung 2). Diese Kernfunktionen sind, wie bereits im Abschnitt 5.1 erläutert, Identify, Detect, Protect, Respond und Recover, welche die fünf Dimensionen des in Abbildung 5 angegebenen Netzdiagramms bilden.

Bei der Betrachtung des Reifegrads ist auch der Aufwand abzuschätzen, der für die Erreichung eines höheren Reifegrads erforderlich ist. Zur Erreichung eines höheren Reifegrads können unter anderem die identifizierten Cybersecurity-Schwachstellen, unter Bezugnahme auf den Ist-Zustand der fünf NIST-Kernfunktionen für das jeweils betrachtete Unternehmen, zugrunde gelegt werden. Dies ist, im Hinblick auf seinen Nutzen, auch wirtschaftlich zu bewerten. Dabei sollte nicht außer Acht gelassen werden, dass neben den wirtschaftlichen Erwägungen zur Einführung von Maßnahmen zur Verbesserung der Cybersecurity in der Regel auch eine Veränderung der Arbeitssituation der betroffenen Mitarbeitenden vorliegen kann, was durch ergänzende Qualifikationsmaßnahmen positiv begleitet werden muss. Trotz dieser Nebenbedingung bietet das Reifegradmodell einen innovativen Ansatz, um eine einfache, verständliche und nachvollziehbare Bestimmung des Ist-Zustands für ein Studienobjekt zu erreichen. Dieser Duktus ist gleichzeitig Grundlage für die Entwicklung der zielorientierten Onlinebefragung und der nachfolgenden Interviewphase. Ergänzend sind nachfolgend einige qualitative Anmerkungen zum Reifegrad angegeben:

- Ein festgestellter Reifegrad $\leq 3$ als Ist-Zustand ist dahin gehend zu deuten, dass noch ein Hindernis in der Entwicklung der ökonomisch vorteilhaften Effekte zu dem Studienobjekt, hier Cybersecurity, vorliegt.
- Ein festgestellter Reifegrad von 4 als Ist-Zustand ist dahin gehend zu deuten, dass bereits eine gewisse Souveränität in der Entwicklung der ökonomisch vorteilhaften Effekte zum Studienobjekt vorliegt.
- Ein festgestellter Reifegrad von 5 als Ist Zustand ist dahin gehend zu deuten, dass das Studienobjekt in der Unternehmensstrategie verankert ist und kontinuierlich weiterentwickelt wird.

Die Kennzahlen in den Dimensionen des Reifegradmodells bilden somit die Basis oder den Indikator für die erforderlichen Cybersecurity-Maßnahmen zur notwendigen Erreichung des angestrebten Soll-Zustands.

## 5.2 SWOT-Analyse

Der Begriff SWOT-Analyse ist ein Akronym aus den Anfangsbuchstaben der englischen Begriffe:

- Strenghts (Stärken)
- Weaknesses (Schwächen)
- Opportunities (Chancen)
- Threats (Risiken).

Eine SWOT-Analyse ist ein pragmatischer Ansatz für eine realistische und zuverlässige Einschätzung einer aktuellen technologischen oder wirtschaftlichen Ausgangssituation (Ist-Situation) zu spezifischen Themenbereichen in einem Unternehmen, beispielsweise zu Versäumnissen bei der Cybersecurity im IT- oder OT-Bereich, einer unzureichenden Umsetzung technologischer Innovationen oder einem verschleppten Einsatz neuer Technologien. Dazu wird mittels einer SWOT-Analyse in der Regel das interne und externe Umfeld des Unternehmens untersucht [32].

Im internen Umfeld wird der Ist-Zustand des Unternehmens beschrieben. Dafür werden die Stärken und Schwächen des Unternehmens aufgelistet und analysiert. Hierbei fließen unterschiedliche Faktoren ein. Für die Stärken stehen unter anderem Innovation, Knowhow, Kundennutzen, Patente, qualifizierte Mitarbeitende, Technologieführerschaft. Schwächen werden beispielsweise durch ein geringeres Qualifikationsniveau der Mitarbeitenden, zu geringe Innovationshöhe oder fehlende agile Reaktion auf Kundenanforderungen dargestellt.

TABELLE 6: SWOT-ANALYSE IN DER PRAXIS [28]

| | |
|---|---|
| Welche **Stärken** sollen ausgebaut werden? | Welche **Schwächen** sollen überwunden werden? |
| Welche **Chancen** sollen genutzt werden? | Welche **Risiken** sollen reduziert werden? |

Durch das externe Umfeld werden die individuellen Einflussfaktoren auf die Chancen und Risiken des Unternehmens beschrieben. Hier gehen Faktoren ein, die beispielsweise durch die Entwicklung der Branchenstruktur oder Branchentrends im technologischen Wandel gekennzeichnet sein können, wie Digitalisierung, neue Technologien, Internet der Dinge (IoT), die den potenziell daraus resultierenden zukünftigen Chancen zugeordnet werden. Diese Faktoren lassen, im Kontext von Risiken, auch eine sich negativ verstärkende Tendenz erkennen, beispielsweise „keine Strategie vorhanden, um der Zunahme von Cyberangriffen auf das Unternehmen durch proaktive Abwehrmaßnahmen Rechnung zu tragen“ oder das „Währungsrisiko durch Wechselkursschwankungen infolge einseitiger Exportausrichtung des Unternehmens“.

Vor dem Hintergrund des voranstehend ausgeführten Sachverhalts wird eine SWOT-Analyse typischerweise in einer Vier-Quadranten-Matrix abgebildet, welche die Dimensionen Stärken, Schwächen, Chancen und Risiken darstellt. Eine SWOT-Analyse ist dabei in der Regel darauf ausgerichtet, den unternehmerischen Erfolg langfristig auszubauen und abzusichern. Das in Tabelle 6 angegebene Strukturbild der SWOT-Analyse zeigt die zugehörigen Dimensionen [32].

Mit der SWOT-Analyse können die wirksamen Maßnahmen identifiziert werden, die erforderlich sind, um vom Ist-Zustand des Unternehmens ausgehend, den zukünftig zu erreichenden Soll-Zustand abbilden zu können. Dafür erfordert die SWOT-Analyse Daten, die in der Regel aus Fragen extrahiert werden, welche mit Blick auf die Charakteristika und Einflussfaktoren gestellt werden. Daraus resultieren strategische Entscheidungen, die neben den Schwerpunktausrichtungen, den Zuständigkeiten und Verantwortlichkeiten auch die daraus ableitbaren Aktivitäten für die Ziele des Unternehmens beinhalten.

Wie in Tabelle 6 gezeigt, folgt das Grundprinzip der SWOT-Analyse dem Duktus, Stärken auszubauen und Schwächen abzubauen, sowie Chancen zu ergreifen und Risiken zu vermeiden. Da es sich hierbei um ein komplexes Wechselspiel der vier Dimensionen handelt, müssen diese, bezogen auf den zu erwartenden Schwierigkeitsgrad für die Zielerreichung, sortiert und priorisiert werden, um darauf aufbauend die zugehörigen erreichbaren Maßnahmen ableiten zu können. Die zu ergreifenden Maßnahmen sind dabei auf das zukünftig zu erreichende Unternehmensziel hin ausgerichtet, dem Soll-Zustand. In erster Linie besteht damit eine einfache Möglichkeit zur Untersuchung des Ist-Zustands. Weiterhin wird mit der SWOT-Analyse eine verlässliche methodische Ausgangsposition erreicht, die für die Entwicklung eines Maßnahmenmodells mitsamt der dazu erforderlichen Strategie zur Erreichung des Soll-Zustands erforderlich ist. Hierfür müssen wesentliche Kernfragen gestellt und beantwortet werden, die wie folgt strukturiert sein können:

- Warum sind einige Bereiche des Unternehmens technologisch innovativer als andere?
- Welche technologischen Trends werden in naher Zukunft großen Einfluss auf das Unternehmen haben?
- Welche Bereiche im Unternahmen fallen besonders durch technologische Probleme auf?
- Welche Chancen bieten neue Technologien für die Produkte oder neue Dienstleistungen des Unternehmens?

TABELLE 7: DARSTELLUNG BEISPIELHAFTER ASPEKTE IM RAHMEN EINER SWOT-ANALYSE ZUM THEMA NEUE TECHNOLOGIEN

| **Stärken** | **Schwächen** |
|---|---|
| Sichere und zuverlässige, bestehende Prozesse vorhanden | Mangelnde Innovationskraft bei technologischen Prozessen |
| Innovationsbereitschaft für neue Technologien vorhanden | Kein Knowhow über neue Technologien vorhanden |
| Knowhow über neue Technologien vorhanden | Nur geringes Knowhow über neue Technologien vorhanden |
| Knowhow in Cybersecurity vorhanden | Nur geringe Erfahrung, um mit Cyberangriffen umzugehen |
| Mitarbeitende begeistern sich für innovative Trends | Geringe Lernbereitschaft, Knowhow über neue Technologien zu erwerben |
| Starke Marktposition gegeben | Wenig innovatives Produktpotenzial im Markt |
| **Chancen** | **Risiken** |
| Bedeutung der Digitalisierung im technischen und organisatorischen Umfeld verstanden | Anforderungen neuer Technologien auf den Arbeitsplatz ist unklar |
| Technologische Trends verstanden | Auswirkungen von Cyberangriffen ist unklar |
| Nachhaltige Bedeutung neuer Technologien verstanden | Abhängigkeit von Knowhow der Lieferfirmen ist vorhanden |
| Anhaltendes Wachstum für innovative Produkte vorhanden | Vorgaben durch Gesetze und Verordnungen auf das Unternehmen sind schwierig abzuschätzen |

Dafür gilt es, belastbare Fakten zu sammeln [33, 34]. Ohne Anspruch auf Vollständigkeit zeigt Tabelle 7 beispielhaft entsprechende Fakten, die im Rahmen der Befragung umgesetzt wurden, um den Ist-Zustand zu ermitteln.

Wie aus Tabelle 7 ersichtlich, resultieren daraus mögliche Fragen in Bezug auf eine Chancenanalyse:

- Können Sie die für Ihr Unternehmen potenziellen Chancen zur Produkt- oder Dienstleistungsinnovation benennen, die durch die Digitalisierung im technischen und organisatorischen Umfeld entstehen können?
- Können Sie die für Ihr Unternehmen potenziellen Chancen zur Produkt- oder Dienstleistungsinnovation benennen, die durch technologische Trends im technologischen und organisatorischen Umfeld entstehen können?
- Können Sie die für Ihr Unternehmen potenziellen Chancen benennen, das erforderliche Wissen und die dafür erforderlichen Ressourcen in ihrem Unternehmen aufzubauen, um neue Technologien nachhaltig einsetzen zu können?
- Können Sie abschätzen, welcher Wettbewerbsvorteil Ihrem Unternehmen durch Einsatz neuer Technologien entstehen könnte?

Die SWOT-Analyse ist damit eine Informationsquelle für die strategische Planung, um die identifizierten Schwächen durch Maximieren der Chancen in Stärken zu transformieren. Das hilft darüber hinaus auch, die identifizierten Risiken zu überwinden.

Wegen der einfachen Handhabung zur Durchführung der SWOT-Analyse ist allerdings zu beachten, dass die Kategorisierung von Fakten im Rahmen der vier Dimensionen subjektiv ausfallen kann. Daher muss beim Entwurf der Befragung stringent und dezidiert vorgegangen werden, um eine möglichst objektive Datenanalyse zu ermöglichen. Hierfür sind im Rahmen eines Brainstormings sowohl für das interne Umfeld als auch für das externe Umfeld die wesentlichen qualitativen Kenngrößen zu definieren. Die Tabelle 8 gibt für das Studienobjekt Cybersecurity dafür einen Überblick.

TABELLE 8: SWOT-ANALYSE MIT POTENZIELLEN FAKTEN ZUR CYBERSECURITY

| **Stärken** | **Schwächen** |
|---|---|
| Die Bedeutung von Cybersecurity in den Geschäftsprozessen ist für Ihr Unternehmen von großer Bedeutung, um möglichen Gefährdungen durch Cyberangriffe vorzubeugen. Hierfür ist in der Regel ein entsprechendes Knowhow erforderlich, um beispielsweise Cyberangriffe am Arbeitsplatz zu erkennen und um diese bestmöglich abwehren zu können. Welche anerkannten methodischen Verfahren sind Ihrer Meinung nach hierbei bereits im Einsatz?<br>- Regelmäßig aktualisierte Antiviren-Software auf den Rechnern<br>- Robuste Zugriffsrichtlinie für Benutzer-Accounts<br>- Robuste Datenverschlüsselungspraktiken<br>- Verwendung eines VPN zur Kontrolle des -Zugriffs auf das Netzwerk, um dessen Gefährdung zu reduzieren<br>- Regelmäßige Updates über versuchte Cyberangriffs-Formen und Klassifikation nach deren Bedrohungspotenzial<br>- Regelmäßig aktualisierte und verbindliche, unternehmensweite Cybersecurity-Strategie | Cybersecurity ist für die Geschäftsprozesse Ihres Unternehmens wichtig. Hierfür sollte auch ein hinreichendes Cybersecurity-Bewusstsein vorhanden sein, um Cyberangriffe zu erkennen und abwehren zu können. Woran könnte es Ihrer Meinung nach liegen, dass effiziente Verfahren noch nicht hinreichend zur Anwendung kommen?<br>- Fehlende regelmäßige Aktualisierung der Antiviren-Software auf den Rechnern<br>- Fehlende Zugriffsrichtlinie für Benutzer-Accounts<br>- Fehlende zentralisierte Verfolgung von Cyberangriffen durch das Cybersecurity-Team<br>- Fehlende Datenverschlüsselungspraktiken<br>- Fehlen einer unternehmensweiten Cybersecurity-Strategie durch das Cybersecurity-Team<br>- Schlechte Ausführung der Update-Prozesse für Sicherheitspatches<br>- Nicht hinreichende Finanzierung erforderlicher Cybersecurity-Maßnahmen |
| **Chancen** | **Risiken** |
| Die Bedeutung von Cybersecurity in den Geschäftsprozessen ist für Ihr Unternehmen von großer Bedeutung, weshalb kontinuierlich an deren Verbesserung gearbeitet werden sollte. So kann auf mögliche Gefährdungen durch Cyberangriffe adäquat reagiert werden. Welche Veränderungen in Ihrem Unternehmen können Ihrer Meinung nach Vorteile bringen?<br>- Regelmäßige Aktualisierung des Knowhows zu neuen Speichertechnologien von Daten, | Die Bedeutung von Cybersecurity in den Geschäftsprozessen Ihres Unternehmens wird anerkannt. Unklar sind jedoch die erforderlichen Schritte, um auf mögliche Cybergefährdungen angemessen reagieren zu können. Wo sehen Sie deshalb die größten Schwachstellen?<br>- Keine verbindliche unternehmensweite Cybersecurity-Strategie, die das einheitliche Vorgehen bei einem Cyberangriff regelt<br>- Keine zentral verwalteten BYOD-Systeme (Mitarbeiter bringen eigene Hardware mit), |

| | |
|---|---|
| um diese immer auf dem neuesten Stand der Technik zu halten und abzusichern<br>- Optionen für die Datenspeicherung innerhalb von Cloud Dienste abwägen, um sie für den potenziellen Einsatz aufzubereiten<br>- Implementierung einer intelligenten Edge Plattform, um mit der sich wandelnden Bedrohungslandschaft zu interagieren und zu lernen (watching the watchers)<br>- Nachhaltiges Wachstum durch ein gegenüber Cyberangriffen geschütztes Geschäftsmodell<br>- Anerkannte Priorität und Unterstützung seitens der Geschäftsführung | die potenziell die Risiken von Informationsdiebstahl/-verlust und das Risiko von Hackerangriffen erhöhen<br>- Ungeschützte offene WLAN-Verbindungen ermöglichen nicht autorisierten Personen den Zugang zum Unternehmensnetzwerk<br>- Angriffsformen durch Einschleusen von Computerviren<br>- Hackerangriffe mit dem Ziel des Einschleusens von Malware<br>- Kein ausreichendes Knowhow im Bereich Cybersecurity aufgebaut, aber Ransomware ist überall<br>- Nichteinhaltung gesetzlicher Vorschriften |

Die Auswertung bietet zielorientierte Hinweise, welche die vorab getroffenen Zielsetzungen unterstützen. Hierfür wird etwa eine Bewertungsskala gewählt, welche die Zuordnungen sehr schlecht, schlecht, mittel, gut, sehr gut für die SWOT-Analysekriterien enthält. Daraus kann sich in der Ergebnisdarstellung ein sogenannter Zick-Zack-Graph in den Zuweisungen zu Stärken-Schwächen-Chancen-Risiken ergeben.

# 5.3 Fragebogenerstellung der Onlinebefragung und Festlegung der Interviewschwerpunkte

## 5.3.1 Hintergrund zum Onlinefragebogen

Bei der Erstellung der Onlinebefragung wurde auf die gezielte Trennung der Bereiche Status quo „Security“ und Status quo „geplanter Technologieeinsatz“ geachtet. In diesen sich ergebenden Bereichen erfolgte die Abfrage auf Grundlage des NIST-CSF-Frameworks. Jedem Teilnehmenden wurden 121 Fragen gestellt, davon 61 Fragen zur Cybersecurity, 60 Fragen zu neuen Technologien und zusätzlich 4 Fragen zur Unternehmenscharakterisierung. Dieser Fragebogen wurde von den Teilnehmenden im Schnitt binnen ca. 30 Minuten beantwortet. Die Hauptbestandteile der Befragung werden in den nachfolgenden beiden Abschnitten beschrieben. Der vollständige Fragebogen ist im Anhang 2 zu finden.

## 5.3.2 Onlinefragebogen zur Cybersecurity

Im ersten Teil der Befragung wurde der aktuelle Stand der Cybersecurity ermittelt. Dabei wurde das in Kapitel 3 beschrieben NIST-Modell herangezogen. Die Fragen, die auf dem Reifegradmodell basieren, spiegeln die einzelnen Kernfunktionen des NIST-Modells wider. Die Formulierung der Fragen stellt eine eindeutige Zuordnung der Antworten sicher. Um eine weitere Dimension der Evaluierung hinzuzufügen, sind neben den NIST-Kernfunktionen die Fragen in die Themen Organisation, IT-Systeme, OT-Systeme sowie IT- und OT-Infrastruktur eingeteilt. Bei der Erfassung von Informationen über die Organisation und die NIST-Kernfunktion „Protect“ wird etwa die Frage gestellt: „Stellt Ihr Unternehmen sicher, dass alle Mitarbeitende in Cybersecurity geschult sind?“. Eine Aufteilung der Fragen zu den unterschiedlichen Kernfunktionen, aber auch den verschiedenen Themen ist Tabelle 9 zu entnehmen. Das Antwortschema war bei jeder Frage gleich. Mit Hilfe des Reifegradmodells wurde eine Skala entwickelt, welche eine lineare Bewertung vorsieht. So konnten die Teilnehmenden eine der Antwortmöglichkeiten wählen, welche in der Tabelle 10 aufgezählt sind. Diese Antwortmöglichkeiten sind angelehnt an die Reifegradstufen aus Tabelle 5.

TABELLE 9: ANZAHL AN FRAGEN IN DEN SCHNITTPUNKTEN VON THEMA UND NIST-KERNFUNKTION

| Thema | NIST-Kernfunktionen | | | | |
|---|---|---|---|---|---|
| | Identify | Protect | Detect | Respond | Recover |
| Organisation | 1 | 3 | 1 | 1 | 1 |
| IT-Systeme | 3 | 2 | 2 | 2 | 2 |
| IT-Infrastruktur | 3 | 4 | 1 | 1 | 2 |
| OT-Systeme | 3 | 2 | 2 | 1 | 2 |
| OT-Infrastruktur | 3 | 4 | 2 | 1 | 2 |

TABELLE 10: ANTWORTMÖGLICHKEITEN FÜR DIE FRAGEN DES STATUS QUO ZUR CYBERSECURITY.

| Stufe | Antwortmöglichkeiten |
|---|---|
| 0 | Nein. |
| 1 | Nein, eine Planung ist aber vorhanden. |
| 2 | Ja, jedoch sind nur Teile der Planung umgesetzt. |
| 3 | Ja, die Planung ist vollständig umgesetzt und dokumentiert. |
| 4 | Ja und unsere Umsetzung wird kontinuierlich auf Effektivität geprüft. |
| 5 | Ja und unsere Umsetzung unterliegt der kontinuierlichen Verbesserung. |

Für eine Aussage zum Status quo der Cybersecurity wurden nicht nur Fragen unter Zuhilfenahme des Reifegradmodells, sondern auch Fragen zu bereits aufgetretenen Cybersecurity-Vorfällen sowie entstandenem Schaden und zur Anzahl von Angriffen gestellt. Ebenso wurden die Art von Cyberangriffen sowie die Hürden, welche einer ausreichenden Cybersecurity-Strategie im Wege stehen, erhoben. Da die Fragen in geschlossener Form gestellt wurden, hatten die teilnehmenden Unternehmen keine Gelegenheit zur Stellungnahme. Die Vertreterin bzw. der Vertreter eines teilnehmenden Unternehmens konnte jedoch am Ende des Fragebogens freiwillig Kontaktinformationen für ein anschließendes Interview zur Erläuterung von Details (siehe Abschnitt 5.3.7) übermitteln.

### 5.3.3 Onlinefragebogen zu neuen Technologien

Abweichend vom Fragebogenteil zur Cybersecurity unterliegt der Teil der neuen Technologie einem anderen Schema. Die hierbei im Fokus stehenden neuen Technologien wurden im Abschnitt 3.4 beschrieben, ähnliche Technologien wie NFV und SDN wurden hierbei zusammengefasst. Insgesamt ergeben sich durch die Zusammenfassung zwölf neue Technologien zur Untersuchung. Um ein möglichst gutes Bild für die neuen Technologien zu erhalten, wurden die folgenden Bereiche erfragt:

- Knowhow,
- Einsatzwahrscheinlichkeit,
- zeitlicher Einfluss,
- Änderungseinfluss und
- Risiko.

TABELLE 11: ANTWORTMÖGLICHKEITEN FÜR DIE FRAGE NACH DEM WISSENSSTAND ZU NEUEN TECHNOLOGIEN.

| Antwortmöglichkeit | Erläuterung |
|---|---|
| 0 (keine) | Die neue Technologie ist nicht bekannt. |
| 1 (gering) | Die neue Technologie ist bekannt, aber die zur Verfügung stehenden Informationen sind noch nicht verstanden und/oder bearbeitet. |
| 2 (mittel) | Die neue Technologie ist bekannt und die zur Verfügung stehenden Informationen sind weitgehend verstanden und/oder bearbeitet. |
| 3 (hoch) | Die neue Technologie ist verstanden und ein darauf fußendes, solides Grundlagenwissen aufgebaut. |
| 4 (sehr hoch) | Die neue Technologie ist verstanden und das Grundlagenwissen wird, aufgrund kontinuierlicher Weiterentwicklung der Technologie, aktiv ständig erweitert. |

Zugrundeliegend ist bei jeder Frage eine lineare Antwortskala. Die Ausprägungen der Skala sind dabei durch je eine Aussage beschrieben, sodass sich Teilnehmende mit der Ausprägung besser identifizieren können. Daraus resultieren die Antwortmöglichkeiten zum Wissensstand, wie in der Tabelle 11 dargestellt.

Wurde bei einem Unternehmen bei der ersten Frage nach dem Knowhow kein Wissen über eine oder mehrere der zwölf Technologien festgestellt, wurden zu diesen Technologien keine weiterführenden Fragen mehr gestellt. Somit konnten Teilnehmende keine Aussagen über Einfluss oder Risiko treffen, da ohne das notwendige Wissen über eine Technologie auch keine qualifizierte Aussage über ebendiese getätigt werden kann. Sollten Unternehmen bzw. Teilnehmende zu allen zwölf abgefragten Technologien über Wissen verfügen, ergeben sich insgesamt 60 Fragen, welche zu beantworten waren. Das Ziel dieses Bereichs des Fragebogens war es, eine Übersicht über die Vor- und Nachteile der neuen Technologien zu erhalten und mit dem aktuell ermittelten Cybersecurity-Risiko zu vergleichen. Außerdem können Prognosen darüber getroffen werden, ob eine Technologie für den Sektor Bahn oder einen Untersektor von Interesse ist sowie welche der Technologien das größte Risiko aufweist.

### 5.3.4 Durchführung der Onlinebefragung

Zur Durchführung der Befragung wurde ein Zeitraum von insgesamt vier Monaten, von September 2021 bis Ende Dezember 2021 gewählt. Angeschrieben wurden Personen aus den in Kapitel 4 beschriebenen Unternehmen. Dabei wurden, wo vorhanden, direkte Kontaktdaten herangezogen, welche über die Webpräsenz des Unternehmens verfügbar waren. Mit Hilfe eines Schreibens des DZSFs an die Unternehmen wurden die Teilnehmerinnen und Teilnehmer auf diese Datenerhebung hingewiesen. Zusätzlich zu den Anschreiben wurde auf den Social-Media-Kanälen der Autoren und des Auftraggebers um die Teilnahme an dieser Studie gebeten. Die Teilnehmenden erhielten einen einmalig nutzbaren Zugangscode, sodass sichergestellt werden konnte, dass nur Vertreter aus Unternehmen teilnehmen konnten, welche aus den gewünschten Untersektoren und nicht aus alternativen Branchen stammten. Ferner war auch eine direkte Ansprache des Autorenteams möglich, um so einen Zugangscode zu erhalten. Durch interne Trennung von Auswertung und Kommunikation zu den Unternehmen konnte im Autorenteam die Anonymität der Teilnehmenden gewährleistet werden.

### 5.3.5 Interviewfragebogen zur Cybersecurity

Der Fragebogen stellt den ersten Teil des Interviewleitfadens dar und diente als Hilfestellung für die Befragung (für den vollständigen Leitfaden, siehe Anhang 4). Hierbei sollte die Möglichkeit genutzt werden, mit offenen Fragen tiefer in ausgewählte Themen einzusteigen, um auf diese Weise den Nachteil der geschlossenen Fragen aus dem Onlinefragebogen auszugleichen. Angesichts dessen wurde die Form des semistrukturierten Interviews (siehe beispielsweise [35]) gewählt. Als Kompromiss zwischen der großen Menge interessanter Themen, welche in einem solchen Interview vertieft werden können, und der Rücksicht auf die Zeit der Interview-Teilnehmenden wurde eine Gesamtdauer inklusive Begrüßung und Verabschiedung von ungefähr einer Stunde eingeplant. Aufgrund der aktuellen Corona-Pandemie, aber auch der räumlichen Distanz zu den Interviewten wurden die Interviews per Videokonferenz durchgeführt.

Im Wesentlichen verfolgten die Interviews drei Kernziele:

- die Klärung von Widersprüchen und Auffälligkeiten,
- die Vertiefung bestimmter Fragen hinsichtlich des Reifegrads und
- die Erhebung von Daten für eine SWOT-Analyse (siehe Abschnitt 5.2).

Das erste Kernziel lag in der Betrachtung von Widersprüchen und Auffälligkeiten. Ein betrachteter Widerspruch lag vor, falls Teilnehmende für eine bestimmte NIST-Kernfunktion angaben, diese durch ihre Cybersecurity-Strategie abzudecken, in der Onlinebefragung für diese Kernfunktion aber ein niedriger Reifegrad (kleiner 3, siehe Abschnitt 5.1) ermittelt wurde. Eine weitere Auffälligkeit von Interesse lag vor, wenn der Reifegrad einer einzelnen Kernfunktion weit unterdurchschnittlich ausfiel, was hier als eine Differenz von zwei oder mehr Reifegradstufen zu den restlichen Kernfunktionen definiert wurde. Um diese Auffälligkeiten aufzulösen, wurden betroffene Themen nochmals angesprochen, jedoch zunächst, ohne die Punkte mit Klärungsbedarf direkt zu adressieren. Stattdessen wurden sie im offenen Gespräch geklärt. Im Fall des unterdurchschnittlichen Reifegrads einzelner Kernfunktionen sollte zudem explizit nachgefragt werden, welche dazugehörigen Maßnahmen im Unternehmen ergriffen wurden und wie diese umgesetzt sind. Die so gewonnenen Erkenntnisse sollten neben der Auflösung von Auffälligkeiten auch der SWOT-Analyse sowie dem vertieften Verständnis der Ursachen des Reifegrads und damit dem zweiten und dritten Kernziel der Interviews dienen.

Neben den hierbei gewonnenen Informationen betraf die Vertiefung des Verständnisses der Ursachen des Reifegrads insbesondere auch der Rolle des Cybersecurity-Beauftragten sowie der Durchführung von Schulungen in den befragten Unternehmen. Bei der Frage nach dem Cybersecurity-Beauftragten konnte im Onlinefragebogen lediglich das Vorhandensein eines solchen abgefragt werden, während in den Interviews darüber hinaus auf die Qualität dieser Rolle, auf den Umfang des Aufgabenbereichs sowie die zeitliche Verfügbarkeit geblickt wurde. In diesem Zuge wurde außerdem die unternehmensweite Organisation der Cybersecurity erfragt. Gleichermaßen wurde der Detailgrad über die Durchführung von Schulungen vertieft, insbesondere hinsichtlich ihrer Häufigkeit, Verpflichtung, ihrem Umfang und dem Vorhandensein einer anschließenden Wissensprüfung.

Die Erhebung von Daten zur SWOT-Analyse war das Hauptziel der „Warum"-Frage, also der Erforschung der eigentlichen Ursache hinter dem Status quo. Hinsichtlich Stärken und Chancen wurde erfragt, wie ein guter Zustand erreicht wurde und was die Unternehmen hierbei maßgeblich unterstützt hat. Speziell bei solchen Unternehmen, welche bereits einen hohen Reifegrad der Cybersecurity aufwiesen, sollte vom Wissen und der Erfahrung der Interviewten profitiert werden, um Empfehlungen abzuleiten, welche zur Verbesserung des Reifegrads in weniger gut aufgestellten Unternehmen genutzt werden können.

Im Gegenzug diente eine Selbsteinschätzung der bestehenden Hindernisse der Erforschung von Schwächen (im Falle von internen Faktoren als Hindernis) sowie Bedrohungen (im Falle von externen Faktoren).

Hierbei wurden zudem die notwendigen Maßnahmen und die benötigten Hilfestellungen zur Überwindung dieser Hindernisse ergründet. Zuletzt wurden außerdem die Wünsche der Befragten an die Politik oder ähnliche Rahmenbedingungen schaffende Organisationen erfragt.

Um die beschriebenen Ziele zu erreichen, wurden die Fragen für jedes Unternehmen spezifisch an ihre Ergebnisse aus der Onlinebefragung angepasst (für ein Beispiel eines unternehmensspezifischen Fragebogens, siehe Anhang 5). Hierbei wurden Kriterien erstellt, um basierend auf den Antworten zu einzelnen oder mehreren Fragen, die Themen zu vertiefen, welche in Hinsicht auf die oben genannten Ziele am vielversprechendsten waren. Ein Beispiel hierfür war die Ergründung von Schulungsstrategien bei Unternehmen, welche bereits seit längerer Zeit erfolgreich Schulungen für die Mitarbeitenden anboten.

Die Interviewpartnerinnen und Interviewpartner wurden basierend auf verschiedenen Kriterien aus den Teilnehmenden der Onlinebefragung gewählt. Das Ziel hierbei lag darin, eine für die an der Onlinebefragung beteiligte Menge von Unternehmen möglichst repräsentative Gruppe zu finden. Zu diesem Zweck wurde darauf geachtet, alle Sektoren (siehe Kapitel 4) abzudecken sowie die Anzahl der Interviewpartner je Sektor an die relative Größe des jeweiligen Sektors anzupassen. Zudem wurden solche Unternehmen gewählt, durch welche die gesamte Breite des Reifegradspektrums sowie die Reichweite der vertretenen Unternehmensgrößen abgedeckt wurden. Letztlich wurden außerdem die betrachteten neuen Technologien (siehe Abschnitt 6.3) berücksichtigt, sodass Teilnehmende mit hinreichender Erfahrung für jede dieser Technologien vertreten waren.

### 5.3.6 Interviewfragebogen zu neuen Technologien

Das Vorgehen zur Abfrage genutzter neuer Technologien war äquivalent zum Vorgehen beim Thema der Cybersecurity. Die Fragen wurden ebenso an die Ergebnisse der Onlinebefragung angepasst und im Anschluss an die Fragen zur Cybersecurity gestellt. Ein Ziel hierbei lag darin, möglichst zu jeder der betrachteten neuen Technologien ein Unternehmen befragen zu können, welches bereits umfassende Erfahrungen mit der jeweiligen Technologie besaß.

Erhoben wurden auch hierbei Daten zur Durchführung einer SWOT Analyse. Zu diesem Zweck wurden die Stärken und Chancen („Können Sie kurz erläutern, welche Stärken bzw. Chancen Sie im Einsatz dieser Technologien sehen?“) sowie Schwächen und Bedrohungen („Was sind aktuell oder waren in der Vergangenheit die größten Hindernisse, welche Sie beim Einsatz dieser Technologien überwinden mussten oder müssen?“) der betroffenen Technologien direkt abgefragt.

### 5.3.7 Durchführung und Protokollierung der Interviews

Das Vorgehen bei der Durchführung sowie Protokollierung der Interviews wurde in der Anleitung für Interviewende im zweiten Teil des Interviewleitfadens detailliert beschrieben. Um über alle Interviews hinweg eine möglichst einheitliche Vorgehensweise einhalten zu können, wurden hier zwei Hilfsmittel definiert.

Zum einen wurde eine Einleitung für das Interview vorformuliert, welche wörtlich übernommen werden konnte. Diese beinhaltet eine Begrüßung, die Erläuterung des Interviewhintergrunds mit Hinweis auf den Bezug zum Onlinefragebogen (für den Fall, dass dieser nicht von der interviewten Person ausgefüllt wurde), einer Erklärung der Datenschutzaspekte sowie der Einweisung der Interviewten.

Zum anderen wurden detaillierte Anweisungen für die Interviewdurchführung geliefert. Hierbei wurde empfohlen, die Interviews mit zwei Personen durchzuführen, eine für die Befragung sowie eine für die Protokollierung. Für die Protokollierung genügte eine stichpunktartige Erfassung des Gesagten, welche

durch relevante Zitate nach Ermessen der protokollierenden Person angereichert werden konnte. Die interviewende Person wurde angewiesen, die Befragung in einer möglichst neutralen Haltung durchzuführen. Dies ist insbesondere bei sensitiven Themen, zu denen die Cybersecurity definitiv gehört, wichtig, um eine offene Gesprächsatmosphäre zu schaffen. Dabei sollten die Fragen des Fragebogens als Orientierung dienen. Falls jedoch interessante Themen angeschnitten wurden, welche nicht durch den Fragebogen abgedeckt waren oder falls Antworten zu knapp oder unklar ausfielen, sollten zusätzliche Fragen zur Erläuterung gestellt werden. Bei den vorgegebenen Fragen wurde darum gebeten, sich an die gegebene Formulierung zu halten, um die Standardisierung der Interviews zu gewährleisten. Um bei der Formulierung darüberhinausgehender Nachfragen zu unterstützen, wurde nochmals das Ziel des Interviews erläutert, auf welches die Fragen abzielen sollten. Dieses lag vornehmlich in der Erforschung des „Warums“, also der eigentlichen Ursache hinter dem Status quo, um bestimmen zu können, wie die aktuelle Situation verbessert werden kann. Des Weiteren wurde darauf hingewiesen, Fragen dergestalt zu formulieren, dass sie die Antwort möglichst wenig leiten und so, dass stets nur eine Frage gleichzeitig gestellt wurde. Diese Anweisungen wurden teilweise durch Beispiele ergänzt, um speziell unerfahrenen Interviewenden die Einhaltung zu erleichtern. Zuletzt wurde eine Liste mit Stichpunkten zu interessanten Themen geliefert, welche als Leitlinie zum Nachfragen dienen konnten. Diese beinhalteten die Frage nach der Motivation, Expertise und Personalkapazität, den einmaligen sowie laufenden Kosten und schließlich den politischen, wirtschaftlichen und regulatorischen Rahmenbedingungen sowie Herausforderungen (siehe dazu Anhang 4).

# 6 Ergebnisse der Onlinebefragung

## 6.1 Einordnung

Im Rahmen dieser Studie wurden insgesamt 711 Unternehmen kontaktiert, weitere vier Unternehmen haben sich um die Teilnahme beworben. Damit ergab sich eine Gesamtstichprobe von 715 Unternehmen. Von den kontaktierten Unternehmen hatten insgesamt 59 Unternehmen die Onlinebefragung vollständig ausgefüllt. Je nach Untersektor erhielten wir eine prozentuale Antwortquote zwischen 5,48 % (23 von 420 Eisenbahnverkehrsunternehmen) und 100 % (Energieversorger). Für den Untersektor Energieversorger hatten wir nur ein Unternehmen kontaktiert, zwei weitere haben sich selbst als Energieversorger eingestuft.

In den folgenden Abschnitten wird anhand verschiedener Analysen näher auf die Ergebnisse der Onlinebefragung eingegangen. Der erste Teil der Ergebnisse ermöglicht einerseits einen umfassenden Überblick über Cyberangriffe in den teilnehmenden Unternehmen und zum anderen auch Einblicke über bereits umgesetzte oder zukünftig geplante Maßnahmen im Bereich der Cybersecurity. Dazu wurde basierend auf den NIST-Kernfunktionen der Reifegrad der teilnehmenden Unternehmen anhand eines umfangreichen Fragebogens ermittelt. Die Ergebnisse sind im Abschnitt 6.2 zusammengefasst.

Im zweiten Teil der Onlinebefragung, gaben die befragten Unternehmen Auskunft über unterschiedliche Aspekte der neuen Technologien, wie Stand des Wissens, den Einsatzmöglichkeiten der neuen Technologien und mögliche Risiken, die durch die Einführung entstehen können. Die Ergebnisse sind dazu im Abschnitt 6.3 zusammengestellt.

## 6.2 Cybersecurity

### 6.2.1 Gesamtreifegrade der acht Untersektoren

Die Abbildung 6 zeigt die Analyse des Reifegrades nach Untersektoren. Diese, sowie die Reifegrade in den einzelnen NIST-Disziplinen, sind zusammen mit den Konfidenzintervallen auch der Tabelle 12 zu entnehmen. Wie deutlich zu erkennen ist, gibt es eine große Bandbreite an individuellen Reifegraden der abgebildeten Untersektoren. Insbesondere der Untersektor EVU deckt das gesamte Spektrum des Reifegrads zwischen 0 und 5 ab. Bei der Analyse ist allerdings zu beachten, dass die Anzahl der teilnehmenden Unternehmen in den jeweiligen Untersektoren sehr unterschiedlich ist. Dies spiegelt sich auch in der Darstellung wider – die Anzahl der antwortenden Fahrzeuginstandhalter und Infrastrukturhersteller ist nicht ausreichend, um vier Quantile zu bilden.

Die EIU fallen gegenüber den anderen Untersektoren deutlich ab, was den Median und alle Quantile betrifft. Während der Median für alle anderen Branchen um einen Wert von 2 liegt, erreichen die EIU nur ein Niveau von 1. Lediglich ein einziger Ausreißer nach oben erreicht ein Niveau von fast 3. In der Analyse ist aber auch zu berücksichtigen, dass die KRITIS-Regelungen in Deutschland hauptsächlich die Infrastrukturbetreiber betreffen und diese Unternehmen vom Gesetz her Maßnahmen zum Schutz ihrer IT- und OT-Systeme nachweisen müssen. Auch das ist vermutlich ein Grund für die Unterschiede zwischen den Reifegraden der Untersektoren.

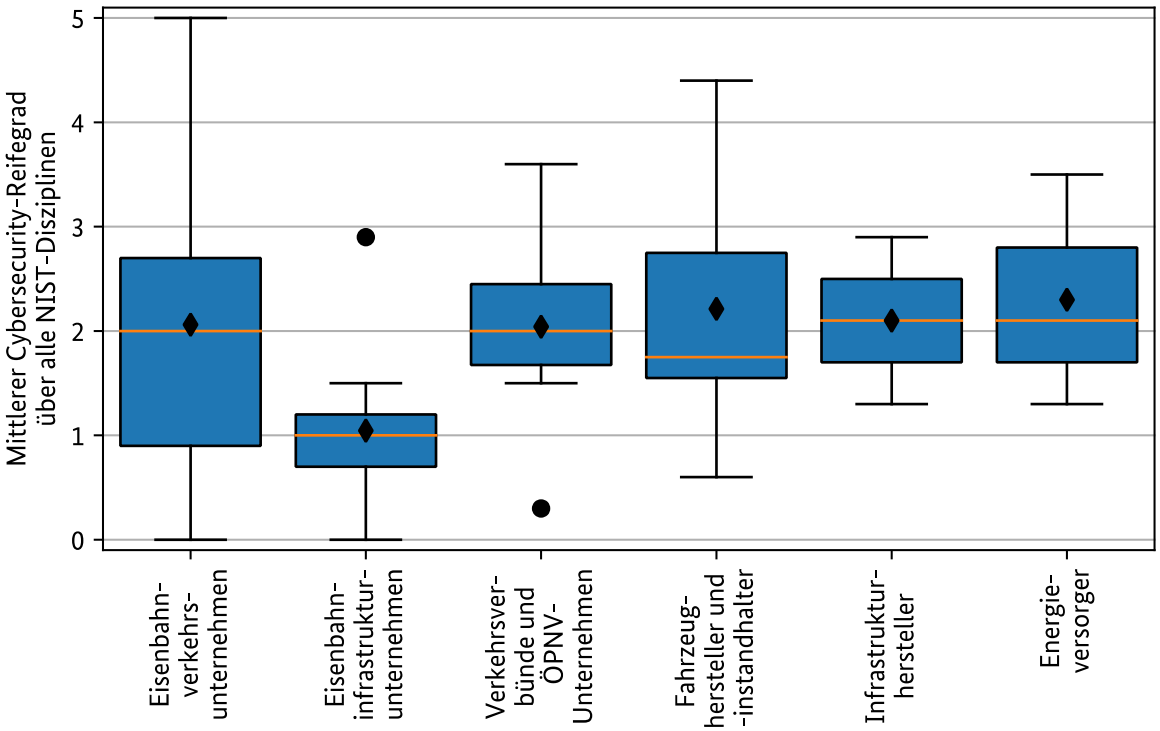


Abbildung 6: Gesamtreifegrad nach Untersektoren

TABELLE 12: REIFEGRAD FÜR DIE NIST-KRITERIEN NACH UNTERSEKTOREN IN MITTELWERTEN UND KONFIDENZINTERVALLEN

| **Untersektoren** | **NIST Reifegrad** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Identity** | | **Protect** | | **Detect** | | **Respond** | | **Recover** | |
| | **$\bar{x}$** | **CI** | **$\bar{x}$** | **CI** | **$\bar{x}$** | **CI** | **$\bar{x}$** | **CI** | **$\bar{x}$** | **CI** |
| Eisenbahnverkehrsunternehmen (EVU) | 1,98 | 0,72 | 2,15 | 0,71 | 1,96 | 0,74 | 1,76 | 0,73 | 2,55 | 0,73 |
| Eisenbahninfrastrukturunternehmen (EIU) | 1,01 | 0,81 | 1,24 | 0,76 | 1,03 | 0,83 | 0,69 | 0,61 | 1,63 | 0,96 |
| Verkehrsverbünde und ÖPNV-Unternehmen | 1,79 | 0,75 | 2,15 | 0,79 | 1,55 | 0,91 | 1,73 | 0,80 | 2,57 | 0,88 |
| Fahrzeughersteller | 2,31 | 1,04 | 2,36 | 1,15 | 1,87 | 1,09 | 1,93 | 1,12 | 2,49 | 1,06 |
| Infrastrukturhersteller | 2,15 | 2,26 | 2,43 | 0,91 | 1,94 | 2,05 | 1,58 | 1,55 | 2,06 | 1,99 |
| Energieversorger | 2,77 | 2,06 | 2,49 | 0,97 | 1,63 | 1,76 | 1,56 | 1,37 | 2,30 | 1,56 |
| Andere | Zur Anonymisierung nicht dargestellt | | | | | | | | | |
| Gesamt | 1,89 | 0,42 | 2,07 | 0,40 | 1,69 | 0,43 | 1,58 | 0,40 | 2,36 | 0,43 |

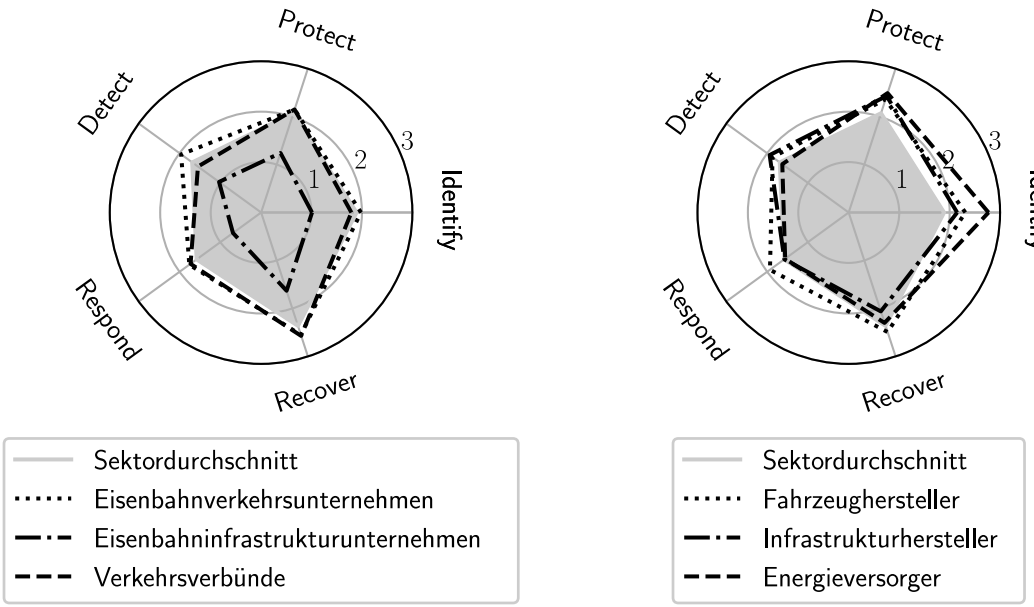


Abbildung 7: Reifegrade der Untersektoren jeweils im Verhältnis zum Gesamtergebnis

Die unterschiedlichen Streuungen in den Sektoren lassen sich unter anderem dadurch erklären, dass die Heterogenität der erfassten Unternehmen zwischen den acht Untersektoren sehr unterschiedlich ist. So hat etwa der Untersektor EVU eine sehr breite Streuung an Unternehmen von der kleinen Museumsbahn bis zum globalen Unternehmen wie die Deutsche Bahn. In den anderen Sektoren ist diese Diversität weit weniger ausgeprägt.

### 6.2.2 Reifegrade in den NIST-Kernfunktionen in den verschiedenen Untersektoren

Die Analyse der Reifegrade in den NIST-Kernfunktionen je Untersektor beantwortet die Frage, ob und wenn ja, wie unterschiedlich die Reifegrade in den NIST-Kernfunktionen in den jeweiligen acht Untersektoren bewertet wurden (siehe Abbildung 7).

Abbildung 7 stellt die Ergebnisse dar. Zur besseren Lesbarkeit und da alle Untersektoren unter diesem Wert liegen, wurde die Skala auf 3 beschränkt. Der grau hinterlegte Bereich innerhalb der beiden Unterabbildungen zeichnet den Durchschnitt aller Teilnehmer über alle acht Untersektoren. Im Verhältnis dazu stellen die Linien in den Abbildungen die Ergebnisse des jeweiligen Untersektors dar. In der linken Unterabbildung fallen die niedrigen Reifegrade im Untersektor EIU auf, während die Reifegrade der Untersektoren EVU und Verkehrsverbünde nahe dem Durchschnitt liegen. In der rechten Unterabbildung fallen die Energieversorger mit überdurchschnittlichen Werten in der Kategorie Identify auf.

### 6.2.3 Reifegrade in Bezug auf die Unternehmensgröße anhand der Mitarbeiteranzahl

Es galt, die Annahme zu überprüfen, dass Unternehmen mit einer größeren Anzahl von Mitarbeiterinnen und Mitarbeiter einen höheren Reifegrad der Cybersecurity erreichen. In Abbildung 8 ist der Gesamtreifegrad der Unternehmen in Abhängigkeit von sechs Kategorien der Unternehmensgröße nach Mitarbeiteranzahl dargestellt. Die Analyse der Daten zum Gesamtreifegrad zwischen der Mitarbeiterzahl und dem Reifegrad in Abbildung 8 ergeben mit Berechnung des Spearman-Koeffizienten [36] einen Wert von 0,42 und zeigen daher eine moderate bis große positive Korrelation [37].

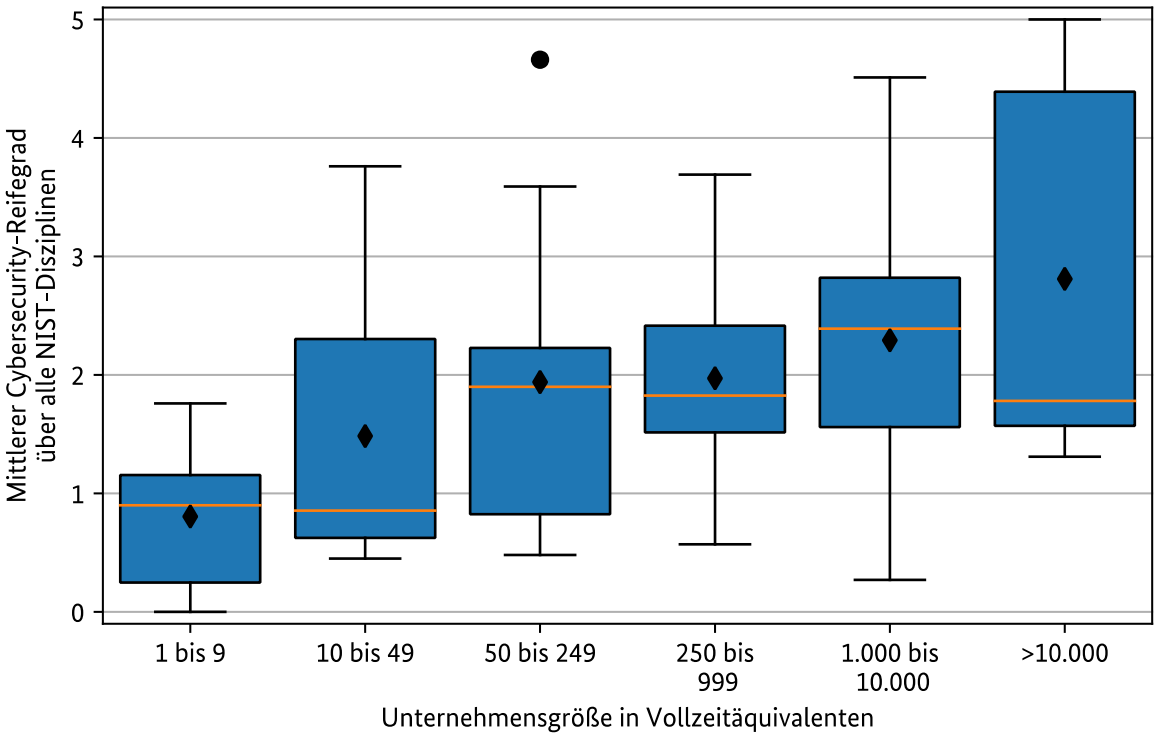


Abbildung 8: Reifegrad nach Unternehmensgröße in Mitarbeiteranzahl

Demnach liegt der Reifegrad kleinerer Unternehmen unter dem Reifegrad größerer Unternehmen, was darauf hindeutet, dass kleinere Unternehmen bisher weniger in Maßnahmen im Bereich der Cybersecurity investiert haben und daher im Umkehrschluss einen größeren zukünftigen Investitionsbedarf im Vergleich zu den größeren Unternehmen in dieser Untersuchung haben. Überdies ist eine wesentliche Änderung bei der Schwelle von 50 Beschäftigten zu erkennen. Hier übersteigt der Median zum ersten Mal den Wert 1. Ein zweiter bemerkenswerter Unterschied tritt nach Überschreiten der Grenze von 10.000 Beschäftigten auf. Während der Median nicht betroffen ist, erreicht das obere Quantil ein Reifegradniveau von 4,69 im Maximum. Statistisch lässt sich dies durch den Kruskal-Wallis-Test belegen. Im Beispiel kann der folgende Code verwendet werden, um den Kruskal-Wallis-Test [38] durchzuführen, wobei der Rei-fegrad als Antwortvariable und die Unternehmensgröße als Prädiktorvariable verwendet werden. Dabei ergaben sich eine Chi-Quadrat-Teststatistik H = 11,2816 und der dazugehörige p-Wert von 0,04607. Da dieser p-Wert unter dem Signifikanzniveau von 0,05 liegt, gibt es einen statistisch signifikanten Unter-schied zwischen den angegebenen Reifegraden der sechs Unternehmensgrößen.

Im Gegensatz dazu wird bei kleineren Unternehmen das zweite Quantil unterhalb eines Reifegrads von 2,5 gedeckelt. Bei Unternehmen zwischen 10 und 10.000 Beschäftigten gibt es eine große Spanne im oberen Quantil, die den Median um einiges übersteigt. Im Vergleich dazu sind bei Unternehmen zwischen 250 und 10.000 Mitarbeitenden diese Spannen auch in umgekehrter Richtung zu finden. Sehr große und äußerst kleine Unternehmen haben hier deutlich geringere Spannen.

Abbildung 9 stellt das Ergebnis des Reifegrads für alle Unternehmen in den fünf NIST-Kernfunktionen dar. Während der Reifegrad der Kernfunktionen Identify und Respond mit der Unternehmensgröße deutlich steigt, verbessert er sich bei den Kernfunktionen Protect, Detect und Recover nur auf mittlerem Niveau. Geringfügige Unterschiede gibt es bei den NIST-Kernfunktionen Detect und Recover. Bemerkenswert ist, dass im Vergleich zu den übrigen NIST-Reifegraden Recover bei Unternehmen mit weniger als 50 Mitarbeitenden bereits auf einem höheren Niveau liegt.

TABELLE 13: VERGLEICH DER 5 KERN-NIST-REIFEGRADE NACH UNTERNEHMENSGRÖßEN [ANZAHL MITARBEITENDE]

| **Anzahl Mitarbeitende** | **Mittelwerte der Reifegrade** | | | | |
|---|---|---|---|---|---|
| | Identify | Protect | Detect | Respond | Recover |
| 1 bis 9 | 0,7 | 0,8 | 0,7 | 0,3 | 1,0 |
| 10 bis 49 | 1,3 | 1,9 | 1,8 | 1,1 | 2,5 |
| 50 bis 249 | 1,4 | 1,8 | 1,5 | 1,6 | 2,5 |
| 250 bis 999 | 1,9 | 2,1 | 1,6 | 1,5 | 2,3 |
| 1.000 bis 10.000 | 2,4 | 2,4 | 1,8 | 1,9 | 2,6 |
| Mehr als 10.000 | 2,8 | 2,9 | 2,6 | 2,6 | 2,9 |
| Gesamtergebnis | 1,9 | 2,1 | 1,7 | 1,6 | 2,4 |

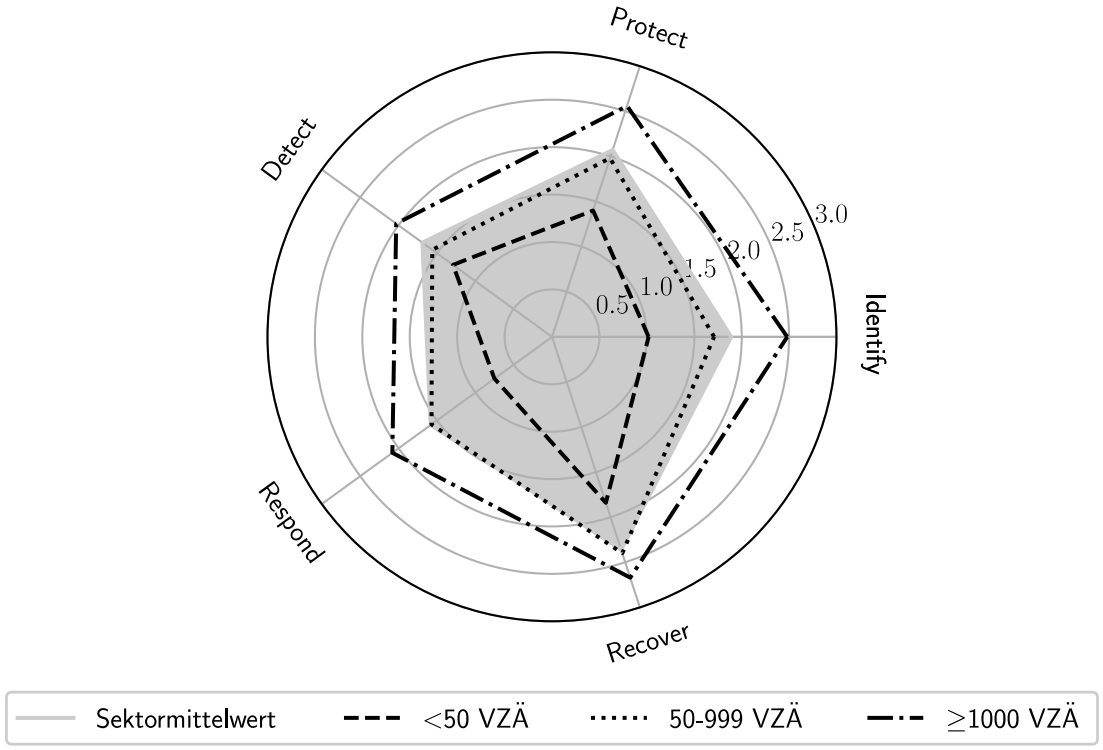


Abbildung 9: Cybersecurity-Reifegrade für unterschiedliche Unternehmensgrößen

Zusammenfassend zeigt das Netzdiagramm in Abbildung 9 aber auch, dass über alle Unternehmensgrößen hinweg, also auch bei den größeren Unternehmen, erheblicher Nachholbedarf bei den Kernfunktionen Respond und Detect existiert.

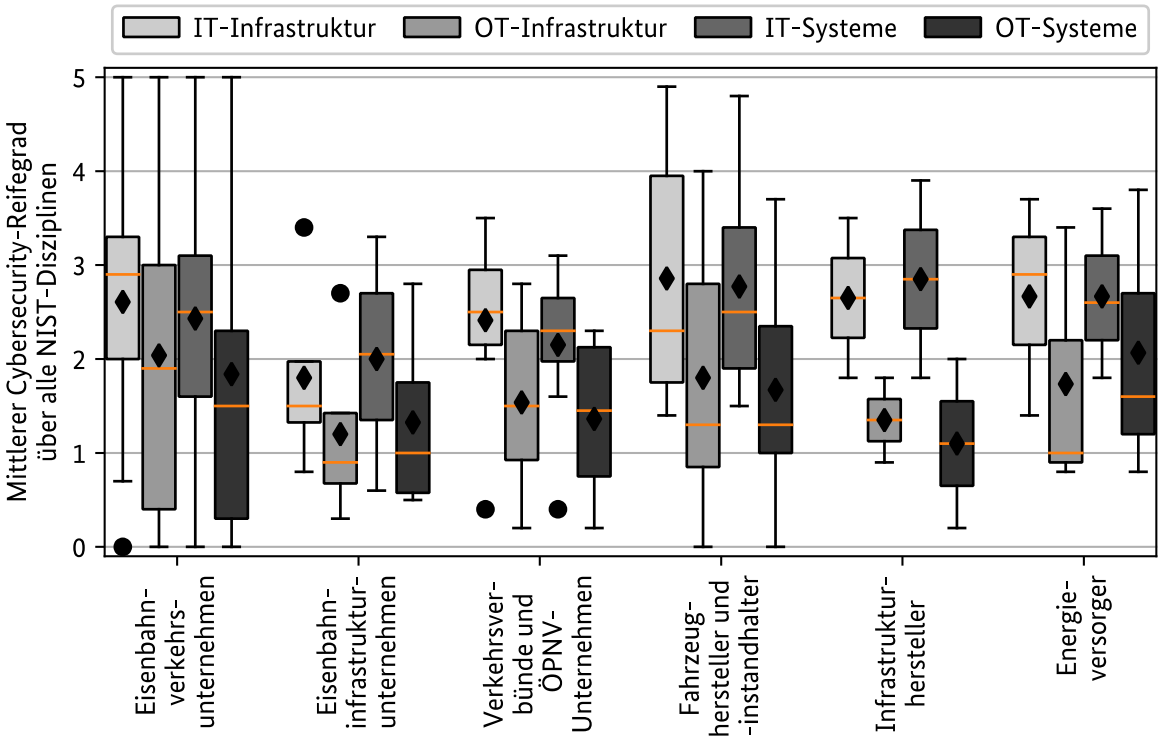


Abbildung 10: Vergleich der Reifegrade IT und OT der untersuchten Untersektoren

### 6.2.4 Vergleich der Reifegrade zwischen IT und OT

Neben den Fragen zum Reifegrad in den jeweiligen NIST-Kernfunktionen wurden, wenn ein Unternehmen Angaben zum Reifegrad zur OT machte, diese eigenständig erhoben und analysiert. Von den 60 Teilnehmenden an der Onlinebefragung machten 38 Unternehmen die weiteren Angaben zum Umsetzungsgrad zur OT-Infrastruktur und zum OT-System. Daraus lässt sich ein Vergleich der jeweiligen durchschnittlichen Reifegrade zwischen der IT-Infrastruktur/-System und der OT Infrastruktur/-System aufstellen (Abbildung 10).

In der Abbildung 10 ist erkennbar, dass die Reifegrade in der OT deutlich schwächer ausgeprägt sind als in der IT. Die Differenz der durchschnittlichen Reifegrade betrug je nach Untersektor zwischen 0,7 und 1 Einheiten.

Weiterhin ist die Differenz der durchschnittlichen Reifegrade zwischen den Untersektoren in der IT deutlich größer als in der OT. Als Grund wird vermutet, dass die Unternehmen sehr wahrscheinlich Cybersecurity-Maßnahmen in der IT gegenüber den Maßnahmen in der OT priorisieren.

## 6.3 Neue Technologien

### 6.3.1 Wissensstand zu neuen Technologien

Generell zeigt sich, dass der Stand des Wissens über die neuen Technologien im Eisenbahnsektor in Abhängigkeit der Technologie variiert. Hier wurden das Wissen über alle zwölf neuen Technologien in allen Untersektoren sowie das kumulierte Wissen über alle neuen Technologien in unterschiedlich großen Unternehmen betrachtet.

Abbildung 11 zeigt die Auswertung der Onlinebefragung und das Ergebnis der Wissensbewertung der einzelnen Technologien.

Zu erkennen ist, dass der Wissensstand in den neuen Technologien 5G, Big Data, Cloud Computing, Cloud Dienste, Glasfaser, Internet der Dinge und Virtualisierung nach eigener Einschätzung der Interviewteilnehmenden am stärksten ausgeprägt ist. Auf der anderen Seite der Selbsteinschätzung stehen mit niedrigem Wissensstand die neuen Technologien Additive Fertigung, Blockchain und drahtlose Sensornetzwerke.

In Abbildung 12 wird über alle Technologien hinweg dargestellt, wie der Wissensstand je nach Unternehmensgröße verteilt ist. Aus der Abbildung lässt sich deutlich erkennen, dass der Wissensstand mit zunehmender Unternehmensgröße steigt. Sehr gut ist auch zu erkennen, dass bei Unternehmen mit mehr als 10.000 Mitarbeitenden der sehr hohe Wissensstand mit 22 % sich deutlich von den anderen Unternehmenskategorien abhebt. Addiert man die als „hoch“ und „sehr hoch“ eingeschätzten Antworten, so ist ein kontinuierlicher Anstieg des Wissensstands von 12 % bei Unternehmen mit <10 Mitarbeitenden hin zu 50 % bei Unternehmen mit >10.000 Mitarbeitenden abzulesen.

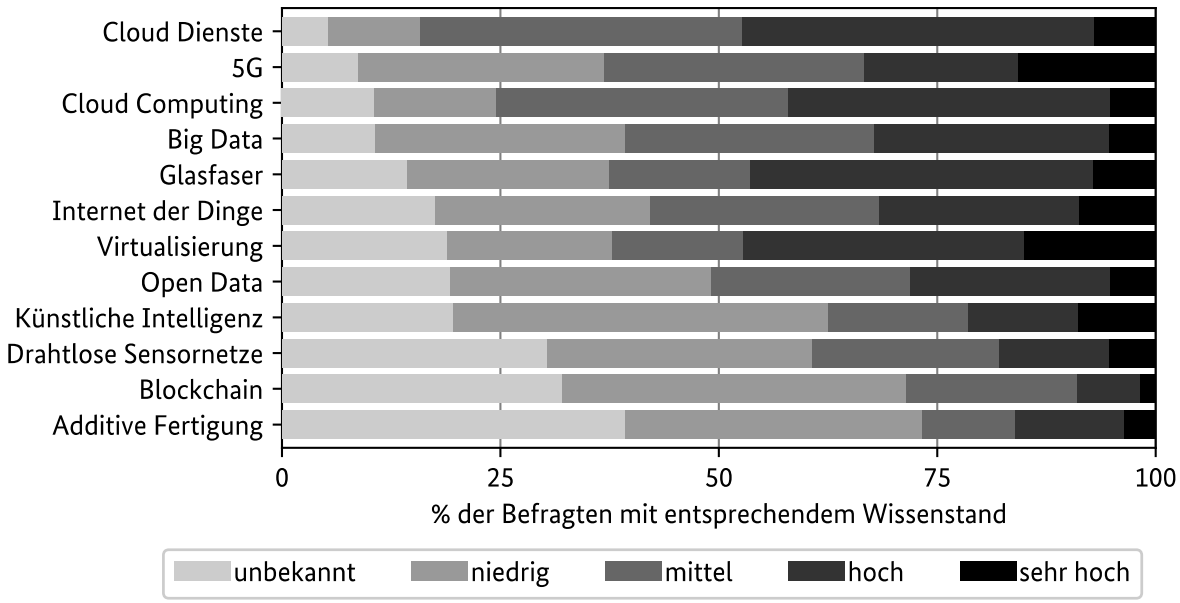


Abbildung 11: Wissensstand zu neuen Technologien

## 6.3.2 Einsatz, Potenziale und zeitlicher Einfluss der neuen Technologien

Das Potenzial der jeweiligen neuen Technologie hinsichtlich des (geplanten) Einsatzes im eigenen Unternehmen wurde kumuliert über alle Unternehmen hinweg bewertet. Dazu zeigt die Abbildung 13 die Häufigkeit, mit der die neuen Technologien in Planung bzw. Pilotierung als auch bereits in der Nutzung sind.

Die neuen Technologien Cloud Dienste, Virtualisierung und Glasfaser sind bereits häufig im Einsatz. Die höchsten Chancen (in Planung und Pilotierung) werden den neuen Technologien 5G, Big Data und Drahtlose Sensornetze eingeräumt.

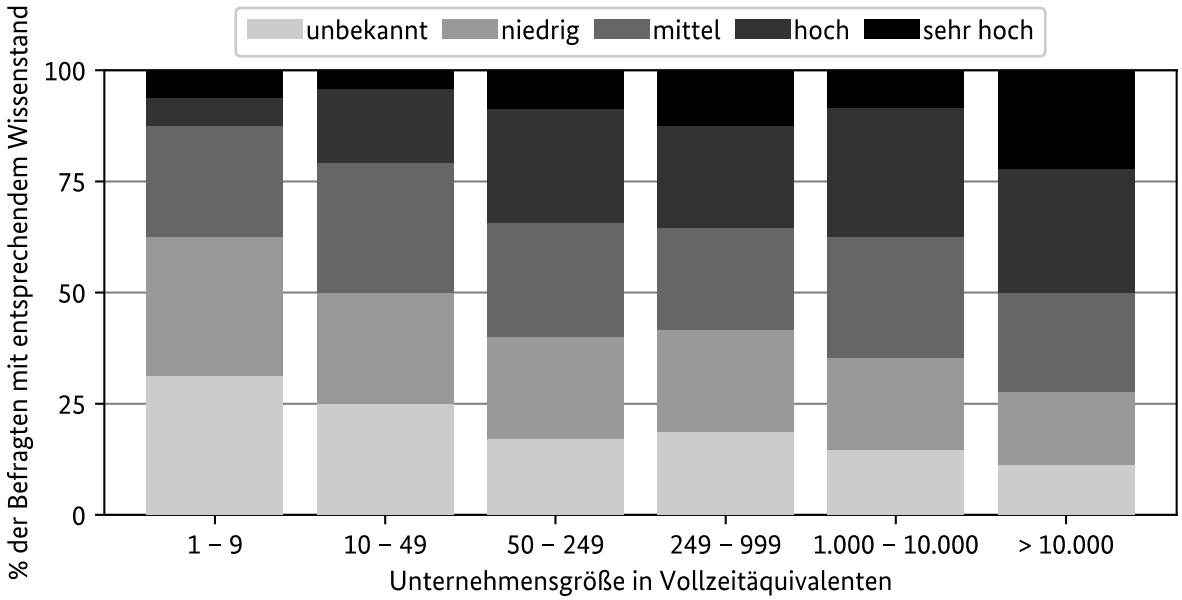


Abbildung 12: Wissensstand über alle Technologien hinweg je nach Unternehmensgröße

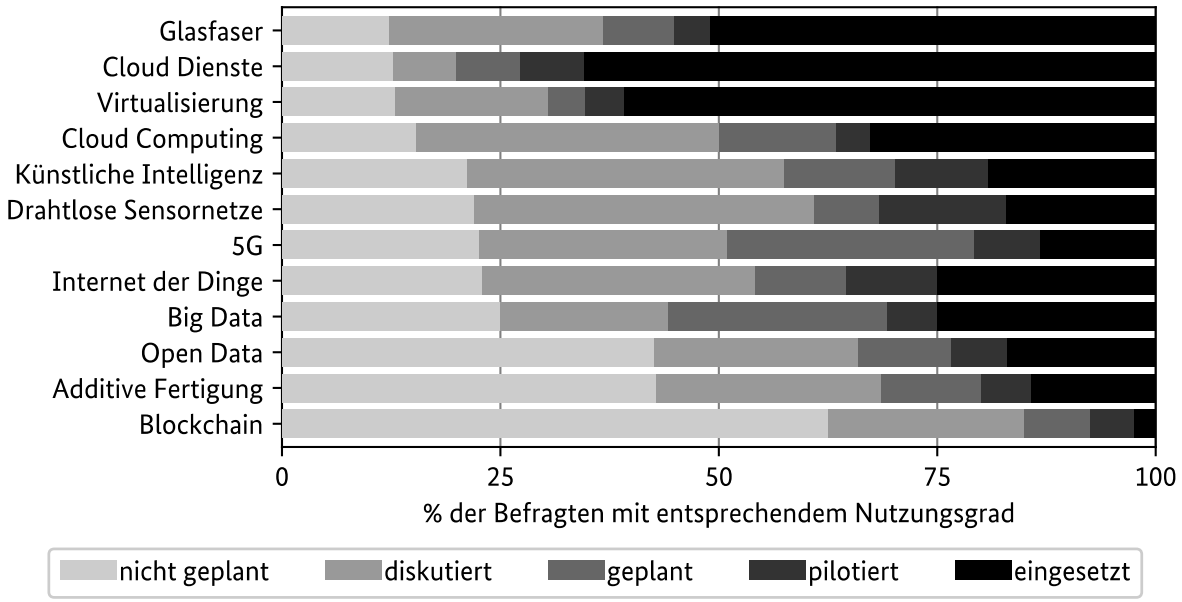


Abbildung 13: (Geplanter) Einsatz der neuen Technologien

Die Analyse der neuen Technologien hinsichtlich des zeitlichen Einflusses zeigt, dass in den nächsten zwei Jahren der größte Einfluss von den Technologien Cloud Dienste und Virtualisierung erwartet wird. Vergleicht man die Ergebnisse zum Wissensstand aus Abbildung 12 mit dem (geplanten) Einsatz der neuen Technologien aus Abbildung 14, so wird erkennbar, dass die neuen Technologien Cloud-Dienste, Glasfaser und Virtualisierung in ihrer relativen Bewertung die höchste Zustimmung erhalten, sich dennoch im Detail der individuellen Bewertung zwischen Nutzung und Wissen unterscheiden.

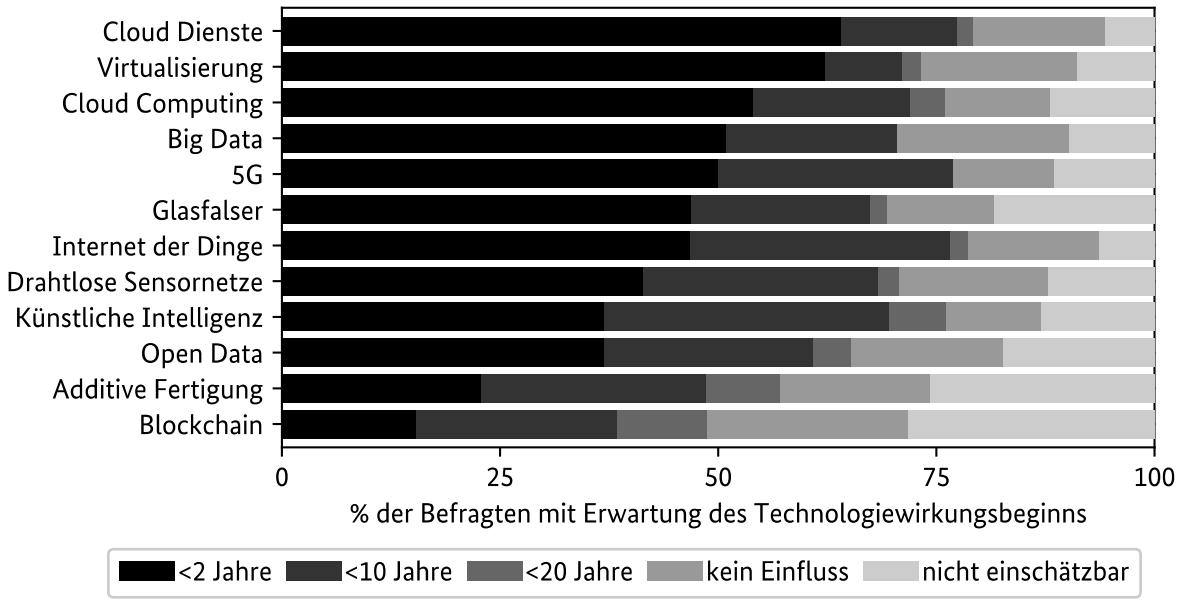


Abbildung 14: Zeitlicher Einfluss der neuen Technologien

### 6.3.3 Veränderungseinfluss und potenzielle Risiken der neuen Technologien

Ein weiterer Untersuchungsgegenstand war der Veränderungseinfluss neuer Technologien auf die zukünftige IT-Landschaft. Die Abbildung 15 zeigt, dass die teilnehmenden Unternehmen den Veränderungseinfluss der vier neuen Technologien Big Data, Cloud Dienste, künstliche Intelligenz und Virtualisierung am höchsten bewerteten. Demgegenüber wird von den neuen Technologien Blockchain, Glasfaser und Open Data kein oder geringer Einfluss auf die Veränderungen gesehen.

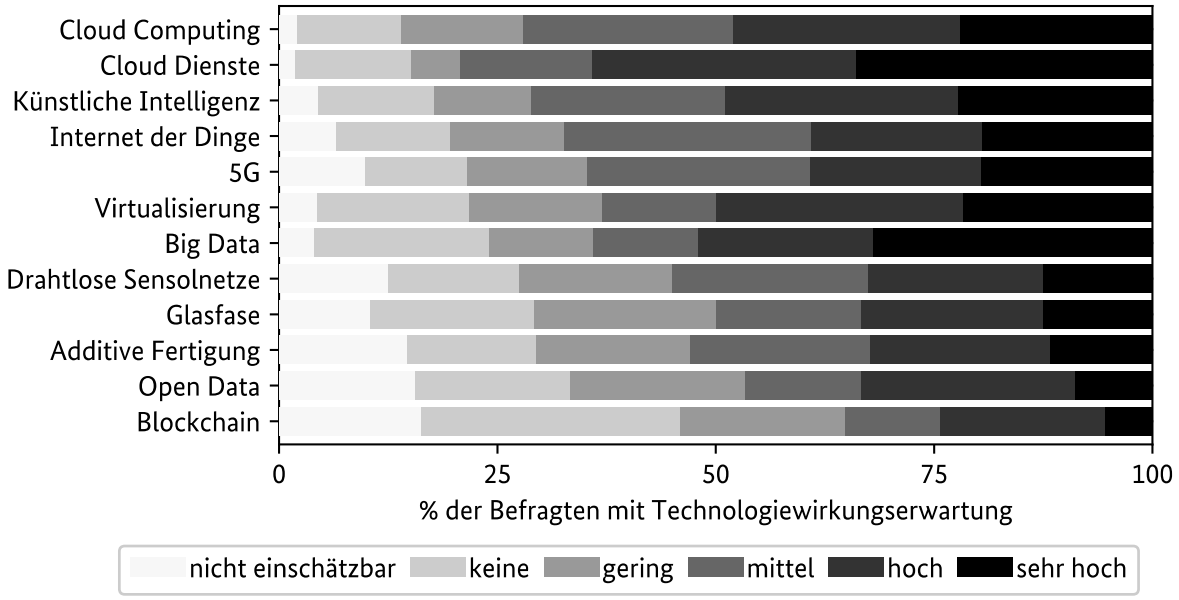


Abbildung 15: Einschätzung des Einflusses der Veränderungen von neuen Technologien

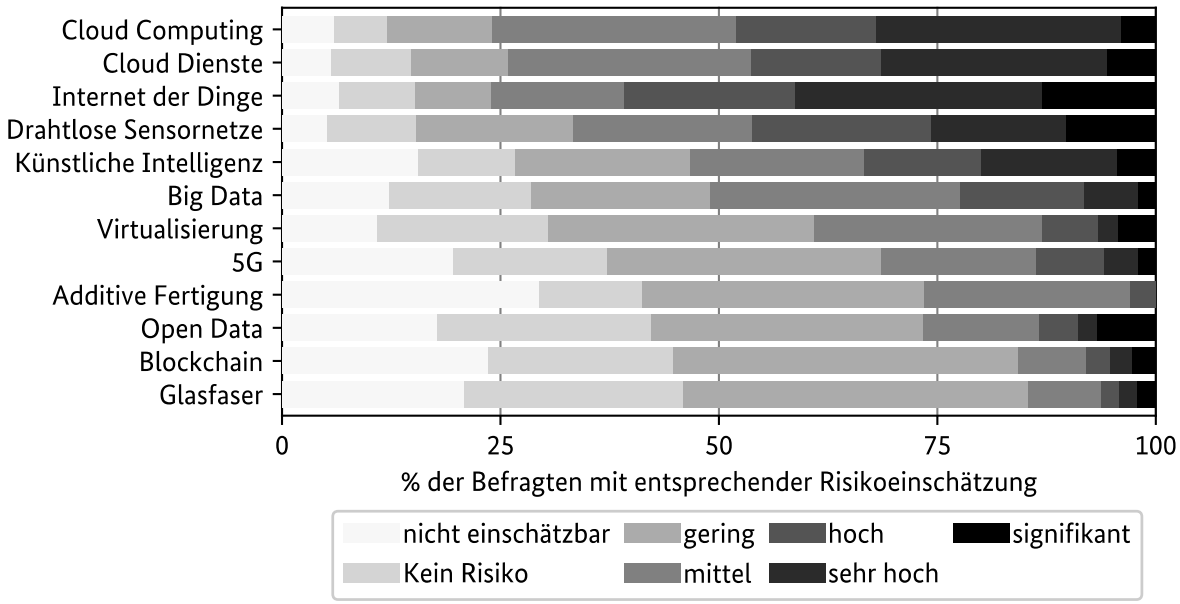


Abbildung 16: Einschätzung des potenziellen Risikos ausgehend zum derzeitigen Risiko

Wird das potenzielle Risiko der Technologien analysiert und dazu die Risikoeinschätzungen durch die Risiken größer als „mittel“ addiert, so ist aus der Darstellung in Abbildung 15 zu erkennen, dass von den Technologien Internet der Dinge, Cloud Dienste und Cloud-Computing die höheren Risiken erwartet werden.

Neue Technologien, von denen aus den Einschätzungen der Teilnehmer „kein Risiko“ oder ein „geringes“ Risiko ausgeht, sind Glasfaser, Blockchain und Open Data.

# 7 Ergebnisse der Interviews

## 7.1 Statistik

Von den 60 Unternehmen der Onlinebefragung hatten sich 24 Unternehmen zur Teilnahme an einem persönlichen Interview bereiterklärt. Davon wurden 12 Unternehmen für die individuellen Interviews ausgewählt. Die Zusammenstellung aller Teilnehmer und der Anteil an Interviewten sind in Tabelle 14 dargestellt. Hierbei wurde auf eine möglichst repräsentative Auswahl der Onlineteilnehmenden geachtet. Unternehmen, die sich für ein Interview bereiterklärt hatten, auf wiederholte Terminanfragen allerdings nicht reagierten, wurden durch ebenfalls geeignete Nachrücker ersetzt.

Je nach Unternehmen dauerten die Interviews zwischen einer und zwei Stunden, wobei jedoch nicht die Frageanzahl, sondern vielmehr der Antwortumfang ausschlaggebend, für die Dauer der Interviews war. Aufgrund des qualitativen Charakters der Interviewergebnisse und ihrer individuellen Art der Durchführung ist eine Auswertung auf der Grundlage der einzelnen Fragen nicht unbedingt sinnvoll. Stattdessen wurde eine Bewertung durchgeführt, um Auffälligkeiten zu klären.

TABELLE 14: ZUSAMMENSETZUNG DER TEILNEHMENDEN FÜR DIE INDIVIDUELLEN INTERVIEWS

| **Untersektoren** | **Stichprobe** | | **Teilnehmende** | | | |
|---|---|---|---|---|---|---|
| | | | **Onlinebefragung*** | | **Interviews** | |
| | # | Anteil | # | Anteil | # | Anteil |
| Eisenbahnverkehrsunternehmen (EVU) | 420 | 59 % | 23 | 38 % | 2 | 17 % |
| Eisenbahninfrastrukturunternehmen (EIU) | 116 | 16 % | 11 | 18 % | 1 | 8 % |
| Verkehrsverbünde und ÖPNV-Unternehmen | 106 | 15 % | 12 | 20 % | 4 | 33 % |
| Fahrzeughersteller und Fahrzeuginstandhalter | 38 | 5 % | 8 | 13 % | 4 | 33 % |
| Infrastrukturhersteller | 27 | 4 % | 2 | 3 % | 0 | 0 % |
| Energieversorger | 1 | 0 % | 3 | 5 % | 0 | 0 % |
| Sonstige | 7 | 1 % | 1 | 2 % | 1 | 8 % |
| Gesamt | 715 | 100 % | 60 | 100 % | 12 | 100 % |

** Die Teilnehmenden wählten in der Onlinebefragung selbst den Sektor aus, dem sie sich zugeordnet sehen.*

## 7.2 Ergebnisse der Interviews zur Cybersecurity

Nachfolgend werden die Ergebnisse der Interviewphase zunächst zusammenfassend und anschließend nach NIST-Funktionen aufgeschlüsselt dargestellt. Als zentrales Thema der Untersuchung wurden dazu auffällige Werte oder Ausreißer aus dem Onlinefragebogen der fünf NIST-Funktionen auf Widersprüche

TABELLE 15: SWOT-ANALYSE DES SEKTORS ZUR CYBERSECURITY

| **Stärken** | **Schwächen** |
|---|---|
| Zuverlässig funktionierende Hardware und physische Strukturen im Bereich der IT und OT<br>Physisch voneinander entkoppelte Kommunikationsmedien<br>Erhöhtes Bewusstsein für Fragen zu aktuellen Entwicklungen der Informations- und Cybersecurity innerhalb der IT-Abteilung<br>Gut eingespielte Organisation und funktionierende Prozesse<br>I. d. R. sehr motivierte und engagierte IT-Fachabteilungen mit Interesse am Thema Cybersecurity | Hohe Abhängigkeit von Lieferfirmen hinsichtlich der angebotenen technischen Standards der zu beschaffenden Hard- und Software (der angebotene ist nicht immer der aktuelle Standard)<br>Geringe Unterstützung durch Behörden und die Politik hinsichtlich der Schaffung von Maßnahmen zur Steigerung der Cybersecurity<br>Mangelndes Bewusstsein des Managements und der Mitarbeitenden für die Cybersecurity<br>Abhängigkeit von herstellenden Unternehmen zur Einrichtung von IT, teilweise auch bei der Wiederherstellung von Sicherungskopien<br>Abstellen von Support und Updates älterer Produkte durch den Hersteller |
| **Chancen** | **Risiken** |
| Nutzung externer Dienstleister für die Übernahme von Cybersecurity-Aufgaben<br>Erhöhung des Bewusstseins für Cybersecurity im Bereich OT<br>Durchgängige Schaffung von Stellen zur Sicherstellung der Funktion „Cybersecurity“ (aktuell häufig nur nebenbei)<br>Anpassung der KRITIS-Regelungen in Richtung Umsetzungsfreundlichkeit und höherem Individualisierungsgrad je Anwenderin bzw. Anwender<br>Unternehmensinterne Richtlinien zur Steigerung der Cybersecurity (z. B. Passwortregeln)<br>Unternehmensinterne Schulungen oder Webinare zum Thema Cybersecurity oder Datenschutz<br>Austauschplattformen innerhalb der Branche zum Thema Cybersecurity<br>Durchgängige Erstellung von Sicherungskopien für IT und OT<br>Offener Umgang und Transparenz zur tatsächlichen Bedrohungslage | Pauschale Vorschriften für verschiedene Bahn-Sektoren und Anwendungsfälle behindern Unternehmen durch mangelnde Individualität, Praktikabilität und Nichtbeachtung der Bedürfnisse<br>Finanzieller Nutzen von Investitionen in die Cybersecurity wird unterschätzt<br>IT-Fachkräftemangel gepaart mit hohen Gehaltsvorstellungen<br>Steigende Gefahr der Anfälligkeit durch die zunehmende Digitalisierung und damit zunehmenden potenziellen Einfallstoren<br>Vergrößerung des technologischen Rückstands durch fehlende Fördermöglichkeiten |

hin untersucht. Daraus ergab sich ein qualitatives Bild über die geführten Interviews, das Hintergrundinformationen zu den Ergebnissen der Onlinebefragung lieferte. Die Ergebnisse wurden als SWOT-Analyse in Tabelle 15 über alle Untersektoren hinweg zusammengefasst. Darin werden aus Sicht der befragten Unternehmen Stärken und Chancen sowie Schwächen und Risiken dargestellt.

Basierend auf den Interviews können zur NIST-Kernfunktion Identify folgende Aussagen getroffen werden:

- Das Management misst der Cybersecurity oft zu wenig Bedeutung bei.
- Die Mitarbeitenden gehen oft zu sorglos mit dem Thema Cybersecurity um.
- Die Rolle des Cybersecurity-Beauftragten ist in Unternehmen häufig unbesetzt oder wird durch den Datenschutzbeauftragten oder die Leiterin/den Leiter der IT übernommen.

In vielen Unternehmen ist die NIST-Kernfunktion Protect im Hinblick auf das Cybersecurity-Bewusstsein dadurch stärker ausgeprägt, da sie Informationssicherheits- oder Datenschutzbeauftragte beschäftigen. Weiterhin sind oft entsprechende Sicherheitssysteme im Einsatz oder die Unternehmen betreiben eigene, entkoppelte Netzwerke, wodurch der Grad der Cybersecurity steigt.

Hinsichtlich der NIST-Kernfunktion Detect wurde festgestellt, dass Unternehmen in unterschiedlichem Maße für das Thema Cybersecurity sensibilisiert sind. So suchen beispielsweise einige Unternehmen mit Systemen aktiv und automatisch nach Anomalien in Logdateien ihrer Systeme, während andere lediglich nach öffentlich bekannten Vorfällen recherchieren und prüfen, ob ihre Systeme davon betroffen sind.

Laut der Onlinebefragung hat die NIST-Kernfunktion Respond den niedrigsten Reifegrad im Eisenbahnsektor. Die meisten Interviews identifizierten hierfür die folgenden Gründe:

- Der Cybersecurity wird in den Unternehmen ein geringer Stellenwert zugeschrieben.
- Es mangelt an Verantwortlichkeiten für das Thema Cybersecurity.
- Es fehlt an Standards zur Arbeit in diesem Themenfeld.
- Es mangelt an Erfahrung im Umgang mit den entsprechenden Prozessen zur Funktion Respond.

Zur Einordnung des insgesamt niedrigen Reifegrads der NIST-Kernfunktion Recover nannten die Interviews verschiedene Gründe:

- Existierende Sicherungsysteme sind veraltet.
- Es liegen hinderliche Vorgaben der Hersteller oder Regulierungsbehörden zur Wiederherstellung von Sicherungskopien oder Ursprungskonfigurationen vor.

Hinsichtlich der offenen Frage zu Eindrücken, aber auch Wünschen und Anregungen an die Politik lassen sich die Antworten in drei Kategorien einordnen. Diese sind Bewusstsein für Cybersecurity, KRITIS und Regularien sowie Förderungen. Eine Aufstellung der Antworten je Kategorie ist in Tabelle 16 gegeben.

## 7.3 Ergebnisse der Interviews zu neuen Technologien

Die Fragen der Interviews hinsichtlich der neuen Technologien können in zwei Hauptrichtungen unterteilt werden:

- Ermittlung der Gründe, weshalb neue Technologien nicht eingesetzt werden
- Verständnis des Umfangs des potenziellen Einsatzes bestimmter neuer Technologien.

Aufgrund des Umfangs der Stichprobe ist die Ergebnisvielfalt hinsichtlich der neuen Technologien eingeschränkt und wurde zusätzlich durch die Vorauswahl reduziert. Der Umfang neuer Technologien, zu dem

TABELLE 16: WÜNSCHE UND ANREGUNGEN AN DIE POLITIK

| |
|---|
| **Bewusstsein für Cybersecurity** |
| Transparenter Umgang mit Bedrohungen, um Cybersecurity in den Alltag zu rücken |
| Informations- und Schulungsmaterial zur aktuellen Situation, zu Problemen und Lösungen |
| Bildungskonzept der schulischen und beruflichen Ausbildung muss hin zu IT und Sicherheit ausgebaut werden |
| Verständnis der Unternehmen für Regularien wird durch sich widersprechende Vorgaben (BSI-Grundschutz vs. Arbeitsschutzrecht vs. DSGVO) gebremst |
| Einrichtung einer Austauschplattform innerhalb der Bahnbranche |
| **KRITIS und Regularien** |
| KRITIS zwingt Unternehmen dazu, Dinge zu tun, die manchmal unzweckmäßig sind |
| BSI und BNetzA müssen erkennen, was für die Unternehmen wirklich relevant ist |
| Für kleine Unternehmen sind die Regeln oft schwer umsetzbar |
| Unklarheit, was KRITIS mit anstehenden Regelungen von den Unternehmen im Detail erreichen will |
| Gleichsetzung des Transportsektors mit anderen Branchen, wie Energie oder Wasserwirtschaft, ist nicht immer zielführend |
| Strengere und belastbare Regularien würden helfen, das Management für Investitionen in neue Maßnahmen zu motivieren |
| Vorgaben und Regelungen aus IT-Sicherheitsgesetz und BSI-Gesetz sind teilweise sehr allgemein verfasst; es fehlt oft eine Kommentierung und Handlungsempfehlung durch das BSI, damit das abstrakte Level der Vorgaben und Regelungen hinsichtlich Umsetzung präzisiert wird |
| Regulatorische Vorgaben sind zu starr, zu veraltet oder zu pauschal |
| Regularien auf nationaler und internationaler Ebene sind nicht immer deckungsgleich |
| **Förderungen** |
| Förderung der Lieferfirmen zur Bereitstellung moderner Lösungen |
| Anpassungen regulatorischer Vorgaben, damit Unternehmen marktgängige Lösungen anbieten können |
| Förderrichtlinien sind anzupassen |
| Förderprogramme zur Einführung von Cybersecurity-Maßnahmen würden begrüßt |

die interviewten Unternehmen in der Onlinebefragung Auffälligkeiten zeigten, ist dadurch ebenfalls begrenzt. Dennoch kann für die Branche ein breiter Überblick zu den Technologien Additive Fertigung, Big Data, Blockchain, Cloud Computing, Cloud Dienste, Glasfaser, Internet der Dinge, KI, Open Data und Virtualisierung gegeben werden. Zu jeder dieser neuen Technologien wurden jeweils ein bis drei Unternehmen befragt. Zu den Technologien 5G und Drahtlose Sensornetze wurde innerhalb der Teilnehmeraus-

wahl kein Interviewteilnehmer ermittelt. Jedoch gab es auch ein Unternehmen, das in der Onlinebefragung antwortete, dass keine neuen Technologien eingesetzt werden. Auch dieses Unternehmen wurde befragt, um die Gründe hierfür zu erfahren.

Übergeordnet wurde festgestellt, dass unabhängig von der Technologie oder dem Untersektor ähnliche Antworten gegeben wurden, weshalb die Ergebnisse der Interviews als allgemeingültig angenommen werden können. Tabelle 17 zeigt die Zusammenfassung der Antworten über alle Interviews zu verschiedenen Fragen hinsichtlich des Einsatzes neuer Technologien.

Tabelle 18 zeigt die Zusammenfassung über alle neuen Technologien und geführten Interviews in Form einer vereinfachten SWOT-Analyse. Hierbei zeigen die Stärken und Chancen neben allgemeinen Eigenschaften auch (neue) Einsatzfelder auf. Hingegen beziehen sich die Schwächen und Risiken auf die Eigenschaften der Technologien im Einsatz.

TABELLE 17: ZUSAMMENFASSUNG ZUM STAND DES EINSATZES NEUER TECHNOLOGIEN

| **Fokus der Frage** | **Antworten** |
|---|---|
| Gründe, weshalb neue Technologien nicht genutzt werden | Der Eisenbahnsektor ist ein sehr konservativer Sektor, der zuverlässige und sichere (geschlossene Netze) Technologie verwendet<br>Glasfasertechnik gilt nicht als neue Technologie<br>IoT-Forschungsprojekte bisher nur im Anfangsstadium gestartet |
| Stärken und Chancen der neuen Technologien | Erschließung von Umsatzpotenzialen durch neue Geschäftsmodelle<br>Schaffung von Geschäftslösungen, die jetzt technisch machbar sind<br>Verbesserung der Prozesseffizienz zur Erhöhung der Prozessgeschwindigkeit oder -qualität oder zur Erzielung von Kosteneinsparungen<br>Neue Dienstleistungen für die Kundinnen und Kunden anbieten<br>Erleichterung und Beschleunigung der täglichen Arbeit der Mitarbeitenden |
| Große zu überwindende Hindernisse | Mitarbeitende und Management von den Vorteilen der neuen Technologien überzeugen<br>Überzeugung des Managements vom finanziellen Nutzen einer Investition<br>Grundlegende und schließlich vertiefte Kenntnisse über neue Technologien erwerben, um Anwendungsfälle zu erstellen<br>Die richtigen Mitarbeiterinnen und Mitarbeiter finden, um Proof of Concepts zu realisieren und neue Lösungen zu implementieren |
| Auswirkungen auf die Arbeit der Mitarbeitenden und wie Veränderungen unterstützt werden können | Es herrscht Abwehrhaltung gegenüber neuen Technologien, da der Zweck der Technologie oft unklar oder hiermit ein Lernaufwand verbunden ist (betrifft insb. ältere Mitarbeitende)<br>Leuchtturmprojekte helfen, Akzeptanz zu schaffen<br>Einbindung von Schlüsselpersonen im Unternehmen und frühzeitige Schulung der Mitarbeitenden |

TABELLE 18: SWOT-ANALYSE DER NEUEN TECHNOLOGIEN

| Neue Technologien | Stärken & Chancen | Schwächen & Risiken |
|---|---|---|
| 5G | Keine Informationen, da kein entsprechendes Unternehmen für den Interviewteil zur Verfügung stand | |
| Additive Fertigung | Herstellung von (Ersatz-)Teilen in kleinen Stückzahlen, z. B. für ältere Züge<br>Kaum Cybersecurity-Risiken | Kosten-Nutzen-Analyse oft schwierig<br>Qualität nicht entsprechend den Serienteilen |
| Big Data | Ermöglicht neue Geschäftsmodelle oder Services<br>Verbesserung der Qualität oder zusätzliche Funktionen des bestehenden Serviceangebots | Datengewinnung stellt oft eine Herausforderung dar, da notwendige Systeme und Schnittstellen fehlen<br>Die Datenhoheit und der Datenschutz schränken häufig die Nutzungsmöglichkeiten ein |
| Blockchain | Erhöhtes Vertrauen in Ergebnisse durch garantierte Rückverfolgbarkeit | Noch kein breiter Anwendungsbereich<br>Mangelnde Akzeptanz und mangelndes Verständnis<br>Schlechte Umweltbilanz<br>Aufwändige Infrastruktur notwendig |
| Cloud Dienste & Computing | Schneller Austausch von Daten<br>Hohe Verfügbarkeit und ortsunabhängiger Zugriff<br>Nutzung von Versionierung<br>Reduzierung des Postverkehrs<br>Steigerung der Kundennähe<br>Hohe Flexibilität hinsichtlich Rechenkapazität und Speicherplatz<br>Geringerer Aufwand für Outsourcing durch spezialisierte Dienstleister | Mangelndes Vertrauen in Datensicherheit<br>Abhängigkeit von Dritten<br>Implementierungskosten und Überwindung von Akzeptanzhürden |
| Glasfaser | Hoher Datendurchsatz | Keine |
| Internet der Dinge | Erfassung und Nutzung von Daten<br>Voraussetzung für eine vorausschauende Instandhaltung | Aufgrund der vielen Schnittstellen bietet es Einfallstore für Cyberangriffe<br>Theoretische Lösungsvielfalt durch teils hohe Kosten eingeschränkt |
| KI & Machine Learning | Automatisierte Bild- und Datenauswertung von Schäden an Bauteilen<br>Auswertung großer Datenmengen<br>Hohe Ergebnisqualität der Technologie spart Zeit und Geld | Eingeschränktes Vertrauen, da Ergebnishergang unbekannt |

| | | |
|---|---|---|
| Open Data | Ermöglicht neue Geschäftsmodelle oder Services<br>Verbesserung der Qualität oder zusätzliche Funktionen des bestehenden Serviceangebots | Datengewinnung stellt oft eine Herausforderung dar, da notwendige Systeme und Schnittstellen fehlen<br>Die Datenhoheit und der Datenschutz schränken häufig die Nutzungsmöglichkeiten ein |
| Virtualisierung, SDN, NFV | Reduktion der Infrastrukturkosten<br>Erhöhte Flexibilität<br>Möglichkeit des „digitalen Zwillings“ | Kosten-Nutzen-Analyse oft schwierig<br>Eingeschränktes Wissen über Technologie und dadurch Anwendungsfälle nicht immer klar |
| Drahtlose Sensornetze | Keine Informationen, da kein entsprechendes Unternehmen für den Interviewteil zur Verfügung stand | |

# 8 Diskussion

## 8.1 Cybersecurity

### 8.1.1 Allgemeine Aussagen

Im Abschnitt 5.1 wurde auf das Reifegradmodell eingegangen. In diesem Zusammenhang sind nachfolgend ergänzend qualitative Anmerkungen zum Reifegrad aufgelistet:

- Ein festgestellter Reifegrad $\leq 3$ ist dahin gehend zu deuten, dass ein Hindernis in der Entwicklung der Cybersecurity und damit ein deutliches Verbesserungspotenzial vorliegt.
- Ein festgestellter Reifegrad von 4 ist dahin gehend zu deuten, dass hier eine gewisse Souveränität in der Entwicklung der Cybersecurity vorliegt.
- Ein festgestellter Reifegrad von 5 ist dahin gehend zu deuten, dass die Cybersecurity in der Unternehmensstrategie verankert ist.

Die Auswertung der Onlineerhebung zur Cybersecurity im Abschnitt 6.2 hat gezeigt, dass die Mediane der Reifegrade in allen Untersektoren bei etwa 2 liegen. Das bedeutet, dass über alle Untersektoren ein deutliches Verbesserungspotenzial feststellbar ist.

### 8.1.2 Sektorenvergleich

Gemäß des Vergleichs der Untersektoren im Abschnitt 6.2 zum Thema Cybersecurity ist der Eisenbahnsektor in drei Gruppen zu unterscheiden. Die EIU weisen den geringsten Reifegrad an Cybersecurity auf, wohingegen die Verkehrsverbünde den höchsten Reifegrad aufzeigten. Die restlichen Untersektoren erreichen im Median einen Wert von etwa 2 – also eine teilweise Umsetzung.

Das nicht hinreichende Abschneiden der EIU ist durch mehrere Faktoren zu erklären. Viele EIU sind sehr klein, haben nur eine zu betreibende Bahnstrecke und teilweise sehr alte (>50 Jahre) Infrastruktur. Insbesondere Museumseisenbahnen verfügen oft nur über mechanische oder elektromechanische Stellwerkstechnik. Moderne elektronische und digitale Stellwerke sind hier nicht nur ein Fremdwort, sondern auch explizit nicht gewünscht, da sie die historischen Ensembles stören würden. Manche dieser Unternehmen verfügen zudem nicht über einen Anschluss an das übergreifende Netz der Deutschen Bahn, sodass hier auch kein Bedarf für eine technische Kommunikation besteht. In diesen Fällen beschränken sich die angreifbaren Systeme auf die Website und den E-Mail-Posteingang des Unternehmens, deren Absicherung kostengünstig durch Dienstleister garantiert werden kann.

Weiterhin verwenden auch größere EIU in großen Bereichen Technologien, die abgekündigt sind oder einem Umbauverbot unterliegen. Der Einsatz moderner Security-Konzepte ist daher nicht möglich, ohne die Zulassung zu verlieren. Dies ergibt sich auch aus den Antworten der SWOT-Analyse. Hier ist im Rahmen der Digitalisierung und dem Einsatz von Custom-off-the-Shelf-Komponenten eine Besserung zu erwarten, da Lösungen einfacher und ohne Zurückgreifen auf Spezialhersteller zwischen den Unternehmen transferiert werden können.

Der hohe Reifegrad der Verkehrsverbünde lässt sich auch dadurch erklären, dass hier generell eher Office- und Verwaltungssysteme im Einsatz sind. Die Anwendung moderner Security-Standards ist daher hier leichter möglich.

Bei den restlichen Unternehmen fällt auf, dass die EVU eine sehr große Varianz aufweisen. Dies ist mit der hohen Diversität in der Größe zu erklären. Von Museumsbahnen oder Unternehmen mit nur einer geleasten Lok bis zu großen EVU mit vielen Triebfahrzeugen ist alles dabei. Bei den Fahrzeugherstellern ist der Überhang der beiden oberen Quantile damit zu erklären, dass gerade die größeren Hersteller hier überdurchschnittlich gut aufgestellt sind.

Insgesamt kann festgestellt werden, dass der Sektor in weiten Teilen gerade in der Transitionsphase der Einführung geeigneter Cybersecurity-Lösungen ist. Im Median ist dieses Ziel teilweise erreicht.

### 8.1.3 Unternehmensgröße

Die Vermutung, dass größere Unternehmen generell besser in Bezug auf die fünf Kernfunktionen des NIST-CSF-Modells aufgestellt sind, wurde durch die Ergebnisse bestätigt. Insbesondere bei sehr großen Unternehmen (> 10.000 Mitarbeitende) ergibt sich ein prägnanteres Bild im Zusammenhang mit den fünf Kernfunktionen des NIST-CSF-Modells, während Unternehmen mit weniger als 10 Mitarbeitenden dagegen schlecht abschneiden.

Dies liegt bei letzterer Gruppe tendenziell daran, dass nicht genug Personal vorhanden ist, um einen dedizierten Security-Verantwortlichen zu benennen und diese Rolle – wenn überhaupt – von der Geschäftsführung mit ausgefüllt wird. Bei etwas größeren Unternehmen nimmt diese Aufgabe oft ein IT-Leiter oder eine beauftragte Person für Datenschutz wahr. Ferner wird ein Fehlen konkreter Standards bemängelt, was gerade für kleinere Unternehmen problematisch ist, da aus den Regelwerken erst umständlich konkrete Handlungsanweisungen abgeleitet werden müssen.

## 8.2 Neue Technologien

### 8.2.1 Wissensstand und Einsatz

Bezüglich des Wissensstands lassen sich mehrere Technologien identifizieren, über die kaum hinreichendes Wissen besteht. Für Additive Fertigung, Blockchain, KI & Machine Learning und Drahtlose Sensornetze erreichen nicht mal ein Viertel der Befragten einen hohen oder sehr hohen Wissensstand. Insbesondere bei der Blockchain, fällt auf, dass nur wenige Unternehmen einen hohen Wissensstand und nur ein Unternehmen einen sehr hohen Wissensstand erreichen. Dies entspricht nicht der politischen Wahrnehmung dieser Technologie und der medialen Aufmerksamkeit, die diese erhält. Vergleichsweise viel Wissen besteht hingegen zu Cloud Computing, Cloud Dienste, Glasfaser und Virtualisierung, SDN und NFV. Aber selbst in diesen Technologien verfügt weniger als die Hälfte der Teilnehmenden über einen hohen oder sehr hohen Wissensstand. Damit kann der generelle Eindruck gewonnen werden, dass die untersuchten Sektoren nur eingeschränkt innovationsaffin sind.

Beim Einsatz der Technologien ergibt sich teilweise ein unterschiedliches Bild. Gleich ist die beschränkte Affinität zur Blockchain, für die über die Hälfte der Unternehmen keinen Einsatz plant und weniger als ein Viertel über eine konkrete Planung verfügt oder sich bereits in Pilotierung oder im Einsatz befindet. Weitere Technologien, die sich zu weniger als 25 % im Einsatz oder der Pilotierung befinden, sind 5G, Additive Fertigung und Open Data. Im Gegenzug befinden sich über die Hälfte der Unternehmen schon in der Einsatzphase von Cloud Dienste, Glasfaser und Virtualisierung, SDN und NFV. Keine Technologie überschreitet, bezogen auf den Einsatz, eine Schwelle von drei Vierteln der befragten Unternehmen. Es gibt also keine Technologie, die im gesamten Sektor bereits im Einsatz ist.

Es ist auffällig, dass bei Cloud Dienste und Virtualisierung der Anteil von Unternehmen mit hohem und sehr hohem Wissensstand deutlich niedriger ist als der Anteil der Unternehmen, die diese Technologien einsetzen. Daraus lässt sich schließen, dass die Unternehmen diese Technologien zwar nutzen, aber nur bedingt verstanden haben. Die Technologien erlauben einen hohen Gewinn an Flexibilität und erschließen viele Funktionalitäten durch die Verlagerungen vieler Aufgaben an externe Dienstleister. Das mangelnde Wissen stellt ein Risiko dar, den Effekt der Technologien, insbesondere auch aus Security-Perspektive, nicht abschließend bewerten zu können und daher unnötige Risiken einzugehen.

### 8.2.2 Zeitlicher Einfluss und Veränderungspotenzial

Mehrere Unternehmen sehen über alle Technologien hinweg keinen Einfluss oder nur langfristigen Einfluss auf das Unternehmen oder trauen sich keine Prognose zu. Erneut glaubt weniger als die Mehrheit der Unternehmen an einen Einfluss der Blockchain und die Mehrheit dieser sieht das Potenzial erst auf einer längeren Zeitschiene. Neben der Blockchain erreicht auch Additive Fertigung keine 50 % bezüglich eines kurz- oder mittelfristigen Einsatzes. Kurzfristig relevant sind vordergründig die schon eingesetzten Technologien Cloud Dienste, Glasfaser und Virtualisierung, SDN und NFV. Weiterhin überschreitet auch Cloud Computing die 50 %-Marke im kurzfristigen Einsatz. Alle weiteren Technologien erreichen mittelfristig über 50 % Einsatzquote.

Diese Ergebnisse lassen sich weitgehend auf die Erwartung des Einflusses der Veränderungen übertragen. Erneut wird der Einfluss der Blockchain von sehr wenigen Teilnehmenden als hoch oder sehr hoch eingestuft. Von den Unternehmen, die geantwortet haben, haben über die Hälfte für Big Data, Cloud Dienste, KI & Machine Learning und Virtualisierung, SDN und NFV einen hohen oder sehr hohen Einfluss prognostiziert. Den mittleren Einfluss eingerechnet, überschreiten Cloud Dienste als einzige Technologie drei Viertel der Antworten. Ihr jetziger und zukünftiger Einfluss auf die anwendenden Unternehmen ist also am größten.

### 8.2.3 Risikoabschätzung

Bei der Einschätzung der Veränderung des Cybersecurity-Risikos ist festzustellen, dass es lediglich eine Technologie gibt, von der die Mehrheit einen Sicherheitsgewinn erwartet: Glasfaser. Dies lässt sich daraus erklären, dass vor allem bei der Kommunikation über Glasfasern ein Abgriff technisch schwieriger wird, da z. B. nicht jeder Laptop mit einem geeigneten Netzwerkadapter ausgerüstet ist. Bei der Blockchain geht zumindest die Hälfte der Befragten von einer Reduzierung des Risikos aus. Die Risikominderungsseite überwog die Risikomehrungsseite bei 5G, Additive Fertigung, Open Data und Virtualisierung, SDN und NFV.

Dagegen sieht die Mehrheit der Befragten eine Steigerung des Sicherheitsrisikos durch das Internet der Dinge, Cloud Computing, Cloud Dienste und Drahtlose Sensornetze. Die Risikomehrungsseite überwiegt zudem bei Big Data.

Interessant ist hier in Rückbeziehung zum Wissensstand und Einsatzgrad nochmals Virtualisierung und Cloud Dienste zu betrachten. Viele Unternehmen setzen bei geringem Wissensstand Cloud Dienste ein, obwohl sie darin ein Risiko sehen. Hierzu ergeben sich zwei mögliche Lesarten: Das Risiko wird bewusst in Kauf genommen oder die Unternehmen vertrauen aufgrund des fehlenden Wissens nicht in die eigene Risikoabschätzung. Bei Virtualisierung, SDN und NFV stellt sich dagegen die Frage, ob die Erwartung der Unternehmen, durch den Einsatz dieser Technologien die Sicherheit steigern zu können, aufgrund des fehlenden Wissens in der Realität berechtigt ist.

### 8.2.4 Limitationen und zukünftige Forschung

Eine große Herausforderung bei der Erstellung der Studie war die teilweise niedrige Rücklaufquote. Diese konnte trotz der gezielten Bewerbung (z. B. durch den Verband Deutscher Verkehrsunternehmen und das Netzwerk Europäischer Eisenbahnen) nicht über den erreichten Stand hinaus gesteigert werden. Für zukünftige Studien muss über weitere Incentives oder ggf. eine Verpflichtung der Unternehmen nachgedacht werden.

Weiterhin sollte bei einer zukünftigen Forschung die Relevanz der Unternehmen geprüft werden. Dazu muss ein Kriterium geschaffen werden, ob Cybersecurity für ein Unternehmen betriebliche Relevanz hat oder nicht. So könnten Unternehmen mit keiner oder geringer Cybersecurity-Relevanz, z. B. Museumsbahnen, aussortiert und Verzerrungen in einzelnen Sektoren vermieden werden.

# 9 Handlungsempfehlungen

Aufgrund der Ergebnisse in Kapitel 6 und deren Diskussion in Kapitel 8 lassen sich mehrere Handlungsempfehlungen ableiten. Sie basieren einerseits auf den Reifegraden der Unternehmen, aber andererseits auf den Zuordnungen der SWOT-Analyse, die die Herkunft von besonders hohen und besonders niedrigen Reifegraden erschließbar macht. Damit ergeben sich eine Reihe von Notwendigkeiten, die im Rahmen von Handlungsempfehlungen nachfolgend zusammengefasst sind.

**Standards und Normen**

- Es bedarf Standards zur Cybersecurity wie NIST-CSF für bestimmte Standardanwendungen, die in zahlreichen Unternehmen vorkommen. Ein Beispiel könnten hierbei die EBA-Checklisten sein, wie sie aus der Fahrzeugzulassung bekannt sind. Diese würden es auch mit weniger tiefgehend geschultem Personal erlauben, entsprechende Punkte abzuarbeiten. Hierzu gehören insbesondere die Punkte Identitäts- und Zugriffsverwaltung sowie Informationssicherheitsorganisation.
- Die besten Rahmenbedingungen für das Informationsrisikomanagement werden schnell nutzlos, wenn kein Prozess zur Umsetzung der Richtlinien vorhanden ist.
- Für Vergabeprozesse sollte die Sicherstellung von Support und Updates von Software verpflichtend umgesetzt werden. Bei Abkündigungen müssen rechtzeitig Ersatzmaßnahmen ergriffen werden.
- Für viele der neuen Technologien sollten Branchenstandards und Open-Source-Out-of-the-Box-Lösungen geschaffen werden, die eine einfache Adaptierung ermöglichen. Hierfür sollten im Rahmen von Pilotprojekten die Grundlagen erarbeitet und als Modellanwendung verbreitet werden.
- Einheitliche, offene Schnittstellen und Systeme für die Datengewinnung sollten definiert werden.

**Awareness schaffen und Knowhow aufbauen**

- Das Bewusstsein für Cybersecurity beim Personal und auf den Managementebenen sollte gestärkt werden. Letzteres kann beispielsweise durch eine stärkere Werbung auf Branchenveranstaltungen erreicht werden, während ersteres durch – ggf. auch verpflichtende – regelmäßige Schulungen geleistet werden kann. Hier kann etwa eine Folge von Zertifikatskursen zugrunde gelegt werden, die in einem qualifizierten Abschluss mündet.
- Die Attraktivität der Branche für IT-Fachkräfte und insbesondere Cybersecurity-Spezialisten sollte gesteigert werden. Konzepte hierfür wären beispielsweise sektorspezifische Gasthörervorlesungen an Hochschulen und Universitäten mit Informatikfachbereichen, Zertifikatserlangung an Hochschulen und Universitäten mit Weiterbildungsprogramm in Cybersecurity, Werbung auf Jobbörsen und Sommerschulen. Weiterhin bedarf es einer Anpassung der Gehaltsstandards im Sektor, sodass kompetitive Gehälter angeboten werden können.
- Forschungsfelder um die neuen Technologien im Bahnsektor sollten dauerhaft stärker in die universitäre Forschung und Lehre einfließen. Hierfür sind notwendige Stellen zu schaffen.
- Es sollte ein regelmäßiges Cybersecurity-Monitoring für die Eisenbahnbranche implementiert werden, dass aufbauend auf dieser Studie in festen Abständen die Ergebnisse aktualisiert und auswertet. Dabei ist zu überlegen, wie durch eine Verpflichtung analog zu anderen Meldepflichten, die Teilnahmebereitschaft gesteigert werden kann. Dies könnte z. B. im Rahmen entsprechender Zertifikatsprogramme erfolgen, die nach erfolgreichem Zertifikatsabschluss als fachbezogener Qualitätsnachweis anrechenbar sind.

**Förderung und Aufbau von Institutionen zur Stärkung der Cybersecurity**

- Zur Vermeidung von Mehrfacharbeiten und der Entwicklung von Insellösungen sollte eine offene branchenweite Austauschplattform zum Thema Cybersecurity geschaffen werden. Hier wäre ein Pilotprojekt denkbar, welches die zugehörigen Standards dafür erarbeitet und festlegt.
- Insbesondere für kleinere und mittlere Unternehmen bedarf es einer Einmalförderung, sodass diese Unternehmen zielorientierte Cybersecurity-Maßnahmen einführen können. Eine gezielte sektorbezogene Förderungsmaßnahme sollte über einen befristeten Zeitraum erfolgen, innerhalb dessen das Thema Cybersecurity ausgehend vom Informationsrisikomanagement über ein Richtlinien- und Compliance-Rahmenwerk bis zum Vorfall- und Bedrohungsmanagement umfassend prototypisch bearbeitet wird.
- Es sollte eine Ansprechstelle für Cybersecurity für Unternehmen im Eisenbahnsektor geschaffen werden, die diese beim Verständnis und der Erfüllung der Anforderungen unterstützt.
- Es sollte eine Beratungsstelle für Datenschutz im Big-Data-Kontext für den Sektor Bahn geschaffen werden, sodass die Grenzen des Möglichen einfach für Unternehmen der Branche ausgelotet werden können.
- Projekte zur erklärbaren künstlichen Intelligenz im Bahnsektor sollten stärker gefördert werden, um hier Ängste abzubauen und Kompetenzen aufzubauen. Hierfür sollten im Rahmen von Pilotprojekten die Grundlagen erarbeitet und als Modellanwendung verbreitet werden.

In den nächsten Schritten empfehlen die Autoren eine Wirksamkeitsanalyse dieser Handlungsempfehlungen zu erstellen, in der Nutzen und Kosten gezielt eingeschätzt werden. Gleichermaßen wären die Zuständigkeiten für die Umsetzung der einzelnen Empfehlungen und auch unterschiedliche Umsetzungsstrategien zu erarbeiten und zu vergleichen.

# 10 Fazit

Durch die zunehmende Digitalisierung und den Einsatz neuer Technologien rücken Cybersecurity-Herausforderungen stärker in den Fokus der Eisenbahn und des öffentlichen Verkehrs. Die vorliegende Studie leistet mit einer zweistufigen Befragung und der Auswertung der Ergebnisse einen Beitrag zu einem besseren Verständnis des existierenden Cybersecurity-Bewusstseins und dem Planungs- und Umsetzungsstand von Cybersecurity-Maßnahmen sowie der aktuellen und geplanten Entwicklung des Einsatzes neuer Technologien.

Im Rahmen dieser Studie wurde festgestellt, dass viele Unternehmen der beiden Sektoren noch ein großes Verbesserungspotenzial über alle Cybersecurity-Facetten hinweg haben. Bei den Untersektoren gibt es darüber hinaus noch große Unterschiede. Insbesondere bei den Eisenbahninfrastrukturunternehmen besteht noch Nachholbedarf. Im weiteren Verlauf der Studie wurden Gründe für diesen Zustand eruiert.

Bezüglich der neuen Technologien stellt die Studie fest, dass einzelne Technologien schon stark verbreitet sind, während andere noch in den Kinderschuhen stecken. Speziell bei der Blockchain besteht eine signifikante Schere zwischen der öffentlichen und politischen Wahrnehmung als Zukunftstechnologie und der Einstufung durch den Sektor. Nur ein Unternehmen hat diese Technologie bereits im Einsatz und sehr wenige planen die Anwendung. Bei einigen Technologien wurde festgestellt, dass das Wissen über diese Technologien unterhalb deren Verbreitungsgrad liegt. In einem Fall handelt es sich um eine Technologie, die durch die Befragten stark als risikomehrend eingestuft wurde. Die Gründe für einen Einsatz sowie den Verzicht auf einen solchen wurden dokumentiert und diskutiert.

Auf Grundlage der Befragungsergebnisse wurden mehrere Handlungsempfehlungen abgeleitet, die sich von Brancheninitiativen über Förderempfehlung bis zur zertifizierten universitären Ausbildung erstrecken. Die detaillierte Ausgestaltung dieser Maßnahmen bietet Potenzial für Folgeprojekte. Weiterhin wird der Bedarf einer regelmäßigen Aktualisierung der Studie im Rahmen eines kontinuierlichen Monitorings festgestellt, um das Verbesserungspotenzial zielgenau klassifizieren und die Wirksamkeit initiierter Maßnahmen evaluieren zu können. Durch Umsetzung der Vorschläge wird die Möglichkeit geschaffen, sowohl die Cybersecurity-Awareness und -Resilienz in den Sektoren zu stärken, als auch bei der Modernisierung durch den Einsatz neuer Technologien zu unterstützen.

# Abbildungsverzeichnis

# Tabellenverzeichnis

# Quellenverzeichnis


1. European Network and Information Security Agency (enisa): Railway Cybersecurity: Security Measures in the Railway Transport Sector. Publications Office, Luxembourg (2020), verfügbar unter: https://www.enisa.europa.eu/publications/railway-cybersecurity/@@download/fullReport

2. National Institute of Standards and Technology: Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. National Institute of Standards and Technology, Gaithersburg, MD (2018), verfügbar unter: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

3. Möller, D.P.F.: Cybersecurity in Digital Transformation: Scope and Applications. Springer International Publishing, Cham (2020), ISBN: 978-3-030-60569-8, verfügbar unter: http://link.springer.com/10.1007/978-3-030-60570-4

4. Vollert, A.: AXA Future Risks Report. AXA, Köln (2021), verfügbar unter: https://www.axa.de/site/axa-de/get/documents_E910020996/axade/medien/medien/studien-und-forschung/future-risk-report-2021/112021/future-risks-report-ergebnisbericht.pdf

5. Huang, P.-C.: Risikoorientierte Systematik zur Bewertung von Rückfallebenenkonzepten des Bahnbetriebs, (2020), verfügbar unter: https://leopard.tu-braunschweig.de/receive/dbbs_mods_00068723

6. Möller, D.P.F.: Guide to Computing Fundamentals in Cyber-Physical Systems. Springer International Publishing, Cham (2016), ISBN: 978-3-319-25176-9, verfügbar unter: http://link.springer.com/10.1007/978-3-319-25178-3

7. Proctor, P.: 8 Reasons More CEOs Will Be Fired Over Cybersecurity Incidents, (2019), verfügbar unter: https://www.gartner.com/en/documents/3904673

8. Lange, M.: Deutsche Unternehmen beim Einsatz neuer Technologien zurückhaltend | Bitkom Research, (2022), verfügbar unter: https://www.bitkom-research.de/de/pressemitteilung/deutsche-unternehmen-beim-einsatz-neuer-technologien-zurueckhaltend

9. Möller, D.P.F., Haas, R.E.: Guide to Automotive Connectivity and Cybersecurity: Trends, Technologies, Innovations and Applications. Springer International Publishing, Cham (2019), ISBN: 978-3-319-73511-5, verfügbar unter: http://link.springer.com/10.1007/978-3-319-73512-2

10. Khoram, E., Chen, A., Liu, D., Ying, L., Wang, Q., Yuan, M., Yu, Z.: Nanophotonic media for artificial neural inference. Photon. Res. ISSN: 2327-9125 7, 823 (2019). https://doi.org/10.1364/PRJ.7.000823

11. Paschen, H., Coenen, C., Fleischer, T., Grünwald, R., Oertel, D., Revermann, C.: Nanotechnologie. Springer-Verlag, Berlin/Heidelberg (2004), ISBN: 978-3-540-21068-9, verfügbar unter: http://link.springer.com/10.1007/3-540-35005-5

12. Bolte, M.-A., Meier, G.D., Möller, I.D.P.: Understanding and predicting the electronic and dynamic behavior of nanoscale magnetic random access memory (MRAM) cells using micromagnetic modelling and simulation. In: Proceedings of the 19th European Conference on Modelling and Simulation 2005 (ECMS 2005). S. 574–579 (2005)

13. Moller, D.P.F.: Enhancement in Intelligent Manufacturing through Circular Economy. In: 2020 IEEE International Conference on Electro Information Technology (EIT). S. 087–092. IEEE, Chicago, IL, USA, ISBN: 978-1-72815-317-9 (2020), verfügbar unter: https://ieeexplore.ieee.org/document/9208321/

14. Moller, D.P.F., Jehle, I.A., Hou, W.: Engineering Education in Intelligent Manufacturing. In: 2020 IEEE International Conference on Electro Information Technology (EIT). S. 007–012. IEEE, Chicago, IL, USA, ISBN: 978-1-72815-317-9 (2020), verfügbar unter: https://ieeexplore.ieee.org/document/9208305/

15. Moeller, D.P.F.: Mathematical and Computational Modeling and Simulation. Springer, Heidelberg (2004), ISBN: 978-3-540-40389-0, verfügbar unter: http://link.springer.com/10.1007/978-3-642-18709-4

16. Kumar, V., Rezaei, J., Akberdina, V., Kuzmin, E. hrsg: Digital Transformation in Industry: Trends, Management, Strategies. Springer International Publishing, Cham (2021), ISBN: 978-3-030-73260-8, verfügbar unter: https://link.springer.com/10.1007/978-3-030-73261-5

17. Möller, D.P.F.: Cutting-Edge Digitization Challenges in Vehicle Cyber-Physical Systems and Cybersecurity. In: Akhilesh, K.B. und Möller, D.P.F. (hrsg.) Smart Technologies. S. 17–34. Springer Singapore, Singapore, ISBN: 9789811371387 (2020), verfügbar unter: http://link.springer.com/10.1007/978-981-13-7139-4_2

18. Manyika, J., Dobbs, R., Chui, M., Bughin, J., Bisson, P., Woetzel, J.: The Internet of Things: Mapping the value beyond the hype. McKinsey Global Institute, McKinsey & Company (2015), verfügbar unter: https://www.mckinsey.com/~/media/mckinsey/industries/technology%20media%20and%20telecommunications/high%20tech/our%20insights/the%20internet%20of%20things%20the%20value%20of%20digitizing%20the%20physical%20world/unlocking_the_Potenzial_of_the_internet_of_things_executive_summary.pdf

19. Iffländer, L., Dmitrienko, A., Hagen, C., Jobst, M., Kounev, S.: Hands Off my Database: Ransomware Detection in Databases through Dynamic Analysis of Query Sequences. Universität Würzburg (2019), verfügbar unter: https://arxiv.org/abs/1907.06775

20. Hagen, C., Dmitrienko, A., Iffländer, L., Jobst, M., Kounev, S.: Efficient and Effective Ransomware Detection in Databases. In: 34th Annual Computer Security Applications Conference (ACSAC). ACM (2018), verfügbar unter: https://se2.informatik.uni-wuerzburg.de/publications/download/paper/1797.pdf

21. Aitor Arriola: Safe architecture for Robust distributed Application Integration in roLling stock 2 (Safe4RAIL-2), (2021), verfügbar unter: https://safe4rail.eu/#approach

22. Deutsche Bahn AG: Digitale Schiene Deutschland, (2022), verfügbar unter: https://digitale-schiene-deutschland.de/de

23. Eisenbahn-Bundesamt: Liste der in Deutschland genehmigten öffentlichen Eisenbahnverkehrsunternehmen, (2020), verfügbar unter: https://www.eba.bund.de/SharedDocs/Downloads/DE/Eisenbahnunternehmen/EVU/evu_brd.xlsx?__blob=publicationFile&v=144

24. Eisenbahn-Bundesamt: Liste der in Deutschland genehmigten Betreiber von Eisenbahnstrecken, (2020), verfügbar unter: https://www.eba.bund.de/SharedDocs/Downloads/DE/Eisenbahnunternehmen/EIU/eiu_oeff.xlsx?__blob=publicationFile&v=41

25. Neumann, L., Sander, A.: Trends und Perspektiven der Instandhaltung von Schienenfahrzeugen in Deutschland. Hans-Böckler-Stiftung (2010), verfügbar unter: https://www.boeckler.de/pdf_fof/96088.pdf

26. Dziambor, U., Rehse, S., Niesen, B.: VDV-Statistik 2019. Verband Deutscher Verkehrsunternehmen (VDV), Köln (2022), verfügbar unter: https://www.vdv.de/vdv-statistik-2019.pdfx

27. Autoren der Wikimedia-Projekte: Liste deutscher Tarif- und Verkehrsverbünde – Wikipedia, (2004), verfügbar unter: https://de.wikipedia.org/w/index.php?title=Liste_deutscher_Tarif-_und_Verkehrsverb%C3%BCnde&oldid=228270123

28. Becker, J., Knackstedt, R., Pöppelbuß, J.: Developing Maturity Models for IT Management: A Procedure Model and its Application. Bus. Inf. Syst. Eng. ISSN: 1867-0202 1, 213–222 (2009). https://doi.org/10.1007/s12599-009-0044-5

29. Venkatraman, V.: The Digital Matrix. LifeTree Media Ltd., Los Angeles (2017), ISBN: 978-1-928055-20-4, verfügbar unter: https://wonderwell.press/books/the-digital-matrix/

30. Rogers, D.L.: The Digital Transformation Playbook: Rethink Your Business for the Digital Age. Columbia University Press, Berlin (2016), ISBN: 978-0-231-54165-7, verfügbar unter: https://www.degruyter.com/document/doi/10.7312/roge17544/html

31. Porter, M., Heppelmann, J.: Wie smarte Produkte den Wettbewerb verändern. Harvard-Business-Manager. ISSN: 0945-6570 36.2014, 34–60 (2014)

32. Künzli, B.: SWOT-Analyse. Führung+Organisation. ISSN: 0722-7485 81, 126–129 (2012)

33. Pachmann, A.: Die SWOT-Analyse als Diagnose in Veränderungsprozessen. GRIN Verlag, München (2001), ISBN: 978-3-638-77473-4, verfügbar unter: https://www.grin.com/document/14799

34. Schneider, W.: Praxisleitfaden SWOT-Analyse: Stärken/Schwächen sowie Chancen/Risiken identifizieren und managen. Books on Demand, Norderstedt (2021), ISBN: 978-3-7526-3889-9, verfügbar unter: https://www.bod.de/buchshop/praxisleitfaden-swot-analyse-willy-schneider-9783752638899

35. Adams, W.C.: Conducting Semi-Structured Interviews. In: Newcomer, K.E., Hatry, H.P., und Wholey, J.S. (hrsg.) Handbook of Practical Program Evaluation. S. 492–505. John Wiley & Sons, Inc., Hoboken, NJ, USA, ISBN: 978-1-119-17138-6 (2015), verfügbar unter: https://onlinelibrary.wiley.com/doi/10.1002/9781119171386.ch19

36. Hartung, J.: Statistik: Lehr- und Handbuch der angewandten Statistik. Oldenbourg Wissenschaftsverlag (2009), ISBN: 978-3-486-59028-9, verfügbar unter: https://www.degruyter.com/document/doi/10.1524/9783486710540/html

37. Cohen, J.: Statistical Power Analysis for the Behavioral Sciences. Routledge (2013), ISBN: 978-1-134-74270-7, verfügbar unter: https://www.taylorfrancis.com/books/9781134742707

38. Kruskal, W.H., Wallis, W.A.: Use of ranks in one-criterion variance analysis. Journal of the American statistical Association. ISSN: 0162-1459 47, 583–621 (1952)

# Anhänge

# Anhang 1: Anschreiben

Deutsches Zentrum für
Schienenverkehrsforschung beim
Eisenbahn-Bundesamt

Prof. Dr.-Ing. Corinna Salander
Direktorin

Deutsches Zentrum für Schienenverkehrsforschung
Postfach 12 09 63, 01010 Dresden

«OrganisationNameVoll»
«OrganisationKurzName»
«Anrede»«Titel»«Vorname»«Nachname»
«Abteilung»
«Straße»
«Postfach»
«Postleitzahl»«Ort»
«LAND»

Bearbeitung: Vorname Nachname
Telefon: Telefonnummer
E-Mail: Name@dzsf.bund.de
info@dzsf.bund.de
Internet: www.dzsf.bund.de
Datum: 30.08.2021

**Geschäftszeichen (bitte im Schriftverkehr immer angeben)**

Pr.8440-8fr/011-1255#013

**Befragung im Rahmen eines Forschungsprojekts zur Cybersecurity im Schienenverkehr**

Sehr geehrte Damen und Herren,

das Deutsche Zentrum für Schienenverkehrsforschung beim Eisenbahn-Bundesamt (DZSF) möchte im Rahmen des Forschungsprojektes „Security und geplanter Technologieeinsatz" einen Eindruck über die Cybersecurity Awareness im Schienenverkehrssektor (Eisenbahn und ÖPNV) in Deutschland erhalten (www.dzsf.bund.de/security-studie).

Im Fokus der Studie steht u. a. der Einsatz eines Modells zur Evaluierung des Reifegrads von gewählten Cybersecurity-Maßnahmen. Mittels eines zweitstufigen Vorgehens durch eine breit angelegte Erhebung und anschließende Experteninterviews soll ein Gesamteindruck über den Sektor gewonnen werden. Gleichzeitig soll der Einsatz neuer Technologien (z. B. 5G, Künstliche Intelligenz, Machine Learning etc.) identifiziert werden, um zukünftige Herausforderungen im Kontext Cybersecurity und damit mögliche Angriffsvektoren frühzeitig zu erkennen.

Ihr Unternehmen wurde in Abstimmung mit uns als relevant und repräsentativ für den Eisenbahnsektor ausgewählt. Daher möchten wir Sie bitten, an der Studie mit Ihrem Know-How teilzunehmen und somit einen entscheidenden Beitrag zur Entwicklung der Cybersecurity im Schienenverkehr in Deutschland zu leisten.

Die Erhebung unterliegt den Anforderungen des wissenschaftlichen Arbeitens, sie ist freiwillig und Analysen und Ergebnisse erfolgen ohne Rückschlussmöglichkeiten auf Ihre Person oder Ihr Unternehmen. Am Ende der Befragung haben Sie jedoch die Möglichkeit, Ihre Kontaktdaten zu hinterlassen. Damit erklären Sie sich Einverstanden, für ein Experteninterview zur Verfügung zu ste-

Hausanschrift:
August-Bebel-Str. 10, 01219 Dresden
Tel.-Nr. +49 (351) 47931-0
De-Mail: poststelle@eba-bund.de-mail.de

Überweisungen an Bundeskasse Trier
Deutsche Bundesbank, Filiale Saarbrücken
BLZ 590 000 00 Konto-Nr. 590 010 20
IBAN DE 81 5900 0000 0059 0010 20 BIC: MARKDEF1590
Leitweg-ID: 991-11203-07

hen. Wenn Sie uns durch dieses Interview unterstützen, erhalten Sie nach dessen Auswertung ein Dokument mit Beschreibung des individuellen Reifegrads Ihres Unternehmens inkl. einer Checkliste für Handlungs- und Umsetzungsempfehlungen zur Verbesserung der Cybersecurity. Die unternehmensbezogenen Daten werden nicht an Dritte weitergegeben.

Die Leistungserbringung erfolgt durch die Auftragnehmer, bestehend aus der Industrieanlagen-Betriebsgesellschaft mbH (Generalunternehmer), der 3DSE Management Consultants GmbH, dem Fraunhofer-Institut für Angewandte und Integrierte Sicherheit sowie dem Institut für Bahntechnik GmbH. Diese treten unter folgenden Logos auf:

Die Erhebung wird im Zeitraum von September bis November 2021 stattfinden.
Wir danken Ihnen bereits im Voraus für Ihre Teilnahme an der Marktbefragung sowie die damit verbundene Offenheit und das uns entgegengebrachte Vertrauen.

Mit freundlichen Grüßen

*Unterschrift*

Prof. Dr.-Ing. Corinna Salander
Direktorin
Deutsches Zentrum für Schienenverkehrsforschung beim Eisenbahn-Bundesamt

**So können Sie teilnehmen:**
Scannen Sie den QR-Code oder geben Sie folgende Adresse in Ihren Browser ein. Sie gelangen zur offiziellen Projektseite beim DZSF und können über „Umfrage starten" direkt beginnen. Geben Sie bitte am Anfang Ihren Zugangsschlüssel* ein.

Adresse: www.dzsf.bund.de/security-studie
Zugangsschlüssel*: «Beschreibung»

**Mit Hilfe des Zugangsschlüssels können wir nachvollziehen, welche Unternehmen bereits Rückmeldung gegeben haben, um Dopplungen zu vermeiden und, falls nötig, Unternehmen gezielt an diese Befragung zu erinnern. Diese Codes werden nach der Erhebung gelöscht, sodass die Daten bei der Analyse nicht mehr in Verbindung mit Ihrem Unternehmen gebracht werden können (außer Sie wünschen dies explizit wie oben beschrieben). Bei Fragen können Sie sich gern an cybersecurity@iabg.de wenden.*

Seite 2 von 2

# Anhang 2: Liste als Datenquelle für die Erstellung des Serienbriefs

Die vollständige Liste wurde als Datenquelle für die Erstellung eines Serienbriefs optimiert und umfasst die folgenden Datenfelder:

Datenfelder der Liste der zu befragenden Unternehmen

| Datenfeld | Bedeutung / Inhalte |
|---|---|
| ANREDE | Optional: Wenn Ansprechperson bekannt |
| TITEL | Optional: Wenn Ansprechperson bekannt |
| VORNAME | Optional: Wenn Ansprechperson bekannt |
| NACHNAME | Optional: Wenn Ansprechperson bekannt |
| ORGANISATIONNAMEVOLL | Name des Unternehmens |
| ORGANISATIONKURZNAME | Optionales Unterscheidungsmerkmal: „Eisenbahnverkehrsunternehmen“ oder „Eisenbahninfrastrukturunternehmen“ oder „ÖPNV-Unternehmen“ |
| ABTEILUNG | Wenn Ansprechperson bekannt.<br>In allen anderen Fällen: „Geschäftsleitung“ |
| POSITION | Optional: Wenn Ansprechperson bekannt |
| STRASSE | Adresse des Unternehmens |
| POSTFACH | (leer) |
| POSTLEITZAHL | Adresse des Unternehmens |
| ORT | Adresse des Unternehmens |
| LAND | Land des Unternehmens, wenn nicht in Deutschland ansässig |
| TELEFONNUMMER | (leer) |
| FAXNUMMER | (leer) |
| EMAIL | Optional: Wenn Ansprechperson bekannt |
| BESCHREIBUNG | Das Passwort für den Onlinezugang |
| FREMDESGESCHAEFTSZEICHEN | (leer) |
| Ist-Organisation | „Ja“ |
| VERSANDART | „Papier“ |
| KATEGORIE | „Empfänger/in“ |

# Anhang 3: Onlinefragebogen

Zur Durchführung der Onlinebefragung wurden eine Reihe von Fragen durch die Teilnehmenden beantwortet. Diese Fragen sind mit der Aufteilung in die drei Bereiche „Status quo Cybersecurity“, „neue Technologien“ und „Demographie“ nachfolgend aufgelistet.

Status quo Cybersecurity

1. Welche Maßnahmen zur Cybersecurity verfolgt Ihr Unternehmen?
2. Welchen prozentualen Anteil des Umsatzes Ihres Unternehmens planen Sie im Zeitraum der nächsten 3 Jahre für Cybersecurity aufzuwenden?
3. Welchen Anteil des Personals in Ihrem Unternehmen machen die Vollzeitäquivalente im Bereich Cybersecurity aus?
4. Welche Formen von Cyberangriffen haben sich in den letzten 3 Jahren in Ihrem Unternehmen ereignet?
5. Wie viele der in der vorherigen Frage genannten Cyberangriffe haben sich als Summe in den letzten 3 Jahren in Ihrem Unternehmen ereignet?
6. Wie bewerten Sie das aktuelle Cybersecuritysrisiko unter Berücksichtigung aktueller Technologien in Ihrem Unternehmen?
7. Welche Vorteile sieht Ihr Unternehmen für die Umsetzung von Cybersecurity?
8. Welche Hindernisse stehen dem Ziel der Cybersecurity in Ihrem Unternehmen möglicherweise im Wege?
9. Wie hoch war der durchschnittliche Schaden, der Ihnen in den letzten 3 Jahren durch Cyberangriffe prozentual entstanden ist, gemessen am Umsatz Ihres Unternehmens?
10. Welche Aussage(n) beschreibt die eingesetzte Cybersecuritysstrategie in Ihrem Unternehmen am besten?
11. Ist in Ihrem Unternehmen die Rolle eines Beauftragten für Cybersecurity vorhanden?
12. Hat Ihr Unternehmen eine Strategie, um Angriffen nachhaltig entgegenzuwirken?
13. Sorgt Ihr Unternehmen dafür, dass alle Mitarbeiterinnen und Mitarbeiter im Cybersecuritysbereich geschult werden?
14. Hat Ihr Unternehmen einen Monitoring-Prozess zur Abfrage des Cybersecurity-Bewusstseins (Cybersecurity Awareness) eingeführt?
15. Sind Mitarbeiterinnen und Mitarbeiter in Ihrem Unternehmen in der Lage, Anomalien im Cybersecuritysbereich zu erkennen und zu melden?
16. Hat Ihr Unternehmen etablierte Prozesse für den Umgang bei akuten Cybersecuritys-Angriffen?
17. Besitzt Ihr Unternehmen etablierte Prozesse für die Behebung der Folgen von Cybersecuritys-Angriffen?
18. Führen Sie eine Teilung Ihrer Systeme in die Bereiche Information Technology (IT) and Operational Technology (OT) durch?
19. Haben Sie eine Schwachstellenanalyse der in Ihrem Unternehmen eingesetzten IT- Systeme durchgeführt?
20. Haben Sie Assets und deren potenziellen Schutzbedarf der in Ihrem Unternehmen eingesetzten IT-Systeme identifiziert?
21. Haben Sie eine Bedrohungsanalyse der in Ihrem Unternehmen eingesetzten IT- Systeme durchgeführt?
22. Sind in Ihrem Unternehmen Unternehmensrichtlinien vorhanden, die aufzeigen, wie sich Mitarbeiterinnen und Mitarbeiter bei der Entdeckung eines Sicherheitsvorfalls in Ihren IT-Systemen verhalten und wen sie kontaktieren sollen?
23. Gab es im Zeitraum der letzten 3 Jahre für sämtliche Mitarbeiterinnen und Mitarbeiter Schulungsmaßnahmen zur Verbesserung des Bewusstseins für Cybersecurity (Cybersecurity Awareness) der IT-Systeme?
24. Sind in Ihrem Unternehmen geeignete Indikatoren/Maßnahmen zum frühzeitigen und/oder proaktiven Erkennen von Sicherheitsvorfällen in Ihren IT-Systemen vorhanden?
25. Hat Ihr Unternehmen Maßnahmen für den Umgang mit einem akuten Cybersecuritysangriff definiert?
26. Führen Sie in Ihrem Unternehmen die Logdaten Ihrer IT-Systeme an zentraler Stelle zusammen?
27. Wenden Sie für Ihre IT-Systeme automatisierte Maßnahmen als Reaktion auf Cybersecuritys-Vorfälle an?

28. Haben Sie in Ihrem Unternehmen Maßnahmen definiert, um die Arbeitsfähigkeit eines IT-Systems nach einem Cybersecuritys-Vorfall wieder herstellen zu können?
29. Führen Sie in Ihrem Unternehmen regelmäßige Backups ihrer IT-Systeme durch?
30. Haben Sie Assets und deren potenziellen Schutzbedarf der in Ihrem Unternehmen eingesetzten OT-Systeme identifiziert?
31. Haben Sie eine Schwachstellenanalyse der in Ihrem Unternehmen eingesetzten OT- Systeme durchgeführt?
32. Haben Sie eine Bedrohungsanalyse der in Ihrem Unternehmen eingesetzten OT- Systeme durchgeführt?
33. Sind in Ihrem Unternehmen Unternehmensrichtlinien vorhanden, die aufzeigen, wie sich Mitarbeiterinnen und Mitarbeiter bei der Entdeckung eines Sicherheitsvorfalls in Ihren OT-Systemen verhalten und wen sie kontaktieren sollen?
34. Gab es im Zeitraum der letzten 3 Jahre für sämtliche Mitarbeiterinnen und Mitarbeiter Schulungsmaßnahmen zur Verbesserung des Bewusstseins für Cybersecurity (Cybersecurity Awareness) der OT-Systeme?
35. Sind in Ihrem Unternehmen geeignete Indikatoren/Maßnahmen zum frühzeitigen und/oder proaktiven Erkennen von Sicherheitsvorfällen in Ihren OT-Systemen vorhanden?
36. Führen Sie in Ihrem Unternehmen die Logdaten Ihrer OT-Systeme an zentraler Stelle zusammen?
37. Wenden Sie für Ihre OT-Systeme automatisierte Maßnahmen als Reaktion auf Cybersecuritys-Vorfälle an?
38. Haben Sie in Ihrem Unternehmen Maßnahmen definiert, um die Arbeitsfähigkeit eines OT-Systems nach einem Cybersecuritys-Vorfall wieder herstellen zu können?
39. Führen Sie in Ihrem Unternehmen regelmäßige Backups Ihrer OT-Systeme durch?
40. Haben Sie Assets und deren potenziellen Schutzbedarf der in Ihrem Unternehmen eingesetzten IT-Infrastruktur identifiziert?
41. Haben Sie eine Schwachstellenanalyse der in Ihrem Unternehmen eingesetzten IT-Infrastruktur durchgeführt?
42. Haben Sie eine Bedrohungsanalyse der in Ihrem Unternehmen eingesetzten IT-Infrastruktur durchgeführt?
43. Führen Sie in der IT-Infrastruktur in Ihrem Unternehmen eine durchgängige Netzsegmentierung durch?
44. Haben Sie in der IT-Infrastruktur in Ihrem Unternehmen die Netzwerksegmente durchgängig durch eine Firewall geschützt?
45. Haben Sie in der IT-Infrastruktur in Ihrem Unternehmen ein durchgängiges Identity- und Accessmanagement eingeführt?
46. Haben Sie Vorgaben und/oder Maßnahmen für die Übertragung und/oder Speicherung von Information/Daten zur Cybersecurity in Ihrem Unternehmen an?
47. Führen Sie in Ihrem Unternehmen die Logdaten Ihrer IT-Infrastruktur an zentraler Stelle zusammen?
48. Wenden Sie für Ihre IT-Infrastruktur automatisierte Maßnahmen als Reaktion auf Cybersecuritys-Vorfälle an?
49. Wenden Sie für Ihre IT-Infrastruktur Maßnahmen an, damit bereits aufgetretene Anomalien zukünftig verhindert werden?
50. Führen Sie in Ihrem Unternehmen regelmäßige Backups Ihrer IT-Infrastruktur durch?
51. Haben Sie Assets und deren potenziellen Schutzbedarf der in Ihrem Unternehmen eingesetzten OT-Infrastruktur identifiziert?
52. Haben Sie eine Schwachstellenanalyse der in Ihrem Unternehmen eingesetzten OT-Infrastruktur durchgeführt?
53. Führen Sie in der OT-Infrastruktur in Ihrem Unternehmen eine durchgängige Netzsegmentierung durch?
54. Haben Sie eine Bedrohungsanalyse der in Ihrem Unternehmen eingesetzten OT-Infrastruktur durchgeführt?
55. Haben Sie in der OT-Infrastruktur in Ihrem Unternehmen die Netzwerksegmente durchgängig durch eine Firewall geschützt?
56. Haben Sie in der OT-Infrastruktur in Ihrem Unternehmen ein durchgängiges Identity- und Accessmanagement eingeführt?
57. Haben Sie in Ihrem Unternehmen Maßnahmen zur Gewährleistung der Cybersecurity in der Supply Chain?
58. Führen Sie in Ihrem Unternehmen die Logdaten Ihrer OT-Infrastruktur an zentraler Stelle zusammen?
59. Wenden Sie Maßnahmen zur Erkennung von Anomalien in Ihrer OT-Infrastruktur an?
60. Wenden Sie für Ihre OT-Infrastruktur automatisierte Maßnahmen als Reaktion auf Cybersecuritys-Vorfälle an?
61. Wenden Sie für Ihre OT-Infrastruktur Maßnahmen an, damit bereits aufgetretene Anomalien zukünftig verhindert werden?
62. Führen Sie in Ihrem Unternehmen regelmäßige Backups Ihrer OT-Infrastruktur durch?

## Neue Technologien

63. Wie schätzt Ihr Unternehmen den aktuellen Wissensstand zu folgenden neuen Technologien in Ihrem Unternehmen ein?
64. Wie schätzt Ihr Unternehmen die Einsatzmöglichkeiten für die folgenden neuen Technologien in Ihrem Unternehmen ein?
65. Wie schätzt Ihr Unternehmen den zeitlichen Einfluss der nachstehend genannten neuen Technologien in der Arbeit in Ihrem Unternehmens-Sektor ein?
66. Wie schätzt Ihr Unternehmen den Veränderungseinfluss der nachstehend genannten neuen Technologien in der Arbeit in Ihrem Unternehmens-Sektor ein?
67. Wie schätzt Ihr Unternehmen das Cybersecuritysrisiko bei Einsatz der neuen Technologien in Ihrem Unternehmen ein?

## Demographie

68. Geben Sie bitte den Umsatz in Euro an, der am nächsten an den Umsatz in ihrem Unternehmen kommt
69. In welchem Sektor ist Ihr Unternehmen vorrangig tätig?
70. Sie haben keinen der genannten Sektoren angegeben
71. Fällt Ihr Unternehmen unter die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz

# Anhang 4: Interviewleitfragen

## Anleitung für Interviewer

### Vorbereitung

Wir empfehlen, dass jedes Interview mit 2 Personen durchgeführt wird: einem Interviewer, welcher einzig die Aufgabe verfolgt die Interviewfragen zu stellen und ggf., abseits der erarbeiteten Fragen, tiefergehende Fragen stellt, sowie einem Protokollanten, der alle wichtigen Informationen niederschreibt. Um das Protokoll zu vereinfachen, sollte im Voraus ein Protokoll-Bogen vorbereitet werden, welcher die geplanten Interview-Fragen enthält, sodass Äußerungen der Interview-Teilnehmenden stets der richtigen Frage zugeordnet werden können. In aller Regel genügen im Protokoll stichpunktartige Mitschriften des Gesagten, markante Zitate können aber ebenfalls eine wichtige Informationsquelle sein. Im Anschluss an das Interview sollte dieses möglichst zeitnah ausgewertet werden, solange die Aussagen noch frisch im Gedächtnis sind, da das Protokoll den Gesamteindruck im Regelfall nicht vollständig wiedergibt.

### Ziel des Interviews

Das Ziel des Interviews ist es, Erkenntnisse zu erlangen, welche die Ableitung von Handlungsempfehlungen an die Politik ermöglicht. Hierfür ist es entscheidend, das „Warum“ zu klären, also z.B. warum die Cybersecurity eines Unternehmens auf dem aktuellen Stand ist oder nicht. Hierfür ist es sowohl entscheidend, herauszufinden, was einer weiteren Verbesserung der Cybersecurity im Weg steht (fehlen beispielsweise Know-How oder finanzielle Mittel?) oder widerspricht (ist ein höheres Sicherheitsniveau womöglich gar nicht notwendig), als auch, was sie bisher gefördert hat (insbesondere bei Unternehmen mit einem hohen Reifegrad: was hat dabei geholfen diesen zu erreichen und könnte so auch für andere Unternehmen hilfreich sein?).

### Durchführung des Interviews

Während des Interviews soll sich der Interviewer an folgende Leitsätze halten:

- Es sollte sich möglichst wortgetreu an die Formulierung und Reihenfolge der Fragen aus dem Fragenkatalog gehalten werden. Dies dient der Vergleichbarkeit der Interviews.
- Das Ziel bei allen Fragen sollte sein, den Ursachen auf den Grund zu kommen. Hierfür sollte stets nach dem „Warum“ gefragt werden. (Beispiel: Wenn erklärt wird, dass im Unternehmen keine verantwortliche Person für IT-Sicherheit existiert, sollte der Grund hierfür herausgefunden werden. Mögliche Gründe könnten sein, dass es bisher keine Priorität dafür gab, der Bedarf nicht bekannt war oder die Kosten hierfür zu hoch waren. Diese Gründe sollten allerdings nur dann vorgeschlagen werden, falls den Interview-Teilnehmenden kein Grund einfällt! Grundsätzlich sollen diese ihre Gründe selbstständig nennen). Das „Warum“ sollte so lange wiederholt werden, bis man die Wurzel gefunden hat.
- Sollten die Interview-Teilnehmer außerdem ein Thema anschneiden, welches für unser Interview interessant ist, dürfen gerne weiterführende Fragen gestellt werden, welche nicht im Fragenkatalog enthalten sind.
    - In diesem Fall sollte stets nur eine Frage gleichzeitig gestellt werden. Das bedeutet auch, dass in jeder Frage nur eine Information abgefragt wird (Beispiel: „Ist das Internet in Ihren Augen sicher?“ statt „Ist das Internet in Ihren Augen sicher und nützlich?“)

    - Außerdem sollte bei der Formulierung der weiterführenden Fragen darauf geachtet werden, dass sie die Antwort nicht beeinflusst (Beispiel: „Bitte erklären Sie in eigenen Worten, was Ihrem Verständnis nach hierbei geschieht“ statt „Haben sie verstanden was hier geschieht?“. Letzteres führt zu einer höheren Häufigkeit der Antwort „ja“, auch wenn das Thema nicht verstanden wurde.)
    - Zum Zweck des Nachfragens ist bei den Interviewfragen eine Liste mit Stichpunkten geführt, welche für jede Frage potenziell von Interesse sein könnten. Diese besteht aus: Motivation, Expertise, Personalkapazität, einmaligen sowie laufenden Kosten und politischen, wirtschaftlichen und regulatorischen Rahmenbedingungen sowie Herausforderungen. Dies sind mögliche Faktoren, die eine Schwierigkeit der Cybersecurity darstellen können und als Denkanstoß für Interviewteilnehmende geliefert werden können, falls diese nicht selbstständig auf Faktoren kommen, welche der Cybersecurity in ihrem Unternehmen im Weg stehen.
- Genauso sollten weiterführende und klärende Fragen gestellt werden, falls eine Antwort sehr knapp oder unklar ausfällt. Die Interpretation durch den Interviewer sollte minimiert werden. (Beispiel: „Könnten Sie das nochmal in anderen Worten wiedergeben?“ statt „Ok, ich glaube ich verstehe, Sie meinen also…“)
- Es sollte immer eine möglichst neutrale Haltung zu dem Gesagten der Interview-Teilnehmenden eingenommen werden, also auch keine starke Reaktion auf Antworten durch den Interviewer erfolgen. Dies ist besonders wichtig bei sensitiven Themen und dient dazu, die Interview-Teilnehmenden nicht zu „verschrecken“. Hierbei sollte eine Haltung eingenommen werden als hätte man jede mögliche Antwort schon früher einmal gehört und könne daher von nichts überrascht werden.

# Einleitung

## Begrüßung und Vorstellung

*„Erst einmal Vielen Dank, dass Sie sich bereit erklärt haben, an unserem Interview teilzunehmen. Kurz zu uns: Wir, das sind [Namen des Interviewers/Protokollanten], sind Mitarbeiter*innen des [Name Ihres Unternehmens] und führen diese Interviews im Auftrag des Deutschen Zentrums für Schienenverkehrsforschung beim Eisenbahn-Bundesamt durch. Ich werde die Fragen stellen, während mein Kollege / meine Kollegin für das Protokoll verantwortlich ist.“*

## Hintergrund des Interviews

*„Noch ein paar kurze Sätze zum Hintergrund des Interviews: Das Interview stellt die zweite Hälfte eines zweistufigen Prozesses dar. Ihr Unternehmen hat bereits an der Onlinebefragung teilgenommen. Mit den heutigen Fragen möchten wir einige der bereits angesprochenen Punkte detaillierter besprechen und hierbei die Möglichkeit für offene Fragen nutzen, die der Online-Fragebogen nicht geboten hat. Daher werden sich die meisten der Fragen, die ich stellen werde, auf Ihre Antworten innerhalb des Online-Fragebogens beziehen.“*

## Datenschutzaspekte

*„Kurz noch ein paar Worte zum Datenschutz. Es ist uns sehr wichtig, vertrauensvoll mit Ihren Daten umzugehen. Daher werden keinerlei Informationen an Dritte weitergegeben. Die gesammelten Informationen werden ausschließlich in anonymisierter Form weiterverarbeitet und publiziert. Hierbei erhalten das DZSF und EBA ausschließlich einen Überblick über die befragten Unternehmen, aber keinen Einblick in die Ergebnisse einzelner Unternehmen.“*

### Einweisung der teilnehmenden Person

*„Noch ein paar Punkte zum Ablauf des Interviews. Das gesamte Gespräch ist für etwa eine Stunde angesetzt, Sie können das Interview aber natürlich an jedem Punkt abbrechen. Außerdem können wir selbstverständlich gerne zu jeder Zeit eine Pause einlegen, wenn Sie das wünschen.*

*Bitte scheuen Sie nicht davor zurück, sofort nachzufragen, wenn Ihnen im Verlauf des Gesprächs ein Begriff nicht geläufig oder eine Frage nicht klar sein sollte.*

*Sie können völlig frei und offen sprechen. Es gibt keine falschen Antworten, denn wir erhoffen uns hier eine Einschätzung aus Ihrer Sicht. Denken Sie dabei nicht unbedingt nur an die eigene Unternehmensstruktur, sondern auch daran, wie sich Abhängigkeiten von anderen Unternehmen sowie gesellschaftliche, politische und organisatorische Rahmenbedingungen auf Ihr Unternehmen auswirken.*

*Haben Sie noch Nachfragen, bevor wir beginnen?“*

## Interview

*Stichpunkte zum Nachfragen (falls nicht angesprochen):*

- *Motivation*
- *Expertise*
- *Personalkapazität*
- *einmalige sowie laufende Kosten*
- *politische, wirtschaftliche und regulatorische Rahmenbedingungen sowie Herausforderungen*

## Fragebogen

### Einleitende Frage:

Bevor wir fachlich einsteigen, würde es mich noch interessieren, was Sie zur Teilnahme an diesem Interview bewegt hat. Was wünschen Sie sich von uns, damit sich die Teilnahme auch für Sie gelohnt hat?

*Online-Fragebogen: Strategie vorhanden **(F12 auf 4 oder höher)** UND Reifegrad in dieser Kernfunktion hoch (4 oder höher)*

Aus dem Online-Fragebogen hat sich ergeben, dass Sie im Bereich der [Kernfunktion einfügen] bereits sehr gut aufgestellt sind. Was hat Sie dazu angetrieben oder Ihnen dabei geholfen, hier einen so guten Stand aufzubauen?

***Online-Fragebogen F13:** Cybersecurity-Beauftragter im Unternehmen vorhanden?*

**Nein**: Sie haben angegeben, in Ihrem Unternehmen gibt es zurzeit keinen Beauftragten für Cybersecurity. Was ist Ihrer Ansicht nach der Hauptgrund hierfür?

**Ja:** Sie haben angegeben Ihr Unternehmen hat einen Beauftragten für Cybersecurity. Können Sie mir bitte erläutern, in welchem Umfang diese Rolle vorliegt, also welche Aufgaben ihm obliegen?
[beantworten lassen, falls nicht angegeben: nur „Nebentätigkeit“ neben anderen Aufgaben oder eine volle Stelle]
Außerdem würde mich interessieren, wie Zusammenarbeit und Kommunikation mit dem Beauftragten in Ihrem Unternehmen stattfinden.

<Anschlussfrage falls zuvor nicht beschrieben:>

Könnten Sie mir noch eine kurze Beschreibung liefern, wie die Organisation der Cybersecurity in Ihrem Unternehmen stattfindet?

*Online-Fragebogen: Missmatch zwischen **Strategie (F12)** und Reifegrad für NIST-Kernfunktion (ein Missmatch liegt vor, falls der Reifegrad kleiner als 3 ist, obwohl eine Strategie vorliegt)*

Sie haben angegeben, dass Ihre Cybersecuritysstrategie unter Anderem Maßnahmen enthält, die ihnen dabei helfen *[Cybersecuritys-Risiken zu identifizieren / sich vor Cybersecuritys-Vorfällen zu schützen / Cybersecuritys-Vorfälle zu entdecken / auf Cybersecuritys-Vorfälle zu reagieren / sich von Cybersecuritys-Vorfällen zu erholen]*. Wie setzen Sie diese in Ihrem Unternehmen um?

*Online-Fragebogen: Einzelne Kernfunktion weit unterdurchschnittlich im Vergleich zu anderen Kernfunktionen (unterdurchschnittlich heißt hier: 2 oder mehr Reifegradstufen niedriger als die restlichen Kernfunktionen)*

Nun würde ich gerne noch auf Maßnahmen zu sprechen kommen, welche dazu dienen *[Cybersecuritys-Risiken zu identifizieren / sich vor Cybersecuritys-Vorfällen zu schützen / Cybersecuritys-Vorfälle zu entdecken / auf Cybersecuritys-Vorfälle zu reagieren / sich von Cybersecuritys-Vorfällen zu erholen]*. Hier ist aus dem Onlinefragebogen hervorgegangen, dass Ihr Unternehmen dazu keine oder nur wenige Maßnahmen verfolgt. Können Sie mir sagen, weswegen das so ist?

***Online-Fragebogen: F10** Welche Hindernisse stehen Cybersecurity im Weg?*

Sie haben angegeben, in Ihrem Unternehmen steht womöglich das fehlende *[Wissen / die Qualifikation der Mitarbeiter / Kapazitäten im IT/ OT Bereich / der wirtschaftliche Nutzen / die Finanzierung / Sonstiges]* einer verbesserten Cybersecurity im Weg. Dem würde ich gerne etwas tiefer auf den Grund gehen. Weshalb fehlt Ihrer Meinung nach die / das […]?

***Online-Fragebogen F4:** Welche Cybersecuritys-Maßnahmen verfolgt Ihr Unternehmen?*

**Für die Bereiche, in denen keine Maßnahmen angegeben wurde:** Sie haben angegeben, dass Ihr Unternehmen keine Maßnahmen zur *[Netzwerksicherheit / IT Sicherheit / OT Sicherheit / Softwaresicherheit / Hardware Sicherheit]* ergreift. Weshalb wurde sich dagegen entschieden, diese zu verfolgen?

*Online-Fragebogen: Werden in Ihrem Unternehmen Backups für die IT-Systeme **(F31)** / OT-Systeme **(F41)** / IT-Infrastruktur **(F52)** / OT-Infrastruktur **(F64)** durchgeführt?*

**Nur falls „Nein" geantwortet wurde:** Sie haben angegeben, dass in Ihrem Unternehmen keine Backups für *[IT-Systeme / OT-Systeme / IT-Infrastruktur / OT-Infrastruktur]* durchgeführt werden. Weshalb wurde sich hier dagegen entschieden, diese durchzuführen?

<antworten lassen>

[Falls noch nicht angesprochen: Haben sie alternative Maßnahmen, die Backup ersetzen?]

***Online-Fragebogen F15:** Sorgt Ihr Unternehmen dafür, dass alle Mitarbeiter*innen im Cybersecuritys-Bereich geschult werden?*

Nein: Sie haben angegeben, dass Mitarbeiter in Ihrem Unternehmen nicht für den Bereich der Cybersecurity geschult werden. Weshalb wurde sich dagegen entschieden?

Ja: Sie haben angegeben, dass Mitarbeiter in Ihrem Unternehmen für den Bereich der Cybersecurity geschult werden. Können Sie mir ein paar mehr Details zu diesen Schulungen geben?

[Frei antworten lassen, dann gegebenenfalls folgende Punkte nochmals ansprechen, falls sie nicht erwähnt wurden: Häufigkeit, Verpflichtung, Umfang, Wissens-Prüfung]

***Online-Fragebogen: NT2:*** *Einsatz neuer Technologien: Einsatz von <Cloud Dienste> oder <Virtualisierung, SDN, NFV> hoch (4 oder höher?)*

Aus dem Onlinefragebogen geht hervor, dass in Ihrem Unternehmen [Technologie einfügen] häufig zum Einsatz kommt. Welche Anwendungen werden hier schwerpunktmäßig genutzt?

***Online-Fragebogen: NT1:*** *Wissen um Neue Technologien & NT2: Einsatz Neuer Technologien*

**Falls Wissen 4 oder höher:** Sie haben angegeben, dass in Ihrem Unternehmen ein hoher Wissensstand zu den folgenden Neuen Technologien vorherrscht. Können Sie kurz erläutern, welche Stärken bzw Chancen Sie im Einsatz dieser Technologien sehen? *[Technologien einzeln abfragen]*

- Technologie 1: *[Technologie einfügen]*
- Technologie 2: *[Technologie einfügen]*

**Falls Wissen maximal 2 und Einsatz 4 oder höher**: Sie haben angegeben, die folgenden Technologien im Einsatz oder zumindest in der Pilotierung zu haben. Was wäre für Sie eine geeignete Unterstützung bei der Erschließung des hierfür notwendigen Wissens?

- *[Technologien einfügen]*

*Online-Fragebogen: NT1: Wissen um neue Technologien & NT2: Einsatz Neuer Technologien*

**Falls bei beiden Fragen 4 oder höher angegeben wurde:** Sie haben angegeben, die folgenden Technologien im Einsatz oder zumindest in der Pilotierung zu haben. Was sind aktuell oder waren in der Vergangenheit die größten Hindernisse, welche Sie beim Einsatz dieser Technologien überwinden mussten oder müssen?

- *[Liste der Technologien wird in Abhängigkeit vom Unternehmen definiert]*

*Online-Fragebogen: NT1: Wissen um neue Technologien & NT4: Veränderungseinfluss Neuer Technologien*

**Nur falls Wissen 4 oder höher und Veränderungseinfluss 4 oder höher**: Für die folgenden Neuen Technologien haben Sie einen hohen Veränderungseinfluss für die Arbeit in Ihrem Unternehmen eingeschätzt. Bitte erläutern Sie mir kurz, wie sich dies auf die Arbeitssituation Ihrer Mitarbeiter auswirken wird und wie diese Änderungen unterstützt werden können.

- *[Technologien einfügen]*

### Abschließende allgemeine Frage:

Haben Sie noch Wünsche an die Politik, womit diese Ihnen bei der Verbesserung Ihrer Cybersecurity behilflich sein könnte?

## Abschied und Dank

*„Damit wären wir von meiner Seite durch. Gibt es noch Punkte, die Sie gerne hinzufügen möchten?“*

<Zeit geben>

*„Sie hätten jetzt nochmal die Chance uns eine Rückmeldung zu geben, wie sie das Interview und den Online-Fragebogen bewerten und wie Sie sich bei der Beantwortung der Frage gefühlt haben.“*

<Zeit geben>

*„Dann danke ich Ihnen erneut für Ihre Zeit und Teilnahme! Bei Nachträgen oder Nachfragen können Sie uns jederzeit direkt kontaktieren.“*

[Den Interviewten Kontaktdaten zu Interviewenden zur Verfügung stellen]

*„Wir gedenken, die Studie im ersten Quartal des kommenden Jahres zu beenden und lassen Ihnen im Anschluss zeitnah die Ergebnisse für Ihr Unternehmen inklusive der versprochenen Checkliste mit möglichen Handlungsempfehlungen zukommen.“*

# Anhang 5: Beispiel eines unternehmensspezifischen Interviewfragebogens

## Einleitende Frage:

Bevor wir fachlich einsteigen, würde es mich noch interessieren, was Sie zur Teilnahme an diesem Interview bewegt hat. Was wünschen Sie sich von uns, damit sich die Teilnahme auch für Sie gelohnt hat?

Protokoll:

- [...]

## Frage 1:

Aus dem Online-Fragebogen hat sich ergeben, dass Sie in allen Bereichen der Cybersecurity bereits sehr gut aufgestellt sind. Was hat Sie dazu angetrieben oder Ihnen dabei geholfen, hier einen so guten Stand aufzubauen?

Protokoll:

- [...]

## Frage 2:

Sie haben angegeben Ihr Unternehmen hat einen Beauftragten für Cybersecurity. Können Sie mir bitte erläutern, in welchem Umfang diese Rolle vorliegt, also welche Aufgaben ihm obliegen? [beantworten lassen, falls nicht angegeben: nur „Nebentätigkeit“ neben anderen Aufgaben oder eine volle Stelle]
Außerdem würde mich interessieren, wie Zusammenarbeit und Kommunikation mit dem Beauftragten in Ihrem Unternehmen stattfinden.

<Anschlussfrage falls zuvor nicht beschrieben:>

Könnten Sie mir noch eine kurze Beschreibung liefern, wie die Organisation der Cybersecurity in Ihrem Unternehmen stattfindet?

Protokoll:

- [...]

## Frage 3:

Sie haben angegeben, in Ihrem Unternehmen stehen womöglich verschiedene Faktoren einer noch weiter verbesserten Cybersecurity im Weg. Dem würde ich gerne etwas tiefer auf den Grund gehen. Weshalb fehlt Ihrer Meinung nach: [einzeln abfragen]

Kapazitäten im Bereich der IT

Finanzierung

Protokoll:

- [...]

## Frage 4:

Sie haben angegeben, dass Ihr Unternehmen keine Maßnahmen zur IT Sicherheit ergreift. Weshalb wurde sich dagegen entschieden, diese zu verfolgen?

Protokoll:

- [...]

## Frage 5:

Sie haben angegeben, dass in Ihrem Unternehmen keine Backups für OT-Systeme und OT-Infrastruktur durchgeführt werden. Weshalb wurde sich hier dagegen entschieden, diese durchzuführen?

<antworten lassen>

[Falls noch nicht angesprochen: Haben sie alternative Maßnahmen, die Backup ersetzen?]

Protokoll:

- [...]

## Frage 6:

Sie haben angegeben, dass Mitarbeiter in Ihrem Unternehmen für den Bereich der Cybersecurity geschult werden. Können Sie mir ein paar mehr Details zu diesen Schulungen geben?
[Frei antworten lassen, dann gegebenenfalls folgende Punkte nochmals ansprechen, falls sie nicht erwähnt wurden: Häufigkeit, Verpflichtung, Umfang, Wissens-Prüfung]

Protokoll:

- [...]

## Frage 7:

Sie haben angegeben, dass in Ihrem Unternehmen ein hoher Wissensstand zu den folgenden Neuen Technologien vorherrscht. Können Sie kurz erläutern, welche Stärken bzw Chancen Sie im Einsatz dieser Technologien sehen? [Technologien einzeln abfragen]

Technologie 1: 5G

Technologie 2: Drahtlose Sensornetze

Protokoll:

- [...]

## Frage 8:

Für beide Technologien [5G & Drahtlose Sensornetze] haben Sie außerdem angegeben, diese bereits im Einsatz zu haben. Was sind aktuell oder waren in der Vergangenheit die größten Hindernisse, welche Sie beim Einsatz dieser Technologien überwinden mussten oder müssen?

Protokoll:

- [...]

## Frage 9:

Und schließlich haben Sie für die gleichen Technologien [5G & Drahtlose Sensornetze] auch einen hohen Veränderungseinfluss für die Arbeit in Ihrem Unternehmen eingeschätzt. Bitte erläutern Sie mir kurz, wie sich dies auf die Arbeitssituation Ihrer Mitarbeiter auswirken wird und wie diese Änderungen unterstützt werden können.

Protokoll:

- [...]

## Abschließende allgemeine Frage:

Haben Sie noch Wünsche an die Politik, womit diese Ihnen bei der Verbesserung Ihrer Cybersecurity behilflich sein könnte?

Protokoll:

- [...]