Sind Eisenbahn- und ÖPNV-Sektor fit für die heutigen Cybersecurity-Herausforderungen?

Cyberangriffe sind inzwischen auch im Eisenbahn- und ÖPNV-Sektor angekommen. Bisher fehlt ein Überblick, wie gut der Sektor sich in Bezug auf Cybersicherheit gerüstet hat. Das DZSF hat daher eine Studie beauftragt, um dies zu analysieren. Hierzu wurde der gesamte Sektor zu einer Befragung eingeladen. Die Studie zeigt großen Aufholbedarf im Gesamtsektor auf und leitet Handlungsempfehlungen zur Stärkung der Cybersecurity ab.

1. Motivation

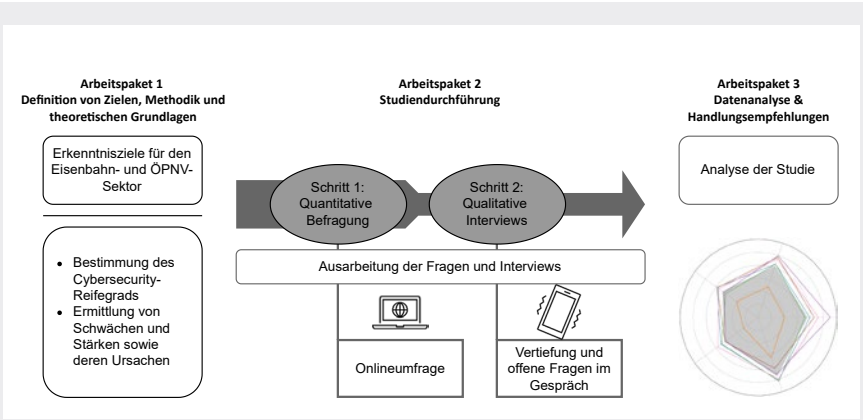
Waren Cyberangriffe vor zehn Jahren vielen Menschen nur aus Filmen bekannt, sind diese inzwischen im Bewusstsein der Öffentlichkeit angekommen. Regelmäßig wird berichtet, dass Cyberkriminelle Daten gestohlen haben oder Infrastrukturen durch Ransomware-Angriffe lahmgelegt wurden. Hierbei werden Trojaner in Systeme eingeschleust, die Daten verschlüsseln, und die Angreifer verlangen eine Überweisung in Form einer Kryptowährung zur Freigabe der Daten. Ransomware-Angriffe sind auch die erste Angriffsart, die Fahrgäste des öffentlichen Verkehrs betraf, als im Jahr 2017 zahlreiche Fahrkartenautomaten und Fahrgastinformationsdisplays dem WannaCry-Trojaner zum Opfer fielen, ihre ursprüngliche Funktion einstellten und nur noch die Lösegeldforderung anzeigten.

Diese Angriffsart reduzierte den Reisekomfort und erzeugte einen wirtschaftlichen Schaden. Aber auch wenn die Fahrgäste keine Tickets mehr erwerben konnten, war der Bahnbetrieb nicht betroffen. Andere Angriffsziele gehen darüber hinaus. Dabei sind bisher vorwiegend die nicht sicherheitskritischen Systeme Ziele von Angriffen geworden. So zielte ein Hackerangriff im Januar 2022 auf die belarussische Eisenbahninfrastruktur, primär auf das Dispositionssystem, ab. Die Hacker erklärten sogar explizit, dass sie keine Reisenden gefährden wollten [1]. Störungen der äquivalenten Systeme in den Niederlanden [2] und in Polen [3] haben zwar laut offiziellen Aussagen nichts mit einem Cyberangriff zu tun, zeigen aber, wie anfällig diese Systeme sind. Die Anschläge auf den Bahnfunk am 8. Oktober 2022 haben aufgezeigt, wie verwundbar unsere Infrastruktur gegenüber gezielten Attacken ist. Auch wenn es sich hierbei um einen rein physischen Angriff gehandelt hat, muss in der Zukunft mit Cyberangriffen und hybriden Angriffen (Kombination aus physischen Angriffen und Cyberangriffen) gerechnet werden. Cyberangriffe auf sicherheitskritische Infrastrukturen wie Stellwerke wurden

Dr. Lukas Iffländer
Referent Cybersecurity
Deutsches Zentrum für Schienenverkehrsforschung
iffländerl@dzsf.bund.de

Dr. Kristin Mühl
Referentin Human Factors
Deutsches Zentrum für Schienenverkehrsforschung
muehlk@dzsf.bund.de

Dipl.-Ing., Dipl.-Wirtsch.-Ing., MBA Michael Nord
Programm-Manager und CISO (Zert.), IABG
nord@iabg.de



1: Abfolge der Arbeitsschritte der Studie

bisher noch nicht erfolgreich bis zum Schadenseintritt durchgeführt oder öffentlich bekannt, bergen aber ein hohes Schadenspotenzial. Mit zunehmender Digitalisierung – deutsche Infrastrukturbetreiber führen derzeit digitale Stellwerke (DSTW) ein – wächst die Herausforderung, auch diesen Bereich abzusichern.

Entsprechend stellt sich die Frage: Sind Eisenbahn- und ÖPNV-Sektor fit für die heutigen Cybersecurity-Herausforderungen? Eine Literaturrecherche liefert wenige Ergebnisse. Am konkretesten ist der Bericht der Europäischen Agentur für Cybersicherheit (ENISA) [4]. Mit den 41 dafür befragten Unternehmen in ganz Europa ist diese Untersuchung jedoch nur beschränkt repräsentativ. Für die deutschen Sektoren ist die Aussagekraft nicht ausreichend.

Im Projekt „Studie Cybersecurity und Technologieeinsatz“ legt das Deutsche Zentrum für Schienenverkehrsforschung beim Eisenbahn-Bundesamt (DZSF) daher den Fokus auf das Cybersecurity-Bewusstsein im deutschen Schienenverkehr. Die Studie wurde im Rahmen der Auftragsforschung gemeinsam mit den Auftragnehmern Industrieanlagen-Betriebsgesellschaft mbH IABG (München), 3DSE Management Consultants GmbH (München), Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC (Berlin) und IFB Institut für Bahntechnik GmbH (Berlin) durchgeführt. Die Projektdurchführung gliedert sich dabei in drei Arbeitspakete (vgl. Bild 1). Ziel der Studie war es, eine möglichst repräsentative Übersicht zum Stand der Cybersecurity im Eisenbahn- und ÖPNV-Sektor in Deutschland zu erhalten. Dafür wurde als erster Schritt eine quantitative Befragung mit geschlossenem Antwortformat erstellt. Auf Basis der Rückläufe dieser Befragung wurde ein qualitativer Leitfaden für Interviews entwickelt, um ausgewählte Fragestellungen zu vertiefen und Diskrepanzen zu hinterfragen.

2. Methodik

2.1. Festlegung und Einladung der zu befragenden Unternehmen

Für die Studie wurden die Untersektoren (1) Eisenbahnverkehrsunternehmen (EVU), (2) Eisenbahninfrastrukturunternehmen (EIU), (3) Verkehrsverbünde und ÖPNV-Unternehmen, (4) Infrastrukturhersteller, (5) Fahrzeughersteller und (6) Fahrzeuginstandhalter, (7) Vertriebsplattformen, (8) Energieversorger und (9) Andere definiert und eine Liste mit entsprechender Klassifikation der Unternehmen erstellt. Die Liste zielt darauf ab, alle in Deutschland tätigen Unternehmen in den definierten Untersektoren abzubilden. Das Verzeichnis der beim Eisenbahn-Bundesamt (EBA) registrierten EIU und EVU ist die Grundlage für die Gruppen (1) und (2). Weitere Gruppen wurden auf Basis einer Marktrecherche sowie vorhandener Verzeichnisse des DZSF und der Auftragnehmer gebildet.

Die zu befragenden Unternehmen wurden alle schriftlich zur Beteiligung eingeladen. Weiterhin wurde über Branchenverbände (z. B. Verband Deutscher Verkehrsunternehmen und die Güterbahnen) sowie auf Veranstaltungen für die Teilnahme geworben.

Für die qualitative Befragung wurden auf Basis der Ergebnisse der quantitativen Studie Unternehmen ausgewählt, die exemplarisch für ihre Branche stehen oder außergewöhnliche Charakteristika aufwiesen.

2.2. Fragebogen- und Leitfadengestaltung

Der Fragebogen für die quantitative Studie orientiert sich an den fünf Kriterien aus dem Cybersecurity-Framework des amerikanischen National Institute of Standards and Technology (NIST) [6]. Diese sind (1) Identify (Identifizieren), (2) Protect (Schützen), (3) Detect (Erkennen), (4) Respond (Reagieren) und (5) Recover (Wiederherstellen). Zu jedem dieser Kriterien gibt es mehrere Fragen, deren Antworten in Summe die Bewertung des Kriteriums bilden. Die Antwortmöglichkeiten lassen sich dabei auf einer Skala von 0 bis 5 abbilden. Die Bedeutung der Stufen ist Tabelle 1 zu entnehmen. Zudem wurde erfragt, ob die Unternehmen zwischen operativer Technik (OT) und Informationstechnik (IT) unterscheiden. Bei OT handelt es sich um Systeme, die eine direkte Auswirkung auf die physische Welt haben, im Bahnbereich können dies z. B. Steuerungssysteme oder Stellwerke sein. Die IT-Systeme haben diese direkte Auswirkung nicht. Wird in den Unternehmen nach OT und IT unterschieden, wurden die Fragen getrennt zu diesen beiden Bereichen gestellt, anderenfalls wurde übergreifend gefragt. Zur besseren Differenzierung der befragten Organisationen wurden auch allgemeine Fragen zum Umsatz, der Mitarbeiterzahl und der Einstufung als kritische Infrastruktur nach KRITIS gestellt. Der entwickelte Fragebogen kann dem Forschungsbericht [5] entnommen werden.

Tabelle 1: Stufen des Reifegradmodells

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 die qualitative Befragung wurden einerseits Fragen basierend auf den Ergebnissen der quantitativen Studie erstellt. Dabei wurden Gründe für bestimmte Ergebnisse erfragt – z. B. um zu klären, warum sich das befragte Unternehmen besonders stark oder schwach einordnete. Weiterhin zielte die Befragung darauf ab, Widersprüche aufzulösen, z. B. wenn ein Unternehmen kaum Kosten für Security angibt, gleichzeitig aber eine vergleichsweise große Anzahl an Vollzeitäquivalenten für diese Aufgabe abstellt. Überdies wurden die Teilnehmenden für eine SWOT-Analyse (Strenghts, Weaknesses, Opportunities, Threats) nach Stärken, Schwächen, Chancen und Risiken beim Thema Cybersicherheit befragt. Zudem wurden in offenen Fragen Eindrücke, aber auch Wünsche und Anregungen an die Politik thematisiert. Der entwickelte Leitfaden kann dem Forschungsbericht [5] entnommen werden.

2.3. Durchführung der Befragung

Die quantitative Studie wurde in Form einer Onlinebefragung durchgeführt. Dazu wurde die browserbasierte Anwendung LimeSurvey verwendet. Die Umfrage stand insgesamt vier Monate von September bis Jahresende 2021 offen.

Die Interviews wurden anschließend mit den ausgewählten Unternehmen per Videokonferenz durchgeführt. Jedes Interview dauerte rund eine Stunde und wurde von zwei Interviewenden aus dem Kreis der Auftragnehmer durchgeführt, die sich Befragung und Protokollierung aufteilten.

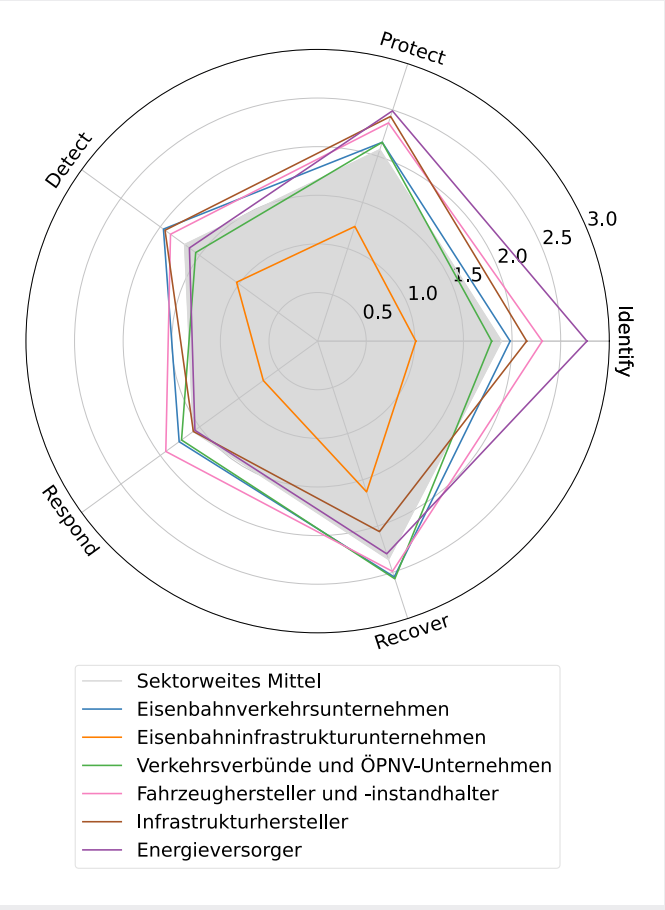
Tabelle 2: Verteilung der zur Teilnahme aufgerufenen Unternehmen, der Rückläufe der Online-Befragung und der ausgewählten Interviewteilnehmenden

	Stichprobe		Teilnehmer*			
			Online-Befragung		Interviews	
Untersektor	#	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 %
Andere	7	1 %	1	2 %	1	8 %
Gesamt	**715**	**100 %**	**60**	**100 %**	**12**	**100 %**

* Die Teilnehmer wählten in der Online-Befragung selbst den Sektor aus, dem sie sich zugeordnet sehen

Tabelle 3: NIST-Reifegrade der unterschiedlichen Untersektoren mit Konfidenzintervallen

Untersektor	Identify	Protect	Detect	Respond	Recover	Total
Eisenbahnverkehrsunternehmen (EVU)	1,98±0,72	2,15±0,71	1,96±0,74	1,76±0,73	2,55±0,73	2,10±0,74
Eisenbahninfrastrukturunternehmen (EIU)	1,01±0,81	1,24±0,76	1,03±0,83	0,69±0,61	1,63±0,96	1,15±0,83
Verkehrsverbünde und ÖPNV-Unternehmen	1,79±0,75	2,15±0,79	1,55±0,91	1,73±0,80	2,57±0,88	1,99±0,86
Fahrzeughersteller und Fahrzeuginstandhalter	2,31±1,04	2,36±1,15	1,87±1,09	1,93±1,12	2,49±1,06	2,24±1,10
Infrastrukturhersteller	2,15±2,26	2,43±0,91	1,94±2,05	1,58±1,55	2,06±1,99	2,12±1,94
Energieversorger	2,77±2,06	2,49±0,97	1,63±1,76	1,56±1,37	2,30±1,56	2,28±1,75
Andere	Zur Anonymisierung keine Detailangaben					
Gesamt	**1,89±0,42**	**2,07±0,04**	**1,69±0,43**	**1,58±0,40**	**2,36±0,43**	**1,96±0,42**



2: Reifegradvergleich der Untersektoren; zur besseren Erkennbarkeit wurde die Darstellung auf den Wertebereich bis 3,0 limitiert, da im Mittel kein Sektor über diesen hinauskommt

Für die Protokollierung erfolgte eine stichpunktartige Erfassung des Gesagten, welches durch relevante Zitate nach Ermessen der protokollierenden Person angereichert werden konnte. Durch die Auftragnehmer wurden die Erkenntnisse für die SWOT-Analyse unter Absicherung der Anonymität der befragten Unternehmen extrahiert und zusammengeführt.

3. Ergebnisse

3.1. Rücklaufquote

Von insgesamt 715 angefragten Unternehmen ergaben sich 60 vollständige Rückläufe. Deren Aufteilung kann Tabelle 2 entnommen werden. Bis auf die EVU bewegen sich die Anteile in einem akzeptablen Verhältnis zur Verteilung innerhalb der Grundgesamtheit. Der Anteil der EVU ist zwar niedriger als in der Grundgesamtheit, sie stellen aber trotzdem die größte Teilgruppe.

Die Rücklaufquote erreichte nicht das angestrebte Ziel, mindestens ein Zehntel jedes Untersektors abzudecken. Es ist allerdings möglich, die im Folgenden vorgestellten relevanten Aussagen zu generieren. Aus den Detaildaten lässt sich herauslesen, dass sowohl bezüglich der

Unternehmensgröße, als auch je Untersektor ausreichend diverse Unternehmen teilgenommen haben. So sind im Untersektor EVU beispielsweise sowohl kleine EVU mit unter zehn Vollzeitäquivalenten, als auch große EVU mit über 10.000 Vollzeitäquivalenten repräsentiert.

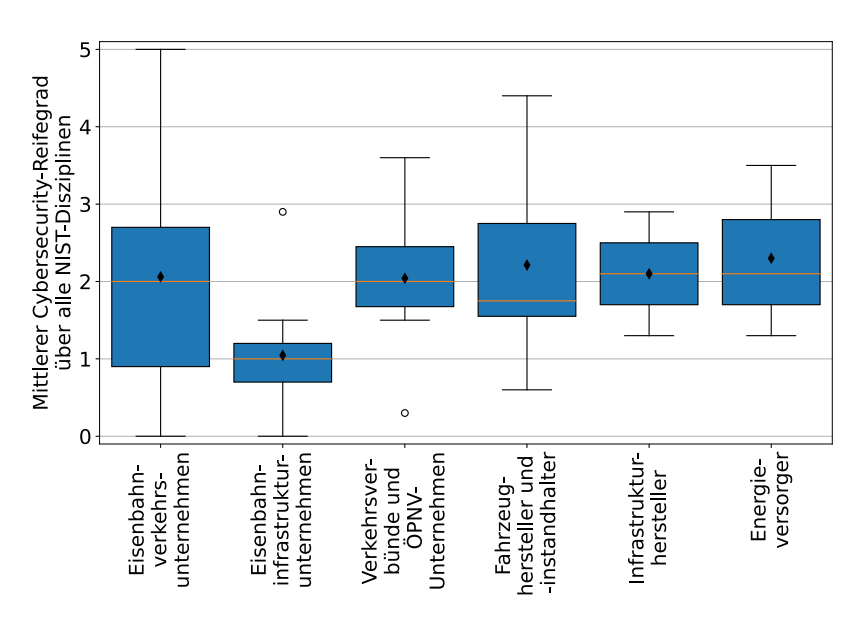
3.2. Security-Reifegrade

Für die Reifegrade wurden pro Untersektor der Mittelwert und das 95 %-Konfidenzintervall ermittelt. Diese sind in Tabelle 3 angegeben. Im Mittel liegt der gesamte Sektor bei Werten um 2,0, wobei die Disziplin Recover mit 2,36 besonders positiv und die Disziplin Respond mit 1,58 besonders negativ hervorstechen. Im Mittel über alle Kategorien wird ein Wert von 1,96 erreicht. Dies bedeutet, dass im Durchschnitt die Unternehmen schon einen Teil der Planung umgesetzt haben. Die teils hohen Konfidenzintervalle zeigen jedoch, dass es hier große Ausreißer nach oben und unten gibt.

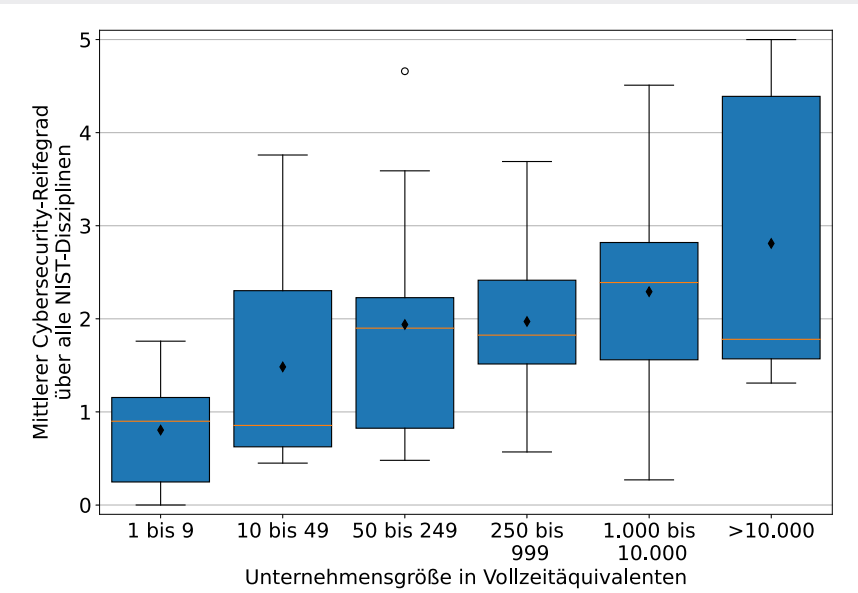
Bild 2 visualisiert die Reifegrade der einzelnen Untersektoren. Hierbei fallen zwischen den Sektoren bedeutende Unterschiede auf. Konsequent unterhalb des Branchenmittels sind hierbei die EIU. Die EVU sowie die Verkehrsverbünde und ÖPNV-Unternehmen sind weitgehend auf dem Branchenniveau. Die Infrastrukturhersteller sind in den Kategorien Identify und Recover teils deutlich weiter als der Rest der Branche, fallen dann aber etwas zurück. Bei den Energieversorgern bildet sich ein ähnliches Bild, wobei diese vergleichsweise hohe Werte bei Identify und Protect haben und in den anderen Kategorien etwa auf dem Branchenmittel liegen. Ohne Schwächen gegenüber dem Restsektor schneiden die Fahrzeughersteller ab, die in allen Disziplinen über dem Branchenniveau sind.

Wie Bild 3 zeigt, sind die Kompetenzen in vielen Untersektoren sehr unterschiedlich verteilt. Während die EIU über alle Kriterien gemittelt knapp den Wert von 1,5 erreichen (mit einem einzigen Ausreißer, der fast den Wert 3 erreicht), zeigen die anderen Untersektoren eine breite Verteilung. Besonders fällt dies bei den EVU auf, die zwischen 0 und 5 alle Einstufungen abdecken, was auf eine besonders hohe Diversität dieses Subsektors hindeutet.

Ein Grund der hohen Diversität ist die Unternehmensgröße. Bild 4 beleuchtet den gesamten Sektor nach Unternehmensgröße. Es zeigt sich, dass Kleinstunternehmen vergleichsweise schlecht abschneiden und kein einziges einen mittleren Wert von 2,0



3: Mittlerer Reifegrad nach Untersektor, dargestellt als Raute in den Box-Plots, die mittlere Linie (in der Box) stellt den Median dar, die obere und untere Kante der Box jeweils das 25 %- und das 75 %-Quantil, Kreise stellen Ausreißer dar



4: Mittlerer Reifegrad nach Unternehmensgröße, dargestellt als Raute in den Box-Plots, die mittlere Linie (in der Box) stellt den Median dar, die obere und untere Kante der Box jeweils das 25 %- und das 75 %-Quantil, Kreise stellen Ausreißer dar

erreicht. In der nächsten Größe verschiebt sich zwar das Spektrum nach oben, der Median verbleibt aber auf niedrigem Niveau unter 1. Erst ab 50 Vollzeitäquivalenten erhöht sich der Median, verbleibt aber auch bei größeren Unternehmen im Bereich von 2. Erst Unternehmen mit über 10.000 Vollzeitäquivalenten erreichen überhaupt die 5,0. Die Korrelation von Reifegrad und Unternehmensgröße erzielt einen Spearman-Koeffizienten von r = .42 und gilt demnach als mittelstarker Zusammenhang.

3.3. Ergebnisse der Interviews

Die Ergebnisse der SWOT-Analyse zur Cybersicherheit im Sektor können Tabelle 4 entnommen werden. Hierfür wurden die

Tabelle 4: SWOT-Analyse des Sektors zur Cybersicherheit

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

Kernaussagen aus den qualitativen Interviews extrahiert und sinngleiche Aussagen zusammengefasst.

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

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

In vielen Unternehmen ist im Hinblick auf das Cybersecurity-Bewusstsein die NIST-Kernfunktion Protect dadurch im Vergleich zu den anderen Kernfunktionen stärker ausgeprägt, dass diese Informationssicherheits- oder Datenschutzbeauftragte beschäftigen. Weiterhin sind bei mehreren Unternehmen entsprechende Sicherheitssysteme im Einsatz oder die Unternehmen betreiben eigene entkoppelte Netzwerke, wodurch der Grad der Cybersicherheit steigt.

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

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

- Der Cybersicherheit in den Unternehmen wird ein geringer Stellenwert zugeschrieben.
- Es mangelt an Verantwortlichkeiten für das Thema Cybersicherheit.
- 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 Interviewten verschiedene Gründe:

- Existierende Backup-Systeme sind veraltet.
- Es liegen hinderliche Vorgaben der Hersteller oder Regulierungsbehörden zur Wiederherstellung von Backups oder Ursprungskonfigurationen vor.

4. Fazit, Handlungsempfehlungen und Ausblick

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 IST-Zustands des Sektors.

Im Rahmen dieser Studie wurde festgestellt, dass viele Unternehmen des Sektors 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.

Die Hauptproblematiken sind demnach mangelndes Bewusstsein und

Motivation beim Management und Mitarbeitenden, ein genereller Mangel an qualifiziertem Personal, ein Fehlen von Orientierungspunkten und empfohlenen Vorgehensweisen.

Basierend auf den Reifegraden, der SWOT-Analyse sowie Rückmeldungen auf offene Fragen zu Wünschen bezüglich des Cybersecurity-Bewusstseins an die Politik, den KRITIS-Regularien und Förderungsmöglichkeiten wurden im Rahmen der Studie die folgenden Handlungsempfehlungen im Bereich Cybersecurity durch das Projektteam abgeleitet:

- Schaffung von Standards für Cybersecurity im Sektor analog zu den EBA-Checklisten für die Fahrzeugzulassung
- Verpflichtung von Support- und Updatekonzepten in Vergabeverfahren
- Stärkung des Bewusstseins für Cybersecurity beim Personal und auf Managementebene durch Branchenveranstaltungen und (ggf. verpflichtende) Schulungen
- Steigerung der Attraktivität der Branche für IT-Fachkräfte in Form der gezielten Bewerbung des Sektors im Curriculum und auf außerakademischen Veranstaltungen, aber auch durch Anpassung des Gehaltsniveaus der Branche
- Einmalförderungen für kleine und mittelständische Unternehmen zur Erreichung eines Cybersecurity-Basisniveaus
- Schaffung einer zentralen beratenden Cybersecurity-Ansprechstelle für Unternehmen im Sektor
- Einführung eines regelmäßigen Cybersecurity-Monitorings auf Basis dieser Studie unter Einbeziehung der Erfahrungswerte aus der Durchführung. Gegebenenfalls ist hierfür eine Verpflichtung notwendig, um eine bessere Rücklaufquote zu erhalten.

Die empfohlenen Maßnahmen sollen in möglichen Folgeprojekten des DZSF in ihrem potenziellen Aufwand-Nutzen-Verhältnis bewertet und weiter ausgestaltet werden. Das DZSF strebt ein regelmäßiges Monitoring an und engagiert sich darüber hinaus für die Stärkung der Kompetenzen und des Bewusstseins für Cybersicherheit. Ähnlich einer umfassend gelebten Sicherheitskultur in der Betriebs- und Arbeitssicherheit braucht es eine Cybersecurity-Kultur. Denn sonst gilt: „If it is not secure, it is not safe."

Literatur

[1] M. Mansholt, „Hacker knacken Bahn-System in Belarus – um Russlands Vormarsch auf die Ukraine zu stoppen", Der Stern, 25. Januar 2022. Zugegriffen: 21. Juli 2022. [Online]. Verfügbar unter: https://www.stern.de/digital/computer/ukraine--hacker-knacken-bahn-system-in-belarus---um-russlands-vormarsch-zu-stoppen-31568190.html
[2] tagesschau, „Nach Software-Panne: Züge in den Niederlanden stehen still", Tagesschau, Apr. 2022, Zugegriffen: 21. Juli 2022. [Online]. Verfügbar unter: https://www.tagesschau.de/ausland/europa/niederlande-bahn-software-panne-101.html
[3] W. Pluta, „Eisenbahn: Mutmaßlicher Computerfehler legt Züge in Polen lahm - Golem.de", Golem.de, März 2022, Zugegriffen: 21. Juli 2022. [Online]. Verfügbar unter: https://www.golem.de/news/eisenbahn-mutmasslicher-computerfehler-legt-zuege-in-polen-lahm-2203-163942.html
[4] D. Liveri, M. Theocharidou, und R. Naydenov, „Railway Cybersecurity", European Union Agency for Cybersecurity, ENISA, Nov. 2020. Zugegriffen: 21. Juli 2022. [Online]. Verfügbar unter: https://www.enisa.europa.eu/publications/railway-cybersecurity/@@download/fullReport
[5] M. Nord, B. Leppla, D. Möller, P. Krause, N. Lenski, und P. Czerkewski, „Studie Security und geplanter Technologieeinsatz", Deutsches Zentrum für Schienenverkehrsforschung beim Eisenbahn-Bundesamt, 2022. doi: 10.48755/dzsf.220011.01.
[6] National Institute of Standards and Technology, „Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1", National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 04162018, Apr. 2018. doi: 10.6028/NIST.CSWP.04162018.

Summary

Is the railway and public transport sector fit for today's cybersecurity challenges?

Cyber attacks have already been arrived in the railway and public transport sector. So far, there is no overview of how well the sector has been prepared in terms of cyber security. For this reason, the German Centre for Rail Traffic Research at the Federal Railway Authority (DZSF) has ordered a two-step study for investigation. For this, the complete sector has been surveyed. The study shows that there is a strong demand for improvement in the entire sector, particularly for the railway infrastructure companies, identifies reasons for obstacles and derives recommendations for actions.