# Cyberangriffe auf das Bahnsystem – Was bisher geschah

## Rückblick auf bisher entdeckte und dokumentierte Cyberangriffe gegen Teilkomponenten des Bahnsystems

**LUKAS IFFLÄNDER | THOMAS BUDER | BRIGITTE BUCHETMANN**

**Cyberangriffe bedrohen zunehmend kritische Infrastrukturen und damit insbesondere auch das Eisenbahnsystem. Für eine Bewertung der Bedrohungslage ist eine Bestandsaufnahme der bekannten Angriffe erforderlich. In diesem Beitrag wird die Methodik dieser Bestandsaufnahme beschrieben und werden die vorgefundenen Angriffe aufgelistet. Die gesammelten Daten werden analysiert und Schlüsse auf regionale Verteilung, die betroffenen Systeme und die Auswirkungen gezogen. Dabei ist ein Schwerpunkt im englischsprachigen Raum festzustellen. Die Mehrheit der Angriffe hat bislang keinen direkten Einfluss auf den Bahnbetrieb.**

### Einleitung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bewertet in seinem aktuellen Bericht zur IT-Sicherheit die Lage als angespannt bis kritisch [1]. Zu dieser Einschätzung gelangte es zum einen durch die festgestellte Ausweitung von Erpressungsmethoden und zum anderen durch die beobachtete neue Dimension des Wirkungsgrades von Cyberangriffen. Ferner vermitteln täglich rund 319000 neue Schadprogrammvarianten die Relevanz der Bedrohung solcher Attacken.

Schon allein aufgrund der Komplexität des Gesamtsystems, der großen Anzahl exponierter Schnittstellen und der Zugehörigkeit zur kritischen Infrastruktur stellt das System Bahn ein Ziel für Angriffe dar. Sowohl die Europäische Cybersecurity Agentur (ENISA) als auch das Deutsche Zentrum für Schienenverkehrsforschung (DZSF) beim Eisenbahn-Bundesamt haben dabei unabhängig voneinander ähnliche Herausforderungen speziell für das Bahnsystem festgestellt [2–4]:

- Während der fortschreitenden digitalen Transformation ist auf ein ausgeglichenes Verhältnis zwischen Wettbewerbsfähigkeit, betrieblichen Anforderungen und Cybersecurity zu achten.
- Eisenbahnunternehmen hängen von einer großen Anzahl an Zulieferern ab, auf deren Cybersecurity sie wenig Einfluss nehmen können.
- Die bisher eingesetzten operativen Technologien (OT) haben aufgrund ihrer Langlebigkeit Probleme, mit den modernen Anforderungen an die Cybersecurity kompatibel zu sein.
- Die Mitarbeiterkultur im Bahnwesen beschäftigte sich bislang wenig mit Fragen der Cybersecurity.
- Existierende Regulierungsanforderungen berücksichtigen nur in geringem Maße Aspekte der Cybersecurity.

| Feldkategorie | Feldname | Feldbeschreibung |
|---|---|---|
| Allgemeines | Datum | Tag des Angriffs, soweit genannt, in manchen Fällen geschätzt oder vertretend für ein Zeitintervall (durch * gekennzeichnet) |
| | Land | Land, in dem der Angriff stattgefunden hat |
| | Bestätigung | Hat das Unternehmen den Vorfall bestätigt? (Ja / Nein) |
| | | Falls nein, werden in der Auswertung nur die Informationen zu „Allgemeines" berücksichtigt. |
| Angriffsmittel | Supply-Chain-Angriff | Wurde nicht das Unternehmen selbst, sondern ein Zulieferer angegriffen? (Ja / Nein) |
| | Erpressung | Wurde das Unternehmen erpresst?[2] (Ja / Nein) |
| | verwendete Angriffsmittel | Angriffsmittel als Freitext, falls bekannt |
| | Name der Malware | Name der verwendeten Malware, auch Vermutungen, falls bekannt |
| | Kategorie | Kategorie des Angriffsmittels zur initialen Kompromittierung |
| Täter | | Freitextfeld für Angaben zum Täter, auch Verdächtigungen |
| Betroffene Systeme | unklar | Fehlen genaue Angaben zu betroffenen Systemen? |
| | interne Kommunikation | War die interne Kommunikation betroffen (E-Mail, Telefon etc.)? |
| | Kommunikation mit Fahrzeug | War die Kommunikation zwischen Triebfahrzeugführer und Zentrale gestört? |
| | Bezahlsystem | War das Bezahlsystem betroffen (Ticketautomaten, Einlasskontrolle, Ticketsystem)? |
| | Bahnhofs-IT | War die digitale Anzeige oder das Videoüberwachungssystem in Bahnhöfen betroffen? |
| | Disposition | Hatten die Betreiber Probleme, die Züge zu orten? |
| | Fahrgastinformation | Waren Fahrgastinformationssysteme (im Bahnhof, auf der Webseite oder der App) eingeschränkt? |
| | Webseite | Gab es falsche oder fehlende Informationen auf der Webseite, oder war sie gar nicht erreichbar? |
| | Daten | Wurden Daten angesehen, verschlüsselt, gelöscht oder gestohlen? |
| Konsequenzen | Bahnbetrieb | Kam es zu Verspätungen oder Ausfällen von Zügen? |
| | Daten veröffentlicht | Wurden gestohlene Daten der Öffentlichkeit zugänglich gemacht? |

**Tab. 1:** Spalten der Datenstruktur mit Erläuterungen

| Datum | Land | Bestätigung | Supply-Chain | Angriffsmittel | Name der Malware | Erpressung | Angriffsmittel Kategorie | Täter | betr. System unklar | Interne Kommunikation | Komm. mit Fahrzeug | Bezahlsystem | Bahnhofs-IT | Disposition | Fahrgastinformation | Webseite | Daten | Bahnbetrieb | Daten veröffentlicht |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 25.12.2014 | China | x | x | | | Nein | unklar | unklar | x | | | | | | | | x | | x |
| 01.07.2015 | UK | | | | | Nein | unklar | unklar | x | | | | | | | | | | |
| 23.12.2015 | Ukraine | | | | BlackEnergy3, KillDIsk | Nein | unklar | Sandwurm | x | | | | | | | | | | |
| 04.03.2016 | Südkorea | | | | | Nein | unklar | Nordkorea | x | | | | | | | | | | |
| 26.11.2016 | USA | x | | Schwachstelle | HDDCryptor | Ja | Exploit | @yandex.com | | x | | x | | | | | x | | |
| 13.05.2017 | Deutschland, Russland | x | | Exploit / Backdoor | WannaCry | Ja | Exploit | Lazarous Group | | | | x | x | | | | | x | |
| 27.06.2017 | Ukraine | x | x | Schwachstelle, Wiper | Petya | Ja | Exploit | unklar | | | | x | | | | | x | | |
| 01.10.2017 | USA | x | | | | Nein | unklar | unklar | | | | | | | | x | x | | |
| 12.10.2017 | Schweden | x | x | DDoS | | Nein | DoS | unklar | | x | | | | x | x | x | | x | |
| 18.11.2017 | USA | x | | | | Ja | unklar | unklar | | | | | | | | x | x | | |
| 23.01.2018 | Kanada | x | | Trojaner / Virus | | Nein | unklar | Nordkorea | x | | | | | | | | | | |
| 14.05.2018 | Dänemark | x | | DDoS | | Nein | DoS | unklar | | x | x | x | | | | x | | | |
| 15.01.2019 | China | x | x | | | Nein | unklar | unklar | | | | | | | | | x | | x |
| 27.01.2020 | USA | x | | | | Nein | unklar | unklar | | | | | | | | | x | | |
| 16.04.2020 | USA | x | | | | Nein | unklar | unklar | | | | | | | | | x | | |
| 07.05.2020 | Schweiz | x | | Ransomware, schwache Zugangsdaten | Nefilim | Ja | Passwort-angriff | unklar | | | | | | | | | x | | x |
| 02.07.2020 | USA | x | | Ransomware, Phishing | NetWalker | Ja | Social Engineering | Netwalker, Circus Spider | | x | | | | | | x | x | | x |
| 23.07.2020 | Spanien | x | | Trojaner / Virus, Ransomware | REvil | Ja | unklar | REvil | | | | | | | | | x | | x |
| 10.08.2020 | USA | x | | | | Nein | unklar | unklar | | x | | | | | x | | x | | |
| 28.10.2020 | Kanada | x | | Ransomware, Phishing | RansomExx | Ja | Social Engineering | unklar | | x | | | | | | x | x | | |
| 05.12.2020 | Kanada | x | | | | Ja | unklar | unklar | | | x | x | | | x | | x | | |
| 15.10.2020 | USA | x | | Ransomware, RaaS | Conti | Ja | Exploit | unklar | | | | | | | | | x | | x |
| 19.03.2021 | Tschechien | x | | | | Nein | unklar | unklar | x | | | | | | | | | | |
| 18.04.2021 | UK | x | | Ransomware | Lockbit | Ja | unklar | unklar | | x | | | | | | | x | | |
| 20.04.2021 | USA | x | | Exploit (zero-day) | | Nein | Exploit | unklar | x | | | | | | | | | | |
| 09.07.2021 | Iran | x | | | Meteor | Nein | unklar | Indra | | | | | x | x | | | | | |
| 20.07.2021 | UK | x | | | | Nein | unklar | unklar | | | | x | | | | | | | |
| 22.07.2021 | South Africa | x | | | Death Kitty | Nein | unklar | unklar | | | | | | | | x | | x | |
| 21.09.2021 | Indien | x | | | | Nein | unklar | IS | | | | | | | | x | | | |
| 24.10.2021 | Ukraine | x | | Drive-by (.exe), Ransomware | BadRabbit | Ja | Social Engineering | unklar | | | | x | | | | | | | |
| 29.10.2021 | Kanada | x | | | | Nein | unklar | unklar | | x | x | | | | x | x | | | |

**Tab. 2:** Liste der Cyberangriffe auf das Eisenbahnsystem

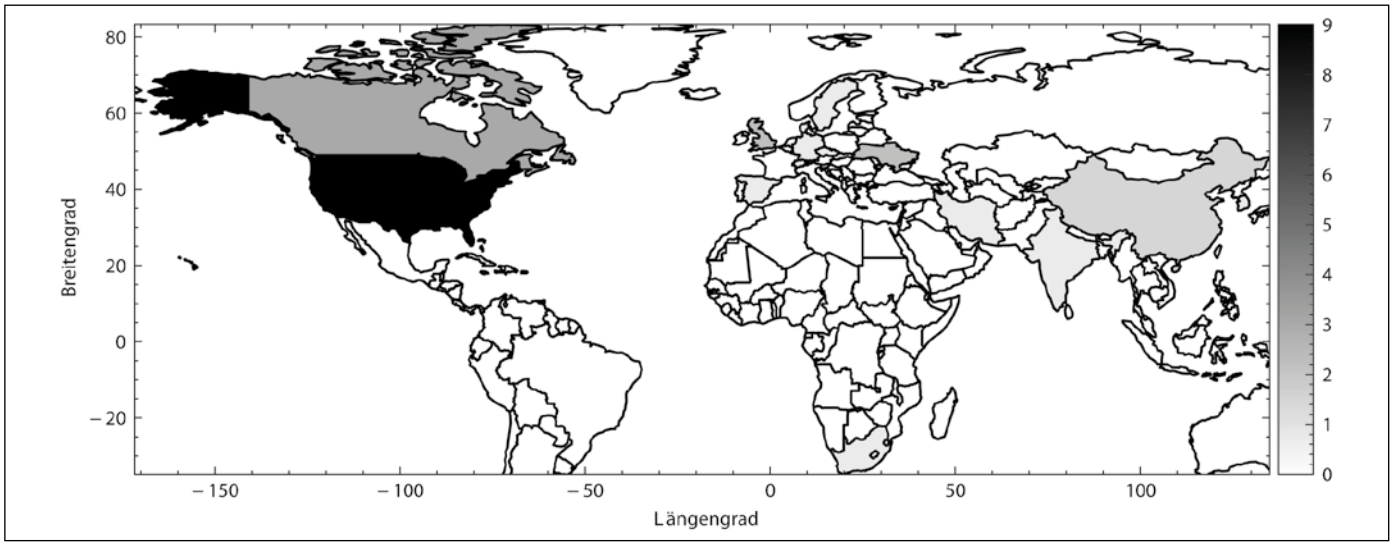


**Abb. 1:** Weltkarte aller bekannter Cyberangriffe auf das Eisenbahnsystem. Je dunkler ein Land eingefärbt wurde, desto mehr Angriffe sind bekannt.

Während sich diese Berichte vorwiegend mit den organisatorischen Herausforderungen beschäftigt haben und erste Lösungsvorschläge aufzeigen, bleibt offen, welche Systeme bereits erfolgreich angegriffen wurden.

Seit Anfang 2021 läuft daher im Auftrag des DZSF das Projekt „Identifikation bestehender Angriffspotenziale für das System Bahn" („Revealing Existing Attack Vulnerabilities in the Rail System", kurz REAVRS). Auftragnehmer sind die Universität der Bundeswehr in München, die Ingenieurgesellschaft für Verkehrs- und Eisenbahnwesen mbH (IVE mbH) und die CreaLab GmbH. Das Projekt beschäftigt sich mit Angriffspotenzialen auf das Eisenbahnsystem sowohl auf physischer als auch auf Cyberebene. Ein erstes Ziel des Projekts bestand dabei in einer historischen Aufarbeitung erfolgter Cyberangriffe.

Dabei wurden die Angriffe systematisiert und strukturiert, und der entstandene Datensatz wurde ausgewertet. Aus dieser Analyse lassen sich Schlüsse ziehen, welche Teilsysteme des Eisenbahnsystems bisher am häufigsten angegriffen wurden und welche Teilsysteme betroffen waren. Im Folgenden wird dargestellt, wie der Datensatz aufgebaut ist und welche Ergebnisse daraus abgeleitet wurden. Zunächst ist die Auswertung der Ergebnisse dargestellt. Danach werden die Einschränkungen diskutiert, und es wird abschließend ein Ausblick auf die weiteren Forschungen des DZSF gegeben.

## Methodik der Recherche und Datensatzstruktur

Gesucht wurde nach Angriffen auf IT- und OT-Systeme, die mit dem Schienenverkehr in Verbindung stehen. Systeme der Informationstechnologie (IT) umfassen den Einsatz von Computern zur Informationsverarbeitung und -verwaltung – im Eisenbahnkontext beispielsweise Vertriebssysteme. Operative Technologie (OT) steht für Systeme, die Maschinen oder Anlagen steuern, die für physische Prozesse verantwortlich sind – ein Eisenbahnbeispiel sind die Stellwerke. Diese Systeme können zu Eisenbahninfrastruktur- und -verkehrsunternehmen, aber auch zur Bahnindustrie gehören.

Der Zeitraum der recherchierten Cyberangriffe umfasste die Jahre 2014 bis 2021. An dieser Stelle soll dennoch auf den ersten bekannten Fall im Schienenverkehr – allerdings außerhalb der Vollbahnen – hingewiesen werden, der im Straßenbahnsystem von Łódź (Polen) bereits 2008 stattfand [5]. Dabei gelang es einem 14-Jährigen per Infrarot-Fernbedienung, die Weichenstellung zu manipulieren, was zur Entgleisung von vier Straßenbahnfahrzeugen und mehreren Verletzten führte.

Die Suche fand im Wesentlichen mithilfe der Suchmaschine Google statt. Suchbegriffe wurden auf Englisch eingegeben („cyber", „attack", „rail", „transport", „hacker" o. Ä.) und in variierender Anzahl und unterschiedlichen Kombinationen abgefragt. Dabei wurden folgende hilfreiche Dokumente identifiziert:

- der ENISA-Report Railway Cybersecurity [4]
- eine Liste von signifikanten Cyberereignissen seit 2006, herausgegeben vom Center for Strategic & International Studies [6]
- eine Liste von Cyberereignissen für den Transportsektor, herausgegeben von der University of Alabama [7]
- eine Liste von Cyberangriffen im Jahr 2021 für den Transportsektor, herausgegeben von der unabhängigen Beratungsfirma KonBriefing.com [8].

Die so recherchierten 31 Cyberangriffe wurden systematisch erfasst. Dazu wurden allgemeine Informationen, die relevanten Angriffsmittel, die Bezeichnung des oder der Täter, die betroffenen Systeme und die Konsequenzen erfasst. Tab. 1 erläutert die einzelnen Spalten der Datenstruktur. Anhand dieser Struktur wurde Tab. 2 erstellt, die einen verkürzten Überblick über alle Angriffe gibt. Zusätzlich zu dieser Tabelle werden nach Projektabschluss (voraussichtlich Q4/2023) ausführliche Informationen zu den Angriffen veröffentlicht.

## Auswertung

Nachfolgend werden die regionale Verteilung, die betroffenen Systeme sowie einzelne Eigenschaften der Angriffe betrachtet. Abb. 1 zeigt die regionale Verteilung der Angriffe. Es ist eine klare Häufung in den Vereinigten Staaten von Amerika festzustellen. Kurz dahinter folgen Großbritannien, Kanada, die Ukraine und China. In Indien, dem Iran, Südafrika und einigen bisher nicht genannten europäischen Ländern sind nur einzelne Angriffe zu verzeichnen. Einschränkungen hinsichtlich dieser Auswertung sind weiter unten im Abschnitt „Diskussion und Einschränkungen" aufgeführt.

Bei den ersten drei Ländern ist die sprachliche Zugänglichkeit der Systeme sicher ein Faktor. Die Anzahl der potenziellen Angreifer mit ausreichenden englischen Sprachkenntnissen dürfte vergleichsweise hoch sein, da Englisch als Standardsprache in der Informatik gilt.

Die vergleichsweise hohe Anzahl von Angriffen auf die ukrainische Eisenbahninfrastruktur ist im Kontext der russischen Besetzung der Halbinsel Krim und der Unterstützung der selbsternannten Volksrepubliken durch die Russische Föderation sowie späterer Versuche, die Gesellschaft und Wirtschaft der Ukraine im Vorlauf der russischen Invasion 2022 zu schwächen, zu sehen.

China weist eine höhere Zahl von Angriffen auf als Indien, obwohl beide Staaten über eine ähnliche Gesamtbevölkerung verfügen. Ein Faktor ist hier die stärkere Digitalisierung der chinesischen Systeme, da viele Strecken erst in den vergangenen Jahren errichtet wurden, während viele indische Strecken noch auf die Zeit der britischen Verwaltung zurückgehen.

Abb. 2 zeigt mehrere relevante Eigenschaften von Angriffen. Cyberangriffe erfolgen oft aus dem Verborgenen. In lediglich etwa 30 % aller Fälle gibt es einen vermutlichen oder nachgewiesenen Täter.

In etwa 40 % der Fälle handelt es sich um Erpressungsversuche. Die beliebteste Strategie ist dabei der Einsatz sogenannter Ransomwares. Diese

verschlüsseln ein System und fordern dann die Nutzer auf, Kryptowährungen zu überweisen, um die Daten freizukaufen. In vielen Fällen werden die Daten auch gar nicht verschlüsselt, sondern gelöscht. Das bekannteste Auftreten dürfte der WannaCry-Angriff im Jahr 2017 gewesen sein, als zahlreiche Fahrgastinformationsanzeigen und Verkaufsautomaten der Deutschen Bahn den Betrieb einstellten und nur noch eine Aufforderung zur Überweisung des Lösegelds anzeigten.

Eine wichtige Erkenntnis ist, dass in den wenigsten Fällen der eigentliche Bahnbetrieb signifikant beeinträchtigt wurde. Weniger als jeder zehnte Angriff war in dieser Hinsicht erfolgreich. Dagegen wurden in etwa jedem fünften Fall Daten entwendet und entweder öffentlich zugänglich gemacht oder im Darknet illegal zum Verkauf angeboten.

Die betroffenen Teilsysteme sind Abb. 3 zu entnehmen. Passend zur häufigen Veröffentlichung entwendeter Daten sind die Daten der Eisenbahnunternehmen ein beliebtes Ziel und bei über der Hälfte der Angriffe betroffen. Weiterhin sind die Webseiten der Unternehmen, die interne Kommunikation und die Bezahlsysteme stark betroffen, gefolgt von den Fahrgastinformationssystemen. Erst danach folgen die Kommunikation mit den Fahrzeugen, die Disposition und die IT der Stationen.

Insgesamt lässt sich daher sagen, dass Angriffe bisher primär auf Daten und „Komfortfunktionen" abzielen anstelle auf die direkte Steuerung des Eisenbahnsystems. Auch die Angriffe mit Auswirkung auf den Betrieb waren auf die Verfügbarkeit ausgerichtet. Das oft diskutierte Szenario: „Hacker stellt Signal auf Fahrt, obwohl ein Abschnitt belegt ist", ist bisher noch nicht vorgekommen.

## Diskussion und Einschränkungen

Die Ergebnisse zeigen, dass es für den Sektor sinnvoll ist, zusätzliche Ressourcen in die Absicherung der nicht betrieblichen IT-Systeme zu stecken, da diese bevorzugte Angriffsziele sind. Auch wurden mehrfach kritische Daten entwendet, sodass insbesondere auch Personal- und Kundendaten ein höheres Schutzbedürfnis haben.

Angriffe auf Komponenten der Leit- und Sicherungstechnik (LST) waren bisher noch nicht erfolgreich. Dies liegt sicher nicht nur daran, dass häufig kaum öffentlich dokumentierte Protokolle und Busse genutzt werden und einige in der LST eingesetzten Komponenten so alt sind, dass viele jüngere Angreifer dazu keinen Bezug haben, sondern auch an der hermetischen Trennung der genutzten Netze. Diese Trennung wird in Zukunft in vielen Fällen verschwimmen. Darüber hinaus soll das Internet Protocol (IP) bestehende Busse und Protokolle ersetzen. IP wird von vielen weit verbreiteten Hacking-Tools unterstützt, ist gut dokumentiert und gehört zur Grundausbildung in der Informatik. Daher ist es trotz bisher nicht erfolgter Angriffe empfehlenswert, aufgrund des möglichen Schadensausmaßes potenzielle Einfallstore proaktiv abzuriegeln.

Die dargelegten Daten und Ergebnisse sind nach bestem Wissen erhoben, unterliegen aber einigen Einschränkungen. Eine erste Einschränkung ist die Sprachauswahl. Die Suche erfolgte in Deutsch und Englisch. Potenzielle Angriffe, die nicht in einer dieser Sprachen und speziell in Sprachen ohne lateinisches Alphabet dokumentiert sind, können daher nicht erfasst werden. Da die englische Sprache in der Welt der Cybersecurity aber stark verbreitet ist, ist dieses Problem vermutlich gering.

Die gesammelten Informationen gehen nur dann mit allen Details in die Analyse ein, wenn eine entsprechende Bestätigung des betroffenen Unternehmens vorliegt. Laut Experten ist von einer immensen Dunkelziffer bei Cyberangriffen auszugehen [9].

Einige Fälle beruhen auf Aussagen von Geheimdiensten oder IT-Sicherheitsfirmen, bei denen von einer gewissen Befangenheit ausgegangen werden muss. Bei einem Angriff, in dem von offizieller Seite eine Schadsoftware namentlich genannt wird, wurden mitunter zusätzliche Quellen zu dieser Malware verwendet, um auf Angriffsmittel bzw. Täter zu schließen, auch wenn die ursprüngliche Quelle zu diesen Informationen keine expliziten Angaben macht.

Gerade in Bezug auf die Ukraine und Russland ist aufgrund des Kriegszustands mit einer hohen Zahl nicht bekannter oder nicht ausreichend

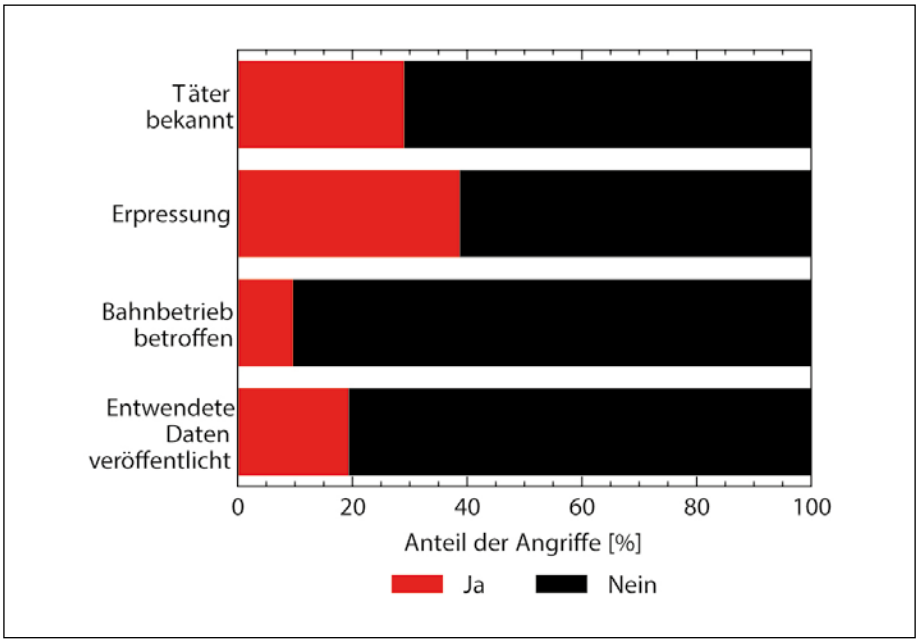


**Abb. 2:** Relevante Eigenschaften von Angriffen

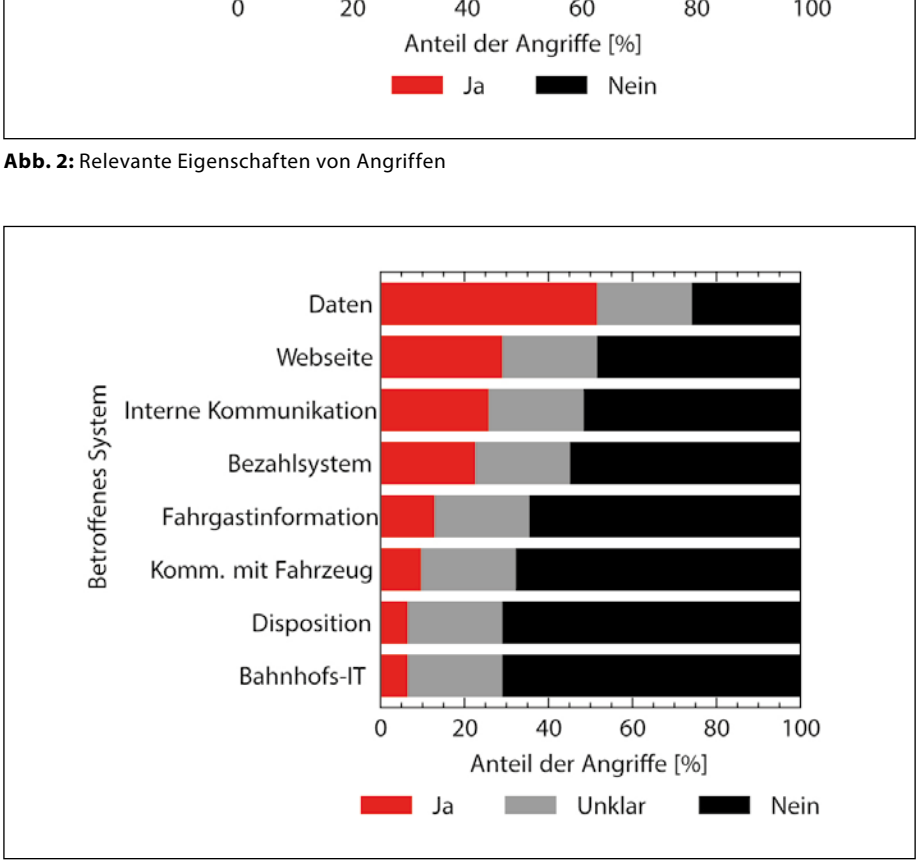


**Abb. 3:** Betroffene Teilsysteme

analysierter Angriffe zu rechnen, die – wenn überhaupt – erst mit der Zeit aufgearbeitet werden können.

## Zusammenfassung und Ausblick

Der Beitrag beschreibt die Methodik und die kondensierten Ergebnisse der Bestandsaufnahme des DZSF bezüglich zuvor beobachteter Cyberangriffe auf das Eisenbahnsystem. Dazu erfolgte eine Quellenrecherche mit Fokus auf Onlinequellen. Auf Basis der strukturiert dokumentierten Angriffe wurden regionale Schwerpunkte identifiziert, die Eigenschaften und Auswirkungen der Angriffe betrachtet sowie Erkenntnisse bezüglich der betroffenen Teilsysteme gezogen. Die Ergebnisse wurden eingeordnet und die Beschränkungen aufgezeigt.

Cyberangriffe sind ein noch junges Phänomen, die Entwicklung ist weiterhin zu beobachten. Das DZSF plant, nach Abschluss des Projekts die Details zu veröffentlichen. Die erstellten Datensätze sollen regelmäßig aktualisiert werden.

Parallel zu dieser Veröffentlichung wird ein Artikel zu den physischen Anschlägen auf das Bahnsystem in der Eisenbahntechnischen Rundschau (ETR) erscheinen. Ein besonders interessanter Kontrast ist hier regional zu sehen. Während es besonders viele physische Angriffe in Russland, Indien und Deutschland gab, liegt der Schwerpunkt der Cyberangriffe im englischsprachigen Raum. Ob hier ein dauerhafter Unterschied besteht oder sich beide Angriffsarten in ihrer regionalen Verteilung angleichen, ist Gegenstand zukünftiger Forschung. ■

## QUELLEN


[1] Die Lage der IT-Sicherheit in Deutschland. Bundesamt für Sicherheit in der Informationstechnik (BSI) (2022), verfügbar unter: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

[2] Möller, D.; Iffländer, L.; Nord, M.; Leppla, B.; Krause, P.; Czerkewski, P.; Lenski, N.; Mühl, K.: Cybersecurity in the German Railway Sector. In: Proceedings of the 17th International Conference on Critical Information Infrastructure Security (CRITIS 2022). Springer (2022)

[3] Nord, M.; Leppla, B.; Möller, D.; Krause, P.; Lenski, N.; Czerkewski, P.: Studie Security und geplanter Technologieeinsatz. Deutsches Zentrum für Schienenverkehrsforschung beim Eisenbahn-Bundesamt (2022), verfügbar unter: https://doi.org/10.48755/dzsf.220011.01

[4] 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

[5] Leyden, J.: Polish teen derails tram after hacking train network. The Register. (2008) , verfügbar unter: https://www.theregister.com/2008/01/11/tram_hack

[6] Significant Cyber Incidents | Strategic Technologies Program | CSIS, (2023), verfügbar unter: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[7] Transportation Cybersecurity Incidents. The University of Alabama (2019), verfügbar unter: https://ati.ua.edu/wp-content/uploads/2021/05/72.pdf

[8] Cyberangriffe 2021 nach Branche, (2022), verfügbar unter: https://konbriefing.com/de-topics/cyber-angriffe-2021-nach-branche.html#ind-transp

[9] Bundeslagebild Cybercrime 2021. (2022), verfügbar unter: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html



**Dr. Lukas Iffländer**
Wissenschaftlicher Referent
Deutsches Zentrum
für Schienenverkehrsforschung
am Eisenbahn-Bundesamt, Dresden
ifflaenderl@dzsf.bund.de

**Dr. Thomas Buder**
Wissenschaftlicher Referent
Deutsches Zentrum
für Schienenverkehrsforschung
am Eisenbahn-Bundesamt, Dresden
budert@dzsf.bund.de

**Dr. Brigitte Buchetmann**
Wiss. Mitarbeiterin
Universität der Bundeswehr München
brigitte.buchetmann@unibw.de

# IRSA 2023

SAVE THE DATE


# 4. International Railway Symposium Aachen

22. bis 23. November 2023
Im Eurogress, Aachen

**www.eurailpress.de/irsa2023**

Die großen Themen im Schienenverkehrssektor sind derzeit Dekarbonisierung, Automatisierung und die Erhöhung von Kapazität und Zuverlässigkeit. Strecken werden elektrifiziert oder Diesel-getriebene Züge zunehmend durch Batterie- oder Wasserstoff-gespeiste Elektroantriebe ersetzt. Dieser Trend ist nicht nur in Europa, sondern weltweit erkennbar. Zur weiteren Attraktivitätssteigerung sollen stillgelegte Strecken reaktiviert werden. Die Automatisierung, also das Fahren ohne Triebfahrzeugführer, ist bis auf Metro- und People-Mover-Netze noch im Entwicklungsstadium. Will man aber eine Verkehrsverlagerung auf die Schiene wirklich erreichen, so muss mangels Personal und zur besseren Ausnutzung der Infrastruktur dieser Pfad weiter verfolgt werden. Basis für mehr Kapazität auf der Schiene ist eine deutlich erhöhte Zuverlässigkeit von Fahrzeugen, Infrastruktur und Betrieb. Zu diesen wichtigen Themen wird an vielen Stellen weltweit geforscht.

Das nun wieder als Präsenzveranstaltung im Aachener Eurogress geplante 4. International Railway Symposium Aachen (IRSA) ist die ideale Plattform für einen intensiven Austausch der Fachleute zu diesen und weiteren aktuellen Themen. Traditionell adressiert die Veranstaltung die technischen Bereiche des Systems Bahn und auch der ÖPNV-Bahnen. Mit der Durchführung der Veranstaltung in Deutsch und Englisch bietet sie zudem ein Forum auch für internationale Vortragende und Gäste.

Weitere Informationen zur Veranstaltung auf der Website!



**VERANSTALTER**

Eurail press
EI ETR Rail
bahn manager RAILIMPACTS

**PARTNER**

RRR Research Center Railways | RWTH AACHEN UNIVERSITY